



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at <http://www.giac.org/registration/gccc>

OSSIM: CIS Critical Security Controls Assessment in a Windows Environment.

Author: Kevin Geil, info@friendandfamilytech.com

Advisors: Marcos Vieyra and Dave Hoelzer

Accepted: September 2017

Abstract

Use of a Security Information and Event Management (SIEM) or log management platform is a recommendation common to several of the “CIS Critical Security Controls For Effective Cyber Defense” (2016). Because the CIS Critical Security Controls (CSC) focus on automation, measurement and continuous improvement of control application, a SIEM is a valuable tool. Alienvault's Open Source SIEM (OSSIM) is free and capable, making it a popular choice for administrators seeking experience with SIEM. While there is a great deal of documentation on OSSIM, specific information that focuses on exactly what events to examine, and then how to report findings is not readily accessible. This paper uses a demo environment to provide specific examples and instructions for using OSSIM to assess a CIS Critical Security Controls implementation in a common environment: A Windows Active Directory domain. The 20 Critical Security Controls can be mapped to other controls in most compliance frameworks and guidelines; therefore, the techniques in this document should be applicable across a wide variety of control implementations.

1. Introduction.

OSSIM is a free, open-source version of Alienvault's commercial USM (Unified Security Management) solution. Deployment and initial configuration of OSSIM is well documented in the "USM Appliance User Guide" (2017), and the "USM Appliance Deployment Guide" (2017). Unfortunately, an instruction manual providing exact steps that can be used to demonstrate compliance with the critical security controls does not seem to exist. When seeking guidance on what events to log and then how to report on them, a common recommendation from vendors and professional services consultants is to "log and report on the things important to your environment," effectively leaving it up to the analyst to decide what to log and audit.

Although different environments have unique characteristics, most businesses have enough standardization with Active Directory (AD), Windows clients and Windows servers that the instructions demonstrated here can accelerate success in SIEM deployment. Although this paper will focus on methods for demonstrating compliance with the Critical Security Controls, the audited items presented are applicable to most technical control frameworks (Mapping and Compliance, 2017). For a spreadsheet mapping the CSC to multiple control frameworks, refer to the "AuditScripts Critical Security Controls Master Mapping" (2017) from Enclave Security. Because of this paper's focus on Microsoft Active Directory environments, detailed examples are provided for auditing Windows-based systems, while examples for other systems, such as network devices, will be brief.

The testing environment for this demo consists of a Windows server 2008 or higher Domain Controller, an OSSIM instance (Version 5.4), and a Windows client (Windows 7, 8.1, or 10). A link to OSSIM installation instructions is included in *Appendix D: Helpful Links*. It is common for video to be unreadable on a new virtual OSSIM instance. Instructions in *Appendix E-1* will remedy this. One of the assessment methods described in CSC 2 involves the use of AppLocker, Microsoft's application whitelisting technology, which is only available in specific versions of Windows (Requirements to use AppLocker, 2017). The testing environment used for much of this demo is based on the hydration kit provided by deploymentresearch.com (Hydration Kit, 2014), the authoritative source on System Center Configuration Manager and Microsoft

Kevin Geil, info@friendandfamilytech.com

operating system deployment. Using the Deployment Fundamentals hydration kit makes for a fast and repeatable Active Directory testing environment. To achieve the best accuracy in asset (host) and service detection, configuring a DNS reverse lookup zone and using static IP addressing or DHCP reservations is recommended. OSSIM tracks assets by IP address, so it's optimal if machine names and addresses stay consistent. For further instructions, see *Appendix C: Environment and Host Configuration*. The Center for Internet Security Critical Security Controls for Effective Cyber Defense Version 6.1 (2017) document is used for this paper.

This paper is not a step by step guide to installing and configuring OSSIM. It is intended to supplement existing documentation provided by Alienvault. The functionality of OSSIM is a subset of Alienvault USM functionality, so documentation for Alienvault USM works well for OSSIM configuration. Where configuration instructions already exist, readers will be directed to the appropriate documentation. As there may be more than one method for achieving a given goal, this paper is also not an exhaustive description of all methods available for accomplishing a particular objective. This paper builds upon existing documentation by providing specific steps so that a beginning analyst can follow these instructions to assess compliance with the Critical Security Controls.

1.1 Data Sources

OSSIM utilizes open source security tools to retrieve, organize, and display information from network assets. The sources of this information are called “data sources” (*USM appliance User Guide*, 2017, 118.). Events from data sources are parsed and normalized through plugins which associate each log event with an “Event Type,” sometimes referred to as a “plugin_sid,” which is the name of a field in the SIEM database. Refer to *Appendix A: Terms* for more information and examples. These plugins are called Data Source Plugins. For links to the open-source projects used by OSSIM, please see *Appendix D: Helpful Links*. The following data sources are pertinent to this demo:

- A. **Syslog:** OSSIM receives logs from hosts on the network and uses “Data Source Plugins” to normalize the events for analysis. The best practice with syslog is to filter logs from each device type into its own discrete log file, which is read by one or more Data Source Plugins. Separating logs in this manner improves
- Kevin Geil, info@friendandfamilytech.com

performance, and keeps data organized. (Castra Consulting, personal communication, November, 2013). For example:

- o A Cisco ASA device sends syslog data to OSSIM
 - o Rsyslog filtering rules send these events to a file. For example: /var/log/cisco-asa.log (USM Appliance Deployment Guide, p 180.).
 - o Lines in cisco-asa.log are parsed and normalized by the ossim-agent, through rules in the cisco-asa Data Source Plugins
 - o Events from Cisco ASA firewalls are viewable in the web UI under the Cisco asa data source (ID 1636).
- B. **Alienvault HIDS:** Based on OSSEC HIDS (OSSEC Host Intrusion Detection System, <http://ossec.github.io/>), Alienvault HIDS agents forward Windows log events to the OSSIM server in a syslog-type format where they are parsed and added to the SIEM data, through the Alienvault-HIDS plugin (Castra Consulting, personal communication, 2015).
- C. **Alienvault NIDS (Network Intrusion Detection System):** Based on the open-source project Suricata, this plugin captures network traffic, analyzes it, and sends alarms to the OSSIM Server. The detection rule feed for OSSIM is based on the Emerging Threats free feed (K. Coe. Personal communication, July 21, 2017). The “Emerging Threats FAQ” offers a detailed description of the free feed rulesets (“Emerging Threats FAQ,” 2017). The commercial product (Alienvault USM) uses a feed based on the Emerging Threats Pro ruleset.
- D. **Database plugins:** OSSIM uses database plugins which query databases and retrieve information, transforming that information into SIEM events.
- E. **Directive events:** Directive events are those generated by OSSIM based on other collected events, or groups of events. A commonly cited example is one in which the system can be configured to generate a separate event with a high risk score in the case of 1000 failed login attempts followed by a successful one in a given period (*USM Appliance User Guide*, 2017, pp 239-260) .

Kevin Geil, info@friendandfamilytech.com

As events are normalized in OSSIM, they are assigned values for priority and reliability, so that a risk score can be determined. A risk score is calculated for each event by multiplying the event priority, reliability, and asset value (assigned when assets are added to the database), and dividing by 25 to normalize the risk between 1 and 10. In simple terms, $Risk = (priority * reliability * asset_value) / 25$. Any event with a risk score greater than 1 will generate an alarm. OSSIM's correlation engine also detects certain combinations of events that are indicative of particularly high-risk behavior. When these correlation rules are triggered, a new event is generated with a higher total risk score (*USM Appliance User Guide*, p 10.). It is easy to start adding assets and log files into OSSIM without understanding how risk is calculated and move blissfully along, but understanding how risk is scored (and in turn how alarms are generated) will make future tuning faster.

The fundamental process for assessing compliance with each control is to:

- Configure prerequisites on network or hosts. After the first three controls, most prerequisites (such as configuration of audit policy, sniffing interfaces, and HIDS agent installation) for subsequent controls will be in place.
- Configure OSSIM Data Source Plugin or detection capability.
- Ensure that Asset values, priority, and reliability are appropriate.
- Create a Data Source (DS) Group. For most endeavors within OSSIM, creating a custom DS Group is helpful for focusing on events of interest to achieve a desired auditing or incident response goal.
- Create a view in SIEM View for export (or reporting in commercial version).

The aforementioned steps will be described in detail for CSCs 1-3. Following the procedures discussed in CSCs 1-3 will satisfy system configuration prerequisites for CSCs 4-20. The detailed steps demonstrated in CSCs 1-3 will also provide a template for OSSIM configuration so that the steps for subsequent controls can be discussed more broadly.

Kevin Geil, info@friendandfamilytech.com

1.2 Differences between OSSIM and Commercial AlienVault Product

OSSIM differs from the commercial product, AlienVault USM, in several ways, a few of which can save analysts significant time. The different methods available for saving views in AlienVault USM versus OSSIM have the biggest impact on workflow. Custom views in AlienVault USM can be saved with search criteria, such as Data Source Plugins, Data Source Groups, or field searches (such as source host). OSSIM only allows saving a view with the selected fields and not the search criteria. Saving search criteria with views is more efficient, as it allows the analyst to simply select a saved view which presents the data in a logical format, as opposed to the necessity of selecting search criteria in OSSIM. AlienVault USM provides the ability for the analyst to create custom report modules from saved views. In this way, information can be compiled and emailed to the appropriate person at regular intervals.

OSSIM does not support the creation of custom report modules at all, which is limiting. For events that are interesting, but not necessarily alarming, such as Dropbox usage, one of the most powerful tuning methods in AlienVault USM is to create a report module for those events, which gets emailed on a schedule. The priority of the event in question can then be decreased, so alarms are not generated, allowing analysts to focus on more important events.

The included security intelligence feed in AlienVault USM is significantly more effective than that of OSSIM. The feed included with AlienVault USM includes more than 2000 correlation directives not included with OSSIM (Compare AlienVault Products, 2017). A feed of correlation directives built by a team of experienced security professionals provides significant value for detecting threats and compromises. If SIEM implementation is done as part of a compliance initiative, it is worth noting that AlienVault USM provides for the digital signing and long-term storage of logs. OSSIM does not do this without additional configuration which is beyond the scope of this paper. If this is of interest, please see *Appendix D: Helpful Links*. Automating reports from OSSIM may be possible using third-party tools. This also, is beyond the scope of this paper.

Kevin Geil, info@friendandfamilytech.com

2. CSC 1. Inventory of Authorized and Unauthorized devices

The Asset Management section of the *USM Appliance User Guide* describes methods for adding assets to the system (2017, pp. 70-108). Once an approved asset inventory is stored in OSSIM's database, the following processes will provide relevant information upon discovery of new assets. At the time of this writing, without customization, OSSIM does not create alarms or events for host discovery, but there is a community plugin which will generate alarms and events for the addition of assets (PacketInspector, 2014). Instructions for setting up the New Asset plugin are available in *Appendix B-2: New Asset Plugin*. Once the new asset plugin is installed, one or two of the machines in the testing environment should be started. After a couple of minutes, the passive asset detection system will discover the new machine(s) and add them to the database. The New Asset plugin will query the OSSIM database and generate an event upon detection of the new asset. Depending on the business' needs, there are a few ways to handle these events. If the plugin is installed exactly as described in Appendix B-2, OSSIM will generate an alarm when an asset is added to the database with a value of 2 (the default) or more. If immediate notification is needed, a policy can be created to email the appropriate party whenever the new asset event occurs. This procedure is documented in the Policy Management section of the *USM Appliance User Guide* (2017, pp. 210-254). If immediate notification is not needed, events from the new asset plugin can be compiled into a custom view in the SIEM context, using the procedure below, depicted in Figure 2-1:

2.1 Configuration

In OSSIM's Web UI,

- A. Select Analysis>SIEM
- B. In the "Data Sources" dropdown, select "New Asset. When the new asset events populate in the list of events,
- C. Click "Change View", and "Create New View".

Kevin Geil, info@friendandfamilytech.com

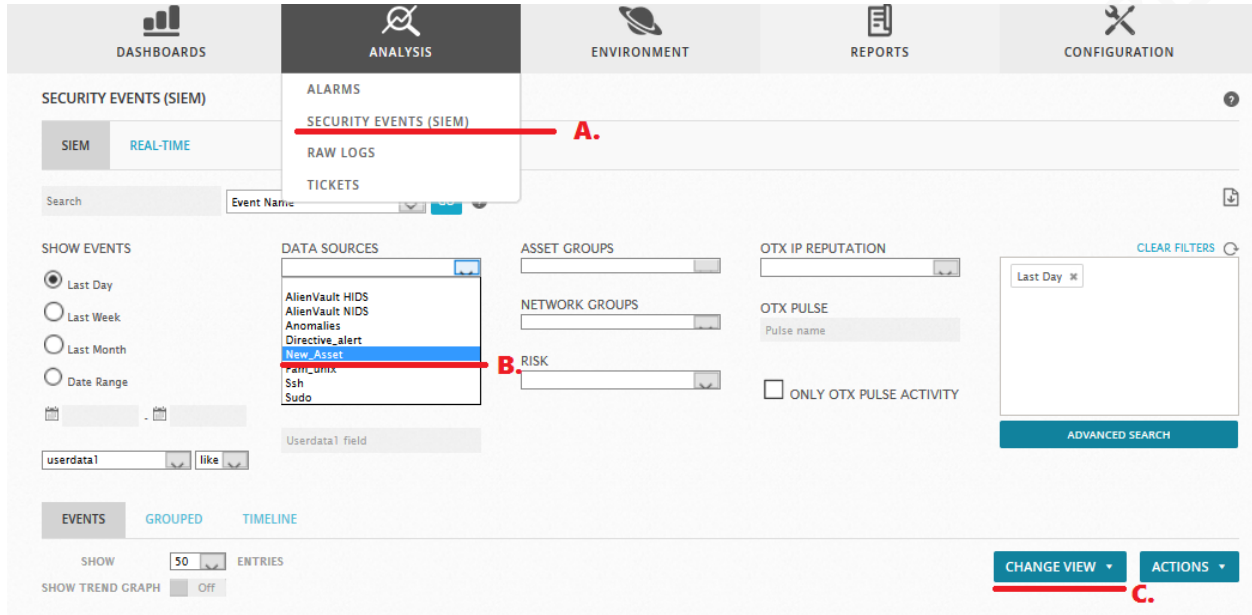


Figure 2-1: Creating a Custom View

D. In the window that pops up, click the plus sign next to:

- Event name
- Received Event Date
- Userdata 1
- Resolved Source IP FQDN
- Source IP

E. Name the view New Asset.

F. Click the “Create” button. This field selection window is shown in Figure 2-2

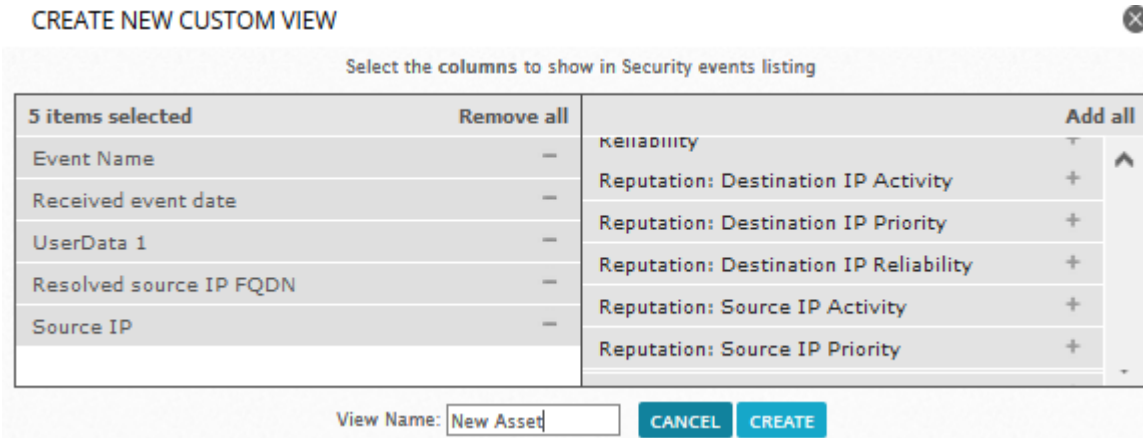


Figure 2-2: Field Selection

Kevin Geil, info@friendandfamilytech.com

G. Decrease the reliability or priority of the new asset plugin so that the number of alarms generated is appropriate for the business goal. OSSIM's default value for networks is 2 and assets are assigned the value of the network in which they are discovered. Thus, when setting the priority of the New Asset events to 2, alarms will be generated for assets with a value of 3 or greater. This is done by clicking Configuration>Threat Intelligence>Data Source, then searching either New Asset or 9720 (the plugin ID) and clicking the magnifying glass icon to the right of the listed plugin. The drop-down menus next to the priority and reliability values allow for adjustment. After this is done, it is easy to check for newly discovered assets by selecting the New_Asset data source, then selecting the "New_Asset" view so that the columns populate properly. After confirming that a newly discovered asset is an approved network device, the asset can be scanned for services and named appropriately. In the commercial version (Alienvault branded products), views can be saved with the data source selection, then saved as a report module, which then can be regularly emailed to the appropriate person.

3. CSC 2. Inventory of authorized and unauthorized software

OSSIM and Alienvault do not have the ability to directly inventory machines for software, but several capabilities can be utilized. Alienvault HIDS can be used to audit Microsoft's AppLocker so that attempts to run unapproved software are tracked. HIDS agents are also capable of recording software installation activity. Several Alienvault NIDS rules exist which detect potentially unwanted software in the environment. To get the most out of these capabilities, several configuration items are recommended:

3.1. Recommendations and prerequisites:

Asset scan: Although not a strict requirement, an asset scan should be performed, complete with reverse DNS lookup, and the hosts should be updated in the database. To ensure that the domain has the capability to support reverse lookup, see *Appendix C: Environment and host configuration*. Detailed instructions for asset scans are available in the *USM Appliance User Guide* (2017, pp. 72-86). For the most accurate scan results, selecting "full scan" and a "normal"

Kevin Geil, info@friendandfamilytech.com

timing template is recommended. For this demo, selecting “use fqdn as hostname” is appropriate when updating the asset database. Depending on the asset value, and the priority/reliability values configured in the new asset plugin, this may generate alarms. If suppression of these alarms is desired, temporarily decrease the priority and reliability for the new asset data source (explained in section 2-G of this paper).

Audit Policies: For this paper, the audit policy recommendations from the CIS Benchmarks document, Section 17: “Advanced Audit Policy Configuration” are used. (CIS Microsoft Windows Server 2012R2, 2017, pp. 202-225.)

Applocker group policies. See *Appendix C: Environment and host configuration*.

3.2. OSSIM Configuration: Enable Applocker rules and edit shared configuration file

Some sets of AlienVault Hids rules are disabled in the default configuration. The following steps will enable the appropriate rules for AppLocker event detection:

- A. Navigate to Environment>Detection>Config. In the window displaying “enabled rules” and “disabled rules”, type “AppLocker” in the search box.
- B. Click the + sign next to the listing for AlienVault-windows-applocker_rules.xml, and click save.

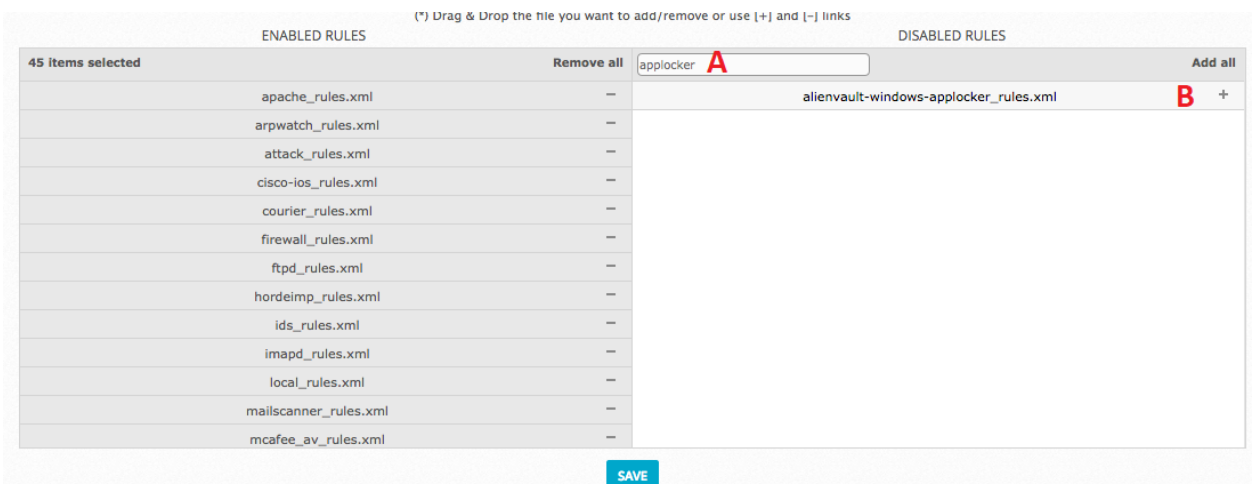


Figure 3-1: Enabling Applocker Rules

Kevin Geil, info@friendandfamilytech.com

- C. From the current page, click Agents>Agent.conf. In order to configure the hids agents to send AppLocker logs to OSSIM, paste the text below (everything from the start of the first <agent_config> tag to the closing </agent_config> tag into the text entry area, so it looks like the screenshot in figure 3-2:

```
<agent_config>
<localfile>
  <location>Microsoft-Windows-AppLocker/EXE and DLL</location>
  <log_format>eventchannel</log_format>
</localfile>
<localfile>
  <location>Microsoft-Windows-AppLocker/MSI and Script</location>
  <log_format>eventchannel</log_format>
</localfile>
</agent_config>
```

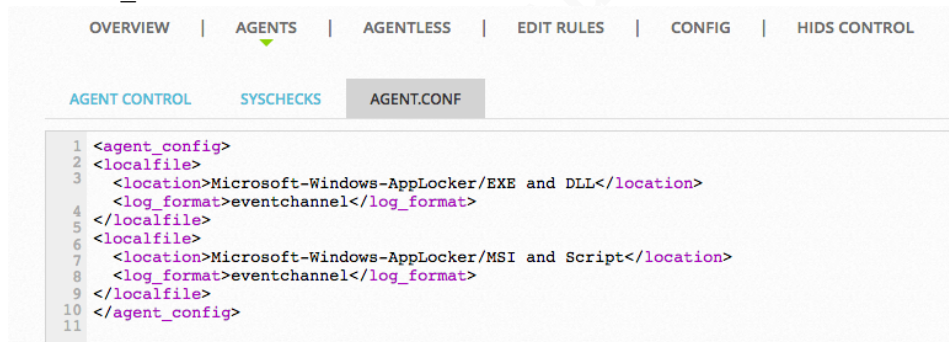


Figure 3-2: Editing shared agent.conf

- D. Click “Hids Control”, and on the right hand side, click “restart” to restart the HIDS service (See figure 3-3). Alienvault Hids will now be configured to alert on AppLocker events.

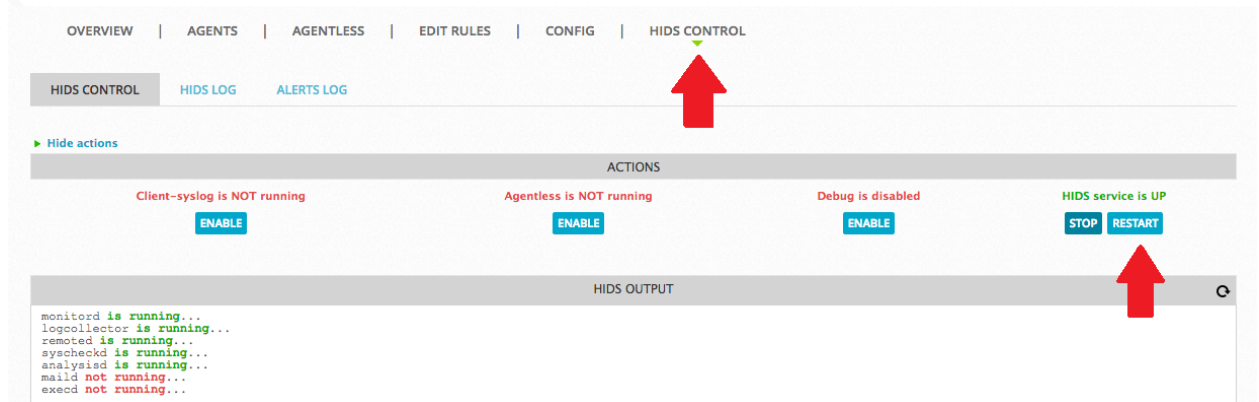


Figure 3-3: Restart HIDS Control

3.3. HIDS Agent Installation: The steps outlined in section 3.2 provide a shared agent configuration for the AlienVault HIDS agents, which should now be installed on hosts. There are Kevin Geil, info@friendandfamilytech.com

several methods of HIDS agent installation, discussed in the *USM Appliance Deployment Guide*, including the Getting Started Wizard (2017, p. 84), and from the HIDS Control Page (2017, p. 115). As documented in the *USM Appliance User Guide* (2017, p. 86), HIDS agents can also be deployed from the asset management page. This method is useful for deploying agents to groups of assets. If HIDS agents were previously installed, restarting HIDS Control, then restarting the HIDS agents on the clients two times will send the shared agent.conf file to the client hosts.

3.4. Create custom data source groups and custom views.

In Alienvault lingo, a data source group is called a “DS Group”. A custom DS group is a subset of event types (sids) from one or more data sources that provides the analyst with data relevant to the task at hand. A DS group can contain plugin events or directive events, but not both. This is because plugin events and directive events are generated and parsed at a different levels within the server (K. Coe, personal communication, July 21, 2017). A custom view is a selection of normalized fields from the events in a DS group. Creation of custom DS groups and views is a frequently repeated process in OSSIM administration. Screenshots and detailed instructions are included below. The method used here can be used as a template for subsequent controls, for which only the event types and names of view fields will be covered.

DS Group Creation: Three DS groups will be created here. Two will include events from Alienvault HIDS agents; one will include events from Alienvault NIDS. The method described below existed in past versions of the *USM Deployment User Guide*, but in the current version, DS Group creation is only contained in the “Creating or Modifying a Policy section of the *USM Appliance User Guide*, (2017, pp. 216-219).

- A. Click Configuration>Threat Intelligence>Data Source>Data Source Groups. Click “Add New Group.” Name this group “Application Installation Activity”, and enter a description. Click “add by data source,” and in the search box, type 7006, then click on the result to open the AlienVault HIDS-windows group that appears. See Figure 3-1 for details.

Kevin Geil, info@friendandfamilytech.com

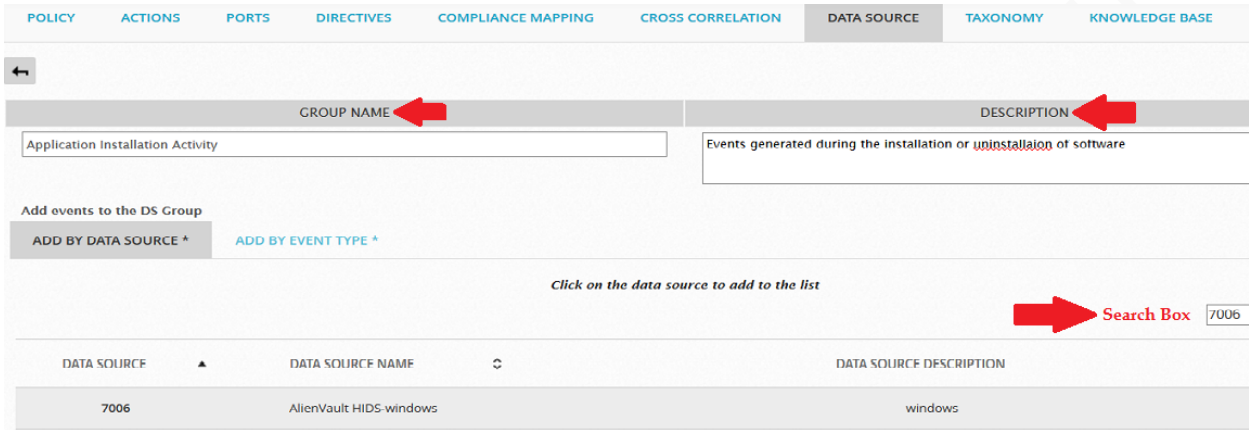


Figure 3-1: Custom DS Group Creation, Step A

B. Click the pencil icon on the right-hand side. See Figure 3-2.

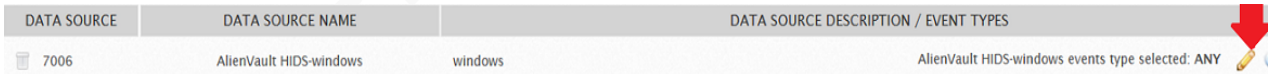


Figure 3-2: Selection of Specific Events (Step B)

C. In the search box, type the word “application.” Click the + sign next to 2 events: 18146, and 18147 and then “submit selection” to add them to the new DS group. This returns the user to the custom DS group window. See Figure 3-3.

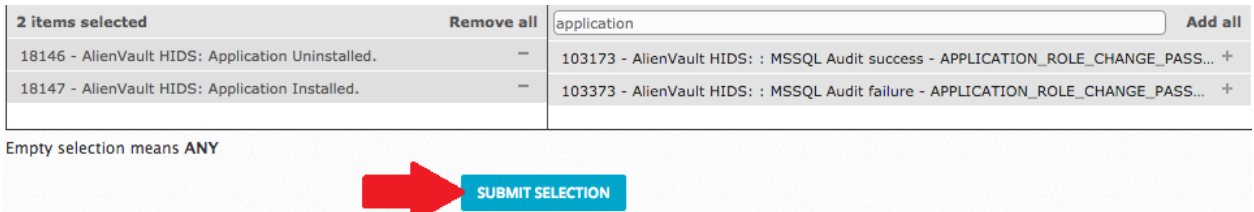


Figure 3-3: Search For and Add sids to the Custom DS Group(Step C)

D. Click “Update” to save the DS group.

Kevin Geil, info@friendandfamilytech.com

- E. AlienVault NIDS software events.** Click Configuration>Threat Intelligence>Data Source>Data Source Groups. Click “Add New Group.” Name this group “Potentially unwanted software.” Click on AlienVault NIDS 1001, and type “policy” in the search box. Click the “Add all” button on the right-hand side. For this demo, the events that will be used are: 2014297 “ET Policy Vulnerable Java Version 1.7.x Detected,” and 2001115 “msi download.”
- F. AppLocker events.** Click Configuration>Threat Intelligence>Data Source>Data Source Groups. Click “Add New Group”. Name this group “AppLocker”. Click “Add by Data Source,” and type “7006” in the search window, and click on the “AlienVault Hids-Windows” group that appears. Click the pencil to add/edit event types, type “AppLocker” in the search window, and click “Add All” to populate the DS group. Currently, the sids are 110020-110025. Group policies for AppLocker are described in *Appendix C: Environment and host configuration*.

3.5. Generate and analyze events: To test detection, follow the steps below.

A. On a Windows client machines with the AlienVault HIDS agent installed, download the following two packages to C:\temp, and install them:

Outdated Java Runtime: <http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase7-521261.html#jre-7u55-oth-JPR>

Microsoft LogParser downloaded from here: <http://www.microsoft.com/en-us/download/details.aspx?id=24659>

B. Once the software is installed, navigate to Analysis/SIEM, and create a view called “Software Installation”, with the following fields:

- Event name
- Received event date
- UserData 3
- Username
- UserData 5

C. Navigate to “SIEM View” by clicking Analysis/Security Events (SIEM), under “Data Source Groups,” select the ds group created in step 3.4 A: Application Installation activity, and the

Kevin Geil, info@friendandfamilytech.com

software installation events will display. This will provide appropriate information regarding software installation.

D. In SIEM View, Select the DS Group created in step 3.4 E: “Potentially unwanted software” under Data Source Groups. In the “Change view” dropdown, select “Default.” Events for “EXE or DLL Windows file download” will populate.

E. On the machine with the vulnerable Java version, navigate to <https://www.java.com/en/download/installed.jsp>, and click “verify,” then “agree and continue,” and run Oracle’s Java detection application.

F. Refresh the events in SIEM view, and the event for “ET Policy Vulnerable Java version 1.7.x” will populate along with the previously detected events.

G. AppLocker Events: IN SIEM View, select the AppLocker DS group created in step 3.4 F. Creating a view with the fields below will provide the pertinent details on AppLocker events:

- Event Name
- Received Event Date
- IDM: Hostname Source IP
- ExtraData Username
- ExtraDataFilename

If AppLocker is planned to be run in block mode in the environment, it may be worth increasing the priority of the sids corresponding to programs getting blocked, so that alarms are generated, administrators are notified, and problems are fixed. Adjusting these values was demonstrated in section 2.1 G of this paper. **Note:** As of this writing (August 2017), the OSSIM plugin is not parsing out the Username and Filename from AppLocker events. A plugin improvement ticket has been submitted to Alienvault, and parsing should improve in the future. As a result, the fields in the view described above might need to be changed to properly reflect the username of the user who attempted to run the application, and the path of the file itself. Double clicking on one of the AppLocker events will show what fields are being currently parsed by the plugin so that adjustments can be made.

Kevin Geil, info@friendandfamilytech.com

4. CSC 3. Secure configurations for hardware and software:

OSSIM has many ways to detect configuration changes to hosts. Once the Alienvault HIDS agent is installed, the default settings for integrity monitoring (FIM) record most registry changes and changes to the “C:\Windows” directory. This functionality is fundamentally the OSSEC syscheck functionality with some directories and registry entries added. Syscheck stores hashes on the OSSIM server for files in critical directories and registry keys. At a regular interval (6 hours by default), checksums for the same files and keys are created and compared to the values on the server. If a change is detected, an alert is generated (Syscheck, 2017).

4.1. Recommendations and prerequisites: The most important recommendation is to start with documented standards and configuration change procedures. A single package installation may generate dozens (maybe hundreds) of FIM events. If these can be correlated to an approved change request, or a planned update installation, filtering out noise is easier.

4.2. OSSIM Configuration:

- A. In addition to the “out of the box” integrity monitoring, critical directories can be added to the configuration. This is easily done through the web UI:
 - Navigate to Environment>Detection>Agents>Syschecks.
 - Under the “Files/Directories monitored” row, a directory path can be entered. For this demo, add the C:\Temp directory, and click save.
- B. Create a custom DS group called Integrity Monitoring using all of the event type IDs from Data Source 7094.
- C. Create a new view with the following fields:

● Event Name	● IDM Hostname Source IP
● Received event date	● ExtraData Filename

4.3. Generate and analyze events. If the Alienvault HIDS agent has been installed on the test client and has been running for several hours, the first syscheck should be completed, Kevin Geil, info@friendandfamilytech.com

and checksums should be stored in OSSIM. If there is uncertainty, syscheck can be initiated in the following ways:

- Allow 24-48 hours for checksums to be created.
- Restart the OSSEC agent on the client by running `C:\program files (x86) ossec-agent\win32ui` as administrator, and clicking “manage” and “restart”.
- Start or restart Syscheck by navigating to Environment>Detection>Agents, and clicking the green circle with the checkmark in it. A confirmation message will appear on the screen.
- Log into the CLI interface of OSSIM, and initiate a recheck by invoking:
 - `#!/var/ossec/bin/agent_control -r -u <agent id>`
 - The agent id for the previous command can be obtained by invoking `#!/var/ossec/bin/agent_control -l` (Syscheck, 2017)

In order to generate the FIM events, the following steps are necessary.

- A. In the test client, add a new text document to `C:\Temp`, and add some text.
- B. Add a line to `C:\Windows\System32\drivers\etc\hosts`.
- C. Allow some time for syscheck to complete again, then log into OSSIM’s web UI.

In order to analyze FIM events, navigate to SIEM View, and select the custom DS group created in step 4.2-B “Integrity Monitoring”, and select the custom view created in step 4.2-C. If this shows a large number of events, there is a search box on the lower left-hand side in SIEM View, where “Filename” can be selected in the dropdown, then “Like” can be selected in the next dropdown, and then the analyst can search for “txt” or “hosts” which can narrow the search, as indicated below in Figure 4-1.

Kevin Geil, info@friendandfamilytech.com

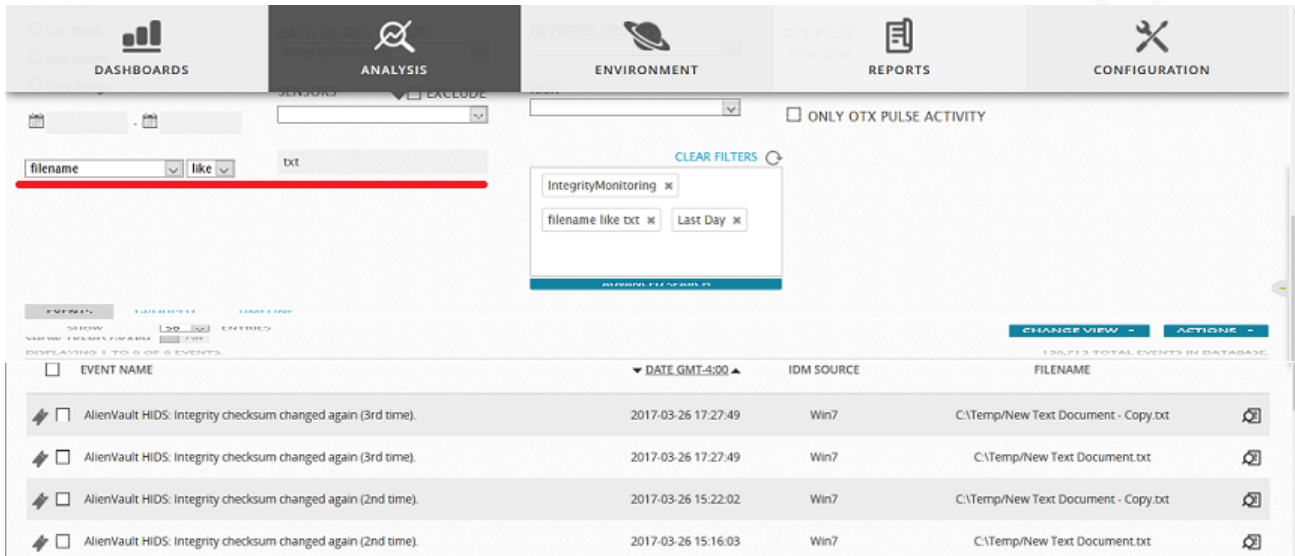


Figure 4-1: Custom View for FIM

As Figure 4-1 shows, the custom view created in steps 4.2 B-C provides the date and time of a FIM event, the item that was changed, and the machine on which it occurred. If the events do not correspond to a change control request, further investigation may be warranted. The common recommendation for implementing FIM is to start slowly, with a small group of uniform machines, and tune the FIM system until desired results are achieved. After that, more machines can be incorporated into the FIM system. Online documentation for OSSEC will provide detailed information on how to tune the syscheck feature.

5. CSC 4. Continuous Vulnerability Assessment and remediation.

Vulnerability assessment, based on OpenVAs, is an included feature. Details on how to set up and run vulnerability scans are contained in the *USM user guide* (2017, pp. 264-300). Authenticated vulnerability scans are recommended for best accuracy. Once the scan is run, reports are available in HTML, PDF, CSV, and NBE format. If regular scans are configured, past reports can be saved for comparison to one another. Aside from being able to track vulnerabilities and mitigation over time, one of the biggest benefits of regular vulnerability scans in OSSIM is cross-correlation. Cross-correlation is a process by which attacks detected by

Kevin Geil, info@friendandfamilytech.com

OSSIM's network IDS are compared to vulnerabilities on the attack targets. If a match is found between an attack and a vulnerability on the target, the "reliability of the IDS event increases to 10" (*USM Appliance User Guide*, p. 260). Because a known attack against a known vulnerability has a high likelihood of succeeding, cross-correlation provides valuable information to the analyst. Another useful feature is that vulnerabilities of associated assets are displayed on the alarms page for use during manual analysis. This gives the analyst the ability to make determinations on host attributes such as the patch level or related vulnerabilities.

6. CSC 5: Controlled use of administrative privileges.

For mature organizations where administrative accounts are only used when planned changes are being made, tracking administrative logins is straightforward. For organizations on the other end of the spectrum, where the generic domain administrator account is used for routine work and domain administrators log into every machine with privileged accounts, the volume of privileged authentications may be too great for effective auditing. There are two correlation directives described in *Appendix B-3: Correlation Directives*, one for organizations on the high end of the maturity spectrum, which tracks all privileged authentication events, and one for organizations on the low end of the maturity spectrum, which tracks authentications using the name "administrator" (or any username the analyst chooses). CSC 5 stipulates that administrative accounts should only be used when required (CIS Critical Security Controls, p. 21). In organizations in strict compliance with this, the directive described in *Appendix B-3.1: Correlation Directive: administrator login (Any administrative account)* should be appropriate. Once they are set up, policies or separate correlation directives can be created so that administrative logins generate alarms based on criteria such as time of logon or asset group membership. The only environmental requirements are a properly configured audit policy, and running Alienvault HIDS agents. The CIS Benchmarks document referenced in section 3.1 provides guidance on audit policy configuration.

To view the events gathered after configuring the correlations directives, a DS Group should be created, based on Data Source 1505 (directive events), and the specific directive events which have been created (custom directive events are assigned IDs starting with 500001). An effective
Kevin Geil, info@friendandfamilytech.com

SIEM view can be created by selecting Event Name, Received event date, Username, UserData 1, IDM Destination Username@Host or IP:port format, and UserData 4, as seen below in Figure 6-1:

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	USERNAME	USERDATA1	DESTINATION	USERDATA4	
<input checked="" type="checkbox"/>	directive_event: General Admin Login	2017-04-11 11:46:35	kevinadmin	TESTDOMAIN	Win-7	Windows Logon with Special privileges	
<input checked="" type="checkbox"/>	directive_event: General Admin Login	2017-04-11 11:46:35	kevinadmin	TESTDOMAIN	Win-7	Windows Logon with Special privileges	
<input checked="" type="checkbox"/>	directive_event: General Admin Login	2017-04-11 11:46:07	kevinadmin	TESTDOMAIN	Win-7	Windows Logon with Special privileges	
<input checked="" type="checkbox"/>	directive_event: General Admin Login	2017-04-11 11:46:07	kevinadmin	TESTDOMAIN	Win-7	Windows Logon with Special privileges	

Priority threshold: 0
Active Event Window (days): 5

< PREVIOUS NEXT >

Figure 6-1 Viewing Administrative Logon Events

With a view similar to the one shown in Figure 6-1, an analyst can take note of an administrative login, and examine information about the affected machine, and the time of the event. These can be compared to service management requests to ensure that proper procedures are being followed. If these events occur in great numbers (hundreds per day on an administrator's workstation), it is likely that administrative accounts are being used for routine use, which is prohibited by CSC 5.

7. CSC 6: Maintenance, Monitoring, and analysis of audit logs

In a production deployment, it is critical that time is being synchronized among all nodes and OSSIM. Fortunately, in an Active Directory domain, domain controllers perform this function, and configuring OSSIM to synchronize with one is well documented in the USM Deployment Guide (2017, p. 68). OSSIM has a message center, which provides alerts if an asset has stopped sending logs, or if OSSIM is receiving logs from a device for which an associated plugin is not enabled or operating. These messages are helpful for validating that devices are sending logs properly (*USM Appliance User Guide*, 2017, pp. 365-370). OSSIM does not offer archiving and digital signing, which is one of the differences between OSSIM and Alienvault, mentioned in section 1.2 of this paper.

7.1. Configure Network boundary devices to log all traffic

Kevin Geil, info@friendandfamilytech.com

OSSIM has plugins available for most major firewall vendors. Procedures for enabling plugins are well documented in the *USM deployment guide* (2017, pp. 160-222). At this point in the demo, it is appropriate to inject sample log data into OSSIM. The scripts to load this sample data, as well as much of the sample data, has been cloned from Santiago Basset's Github site (2017), and augmented for this demo. In collaboration with Joe Schreiber (aka Packet Inspector), Basset has created a fantastic, easy to use tool for placing sample data into an OSSIM deployment. To obtain and run the tool, log into OSSIM using either a console session or SSH, and gain root access by selecting the "Jailbreak System" option. If guidance on jailbreaking and invoking commands is needed, refer to *Appendix B*. After jailbreaking OSSIM, install git, and clone the Alienvault demo scripts repository using the following commands:

```
alienvault# apt-get update;apt-get -y install git;git clone  
https://github.com/kgeil/Alienvault-Demo_scripts
```

Next, navigate to the Alienvault-Demo scripts directory by invoking:

```
alienvault:~# cd Alienvault-Demo_scripts/
```

From here, to install the demo scripts, and add the proper sonicwall events, invoke:

```
alienvault# perl install.pl ; sonicwall/convert_sonicwall.sh
```

The installed demo data will be used to demonstrate auditing of some subsequent controls. Data from Sonicwall, Fortigate, and Cisco ASA firewalls is included in the sample data. Selecting each of these as a data source will demonstrate a variety of firewall log events. Once the demo scripts have been run, an easy way to analyze network traffic logs from SIEM View is to type the word "connection" in the search box next to Event name. The results will look similar to *Figure 7-1*.

Kevin Geil, info@friendandfamilytech.com

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	SENSOR	OTX	SOURCE	DESTINATION
	SonicWALL: TCP connection dropped	2017-08-30 18:39:06	alienvault	N/A	209.213.234.153:1447	209.128.98.150:135
	SonicWALL: Connection opened	2017-08-30 15:31:42	alienvault	N/A	10.0.16.2:4140	10.0.16.46:443
	ASA: The first SVC connection was established for the SVC session	2017-08-30 10:41:40	alienvault		50.74.173.203	0.0.0.0
	ASA: The DAP records that were selected for the connection are listed	2017-08-30 10:41:39	alienvault	N/A	72.78.207.231	0.0.0.0
	SonicWALL: Connection opened	2017-08-30 11:22:57	alienvault	N/A	10.0.16.2:2129	10.0.16.46:443

Figure 7-1 Connection logs

As shown in *Figure 7-1*, in addition to basic fields such as event name, source, destination, risk and asset value, there is a column for OTX (Online Threat Exchange). OTX is a platform supported by Alienvault for the exchange of threat information (“Welcome to AlienVault Open Threat Exchange,” 2017). In the context of network connection analysis, the OTX icon indicates that malicious activity has been associated with a particular IP address. Right clicking on the IP address next to the icon offers several options useful for incident investigation, including “Look up in OTX (shown below in *Figure 7-2*).”

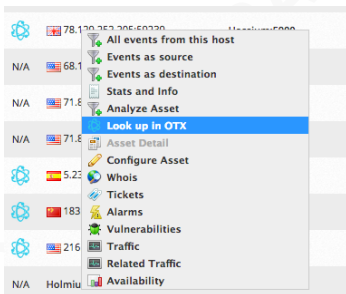


Figure 7-2 IP lookup options

This link brings the user to the OTX site, where analysts can examine indicators of compromise associated with the IP address in question. OTX lookup, as well as the other options available in the right-click menu, provide multiple options useful in gaining awareness of host communications (*IP Reputation Explained, 2017*).

Kevin Geil, info@friendandfamilytech.com

9. CSC 7: Email and Web Browser Protections

Malware, phishing exploits, and unusual user agent strings are all detected by the Alienvault NIDS agent. To view NIDS events in Siem view, Alienvault NIDS can be selected as a Data Source, and the default view works for most purposes. An easy demonstration for this is to change the user agent string in Firefox to: “Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; AntivirXP08; .NET CLR 1.1.4322)”, and browse to any site. Instructions for changing user agent strings are readily available online (Hoffman, 2016). As demonstrated in section three, outdated browser plugins are also recognized by Alienvault NIDS. Plugins are available for spam appliances such as Cisco Ironport, Spam Assassin, Barracuda, and McAfee Anti-Spam.

10. CSC 8: Malware protection

OSSIM offers plugins for most centrally managed antivirus products (Alienvault USM Appliance Plugins List, 2017). Once installed, correlation directives can be developed that will raise the reliability of any alarm detected within a certain time period of malware detection. The sample data loaded in section 8 provides examples of malware activity detected by Alienvault HIDS.

11. CSC 9: Limitation and Control of Network Ports, Protocols, and Services, and CSC 11 Secure Configurations for Networked Devices such as Firewalls, Routers, and Switches.

Assuming that router, switch, and firewall configurations are documented, configuration changes on these devices can be evaluated and correlated with change management requests. Even without a mature configuration management process, tracking configuration changes made to networked devices provides substantial value to an organization. In addition to evaluating potential security impacts of network device changes, an analyst capable of presenting a list of

Kevin Geil, info@friendandfamilytech.com

device changes over a period of time can save an organization’s networking team significant time during a downtime event. Finally, recognizing how much unplanned, undocumented change occurs may be a good first step in adopting change management procedures.

Below are examples of configuration changes on Sonicwalls and Cisco ASA firewalls. An effective method for finding interesting events (including device configuration changes) is to view events in SIEM view, limit by data source, clicking the “grouped” button. The most frequent events are often normal events, but can point to either security incidents or configuration errors, such as 15,000 failed VPN tunnel negotiations. Often, configuration changes and valuable security events will show up in the least frequent events. These can become the basis for custom DS groups for faster analysis.

Examples used in this demo focus on logs from two popular firewalls: Sonicwall, and Cisco ASA. Cisco ASA configuration changes can be viewed by creating a DS Group using Data Source 1636 (cisco-ASA), and Data Source ID 111008 (“ASA: the user entered any command”). A custom view containing “Event Name,” “Received Event Date,” “Username,” and “Userdata 2” shows the user making the change, and the command invoked. See *Figure 11-1* for an example.

▼ DATE GMT-4:00 ▲	EVENT NAME	USERNAME	USERDATA2
2017-08-30 10:59:44	ASA: The user entered any command	enable_15	access-list OUTSIDE_IN extended permit tcp an...
2017-08-30 10:59:41	ASA: The user entered any command	enable_15	access-group OUTSIDE_IN in interface outside
2017-08-30 10:59:41	ASA: The user entered any command	enable_15	access-list OUTSIDE_IN extended permit tcp an...

Figure 11-1 Cisco ASA Changes

Similarly, a custom DS group using Data Source 1573 (Sonicwall), and event IDs 440-443 will highlight Sonicwall access rule change events. A custom view containing fields “Event Name,” “Received Event Date,” “Username,” and Userdata 4, 5, 6, and 7 will provide information on the person who made the rule, and the zones affected (Shown in Figure 11-2).

Kevin Geil, info@friendandfamilytech.com

<input type="checkbox"/>	▼ DATE GMT-4:00 ▲	USERNAME	USERDATA4	USERDATA5	USERDATA6	USERDATA7	EVENT NAME
🔍 <input type="checkbox"/>	2017-06-30 12:17:20	Tom	Access rule deleted	Allow	Secure Subnets	IT workstations	SonicWALL: Access rule deleted
🔍 <input type="checkbox"/>	2017-06-30 12:28:24	Dick	Access rule deleted	Allow	IT workstations	Secure Subnets	SonicWALL: Access rule deleted
🔍 <input type="checkbox"/>	2017-06-30 12:33:58	Harry	Access rule added	Allow	Secure Subnets	IT workstations	SonicWALL: Access rule added
🔍 <input type="checkbox"/>	2017-06-30 12:33:58	FWAdmin	Access rule added	Allow	IT workstations	Secure Subnets	SonicWALL: Access rule added

Figure 11-2 Sonicwall Changes

As the two prior examples show, OSSIM can be configured to obtain a wealth of information about network device configuration changes, in order to help assess compliance with CSC 9.

12. CSC 12: Boundary defense:

With the sample data loaded, selecting Cisco-ASA or Sonicwall as the Data Source in SIEM view will provide a great deal of events to report on. For example, VPN logins for the Sonicwall plugin can be viewed by creating a DS group with Data Source 1573, and event types 237 and 1080. Selecting this DS group and creating a custom view including “received event date,” “event name,” “username,” “source IP,” and “destination IP” will provide the analyst with who, what when and from where for VPN logins (Shown in Figure 12-1). The sample data for the Cisco asa will provide interesting information by creating a DS group with Data Source 1636 and event type IDs from 338001- 338008. The custom view for these events should include “event name,” “received event date,” “source IP,” “destination IP,” and “OTX”.

▼ DATE GMT-4:00 ▲	EVENT NAME	USERNAME	SRC IP	DST IP
2017-06-30 21:46:10	SonicWALL: VPN zone remote user login allowed	Nadia	203.0.113.217	198.51.100.55
2017-06-30 20:47:35	SonicWALL: VPN zone remote user login allowed	Nadia	203.0.113.217	198.51.100.55
2017-06-30 10:25:21	SonicWALL: SSLVPN zone remote user login allowed	MAMA	203.0.113.217	198.51.100.55

Figure 12-1 Sonicwall VPN logins

Kevin Geil, info@friendandfamilytech.com

▼ DATE GMT-4:00 ▲	EVENT NAME	SRC IP	DST IP	OTX
2017-06-30 16:54:32	ASA: Traffic to a blacklisted IP address in the dynamic filter database has appeared	192.168.100.76	69.69.164.41	N/A
2017-06-30 16:54:32	ASA: Traffic to a blacklisted IP address in the dynamic filter database has appeared	192.168.100.76	105.233.27.142	N/A
2017-06-30 16:54:32	ASA: Traffic to a blacklisted IP address in the dynamic filter database has appeared	192.168.100.76	25.228.203.167	N/A
2017-06-30 16:54:31	ASA: Traffic to a blacklisted IP address in the dynamic filter database was denied	192.168.100.76	121.243.225.12	

Figure 12-2 Cisco ASA Blacklisted IP analysis

General browsing of the sample data in SIEM view should prove interesting to a curious analyst, and should spark ideas for future analysis and DS group creation. Investigating all such possibilities is well beyond the scope of this paper.

13. CSC 13: Data Protection:

Tracking USB drive usage can be done by creating a custom DS group from Data Source 7006, and event type ID 100051: USB device added or removed. As shown in Figure 13.1, a view using Event name, Date, and Source IP FQDN will provide the analyst with the date, time, and host machine on which a USB device was inserted or removed.

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	SOURCE	DESTINATION
<input checked="" type="checkbox"/>	AlienVault HIDS: USB device added/removed	2017-05-31 09:37:20	Win7-test	0.0.0.0
<input checked="" type="checkbox"/>	AlienVault HIDS: USB device added/removed	2017-05-22 14:45:19	Win10-test	0.0.0.0
<input checked="" type="checkbox"/>	AlienVault HIDS: USB device added/removed	2017-05-22 14:44:13	Win7-test	0.0.0.0

Figure 13-1: USB device usage

Basic data leakage detection rules using Alienvault NIDS are included, but are not enabled by default, presumably due to performance concerns. These rules, located in `/etc/suricata/rules/emerging-policy.rules`, are not enabled by default. They can be enabled following instructions in Alienvault’s article “Customizing Alienvault’s NIDS Rules (2017).” Object access auditing using OSSIM is covered in the following section. If configured, object access auditing can also be used to track down the potential source of a data leak.

Kevin Geil, info@friendandfamilytech.com

14. CSC 14: Controlled Access Based on the Need to Know

Because permissions to Active Directory objects and files are routinely granted to groups, it is important to track changes to AD group membership when assessing compliance with CSC 14. This can be accomplished by creating a DS group that contains event types 18128, 18143, and 18144 from data source 7043, and everything from data sources 7099, and 7107. A custom view containing the fields listed below, and shown in Figure 14-1 will show the name of the administrator performing the action, the user account affected, and the group affected:

- Event Name
- Received Event Date
- Extradata Username
- Userdata8
- Userdata 5

<input type="checkbox"/> EVENT NAME	▼ DATE GMT-4:00 ▲	USERNAME	USERDATA8	USERDATA5
<input type="checkbox"/> AlienVault HIDS: Security Enabled Local Group Member Added	2017-05-21 18:01:09	administrator	Account Operators	Account name: Kevin User / Security ID: S-1-5-2-
<input type="checkbox"/> AlienVault HIDS: Security Enabled Local Group Changed	2017-05-21 18:01:09	administrator	Account Operators	Empty
<input type="checkbox"/> AlienVault HIDS: Security Enabled Global Group Member Removed	2017-05-21 18:00:49	administrator	TestSecure	Account name: Kevin User / Security ID: S-1-5-2-
<input type="checkbox"/> AlienVault HIDS: Security Enabled Global Group Changed	2017-05-21 18:00:49	administrator	TestSecure	Empty

Figure 14-1: Group membership changes

In addition to group membership changes, access to sensitive data that is audited using object access control can be monitored using OSSIM. For this demo, object access auditing was set up on C:\temp on the Windows 7 machine. See *Appendix E: Helpful links* for instructions on setting up object access auditing. Creation, editing, and deleting of documents will generate the log events needed for viewing in OSSIM. A DS group consisting of Data Source 7006, with event type IDs of 12009-12012 will show events for file additions, file access, editing, and deletion. A custom view (shown in Figure 14-2) using “Event Name,” “Received event date,” “Extradata Filename,” and “Extradata Username” will show relevant information on object access auditing.

Kevin Geil, info@friendandfamilytech.com

<input type="checkbox"/>	EVENT NAME	▼ DATE GMT-4:00 ▲	FILENAME	USERNAME
<input checked="" type="checkbox"/>	AlienVault HIDS: FIM: Windows file edited	2017-04-18 09:22:04	C:\Temp\FileAccess.txt	kevinadmin
<input checked="" type="checkbox"/>	AlienVault HIDS: FIM: Windows file added	2017-04-18 06:25:52	C:\Temp\Sensitive.txt	kevinadmin
<input checked="" type="checkbox"/>	AlienVault HIDS: FIM: Windows file deleted	2017-04-18 06:24:36	C:\Temp\New Text Document (2).txt	kevinadmin

Figure 14-2: Object access auditing

As figure 14-2 above shows, editing, addition, and deletion of files can be tracked for certain directories, and shows the user making the change.

15. Wireless Access control

OSSIM wireless intrusion detection relies on the use of sensors running Kismet and sending logs into OSSIM. Setting this up is not documented in great detail, and is beyond the scope of this paper. OSSIM does, however, have the capabilities to parse logs from several different enterprise wireless systems. The Aruba-6 test data that was loaded into OSSIM in section eight contains events related to wireless authentication and rogue access point detection. Selecting Aruba-6 as the Data Source, and grouping the events provides suitable information. For example, the event type ID 127037: Aruba Wireless: AP: Station Associated to Rogue AP provides information on the client mac address (userdata1), rogue AP mac address (userdata2), and the SSID (userdata3).

16. CSC 16: Account Monitoring and Control.

Alienvault HIDS provides simple and accurate monitoring of user accounts being enabled, disabled, or locked out. For accounts enabled or disabled, a DS group containing the following event type IDs from Data Source 7043: 18110 (account enabled), 18111 (account changed), and 18112 (account disabled or deleted), will provide information on account management events. After testing by disabling/enabling a user, and changing something like account expiration, a view containing Event name and date, “ExtraData username,” and “userdata8” will show the account affected and the administrator performing the action. For lockouts, event type 18116 from Data source 7012, and event type 18142

Kevin Geil, info@friendandfamilytech.com

from Data Source 7043 using the same view as account management provides details pertinent to these events. Figure 16.1 below shows a sample of this view.

EVENT NAME	▼ DATE GMT-4:00 ▲	USERNAME	USERDATA8
AlienVault HIDS: User account enabled or created.	2017-08-01 14:17:53	kevinadmin	Nadia
AlienVault HIDS: User account enabled or created.	2017-08-01 14:17:53	kevinadmin	Nadia
AlienVault HIDS: User account changed.	2017-08-01 14:17:53	kevinadmin	Nadia
AlienVault HIDS: User account changed.	2017-08-01 14:16:50	kevinadmin	ktester
AlienVault HIDS: User account disabled or deleted.	2017-08-01 14:16:50	kevinadmin	ktester
AlienVault HIDS: User account unlocked.	2017-08-01 14:16:42	kevinadmin	ktester
AlienVault HIDS: User account locked out (multiple login errors).	2017-08-01 14:16:22	ktester	WIN7-1

Figure 16-1: Account Monitoring

The custom view shown in Figure 16-1 will provide the analyst with the action performed, the account affected, and the user performing the action.

17. CSC 19: Incident Response and Management, and CSC 20: Penetration Tests and Red Team Exercises

The skills gained by performing the exercises in this paper provide a foundation on which an effective incident response program can be built. Provided that the right events are being processed by OSSIM, an analyst will be able to track down the moment and method of compromise when it occurs. If a host is under suspicion as being compromised, as shown in Figure 17-1, right clicking on its name in SIEM View provides several options useful for initial incident response. For example, selecting “all events from this host” will provide a wealth of information on the activities surrounding the host in question.

Kevin Geil, info@friendandfamilytech.com



Figure 17-1: Right click options in SIEM View

When the events populate, an analyst will see network connections, FIM events, vulnerabilities, and other useful events for finding the root cause of compromise.

Penetration testing and red team exercises are valuable to analysts of any skill level for learning and improving incident response techniques. For a novice, penetration testing in a demo environment such as the one used in this paper will show the analyst what events are useful for investigation, as well as any blind spots that may exist in logging or packet capture. For the most seasoned analyst, discovering and responding to the activities of an external penetration testing team and then discussing findings with that team at the end of the penetration test is a valuable opportunity for improving incident response capabilities. Demonstrating a penetration test and incident response is beyond the scope of this paper; The “USM Appliance User Guide” provides some detail on using OSSIM for incident response, and multiple helpful links for further research (2017, pp. 57-64).

17. Conclusion:

Perhaps the greatest opportunity gained by assessing compliance with the Critical Security Controls using the techniques presented in this paper is the ability to take snapshots of an organization’s security stance and compare them over time. With each snapshot, analysts can use their findings to improve the organization’s processes. For example, analysts can use the discovery of new assets using the techniques described in CSC 1 as an opportunity to discuss configuration and change management goals for the organization. At the beginning of an organization’s journey through a CSC implementation, the process might be reactive: discussing a discovered asset with colleagues after the fact to find out who the system owner is, and how it is configured.

Kevin Geil, info@friendandfamilytech.com

After several iterations of process improvement, the procedure upon discovery of a new asset might simply involve checking a change request database or asset inventory spreadsheet. Assessment of each security control should be done in this manner, with a goal of improving processes.

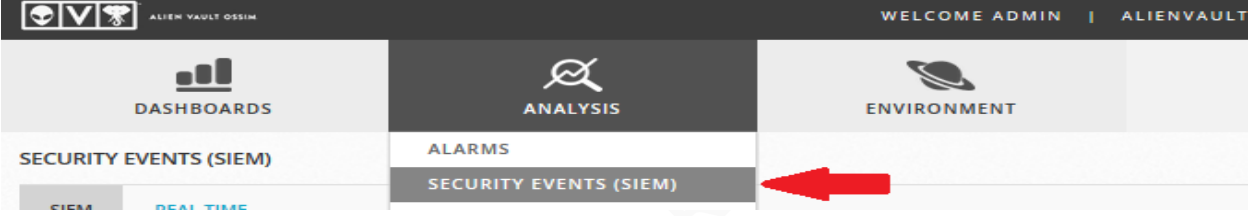
The analysis process itself is an area rich with improvement opportunity. As is the case with most technical endeavors, there are often several approaches to reaching a goal, and OSSIM is no different. Covering every available method for assessing compliance with the Critical Security Controls is well beyond the scope of this paper. Further research on the collection and analysis of events from more devices, or add-on log generators such as “Sysmon” (2017) can provide significant value to OSSIM analysts seeking deep insight into the activity on their networks. Due to the ever-changing nature of computer networks, vulnerabilities, and attacks, opportunities for such research are only limited by the analyst’s imagination and desire to learn, keeping SIEM management a fascinating and rewarding endeavor.

Kevin Geil, info@friendandfamilytech.com

Appendix A: Terms and Abbreviations

Assets	Alienvault/Ossim term for network hosts.
Data source	In Alienvault's documentation, a data source is defined as "External applications whose data are collected and evaluated by a plugin, and translated into an event within the USM taxonomy". (<i>USM Appliance User Guide</i> , 2017, p. 37). What this means when working within the web UI is the aggregate of event types of a particular kind. Example: Data Source 7006 AlienVault HIDS-windows contains most of the events received by HIDS agents installed on Windows clients.
Data Source (DS) Groups	A DS group is a collection of event type IDs. DS groups are very useful for filtering SIEM data, and are critical for efficient analysis. Custom DS groups are essential for efficient analysis
DS Group	Abbreviation for Data Source Group.
Event type:	Sometimes referred to as a "plugin_sid", or simply a "sid", which is the name of its field in the database. Event types have a child relationship to the Data Source. (<i>USM Appliance User Guide</i> , 2017.42, 117) Example: event type ID 18147: Application installed is contained within Data Source 7006 AlienVault HIDS-Windows.
Jailbreak	Logging into OSSIM via ssh or the console presents the user with a menu screen. One of the options is "Jailbreak the system", which, when selected, provides command line access with root privileges to the user.
Normalization	The process of parsing logs into separate fields in a standardized format so that they can be analyzed. An example would be taking multiple types of date formats and converting them into a single format before storing in the database. (<i>USM Appliance Deployment Guide</i> , 2017, p. 160). The risk is also calculated with a normalizing formula

Kevin Geil, info@friendandfamilytech.com

<p>SIEM View:</p>	<p>Navigate to what is called “SIEM View” by selecting Analysis>Security Events (SIEM). SIEM view is where an analyst looks at and filters events. (<i>USM Appliance User Guide</i>. P. 36.)</p> 
<p>Syslog</p>	<p>Originally designed for recording debugging information on UNIX systems, it is commonly used for transmission/reception of log data from network devices. Syslog data from remote hosts is received on TCP/UDP port 514 (Chuvakin, 52).</p>
<p>Web UI:</p>	<p>The browser based user interface for OSSIM.</p>

Kevin Geil, info@friendandfamilytech.com

Appendix B: OSSIM Configuration tasks

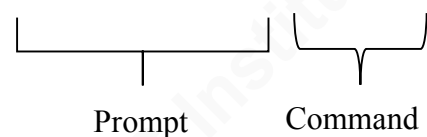
1. Jailbreaking the device

Many of the configuration examples in this document require root level access to the underlying Debian system that runs OSSIM. To do this, connect to the OSSIM machine by either virtual console, or by ssh. When the green welcome screen appears, select 3, read the message (at least for the first time), tab over to select OK, then hit enter.

1.1. Conventions: The following conventions will be used for this guide.

- Invoking commands: The prompt is indicated as: `alienvault:~#`, and the text that follows is the command.

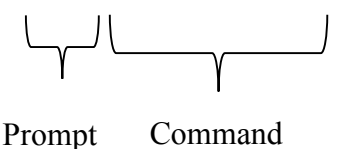
```
alienvault:~# ls -lah
```



Prompt Command

- MYSQL command prompt: Similar to above, the prompt is indicated by `mysql>`, and the text following that is the command.

```
mysql>SHOW TABLES
```



Prompt Command

1.2. Git installation.

In order to follow the instructions below, and to install the demo scripts used in section 7.1, Git will need to be installed. This is done by invoking:

```
alienvault:~# apt-get update && apt-get install git
```

Kevin Geil, info@friendandfamilytech.com

2. New Asset plugin: Installation instructions:

2.1. NOTE: This plugin may not be needed in the near future. A plugin configuration file, `/etc/ossim/agent/plugins/nmap-hosts.cfg`, essentially the same as the plugin described below, is currently included with the product, but the events for this plugin do not appear to be in the database, and the plugin ID (5003) is a duplicate of another plugin currently assigned to “osvdb”. The `nmap-hosts.cfg` file shows a version of 0.0.1, and a last modification date of 2017-01-27. If either of these attributes change, users may want to attempt to use the plugin included with the product instead of the following customization.

2.2. Jailbreak the OSSIM machine (see Appendix B, section 1)

2.3. Obtain the plugin files:

```
alienvault:~# git clone
https://github.com/packetinspector/AlienVault-Plugins
```

2.4. Move `newasset.cfg` into `/etc/ossim/agent/plugins`

```
alienvault:~# mv AlienVault-Plugins/newasset.cfg
/etc/ossim/agent/plugins/
```

2.5. Add plugin ID and SID into database by invoking:

```
alienvault:~# cat newasset.sql | ossim-db
```

2.6. Copy the password from the database section of `/etc/ossim/ossim-setup.conf`. This can be obtained by invoking:

```
alienvault:~# cat /etc/ossim/ossim_setup.conf | grep pass=
```

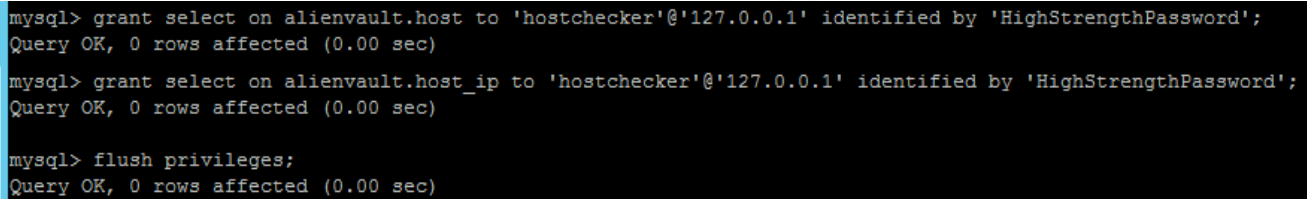
2.7. Enter the mysql context by invoking `alienvault:~#mysql -u root -p`. When prompted for the password, use the password obtained in step 2.5.

2.8. Use the mysql commands that follow to create the user for the plugin, and grant privileges to that user (See figure B-2-1). Any username/password combination will work, but the `newasset.cfg` file must be edited to reflect this (in the `user=` field, and in the `password=` field. Enter the commands as follows (shown in Figure 2-1):

```
mysql>CREATE USER 'hostchecker'@'127.0.0.1' IDENTIFIED BY
'HighStrengthPassword';
```

Kevin Geil, info@friendandfamilytech.com

```
mysql>GRANT SELECT ON alienvault.host to  
'hostchecker'@'127.0.0.1' IDENTIFIED BY  
'HighStrengthPassword';  
mysql>GRANT SELECT ON alienvault.host_ip to  
'hostchecker'@'127.0.0.1' IDENTIFIED BY  
'HighStrengthPassword';  
mysql>flush privileges;
```



```
mysql> grant select on alienvault.host to 'hostchecker'@'127.0.0.1' identified by 'HighStrengthPassword';  
Query OK, 0 rows affected (0.00 sec)  
mysql> grant select on alienvault.host_ip to 'hostchecker'@'127.0.0.1' identified by 'HighStrengthPassword';  
Query OK, 0 rows affected (0.00 sec)  
mysql> flush privileges;  
Query OK, 0 rows affected (0.00 sec)
```

Figure B- 2.1: Grant statements and flush privileges

- A.** Optional: If you want to confirm that the plugin was entered correctly into the database, invoke the commands below. The results should look like Figure B-2.2.

```
mysql>SELECT id, type, name, description, product_type,  
vendor FROM plugin WHERE id=9720;
```

```
mysql> SELECT plugin_id, sid, class_ID, reliability,  
priority, name, subcategory_id, category_id FROM  
plugin_sid WHERE plugin_id=9720;
```

Kevin Geil, info@friendandfamilytech.com

```
mysql> SELECT id, type, name, description, product_type, vendor FROM plugin WHERE id=9720;
+-----+-----+-----+-----+-----+-----+
| id | type | name | description | product_type | vendor |
+-----+-----+-----+-----+-----+-----+
| 9720 | 1 | New_Asset | Custom New_Asset | 10 | New_Asset |
+-----+-----+-----+-----+-----+-----+
1 row in set (0.01 sec)

mysql> SELECT plugin_id, sid, class_id, reliability, priority, name, subcategory_id, category_id FROM plugin_sid WHERE
plugin_id=9720;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| plugin_id | sid | class_id | reliability | priority | name | subcategory_id | category_id |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 9720 | 21 | NULL | 5 | 5 | New_Asset: New asset discovered | 71 | 16 |
| 9720 | 31 | NULL | 1 | 1 | New_Asset: Other Info | 71 | 16 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

Figure B-2.2: Confirming successful SQL statements

2.9. Type exit to get back to the command prompt.

2.10. Edit /etc/ossim/agent/plugins/newasset.cfg to make certain that the username and password match what was entered in the mysql statements in step 3.8. The sleep setting can also be adjusted (default is 300 seconds, I changed it to 60 for the purposes of this demo). This value should be adjusted to accommodate the business goal for detecting new devices on the network (See figure B-2-3 below).

```
source=database
source_type=mysql
source_ip=127.0.0.1
user=hostchecker
password=HighStrengthPassword
db=alienvault
sleep=60
[start_query]
```

Figure B-2.3 Editing newasset.cfg

2.11. Restart the ossim-agent so that the system will recognize the plugin by invoking:
alienvault:~#/etc/init.d/ossim-agent restart

2.12. Log into the web UI by pointing your browser to the OSSIM management IP address. If this is a brand new installation, you'll need to provide a username and password for the admin user.

Kevin Geil, info@friendandfamilytech.com

- 2.13.** Once in the web UI, enable the newasset plugin by going to Configuration/deployment, and clicking the magnifying glass icon on the right hand side of your ossim server. Select Sensor Configuration, then Collection. Scroll down on the right until you see the newasset plugin, then click the + sign next to it, which slides it over to the left (plugins enabled) side, and click apply changes. Your newasset plugin will now generate events whenever an asset is discovered or added to the system. Detailed instructions for enabling plugins are documented in Alienvault's USM appliance deployment guide (2017, 175). Sometimes, if the plugin doesn't seem to be working, disabling and re-enabling it through the ssh menu fixes it.

3. Correlation Directives

The main Windows events used for tracking administrative logons are 4624: Audit Success (An account was successfully logged on), and 4672: "Special privileges assigned to new logon". The 4624 Audit success events are registered every time an account successfully logs on to a computer, and the 4672 event is recorded every time administrator privileges are assigned to a user account after it authenticates. (Smith, 2017) The number of audit success events at first seems extraordinary. This is because a login to a computer involves accessing not just the computer, but negotiating a Kerberos session with the domain controller, accessing the netlogon share (sysvol), reading group policies, logon scripts, several other actions. (Fitzgerald, 2005.). If we just increased the priority of these events, the analyst would be flooded with alarms. Correlation directives are effective at limiting the number of alarms by matching criteria for multiple events. The first directive described below will generate an alarm for a 4624 authentication success event followed by a 4672 "Special privileges" event within 10 seconds, allowing analysts to focus on administrative activity without getting an alarm for every authentication event. The second directive below will generate alarms when an account with the username of Administrator is used to log in, so that use of generic accounts can be curtailed.

3.1. Correlation Directive: administrator login (Any administrative account):

Kevin Geil, info@friendandfamilytech.com

Navigate to Configuration>Threat Intelligence>Directives, Click New Directive, and in the box that pops up, enter the text as shown in Figure B-3.1:

- A. Name for the Directive: Administrator login
- B. Intent: Environmental Awareness
- C. Strategy: Suspicious Behavior
- D. Method: Administrative Login
- E. Set Priority to 3 (default)
- F. Click Next

Figure B-3.1 Correlation Directive first

- G. The next window refers to the first rule being created. Under “Name for the rule”, enter “Administrator Login”, and click Next.
- H. For Event types: type alienvault hids-authentication in the search box, and click Alienvault Hids-Authentication Success in the filtered results (See figure B-3-2).

Figure B-3.2

In the Plugin signatures section, type 18107 in the search box, and click the + sign next to Alienvault Hids: Windows Logon Success to add it to the plugin signature (see figure B- Kevin Geil, info@friendandfamilytech.com

3-3). Click Next.

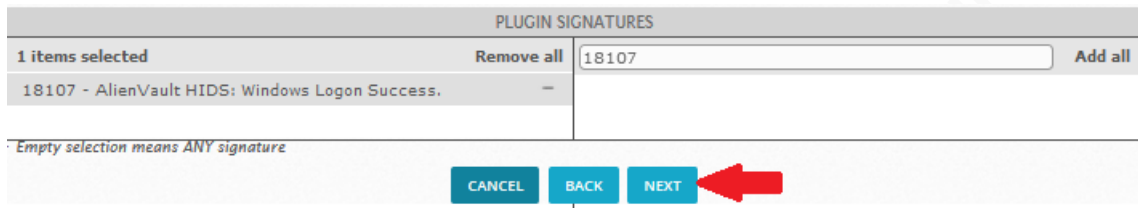


Figure B-3.3 Signature Selection

I. Click next again in the Network section (see figure B-3.4).

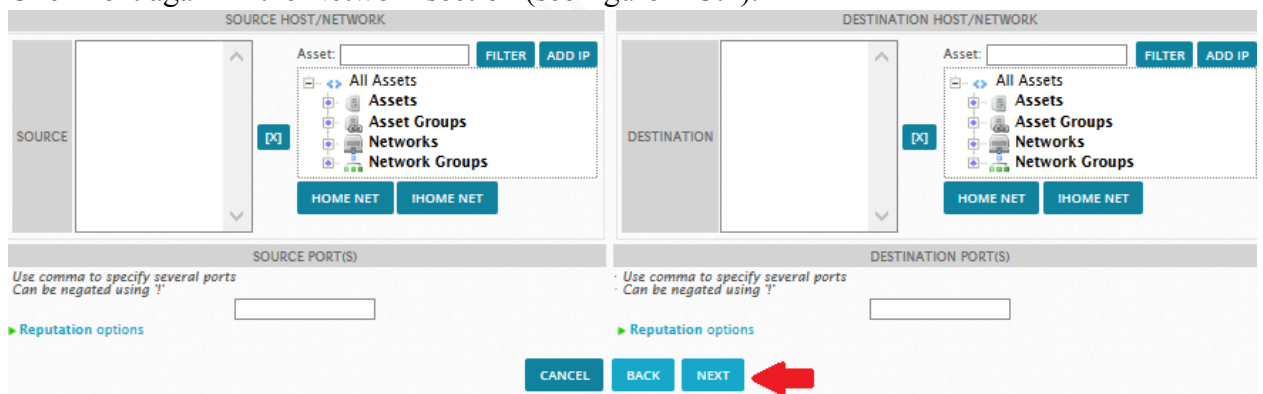


Figure B-3.4 Network Selection. Blank entries default to “any”.

J. The next window refers to the reliability of the directive. Select a reliability of 4, and click “Finish”.

K. Click the + sign under the Action portion of the rule, which will show the tooltip popup: “Create a rule inside (Level 2)”. See Figure B-3.5 for details

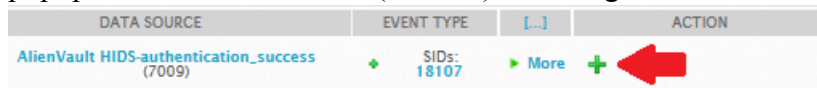


Figure B-3.5 Creating second rule

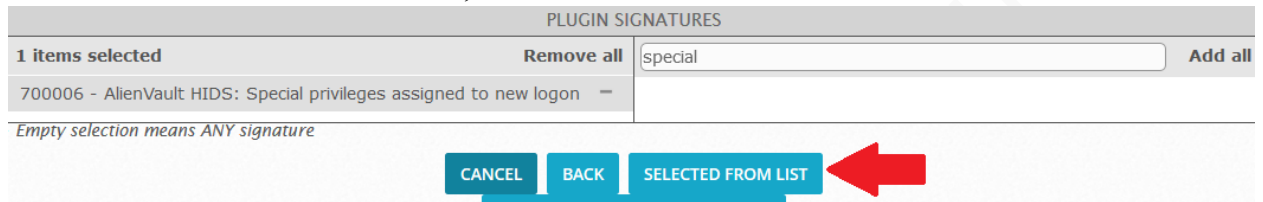
L. It’s OK here to give the rule the same name as the first, so, Name the Rule “Administrator Login” again, and click next.

M. In the Event Types dialog box, select Alienvault HIDS-Authentication_Success, as shown above in Figure B-3.2.

N. In the Plugin Signatures dialog box, type “special” in the search bar, and click the + sign next to 700006-AlienVault HIDS: Special privileges assigned to new... to move it

Kevin Geil, info@friendandfamilytech.com

over to the left hand side of the box, and click “Selected From List” at the bottom.



- O. Network Dialog Box: For the asset, leave the source host/network selection blank, and on the Destination Host/Network, click the dropdown “From a parent rule:”, and select “Destination IP from Level 1”, as shown in Figure B-3-6, and click Next.

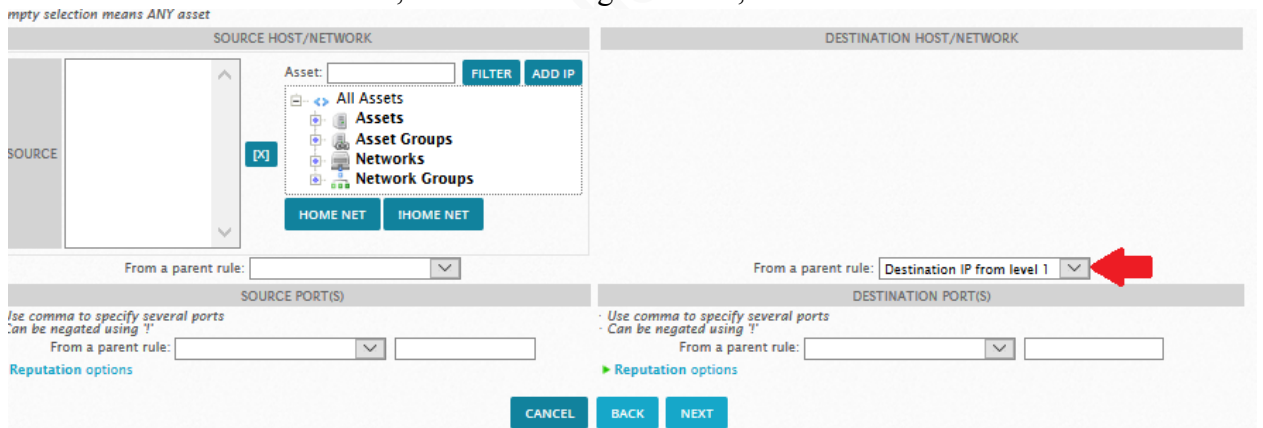


Figure B-3.6 Network dialog box

- P. Select a reliability of 5, and click Next, next again for the protocol selection and sensor selection, and for occurrence, select 1, which will bring you to the timeout selection. Click 10, which brings you to the Sticky Different selection, Click None. In the “Other” dialog box, enter 1:USERNAME in the username box, as shown in Figure B-3.7, click Next, and Finish.

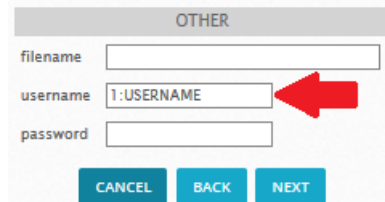


Figure B-3.7 Username selection

- Q. Click the button for “Reload Directives”, which will have turned red for you after adding a new directive (Figure B-3.8).

Kevin Geil, info@friendandfamilytech.com

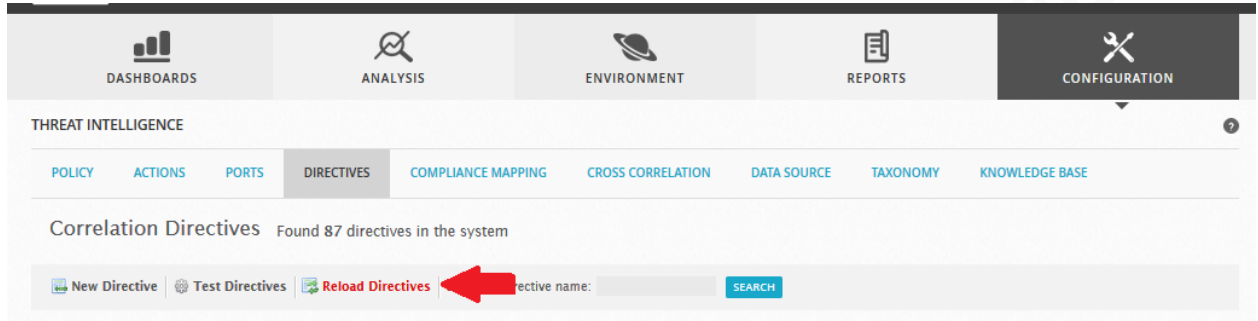


Figure B-3.8 Reloading directives

An alarm will now be generated if an account with administrative privileges logs into a client machine.

4. Correlation Directive: administrator login (Generic account with username 'administrator'):

The procedure is similar to the one above, but the username parameter will be used.

Navigate to Configuration>Threat Intelligence>Directives, Click New Directive, and in the box that pops up, enter the following, shown in Figure B-4.1:

- A. Name for the Directive: GenericAdministrator login
- B. Intent: Environmental Awareness
- C. Strategy: Default Credentials
- D. Method: Username:Administrator
- E. Set Priority to 3 (default)
- F. Click Next

The screenshot shows a dialog box titled 'NAME FOR THE DIRECTIVE'. It has several sections:

- NAME FOR THE DIRECTIVE:** A text input field containing 'Generic Administrator login' with a red 'A.' to its right.
- TAXONOMY:**
 - Intent:** A dropdown menu set to 'Environmental Awareness' with a red 'B.' to its right.
 - Strategy:** A dropdown menu set to 'Default Credentials' with a red 'C.' to its right.
 - Method:** A text input field containing 'Username: Administrator' with a red 'D.' to its right.
- PRIORITY:** A vertical list of buttons numbered 0 through 5. The button for '3' is highlighted in a darker blue and has a red 'E.' to its right.
- At the bottom, there are two buttons: 'CANCEL' and 'NEXT'. The 'NEXT' button has a red 'F.' to its right.

Figure B-4.1: Directive first options

Kevin Geil, info@friendandfamilytech.com

- G. The next window refers to the first rule being created. Under “Name for the rule”, enter “Generic Administrator Login”, and click Next.
- H. For Event types: type alienvault hids-authentication, and click Alienvault Hids-Authentication Success in the filtered results (shown in Figure B-4.2).

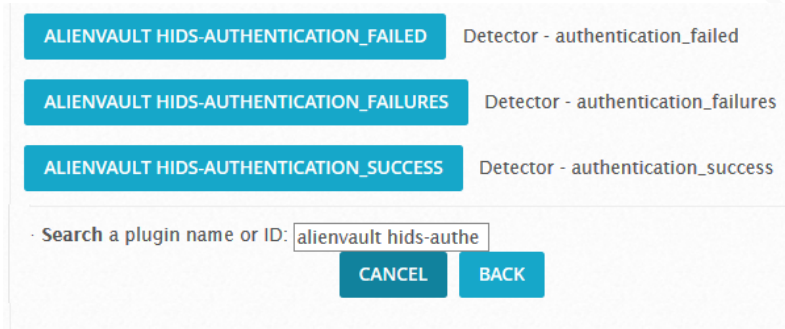


Figure B-4.2: Selecting event type

- I. In the Plugin signatures section, type 18107 in the search box, and click the + sign next to Alienvault Hids: Windows Logon Success (as shown in Figure B-4.3) to add it to the plugin signature. Click Next.

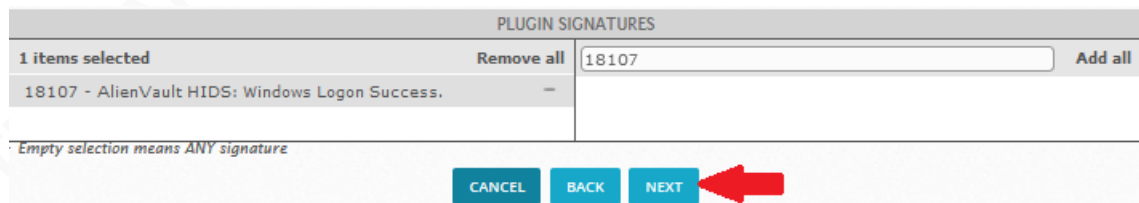


Figure B-4.3: Selecting Plugin Signature

- J. Click next again in the Network section. Leaving the selections blank defaults to “any” (Shown in Figure B-4.4).

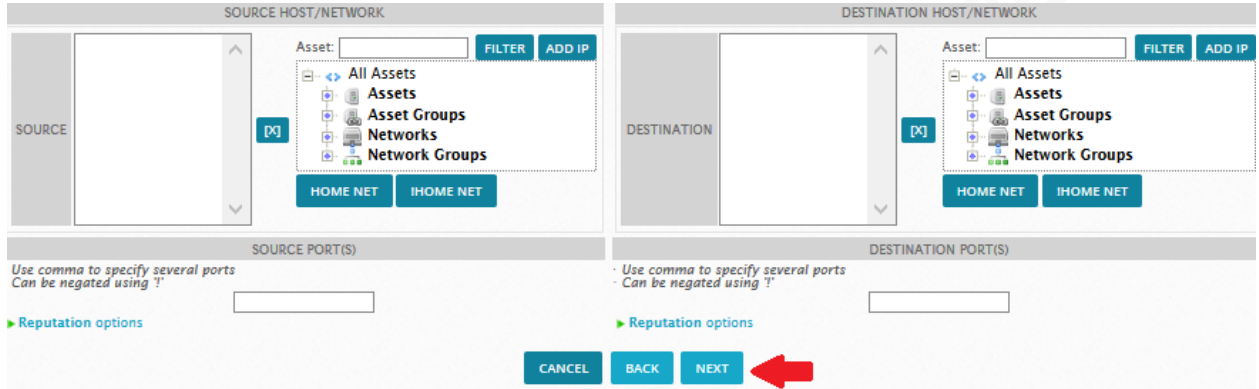


Figure B-4.4 Network Selection

- K. Select a reliability of 4, and click Next, then “Finish”
- L. The new directive will be displayed at the bottom of the “User Contributed” section.
- M. Click the dropdown next to the “Rules” section. See Figure B-4.5 for steps M-O.
- N. Click the dropdown that is now visible next to the word “More” on the right hand side.
- O. Under “Username”, click in the “click to edit” field, and enter “Administrator”, and click OK.

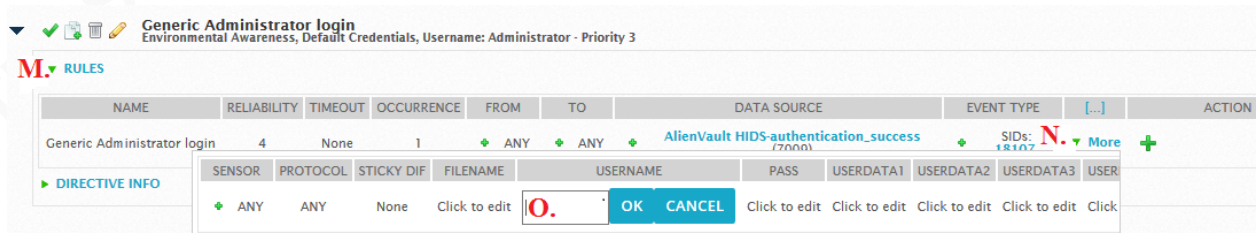


Figure B-4-5: Username selection

- P. Click “Reload Directives” at the top of the screen (see figure 4-8). An alarm will now be generated if the account with the username “Administrator” logs into one of your clients. Of course, this can be done for any username desired.

Kevin Geil, info@friendandfamilytech.com

Appendix C: Environment and host configuration

- **DNS reverse lookup zone and DHCP registration configuration:**
[https://technet.microsoft.com/en-us/library/cc725670\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc725670(v=ws.10).aspx)
- DHCP Server Configuration:
<https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>
- Configure DHCP Server to register host in DNS:
 - Create new AD user in your domain, and add it to the DHCP Administrators group in AD.
 - Open Dhcp Management (start/run dhcpmgmt.msc), and add the credentials:
 - right click IPv4, click the advanced tab, and next to DNS dynamic update registration credentials, click “Credentials”, and enter the appropriate information. Details can be found here: [https://technet.microsoft.com/en-us/library/ee941181\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/ee941181(v=ws.10).aspx)
- Invoke ipconfig /release && ipconfig /renew on any dhcp clients, and their names will get registered in the reverse lookup zone, thus making the FQDN available to OSSIM’s asset scanner.

Applocker configuration:

- Create new GPO called Applocker.
 - Enable Application Identity service under Computer Configuration>Policies>Windows Settings>Security Settings>System Services. Check the box to “define this policy setting”, and set the service startup mode to “automatic”
 - Configure AppLocker: Computer Configuration>Policies>Windows Settings>Security Settings>Application Control Policies>Select AppLocker, Click “Configure Rule Enforcement” For each one, check the box for “Configured”, then the dropdown for “Audit Only”, and click “OK”.

Kevin Geil, info@friendandfamilytech.com

- Right click “Executable Rules”, and click “Create new Rule”.
 - Click “Next” in the “Before You Begin” section, and next again in the Permissions section (keeping the radio button on Allow, and User or group: Everyone).
 - In the “Conditions” section, select “Path”, and click next.
 - In the “Path section, enter %WINDIR% in the box, and click next.
 - Click “Next” again in the Exceptions section.
 - Give the rule an appropriate name and description, and click “Create”.
 - Decline the offer to “Create default Rules”.
 - Repeat Step 4, using %PROGRAMFILES% for the path variable.
 - Repeat step 4, but for step 4.a, select “deny”, and populate the path in 4.c with C:\Temp
-
- Apply the group policy to the appropriate OU in Active Directory Users and computers (in my case, it is ViaMonstra/Workstations).
 - Invoke gpupdate /force at a command prompt on the clients.
 - Either reboot, or start the Application Identity service on the host to be tested.

Appendix D: Helpful links

OSSIM Installation instructions:

<http://linoxide.com/security/install-configure-alienvault-siem-ossim/>

Best Practices for Configuring your OSSIM Installation webinar:

<https://www.alienvault.com/resource-center/webcasts/ossim-training-best-practices-for-configuring-your-ossim-installation>

OSSEC Documentation:

<https://ossec.github.io/docs/>

Snort Documentation:

<https://www.snort.org/documents#OfficialDocumentation>

Suricata Documentation:

<https://suricata-ids.org/docs/>

Object Access Auditing Instructions:

[https://technet.microsoft.com/en-us/library/cc771070\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771070(v=ws.11).aspx)

Raw Logger option for OSSIM users:

<https://www.alienvault.com/forums/discussion/1206/raw-logger-replacement-for-us-opensource-folks-logstash-kibana-elasticsearch/p1>

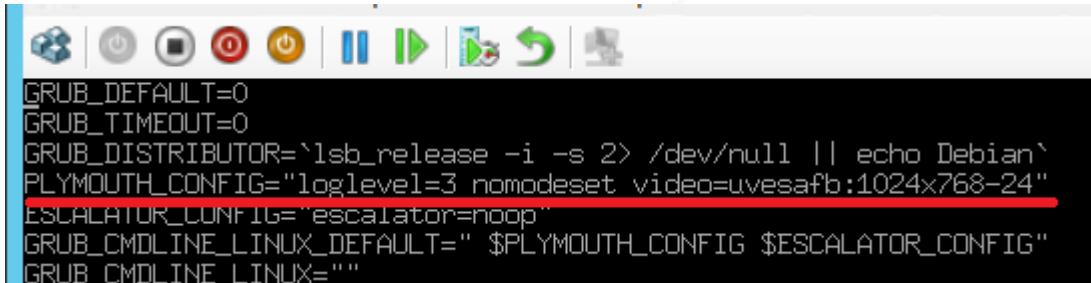
Wireless IDS documentation for OSSIM/Alienvault:

<https://www.alienvault.com/documentation/usm-appliance/kb/2016/04/wids-modifying-kismet-scripts-to-work-with-kismet-2008-and-kismet-2013.htm>

Kevin Geil, info@friendandfamilytech.com

Appendix E: General tips for navigating within OSSIM and moving files between hosts:

1. After installing OSSIM, video may not display on the VM console. To fix this, SSH into the OSSIM machine, and edit `/etc/default/grub`
Change: `PLYMOUTH_CONFIG="loglevel=3 splash vga=792"` to:
`PLYMOUTH_CONFIG="loglevel=3 nomodeset video=uvesafb:1024x768-24"`

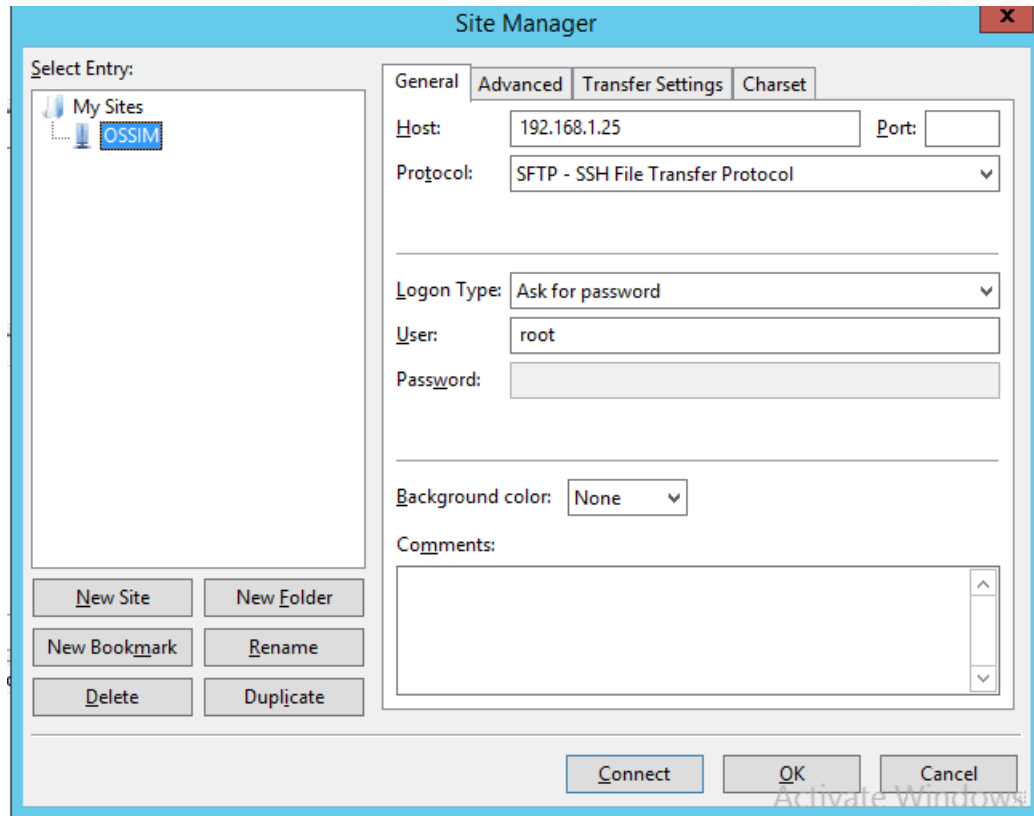


```
GRUB_DEFAULT=0
GRUB_TIMEOUT=0
GRUB_DISTRIBUTOR=`lsb_release -i -s 2> /dev/null || echo Debian`
PLYMOUTH_CONFIG="loglevel=3 nomodeset video=uvesafb:1024x768-24"
ESCALATOR_CONFIG="escalator=noop"
GRUB_CMDLINE_LINUX_DEFAULT=" $PLYMOUTH_CONFIG $ESCALATOR_CONFIG"
GRUB_CMDLINE_LINUX=""
```

Then invoke: `alienvault:/etc/default# update-grub`
 (AGWorksAlien, 2017)

2. **Copying files between Windows and Linux using Filezilla and SFTP:**
 - A. Open Filezilla, click File/Site Manager, then New Site
 - B. In the host field, enter the IP of your OSSIM box.
 - C. In the Protocol field: Select SFTP – SSH File Transfer Protocol
 - D. In the Logon Type field, select Ask for password (in a production environment, using keyfiles is recommended).
 - E. For User, type in root
 - F. Click connect, and you will have access to move files using the filezilla window.

Kevin Geil, info@friendandfamilytech.com



G.

3. Troubleshooting:

A. MYSQL Query logging:

Edit `/etc/mysql/my.cnf`

Add line under `#general_log=On` to read:

```
general_log=1
```

Restart the mysql service by invoking:

```
#!/etc/init.d/mysql restart
```

Queries will then be logged to the location specified in `my.cnf` (Default path is usually: `/var/log/mysql/mysql.log`).

B. Changing verbosity on agent.log:

1. Edit `/etc/ossim/agent/config.cfg` so that the line `verbose=info` reads `verbose=debug`.

Kevin Geil, info@friendandfamilytech.com

2. Take note of the location of the log file. The default location for agent.log is /var/log/alienvault/agent/agent.log.
3. Restart the OSSIM agent by invoking:
#/etc/init.d/ossim-agent restart

```
[log]
error=/var/log/alienvault/agent/agent_error.log
file=/var/log/alienvault/agent/agent.log
stats=/var/log/alienvault/agent/agent_stats.log
verbose=info
```

Kevin Geil, info@friendandfamilytech.com

References

- AgWorksAlien (online alias). (November 20, 2015). VGA Console unreadable. Message posted to <https://www.alienvault.com/forums/discussion/comment/17888/>
- Alienvault USM Appliance Plugins List. Retrieved July 30, 2017, from <https://www.alienvault.com/docs/data-sheets/usm-plugins-list.pdf>
- Apply or modify auditing policy settings for a local file or folder. (2017). Retrieved March 10, 2017, from [https://technet.microsoft.com/en-us/library/cc771070\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771070(v=ws.11).aspx)
- AuditScripts Critical Security Controls Master Mapping, 2016. Retrieved March 22, 2017, from <http://www.auditscripts.com/download/2742/>
- Bassett, Santiago. Alienvault Demo Scripts. Retrieved July 3, 2017 from https://github.com/santiago-bassett/Alienvault-Demo_scripts
- Castra Consulting: Personal conversations July 2015-July 2016. <https://castraconsulting.com/>
- Coe, Kenneth. Alienvault Employee. Personal Communication July 21, 2017.
- The CIS Critical Security Controls for Effective Cyber Defense Version 6.1. Retrieved June 30, 2017, from <https://learn.cisecurity.org/20-controls-download>
- CIS Microsoft Windows Server 2012R2 v.1.10, 11-4-2014. Retrieved March 22, 2017, from https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v1.1.0.pdf
- Compare Alienvault Products. Retrieved May 1, 2017, from <https://www.alienvault.com/products/compare-ossim-to-alienvault-usm>
- Customizing Alienvault Nids Rules. Retrieved June 30, 2017, from <https://www.alienvault.com/documentation/usm-appliance/ids-configuration/customizing-alienvault-nids-rules.htm>
- Emerging Threats FAQ. Retrieved July 31, 2017, from http://docs.emergingthreats.net/bin/view/Main/EmergingFAQ#What_is_Emerging_Threats
- Fitzgerald, E. Deciphering Account Logon Events. Retrieved June 10, 2017 from msdn.microsoft.com, <https://blogs.msdn.microsoft.com/ericfitz/2005/08/04/deciphering-account-logon-events/>.

Kevin Geil, info@friendandfamilytech.com

Hoffman, C. How to Change your Browser's User Agent Without Installing Any Extensions. (2016, October 9). Retrieved March 24, 2017, from <https://www.howtogeek.com/113439/how-to-change-your-browsers-user-agent-without-installing-any-extensions/>

Hydration Kit for System Center 2012R2 is available for download. (2014). Retrieved March 24, 2017, from <http://deploymentresearch.com/Research/Post/407/The-Hydration-Kit-for-System-Center-2012-R2-is-available-for-download>

IP Reputation Explained. (2017). Retrieved July 31, 2017 from <https://www.alienvault.com/documentation/usm-appliance/kb/2015/05/ip-reputation-explained.htm>

Lich, Brian. (2017, April). Requirements to Use Applocker. Retrieved March 10, 2017, from <https://docs.microsoft.com/en-us/windows/device-security/applocker/requirements-to-use-applocker>

Mapping and Compliance. (2017). Retrieved March 10, 2017, from <https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/>

PacketInspector (online alias). (January 4, 2014). Make an Event for a new Asset. Message posted to <https://www.alienvault.com/forums/discussion/2177/>

Smith, R.F., (n.d.). Windows Security Log Event ID 4672. Retrieved March 10, 2017, from Ultimate Windows Security.com, <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4624>

Smith, R.F., (n.d.). Windows Security Log Event ID 4672. Retrieved March 10, 2017, from Ultimate Windows Security.com, <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4672>

Syscheck. Retrieved March 10, 2017, from <http://ossec-docs.readthedocs.io/en/latest/manual/syscheck/>

Sysmon. Retrieved May 24, 2017, from <https://technet.microsoft.com/en-us/sysinternals/sysmon>

The Center For Internet Security Critical Security Controls for Effective Cyber Defense, Version 6.1. (31, August, 2016). Retrieved March 23, 2017, from <https://learn.cisecurity.org/20-controls-download>

Kevin Geil, info@friendandfamilytech.com

USM Appliance Deployment Guide. San Mateo, California: Alienvault, 2017. 27 June.
Retrieved from <https://www.alienvault.com/documentation/resources/pdf/usm-appliance-deployment-guide.pdf>

USM Appliance User Guide. San Mateo, California: Alienvault, 2017. 27 June. Retrieved From
<https://www.alienvault.com/documentation/resources/pdf/usm-appliance-user-guide.pdf>

What are the differences in the rule sets?. Retrieved March 24, 2017, from
<https://www.snort.org/faq/what-are-the-differences-in-the-rule-sets>.

Welcome to AlienVault Open Threat Exchange!. Retrieved June 1, 2017, from
<https://www.alienvault.com/open-threat-exchange>

Kevin Geil, info@friendandfamilytech.com