# Table of Contents

**User Manual** ................................................................................................................................. 3
  Introduction to DefenseStorm ............................................................................................................ 3
  Guardian ........................................................................................................................................... 4
  The DefenseStorm Virtual Machine .................................................................................................. 8
  Web Console ...................................................................................................................................... 23
  Dashboard ........................................................................................................................................ 28
  Creating your Profile ......................................................................................................................... 35
  Create a New User .............................................................................................................................. 36
  Two-Factor Authentication ................................................................................................................ 37
  Events .............................................................................................................................................. 39
  Alert Inbox ........................................................................................................................................ 49
  Triggers ........................................................................................................................................... 51
  Assets .............................................................................................................................................. 55
  PatternScout Engine ........................................................................................................................ 63
  Policy Reporting ............................................................................................................................... 65
  Integrations ....................................................................................................................................... 68
  ThreatMatch ..................................................................................................................................... 73
  Classifiers ....................................................................................................................................... 77
  Tickets ............................................................................................................................................. 80

**Release Notes** ................................................................................................................................. 85
  11.7.17: Windows Agent .................................................................................................................... 85

**Frequently Asked Questions** .......................................................................................................... 86

**Playbooks** ....................................................................................................................................... 99
  Compliance ...................................................................................................................................... 99
    DefenseStorm, Guardian, and the FFIEC ......................................................................................... 99
  Cybersecurity .................................................................................................................................. 128
    Alert Inbox: Best Practices ............................................................................................................. 128
    Suspicious Event in Dashboard ...................................................................................................... 131
  Troubleshooting ............................................................................................................................... 138
    DVM TroubleShooting .................................................................................................................... 138
    Alert Significance .......................................................................................................................... 151

**Download Links** ............................................................................................................................ 199

**Advanced** ...................................................................................................................................... 200
  Collecting Logs from Windows Machines ......................................................................................... 200
  Managing Powershell ........................................................................................................................ 215
  Windows Monitoring Installation Guide .......................................................................................... 218
  Setting up to receive SNMP Traps .................................................................................................... 223
  Configuring rsyslog to forward data ............................................................................................... 225
  Query Syntax ................................................................................................................................... 226
DefenseStorm communicates with your system through the DVM (DefenseStorm virtual machine) or the DWA (DefenseStorm Windows Agent) depending on your asset type. Once data reaches our cloud, it is pre-processed via classifiers and placed within a datastore. Triggers search through live data to generate an alert, incident, email, or a combination of the three.

Contact Us

There are a few different ways to contact DefenseStorm. You can contact us through Connect, Guardian, or the Knowledge Base.

- **Connect**: Technical issues with the product, DVM, or Web Console.
- **Guardian**: Security concerns or potential threats on your network.
- **Knowledge Center**: General questions on functionality, or request for additional documentation.
Guardian is our internal team of cybersecurity experts. They provide 24/7 monitoring and analysis of your network to help keep you secure, even after-business hours. Potential intrusions are monitored and analyzed in real-time, through historical trends, and threat sourcing feeds such as Infragard.

### Services Provided

- **Trigger development and maintenance.** *Any trigger you create requires a discussion between you and Guardian to discuss expectations before Guardian begins to actively monitor said trigger.*
- Classifier development and maintenance
- Log analysis
- ThreatMatch verification/analysis
- Gap analysis for potential instrumentation sources to improve visibility
- **Incident Management**
  - Analyze and Remediate open incidents
  - Assigning to customer when further action is necessary

### Unavailable Services

Guardian can only provide recommendations for network changes, not execution. For Example, Guardian cannot:

- Add blocks to your Firewall
- Block traffic from other countries
- Management of any device or appliance

### Ways to Contact Guardian

Copyright © 2015 - 2016 DefenseStorm, LLC. All rights reserved.
For any issues regarding your network security or alert questions, use the DefenseStorm Console to create an Incident. For example, if you want to know why you received an alert for ftp traffic, or what an alert means.

Go to the Incident page of your Console, and select the + sign.

Once the New Incident window displays, list Guardian as the Incident Owner and fill in any additional information or any questions you have. Select Create to finish the process.

You can also feel free to send Guardian an email or for an immediate response, call.

- Via email: guardian@defensestorm.com
- Via phone: 1-251-333-6557

What does Guardian need from you?

Guardian needs the following artifacts from you to efficiently monitor and analyze your network.

- Asset List
- Network diagrams
- Technical security controls inventory (NAV, AV, etc.)
- User List (phone & email)
- Security Policies
- Incident Response Plan
- Privileged Account Management
- Third Party Vendor Management

Guardian Service Level Agreement's (SLA'S)
The timelines listed in the table below are the maximum response times for Guardian to initiate triage for system incidents.

<table>
<thead>
<tr>
<th>System Generated Actionable Item</th>
<th>Severity</th>
<th>Response Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Incidents</td>
<td>High</td>
<td>2 hours</td>
</tr>
<tr>
<td></td>
<td>Medium</td>
<td>12 hours</td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td>Next Biz Day</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Contact for Escalation Cases**

In order to streamline the triage process, provide Guardian with who to contact and when, by filling out the escalation use case chart located in your Base Camp. Below is an example of the chart filled in.
After Hours
5pm - 8am EST

Critical?

Yes

No

Assign Incident to:
John Doe jdoe@email.com
Add as Watcher:
Jane Doe jadoe@email.com

How, and who?
Via Email no response in 10 min then via phone
1. John Doe jdoe@email.com 555-5555-5555
2. Jane Doe jadoe@email.com 555-5555-5555
3. Jerry Doe jedoe@email.com 565-565-5656

Business Hours
8am - 5pm EST

Critical?

No

Yes

How, and who?
Via Email no response in 10 min then via phone
1. John Smith jsmith@email.com 666-666-6666
2. Jane Smith jasmit@email.com 666-666-6666
3. Jerry Smith jsmith@email.com 666-666-6666
Why should I use the DVM to integrate my network?

Leveraging the DefenseStorm Virtual Machine (DVM) is the best practices strategy for integrating your network with the DefenseStorm Cloud solution. The DVM acts as a gateway, allowing you to send information to the DVM, which then securely sends the data to the DefenseStorm Cloud. The DVM accepts Syslog (both formatted and unformatted) for transferring data.

Have you Deployed the DVM Before?

Deploying your DefenseStorm Virtual Machine is part of our on-boarding process. It is done on-site via our DefenseStorm Install team. After the initial deployment, periodic updates are required to ensure you have the most up to date features. You are notified via Release Notes when DVM upgrades are recommended.

If you have already installed the DVM and just want to apply an update, follow the instructions below for Upgrading your DVM. If you need to install the system from the beginning, skip down to the section, DVM Installation, and follow the instructions for your host specifications.

Upgrading your DVM

Upgrading your DVM keeps your network protection up to date and have the best features. To determine if your DVM is eligible for upgrade, select Option 8: Get DVM Status, and view your version number. If your version number does not display, please open a support ticket for upgrade assistance. If a version number displays, complete the steps below.

Pre-Upgrade

There are a few steps required to ensure that your DVM environment is ready for a successful backup.

Which files need to be backed up?

To prevent any alterations to configuration files, we recommend that you back them up prior to upgrade, and restore them once the upgrade has completed. The following files should be backed up, if present, before initiating a DVM upgrade. This allows you to restore
configurations after the upgrade process in case any files are overwritten.

As listed in the table, some files may not be present on your network, therefore, they do not need to be backed up.

<table>
<thead>
<tr>
<th>Configuration File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/praesidio/praesidio.conf</td>
<td>This is the DVM's primary configuration file, and contains the provisioned DVM API key as seen in the web console.</td>
</tr>
<tr>
<td>/etc/syslog-ng/conf.d/praesidio.conf</td>
<td>This is the syslog-ng configuration file, generated during DVM servicing by the pConfig script.</td>
</tr>
<tr>
<td>Optional Files</td>
<td>The below files may not exist unless customized</td>
</tr>
<tr>
<td>/etc/syslog-ng/conf.d/snmp.conf</td>
<td>SNMP configuration files, generated / modified as part of DVM SNMP configuration. (See connect article for details)</td>
</tr>
<tr>
<td>/etc/default/snmpd</td>
<td></td>
</tr>
<tr>
<td>/lib/ufw/user.rules</td>
<td>User-generated firewall rules files for IPv4 and IPv6. This is modified during setup of SSH and SNMP, among other protocols.</td>
</tr>
<tr>
<td>/lib/ufw/user6.rules</td>
<td></td>
</tr>
</tbody>
</table>

**How do back them up through the DVM Menu**

The following steps create a folder called "dvm_yyyymmdd" in the ds user's home directory on the DVM, then backup the configurations listed in the table above to the folder.

In the DVM menu, select option (10) Bash Shell, then do the following:
<table>
<thead>
<tr>
<th>Type this Command</th>
<th>Action</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd ~</td>
<td>Enter</td>
<td>Navigate to the current user’s home directory.</td>
</tr>
<tr>
<td>mkdir dvm_20171025</td>
<td>Enter</td>
<td>Make new backup folder (change date portion to current date)</td>
</tr>
<tr>
<td>cd dvm_20171025</td>
<td>Enter</td>
<td>Navigate into new backup folder.</td>
</tr>
<tr>
<td>sudo cp /etc/praesidio/praesidio.conf .</td>
<td>Enter</td>
<td>Copy the /etc/praesidio/praesidio.conf file to here (the backup folder). Enter DVM login password if prompted.</td>
</tr>
<tr>
<td>sudo cp /etc/syslog-ng/conf.d/praesidio.conf .</td>
<td>Enter</td>
<td>Copy the /etc/syslog-ng/conf.d/praesidio.conf file to here (the backup folder).</td>
</tr>
<tr>
<td>-- optional section --</td>
<td></td>
<td>Ignore any copy failures for the below files; may not exist.</td>
</tr>
<tr>
<td>sudo cp /etc/syslog-ng/conf.d/snmp.conf .</td>
<td>Enter</td>
<td>Copy the /etc/syslog-ng/conf.d/snmp.conf file to here (the backup folder).</td>
</tr>
<tr>
<td>sudo cp /etc/default/snmpd .</td>
<td>Enter</td>
<td>Copy the /etc/default/snmpd file to here (the backup folder).</td>
</tr>
<tr>
<td>sudo cp /lib/ufw/user.rules .</td>
<td>Enter</td>
<td>Copy the /lib/ufw/user.rules file to here (the backup folder).</td>
</tr>
</tbody>
</table>
sudo cp /lib/ufw/user6.rules

Enter

Copy the /lib/ufw/user6.rules file to here (the backup folder).

**Increasing max_connections using Bash Shell**

If your host counts exceed 100 (for Unix / appliances) or 500 (for NXLog server installs, or Windows Agent installs on Windows workstations / laptops), we recommend increasing the max_connections option on your DVM.

The default ports, connection counts, and port uses are described below:

<table>
<thead>
<tr>
<th>Port</th>
<th>Max Connection Count</th>
<th>Port Description</th>
<th>Host Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 514</td>
<td>100</td>
<td>Standard RFC-compliant Syslog port.</td>
<td>Unix / Linux, appliances</td>
</tr>
<tr>
<td>TCP 516</td>
<td>100</td>
<td>Non-strict syslog port.  This is used for devices that send events over syslog, but whose formats do not comply with the RFC format. Cisco Meraki devices are an example of this.</td>
<td>Appliances (non-compliant)</td>
</tr>
<tr>
<td>TCP 601</td>
<td>500</td>
<td>Syslog port used by Windows NXLog clients.</td>
<td>Windows</td>
</tr>
<tr>
<td>TCP 1602</td>
<td>500</td>
<td>Syslog port used by the DefenseStorm Windows Agent.</td>
<td>Windows</td>
</tr>
</tbody>
</table>
If your host counts exceed 100 (for Linux / appliances) or 500 (for NXLog server installs, or Windows Agent installs on Windows workstations / laptops), you should modify the following section to increase the number of maximum connections. The default CPU and RAM amounts provisioned on the DVM image can support raising these counts up to 1500; if you need more concurrent connections than this, we suggest increasing the resources available to the VM instance first.

Steps to open the file, navigate to the configuration file section, and change the value are below. Select option 10: Bash Shell through the DVM Main Menu, and perform the following command steps.

<table>
<thead>
<tr>
<th>Type this Command</th>
<th>Action</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd /etc/praesidio/</td>
<td>Enter</td>
<td>Navigate to the DVM configuration directory.</td>
</tr>
<tr>
<td>sudo vi praesidio.conf</td>
<td>Enter</td>
<td>Open the praesidio.conf file in Vi. Provide DVM login password if prompted.</td>
</tr>
<tr>
<td>-- repeat next 5 steps for each count to change --</td>
<td></td>
<td></td>
</tr>
<tr>
<td>/tcp### (e.g. /tcp514)</td>
<td>Enter</td>
<td>Moves the edit cursor to the line for tcp### (if editing TCP514 counts, type /tcp514)</td>
</tr>
<tr>
<td>ww</td>
<td></td>
<td>Move the cursor two words to the right. Should be under the count number (100, 500) at this point.</td>
</tr>
</tbody>
</table>
If you make a mistake and need to revert all changes and restart from the original file, type the following sequence to quit without saving.

<table>
<thead>
<tr>
<th>Type this Command</th>
<th>Action (hit)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESC</td>
<td>Enter</td>
<td>Exit any edit modes</td>
</tr>
<tr>
<td>:q!</td>
<td>Enter</td>
<td>Quit without saving.</td>
</tr>
</tbody>
</table>

**Upgrade**

Once you have backed up all required configuration files and increasing the max_connections if necessary, follow the steps listed below to upgrade your DVM.

1. Access your DVM Main Menu.
2. Select Option 7: Update/Upgrade DVM.
3. Input your DVM console user (ds user) password when prompted. Text scrolls by on the screen during the upgrade process. Always accept the default options. Do you want to overwrite praesidio file, default is No, select this option. Deleting this file deletes all previous configurations and files.

4. Once the upgrade is finished, login to your console as usual.

DVM Installation

If you have never installed the DefenseStorm virtual machine, follow these steps based on your virtual machine environment. The DefenseStorm Virtual Machine (DVM) image is available for the following environments:

VMWare

You can obtain detailed information about deploying an OVA image directly from VMWare at the following location:

How to Install DVM VMware Image

To download the VMware OVA, follow the steps below:

1. Download the OVA
2. Deploy the OVA image to VSphere/ESXi
3. Power on the DefenseStorm Virtual Machine
4. Open the Console to begin configuration
5. Scroll down to Configuring the DVM, and follow the instructions.

**Hyper-V**

This section details the minimum recommended specifications for Hyper-V host servers to perform efficiently.

We recommend 2012 R2 and above. According to Microsoft, the end of life dates are as follows:

- Server 2012 R2 end of life is January 2020
- Server 2016 end of life estimated as 2025-2026

**Server Core install options**

As an alternative to a paid option, Hyper-V Server can be installed on a host to enable Hyper-V services on a headless server. This is a Server Core-based OS, and is command-line based.

Images are provided by Microsoft at the following URLs:


For all other SKUs, the Server Core install option can be used to further reduce the resources used by the host (reduces host OS storage footprint by ~4 GB) as long as no other roles are active on the Windows host; however, the VMs must be managed remotely or through PowerShell if this option is chosen. If this option is used, ensure that remote management is set up as part of provisioning the Hyper-V host.
**Windows Server Minimum Recommended Specs**

Note: These specifications assume that only remote management and the Hyper-V Server roles are enabled on the Windows Server install. Using this host for additional roles and/or services may require additional resources depending on which roles are enabled.

**OS SKU (select one):** Hyper-V Server (see below), Server Standard, Server Datacenter, Server Enterprise

**CPU:** multi-core, 64-bit CPU

- must support virtualization and DEP (data execution prevention)

**RAM:** 4 GB

- 2 GB RAM for hyper-v host, 1-2 GB for DVM

**Disk size:** 100 GB.

- Recommend sizing this higher if possible (200GB+) to allow for VM snapshotting and account for troubleshooting scenarios where DVM reprovisioning alongside an existing copy is necessary.
- 100 GB breakdown: minimum 32 GB for Windows install + 28 GB space for windows updates, 20 GB for DVM, and 30 GB free space for VM image upgrades.

**Network adapter:** Gigabit ethernet network adapter

- At least 10 Mb/s peak outbound network bandwidth to internet (Spikes of high event volume may require higher peak upload bandwidth to avoid queueing event data on the DVM).

**How to Install the DVM Hyper-V Image**

1. Download the zip file
2. Deploy the Hyper-V image to the Windows Server Host.
4. Open the Console to begin configuration.
5. Scroll down to Configuring the DVM, and follow the instructions.

**Configuring the DVM**

After you have installed the DVM via VMware or Hyper-V, follow these instructions to configure your DVM settings.

1. Log into the DVM console
   
   username: ds / password: defensestorm

2. Change the Password for the Console (forced by system)

   ```
   Ubuntu 14.04.4 LTS ubuntu tty1
   ubuntu login: ds
   Password:
   You are required to change your password immediately (root enforced)
   Changing password for ds.
   (current) UNIX password:
   Enter new UNIX password:
   Retype new UNIX password:
   ```

3. Configure Time Zone
   
   Select option 5 and then answer the questions regarding your local timezone
4. Configure Networking
   - Choose to enable DHCP
   - Set the static IP address.
   - Set the Netmask
   - Set the Gateway
   - Set the Nameserver 1, 2, and 3. If there is no Nameserver 2 or 3, then leave the field blank and select ‘OK’.

5. Set DefenseStorm Credentials
   - Input the Administrator email address.
Input the Administrator password. Once your credentials have been successfully created, you see the following message:

![Message](image)

6. Verify Network Connectivity

Option 6: Troubleshooting, then option 1: Connectivity Tests

![Menu](image)

Once the network tests have passed, you see the following message:

![Message](image)

7. Verify that the DVM is sending messages to the Console by verifying that the API key displayed through your web console and your DVM menu are the same.

Within your DVM, select option 8: Get DVM Status to view your API key.
After you have seen the api key through your DVM, open your Web Console to verify that events are coming through and are associated with the same api key. Go to Events, and select the API key from the filter options drop-down list.

Enabling DVM Event Compression

The DVM supports compression to help with limited egress bandwidth. Compression also helps in some instances where events were being dropped during ingestion. Log into the DVM and enter the following information.

1. Select option (10) Bash Shell
2. type `sudo vi /etc/praesidio/praesidio.conf` (Enter DVM logon credentials if prompted)

3. After config file is displayed, type the following:

<table>
<thead>
<tr>
<th>Type this Command</th>
<th>Action (hit)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/Flush</code></td>
<td>Enter</td>
<td>With cursor on the <code>/Flush</code> line, type the next command.</td>
</tr>
<tr>
<td><code>o</code></td>
<td></td>
<td>Creates new line for typing</td>
</tr>
<tr>
<td>Compress=True</td>
<td>Enter, ESC</td>
<td>This adds the command to the file and exits edit mode.</td>
</tr>
<tr>
<td></td>
<td><code>:wq</code></td>
<td>Hit Enter</td>
</tr>
</tbody>
</table>

When entered correctly, the command line looks like this:
4. Restart syslog-ng service with the new configuration file upon display of the command prompt.
   
   ```
   sudo service syslog-ng reload (hit enter)
   
   exit (hit enter)
   ```

   If syslog restarts without error, the compression feature has been successfully enabled.
All the great features offered by DefenseStorm are performed through the Web Console. This includes the Dashboard and all its features (See Dashboard), as well as Alerts, Policy, Assets, and more! For help logging into the console, see our Login FAQ. The Dashboard is the initial login page that shows a high level glance into your Network. The dashboard is made up of the following tiles:

- Events filter and examine events
- Network Connections geographically see network connections
- Incidents list of open incidents
- Total Events shows a total of how many events occur each day

Events

Events is an extremely powerful search engine that gives you the ability to investigate events thoroughly and efficiently. Queries can be as simple or complex as you make them using straightforward search query language. See Events for more detailed information.
Classifiers

Classifiers allow you to pre-process your data by creating fields, deleting data, and changing field values. See Classifiers for more detailed information.

Alert Inbox

Alert Inbox is a way to manage the alerts that your triggers generate. It was inspired by the "Inbox Zero* principles. It shows useful and actionable information that helps you respond quickly. See Alert Inbox for more detailed information.
**ThreatMatch**

ThreatMatch gives you the ability to turn on feeds and use Threat Intelligence Sources to identify risks. See [ThreatMatch](#) for more detailed information.

<table>
<thead>
<tr>
<th>Alerts</th>
<th>Triggers</th>
<th>Library</th>
<th>ThreatMatch</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Alerts" /></td>
<td><img src="image" alt="Triggers" /></td>
<td><img src="image" alt="Library" /></td>
<td><img src="image" alt="ThreatMatch" /></td>
</tr>
</tbody>
</table>

**Tickets**

The Tickets section of the dashboard is where you create incidents, or monitor and update existing incidents created by the system. See [Tickets](#) for more detailed information.
Policy

Policy utilizes built-in compliance tools that link your policies to system alerts and help you define, enforce, and report on your security policies.
Assets

Assets allows you to manage assets that are sending data to the DVM. The Assets page displays all tracked and untracked assets. An untracked asset is an asset that has not been officially added to the Console (by providing it with a name, IP, and hostname) but is still sending data to it. See Assets for more detailed information.
The Dashboard is a high level glance into your network made up of 4 sections including Events, Network Connections, Incidents and Total Events. To display highly-relevant information at a just a single glance. Seeing irregularities in your network has never been quicker.

### Events

Events is a graphical interface where you can filter and examine events. The interface displays the last 6 hours, totaled in the upper right of the graph. If you move your cursor to a particular spot on the graph, a window displays the time and events that occurred within the frame.

Events are filtered and displayed by Category or Severity.

- **Category** - defaults to the top 5 categories with the most events. See screenshot 1 below for example.
- **Severity** - displays None, Low, Medium, or High. See screenshot 2 below for example.
Click on the cog icon to add filters to the Events window by selecting New Search or choosing an already available filter.
If you select New Search, the dashboard brings up 3 fields at the bottom of the graph where you can name your search and include criteria in the Query row.
Once written, use the Test button to verify results. If satisfied, click Save to add the filter into the drop down selection list. Click anywhere on the data in the graph and you will be taken to the Events page for review.
Network Connections

Network Connections is a tool that allows you to geographically see activities pertaining to your Network.

You can zoom in and out on the map to view particular areas using the + / - signs. Click on a red circle to see the location. If you click on the location, all events for only that location display.

Tickets

Tickets provides a list of current open or watched Incidents. Clicking on an individual incident displays even more detailed information.
Total Events

Total Events shows a total of how many events occurred daily over a 7 day span. The counter on the upper right corner is a live count of events as they arrive in the console. Clicking on a specific bar in the graph takes you to the Search page to review your events for the day.
Creating your profile through the DefenseStorm Console couldn’t be easier. Simply click on the Settings logo (the gear icon) at the bottom left of your screen, and then select the Profile tab. This opens the Edit Profile window where you can fill in all desired information and enable two-factor authentication.

For more information on two-factor authentication, see [Two-Factor Authentication](#).
1. As a user with administrative privileges, log into the DefenseStorm Console and click on the Settings tab (gear icon) in the bottom left edge of console.

2. Click on the + icon button on the upper right side of the screen.

3. Complete the user form with desired information and click Save. After the user is created, they receive an email with simple instructions on how to complete setup.

The three user roles are:
- Administrator
- Power User
- User
- Read-Only User
Two-Factor Authentication

While enabling two-factor authentication is not required, it does provide an extra layer of security. During the on-boarding, installation process, 2FA is automatically set up for your organization. When creating new users after the install, it is recommended to enable 2FA on those accounts as well.

You sign in with something you know (your password) and something you have (a code sent to your phone).

Setting up two-factor authentication

To set up two-factor authentication as an individual user:

1. Select the Settings tab (gear symbol) at the bottom left of Console.
2. Select Profile and then the blue Set Up button to the right of Two-Factor authentication.

   ![Console Settings](image)

3. Instructions are displayed directly through the UI. Make sure to select the correct device type.
   The QR code and secret key are found on the Input Token page within Settings.

Using two-factor authentication

Once you have setup two-factor authentication, begin using it by following the steps below:
1. Sign into DefenseStorm with your email and password.

2. Verification code prompt displays:

```
Verification Code

Authenticate
```

3. Open the Google Authenticator app and enter the six - eight digit verification code. If the code is flashing red, wait until a new code appears in blue. Once the code is entered, you are fully logged into the system.
The Events page is a powerful search engine used to investigate network activity thoroughly and efficiently. DefenseStorm displays activity that generates a log (or alert) as an event. Your search queries can be as simple or complex as desired by using any one or a combination of the search methods explained in this article.

**Types of Events Displayed**

There are two types of events that display in the Console: log events and alert events. Log events are generated through the DVM each time an activity providing log information is performed. An alert event, or alert derivative, is generated each time an alert is triggered.

**Log Events**

The DefenseStorm DVM takes all logs generated from network activity and creates a searchable event that is displayed through the Console. These events can be used to create incidents, alerts, and triggers.

A majority of events displayed in the Console are log events. For a list of the most common and
Alert Derivatives (alert events)

The idea behind Alert Derivatives is to allow alerts to be searched for, alerted on, and monitored through the events page. This event type is a composite of all events that triggered the alert.

For example, if we had a query for geo_dest.country:china, and two users, Angela and Andrew had connected to a Chinese server in a given hour, the alert event would have both hostname: "John's PC" and hostname: "Angela's PC". A search in the console for hostname: "Angela's PC" geo_dest.country:china would return both the event that caused the alert to fire and the event for the alert.

Using Alert Derivatives

The Alert Derivatives functionality creates a centralized and simple way to view your alerts through the addition of the alert event. When searching through events, the alert events can easily be included or excluded by using category:alert.

<table>
<thead>
<tr>
<th>TIMESTAMP</th>
<th>MESSAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-12 17:45:00 PDT</td>
<td>Alert fired &quot;Ticket_Integration_Test&quot; with 85 events</td>
</tr>
<tr>
<td>api_key</td>
<td>ZrkH4MjJGN</td>
</tr>
<tr>
<td>api_key</td>
<td>St8BtmZNuU</td>
</tr>
<tr>
<td>app_name</td>
<td>DefenseStorm Agent</td>
</tr>
<tr>
<td>category</td>
<td>alert</td>
</tr>
<tr>
<td>hostname</td>
<td>192.168.100.23 (Untracked Asset)</td>
</tr>
<tr>
<td>message</td>
<td>Alert fired &quot;Ticket_Integration_Test&quot; with 85 events</td>
</tr>
</tbody>
</table>

Excluding Alert Events from the Platform

In some instances you may choose to exclude alert events from being searchable or alertable in the platform. This can be accomplished by creating a Classifier. Follow these steps:

1. Log into console and go to the Classifier section by following this URL:
2. Give the Classifier an intuitive name (e.g. “Remove Alert Event”).
3. Select the checkbox to “Drop Event”.
4. Save the Classifier. Here is an example of how the Classifier may look:

Excluding alert events from queries

In some instances you may want to ingest Alert events, but exclude them from queries. To do so, include the following flag to your query:

```
$category:alert
```

Alert Event Fields

In addition to all log event fields, alert events also contain the following:

- **timestamp** - the beginning of the interval that we alerted upon
- **category** - always "alert"
- **trigger_name** - the user-friendly name of the trigger
- **trigger_id** - the internal GUID of the trigger
- **trigger_query** - the query string for the trigger
- **trigger_interval** - the number of seconds in each trigger interval
- **severity** - high/medium/low, copied from the trigger
- **event_count** - number of hits in the search that fired the trigger
The following information (found in the original log events) will not be duplicated to the alert event:

- message
- timestamp
- ingest_timestamp
- event_count
- unparsed_expanded_message
- unparsed_message
- raw_message
- praesidio_parse_nanos
- percolator_tag

Searching Events

DefenseStorm provides several different methods for searching through events. These search methods can either be used on their own, or combined together for the most specific, narrow results. The methods of searching are:

- Query Syntax
- Time frame
- Event spike
- Filter options
- Aggregation

Query Syntax

The DefenseStorm Events page follows the format of ElasticSearch "Query String Queries". For details regarding Query Syntax, see the article, DefenseStorm Query Syntax. For help within the console, select the question mark icon to the right of the search bar. The icon displays example search terms.
Time Frame

The DefenseStorm Events page provides a calendar to narrow down your events by time frame. If you want all events for a specific day, select During to update the calendar to your desired day. The calendar also allows you to select a smaller time frame, such as Last Hour, or Last 3 Hours.

Event Spike

Within the Events page, it displays a graph with all received log events. If you see suspicious activity through the graph, you can drag the bars to display only events associated with the suspicious activity.
Filter Options

Within the DefenseStorm Events page, there is the option to search through events by filtering. To search by filtering, drill-down through the filters and select the desired checkboxes to display only associated events.

Aggregation

The Aggregate feature allows you to group your events before searching to greatly reduce the number of events displayed; therefore increasing result speed and accuracy.

1. Enter an Aggregate Field

2. In the screenshot below, the events have been grouped by the primary aggregate field:
From here you can either select one of the displayed account domains, or add a secondary field to further narrow down the displayed domain events.

The default view when both the primary and secondary fields are utilized, is the Spreadsheet View (as shown above). To simplify your view, select Compound from the View drop-down list. The Compound view allows you to better understand the relationship between the values of your two aggregate fields by displaying them side-by-side with their associated event count.

3. Select the Desired result to view events

Once you click on the desired compound result, in this example, account_domain:postilionoffice and user_domain:postilionoffice, a filter is applied to all events and the 56 events display.
Saving a search

Saving your search allows you to reuse all methods of searching without having to fill in the fields. For example, if you used a combination of Aggregation and Query Syntax, saving the search allows you to select the search without having to reapply the primary/second aggregate fields and the search query. The option to save your search is in the top right of the event graph.

![Event graph with saving search highlighted](image)

To view all previously saved searches, select Saved Searches from the top navigation of the Events page.

![Saved Searches page](image)

The Saved Searches page displays the name of your search, the date it was created, and gives you the option to edit your search. Selecting a search takes you to the Events page and applies the saved search parameters.

Create a new Incident

If the results of an event search are something you would like to further investigate, or send to Guardian to investigate, you can create a new incident directly from the Events page. Select Incident > New Incident. This displays the New Incident window where you fill-in the desired fields, and select Create to complete.
Create a Trigger

To receive an alert the next time an event matching your search parameters comes through the console, create a Trigger. Select Trigger within the events page. This takes you to the Alert > Trigger page where you fill-in desired fields, and select Save to complete.

Create a Classifier

If the results of your search parameters are something you would like to modify using metadata, create a classifier. Select Classifier from the Events page. This takes you to the Events > Classifier page where you fill-in desired fields, and select Save to complete.
Download a CSV

If you select to export a CSV from the main Events page, it downloads the first 10,000 event results. To create a CSV export with a smaller number of events, you can export a CSV during any stage of searching. The CSV option exports all events matching your search parameters.

Copyright © 2015 – 2016 DefenseStorm, LLC. All rights reserved.
Alert Inbox is a way to manage the alerts generated by active triggers, PatternScout, or ThreatMatch. Inspired by the 'Inbox Zero' principles, it was designed to stay empty. We follow this principle by providing different states for organization of all alerts. Once an alert is fired, it shows up as New in the Alert Inbox. During alert investigation, click ✓ (acknowledge) to send it from the New folder, to the Acknowledged folder. This signifies that the alert is no longer new, but has not been handled or completed.

Viewing Associated Events

To view the events associated with an alert, simply click on the number next to Count. This opens the Events tab with all events related to the alert.

Handling an Alert

After an alert has been investigated, move it to one of the following Handled states:

- Escalated generates an incident ticket, which takes over as the final destination for that
alert. Even though it creates an incident, it can still be marked as False Positive if that is the result.

- **False Positive** means the trigger that generated the alert shouldn’t have fired. Maybe the query needs to be tuned, or the thresholds, or maybe anomaly detection detected a deviation that wasn’t malicious. Be careful marking an alert is a false positive because it affects future anomaly detection.

- **Dismissed** is the middle ground, where it’s not an incident, but also not a false positive.
Triggers

Triggers are used to track events based on query strings; when a condition is met or an anomaly is detected, an alert is sent to the Alert Inbox. In addition to receiving an alert through the alert inbox within the console, you can also select to have an email sent to your personal account, or have an incident created automatically. For example, if you have come across a bad IP in the past, you could create a trigger to automatically create an incident for Guardian to begin investigation or remediation. The faster you receive an alert, the faster you can identify and stop a threat.

Guardian, our internal security team, has created a library of triggers that come default on your console. These triggers are created based off their cybersecurity expertise and customer requests.

Adding / Modifying Triggers

There are two different ways to add triggers on your network. You can modify triggers from the trigger library, or create your own from scratch. Triggers from the library can be copied to your network and edited to provide customized triggers for your network.

Whether you decide to use a base trigger from the library, or to create you own, the following fields can be filled in and/or modified:

Search Query

- **Query String**: Conditions trigger is set to search on. Include `category:alert` in the query string to prevent duplicate alerts. For more information on query strings, see XXXXXXXXXXX.
- **Aggregate**: Field to group by. For example, if you want to create a trigger to fire if a larger number of alerts for a specified username go off, you would enter `user_name` in this field.
- **Function**: How the number of alerts display.
  - Count (default)
  - Average
  - Count distinct
  - Max
  - Min
Information

- **Trigger Name:** Choose a meaningful name for quick identification. Append your custom trigger with your company initials.
- **Description:** Displays within your list of triggers, so make it a short, simple explanation of why you created this trigger.
- **Severity:** How critical this trigger is. Options are None, Low, Medium, or High.

Schedule

- **Interval:** How often the alert should run. It is recommended to select a field here to reduce noise and alert overload. *Once a Trigger is saved you cannot modify the interval as it affects the anomaly detection. To edit an interval, simply clone the trigger and adjust it.*

Alert Conditions

- **Alert Conditions:** Limits the number of events in a specified interval. Anomaly Detection learns user normalities, and creates a trigger if the user norm is deviated from.
- **PatternScout:** Options to enable dynamic thresholds and the PatternScout anomaly detection.

Tags

- **Tags:** Add searchable tags to your triggers for quicker searches and enhanced reporting.

Notifications

- **Email Notifications:** User email you would like to send an alert to. To add multiple addresses, click the + sign for another row.
- **Create an Incident:** Selecting an owner creates an incident when trigger criteria is met.

Results Fields to include in Email

- **Result Fields to Include in email:** If there are particular field values you would like included in the alert, add them here. For details on fields that can be included in the email, see our
Policy

- **Policies:** Triggers can be linked to a specific policy for metrics and reporting.

Creating a new trigger

1. Select Alerts > Triggers.
2. Click the + at the far right of the screen.
3. Complete the trigger form by filling in all desired fields based on the information provided above.
4. Select Save to enable the trigger.

Adding a trigger from the library

1. Select Alerts > Library to display the list of trigger groups.
2. Click on the desired group to display individual triggers.
3. Select the checkbox(es) of the triggers you wish to copy to your network.
4. Click Copy Selected.
5. Go to Alerts > Triggers and click on the trigger copied to your network.
6. Review and modify the trigger as desired. Select Save to enable the trigger.

Modifying a trigger

1. Go to Alerts > Triggers.
2. Select the trigger you wish to modify.
3. Modify fields as desired. Select Save to enable the modified trigger.
Searching Triggers

You can search through triggers to create a more manageable and useful list for reporting or tracking purposes.

1. Select Alerts in the left navigation and then Triggers.
2. Filter your triggers as desired using Search, and the Status/Severity filters.
3. Select the cloud icon to generate the CSV of filtered triggers.
4. Save as an Excel sheet and format as desired for reporting.
The Assets page automatically displays all assets sending data to the DefenseStorm Console via IP address, MAC address, and hostnames. If an asset is sending data to your console, but has not been manually added or properly uploaded prior to data ingestion, it displays as an untracked asset. For the best results, track/merge or investigate all untracked assets.

**Setup, Configuration, and Importation of Assets**

Importing your assets is typically done during the DefenseStorm on-boarding process, but there are several other instances where it may be necessary as well. For example, infrastructure changes such as upgrading hardware, routers, or switches may create the need to import your asset list. If your list of assets becomes unmanageable due to a high number of untracked assets, it may also be best to re-import.

Assets was designed to work with your network. With that in mind, there are different requirements for each network type: static, DHCP, or a mixed network. Most networks are considered mixed.

**Special considerations**

- If your network is mixed, or DHCP, then NXLog is required.
- Hostnames include the following:
  - Machine hostname and FQDN
  - DNS hostname and FQDN
  - Aliases and FQDN

1. Identify everything on network
   - Mixed = Hostnames, IP, MAC required for DHCP host
   - Static = IP, Hostnames, optional MAC
   - DHCP = Hostname and MAC address
2. Load list into the assets tracking system
3. Turn on auto discovery
4. Clean it up (how complete your information from step 1 is determines cleanliness)
5. Additional configurations

- CIDR ranges
- Detect Bare Mac Addresses - Only select this option if you are tracking every single MAC address. If you select this option and not all MAC addresses are properly listed, it results in duplicate assets.

Import Recommendations

While only a few fields are required to track an asset, we highly recommend answering as many fields as possible to reduce the possibility for duplicate assets. Multiple IP and MAC addresses can be associated with a single asset via a comma-separated list inside the field, surrounded by quotes. If using excel to export to CSV, these extra quotes are added automatically.

The following Asset fields are highly recommended:

- Owner
- Asset Name
- Asset Importance
- Asset Tag
- Asset Hostname

Only include the ID field if you are importing assets that have previously been exported. The id number is from the export to ensure you are updating the existing asset as part of your import, rather than creating a new asset.

Known Limitations

If the data to import contains mixed entries (in which some are only MAC addresses, and some only have IP addresses), null values must be manually inserted into the CSV, as these are read in pairs during import.

Example with three mixed entries:

- (11.11.11.11, null)
- (22.22.22.23, null)
The following line can be used as the first line of a CSV file, then opened in an editor of your choice to continue inputting data. (note: row spans multiple lines on this document).

Name, ID, Owner, Hostname, IP Address, MAC Address, Importance, Description, OS, Product Vendor, Product Name, Product Version, Server Purpose / Notes

Organization of the Assets Page

After you have uploaded and ensured all assets are tracked, use the information in this section to keep an up to date record of your assets and their activity.

Below is a screenshot of the Assets page.

There are eight sortable columns (from left to right):

- **Importance**: Displays as either none, one, two, or three dots. Knowing the importance of
an assets helps Guardian, or your internal security team, provide better management by ensuring your critical systems are always alert free. If you update the importance of your asset, open a connect ticket so that any customer triggers can be updated as well.

- **Name**: When you track your asset, the name you enter displays here; this is searchable. If an asset has not been added, this displays as untracked.

- **Heartbeat**: The last time data was received. In order to receive heartbeat data, automatic asset detection must be enabled and an IP address must be listed.
  - Grey: Never
  - Green: Within the last 24 hours
  - Yellow: Within the last 7 days
  - Red: Within the last 30 days, but not the last 7

- **Hostname**: The hostname you give the asset displays here, this is searchable.

- **IP Address**: The IP address of the asset, this is searchable.

- **MAC Address**: The MAC address of the asset, this is searchable.

- **Last Seen**: This is updated when events are matched to the asset via IP address. Any untracked assets that have not been seen for 30 or more days, are automatically deactivated. This allows the associated MAC and IP addresses to be available for future use.

- **Events**: Takes you to the Events page and only displays events for the selected asset.

In addition to the ability to sort columns, you have several other options when organizing your assets.

- **Asset Settings**: Change the number of assets displayed per page, disable asset auto-detection, and include/exclude CIDR ranges.

- **Trashcan**: Bulk deletion of depreciated or invalid assets.

- **Cloud Download**: Create a CSV export of selected assets.

- **Cloud Upload**: Upload your assets to the console via CSV file.

- **Plus**: Add a new asset to your console.
Managing Untracked assets

An untracked asset is an asset that has not been added to the Console (by providing it with a name, IP, and hostname) but is sending data. You have three options with an Untracked Asset:

- **Merge into existing asset**: This option is good for employees that have more than one asset sending data to the console. For example, Bob has a laptop, desktop, and a mobile device.
- **Track this asset**: Make your asset official. Give the asset a name, IP, hostname, and all other known information.
- **Create incident from this asset**: When an unknown asset displays on your console, create an incident for Guardian (or your internal security team) to investigate.

**To Track an Asset**

An asset must be tracked before any changes or updates can be made. Complete the following steps to track your untracked asset.

1. Click the “v” arrow to the right of the Name and then select Track This Asset.
2. The Add Tracked Asset window displays. Add as much information as possible.
3. After an asset has been added, click on the asset name to display the Asset Details window where you can view, edit, and delete the asset.

How to Create a Filtered CSV Export of Assets

This gives you the ability to filter down your assets to a useful and manageable list to be exported, saved, formatted, and used for reporting.

1. Select Assets in the left navigation.
2. Filter your assets as desired by using Tracked status, Importance, Filter by Tag, or Searching options.
3. Select the cloud icon to generate a CSV of the filtered assets.
Managing your Asset List

After the initial upload of your assets, there are a few best practices that will help keep your asset list tidy and up to date.

High number of untracked assets

1. Delete all existing assets from the console. This does not delete or interfere with existing and/or incoming data.
2. Upload your updated Asset list to the console as described earlier in this article. This allows your console to receive a fresh start and gives you a strong foundation for future asset management.

Regular Asset Maintenance

1. Each week ensure that there are no untracked assets by selecting untracked, and seeing that none display.
2. If you do see untracked assets, investigate and determine if it needs to be merged into an existing asset, added as a new tracked asset, or if it needs Guardian attention.
3. If it is an addition to an asset that has already been tracked, select to merge the asset.
4. If it is an entirely new asset that has been added to the network since your initial upload, select to track this asset.
5. If it needs investigation,
   - Select Create Incident from this Asset, and fill it out as such:
     - Title: Unknown Asset
     - Owner: Guardian (or your internal security team)
     - Severity: Low
     - Description: What steps you have already taken to figure out what this asset could be, along with your conclusion.

4. Save as an Excel sheet and format as desired.
PatternScout allows you to use anomaly detection to search for any potentially malicious activity on your network through machine-learning. We take two weeks worth of data to create a baseline that is used to distinguish between an anomaly and regular activity.

To create the most user friendly, adaptable, and efficient version of anomaly detection, the PatternScout functionality is within triggers and alerts.

PatternScout Engine

Since the first release of PatternScout, we have been learning what works best and what is needed for the real-world of cybersecurity. Each customer network is different, and anomaly detection must be able to adapt. Improving this flexibility, functionality, and ease of use is our main goal.

We learned that in some cases, anomaly detection alerts were too noisy. We have improved the algorithms to make Volumetric, Protocol, and Temporal produce fewer false alerts. We have also added support for Lateral, Geographic, and Role based anomaly detection. Anomaly detection has also been simplified by providing all details to the alert inbox, instead of going to the PatternScout page.

Using PatternScout Engine

DefenseStorm has created a list of default triggers for Volumetric, Protocol, Temporal, Lateral, Geographic, and Role based anomaly detection. To utilize the PatternScout Engine, copy and enable the triggers on your network to begin detecting anomalies. To do this, follow these steps:

1. Go to Alerts > Library and scroll down until you see PatternScout.
2. Open PatternScout and select the desired triggers to copy them to your network.

3. After they have been copied to your network, they display in the Alerts > Trigger page.

4. Enable the triggers by selecting the power icon to the left of the trigger name. Blue signifies the trigger is enabled.

For further instruction and information on triggers, see Triggers.
In addition to having scheduled reports, reports can also be generated on-demand. Generating the Cybersecurity Report on-demand does not interfere with any scheduled reporting.

Scheduled Reports

Scheduling reports allows you to set predetermined times for reports to be sent via email; they can be sent daily, weekly, monthly, or a combination of the three. This gives you the ability to set schedules for different users if desired. Tom can have daily reports, while Sally and Mary have weekly reports.

To schedule a report

Go to the Policy page of your Console, select Scheduled Reports, and then chose a date range (Daily, Weekly, Monthly). Once you have selected the date range, select the option to Configure Daily Reports.

Selecting to configure your reports gives you the options to input email addresses as well as your timezone. Select Save to schedule your report.

On-Demand Reports

The Cybersecurity report was designed with you in mind, making sure that each metric graph has business pertinent information and is easily understandable. This report makes presenting technical Cybersecurity details to your board, quick and easy.
To generate the report

Go to the Policy page of your Console, select On-Demand Reports, and then chose a date range for your report data.

Note: If you select a date range that includes the current day, the report will begin generating at midnight of your time zone; and then require an additional 4 hours for generation to complete.

This generates a word file that allows notes, comments, or additional commentary to be added. Once the report has all desired information, save it as a PDF for distribution. Below is an example on-demand CyberSecurity Report.
Reports generated previously

Your DefenseStorm console also saves all previously generated Cybersecurity reports. These reports can be downloaded again by simply selecting the download icon.
Cloud security has become an essential part of protecting the modern financial institution from cyberattack. Therefore, DefenseStorm has expanded our support platform to secure your cloud resources at no additional charge. The following is supported with the most recent DefenseStorm release:

- AWS: CloudTrail, ELB
- OpenDNS
- Office 365

**AWS: CloudTrail and ELB**

DefenseStorm Cloud watches and alerts on parts of AWS that Amazon doesn’t secure, like your OS, network config, applications and access management. CloudTrail is a web service that provides visibility into user activity by recording API calls made on your account and delivers log files to your Amazon S3 bucket. This information helps you track changes made to your AWS resources and to troubleshoot operational issues. If you are using AWS, CloudTrail should be enabled. The DefenseStorm platform ingests the ELB access logs that capture detailed information about requests sent to the load balancer. Perform the following steps to setup the AWS features through the DefenseStorm UI.

1. **Select Settings, Integrations**

   Select the Amazon Web Services icon to open the Add Amazon Web Services Account.
2. Input your Amazon Web Services Account information and select Create.

3. Connect CloudTrail to DefenseStorm by selecting the gear icon on CloudTrail and follow the displayed instructions.

4. Connect your AWS ELB to DefenseStorm by selecting the gear icon on Elastic Load Balancing, and then following the instructions displayed in the Elastic Load Balancer Setup.

OpenDNS
OpenDNS offers network security by reviewing all of your employees network connections on...
or off the corporate network. Since DefenseStorm is a layer that can “see everything”, we correlate the events OpenDNS captures when users leave the corporate network with the rest of your corporate network.

To enable the OpenDNS functionality, contact DefenseStorm for assistance.

Office 365

Adding Office 365 services is as easy as adding a cloud app. To avoid creating multiple passwords, the administrator uses their Active Directory (AD) credentials to setup Office 365 integration and ingestion of logs. Integration with Office 365 supports the following activities:

- File and folder
- Sharing and access request
- Synchronization
- Site administration
- Exchange mailbox
- User administration
- Group administration
- Application administration
- Role administration
- Directory administration

1. Select Settings, Integrations
   Select the Office 365 icon and select the option to Add Office 365 Account.

2. Select Add Office 365 Account
   Once you select to add your O365 account, the following window displays with instructions on how to add your account to DefenseStorm through Microsoft.
3. Once you have selected the link and followed the steps provided by Microsoft, all that’s left is to give your Office 365 account a display name. You are redirected back to the DefenseStorm Console, where you see the following:

4. After the display name is added, a message displays saying that you have successfully integrated with Office 365. The organization added displays in the Office 365 integrations page along with any other accounts added, and begins receiving logs.

Note: Auditing on Exchange Mailboxes is off by default. To turn on auditing and receive email information, see the Office365 FAQ article.
### Office 365 Integrations

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dev Account</strong></td>
<td>Office</td>
<td></td>
</tr>
<tr>
<td><strong>Nick's O365</strong></td>
<td>Office</td>
<td></td>
</tr>
<tr>
<td>Last Received:</td>
<td>No data</td>
<td>No data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ThreatMatch gives you the ability to subscribe to feeds from different government and threat services. We search historically over all events to see if there are any interactions with suspect sources. Even if you are not subscribed, you can see matches on the ThreatMatch page. Subscribing to a source gives you email alerts when matches are found. If you wish to subscribe or unsubscribe from a source, simply select the checkbox in the upper right of the source box.

ThreatMatch is located in the Alerts section of the console. For source details, select the source name, highlighted in blue. The Matches field shows the number of events in your console that correspond to the indicators, clicking on it displays a pop-up window with a list of the items found.

### Uploading Indicators of Compromise

One of the features available through the utilization of ThreatMatch is the blocking and tracking of indicators of compromise (IOC’s). An IOC can be anything from IP addresses, malicious files, or URL’s. To upload an IOC into ThreatMatch:

1. Go to Alerts > ThreatMatch > Select the + to create a new threat source.
2. Once a new threat source has been created, a cloud icon displays. Select the cloud icon.

3. Input information into the Upload new threat indicators window in order to begin tracking and blocking IOCs. There are several things to consider when choosing to upload a file instead of typing in each indicator per line:

1. The upload able files must be .txt (notepad, etc)
2. No combination documents. For example, one document is all domains, one document is all IPs, and one document is all hashes.
3. “domain” includes all subdomains.
4. domain.com includes only the one domain, no subdomains.

4. Input information into the Upload new threat indicators window in order to begin tracking and blocking IOCs. There are several things to consider when choosing to upload a file instead of typing in each indicator per line:
Due to the rapid rate of change in IOCs, DefenseStorm recommends that if you input a date range, that it look no farther than 3 months ahead. We also recommend that it only go back on month. This date range of back 1, forward 3 provides the best range of coverage. *Since URLs remain constant, putting a date range for them is not necessary.*

5. Select Save to begin tracking and blocking IOCs.

### ThreatMatch Classifiers

Have you ever wanted to exclude events from ThreatMatch, say for items that were handled by the firewall? Well, simply create a Classifier, select the exclude from ThreatMatch checkbox, and you'll no longer be awakened in the middle of the night with an alert only to find out it was dealt with by the appropriate system.
To create a ThreatMatch Classifier, follow the steps listed below:

1. Make a query that matches events you’d like to exclude. For example: `app_name:"Cisco ASA" deny`
2. Click the "Create a Classifier" button to the right of the search box and dates, which looks like a tag.
3. Add a name to your classifier, like "ThreatMatch exclude ASA Deny" and
4. Check the "Exclude from ThreatMatch" checkbox.
5. Select save. You can create several classifiers which each exclude a different type of message from ThreatMatch as they are indexed.
Classifiers are used to manipulate or preprocess events before they get to the DefenseStorm Console. Manipulating events occurs when you change metadata before it displays in the console. For example, you can name an IP address so that the console displays the hostname as your specified name rather than the IP. You can also choose to drop an event before it reaches the console.

**WARNING:** Dropping events means that the event is not logged within our system at all. It is not searchable and does not trigger alerts.

### How to use classifiers

Classifiers allow you to reduce the noise caused by a high volume of false positive alerts. You can exclude events, apply change attributes, or drop events all together.

Excluding events means that you will not receive an alert. The data is still logged, and is searchable through the Events page of the console. Dropping an event means that before the data gets to the console, it is thrown out. Since this data never reaches our console, it is not searchable or logged.

You can apply change attributes to the metadata to make data more useful. For example, IP address 123.456.789.1 is Joe’s PC, you could create an apply change attribute to display Joe’s PC as Joe’s PC in place of the IP address. The IP address is still listed within the event field ‘ip_src’.

### How to create a classifier

Classifiers are powerful and can have a large impact on the functionality and noise of your console. We have provided the recommended steps to ensure your classifiers are syntactically correct and function properly.

1. Go to the Events page, and enter what you want the classifier to look for. You can manually add the search parameters, or use the filter options.
2. Once you are happy with the results of your event search, select the option to create a classifier. This sends you to the Classifiers page, where the Query String field is auto-populated with your event search terms.

3. In the Classifiers window, fill in all desired fields. You must select to either drop, exclude, or apply an attribute for the classifier to work.
   - Tag Name: Classifiers should have meaningful, easily identifiable names.
   - Query String: [Auto-populated from the event search] Conditions the classifier is set to search on.

4. If you create a classifier for ‘WDAP’, it matches all events that contain ‘WDAP’. If you create a classifier NOT ‘WDAP’, it matches events that do not contain ‘WDAP’. This is the opposite of writing NOT or - within the command line text.
- Drop event: Warning: If drop event is checked, it does not log the event. Events that match this classifier are not searchable and do not trigger alerts. (Be careful using this!)
- Exclude from ThreatMatch, PatternScout, or Asset Detection to stop receiving alerts on events that match the classifier.
- Attributes to Apply: Select the key you'd like to update and the value you want the key to have. If you have more than one, click the plus sign. For example, a group of events have a category of 'None' and the organization wants to categorize these events based on information contained within the event.
  - Key = Category
  - Value = Research (or whatever value you choose)

5. Another example is if a particular system is sending events with severity of high, yet it is in fact a low (e.g. Websense blocks an incoming request yet marks it high even though it was blocked).
  - Key = Severity
  - Value = Low

6. Once all desired fields have been filled in appropriately, select Save to complete and enable your classifier.

7. After setting up the classifier, you can search for _exists_:tag_queries to display events that have matched one or more classifiers.

**Pausing, editing, or deleting a classifier**

Once the classifier is created, you have the option to pause, edit, or delete it. Once a classifier is active (enabled), a blue power icon displays to the left. If classifiers are paused (disabled), the power icon is gray. To activate or pause a classifier, simply click the power icon and it will toggle from blue to gray.
Tickets are used to track events that require research and possible action from within the DefenseStorm web console. Tickets can be either system generated (from Alerts, ThreatMatches or PatternScout) or manually created. You can also filter and generate a CSV list for formatting and reporting purposes.

There are two ways to manually create a Ticket:

1. From the Tickets page
2. From the Events page

Creating an incident from the Tickets page

1. Select the Tickets tab on the left-hand side of the screen.
2. Click on the blue plus sign on the top right. New Incident window displays.
3. Give your incident a title and assign an owner. If you want Guardian to review the incident, then select Guardian as the owner.
4. Severity is set to None by default, but can be changed to High, Medium, or Low.
5. Enter any important information relevant to the incident in the Description section.
6. Select Create to save the incident. Once an incident is created, it is automatically placed in the Triage state.

Reviewing and editing an incident
After selecting the Tickets tab, the window displays all created incidents.

1. Click on an Incident to open for review. Detailed information displays.

![Triage - Incident requires further analysis to determine next steps. This is the default state when an incident is created.](image1)

2. Select the icons to the left for further details about the incident.

3. Edit the incident (by selecting the pencil icon). Add attachments, links, policies, watchers or updating state, owner or severity.

   **Incident States are:**
   - **Triage** - Incident requires further analysis to determine next steps. This is the default state when an incident is created.
   - **Analysis** - The incident has been escalated and is undergoing further analysis.
   - **Remediation** - Negative impacts from the incident have been determined and efforts are underway to resolve any residual damage as well as remedy the root cause.
   - **Resolved** - There is still action required (updating or documenting), but the issue has been discovered.
   - **Closed** - No further action needs to be taken.

   **Links are connections to other incidents.**
   - **Files** allow uploading of any files that were associated with the investigation.
   - **You can assign other watchers or choose to add yourself as a watcher.** A watcher is someone being cc’d on an incident so they can be kept up to date on status via email. If you prefer to not receive emails, you can log into the console view updates that way.
You can assign a policy to the incident for tracking and reporting purposes.

4. To view all actions pertaining to an incident, select the Activity Log icon on the left side of the screen.

Creating an Incident through the Events page

If the results of a query are something you would like to further investigate or send to Guardian to investigate, you can create a new incident directly from the Events page.
1. Select the Incident option underneath the event graph. A window displays with information regarding recently viewed incidents, and at the very bottom, the option to create a new incident.

2. Once you select New Incident, the Create Incident window displays. Fill out fields as described above, and select Create.

How to Create a Filtered CSV Export

You now have the ability to create filtered CSV exports for your long list of incidents. Filter down your lists to a useful and manageable number that can be exported, saved, formatted, and used for reporting. Follow the steps below:

1. Select Incidents in the left navigation.
2. Filter down your incidents as desired by State, Owner, Created By, or a Title Search.
3. Select the cloud icon to generate your CSV.
4. Save as an Excel sheet, and format as desired for reporting.
<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Description</th>
<th>State</th>
<th>Owner</th>
<th>Created</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>1106</td>
<td>VPN User Audit</td>
<td>Remediating the possible malicious activity detected on your network</td>
<td>Alex</td>
<td>2017-07-17 by Alex</td>
<td>2017-08-14 by Alex</td>
<td></td>
</tr>
<tr>
<td>1142</td>
<td>Threat Scan Results: Found 1 possible malicious activity on your network</td>
<td>Traged</td>
<td>Alex</td>
<td>2017-06-30 by System</td>
<td>2017-06-30 by Alex</td>
<td></td>
</tr>
<tr>
<td>1137</td>
<td>Possible Malicious event</td>
<td>Traged</td>
<td>Edge</td>
<td>2017-06-27 by Edge</td>
<td>2017-06-27 by Edge</td>
<td></td>
</tr>
<tr>
<td>1126</td>
<td>Threat Scan Results: Found 1 possible malicious activity on your network</td>
<td>Traged</td>
<td>Alex</td>
<td>2017-06-26 by System</td>
<td>2017-06-26 by Alex</td>
<td></td>
</tr>
</tbody>
</table>
Whats New?

This release provides updates for the Windows agent to improve upgrade times, and remove automatic popups from the systray application upon login. If you wish to see the information for the Windows Agent, you can double click the systray icon to display the information.

What Do I Need to Do?

The upgrade to the Windows Agent is automatic and requires no action on your part. If you have never installed the Windows Agent, and would like to do so, see our Downloads Page for the most recent version.
Think your Network May be Compromised?

**STEP 1: Disconnect the problem machine from your network**

While we do not promote one solution over any other, we recommend using a sandbox solution to disconnect the host from the network. If none are available, disconnect the host from all network connections. This prevents the malware from spreading or calling home.

**STEP 2: Delete any new files or programs that do not belong**

New programs and files could contain malware. Deleting these newly installed programs or files could prevent the spread or increased severity of malware.

**STEP 3: Re-image the machine**

After uninstalling new programs and files, if you still see unsolicited calls outs or unusual application behavior and are still unsure that the malware was deleted, you can re-image the machine to remove any rootkits. *When a machine is re-imaged, user profiles need to be re-uploaded.*

**STEP 4: User Training**

To reduce risk of malware infection, put the user through remedial training to ensure they understand malware and how it can spread. For example, spam emails, websites, contaminated drives, and it can even come pre-installed on some software packages.

**STEP 5: Continued Monitoring**

After all the above steps have been completed, continue to monitor the host for a minimum of 7 days to look for unsolicited call outs.

Login

**What do I do after my user has been created?**

When your User ID is set up in the console you receive an email with a link (or copy and paste the link into your browser) to complete the setup. This displays a field for your desired
I forgot my password

If you forget your password, follow these steps to set a new one.

STEP 1: Go to the https://console.defensestorm.com/#/login

STEP 2: Select “Forget your password?.”

STEP 3: Enter your email address and select Reset Password.

Upgrading my DVM

How do I know when to upgrade my DVM?

DefenseStorm notifies you via Release Notes when there is a new version to be installed.

Am I Eligible to Upgrade Through the DVM?

Within your DVM Main Menu, select Option 8: Get DVM Status to see if a version number is displayed. If your version number does not display, please contact DefenseStorm for upgrade assistance.

How do I upgrade my DVM?

Once you have determined you are eligible to upgrade through the DVM main menu, see The DefenseStorm Virtual Machine for instructions.
What are best practices for asset management?

The key to asset management is regular checks of your account. Once a week, look through your asset list and track/merge or open an incident on any untracked assets found. Doing this on a regular basis, will keep your asset list clean and tidy. See Assets for more recommendations and instructions.

What do I do if I see a suspicious untracked asset?

If you see an untracked asset that you believe should not be sending data to your network, the best way to investigate is to create a ticket directly from the untracked asset, naming Guardian as the owner. Once the ticket is created, an email is sent to Guardian where they look for malicious activity.

Data Retention

What is cold storage?

As part of DefenseStorm’s data retention, we keep 90 days worth of searchable event data as live storage. Any event data after 90 days is considered cold storage. If you need data from cold storage any reason, such as auditing or investigative purposes, simply submit a request to DefenseStorm.

How do I request my data stored in cold storage?

Open a new Connect Support Ticket to DefenseStorm with the specific information regarding the data you wish to be have restored. The specific information could simply be a date range, certain users within a date range, or even certain machines within a date range.

How long does it take to restore requested data?

The time frame for restoring cold data is dependent on how much data is requested and other network factors. Estimates are provided on a case-by-case basis after DefenseStorm has an opportunity to review all relevant and necessary details. This ensures accuracy and that your estimate is specific to you and your restore needs.

Input Token

What is an Input Token?
An input token is a system generated administrative user account created during the initial setup and configuration of DefenseStorm ground services. The system uses your email and password to create the tokens. The input token also contains the DefenseStorm Key and Secret; which may be necessary for some application integrations.

Select the Input Tokens after you select the Settings tab (gear icon) on the far bottom left of your screen.

How does it relate?

The Input Token is how events are authenticated. You can use the aggregate feature to filter down your events to display which Input Token is generating the most events. The api_key filter name is the Input Token key.

Supported Parsers

- ADFS
- ADTran
  - Switch (NetVanta)
- Allied Telesis
- Barracuda
  - Barracuda SSL VPN
  - Web Security Gateway
- Bit9
- Bro Files
  - supported log file list is: conn, dhcp, dns, dpd, files, ftp, http, notice, smtp, software, ssh, ssl, syslog, tunnels, weird, snmp, x509. Full Bro log list: https://www.bro.org/sphinx/script-reference/log-files.html
- Carbon Black
  - Carbon Black Server 8.x (+ all previous versions)
- Cisco
  - 2504 Series
- 4500 Series
- 2921 Parser for IOS VoIP Router
- Prime Parser
- SourceFire
- 9396 NXOS Core Router
- Security
- Identity Services Engine (ISE)
- C2921 VoIP Gateway
- Meraki
- 9396 NXOS Core Router
- 2960 Switch
- Small Business Router (RV____ models)
  - DHCP NXLog Error
  - ESXi
  - F5 Load Balancers
  - Fortigate
  - HP
    - ProCurve Switch
  - IBM
    - Proventia Server Intrusion Protection System
  - Infoblox DNS
  - IPS Syslog
  - iSensor Message
  - Juniper
    - Switch
    - Firewall
  - McAfee
    - Epo
    - Web Filter
    - Web Gateway
  - Microsoft
    - IIS
- NetFlow
- PaloAlto
- Proofpoint
- Reactor
- RSA Authentication Manager
- Sentinel IPS
- Shortel Logs
- SNMP Trap
- Software versions - Instead of showing up as IP addresses, the parser displays the actual software version.
- SonicWall
  - Messages
  - Firewall
- Sophos
  - Sophos Cloud Installer / AutoUpdater
  - Sophos XG Firewall
- Symantec
  - SEP
  - Server
- TrendNet
  - Switch
- VMware
  - ESXi / vSphere
  - vCenter
- WebSense
  - Websense Email Gateway
- Windows
  - ADFS Audit Logs
  - Security Audit Logs
  - Events
  - Event Account Change
  - Exchange Server Audit Logs
Elasticsearch Boolean Logic

Grouping is extremely important when using boolean logic in your queries because Elasticsearch, the underlying engine, doesn't behave exactly as expected. The implications are that you may miss something in a search or you may unintentionally exclude events if using classifiers.

In any classifier where there are OR terms and no parentheses, the way to read it is that any term touching an OR is optional. Whenever an OR is used, all the OR terms must be grouped in a set of parentheses. In certain cases this requires also parenthesizing the AND terms. See below for examples.

Classifier Rule - (ThreatMatch Drop Denied)

- app_name:"Cisco ASA" AND (Deny OR denied OR discarded)

The following search would match anything:

- app_name:"Cisco ASA"

To make the OR required the classifier rule should be written as:

- app_name:"Cisco ASA" AND (Deny OR denied OR discarded)

Threat Sharing Sources

All threat sharing sources are used for anomaly detection and are found on the ThreatMatch page of your DefenseStorm console. You can subscribe or unsubscribe from each threat source individually. For more information on ThreatMatch, and how it works with your cybersecurity program, see Using ThreatMatch. AlienVault

- Bambenek
- CrimeTracker
- DefenseStorm
- DNS-BH
- DShield
- FS-ISAC
- InfraGard
- Malcode
- MalwareDomains
- OpenBL
- Tor Exit Nodes
- ZeuS Tracker

### Event Fields and Descriptions

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Similar Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>The action</td>
<td>taken_action</td>
</tr>
<tr>
<td>api_key</td>
<td>The DefenseStorm API key used to send the message. Usually one per DefenseStorm Virtual Machine. For Cloud integrations, a unique ID per integration.</td>
<td></td>
</tr>
<tr>
<td>bytes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>category</td>
<td>The type of the message, app_name dependent</td>
<td>type, subcategory, event_type, channel</td>
</tr>
<tr>
<td>connection_direction</td>
<td>DefenseStorm’s best guess at whether or not this is an outbound, inbound, or internal connection</td>
<td></td>
</tr>
<tr>
<td>dest_port</td>
<td>Destination port</td>
<td></td>
</tr>
<tr>
<td><strong>domain</strong></td>
<td>The Windows domain associated with the request</td>
<td>user_domain, target_domain, account_domain, used_account_domain, caller_domain, group_domain, network_account_domain, ad_domain, subject_domain_name, new_account_domain, target_domain_name</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>endpoint_ip</strong></td>
<td>All the IP addresses that could be considered on your network</td>
<td></td>
</tr>
<tr>
<td><strong>event_id</strong></td>
<td>The event ID (if any) associated with the event</td>
<td></td>
</tr>
<tr>
<td><strong>file_hash</strong></td>
<td>The MD5, SHA1, SHA256 or similar hash value of the file</td>
<td>hash</td>
</tr>
<tr>
<td><strong>file_name</strong></td>
<td>The name or path of the file associated with the event</td>
<td>file_path, src_file_name, dest_file_name, target_filename, old_file_path, new_file_path</td>
</tr>
<tr>
<td><strong>geo_dest</strong></td>
<td>Destination Geographic Information</td>
<td></td>
</tr>
<tr>
<td><strong>geo_src</strong></td>
<td>Source Geographic Information</td>
<td></td>
</tr>
<tr>
<td><strong>group_name</strong></td>
<td>The name of a group that the event invoked acts on</td>
<td></td>
</tr>
<tr>
<td><strong>hostname</strong></td>
<td>Usually the name for the machine sending the message.</td>
<td>src_hostname, dest_hostname, client_hostname, sensor_hostname, global_hostname, local_hostname, src_translated_hostname, dest_translated_hostname, real_hostname, map_hostname</td>
</tr>
<tr>
<td><strong>http_host</strong></td>
<td>The HTTP hostname of the HTTP request</td>
<td>dest_host</td>
</tr>
<tr>
<td><strong>http_path</strong></td>
<td>The HTTP path of the URI</td>
<td>path</td>
</tr>
<tr>
<td><strong>http_url</strong></td>
<td>The HTTP URI of the request</td>
<td>url</td>
</tr>
<tr>
<td><strong>http_user_agent</strong></td>
<td>The User Agent associated with the request</td>
<td>user_agent</td>
</tr>
<tr>
<td><strong>image</strong></td>
<td>The path to the executable being run</td>
<td>process, process_name, process_command_line</td>
</tr>
<tr>
<td><strong>ingestion_timestamp</strong></td>
<td>The actual time DefenseStorm received the message</td>
<td></td>
</tr>
<tr>
<td><strong>ip_dest</strong></td>
<td>Destination IP address</td>
<td></td>
</tr>
<tr>
<td><strong>ip_foreign</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ip_global</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ip_local</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ip_src</strong></td>
<td>Source IP address</td>
<td></td>
</tr>
<tr>
<td><strong>ip_type_dest</strong></td>
<td>Private, Public, Reserved, or Multicast IP Address for Destination</td>
<td></td>
</tr>
<tr>
<td><strong>ip_type_src</strong></td>
<td>Private, Public, Reserved, or Multicast IP Address for Source</td>
<td></td>
</tr>
<tr>
<td><strong>logon_type</strong></td>
<td>The Windows logon type</td>
<td></td>
</tr>
<tr>
<td><strong>mac_address</strong></td>
<td>The MAC address for the event</td>
<td></td>
</tr>
<tr>
<td><strong>message</strong></td>
<td>A human readable description of the event</td>
<td></td>
</tr>
<tr>
<td><strong>protocol</strong></td>
<td>Usually TCP or UDP</td>
<td></td>
</tr>
<tr>
<td><strong>received_bytes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>sensor_ip</strong></td>
<td>The IP address of the machine</td>
<td></td>
</tr>
<tr>
<td><strong>unparsed_message,</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>expanded_message,</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>short_message</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>sending_bytes</strong></td>
<td>generating the message</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>severity</strong></td>
<td>NONE, LOW, MEDIUM, HIGH</td>
<td></td>
</tr>
<tr>
<td><strong>src_port</strong></td>
<td>Source port</td>
<td></td>
</tr>
<tr>
<td><strong>timestamp</strong></td>
<td>The time the message was allegedly generated</td>
<td></td>
</tr>
<tr>
<td></td>
<td>nx_timestamp,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>event_received_timestamp,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>creation_timestamp,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>logged_timestamp,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>registration_timestamp</td>
<td></td>
</tr>
<tr>
<td><strong>total_bytes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>user_name</strong></td>
<td>The name of the user involved in the event</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user, account_name,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>target_user_name,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>username, user_id,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subject_user_name,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>new_account_name</td>
<td></td>
</tr>
<tr>
<td><strong>unparsed_extended_message</strong></td>
<td>The windows event log messages may have a section Windows names “extended message”. The unparsed_extended_message is a specific windows event log message that contains sections of the long form windows event log message for which the DefenseStorm platform did not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>unparsed_message</td>
<td></td>
</tr>
</tbody>
</table>
have specific matches (i.e. could not parse completely)
The Federal Financial Institutions Examination Council (FFIEC) is a formal U.S. government interagency body that includes five banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). It is “empowered to prescribe uniform principles, standards, and report forms to promote uniformity in the supervision of financial institutions”. It also oversees real estate appraisal in the United States. Its regulations are contained in title 12 of the Code of Federal Regulations.

This playbook provides detailed information on the FFIEC government requirement criteria. Some of these statements are met by having DefenseStorm on your network, and some require additional action on your part. This playbook tells you exactly what DefenseStorm does for you, and how you can help DefenseStorm improve your FFIEC compliance.

### D1.G.Ov.B.3 - Annual report of overall security status

**Statement:** Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5)

**DefenseStorm:** Yes. The CyberSecurity Report.

**Customer:** Annually provide the Cybersecurity Report to board-level executives.

### D1.G.Ov.Int.1 - Cybersecurity expertise

**Statement:** The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.

**DefenseStorm:** Yes, if...
**D1.G.Ov.Int.2 - Standard review of threat intelligence trends and security posture**

Statement: The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institutions security posture.


Customer: Include the Cybersecurity Report in all board meetings.

**D1.G.SP.B.3 - Threat information Sharing**

Statement: The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. (FFIEC EBanding Booklet, page 28).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: To further your compliance, take part in the peer-to-peer forum offered in Connect to share further information with DefenseStorm peers.

**D1.G.SP.B.6 - Incident response and resilience**

Statement: The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. (FFIEC Information Security Booklet, page 83).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.
D1.G.IT.B.1 - Asset Inventory

Statement: An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9).

DefenseStorm: Yes, Partially. The asset information that DefenseStorm collects is an incomplete view. DefenseStorm gets partial views through the utilization of the following programs: Pwnie, Nessus, Agents, and Logs. Alerts based on discovery of Untracked Assets, also on discovery of new/changed software/hostnames/etc.

Customer: Utilize Pwnie, Nessus, Agents, and Logs to help give DefenseStorm the most complete view into your assets.

D1.G.IT.B.2 - Asset protection prioritization

Statement: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. (FFIEC Information Security Booklet, page 12)

DefenseStorm: Yes, partially.

Customer: You must leverage the “owner” and “importance” descriptions in the Assets page.

D1.G.IT.E.1 - Annual update of assets

Statement: The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.

DefenseStorm: Yes, partially. Alert on new/untracked asset. Similar to alert an asset not talking to us, etc.

Customer: Create a CSV export of your assets at least annually.

D1.G.IT.E.3 - EOL management
Statement: The institution proactively manages system EOL (e.g., replacement) to limit security risks.

DefenseStorm: Yes, partially.

Customer: For complete compliance, leverage Pwnie/Nessus with DefenseStorm.

**D2.TI.Ti.B.1 - Threat information sources**

Statement: The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). (FFIEC EBanking Work Program, page 28)

DefenseStorm: Yes. Over a dozen sources. See the Threat Sharing Sources Knowledge Base article.

Customer: Ensure that ThreatMatch is enabled.

**D2.TI.Ti.B.2 - Threat monitoring**

Statement: Threat information is used to monitor threats and vulnerabilities. (FFIEC Information Security Booklet, page 83)


Customer: Make sure ThreatMatch is enabled. For more complete compliance, utilize Pwnie and Nessus for threat and vulnerability monitoring through Guardian.

**D2.TI.Ti.B.3 - Enhance risk management**

Statement: Threat information is used to enhance internal risk management and controls.
DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: For increased compliance, leverage Guardian recommendations. You can also leverage the daily Guardian Intel Report to enhance risk management and controls.

**D2.TI.Ti.E.1 - Information, analysis, and mitigation recommendations**

Statement: Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.

DefenseStorm: Yes, if...

Customer: To further your compliance, utilize Guardian.

**D2.TI.Ti.Int.1 - Formal implementation of a threat intelligence program**

Statement: A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.

DefenseStorm: Yes. DefenseStorm provides external providers. Console enables internal sources via download of internal threat feeds.

Customer: Make sure ThreatMatch is enabled.

**D2.TI.Ti.Int.2 - Collection protocols**

Statement: Protocols are implemented for collecting information from industry peers and government.
DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: Utilize the Guardian team; they have defined protocols for accomplishing this.

D2.TI.Ti.Int.3 - Central cyber threat repository

Statement: A read-only, central repository of cyber threat intelligence is maintained.

DefenseStorm: Yes, via Connect.

Customer: To further your compliance, utilize Guardian.

D2.TI.Ti.A.1 - Use of a cyber intelligence model

Statement: A cyber intelligence model is used for gathering threat information.

DefenseStorm: Yes. Via DefenseStorm’s methodology for collecting intelligence and distribution through our daily news.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D2.TI.Ti.A.2 - Receive threats automatically

Statement: Threat intelligence is automatically received from multiple sources in real time.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: Make sure ThreatMatch is enabled.

D2.TI.Ti.A.3 - Geopolitical threat intelligence

Statement: The institution’s threat intelligence includes information related to geopolitical
events that could increase cybersecurity threat levels.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: Make sure ThreatMatch is enabled.

D2.TI.Ti.Inn.2 - Investment in threat intelligence and collaboration

Statement: The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared.

DefenseStorm: Yes, DefenseStorm does this on your behalf.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D2.TI.Ma.B.1 - Secured review and retainer of logs

Statement: Audit log records and other security event logs are reviewed and retained in a secure manner. (FFIEC Information Security Booklet, page 79).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Simple having DefenseStorm meets this criteria.

D2.TI.Ma.B.2 - Investigation of events

Statement: Computer event logs are used for investigations once an event has occurred. (FFIEC Information Security Booklet, page 83).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: To further your compliance, utilize Guardian.
D2.TI.Ma.E.1 - Discovery of emerging threats

Statement: A process is implemented to monitor threat information to discover emerging threats.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: To further your compliance, utilize Guardian. Guardian tracking the threat feeds and leveraging that data to better monitor your network.

D2.TI.Ma.E.2 - Threat analysis team

Statement: The threat information and analysis process is assigned to a specific group or individual.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: To further your compliance, utilize Guardian.

D2.TI.Ma.E.3 - Security Operations Center (SOC)

Statement: Security processes and technology are centralized and coordinated in a Security Operations Center (SOC) or equivalent.

DefenseStorm: Yes, partially.

Customer: To further your compliance, utilize Guardian. Centralized and coordinated through Guardian depending on Rules of Engagement established with DefenseStorm. Guardian provides the 24/7 Monitor Center and response via Active Response.

D2.TI.Ma.E.4 - Continuous system monitoring
Statement: Monitoring systems operate continuously with adequate support for efficient incident handling.

DefenseStorm: Yes, if...

Customer: To further your compliance, utilize Guardian.

**D2.TI.Ma.Int.1 - Multiple source threat evaluation**

Statement: A threat intelligence team is in place that evaluates threat intelligence from multiple sources for credibility, relevance, and exposure.

DefenseStorm: Yes, if...

Customer: To further your compliance, utilize Guardian.

**D2.TI.Is.B.1 - Internal sharing of threats**

Statement: Information security threats are gathered and shared with applicable internal employees. (FFIEC Information Security Booklet, page 83).

DefenseStorm: Yes, via Guardian and Connect.

Customer: To further your compliance, utilize Guardian and Connect.

**D2.TI.Is.B.3 - Law enforcement**

Statement: Information about threats is shared with law enforcement and regulators when required or prompted. (FFIEC Information Security Booklet, page 84).

DefenseStorm: Yes. Within your IR policy/plan, you should have points of contacts with law enforcement. If DefenseStorm takes on the role of your trusted advisor, we should be added into the plan.

Customer: Add DefenseStorm to your Incident Response (IR) plan.
D2.TI.Is.E.2 - Information-sharing meetings

Statement: A representative from the institution participates in law enforcement or information-sharing organization meetings.

DefenseStorm: Yes. DefenseStorm participates in FS-ISAC and Infraguard meetings, gatherings, etc.

Customer: To further your compliance, utilize Guardian.

D2.TI.Is.Int.1 - Internal, formal, sharing protocol

Statement: A formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function.

DefenseStorm: Yes, partially. DefenseStorm provides all the necessary data via Connect, Pwnie/Nessus reports, and incident information.

Customer: Define and implement the formal protocol using the data provided by DefenseStorm.

D2.TI.Is.A.2 - Peer institution sharing

Statement: Relationships exist with employees of peer institutions for sharing cyber threat intelligence.

DefenseStorm: Yes, via connect.

Customer: To further your compliance, utilize Connect forums.

D3.PC.Im.B.1 - Perimeter defense tools
Statement: Network perimeter defense tools (e.g., border router and firewall) are used. (FFIEC Information Security Booklet, page 33).

DefenseStorm: Yes. DefenseStorm can monitor via alerts to ensure this control is in place and event data is being received.

Customer: To further your compliance, create a policy based on assessments.

**D3.PC.Im.B.3 - Port monitoring**

Statement: All ports are monitored. (FFIEC Information Security Booklet, page 50).

DefenseStorm: Yes. DefenseStorm is monitoring via Firewall, Network Switch, and other logs.

Customer: For further compliance, utilize SecurityOnion and Pwnie/Nessus.

**D3.PC.Im.B.5 - System configurations**

Statement: System configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. (FFIEC Information Security Booklet, page 56).

DefenseStorm: Yes, partially...

Customer: For further compliance, utilize Pwnie and Nessus with DefenseStorm.

**D3.PC.Im.B.7 - Selective access for system configurations**

Statement: Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. (FFIEC Information Security Booklet, page 56).

DefenseStorm: Yes, partially. DefenseStorm provides the monitoring to enable you to be alerted and audit these types of access and changes.

Customer: Make sure your policy is set up for the monitoring aspect.
D3.PC.Im.B.10 - Encryption for authentication and transmission

Statement: Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) (FFIEC Information Security Booklet, page 40).

DefenseStorm: Yes, partially.

Customer: For further compliance, utilize Pwnie and Nessus.

D3.DC.Th.B.2 - Attack detection tools

Statement: Antivirus and anti-malware tools are used to detect attacks. (FFIEC Information Security Booklet, page 55).

DefenseStorm: Yes, partially. DefenseStorm is part of the overall malware detection toolset.

Customer: Ensure that ThreatMatch and PatternScout are enabled and utilized.

D3.DC.An.B.1 - Anomaly detection

Statement: The institution is able to detect anomalous activities through monitoring across the environment. (FFIEC Information Security Booklet, page 32).

DefenseStorm: Yes. PatternScout.

Customer: Leverage PatternScout.

D3.DC.An.B.3 - Log review

Statement: Logs of physical and/or logical access are reviewed following events. (FFIEC
D3.DC.An.B.4 - Critical system access

Statement: Access to critical systems by third parties is monitored for unauthorized or unusual activity. (FFIEC Outsourcing Booklet, page 26).

DefenseStorm: Yes. Onboarding policies.

Customer: For further compliance, utilize Guardian. They work with you to identify critical systems and third party access information in order to provide appropriate alerting and monitoring related to third party access. Who are your third party vendors that access, how do they access. What systems do they access, when do they access, etc.

D3.DC.An.B.5 - Elevated privileges


DefenseStorm: Yes.

Customer: For further compliance, utilize Guardian. Guardian monitors based on information collected during onboarding for privileged accounts.

D3.DC.An.E.2 - Regular log review

Statement: Security logs are reviewed regularly.

DefenseStorm: Yes, if...

Customer: For compliance, utilize Guardian.
D3.DC.An.E.3 - System access traceability

Statement: Logs provide traceability for all system access by individual users.

DefenseStorm: Yes, if...

Customer: Fully implemented and instrumented to provide us with the data.

D3.DC.An.E.4 - Established thresholds

Statement: Thresholds have been established to determine activity within logs that would warrant management response.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: Make sure that PatternScout and Alert Thresholds are configured via Guardian for monitoring.

D3.DC.An.Int.3 - Monitor and alert on log anomalies

Statement: Tools actively monitor security logs for anomalous behavior and alert within established parameters.


Customer: For further compliance, utilize Guardian.

D3.DC.An.Int.4 - Restricted, centralized log server

Statement: Audit logs are backed up to a centralized log server or media that is difficult to alter.

DefenseStorm: Yes. Leveraging DefenseStorm.
Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D3.DC.An.Int.5 - Periodic threshold evaluation**

Statement: Thresholds for security logging are evaluated periodically.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: For compliance, utilize Guardian. They do this dynamically based on your instrumentation, quality, and changes.

**D3.DC.An.Int.6 - Alerts correlated across all business units**

Statement: Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDoS attack).

DefenseStorm: Yes if...

Customer: Fully implemented and instrumented to provide us with the data.

**D3.DC.An.A.3 - Employee behaviour**

Statement: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: For compliance, utilize role based PatternScout.
D3.DC.Ev.B.1 - Established activity baseline

Statement: A normal network activity baseline is established. (FFIEC Information Security Booklet, page 77).

DefenseStorm: Yes. DefenseStorm is providing this capability via PatternScout and Event Thresholds set by Guardian.

Customer: For further compliance, utilize Guardian.

D3.DC.Ev.B.2 - Potential attack notification

Statement: Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. (FFIEC Information Security Booklet, page 78).

DefenseStorm: Yes. DefenseStorm monitors and escalates back to you.

Customer: For further compliance, utilize Guardian for escalation and resolution help.

D3.DC.Ev.B.3 - Monitor for unauthorized access

Statement: Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. (FFIEC Information Security Work Program, Objective II: M-9).


Customer: For further compliance, utilize Pwnie and Nessus.

D3.DC.Ev.B.4 - Assigned monitor

Statement: Responsibilities for monitoring and reporting suspicious systems activity have been assigned. (FFIEC Information Security Booklet, page 83).

DefenseStorm: Yes. DefenseStorm monitors and escalates to you based on our Rules of Engagement with you.
Customer: Ensure the Rules of Engagement allow for compliance.

**D3.DC.Ev.B.5 - Physical environment unauthorized access**

Statement: The physical environment is monitored to detect potential unauthorized access. (FFIEC Information Security Booklet, page 47).

DefenseStorm: Yes, if...

Customer: Provide DefenseStorm with access log information from physical controls.

**D3.DC.Ev.E.1 - Event correlation tool**

Statement: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).

DefenseStorm: Yes. DefenseStorm is the correlation tool, Guardian are the correlation experts.

Customer: For further compliance, utilize Guardian.

**D3.DC.Ev.Int.2 - Reliable event detection**

Statement: Event detection processes are proven reliable.

DefenseStorm: Yes. Leveraging Guardian.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D3.DC.Ev.Int.2 - Critical Asset monitoring**
Statement: Specialized security monitoring is used for critical assets throughout the infrastructure.

DefenseStorm: Yes. DefenseStorm is a specialized monitoring that is refining monitoring for critical assets, if...

Customer: Properly identify critical assets to us via the importance column of the assets page on the Console.

D3.DC.Ev.A.1 - Detect unauthorized changes

Statement: Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices.

DefenseStorm: Yes, via monitoring triggers for system changes.

Customer: Ensure that triggers for system changes are active.

D3.DC.Ev.A.3 - Automatic network change alerts

Statement: Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur.

DefenseStorm: Yes, partial for software. Through monitoring triggers for system changes and asset alerts on changes to software for a windows asset.

Customer: Ensure that your triggers are activated to alert in changes to software for a windows asset.

D3.DC.Ev.A.4 - Tools can correlate events

Statement: Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters.

DefenseStorm: Yes. Leveraging DefenseStorm.
Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D3.DC.Ev.Inn.1 - Predictive event correlation

Statement: The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur.

DefenseStorm: Yes. As your representative, DefenseStorm is continuing to develop tools that provide predictive correlation based on event data received.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D3.DC.Ev.Inn.2 - Investing in intelligence and collaboration

Statement: The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared.

DefenseStorm: Yes. Being your vendor and providing cybersecurity stack, DefenseStorm does this for you.

Customer: Ensure ThreatMatch is enabled.

D5.IR.Pl.B.4 - Team diversity

Statement: The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g., management, legal, public relations, as well as information technology). (FFIEC Information Security Booklet, page 84).
DefenseStorm: Yes, if...

Customer: Utilize Guardian. They provide Cybersecurity expertise in the Response Team.

**D5.IR.Te.B.1 - Improvement scenarios**

Statement: Scenarios are used to improve incident detection and response. (FFIEC Information Security Booklet, page 71).

DefenseStorm: Red Team.

Customer: No further action required.

**D5.IR.Te.B.2 - Third party collaboration**


DefenseStorm: Yes, if...

Customer: Incorporate DefenseStorm into your business continuity testing.

**D5.IR.Te.E.2 - Response improvement**

Statement: Widely reported events are used to evaluate and improve the institution’s response. Guardian provides the information.

DefenseStorm: Yes, partially. DefenseStorm provides the data.

Customer: For complete compliance, leverage the data from DefenseStorm to improve your responses.

**D5.IR.Te.Int.1 - Analysis of attack scenarios**

Statement: Cyber-attack scenarios are analyzed to determine potential impact to critical
D5.IR.Te.Int.2 - Participation in cyber exercises

Statement: The institution participates in sector-specific cyber exercises or scenarios (e.g., FS-ISAC Cyber Attack (against) Payment Processors (CAPP)).

DefenseStorm: Red Team.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.IR.Te.Int.3 - Analysis of resilience testing

Statement: Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution.

DefenseStorm: Red Team.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.IR.Te.Int.4 - Critical system stress testing

Statement: The critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS).

DefenseStorm: Red Team.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.
D5.IR.Te.Int.5 - Utilization of cyber event exercises

Statement: The results of cyber event exercises are used to improve the incident response plan and automated triggers.

DefenseStorm: Yes. DefenseStorm provides the data.

Customer: For compliance, leverage the DefenseStorm output of these types of activities.

D5.IR.Te.A.1 - Comprehensive resilience testing

Statement: Resilience testing is comprehensive and coordinated across all critical business functions.

DefenseStorm: Red Team.

Customer: No further action necessary. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.IR.Te.A.2 - Utilization of known attacks

Statement: The institution validates that it is able to recover from cyber events similar to by known sophisticated attacks at other organizations.

DefenseStorm: Red Team - leveraging data/experience across customers.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.IR.Te.A.3 - Internal hacking team (Red Team)

Statement: Incident response testing evaluates the institution from an attacker’s perspective to determine how the institution or its assets at critical third parties may be targeted.
Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D5.IR.Te.A.4 - Root cause correction**

Statement: The institution corrects root causes for problems discovered during cybersecurity resilience testing.

DefenseStorm: Yes. DefenseStorm provides the data and recommendations.

Customer: For compliance, utilize the data provided by DefenseStorm.

**D5.DR.De.B.1 - Alert parameters**


Customer: Ensure triggers are activated.

**D5.DR.De.B.2 - Risk indicator information**

Statement: System performance reports contain information that can be used as a risk indicator to detect information security incidents. (FFIEC Information Security Booklet, page 86).


Customer: Ensure that ThreatMatch and PatternScout are enabled for the best compliance.
D5.DR.De.B.3 - Initiation of the incident response program

Statement: Tools and processes are in place to detect, alert, and trigger the incident response program. (FFIEC Information Security Booklet, page 84).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.DR.De.E.1 - Potential threatening internal activity

Statement: The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.DR.De.Int.1 - Anomaly detection

Statement: The incident response program is triggered when anomalous behaviors and attack patterns or signatures are detected.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.DR.De.Int.2 - Discover infiltration pre-damage
Statement: The institution has the ability to discover infiltration, before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D5.DR.De.Int.3 - Appropriate personnel alert**

Statement: Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D5.DR.De.Int.4 - Correlation of network and system alerts**

Statement: Network and system alerts are correlated across business units to better detect and prevent multifaceted attacks (e.g., simultaneous DDoS attack and account takeover).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D5.DR.De.Int.5 - Enterprise level event correlation**

Statement: Incident detection processes are capable of correlating events across the enterprise.
DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.DR.De.A.1 - External and internal threat detection

Statement: Sophisticated and adaptive technologies are deployed that can detect and alert the incident response team of specific tasks when threat indicators across the enterprise indicate potential external and internal threats.

DefenseStorm: Yes. ThreatMatch, PatternScout, Triggers.

Customer: Ensure that ThreatMatch, PatternScout, and Triggers are enabled.

D5.DR.De.A.2 - Specialized security monitoring

Statement: Automated tools are implemented to provide specialized security monitoring based on the risk of the assets to detect and alert incident response teams in real time.

DefenseStorm: Yes. DefenseStorm is the specialized tool and can be tuned for more specialized monitoring of identified high risk systems that.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.DR.Re.B.1 - Incident containment

Statement: Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. (FFIEC Information Security Booklet, page 84).

DefenseStorm: Yes, through Guardian.
Customer: Utilize Guardian. They provide alerting, recommendations, and expertise on mitigation.

**D5.DR.Re.E.6 - Incident records**

Statement: Records are generated to support incident investigation and mitigation.

DefenseStorm: Yes. Incident Ticketing system.

Customer: Utilize the incident ticketing system on your DefenseStorm console.

**D5.DR.Re.E.7 - Mitigation by third parties**

Statement: The institution calls upon third parties, as needed, to provide mitigation services.

DefenseStorm: Red Team.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

**D5.DR.Re.E.8 - Security improvement from event analysis**

Statement: Analysis of events is used to improve the institution’s security measures and policies.

DefenseStorm: Yes, partially.

Customer: For further compliance, utilize Guardian. They perform continuous improvement based on lessons learned dealing with incidents.

**D5.DR.Re.A.1 - Management and intelligence collaboration**
Statement: The incident management function collaborates effectively with the cyber threat intelligence function during an incident.

DefenseStorm: Yes if...

Customer: Guardian is appropriately integrated into your IR Plan.

D5.DR.Re.A.2 - Proactive response to threats

Statement: Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents.

DefenseStorm: Yes if...

Customer: Guardian is appropriately integrated into your IT team. (force-multiplier if you are leveraging DefenseStorm effectively).

D5.DR.Re.A.3 - Timely response to attacks

Statement: Technical measures apply defense-in-depth techniques such as deep packet inspection and black holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks.


Customer: Requires appropriate instrumentation and configuration of PatternScout as well as ThreatMatch.

D5.ER.Es.B.3 - Annual reporting

Statement: The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. (FFIEC Information Security Booklet, page 5).

Customer: Display the Cybersecurity Report to the board.

D5.ER.Es.B.4 - Incident management

Statement: Incidents are classified, logged, and tracked. (FFIEC Operations Booklet, page 28).

DefenseStorm: Yes. Leveraging DefenseStorm.

Customer: No further action required. Having DefenseStorm as your cybersecurity company meets the criteria.

D5.ER.Es.E.3 - Incident tracking

Statement: Tracked cyber incidents are correlated for trend analysis and reporting.


Customer: For further compliance, utilize Guardian for trend analysis.

D5.ER.Es.A.2 - Management level metric review

Statement: Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.


Customer: Utilize the Cybersecurity Report as part of board meetings.
Alert Inbox: Best Practices

This playbook provides detailed instructions on best practices for properly utilizing the Alert Inbox. Whether you are a Guardian customer or not, knowing our recommended best practices greatly benefits your network security. For other information about the Alert Inbox, see Using Alerts.

Guardian Customer Alert Inbox Best Practices

If you are a Guardian customer, you may be curious about how Guardian uses your Alert Inbox, and what you could be doing in combination. This section describes how you can work alongside Guardian to provide the best network security.

What does Guardian do with my Alert Inbox?

Guardian routinely sorts your Alerts and begins investigating through the associated events for the cause of the alert. Once they have worked through an event, they categorize it as one of the following:

- Escalated - Additional investigation is needed and Guardian may require assistance for network changes.
- Dismissed - An alert that has been reviewed and determined to not need further investigation or assistance.
- False Positive - Should not have been flagged as an alert.

How can I help Guardian?

- Notify Guardian of any network changes, patching, or other system changes including the editing of triggers.
- Escalating Alerts lets Guardian know that you have looked at it, and need assistance.
- If you think an Alert should be categorized as False Positive or Dismissed, instead of
categorizing it, send Guardian an email letting them know. This prevents any interference with anomaly detection and incorrect categorization.

Non-Guardian Alert Inbox Best Practices

If you are not a Guardian customer, there are many things you can do to help keep your network secure with your Alert Inbox. The plays in this section describe how you and your internal security team can provide the best network security.

The more often the plays in this playbook are implemented, the easier your daily workload is.

**Step 1: Open Alert Inbox and Sort Alerts**

Routinely sort your Alerts in the manner that best suits your time constraints. For example, if you have very limited time and can maybe only get through a few alerts, we recommend sorting your alerts by the highest severity. This way the few alerts you are able to analyze are the most severe.

However, if you have dedicated time to complete all or most alerts each day, sorting from oldest to newest provides the best overall picture of what has been happening on your network since the previous day.

**Step 2: View Events Within Alerts**

Once you have sorted your alerts, select the count number to investigate the events that are related to the alert.
Step 3: Categorize

After investigation into each Alert, categorize it into one of the following:

- Escalated - Sent to your internal security team
- Dismissed - The alert does not need additional analysis by your internal security team.
- False Positive - Should not have been flagged as an alert
This playbook provides detailed instructions, as well as a flowchart for when you see a suspicious Event displayed on your DefenseStorm Dashboard. Knowing what to do when you see something suspicious is the first defense against a cyber attack. Use the play described here to be aware of potential threats before they harm your network.

**STEP 1: Go to the Events Page**
If you see a suspicious spike on the Events portion of your DefenseStorm Dashboard, select the spike to go to the Events page to determine cause.

**STEP 2: Display Only Associated Events**
Once you are in the Events page, move the bars within the graph to pinpoint the spike that caused suspicion.

**STEP 3: Determine Cause**
After you have selected your area to investigate, drill down with filter options to find which application shows the spike. In the screenshot below, CiscoASA is selected as a possible cause, but as you can see, the spike does not display in the graph. Therefore, CiscoASA is not the
The screenshot below is when Malaysia is selected. This clearly displays the suspicious spike and is already rated as a high possibility for threat by the system.

STEP 4: Individual Event Information

To help investigate your system for other related events and alerts, select an individual event from the displayed list. For example, in the screenshot below you can see that the files were sent over using http, and that several files were specifically called out as being high potential threats. This information will be helpful when sorting through your Alert Inbox.
STEP 5: Create an Incident

After you have done a bit of research into an event, select a few events and create an incident.

Fill out the New Incident window as desired, and select Create. All the selected events are now associated with this incident.
STEP 6: Look for Related Alerts

After you have created the incident, go to your Alert Inbox to see if any alerts seem to be related. Remember in STEP 4: Individual Event Information, you looked at the details of an event, here is when it helps. When scrolling through your alert inbox, look for alerts that have to do with the details of your event. In this example, we look for http and the specific files listed. In the screenshot below, we did find alerts associated with HTTP, and selected that group of alerts. This alert has a count of 1015. Select the count number to determine if this alert grouping is indeed related to your incident.

Once you have clicked on the count number, it takes you to the Events page; but only events for the selected alert are displayed. The screenshot below shows that on page 4 of events, we found the event that is related to our incident from the suspicious spike.
Selecting the event gives you more details so you can verify the event has the same source as the one causing your spike.

**STEP 7: Escalate Related Alert**

If you find an alert that is related, as we did in the previous step, escalate that alert grouping to your incident. To do this, simply return to your Alert Inbox, select the Alert group, and escalate it to the incident. Once you escalate the alert to your incident, all alerts associated with the alert group, in this case (g), are also associated with the incident.

**STEP 8: View Incident**
After events and alerts have been attached to your incident, go to the Incidents page and view the incident.

Step 9: Assign the Incident

Now that you have created your incident and added relevant alerts, it’s time to edit the incident. Edit the incident in the following ways:

- Change your ticket state to Analysis.
- Assign Guardian as the incident owner to send them the incident.

You can also add watchers to your incident. Watchers cannot make changes, but are made aware of what is going on.

DefenseStorm Console Tip: All events and alerts that are associated with an Incident are kept forever as part of incident resolution statistics. So you can always come back to a certain incident and report on it.

STEP 10: Add-Ons

The incidents page also allows you to add attachments, links, and policies to your incident to provide any desired additional information.
The Play

The flowchart below shows the play to help your company successfully analyze suspicious activity displayed on your dashboard.
This playbook provides detailed instructions for common DVM troubleshooting resolutions. Knowing what to do when your system displays certain symptoms could greatly reduce your chance of data loss. Use the plays described here to quickly troubleshoot your DVM and get it back up and running smoothly.

First Step

The first step in the event that your DVM goes down, is to contact DefenseStorm. We have been notified of the issue and have started remediation based on our prior agreement with you.

Rebooting the DVM is the last step taken. While the DVM is down, it is still attempting to send logs, and once the connection is made all the logs utilizing TCP Protocol from when the DVM was down are sent to the console, and they display correctly since we utilize the ingestion timestamp, not the time of connection.

Note for Cloud based services

In the event that you DVM goes down, we still receive logs from cloud based service like Office365 and OpenDNS. These items flow from their cloud directly to our cloud, not the DVM. If you laptop utilizes the DefenseStorm Windows Agent (DWA), this also sends data directly to our cloud, bypassing the DVM. Rebooting the DVM causes all logs from the time it went down until the time it is back up to be lost.

DVM Alerts and Troubleshooting Resolutions

Reset DVM Clock

Run the following commands
Disk Almost Full

**Symptom:** DVM gives warning that the disk space is full.

**Cause (possible):** When logs do not rotate off the system as expected or update packages are downloaded more than once, therefore taking up double the space.

**Mitigation Steps:** Manually clean the logs off the system or purge more space.

**STEP 1:** Determine if the disk is full because of log rotation error

Check /var/log for runaway log file sizes (ls -lh /var/log), inspect any very long file using tail -n 40 filenamehere.

**STEP 2:** Determine if the disk is full because of already applied update packages

Run the sudo apt-get autoremove --purge command. This first runs an analysis estimating the reclaimable space, and can be cancelled at this point before any permanent removal is triggered.

**Space commands**

- **df**
  - display disk usage by device

- **du -h**
  - display size of directory, append / to display per file

- **uname -r**
  - display active DVM kernel version (useful when comparing packages on disk)
**Sudo commands**

These commands will need the DVM administrator to input the DVM login password. (commands below: | = |)

- `sudo du -x / | sort -n` — get size of all file objects, then sort top-down
- `sudo apt-get autoremove --purge` — remove all unused / already installed packages

**Syslog Configuration Problems**

**Symptom:** /var/log/syslog-ng.log contains spammed error lines such as, maximum connections reached; rejecting connection. Maximum concurrent connections: 500.

**STEP 1:** Check DVM configuration (the SyslogNG section), and inspect the maxconnections values. If this is lower than the number of machines registered to the DVM, error log spam can overflow the log file size (and possibly fill disk).

The following lines display in: /etc/praesidio/praesidio.conf:

- `[SyslogNG] (port 514, 516, 601…..)`
- `Tcp514maxconnections = 100`
- `Tcp516maxconnections = 100`
- `Tcp601maxconnections = 500`

**STEP 2:** Increase the number of connections for the port in use (example: = 1000),

run `sudo vi /etc/praesidio/praesidio.conf`

**STEP 3:** Edit `/etc/syslog-ng/conf.d/praesidio.conf`
For all config sections that look like:

```plaintext
network(
    ...
    tags("tcp514")
    tags("tcp516")
    tags("tcp601")
)
```

Where `max_connections(100)` is present, replace with `max_connections(1000)`. Or some other high number to reduce possibility of this occurring again.

**STEP 4: Repeat for the other conf sections for ports 516 and 601.**

**STEP 5: Log clean up and final check**

- Delete the error.log and error.log.1 files. (sudo rm error.log)
- Reboot the box (sudo reboot)
- DVM Console --> Get DVM Status
- DVM Console --> Troubleshooting

**STEP 6: Post reboot log check**

Bash Shell --> Check contents of error.log in /var/log.

- Run the command `Tail -n 50 error.log`

**STEP 7: Post reboot monitor of syslog**

Syslog-ng.conf (syslogng)

- Run the command `/etc/syslog-ng/conf.d/praesidio.conf`

---

**Frequent DVM Reboot Alerts**

**Symptom:** The DVM sends unusually frequent reboot alerts.

**Cause:** The reboot required flag sets when an OS package upgrade requests it. The DVM is hardcoded to check for security updates daily. Until all packages have been updated, the alert may continue to display frequently.
Mitigation Steps: Enable the automatic DVM reboot feature. This only reboots the DVM if a security update has been applied in the last day that requires it.

STEP 1: Select Option (11) Configure Automatic Security Updates

Within the DVM’s Main Menu, select option 11 to enable Automatic Security Updates.

[Screenshot of main menu here]

STEP 2: Select Automatic Reboot Time

After you select to enable automatic reboot, set the reboot time.

DVM down soon after reboot

Symptom: After being rebooted, the DVM went down again after an hour.

Root cause: Disk failure was due to log spam from syslog-ng due to too many client connections. For example, if the maximum pool (port 601) is set to 500, and there are 800 machines configured for communication with the DVM, the error spam fills the disk and prevents syslog-ng from starting. This causes event data to never make it to the DefenseStorm platform.

Mitigation Steps: The following actions brought the DVM back to a stable state, and it should prevent this from reoccurring in the near future.
STEP 1: Run the command >> Df -h

• Dev/sd117gb/1.1bg free

STEP 2: Run the command >> Du -h/var/log

• 16G/var/log

STEP 3: Run the command >> cd/var/log

STEP 4: Run the command >> tail python_sqs.log (blank)

STEP 5: Run the command >> ls -lh

• Error.log4.5G
• Error.log.1 (sep 18)  5.8G
• Syslog3.#G

STEP 6: Run the command >> tail error.log

• “Rejecting connection from client: maximum connection attempts reached”
  ○ IPs listed are local bank IPs.
    • Desktops, Windows servers, various hardware

STEP 7: Run the command >> du -h .

• 16G/var/log
• ....


STEP 8: Identify the syslog config problem

correct the syslog config problem before purging logs and restoring customer asset connectivity to DVM.

1.
1. Check DVM configuration (the SyslongNG section), and inspect the maxconnections values. If this is lower than the number of machines registered to the DVM, error log spam can overflow the log file size (and possible fill disk).

/etc/praesidio/praesidio.conf

[SyslogNG] (port 514, 516, 601….)

Tcp514maxconnections = 100
Tcp516maxconnections = 100
Tcp601maxconnections = 500

>> sudo vi/etc/praesidio/praesidio.conf

- Changed entries to 1000 on each port.

>> /etc/syslog-ng/conf.d/praesidio.conf

STEP 9: Mitigation steps for this file:

For all config regions that look like:

Network (
...

  tags("tcp514")
  tags("tcp516")
  tags("tcp601")

Example:

Network (  
  port(514)  
  ...
  ...

...
Max_connections (100)

tags("tcp514")

**STEP 10:** Change highlighted to: `max_connections(1000)`

**STEP 11:** Repeat for other conf sections for 516 and 601.

**STEP 12:** Delete the `error.log` and `error.log.1` files.

Run the following command `>> sudo rm error.log`

**STEP 13:** Reboot the box

Run the following command `>> sudo reboot`

**STEP 14:** DVM Console → Get DVM Status

- All services up, 37% disk usage, queues are empty

**STEP 15:** DVM Console → Verification of resolution

1. Ran connectivity test, all green now
2. Post reboot log check:
   1. Bash Shell → Check contents of `error.log` in `/var/log`
   2. Run command `>> Tail -n 50 error.log`

   1. Just NTP errors observed. No issues with IPs right now.

---

**Verify data flow**

**STEP 1:** Open a shell session on the DVM.

**STEP 2:** From the DVM, run the following command:

```
sudo tcpdump -vvv -s 4096 -X host 10.10.10.10
```
And port 514 where the IP address is the device sending log data and the port is the port it is
sending to, which is typically 514 or 516.

**Increase partition size**

For the purpose of this procedure, we are increasing the primary partition to 22 gigs. Always make
a snapshot of backup of the current instance, just in case something goes wrong.

**STEP 1:** Log into the DVM and go to the command line.

**STEP 1:** Turn off swap

```bash
sudo swapoff --all --verbose
```

**STEP 1:** Remove swap partition

```bash
sudo parted /dev/sda rm 2
```

**STEP 1:** Resize root partition

```bash
sudo parted /dev/sda resizepart 1 yes 24000
```

**STEP 6:** Interactively make new swap partition

```
praesidio@ubuntu:~$ sudo parted /dev/sda mkpart
Partition type? primary/extended? primary
File system type? [ext2]? linux-swap
Start? 24001
End? 25000
```

**STEP 7:** Make swap filesystem

```bash
sudo mkswap /dev/sda2
```

**STEP 8:** Turn swap back on

```bash
sudo swapon --all --verbose
```
STEP 9: Resize root filesystem

```bash
sudo resize2fs /dev/sda1 22000M
```

STEP 10: Check that filesystem has grown

```bash
df -h
```

STEP 11: Reboot

```bash
sudo reboot
```

STEP 12: After reboot check that filesystem is still 22GB

```bash
df -h
```

STEP 13: Check swap is present (you should see 900 odd M for swap)

```bash
free -h
```

**High CPU Usage**

Symptom: Seems that the DVM is running hot with a low number of CPUs.

Cause: While copying the syslog file, the DVM got stuck in a bad state.

Mitigation Steps: If it is the syslog file that is stuck, you can restart it without having to reboot the whole system. The following steps bring the DVM back to a healthy state and should return the DVM to a normal usage.

STEP 1: Enter the bash shell

Execute the command `sudo top`

This provides a table with all running processes. At least one process should display a high CPU percentage.

STEP 2: Restart the stuck process or DVM

If syslog-ng service is the process stuck, then you can restart it, without rebooting the whole system by executing the following command: `sudo/etc/init.d/syslog-ng restart`
If syslog-ng is not the process that is stuck, you can always try a reboot of the DVM itself. If that still does not set the DVM to a healthy CPU usage state, then escalate this further to DefenseStorm.

Missed Events

Symptom: Console may miss a few event logs.

Cause: Traffic too high, and compression setting not correct.

Mitigation Steps: If you believe your DVM may be dropping events, you can follow these mitigation steps to create a fallback for network monitoring.

STEP 1: Nload

1. Nload provides a good picture of overall network utilization in real-time, displayed per network interface. Useful to determine if a single NIC is saturated.

2. Install steps:

   1. Sudo apt-get update
   2. Sudo apt-get upgrade
   3. Sudo apt-get install nload

STEP 2: Iftop

1. Iftop provides a good picture of overall network utilization, with utilization displayed on a per-process level. Useful to determine with processes are using bandwidth and identify unexpected sources.

2. Install steps:

   1. Sudo apt-get install iftop

Usage:
Iftop, ran by itself, drops into a console monitoring mode. For the DVM, you’ll want to identify the processes that are:

- Receiving traffic on syslog ports
- Sending traffic out to an external AWS IP over port 443 (https)

Screenshots of the various values here, along with the measured totals from vnstat, should help us understand the characteristics of the network better.

STEP 3:Mtr (on ubuntu: mtr-tiny)

1. MTR can be used to trace network routes and obtain reporting data. Useful to determine if the path to our SQS server (Amazon US-West) is congested, and if the source of the issue is within the customer network, customer ISP, or caused by an external network location altogether

2. Install steps:

   1. Sudo apt-get install mtr-tiny

Additional info (external link to Linode’s website):
https://www.linode.com/docs/networking/diagnostics/diagnosing-network-issues-with-mtr

**Down Disk Queue during Start-up**

Sometimes during the initial DVM startup, the screen displays a disk write error (example shown below).
To correct this error, simply reboot the DVM by selecting Option 9 - Reboot from the DVM main menu.
This playbook provides detailed information on the cybersecurity significance of alerts you may see through the DefenseStorm Console. These alerts are taken from the Trigger Library (Alerts > Library) and from the expertise of Guardian and their knowledge of additional common alerts.

**Bro IDS**

**Bro FTP**

Query: `app_name:(bro ftp)`

Details: Bro is a network analysis framework that is included with the Security Onion software and has many protocol analyzers. One of these protocol analyzers is the ability to monitor FTP traffic.

Guardian Comment: A Bro FTP trigger is associated with an insecure file transfer protocol (FTP), and may indicate data exfiltration. SHA1 and MD5 hash values are also contained in the data as well as name and path.

**Bro RADIUS**

Query: `app_name:(bro_radius)`

Details: Bro is a network analysis framework that is included with the Security Onion software and has many protocol analyzers. One of these protocol analyzers is the ability to monitor BRO RADIUS traffic.

Guardian Comment: A Bro RADIS trigger is associated with a Remote Authentication Dial-In User Service Remote Authentication Dial-In User Service (RADIUS), which is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
Bro SSH

Query: app_name:(bro_ssh)

Details: Bro is a network analysis framework that is included with the Security Onion software and has many protocol analyzers. One of these protocol analyzers is the ability to monitor SSH traffic.

Guardian Comment: A Bro SSH trigger is associated with Secure Shell (SSH) which is a secure way to transfer data over the Internet. This is useful to detect and monitor SSH network connections.

Bro Tunnels

Query: app_name:(bro_tunnels)

Details: Bro is a network analysis framework that is included with the Security Onion software and has many protocol analyzers. One of these protocol analyzers is the ability to monitor tunnel traffic.

Guardian Comment: A Bro Tunnel is associated with any connection that occurs over a tunnel such as (Teredo, AYIYA, or IP-in-IP). This is useful to detect and monitor tunnel network connections.

Security Onion Offline

Query: bro*

Details: Bro is a network analysis framework that is included with the Security Onion software.

Guardian Comment: A Security Onion Offline trigger is associated with anytime the Security Onion software is offline or not logging. It’s important to restart and restore the Security Onion hardware and services in order to provide additional security logs and visibility into the network.
Cisco ASA AAA Login

Query: (syslog_level:6) category: ("user authentication" OR "vpn client" OR "command interface")

Details: Cisco recommends to enable AAA (Authentication, Authorization, and Accounting) authentication on the firewall, in order to increase the security of the device. AAA ensures that only authorized users have access to the management of the firewall.

Guardian Comment: A Cisco ASA AAA Login trigger is associated with indicating a login of VPN users, firewall sessions, or administrators. It is useful and important to detect and monitor this type of network activity.

Cisco ASA CLI Activity

Query: app_name: ("cisco Cisco ASA") category: ("command interface")

Details: Cisco CLI (Command Line Interface) is the primary method to manage, and monitor Cisco firewalls.

Guardian Comment: A Cisco ASA CLI Activity trigger is associated with command-line interface activity. It is useful and important to detect and monitor CLI activity.

Cisco ASA Duplicate TCP Syns

Query: (syslog_level:4 AND "Duplicate TCP") app_name: ("cisco Cisco ASA")

Details: Cisco message to show when the firewall detects duplicate TCP syns on the network.

Guardian Comment: Notification that a duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number than the SYN that opened the embryonic connection. This could indicate that SYNs are being spoofed.

Cisco ASA Failed To Locate Egress Interface

Copyright © 2015 - 2016 DefenseStorm, LLC. All rights reserved.
Query: syslog_level:6 AND "Failed to locate egress"

Details: Cisco error message to show when the firewall fails to locate the egress interface.

Guardian Comment: A Cisco ASA failed to locate egress interface trigger is a notification that ASA failed to locate egress interface. This is usually indicative of a network problem that needs to be escalated to the POC for resolution if the error messages are continuous.

Cisco ASA Failed to Locate Next Hop

Query: syslog_level:6 AND "Failed to locate next hop"

Details: Cisco ASA error message when the firewall is unable to locate the next hop on the network.

Guardian Comment: A Cisco ASA failed to locate next hop trigger is a notification that due to a misconfiguration ASA failed to locate next hop. This is usually indicative of a network problem that needs to be escalated to the POC (point of contact) for resolution if the error messages are continuous.

Cisco ASA Firewall Changes

Query: (write OR "111010" IR "101008" -teardown) app_name:"cisco asa"

Details: Cisco ASA message when the firewall detects any firewall change on the device.

Guardian Comment: A Cisco ASA firewall changes trigger, is a notification that configuration changes have been made by a user. It’s important to track firewall changes with proper change controls on a network, in order to detect any unauthorized firewall changes.

Cisco ASA Invalid Transport

Query: syslog_level:4 AND "invalid transport"

Details: Cisco ASA error message when the firewall detects an invalid transport, which the source or the destination protocol port number is equal to 0.
Guardian Comment: A Cisco ASA invalid transport trigger is a notification that there is an invalid transport number. If this error message occurs on the internal network is could be indicative of a network problem, or if coming from an externally it could be a sign of DDOS attack.

**Cisco ASA Monitor Denied Packets for DDoS**

Query: (deny) app_name:("Cisco ASA")

Details: Cisco ASA message occurs when anytime a deny event is logged on the firewall.

Guardian Comment: A Cisco ASA monitor denied packets for DDOS trigger is a notification that the firewall denied packets to prevent a potential DDoS attack. This may or may not indicate a DDOS attack.

**Cisco ASA NAT Reverse Path Failure**

Query: (syslog_level:5 AND "NAT reverse path failure") app_name:("cisco Cisco ASA")

Details: Cisco ASA message occurs when the NAT rules don’t match, usually indicative of site to site VPN.

Guardian Comment: A Cisco ASA NAT (Network Address Translation) reverse path failure is a notification that NAT rules don’t match in both directions across interfaces. This indicates a networking problem that needs to be corrected by a network engineer.

**Cisco ASA Received ARP Request Collision**

Query: (syslog_level:4 AND "Received ARP") app_name:("cisco Cisco ASA")

Details: Cisco ASA warning message occurs when two devices on the network obtain the same the ip address with the same MAC address.

Guardian Comment: A Cisco ASA received ARP request collision is a notification that there is a duplicate IP address in the network. This indicates a networking problem that needs to be corrected by a network engineer, or this also can be a security attack and a device is trying to
flood a network.

Cisco ASA Sshd Fatal System Error

Query: syslog_level:2 AND "fatal"

Details: Cisco ASA message occurs when SSHd fails to authenticate a user over the SSH protocol. This could be caused by wrong/missing encryption keys, or incorrect passphrase.

Guardian Comment: A Cisco ASA Sshd fatal system error is a notification that SSHd failed to authenticate a user. If a network receives multiple messages when this occurs, it could indicate a security attack/problem and needs to be further investigated by the onsite network engineer.

Cisco ASA System Memory >85%

Query: syslog_level:2 AND "System Memory"

Details: Cisco ASA message occurs when the firewall is low on free memory, which could cause packet drop problem, and networking problem.

Guardian Comment: A Cisco ASA System Memory >85% is a notification that system is low on free memory. This could indicate a sustained network attack that is using system memory, or a physical problem with the device.

DVM

DVM Disk Almost Full

Query: app_name:PVM_STATS root_partition:("90%" OR "91%" OR "92%" OR "93%" OR "94%" OR...
Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored.

Guardian Comment: DefenseStorm Virtual Machine has disk near capacity and can cause failure to the DVM if not addressed in a timely manner. This usually will be resolved automatically on a nightly reboot, but if not this might need to be escalated to the Engineering Team.

**DVM Disk Queue Large**

Query: app_name:PVM_STATS disk_queue_count:>1000

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored.

Guardian Comment: DefenseStorm Virtual Machine has a disk queue issue which occurs when a large amount of DVM events are failing to send to SQS, and 1000+ events have been stored on the disk. The cause could be an overloaded DVM, too many hosts on one DVM, or a problem with the ingestion service.

**DVM Disk Queue Malfunctioning**

Query: app_name:PVM_STATS -pdiskqueue:UP

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored. This triggered when the DVM’s disk queue service (pDiskQueue) is either not running or not able to process events.

Guardian Comment: DefenseStorm Virtual Machine has a disk queue issue. This may be resolved by restarting the pDiskQueue service, and restarting the DVM. This error becomes critical when both syslog-ng service and pDiskQueue service aren’t running.
**DVM Dropped Events**

Query: `app_name:PVM_STATS dropped_events:>0`

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored. This alert occurs when the number of events reaches a certain threshold.

Guardian Comment: DefenseStorm Virtual Machine (DVM) keeps a running total count since the syslog-ng service was started. This count doesn’t not reset during normal operation and it may be necessary for Engineering to manual adjust this count on per customer basis as needed.

**DVM Error**

Query: `app_name:PVM_STATS severity:high`

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored.

Guardian Comment: DefenseStorm Virtual Machine generic error message. These types of events will need to be investigated by Engineering with the customer to find root cause if error message persist over time.

**DVM No Stats**

Query: `app_name:PVM_STATS`

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored. This alert indicates that no heartbeat message from the DVM have been received in the specified timeframe.

Guardian Comment: DefenseStorm Virtual Machine stopped log processing. If error message persists Guardian recommends following the general DVM guide on Connect for basic network and SQS troubleshooting steps. In some cases, Engineering will need to be engage with the customer to further troubleshoot the problem and find root cause.
DVM Reboot Required

Query: app_name:PVM_STATS reboot_required:true

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored. This alert is triggered when the DVM has downloaded automatic security updates and require a DVM reboot in order to apply the updates.

Guardian Comment: DefenseStorm Virtual Machine reports reboot required. If the customer has enabled automatic reboot for DVM updates and specified a timeframe, then this alert should clear once the time has occurred. If the customer has disabled automatic reboot for updates, then the alert will continue to fire until the customer has manually rebooted the DVM.

DVM Syslog-NG Malfunctioning

Query: app_name:PVM_STATS -syslog_ng:UP

Details: The DefenseStorm Virtual Machine (DVM), as of version 1.0.7, sends 1 minute heartbeats to the Web Console and those heartbeats contain information to be monitored. This alert triggers when the syslog-ng service is down on the DVM.

Guardian Comment: This is the primary event ingestion service which pushes log data from customer hosts into the DefenseStorm SQS queue. DefenseStorm Virtual Machine has a syslog-ng issue.

FortiGate

FortiGate Administrator Activity

Query: app_name:(fortigate) subtype:(system) AND "Administrator"

Details: This is the default notification for administrator activity on a Fortinet firewall.
Guardian Comment: A FortiGate Administrator Activity trigger is notification of administrator activity. This is important to detect and monitor who is making changes on the firewall.

**FortiGate Category Hacking**

Query: ( "type=utm" AND (cat=3 catdesc="Hacking")) app_name:(fortigate)

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate Category Spam Url trigger indicates that a user/system accessed a web page or domain that was rated as hacking, which may have tools, processes, and procedures related to hacking.

**Fortigate Category Malicious Websites (Blocked)**

Query: ("type=utm" AND (cat=26)) app_name:(fortigate)

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate Category Malicious Websites blocked trigger indicates that a user/system accessed a web page or domain that was classified as a malicious website and was blocked by the firewall. Malicious webpages can be used to harvest information from client computers, download malicious files with a virus or trojan.

**Fortigate Category Phishing**

Query: "type=utm’ AND (cat=61 catdesc="Phishing")

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate Category Phishing trigger indicates that a user accessed a web page or domain that is commonly found in reported phishing related emails.
FortiGate Category Proxy Avoidance

Query: "type=utm" AND (cat=59 catdesc="Proxy Avoidance")

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate Category Proxy Avoidance trigger indicates that a user/system accessed a web page or domain that has information or tools on bypassing firewall controls and policy via anonymous proxy servers.

FortiGate Category Spam URLs

Query: "type=utm" AND (cat=86 catdesc="Spam URLs")

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate Category Spam URL trigger indicates that a user accessed a webpage or domain that is commonly found in spam related emails.

FortiGate Configuration Backup

Query: app_name:(fortigate) subtype:(system) AND "backed up the configuration"

Details: This is the notification when a user performs a configuration backup on the Fortinet firewall.

Guardian Comment: A FortiGate Configuration Backup trigger is a notification that the system backed up the configuration. This is important to monitor and detect who is making a backup of the firewall configuration.

FortiGate IPSEC VPN Errors
Query: "type=event" "subtype=vpn***" AND "error"

Details: This is the notification when an IPSEC VPN error occurs on the network.

Guardian Comment: A FortiGate IPSEC VPN Error trigger is a notification of errors generated during Phase1 or Phase2 of VPNs. It is important to detect and monitor VPN errors on a network, this could detect unauthorized remote access on the firewall, or configuration problems on the network.

**FortiGate IPS Signature Detected**

Query: "Type: utm;" AND " Subtype: ips"

Details: The FortiGate firewalls offers an Intrusion Protection System (IPS) in order to activity monitor and block external network based attacks and threats. The IPS is turned is signature based, and is tuned often by Fortinet.

Guardian Comment: A FortiGate IPS Signature Detected trigger is a notification that the intrusion prevention system (IPS) has detected a known signature.

**FortiGate Phish Detection**

Query: "Phishing") category:(phishing) app_name:(fortigate)

Details: This is a notification when phishing is detected on the firewall.

Guardian Comment: A FortiGate Phish Detection trigger is a notification that phishing activity was detected.

**FortiGate Proxy Avoidance**

Query: app_name:(fortigate) category:="proxy avoidance"

Details: This is a notification when proxy avoidance is detected on the firewall.

Guardian Comment: A FortiGate Proxy Avoidance trigger is a notification of proxy avoidance.
possibly to bypass browsing restrictions.

**FortiGate URLs Blocked By Policy**

Query: 

```
("URL was blocked because it is in the URL filter list") app_name:(fortigate)
```

Details: The Fortinet firewall includes FortiGuard URL which provides web filtering protection. It includes many web content categories and classifications.

Guardian Comment: A FortiGate URLs Blocked by Policy trigger indicates that a user accessed a web page or domain that was blocked by policy, which was set by the firewall administrator.

**FortiGate VPN Critical Events**

Query: 

```
"type-event" "subtype=vpn level=critical"
```

Details: This is a notification when a critical VPN event is logged from the firewall.

Guardian Comment: A FortiGate VPN Critical Events is a trigger for a notification of VPN critical errors. It is important to detect and monitor VPN errors on a network, this could detect unauthorized remote access on the firewall, or configuration problems on the network.

**FortiGate VPN Error Events**

Query: 

```
"type-event" "subtype=vpn level=error"
```

Details: This is a notification when VPN error events are logged from the firewall.

Guardian Comment: A FortiGate VPN Error Events is a trigger for a notification of a VPN error occurrence. It is important to detect and monitor VPN errors on a network, this could detect unauthorized remote access on the firewall, or configuration problems on the network.
Location

Source/Destination China

Query: geo_dest.country:china OR geo_src.country:china

Details: Detection of network that is either source or destination China, which is usually malicious.

Guardian Comment: A Source/Destination China trigger could be associated with malicious traffic on the network. There are some advertisers that leverage servers in China for advertising, but for the most part most of the traffic is malicious.

Source/Destination Russia

Query: geo_dest.country:russia OR geo_src.country:russia

Details: Detection of network that is either source or destination Russia, which is usually malicious.

Guardian Comment: A Source/Destination Russia trigger could be associated with malicious traffic on the network. There are some advertisers that leverage servers in Russia for advertising, but for the most part most of the traffic is malicious.

Source/Destination Iran

Query: geo_dest.country:iran OR geo_src.country:iran

Details: Detection of network that is either source or destination Iran, which is usually malicious.

Guardian Comment: A Source/Destination Iran trigger could be associated with malicious traffic on the network.

Source/Destination Ukraine
Query: geo_dest.country:ukraine OR geo_src.country:ukraine

Details: Detection of network that is either source or destination Ukraine, which is usually malicious.

Guardian Comment: A Source/Destination Ukraine trigger could be associated with malicious traffic on the network.

Source/Destination Brazil

Query: geo_dest.country:brazil OR geo_src.country:brazil

Details: Detection of network that is either source or destination Brazil, which is usually malicious.

Guardian Comment: A Source/Destination Brazil trigger could be associated with malicious traffic on the network.

Source/Destination North Korea

Query: geo_dest.country:(north korea) OR geo_src.country:(north korea)

Details: Detection of network that is either source or destination North Korea, which is usually malicious.

Guardian Comment: A Source/Destination North Korea trigger could be associated with malicious traffic on the network.

Source/Destination Romania

Query: geo_dest.country:(romania) OR geo_src.country:(romania)

Details: Detection of network that is either source or destination Romania, which is usually malicious.

Guardian Comment: A Source/Destination Romania trigger could be associated with malicious traffic on the network.
traffic on the network.

Microsoft Windows

Account Lockouts

Query: event_id:4740 OR category:"account lockout"

Details: A user account was locked

Guardian Comment: A user account locking alone is not an indication of an attack but normally the first step of gaining access before an attack can begin. If you see failed logins or account lockouts at a rate higher than a user can generate (100’s in an hour) or outside of normal business hours contact the bank POC or the user whose account was locked and have them verify they locked their account. If they did not find lock their account or attempt to login at this time recommend running antivirus on the machine to check for malware.

Administrator Failed Login (Bad Password or Unknown Username)

Query: event_id: (4625) AND "Status: 0xc000006d Sub Status: 0xc0000064"AND "Account Name: administrator"

Details: An administrator failed to authenticate (failed login, bad password, unknown username.)

Guardian Comment: A single failed login for an administrator is not alone an indication of an attack but repeated failed login attempts (examples 1 per hour over days or 100 over an hour) should be investigated. Typically a “noisy hacker” will use a tool that attempts over a 100 passwords per minute however a hacker that is attempting to hide their trail might attempt a lower rate so it doesn’t draw as much attention. These should be monitored and if more than 5 to 10 appear in a week recommend following up with bank POC and ensuring this is not a maintenance issue with a password that has expired, if the bank POC can not identify what
caused the failed logins recommend running anitvirus on the machine to check for malware. If none is found host should be monitored by bank POC to find out if on site personnel are attempting to access an account they don’t have privileges to.

**Alert on Anonymous Logins**

**Query:** user_name: ("anonymous logon")

**Details:** means that an anonymous logon has been completed to the server. If you want to disable this have a look at this article on restricting anonymous access:

Guardian Comment: While Guardian personally recommends disabling for auditing purposes. Anonymous logon events in your Security log look more dangerous than they really are. By default, the information you can access when you connect anonymously is extremely limited — basically, you can access only a list of shared folders and usernames. (I know; that gives an intruder a list of targets, but there are lots of other ways to get usernames.)

You can completely disable anonymous logins (aka null sessions), but doing so might affect accessibility by users in trusting domains. Before changing policies throughout your domain, I suggest testing them on a limited number of systems.

**Source:** [http://windowsitpro.com/systems-management/disabling-logging-anonymous-logon-events](http://windowsitpro.com/systems-management/disabling-logging-anonymous-logon-events)

**An Attempt Was Made To Access An Object**

**Query:** (event_id:4663) app_name: ("microsoft-windows-security-auditing")

**Details:** An attempt was made to access an object.

Guardian Comment: Alone an attempt to access a shared object represents no security risk, and should be considered normal activity, however combined with other alerts such as a failed login combined by a successful login outside of business hours could represent a host that has been compromised and the attacker is now attempting to escalate privileges. Note events 4656 and 4658 will not appear unless the subcategory "Handle Manipulation" is enabled along with the target sub-category. Microsoft explains that this was done to make it more difficult to enable these noisy events. They feel the event 4663 is better.
A Network Share Object Was Accessed

Query: (event_id:5140) app_name:("microsoft-windows-security-auditing")

Details: A network share object was accessed.

Guardian Comment: Similar to an attempt was made to access a shared object, this alone does not represent an indication of an attack and is normal activity, however combined with other alerts should be investigated closely. An attacker may attempt to gain access to a host then escalate their privileges or see what they can access inside the network.

A New Process Has Been Created

Query: (event_id:4688) app_name:("microsoft-windows-security-auditing")

Details: New process creation.

Guardian Comment: This is normal activity, however if this activity is seen outside of business hours or if you see this activity changing or creating processes in temp folders it should be investigated fully to ensure the process created is valid.

Application Error

Query: ([event_id:1000]) app_name:(application_error)

Details: Application reported an error.

Guardian Comment: It is common to see application error, or crashed messages, however if there is a spike in activity it will most likely represent a configuration error after some time of system change but should be investigated to verify.
**AppLocker Block**

Query: event_id:(8003 OR 8004) AND severity:(high OR medium) AND app_name:microsoft-Windows-applocker

Details: was allowed to run but would have been prevented from running if the AppLocker policy were enforced (8003) or was not allowed to run (8004) had Enforce rules enforcement mode were enabled.

Guardian Comment: Depending on whether or not an AppLocker policy was enforced, a file may or may not be allowed to run.

**A Service Was Changed From Auto Start to Demand Start**

Query: (event_id:7040) app_name:(service_control_manager)

Details: Service start change from auto to demand start.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

**Audit Log Cleared**

Query: (event_id:7040) app_name:(service_control_manager)

Details: The audit log was cleared.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

**Audit Policy Changed on Object**

Query: event_id:4715
Details: The audit policy (SACL) on an object was changed.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

**Backup Of Protection Master Key**

Query: event_id:4692 AND "Backup"

Details: Backup of data protection master key was attempted.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

**Blue Screen of Death**

Query: (event_id:1001) app_name:("microsoft-windows-wer-systemerrorreporting")

Details: Windows crash with blue screen of death.

Guardian Comment: It is normal to see two or three of these in a month, however a large amount 3 in a 24 hour period could indicate an malware on the network and hosts should be reviewed individually and compared against each other for other threat alerts.

**Boot Start Or System Start Driver(s) Did Not Load**

Query: (event_id:(7026)) app_name:(service_control_manager)

Details: Boot Start or System Start driver(s) did not load.

Guardian Comment: This alerts should be considered normal however a spike in activity could indicate a configuration error or that malware has made it onto a host an alerted the host. This activity should be reviewed and if a host spikes it should be scanned for malware.
Command Prompt and Batch File Execution

Query: (cmd.exe) AND (*.bat)

Details: DOS command shell and batch file processing.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

Detected An Invalid Image Hash Of A File

Query: (event_id:5038) app_name:("microsoft-windows-security-auditing")

Details: Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.

Guardian Comment: An invalid hash indicates corruption of the image intended to be used.

Detected An Invalid Page Hash Of An Image File

Query: (event_id:6281) app_name:("microsoft-windows-security-auditing")

Details: Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.

Guardian Comment: An invalid page hash indicates corruption of the image intended to be used. The hash inside this file should be scanned on a site such as virustotal to verify it as harmless.

Detected Malware
Query:  event_id:(1006) AND event_type:WARNING

Details: The antimalware engine found malware or other potentially unwanted software (Windows Defender Event).

Guardian Comment: This alert needs to be reviewed and the hash inside the file scanned and verified as harmless on a site such as virustotal.

---

**Encrypted Recovery Policy Changed**

Query:  (event_id:4714) app_name:("microsoft-windows-security-auditing")

Details: Encrypted data recovery policy was changed.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could indicate an issue.

---

**Enhanced Mitigation Experience Toolkit**

Query:  app_name:(emet) event_id:(52)

Details: EMET crash.

Guardian Comment: EMET notifies users when a mitigation event occurs (via an application in Taskbar Notification Area, aka System Tray) and events are recorded into Application log of Event Viewer. You can also use the icon to open EMET.

Source: https://support.microsoft.com/en-us/kb/2458544

---

**Failed Kernel Driver Loading**

Query:  (event_id:2119) app_name:("microsoft-windows-kernel-pnp")

Details: Kernel driver failed during loading
Guardian Comment: Plug and play device driver failed to load. This is normal but if a spike occurs review the host that spiked to ensure it was a maintenance related, if other attack indicators are found recommend removing machine host from network and running an antivirus check on machine.

**Group Policy Application Failed Due to Connectivity**

Query: (event_id:1129) app_name: ("microsoft-windows-grouppolicy")

Details: This may be a transient condition. A success message would be generated once the machine gets connected to the domain controller and Group Policy has successfully processed. If you do not see a success message for several hours, then contact your administrator.

Guardian Comment: The processing of Group Policy failed because of lack of network connectivity to a domain controller.

**Group Policy Error**

Query: (event_id:1125) app_name: ("microsoft-windows-grouppolicy")

Details: The processing of Group Policy failed because of an internal system error. Please see the Group Policy operational log for the specific error message. An attempt will be made to process Group Policy again at the next refresh cycle.

Guardian Comment: The Group Policy service detected an internal error during Group Policy processing.

**Host Shutdown Or Restart**

Query: (event_id:1074) app_name: (user32)

Details: System restart/reboot due to user or software input.

Guardian Comment: Normal activity but should be monitored, if there is a spike in this activity and combined with other alerts such as successful logins outside of normal times could
Internet Explorer Add-On Application

Query: event_id:(1 OR 2) AND app_name:application-addon-event-provider

Details: Add on applications in Internet Explorer

Guardian Comment: While add-ons can make your browsing experience better by giving you access to great web content, some add-ons can pose security, privacy, or performance risks. Make sure any add-ons you install are from a trusted source.

Note: plug-ins should be approved on an as needed basis, these can open up back door vulnerabilities to your network and should not be left up to end users to add without an approval process.

Kerberos Pre-Authentication Failure

Query: ((event_id:4771) app_name:('microsoft-windows-security-auditing'))
event_type:audit_failure

Details: System restart/reboot due to user or software input.

Guardian Comment: At the beginning of the day when a user sits down at his or her workstation and enters his domain username and password, the workstation contacts a local DC and requests a TGT. If the username and password are correct and the user account passes status and restriction checks, the DC grants the TGT and logs event ID 4768 (authentication ticket granted).

If the ticket request fails, Windows either logs this event, failure 4771, or 4768 if the problem arose during "pre-authentication". In Windows Kerberos, password verification takes place during pre-authentication.

The User field for this event (and all other events in the Audit account logon event category) doesn't help you determine who the user was; the field always reads N/A. Rather look at the Account Information: fields, which identify the user who logged on and the user account's DNS suffix. The User ID field provides the SID of the account.
Windows logs other instances of event ID 4768 when a computer in the domain needs to authenticate to the DC typically when a workstation boots up or a server restarts. In these instances, you’ll find a computer name in the User Name and fields. Computer generated kerberos events are always identifiable by the $ after the computer account’s name.

Source: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4771

### Keberos Authentication Ticket audit failure

Query: (event_id:4768) app_name:('microsoft-windows-security-auditing') NOT service_name:krbtgt event_type:audit_failure) NOT account_name:('$') NOT target_user_name:('$')

Details: System restart/reboot due to user or software input.

Guardian Comment: This is covered in section above under Kerberos Pre-Authentication Failure tab.

Source: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4771

### Kerberos Service Ticket audit failure

Query: (event_id:4769) app_name:('microsoft-windows-security-auditing') NOT service_name:krbtgt event_type:audit_failure

Details: System restart/reboot due to user or software input.

Guardian Comment: This lets you monitor the granting of service tickets. Service tickets are obtained whenever a user or computer accesses a server on the network. For example, when a user maps a drive to a file server, the resulting service ticket request generates event ID 4769 on the DC. Alone this is not an indication of an security event but combined with other alerts could indicate an attempt of an attacker to alert the victim network.

Source: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4769
Login Failure Bad Password Or User Name Unknown

Query: event_id:(4625) AND "Status: 0xc000006d Sub Status: 0xc0000064"

Details: Identifies the account that requested the logon - NOT the user who just attempted logged on. Subject is usually Null or one of the Service principals and not usually useful information. See New Logon for who just logged on to the system.

Guardian Comment: This is a useful event because it documents each and every failed attempt to logon to the local computer regardless of logon type, location of the user or type of account. Alone this is normal activity, however if you see several hundred failed logins for a user (especially outside of business hours) recommend following up with the user to ensure they actually made the login attempts.

Login with Explicit Credentials

Query: (event_id:4648) app_name:("microsoft-windows-security-auditing")

Details: Event 4648 is a useful event for tracking several different situations:

- A user connects to a server or runs a program locally using alternate credentials. For instance, a user maps a drive to a server but specifies a different user’s credentials or opens a shortcut under RunAs by shift-control-right-clicking on the shortcut, selecting Run as..., and then filling in a different user’s credentials in the dialog box that appears. Or a user logs on to a web site using new specific credentials. That is the case above in the example - Administrator was logged on to the local computer and then accessed a SharePoint server sp01.icemail.com as rsmith@mtg.com.
- This event is also logged when a process logs on as a different account such as when the Scheduled Tasks service starts a task as the specified user. Logged on user: specifies the original user account.
- With User Account Control enabled, an end user runs a program requiring admin authority. You will get this event where the process information is consent.exe. Unfortunately, Subject does not identify the end user.
Guardian Comment: Monitored for unauthorized access or indicator of a potential breach.

This is normal but if a noticeable spike occurs (noticeable in 30 day view) review the host that spiked to ensure it was a maintenance related, if other attack indicators are found recommend removing machine host from network and running an antivirus check on machine.

Logon Events (Success)

Query: (event_id:4624) app_name:('microsoft-windows-security-auditing')

Details: Successful logon detected.

Guardian Comment: This is a highly valuable event since it documents each and every successful attempt to logon to the local computer regardless of logon type, location of the user or type of account. If you see a spike in activity that can not be related to patching, maintenance etc or if you see a login for a user outside of normal work hours (example Sarah normally logsins between 8-5 and has now logged in at 3am on a Sunday morning. Review activity to see what was done under her ID and hostname, if activity appears legitimate close the incident but if you see other attack indicators such as event_id 4624 (pass-the-hash-detection) and multiple failed logins before the successful login contact bank POC to verify if activity is legitimate.

Logon Type 3 & NTLM Auth (Pass-The-Hash Detection)

Query: (event_id: 4624 and logon_type: 3 AND auth_package: NTLM) app_name:('microsoft-windows-security-auditing')

Details: This event basically means an account was logged on successfully.

Guardian Comment: While this event is not a direct indication of an attack, this alert should be monitored. If the activity occurs outside of business hours or if the activity occurs on a new host, Guardian team contact bank POC to ensure activity is valid. Note: This could represent attempts to use local accounts to log on remotely from other systems. If not occurs and is not approved by explicitly approved by bank POC contact them to ensure an escalation of privileges has not occurred.
New MSI File Installed

Query: (event_id:(1022 OR 1033)) app_name:(msiinstaller)

Details: Windows successfully installed an update or the software package. Event ID 1033 may include additional information such as product name, product version, product language, and installation success or error status. This is a normal, informational event, recording the installation of a program. However, only if the status code is 0 the installation is actually successful. Any other code would indicate that the installation encountered a problem.

Guardian Comment: Microsoft Windows Installer is used to install applications on a computer. Unusual activity or installation of unapproved applications may indicate malicious activity.

Password Change Attempt

Query: (event_id:4723) app_name:("microsoft-windows-security-auditing")

Details: The user attempted to change his/her own password. This event is logged as a failure if his new password fails to meet the password policy. If the user fails to correctly enter his old password this event is not logged.

Guardian Comment: Password activity is of significant interest. Failure of this type indicates the user may not be familiar with the password policy and may be an outsider.

Password Reset Attempt

Query: (event_id:(4724)) app_name:("microsoft-windows-security-auditing")

Details: This event is logged as a failure if the new password fails to meet the password policy. This event is logged as a failure if his new password fails to meet the password policy. If the user fails to correctly enter his old password this event is not logged.

Guardian Comment: Auditing password reset attempts on the network and watching for potential malicious activity.
Powershell Execution

Query: (cmd /c powershell)

Details: Powershell execution from command line (cmd.exe). PowerShell is a built-in command shell available on every supported version of Microsoft Windows (Windows 7 / Windows 2008 R2 and newer) and provides incredible flexibility and functionality to manage Windows systems. This power makes PowerShell an enticing tool for attackers.

Guardian Comment: PowerShell is a significant attack vector. Attackers often invoke PowerShell code on a computer since it can be run in memory where antivirus can’t see it.

RADIUS Server User Authentication Failure

Query: (event_id:6273) app_name:("microsoft-windows-security-auditing")

Details: When Network Policy Server (NPS) is configured as a RADIUS server, it performs authentication, authorization, and accounting for connection requests received from configured RADIUS clients. If authentication and authorization are successful, users and computers are granted access to the network resources for which they have permissions.

Guardian Comment: Network Policy Server denied access to a user. Failed user authentication may indicate malicious activity or network hygiene issues.

Remote Desktop Logon/Logoff

Query: (event_id: (4634) AND logon_type: 10) app_name:("microsoft-windows-security-auditing")

Details: An account was logged off. When you access a computer through Terminal Services, Remote Desktop or Remote Assistance windows logs the logon attempt with logon type 10 which makes it easy to distinguish true console logons from a remote desktop session

Guardian Comment: Unusual logon/logoff activity may indicate malicious activity.
Security Enabled Global Group Changed

Query: (event_id:4737) app_name:("microsoft-windows-security-auditing")

Details: In Active Directory Users and Computers "Security Enabled" groups are simply referred to as Security groups. AD has 2 types of groups: Security and Distribution. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Security (security enabled) groups can be used for permissions, rights and as distribution lists. This event indicates a security-enabled global group was changed. Global means the group can be granted access in any trusting domain but may only have members from its own domain.

Guardian Comment: This event is only logged on domain controllers. The event possibly indicates unauthorized changes in permissions or rights.

Security Enabled Global Group Created

Query: (event_id:4727) app_name:("microsoft-windows-security-auditing")

Details: In Active Directory Users and Computers "Security Enabled" groups are simply referred to as Security groups. AD has 2 types of groups: Security and Distribution. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Security (security enabled) groups can be used for permissions, rights and as distribution lists. This event indicates a security-enabled global group was created. Global means the group can be granted access in any trusting domain but may only have members from its own domain.
Guardian Comment: This event is only logged on domain controllers. The event possibly indicates an unauthorized group with permissions or rights.

Security Enabled Local Group Changed

Query: (event_id:4735) app_name:("microsoft-windows-security-auditing")

Details: In Active Directory Users and Computers "Security Enabled" groups are simply referred to as Security groups. AD has 2 types of groups: Security and Distribution. Distribution (security disabled) groups are for distribution lists in Exchange and cannot be assigned permissions or rights. Security (security enabled) groups can be used for permissions, rights
and as distribution lists. This event indicates a security-enabled local group was changed. All groups are security groups in the computer’s SAM. Local SAM groups can be granted access to objects on the local computer only but may have members from the local SAM and any trusted domain.

Guardian Comment: A security-enabled local group was changed, possibly indicating unauthorized changes in permissions or rights. This event is logged on domain controllers for Active Directory domain local groups and member computer for local SAM groups. You can determine if the group is a domain or SAM group by comparing Group Domain: to the Computer: name. If they match you have a SAM group, if they differ you have a domain group.

Service Terminated Unexpectedly

Query: (event_id:7034) app_name:(service_control_manager)

Details: Service Control Manager (SCM) stops services and driver services. It also reports when services terminate unexpectedly or fail to restart after it takes corrective action. This can also be generated when a service is terminated by the user via “Task Manager”.

Guardian Comment: The message reads “The service terminated unexpectedly. It has done this “n” time(s)”. Anomalous levels of service terminations indicates possible malicious activity.

Service Was Installed

Query: (event_id:7045) app_name:(service_control_manager)

Details: A service was installed in the system.

Guardian Comment: Unauthorized service installation indicates possible malicious activity.

Sysmon CreateRemoteThread Detected

Query: (event_id:8) app_name: (“microsoft-windows-sysmon”) 

Details: The CreateRemoteThread event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The
event indicates the source and target process. It gives information on the code that will be run in the new thread: StartAddress, StartModule and StartFunction.

Guardian Comment: This event is used to track the activity of malicious processes.

Sysmon RawAccessRead Detected

Query: (event_id:9) app_name:('microsoft-windows-sysmon')

Details: The RawAccessRead event detects when a process conducts reading operations from the drive using the `\\.\` denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process and target device.

Guardian Comment: This event is used to track the activity of malicious processes.

Sysmon Driver Loaded

Query: (event_id:6) app_name:('microsoft-windows-sysmon')

Details: The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.

Guardian Comment: This event should be configured carefully, as monitoring all image load events will generate a large number of events.

Sysmon Error

Query: (event_id:255) app_name:('microsoft-windows-sysmon')

Details: This event is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service.
Guardian Comment: The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as a signature.

Sysmon File Creation Time Changed

Query: (event_id:2) app_name:('microsoft-windows-sysmon')

Details: The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system.

Guardian Comment: Many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.

Sysmon Image Loaded

Query: (event_id:7) app_name:('microsoft-windows-sysmon')

Details: The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the –l option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.

Guardian Comment: This event should be configured carefully as it generates a significant number of events.

Sysmon Network Connection Detected

Query: (event_id:3) app_name:('microsoft-windows-sysmon')

Details: The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields.
Guardian Comment: The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

**Sysmon Process Creation**

Query: (event_id:1) app_name: ("microsoft-windows-sysmon")

Details: The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

Guardian Comment: This event is used to track the activity of malicious processes.

**Sysmon Process Terminated**

Query: (event_id:5) app_name: ("microsoft-windows-sysmon")

Details: The process terminate event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.

Guardian Comment: This event is used to track the activity of malicious processes.

**Sysmon Service State Changed**

Query: (event_id:4) app_name: ("microsoft-windows-sysmon")

Details: The service state change event reports the state of the Sysmon service (started or stopped).

Guardian Comment: This event is used to track the activity of malicious processes.

**The Windows Filtering Platform Permitted A Connection**
Query: (event_id:5156) app_name:("microsoft-windows-security-auditing")

Details: The Windows filtering platform permitted a connection.

Guardian Comment: Event ID 5156 should occur if the Success or Failure audit was enabled for Filtering Platform Connection in Advanced Audit Policy Configuration setting which is available from Windows 2008 R2 and later versions.

Updated Packages Installed

Query: (event_id:2) app_name:("microsoft-windows-servicing")

Details: Windows installed package updates.

Guardian Comment: The Windows Installer package is an .msi file that contains explicit instructions about installing and removing specific applications.

User Account Changes

Query: event_id:4725 OR event_id:4722 OR event_id:4723 OR event_id:4724 OR event_id:4726 OR event_id:4767

Details: Account created, disabled, enabled, deleted, unlocked, password change attempt, password reset attempt.

Guardian Comment: Account changes are monitored for unusual and/or malicious activity.

User Account Created

Query: (event_id:4720) app_name:("microsoft-windows-security-auditing")

Details: An account was created.

Guardian Comment: Account changes are monitored for unusual and/or malicious activity.
User Account Was Deleted

Query: (event_id:4726) app_name:('microsoft-windows-security-auditing')

Details: A user account was deleted.

Guardian Comment: Auditing for unauthorized account changes.

User Account Disabled

Query: (event_id:4725) app_name:('microsoft-windows-security-auditing')

Details: A user account was disabled.

Guardian Comment: Account changes are monitored for unusual and/or malicious activity.

User Account Enabled

Query: (event_id:4722) app_name:('microsoft-windows-security-auditing')

Details: A user account was enabled. This is logged when an account along with an account creation event when an account is created, and when an account is enabled after being disabled.

Guardian Comment: Monitoring for false accounts and elevation of unauthorized privileges.

User Account Unlocked

Query: (event_id:4722) app_name:('microsoft-windows-security-auditing')

Details: A user account was unlocked.

Guardian Comment: Account changes are monitored for unusual and/or malicious activity.
User Added to Security Enabled Local Group

Query: event_id: (4732) app_name: ("microsoft-windows-security-auditing")

Details: This event generates every time a new member was added to a security-enabled (security) local group.

This event generates on domain controllers, member servers, and workstations.

For every added member you will get separate 4732 event.

Guardian Comment: Monitoring for false accounts and elevation of unauthorized privileges.

User Added to Security Enabled Universal Group

Query: (event_id: (4756)) app_name: ("microsoft-windows-security-auditing")

Details: A member was added to a security-enabled universal group.

Guardian Comment: Monitoring for false accounts and elevation of unauthorized privileges.

Windows - Error Reporting

Query: (event_id: (1001)) app_name: (windows_error_reporting)

Details: The 1001 event is logged by the Windows Error Reporting infrastructure for all reports (for example, application crashes, hangs, and generic reports).

The event contains a summary of the report's signatures, Windows Error Reporting bucket information, and other fields that describe the state of the report. This event is logged in the Application event log. Event 1001 is logged at any time the report transitions state (that is, goes to the queue and comes out of the queue). Thus, it is possible to see multiple 1001 events for the same report.

Guardian Comment: Monitored for routine application failures and possible indicators of compromise.
Network

Cisco Call Manager Failure

Query: syslog_level:2 AND "%UC_CALLMANAGER-2-CallManagerFailure"

Details: Notification that an internal failure occurred in the Cisco CallManager service. The service should restart in an attempt to clear the failure.

Guardian Comment: The Cisco Call Manager service should be restarted.

Cisco Call Manager Gateway Failure Message

Query: syslog_level:2 AND "%UC_CALLMANAGER-2-MGCPEndpointLostComm:"

Details: Notification that some failure occurred in the Cisco CallManager system

Guardian Comment: Errors are occurring in the Call Manager Gateway - review logs for additional details surrounding failure.

Cisco DHCP Activity

Query: syslog_level:6 AND DHCP

Details: Notification of Dynamic Host Configuration Protocol (DHCP) client activities.

Guardian Comment: Alert based on DHCP activity, as traditionally machines are configured with static IP's. Review log for source IP and reconfigure.

Cisco DNS Drops

Query: syslog_level:4 AND "dropped UDP DNS"

Details: Notification that a DNS packet has been dropped
Guardian Comment: A DNS dropped packet by itself is not an issue. A dropped packet becomes an issue when it is a connection that you want to make, but your firewall keeps dropping the connection. Another good use for this is to monitor who is attempting to access sites that you know to be malicious.

Cisco Environmental Monitor Alerts

Query: envmon
Details: Notification that an environmental monitor threshold has been exceeded
Guardian Comment: Review log details to ascertain what triggered the alert (e.g. CPU temps, fan speed, etc)

Cisco Ethernet Duplex Mismatch Error

Query: duplex mismatch
Details: Notification that two connected devices are operating in different duplex modes
Guardian Comment: Reconfigure duplex to match, and or set both ends to auto-duplex.

Cisco FAN Alert

Query: "%FAN-***
Details: Notification of a potential fan failure
Guardian Comment: Full diagnostics is highly recommended to prevent any hardware failure.

Cisco Unified Messaging Fail

Query: CDRFileDeliveryFailureContinues
Details: Notification of a Unified Messaging Service failure

Guardian Comment: Review service logs; issue could be from incorrect password to certificates, dependent on the logs.

Cisco VLAN Mismatch

Query: vlan mismatch

Details: Notification of a VLAN mismatch between two connected devices

Guardian Comment: Recommend to review and troubleshoot VLAN configuration on router.

FTP Traffic

Query: service_port:"21" AND NOT praesidio_skip_ad:true

Details: Monitor FTP traffic

Guardian Comment: Both source and destination of traffic should be verified to ensure no data exfiltration is occurring.

Monitor the number of errors

Query: error

Details: Detecting errors like dropped packets or retransmissions on the network level is relatively easy. Figuring out if those errors affect the performance and connectivity of your services is however another matter.

Guardian Comment: Monitoring activity for anomalous activity.

No Data
Query: *

Details: No events received from customer.

Guardian Comment: nxlog services may need to be restarting, and of the DVM may need restarting, or further troubleshooting.

**RDP Traffic**

Query: service_port:“3389” AND NOT praesidio_skip_ad:true

Details: Monitor Remote Desktop Protocol traffic

Guardian Comment: Verify source of IP traffic (e.g. internal/VPN). If source IP is external and not recognized, check NAT ruleset on firewall for open source NAT's, and proceed to lock/disable NAT.

**RSH/Rlogin Traffic**

Query: service_port:“514” AND NOT praesidio_skip_ad:true

Details: Monitor Remote sync and remote login traffic.

Guardian Comment: Investigate into source traffic, as Rlogin is a deprecated remote login procedure that has security flaws, and was replaced by SSH.

**SMTP Traffic**

Query: service_port:“25” AND NOT praesidio_skip_ad:true

Details: Monitor Simple Mail Transfer Protocol traffic.

Guardian Comment: This traffic is commonly associated with email traffic.

**SSH Access By Admin**

Copyright © 2015 - 2016 DefenseStorm, LLC. All rights reserved.
Query: (SSH access by user admin)

Details: Notification of SSH by admin account

Guardian Comment: Verify source of traffic, and with user who has admin credentials of login history.

**SSH Traffic**

Query: service_port:"22" AND NOT praesidio_skip_ad:true

Details: Monitor Secure Shell traffic.

Guardian Comment: Review logs and source of traffic to ensure SSH traffic is expected.

**Telnet Traffic**

Query: service_port:"23" AND NOT praesidio_skip_ad:true

Details: Monitor Telnet traffic

Guardian Comment: Telnet is an outdated protocol and virtually deprecated. Investigation into telnet traffic is advised.

**Palo Alto Networks**

**Palo Alto Anonymizer**

Query: subtype:proxy-avoidance-and-anonymizers -drop

Details: TOR or other anonymizer traffic

Guardian Comment: Investigation into traffic is highly recommended as traffic is going out via proxy avoidance, and randomly exiting on a node elsewhere in the world.
Palo Alto DNS Botnet Signature

Query: threat_type:("dns botnet signatures")

Details: Notification of DNS Botnet Signatures

Guardian Comment: Investigation and triage of source of traffic is recommended, as DNS traffic associated known botnet domains has been detected.

Palo Alto Drop Events

Query: app_name:"palo alto networks firewall" category:drop

Details: Notification of dropped events.

Guardian Comment: The Palo Alto is dropping traffic. This is most commonly seen with ACL’s.

Palo Alto End Events

Query: app_name:"palo alto networks firewall" category:end

Details: Notification on end events

Guardian Comment: End event logging is used for troubleshooting connectivity and applications, from threats to session time-outs.

Palo Alto Failed To Update

Query: (failed to check) app_name:"palo alto networks firewall" category:(general)

Details: Notification on failed to update events.

Guardian Comment: The firewall failed to update definitions and or firmware.
Palo Alto Firewall Login/Logout Audit

Query: ("logged in" OR "logged out") app_name:"palo alto networks firewall" category:(general)

Details: Notification of the login and logout audit

Guardian Comment: This alert is generated whenever a user has logged into, or out of, the Palo Alto firewall.

Palo Alto HA Down

Query: (down) app_name:"palo alto networks firewall" category:(ha)

Details: Notification of HA down events

Guardian Comment: High Availability pairing is down.

Palo Alto HA Events

Query: system(ha) app_name:"palo alto networks firewall"

Details: Notification of HA events

Guardian Comment: Alert is generated with the primary firewall has failed over to the secondary.

Palo Alto License Expiring

Query: (license expire) app_name:"palo alto networks firewall"

Details: Notification of license expiring

Guardian Comment: Alert related to licensing on the firewall expired. Advise to renew
licensing so there is no lack in firewall coverage (e.g. web filtering).

Palo Alto Networks Terminal Server Failed to Connect

Query: connection error app_name:"palo alto networks firewall"

Details: Notification of when terminal server fails to connect.

Guardian Comment: There is connectivity issues between the Palo Alto firewall and the terminal server agent. Recommend to review tsa configuration.

Palo Alto Spyware Detected

Query: app_name:"palo alto networks firewall" category:(spyware)

Details: Notification when spyware is detected on the network

Guardian Comment: Spyware has been detected on the network per the definitions on the firewall. Recommend AV scanning of source IP if internal.

Palo Alto SQL Injection Detected

Query: app_name:"palo alto networks firewall" and message:HTTP SQL Injection Attempt

Details: Notification when SQL Injection is detected on the network

Guardian Comment:

Palo Alto Suspicious DNS Query

Query: Suspicious DNS Query app_name:"palo alto networks firewall"

Details: app_name:"palo alto networks firewall" and message:HTTP SQL Injection Attempt
Guardian Comment: A suspicious DNS query has occurred. Review logs to vet that the traffic was not malicious.

**Palo Alto Userid Events**

Query: app_name:"palo alto networks firewall" category:userid
Details: Notification when userid events occur on the network
Guardian Comment: Review log to see what policy violation triggered the event.

**Palo Alto Virus Detected**

Query: app_name:"palo alto networks firewall" category:(virus) -deny
Details: Notification when a virus is detected on the network
Guardian Comment: The firewall has detected a virus on the network. Triage and remediation is highly advised.

**Palo Alto Vulnerability Detected**

Query: app_name:"palo alto networks firewall" category:vulnerability
Details: Notification when a vulnerability is detected on the network.
Guardian Comment: The firewall has detected vulnerabilities. Recommend to investigate and patch vulnerability, and if not, methods to minimize risk.

**New Application Installation**

Query: event_id: (903 OR 904)
Details: The Software Protection service has stopped.
These are events associated with SPPSVC service startup (event id 900) and shutdown (event id 903). The service is designed to shut down when nobody is using it. An application may call SL API, which will cause the service to wake up.

Here is some additional information that may help to investigate anomalies in SPPSVC wakeup-shutdown pattern (notice that starting up because some other app calls SL API is not an anomaly).

First of all, before the service shuts down, it updates a Windows Task Scheduler task under Microsoft/Windows/SoftwareProtectionPlatform. This task is scheduled to wake up SPPSVC approximately minutes after a successful SPPSVC renewal (typically seven days later). You may want to look at this entry to verify that the next wake up time is consistent with your KMS renewal interval. Pay attention to the “Next Run Time” and “Last Run Time” fields. (This task schedule entry is hidden, so you need to enable viewing hidden tasks from the View menu in the Task Scheduler).

Secondly, another potential reason for SPPSVC to keep waking up is another service: SPPUINOTIFY. This normally (when the system is in the licensed state) should run during KMS renewal and should shut itself down after the renewal has succeeded.

If both of the above are right (that is the task scheduler task is scheduled outside of 2 hours and sppuinotify service is stopped), then there can be only an external reason for SPPSVC to wake up.

Guardian Comment: Monitored for unauthorized applications being permitted on the network. Also useful for performing software auditing on a network, ie. patching.

**Login Failed Bad Password or Username Unknown**

Query: `event_id:(4625) AND "Status: 0xc000006d Sub Status: 0xc0000064"`

Details: This trigger leverages the same Event ID as “Failed Login” but is specific to these types of failures:

- bad username or authentication information.
- user name does not exist.

Guardian Comment: Monitored for unauthorized access or indicator of a potential breach. Also, useful for determining network hygiene issues.
Download Links

DefenseStorm Virtual Machine

VMWare (OVA File) v1.1.3

Microsoft Hyper-V (Zip) v1.1.3

DefenseStorm Windows Agent

https://windowsagent.defensestorm.com/dist/1.4.4/DefenseStorm.msi
The type of network asset determines how we collect Windows logs from them. There are two different software products that DefenseStorm recommends to collect Windows logs. Depending on your scenario you may have to use one or both. The two software products are:

- **NXLog** (for Windows Servers and domain controllers)
- **DefenseStorm Windows Agent** (for laptops and individual workstations)

Both NXLog and the DWA require utilization of sysmon to collect the most data.

## Windows Audit Log Recommendations

Within the Windows Operating system, there are audit logs that can be configured to track success or failure of certain events. For example, once audit logs are activated for logon attempts, you can choose to track if a logon attempt is successful, if it fails, or both. Guardian has prepared examples for each option within the Windows Operating System to help send the most useful logs to your DefenseStorm DVM and reduce noise on your system.

The following items can be monitored:

- Changes to user account and resource permissions.
- Failed attempts by users to log on.
- Failed attempts to access resources.
- Changes to system files.

This link provides the PDF list of Guardian recommendations. [Guardian Windows Audit Recommendations](#).

## Windows Agent

The DefenseStorm Windows Agent (DWA) is a program installed on Windows workstations and laptops to collect and forward log data to the DefenseStorm Security Data Platform. Your IT security team can now track any local Windows event activity. To ensure all event data is logged and tracked, it is captured even when a device is offline. The DefenseStorm Windows Agent also has automatic software updates, so you always have the most up-to-date version.
Features

- Windows based installer file that supports both full GUI and cmd line installations
- Full documentation for installer usage with options
- Support for two-factor authentication
- Login via username/password
- Login via temporary token/secret/orgId
- Local event logs collection
- Windows event logging
- Full offline logging, with offline events being sent to the server upon being reconnected to a network.
- Application auto updates itself from the DefenseStorm cloud
- Auto updates can be turned off upon installation
- Support for sending data via DefenseStorm Virtual Machine (DVM) or sending data directly to the DefenseStorm platform via the Internet
-Fallback sending data to DVM or Internet if either is unavailable.

Limitations

- Requires .NET 4.5 to be installed
- Installer requires that user has administrative permissions
- Computer must be connected to the network for authentication during installation
- Offline Logging:
  - Local logs may fail to upload if the client has been offline for long periods of time
  - Local file logging requires edits to the configuration file, followed by a service restart to take effect

Installation

The Windows Agent can send data directly to the DefenseStorm platform directly via the Cloud.
This is the default behavior. It can also send traffic directly to the DVM.

In the event that either method is unavailable, the Windows Agent can be configured to fallback to the available method. For example, if the DVM is unavailable, the agent can automatically switch to send messages to the Cloud. When the DVM is available again, the Windows Agent switches back to the DVM. This way your network is always being monitored and potential threats analyzed.

Follow the instructions listed below to configure the desired behavior during the installation process.

Note: If you have any problems with installation, there’s a "View Log" button at the end of the installation that is helpful. Also, the event logs from the Event Viewer are useful too. During installation, there is a prompt for API tokens and Org ID. There is also a tab for username and password.

**Command line installation**

To execute the installer silently, run the following command. Authentication switches for the web service (be it key based or username) must be included for this installation method.

```
msiexec /package DefenseStorm.WindowsAgent.Installer.msi /quiet
APIKEY=key APISECRET=secret ORGID=id
```

Comprehensive list of the command line switches:

- **UPDATES** {bool, default True. Toggles automatic application updates}
- **WINDOWSUSER** {string, default LocalSystem. Specifies user account to run the agent under. This is not recommended.}
- **WINDOWSPASSWORD** {string, default NULL. Specifies user account to run the agent under's password. This is not recommended}
- **APIUSER** {string, default NULL. DefenseStorm Username for API access- must have accompanying APIPASSWORD set as well.}
- **APIPASSWORD** {string, default NULL. DefenseStorm Password for API access- must have accompanying APIUSER set as well.}
- **APIKEY** {string, default NULL. DefenseStorm Key for API access- must have accompanying
APISECRET and ORGID set as well.

- **APISECRET** {string, default NULL. DefenseStorm Secret for API access- must have accompanying APIKEY and ORGID set as well.}
- **ORGID** {string, default NULL. DefenseStorm org id for API access- must have accompanying APISECRET and APIKEY set as well.}
- **SENDEVENTS** {string, default NULL. DefenseStorm org id for API access- must have accompanying APISECRET and APIKEY set as well.}
  - Inserting DS means your send data to the cloud, DVM is only the DVM, and BOTH allows fallback in the event one is unavailable.
  - If choosing DVM or BOTH, you must enter DVMHOST into the command line. This option defaults to the DVM first, then to the cloud as fallback.

To allow Cloud as a fallback

If you want your DWA to send events through the Cloud in the event that the DVM is unavailable, enter the following commands:

```bash
msiexec /package DefenseStorm.WindowsAgent.Installer.msi /quiet
APIKEY=key APISECRET=secret ORGID=id SENDEVENTS=both DVMHOST=dvm.mycompany.com
```

*Replace the `dvm.mycompany.com` portion of the code with your DVM IP address.*

To only send events through the DVM

If you want your DWA to only send events through the DVM, enter the following commands:

```bash
msiexec /package DefenseStorm.WindowsAgent.Installer.msi /quiet
APIKEY=key APISECRET=secret ORGID=id SENDEVENTS=dvm DVMHOST=dvm.mycompany.com
```

*Replace the `dvm.mycompany.com` portion of the code with your DVM IP address.*
GUI Installation

To install the DefenseStorm Windows Agent manually through the installation gui on an individual workstations, follow these instructions.

1. Obtain DWA installer files.

2. Run the Installer. After you select to run the installer, you see the following window to begin installation.

3. Agree to the terms and conditions by selecting the checkbox on the next window, select Next.

4. Select Next to keep the default folder location for the agent.
5. Select how to send data. Chose to either send data ‘Directly to DefenseStorm’, ‘Through the DVM’, or ‘Through the DVM if available, directly otherwise’.

If you chose to send data through the DVM only, or through the DVM if available, directly otherwise, you must input your DVM IP Address.
6. Input Token/Key/OrgID from the web console.

- Log in to the web console, click Settings icon at the bottom of the left sidebar, select Input Token from the header menu, and then Get Agent Token.

Web console view

Installer view
After the information is placed in the installer window, select Next.

7. Select Auto-Updates. Click Next.

8. You see the following pop-up, select YES to allow it to complete the install.
9. The installation completes.

10. Verify that the DefenseStorm Windows Agent is installed correctly by completing the steps in the next session, Searching Windows Event Logs.

Searching Windows Event Logs

To view event logs associated with the DefenseStorm Windows Agent, go to the Event page, and
type app_name:"DefenseStorm Agent" into the search bar.

The following is a comprehensive list of the logs we collect from your Windows machines:

- All DefenseStorm logs
- MSI
- All Application Errors
- All Application Hangs
- All CAPI2 Logs
- Security
- Setup
- PowerShell Admin
- PowerShell Operational
- Task Scheduler Admin
- Task Scheduler
- SMB Server
- AppLocker EXE and DLL Error
- AppLocker MSI and Script Error
- SRP Block Error
- System Errors and Warnings
- Windows Error Reporting
- EMET
- Windows Service Fails or Crashes Error
- Windows Service Fails or Crashes Other
- Windows Update Errors
- Windows Firewall
- Clearing Event Logs
- New Kernel Filter Driver
- New Windows Service
- New Application Installation/Update/Removal
- Windows Update Installed
- Code Integrity
- Failed Kernel Driver Loading
- Group Policy Errors
- Windows Defender
- Network Connection and Disconnection Status
- Wireless connection Info
- Mass Storage Installation
- Printing Document
- Sysmon

Advanced Configuration - Additional log sources

You have the ability to add additional windows event logs events through either Windows Event Log or from an arbitrary text file.

Windows Event Logs

The Windows Agent is configured by default to read from default log sources we deem most important from Windows Events. However, you may choose to expand beyond the sources we configure by adding your own.

To do so, modify the ClientLogSources.json file. Below is a screenshot of Windows events viewed through Windows Event Viewer.
So you can add any of these log sources by editing the ClientLogSources.json file within the C:\Programfiles\DefenseStorm\Data folder. There are 5 fields for each log source entry:

```json
{
    "comment": "Comment 1",
    "log_name": "Application",
    "source": "DefenseStorm",
    "level": ["error", "warning"],
    "event_id": [7022, 7023]
}
```

- comment can have any text
- log_name is the same that appears in the `Log` column. Mandatory field.
- source is the `Source` column
  - Omitting means, all sources.
- level column, whose valid values are: Critical, Error, Warning, Information, LogAlways, Verbose.
  - Omitting means all levels.
- event_id is an array of numbers from the `Event ID` column, and `level` is the one you see in the
  - Omitting means all events.

### Arbitrary Text Files and DNS files

The second method to ingest logs is to read from an arbitrary text file. The file "Config.json" is where you can set which files they want the Windows Agent to monitor.

The DNS files are in a specific format, it's the default "Debug Log" format of Windows DNS. The Generic files can be in any format as long as they are composed of lines. There are two lists, one for DNS files (they have a special format), and "Generic" is for every other kind of file.

```json
{

```
NXLog

Well known Community Edition tool for collecting information from windows systems. DefenseStorm leverages it when data needs to be collected that is out of the current scope of DWA features.

Limitations:

- Complex to configure
- No auto-updates

Installing NXLog

Perform the default installation. You can either install the software into the default location, or choose a custom location. You do not need to configure NXLog because the Windows Setup Tool completes that for you. You can obtain NXLog Community Edition from: http://nxlog.org/products/nxlog-community-edition/download

NXLog also supports a command line silent installation. To install, use the following command:

msiexec /I “nxlog-ce-2.9.1504.msi” /quiet

You can specify a custom installation directory with the INSTALLDIR parameter:

msiexec /I “nxlog-ce-2.9.1504.msi” /quiet INSTALLDIR="C:\NXLog"

Collecting DNS Logs
1. In DNS Manager, get to the DNS Server and Properties and Debug Logging Tab

2. Ensure only the following are checked
   - Log packets for debugging
   - Incoming
   - Transport Protocol: UDP and TCP
   - Queries/Transfers
   - Updates
   - Packet Type: Request and Response

3. Do NOT check Details.

4. Specify a File path and Name, and a Maximum Size.

5. Add the following to the end of nxlog-base.conf. Change the File name/location based on what you entered in configuration above.

```
Module im_file
File 'C:\DNS Logs\log.txt'
InputType LineBased
CloseWhenIdle TRUE
Exec if $raw_event == "" drop();
Exec 
$hostname = hostname_fqdn(); \n$SourceName = "Microsoft-Windows-DNS"; \n$Message = $raw_event;
Path in-DNSLogs => syslogng-out
```
6. Restart NXLog and check the nxlog.log output.

7. Check the web console with the following query: app_name:microsoft-windows-dns
Current reports on the use of Windows PowerShell as an attack platform bring up the increased need to detect and prevent the abuse of our system administration ecosystem. The recent release of Mandiant’s M-Trends 2017 annual report highlights the development of more sophisticated tactics, techniques, and procedures (TTP) by financial threat actors against banking targets in Asia and Europe. These attacks are employing internal system administration tools, specifically Windows PowerShell, to fly under the radar and maintain persistence.

“Windows PowerShell is a good example of a relatively new attack vector that many organizations are not monitoring and logging. Attackers are increasingly leveraging Windows PowerShell to conduct their operations when undertaking malicious activity within a victim’s environment. In many environments, PowerShell does not leave artifacts indicating its usage. This situation can be improved by upgrading older versions of PowerShell (such as 2.0) to later, more robust logging versions (5.0 offers a much broader range of security information) and by implementing additional logging features such as Sysmon. The bottom line from an incident response perspective is that while PowerShell logging was not a typically monitored event to maintain effective cyber threat visibility five years ago, it most definitely is now.”

Windows PowerShell was developed by Microsoft to provide a system administration infrastructure that provides more power and flexibility to perform automated routine tasks and configuration management across their entire domain. PowerShell is based on the .NET framework and provides a command-line shell as well as a powerful scripting language. The PowerShell Gallery gives system administrators a list of modules and scripts to deploy on their domain and the ability to contribute their own for the community.

However, many security researchers and penetration testers have developed a number of post-exploitation tools using PowerShell—PowerSploit, Empire, PoshSec, PowerUp and PowerView are just a few examples. Blue Teams need to actively search for the execution of these modules and react quickly when they appear in their log data.
Thankfully, Microsoft added some instrumentation capabilities to PowerShell starting in version 3.0. Windows 7 and Server 2008 ship with PowerShell version 2.0, so system administrators need to upgrade the .NET framework and the Windows Management Framework to version 5.0.

Threat actors are aware that PowerShell version 2.0 does not log and are taking advantage of that by forcing the use of version 2.0; which is supported for backwards compatibility reasons. The command to do so is quite simple and may be run in a command shell or PowerShell:

```
PowerShell.exe -Version 2 "your command arguments here"
```

Incident responders need greater visibility to detect the use of PowerShell version 2 in addition to current versions. Instrumenting Windows Powershell is fairly straight forward because the tool leverages Microsoft’s existing event logging capabilities. We recommend that you enable PowerShell logging according to the procedures outlined by Matthew Dunwoody (Mandiant/FireEye).

To obtain the visibility necessary to audit PowerShell command line, module, and script execution, do the following:

- Upgrade to the current version
- Enable logging capabilities through group policy
- Increase windows instrumentation through Sysmon

**External Procedure Links**

See below for the procedures to enable PowerShell logging: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

We also recommend installation and configuration of the current version of Microsoft’s System Monitoring tool called Sysmon. It is available here: https://technet.microsoft.com/en-us/sysmon

A tuned configuration template for Sysmon is available for download from Github here: https://github.com/DefenseStorm/sysmon-config
Suspicious Cmd Line Arguments

Execution of PowerShell with command line arguments that include the following should be regarded as suspicious and prompt further investigation:

- PowerShell.exe -Version 2
- PowerShell.exe -EncodedCommand
- PowerShell.exe -ExecutionPolicy Bypass
- PowerShell.exe -NonInteractive
- PowerShell.exe -NoProfile
- PowerShell.exe -WindowStyle Hidden
Verified Systems and Configurations

The DefenseStorm Solution can collect events and logs from Windows systems. The following Windows systems are tested and verified:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1

The configuration described below can be used to collect Windows event/log information:

- Windows System Events
- Sysmon Events
- DHCP Logs
- IIS Logs
- Windows Inventory Information

The configuration can also be expanded to collect information from any log file written to a Windows system.

Best practices for monitoring Windows systems

Requires the following components:

- **NXLog Community Edition (REQUIRED):** Used to transfer logs and events to DefenseStorm.
- **Sysmon (Optional):** Used to collect additional network and process information from the windows system.
Praesidio Windows Tool (PWT) (REQUIRED): The Windows Setup Tool is used to ease configuration of NXLog.

**NXLog Community Edition**

Perform the default installation. You can either install the software into the default location, or choose a custom location. You do not need to configure NXLog because the Windows Setup Tool completes that for you. You can obtain NXLog Community Edition from: http://nxlog.org/products/nxlog-community-edition/download

NXLog also supports a command line silent installation. To install, use the following command syntax:

```
msiexec /I “nxlog-ce-2.9.1504.msi” /quiet
```

You can specify a custom installation directory with the INSTALLDIR parameter:

```
msiexec /I “nxlog-ce-2.9.1504.msi” /quiet INSTALLDIR=\"C:\NXLog\" 
```

**Sysmon**

Sysmon does not require an installation package, so the executable can be pushed out over a network and easily scripted by the command in this procedure, run on individual machines.

Note: Sysmon can be placed anywhere on the disk, the locations listed below are guardian recommendations.

To install Sysmon, perform the following steps:

1. Download and unzip [Sysmon from Microsoft](https://docs.microsoft.com) to windows\system32
2. Download both .xml files from [github](https://github.com) to windows\system32
3. From the cmd line, as admin, run the following command: sysmon.exe -accepteula -i sysmonconfig-export.xml

**Windows Setup Tool (enables Windows to Syslog translation)**
The Windows Setup Tool supports either a command line or graphical installation. For the graphical installation, simply double click on the MSI. Download the PWT here: **Praesidio Windows Tool**. For command line installation, use the following syntax:

```
msiexec /i "WindowsSetupTool.msi" /quiet
```

You can also specify an alternate installation directory with the APPDIR parameter:

```
msiexec /i "WindowsSetupTool.msi" /quiet APPDIR="D:\Praesidio"
```

## Configuration for Transmitting Events

**STEP 1:** Run the DefenseStorm NXLog Configuration Tool as Administrator.

**STEP 2:** Enter/Browse for the NXLog Root Directory.

**STEP 3:** Select Items to monitor:

- **Events**: Collect Windows Events from the Windows Event Logs on the system.
- **DHCP Logs**: Only select for Windows Servers that are providing DHCP services to the network.
- **IIS Logs**: Only select for Windows Servers that are running the IIS services.
- **Sysmon**: Collect Windows Event logs generated by the Windows Sysmon tool.
- **Inventory Info**: Collect additional system information, such as local users/groups, installed software and versions, and WMI system information hourly to populate the asset information in the Console.

**STEP 4**: Select the log destination.

**STEP 5**: Login to Local Syslog - Use this option to log into the DefenseStorm Virtual Machine (DVM).

- Enter the IP Address of the DVM/Syslog Server
- Use Port 601 for the DVM or enter the Port of your Syslog Server

*Note: This tool automatically uses TCP and IETF Formatted Syslog.*

**STEP 6**: Login to the DefenseStorm Cloud - Use this option to send event information directly to DefenseStorm.

- Enter the DefenseStorm Key and the DefenseStorm Secret you obtain from your DefenseStorm Console.

**STEP 7**: Select Overwrite All Config Files

1. Recommended: The tool overwrites all config files in the NXLog configuration directory with template files that were delivered with the Windows Setup Tool. Do not select this option if you have customized the configuration files. In this case, only the nxlog.conf file is overwritten and all other files remain unaltered.

**STEP 8**: Click Save.

**STEP 9**: Click Restart NXLog to restart the NXLog Service.

**STEP 10**: Click View NXLog Logfile to verify that the service started up fully without errors.
Automation: Installing nxlog with GPO Script

Use the attached script to automate the installation of nxlog with GPO.

AutomatedInstallBatch.bat
Setting up to receive SNMP Traps

Prerequisites

- SNMP client auth config details (if SNMP traps already set up in org. and/or this is a DVM migration)
- DVM credentials & access

Procedure

1. Execute the following commands to install the required modules

```
$ sudo apt-get install snmp snmpd snmp-mibs-downloader
```

2. Edit the file at /etc/default/snmpd and change the following 3 values for these variables (the last line, set TRAPDOPTS, is a long line and is wrapped):

```
>> /etc/default/snmpd

set SNMPDRUN=no
set TRAPDRUN=yes
set TRAPDOPTS='-Lsd -Oq -p /var/run/snmptrapd.pid -M /usr/share/mibs/ietf:/usr/share/mibs/iana:/usr/share/mibs/defensestorm -m ALL'
```

3. Create a new config file for syslog-ng to pick up SNMP Traps from the log file:

```
>> /etc/syslog-ng/conf.d/snmpd.conf

log {
    source(s_src);
    filter(f_daemon);
    rewrite(r_praesidio);
    log { filter(f_0); destination(d_praesidiosqs_0); };
    log { filter(f_1); destination(d_praesidiosqs_1); };
    log { filter(f_2); destination(d_praesidiosqs_2); };
    log { filter(f_3); destination(d_praesidiosqs_3); };
    flags("Flow_control");
};
```

4. Edit the /etc/snmp/snmp.conf and comment the mibs line out

5. Edit the /etc/snmp/snmptrapd.conf and add lines following the example below.

DefenseStorm recommends SNMP v3 with authentication. If the system you want to send traps from does not support authentication, use the SNMP v2c setup and change the community string. For SNMP v2c

```
For unauthenticated SNMP, add the following line
```
disableAuthorization yes
Next, edit the /etc/snmp/snmpd.conf file and change the Community String from "public" to a string specific to the organization.
For SNMP v3

If this is a new SNMP trap integration
Change the username SHA and AES passphrases to private values for your environment. SNMP sources will need to be configured to use these new values.

If this is a migration from a previous DVM version
Change the username SHA and AES passphrases to the values in the old DVM's /etc/snmp/snmptrapd.conf. These should match the auth credentials saved in the SNMP trap message sources.
You will need 3 values
User name: ds
SHA Pass: "defensestorm"
AES Pass: "defensestorm"

Example: file edits for creating new SNMP configuration
>> /etc/snmp/snmptrapd.conf

createUser -e 0x800013700465504f5f536572766572 ds SHA "defensestorm" AES "defensestorm"
authUser log ds

6. Copy any MIBS you obtain from your software vendors into the following directory:

mibs go into /usr/share/mibs/defensestorm

If this is a DVM migration, copy MIB files in folders from the old DVM into /usr/share/mibs/defensestorm. Check old DVM snmpd file for other MIB locations under TRAPDOPTS.

7. Allow the SNMP Traps in UFW

$ sudo ufw allow 162

8. Restart snmpd and syslog-ng

$ sudo systemctl restart syslog-ng
$ sudo systemctl restart snmpd
STEP 1: Add a line to the bottom of the /etc/rsyslog.conf file to forward all log event data to the DVM that follows this style:

```
.*  @@IP_ADDRESS:514
```

STEP 2: Where IP_ADDRESS should be replaced with the IP address of your DVM. For example, if your DVM IP address was 192.168.10.12, then the line would look like:

```
.*  @@192.168.10.12:514
```
The query string is parsed into a series of terms and operators. A term can be a single word — quick or brown — or a phrase, surrounded by double quotes — "quick brown" — which searches for all the words in the phrase, in the same order. Operators allow you to customize the search.

**Field Names**

The default_field is searched for the search terms, but it is possible to specify other fields in the query syntax.

- where the status field contains active
  
  status:active

- where the title field contains quick or brown. If you omit the OR operator the default operator is used
  
  title:(quick OR brown) title:(quick brown)

  - where the author field contains the exact phrase "john smith" author:"John Smith"

- where any of the fields book.title, book.content or book.date contains quick or brown (note how we need to escape the * with a backslash):
  
  book.*:(quick brown)

- where the field title has no value (or is missing):
  
  _missing_:title

- where the field title has any non-null value:
  
  _exists_:title
Wildcards

Wildcard searches can be run on individual terms, using ? to replace a single character, and * to replace zero or more characters:

`qu?ck bro*`

Be aware that wildcard queries can use an enormous amount of memory and perform poorly — just think how many terms need to be queried to match the query string "a*b*c*".

Allowing a wildcard at the beginning of a word (eg "*ing") is particularly heavy, because all terms in the index need to be examined, just in case they match.

Wildcarded terms are not analyzed by default — they are lowercased (lowercase_expanded_terms defaults to true) but no further analysis is done, mainly because it is impossible to accurately analyze a word that is missing some of its letters. If you use wildcards your text must match the case of the text you are trying to match against.

Regular Expressions

Only use this method against single fields. Regular expression patterns can be embedded in the query string by wrapping them in forward-slashes (/):

`name:/joh?n(ath\[oa\]n)/`

The supported regular expression syntax is explained later in this document in Appendix A.

Fuzziness

This is a full-text search option (multiple words / whitespace OK) and should work in conjunction with wildcards. We can search for terms that are similar to, but not exactly like our search terms, using the “fuzzy” operator:

`quikc~ brwn~ foks~`

This uses the Damerau-Levenshtein distance to find all terms with a maximum of two changes, where a change is the insertion, deletion or substitution of a single character, or transposition of two adjacent characters.
The default edit distance is 2, but an edit distance of 1 should be sufficient to catch 80% of all human misspellings. It can be specified as:

quikc~1

Proximity Searches

While a phrase query (eg "john smith") expects all of the terms in exactly the same order, a proximity query allows the specified words to be further apart or in a different order. In the same way that fuzzy queries can specify a maximum edit distance for characters in a word, a proximity search allows us to specify a maximum edit distance of words in a phrase:

'fox quick'~5

The closer the text in a field is to the original order specified in the query string, the more relevant that document is considered to be. When compared to the above example query, the phrase "quick fox" would be considered more relevant than "quick brown fox".

Ranges

Ranges can be specified for date, numeric or string fields. Inclusive ranges are specified with square brackets [min TO max] and exclusive ranges with curly brackets {min TO max}. The parsing of ranges in query strings can be complex and error prone.

- All days in 2012:
  
  date:[2012-01-01 TO 2012-12-31]

- Numbers 1..5
  
  count:[1 TO 5]

- Tags between alpha and omega, excluding alpha and omega:
  
  tag:{alpha TO omega}

- Numbers from 10 upwards
Curly and square brackets can be combined:

- Numbers from 1 up to but not including 5
  \[
  \text{count:}[1..5]
  \]

- Ranges with one side unbounded can use the following syntax:
  \[
  \text{age}>10 \quad \text{age}>=10 \quad \text{age}<10 \quad \text{age}<=10
  \]

- To combine an upper and lower bound with the simplified syntax, you would need to join two clauses with an AND operator:
  \[
  \text{age}:>(=10 \text{ AND } <20) \quad \text{age}:+(=10 \text{ AND } <20)
  \]

**Boosting**

Use the boost operator ^ to make one term more relevant than another. For instance, if we want to find all documents about foxes, but we are especially interested in quick foxes:

\[
\text{quick}^2 \text{ fox}
\]

The default boost value is 1, but can be any positive floating point number. Boosts between 0 and 1 reduce relevance. Boosts can also be applied to phrases or to groups:

\[
\text{"john smith}^2 \text{ (foo bar}^4
\]

**Boolean Operators**

By default, all terms are optional, as long as one term matches. A search for foo bar baz will find any document that contains one or more of foo or bar or baz. We have already discussed the default_operator above which allows you to force all terms to be required, but there are...
also boolean operators which can be used in the query string itself to provide more control.

The preferred operators are + (this term must be present) and - (this term must not be present). All other terms are optional. For example, this query:

`quick brown +fox -news`

states that:

- fox must be present
- news must not be present
- quick and brown are optional — their presence increases the relevance

The familiar operators AND, OR, and NOT (also written &&, || and !) are also supported. However, the effects of these operators can be more complicated than is obvious at first glance. NOT takes precedence over AND, which takes precedence over OR. While the + and - only affect the term to the right of the operator, AND and OR can affect the terms to the left and right.

Rewriting the above query using AND, OR, and NOT demonstrates the complexity:

`quick OR brown AND fox AND NOT news`

This is incorrect, because brown is now a required term.

`(quick OR brown) AND fox AND NOT news`

This is incorrect because at least one of quick or brown is now required and the search for those terms would be scored differently from the original query.

`((quick AND fox) OR (brown AND fox) OR fox) AND NOT news`

This form now replicates the logic from the original query correctly, but the relevance scoring bares little resemblance to the original.

In contrast, the same query rewritten using the match query would look like this:

```
{  "bool": {  "must": { "match": "fox"  },  "should": { "match": "quick brown" },  "must_not": { "match": "news"  }  }
```

**Grouping**

Multiple terms or clauses can be grouped together with parentheses to form sub-queries:
Groups can be used to target a particular field, or to boost the result of a sub-query:

status:(active OR pending) title:(full text search)^2

Reserved Characters

If you need to use any of the characters which function as operators in your query itself (and not as operators), then you should escape them with a leading backslash. For instance, to search for \((1+1)=2\), you would need to write your query as\\((1\+1)=2\\)\).

The reserved characters are: + - && || ! ( ) { } \[ \] ^ " ~ * ? : /

Failing to escape these special characters correctly could lead to a syntax error which prevents your query from running.

Watch this space

A space may also be a reserved character. For instance, if you have a synonym list which converts "wi fi" to "wifi", a query_string search for "wi fi" would fail. The query string parser would interpret your query as a search for "wi OR fi", while the token stored in your index is actually "wifi". Escaping the space will protect it from being touched by the query string parser: "wi\ fi".

Empty Query

If the query string is empty or only contains whitespaces the query string is interpreted as a no_docs_query and will yield an empty result set.

Appendix A: Regular Expression Query
Regular Expression syntax

Regular expression queries are supported by the regexp and the query_string queries. The Lucene regular expression engine is not Perl-compatible but supports a smaller range of operators. We are not going to explain regular expressions, just the supported operators.

Standard Operators

Standard operators are always enable through the DefenseStorm Console. For more detailed information about standard operators, see Standard Query Operators Overview from Microsoft.

Anchoring

Most regular expression engines allow you to match any part of a string. If you want the regexp pattern to start at the beginning of the string or finish at the end of the string, then you have to anchor it specifically, using ^ to indicate the beginning or $ to indicate the end.

Lucene’s patterns are always anchored. The pattern provided must match the entire string. For string “abcde”:

ab.* # match abcd # no match

Allowed characters

Any Unicode characters may be used in the pattern, but certain characters are reserved and must be escaped. The standard reserved characters are:

. ? + * | {} () \n
If you enable optional features (see below) then these characters may also be reserved:

# @ & < > ~

Any reserved character can be escaped with a backslash “\” including a literal backslash
Additionally, any characters (except double quotes) are interpreted literally when surrounded by double quotes:

john"@smith.com"

**Match any character**

The period "." can be used to represent any character. For string "abcde":

```
ab... # match a.c.e # match
```

**One-or-more**

The plus sign "+" can be used to repeat the preceding shortest pattern once or more times. For string "aaabbb":

```
 a+b+ # match aa+bb+ # match a+ # match aa+b+ # match
```

**Zero-or-more**

The asterisk "*" can be used to match the preceding shortest pattern zero-or-more times. For string "aaabbb":

```
a\'b\' # match a\'b\'c\' # match .\'bbb\'. # match aaa\'bbb\' # match
```

**Zero-or-one**

The question mark "?" makes the preceding shortest pattern optional. It matches zero or one times. For string "aaabbb":

```
```
Min-to-max

Curly brackets "{}" can be used to specify a minimum and (optionally) a maximum number of times the preceding shortest pattern can repeat. The allowed forms are:

{5}  # repeat exactly 5 times {2,5}  # repeat at least twice and at most 5 times {2,}  # repeat at least twice

For string "aaabbb":

a{3}b{3}  # match a{2,4}b{2,4}  # match a{2,}b{2,}  # match .{3}.{3}  # match a{4}b{4}  # no match a{4,6}b{4,6}  # no match a{4,}b{4,}  # no match

Grouping

Parentheses "()" can be used to form sub-patterns. The quantity operators listed above operate on the shortest previous pattern, which can be a group. For string "ababab":

(ab)+  # match ab(ab)+  # match (.)+  # match (.)+  # no match (ab)’  # match abab(ab)?  # match ab(ab)?  # no match (ab){3}  # match (ab){1,2}  # no match

Alternate

The pipe symbol "|" acts as an OR operator. The match succeeds if the pattern on either the left-hand side OR the right-hand side matches. The alternation applies to the longest pattern, not the shortest. For string "aabb":

aabb|bb  # match aacc|bb  # no match aa(cc|bb)  # match a+b  # no match a+b|b+a  # match a+(b|c)+  # match

Character classes

Ranges of potential characters may be represented as character classes by enclosing them in square brackets "[]". A leading ^ negates the character class. The allowed forms are:

[abc]  # ‘a’ or ‘b’ or ‘c’ [a-c]  # ‘a’ or ‘b’ or ‘c’ \[a-c\]  # ‘-‘ or ‘a’ or ‘b’ or ‘c’ [abc-\]  # ‘-‘ or ‘a’ or ‘b’ or ‘c’ \[~abc\]  # any character except ‘a’ or ‘b’ or ‘c’ \[^a-c\]  # any character except ‘a’ or ‘b’ or ‘c’ \[^abc\]  # any character except ‘-‘ or ‘a’ or ‘b’ or ‘c’
Note that the dash "-" indicates a range of characters, unless it is the first character or if it is escaped with a backslash.

For string "abcd":

\alcdl+ # match \[a-dl]+ # match \[^a-dl]+ # no match