ISE6100 GIAC Enterprises
Final Step By Step
Description
GIAC Enterprise SIEM Implementation Project

ISE 6100 – Security Project Practicum – Step By Step Solution Description

Authors: Alyssa Robinson, lyssanr@yahoo.com
        David Fletcher, 6fletch9@gmail.com
        Wes Whitteker, wes_whitt@yahoo.com
        Advisor: Toby Gouker & Chris Crowley
        Accepted: April 27th 2016

Abstract

GIAC Enterprises, a small to medium size business, has grown to a point where their current manual log analysis process is no longer efficient or effective. As such, GIAC Enterprises was forced to look for a SIEM solution that automates the correlation and analysis of system logs. GIAC Enterprises had a significant financial constraint, which required them to focus their investigation on several open source solution options. After investigation, GIAC Enterprises settled on AlienVault’s OSSIM product for their solution. The result of this research is the following OSSIM implementation guide.
1. Introduction

GIAC Enterprises is a small to medium-sized growing business. To support their growing business, GIAC Enterprises has recently gone through significant infrastructure expansion, adding a second datacenter for business continuity efforts. The combination of an expanding web infrastructure, multiple datacenters, and corporate headquarters has created a situation where the volume of logs generated from this infrastructure can no longer be monitored manually by their security staff.

This inability has directly impacted GIAC Enterprises Incident Response capabilities, which has undermined the strength of their overall security posture. Thus, the GIAC Enterprises security analysts have investigated options for automating the analysis of logs through the use of a Security Information and Event Management (SIEM) solution. After choosing AlienVault’s Open Source SIEM (OSSIM) solution, the GIAC Enterprises security analysts developed a pilot implementation of OSSIM. What follows is a description of the SIEM selection process and a step-by-step description of its implementation.

2. GIAC Enterprises Solution

2.1. GIAC Enterprises Environment

GIAC Enterprises is the largest supplier of Fortune Cookie sayings in the world. They have a central business and IT organization, two data center locations, and a contracted (1099) mobile work force. GIAC Enterprises consists of approximately 1,000 employees with 200 people in central business and IT. The primary platform used internally at GIAC Enterprises for desktops and servers is Microsoft Windows. The two datacenters house the fortune cookie sayings and are configured to support disaster recovery.

GIAC Enterprises has a large number of individual contractors that submit fortune cookie sayings via a mobile application. The mobile application allows the contractors to upload the new sayings via a representational state transfer (REST) API hosted on a farm of Apache web servers, which communicate to a MySQL backend. The web servers are
fron by HAproxy load balancers and web application firewalls (WAFs), which provide high availability and an additional layer of security. Below is an architecture diagram showing an overview of the log sources within GIAC Enterprises.

![Architecture Diagram](image)

**Figure 1: GIAC Enterprises Architecture and Log Source Diagram**

### 2.2. SIEM Overview

SIEM technology allows companies to store, correlate and analyze security events. The events are primarily correlated from normalized log data, but can also come from other sources such as Netflow data, threat and vulnerability information, and asset databases or user data (Kavanagh & Rochford, 2016). Processing and correlating this information allows SIEM systems to determine which events are significant and alert on suspected issues in near real-time (Jaquith, 2007). In addition to alerting, SIEM systems allow for reporting and searching of historical data for compliance and/or incident response (Kavanagh & Rochford, 2016).

### 2.3. Commercial vs. Open Source

Commercial SIEM products offer robust features, including support for processing diverse log and event sources, regularly-updated threat and alert signature data, and reports for compliance with multiple standards (Scarfone, 2015). These
commercial products can also scale to support environments with up to 25,000 events per second, but can come with price tags of hundreds of thousands of dollars (Kavanagh & Rochford, 2016). Considering the high costs of most commercial SIEM solutions, there is incentive for organizations to look for lower cost alternatives through open source software (OSS) solutions. However, as with many OSS solutions, the reduced costs will often come with reduced support, a lack of specific features, or a degradation in performance or functionality. All of these factors were considered when assessing solutions for use within the GIAC Enterprises environment.

2.4. Selection Scoping

The primary constraint for GIAC Enterprise’s solution selection was product cost, which immediately eliminated all worthy commercial solutions. After elimination of commercial options, the security analysts narrowed their scope of selection to OSS solutions that focused on the correlation of log data, with mature reporting and alerting capabilities. Additionally, the analysts considered OSS solutions that had active development and support communities; the ability to ingest data from multiple sources; and the ability to scale with the organization.

After considering multiple options that could support the logging, reporting, and scalability desired, AlienVault’s OSSIM OSS solution rose above the rest. OSSIM was the best solution for an Open Source SIEM that could meet both GIAC Enterprise’s immediate and long-term needs. OSSIM has been in existence for several years and has a very active support community. In addition, OSSIM has external add-on support as well as the option to upgrade to AlienVault’s commercial SIEM, Unified Security Management (USM), if paid support or advanced features like external user authentication, automated update, or distributed deployments are needed in the future.

Further, unlike log-only solutions such as Graylog and Enterprise Log Search and Archive (ELSA), OSSIM has built-in correlation with threat feeds as well as network and host-based IDS data that will allow GIAC Enterprises to integrate and correlate more event data sources in the future. These expansive capabilities of OSSIM will allow GIAC Enterprises the ability to gain a deeper understanding of security risks and events in their environment. One feature that is lacking in OSSIM is long-term log storage and
correlation, but some promising work has been done to integrate an Elasticsearch, Logstash, Kibana (ELK) based logging system with OSSIM to extend its log archiving capabilities (Vassallo, 2015). The feature matrix that was used during the selection of OSSIM as the final solution can be found in the appropriate section of the appendix.

3. OSSIM Pilot Environment

3.1. OSSIM Architecture

OSSIM has two primary architectural pieces known as the sensor node (or simply the “sensor”) and control node (or simply the “server”). Essentially, the sensor does all the data collection, and the server does the data correlation and analysis. The commercial version of OSSIM, USM, has a third component called the logger, which is used for long term log storage. The lack of the logger is the key technical differentiator between OSSIM and USM (AlienVault, 2016). It’s important to note that because the products are so similar, AlienVault only publishes documentation related to USM and recommends the use of this documentation when setting up an OSSIM instance.

Since GIAC Enterprises used OSSIM for their pilot, only the sensor and server components were implemented. These components can be deployed as an all-in-one instance or on separate hardware. For the GIAC Enterprises pilot, a simple all-in-one deployment was used, which is represented in the architecture diagram in the previous section. OSSIM accomplishes its tasks through a collection of several open source security tools whose major functionalities include SIEM, Asset Discovery, Vulnerability Assessment, Threat Detection, and Behavioral Monitoring. The image below provides a graphical representation of this functionality:
For the GIAC Enterprises pilot, the SIEM, asset discovery, threat detection, vulnerability assessment, and log collection functions were tested. The primary open source security tools that are used within each OSSIM functional group include the following:

**Asset Discovery**: Nmap & Prads

**Behavioral Monitoring**: Netflow, Ntop, Nagios

**Threat Detection**: Snort, Suricata, OSSEC

**Vulnerability Assessment**: OpenVAS

**External Log Collectors**: syslog (rsyslog), WMI, SDEE (AlienVault, n.d. a)

### 3.2. Ports, Protocols, and Services

Below is a listing of the ports, protocols, and services used by OSSIM for both internal and external connections. The intent of this information is to understand the firewall rules that need to be created in order to enable certain features of the OSSIM instance. The GIAC Enterprises pilot environment was an all-in-one deployment, which eliminates the need to open any firewall port ports between the OSSIM sensor and server. As a reminder, AlienVault recommends the use of USM documentation for OSSIM deployments. As such, the references to “USM” below should be used for OSSIM.

<table>
<thead>
<tr>
<th>Target</th>
<th>Port (TCP)</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>data.alienvault.com</td>
<td>80</td>
<td>AlienVault product and feed update</td>
</tr>
<tr>
<td>maps-api-ssl.google.com</td>
<td>443</td>
<td>Asset Location</td>
</tr>
<tr>
<td>messages.alienvault.com</td>
<td>443</td>
<td>Message Center</td>
</tr>
<tr>
<td>support.alienvault.com</td>
<td>20, 21</td>
<td>AlienVault Doctor</td>
</tr>
<tr>
<td>telemetry.alienvault.com</td>
<td>443</td>
<td>Telemetry Data Collection</td>
</tr>
</tbody>
</table>
3.3. OSSIM Image Installation

In order to install the OSSIM software, the first step is to download the latest ISO image from the AlienVault website (AlienVault, 2016). Once the ISO has been obtained, a new virtual machine must be built for each component (control and sensor node). The OSSIM pilot environment was built within an Amazon Web Services (AWS) instance. However, there is no pre-built OSSIM instance for AWS so the initial image was built in a third-party virtualization platform first and then converted to an Amazon Machine Image (AMI) from that platform. AMI conversion is available for a number of virtualization platforms. Guidance on converting virtualization formats can be found at the following URL: https://aws.amazon.com/ec2/vm-import/.

While reviewing the USM installation material, a link to “AlienVault USM for AWS” documentation was found (AlienVault, n.d. c). This documentation identifies USM availability for AWS and recommends baseline standards for USM deployment within the AWS environment. These recommendations served as a guide for deployment of OSSIM within the pilot OSSIM AWS environment. The recommendations in the AWS documentation are as follows:

<table>
<thead>
<tr>
<th>Node</th>
<th>Processor Cores</th>
<th>RAM</th>
<th>Disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>2</td>
<td>15 GB</td>
<td>256 GB</td>
</tr>
</tbody>
</table>
Due to local hardware limitations (16 GB of physical RAM available) the VMware instance was built with 8 GB of RAM. The Control node was assigned 2 virtual cores and 64 GB of hard disk space. The sensor node had the same characteristics with 32 GB of hard disk space. Once the image was built locally, it was uploaded and installed in the AWS environment. The technical details of how to execute the image build and AWS upload can be found in the associated section in the appendix.

3.4. Network Configuration and Asset Discovery

After initially installing the OSSIM sensor, one of the first activities that should be accomplished is configuration of the networks that OSSIM will be monitoring. Configuring networks informs the sensor of what networks to monitor and also enables automated asset discovery scanning. With automated asset scanning, the sensor is capable of notifying security analysts whenever a new asset appears on one of the monitored networks. This capability aligns with Critical Security Control 1 (Inventory of Authorized and Unauthorized Devices), which increases security awareness by explicitly identifying the devices that are authorized on each of the target networks (CIS, n.d.).

The first step in preparing for this configuration is to identify the networks that the OSSIM sensor will be monitoring. GIAC Enterprises has resources on two subnets which are used to process fortunes. The first segment is a DMZ network which contains the web server that processes incoming fortunes and the mobile device management solution. The fortunes that are collected by the web server are then sent to a back-end MySQL database that resides on an internal segment along with Windows servers that provide authentication services. The external network is a special network used for monitoring malicious activity and any networks that do not fit into the DMZ or internal network categories. The details for these networks can be seen in the table below.

<table>
<thead>
<tr>
<th>Name</th>
<th>CIDR</th>
<th>Asset Value</th>
<th>External?</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIAC Enterprises DMZ</td>
<td>192.168.0.0/24</td>
<td>3</td>
<td>No</td>
<td>GIAC Enterprises</td>
</tr>
<tr>
<td>GIAC Enterprises Internal</td>
<td>192.168.2.0/24</td>
<td>4</td>
<td>No</td>
<td>GIAC Enterprises</td>
</tr>
<tr>
<td>External</td>
<td>TBD</td>
<td>2</td>
<td>Yes</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Figure 6: GIAC Enterprises OSSIM Sensor Monitored Networks
The asset value identifies the relative value of the assets that reside within this network segment. When OSSIM calculates risk associated with a given resource this value is one of the parameters used in the multiplicative calculation. The scale for value is 1-5 with 1 being the least valuable, 5 being the most valuable, and 2 being the default value for a network. The external parameter identifies the resource as belonging to the organization or not. The owner field is simple text that allows easy reference for identifying the purpose of a network resource. Additionally, the OSSIM sensor can be configured to monitor potential attackers. The attacking device or network must be configured as another monitored network, similar to what would be done for a legitimate network. The one exception is that the network or resource must be marked as external using the OSSIM interface. The technical details of the GIAC Enterprises network and asset discovery configuration can be found in the applicable section of the appendix.

4. Deploying HIDS Agents

As noted in the sections above, OSSIM has integrated Open Source HIDS SECurity (OSSEC) for endpoint security functions. The OSSEC project has been managed by Trend Micro since 2009, with commitment to keep the project as open source software. The project homepage can be found at the location: http://ossec.github.io/. The official description of OSSEC is as follows:

OSSEC is a scalable, multi-platform, open source Host-based Intrusion Detection System (HIDS). It has a powerful correlation and analysis engine, integrating log analysis, file integrity checking, Windows registry monitoring, centralized policy enforcement, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows. (OSSEC, n.d.)

The AlienVault HIDS architecture uses a server and agent model for data collection. The agent runs on the monitored endpoints while the server component runs as part of the OSSIM sensor. A graphical depiction of this communication can be seen in the architecture diagram below:
The agent doesn’t do any data correlation. All data collected by the agents is sent by the agents’ agentd daemon to the OSSIM sensor on UDP port 1514 for normalization. Agents use pre-shared keys to authenticate themselves with the OSSIM sensor. The sensor then hands the normalized data to the OSSIM server component for analysis and correlation (AlienVault, Inc., n.d. d). This communication is depicted in the architecture diagram below:
It’s important to note that the HIDS agents do not provide the OSSIM with raw logs from its monitored hosts. If raw logs are needed, a separate logging capability must be configured. Collecting raw logs is described in the logging section below. Additionally, OSSEC has the ability to collect data without using an agent through either syslog or WMI-based configurations (OSSEC, n.d. a). Though the GIAC Enterprises pilot environment’s primary goal was to automate the analysis of logs, the security team felt that the additional context provided by the HIDS functionality would aid the overall quality of the automated analysis through cross-correlation.

### 4.1. HIDS (Windows Hosts)

Before deploying the HIDS agent to Windows systems from the OSSIM console, the following ports must be opened from the console in the Windows firewall and/or network access controls lists or security groups: TCP 139 and TCP 445. TCP and UDP 1514 also need to be open from the agent systems to the OSSIM agent (AlienVault, Inc., n.d. f). For any systems not on an Active Directory domain, User Account Control features need to be deployed during install. Additionally, the correct group policy security settings must be set (see [https://www.alienvault.com/documentation/usm-v5/asset-management/deploying-hids-agents.htm](https://www.alienvault.com/documentation/usm-v5/asset-management/deploying-hids-agents.htm))
AlienVault uses the OSSEC Windows agent to receive and correlate events from windows hosts; this Host-based Intrusion Detection (HIDS) agent monitors the Windows registry, event logs, file integrity and has some rootkit detection capabilities (OSSEC, 2015). While it is also possible to configure WMI-based monitoring with the WMI plugin, the GIAC team is interested in in the additional data provided by the HIDS agent and in possibly utilizing the active response feature of the agent to stop attacks in the future and has deployed the agents to the windows systems that make up GIAC’s Active Directory infrastructure.

Windows HIDS Agent deployments can be pushed from OSSIM in an ad hoc or bulk deployment fashion. Additionally, the installation file could be downloaded from OSSIM and installed manually or using automated software deployment solutions. The Windows operating system must be one of the following: Microsoft Windows XP, Windows 7, 8, or 10, Windows Server 2003, 2008 or 2012. The deployment will require a user account with administrator privileges for the respective OS. For the GIAC Enterprises deployment, an ad hoc agent push from OSSIM was used. The technical details of this deployment can be found in the HIDS deployment section of the appendix (AlienVault, n.d. e & AlienVault, n.d. f).

4.2. HIDS (Non-Windows Hosts)

For non-windows based deployments, OSSIM doesn’t have the ability to push the agent installation. Each installation must be completed directly on the respective endpoint system. The other option for non-windows based systems is an agentless deployment. If an agent based deployment is desired, AlienVault recommends that you download the latest installed directly from the OSSEC download page: http://ossec.github.io/downloads.html. For the GIAC Enterprises deployment, an agent based deployment was used; the technical details of this deployment can be found in the HIDS deployment section of the appendix (AlienVault, n.d. e & AlienVault, n.d. f).

5. Logging

This section covers the primary purpose of the GIAC Enterprises pilot OSS SIEM implementation -- automated log collection and analysis. As stated by Rob Joyce (2016),
Chief of the National Security Agency’s Tailored Access Operations (TAO) organization, logging is the “rock bottom bedrock foundation of understanding if you’ve got a problem”. As such, AlienVault has made log collection a key function of their OSSIM by developing a very robust logging function within their architecture that offers scalability as well as compatibility. OSSIM uses rsyslog (UDP Port 514) as its default syslog implementation storing all log feeds in the following default location “/var/log/alienvault/devices/<device_ip>”. Below is an architecture diagram showing the flow of this information:

![OSSEC Integration Diagram](image)

In addition to receiving syslog information, OSSIM supports the collection of log data through the use of several additional mechanisms such as:

- Remote Database Monitoring (MySQL & MS SQL)
- Windows Management Instrumentation (WMI) (Doesn’t support samba4/NTLMv2…just NTLMv1)
- Security Device Event Exchange (SDEE) (i.e. Cisco)
- Remote Log File Collection (Monitors Log File in Remote System)

(AlienVault, Inc., n.d. g)

5.1. GIAC Environment Log Sources

The following is a list of potential log sources within the GIAC pilot environment:
As described above, OSSEC was deployed to two Linux servers. Rather than just receiving the distilled event information from OSSEC it was decided that full log capture and analysis from these servers was desirable. This is largely due to the fact that these two devices host the core of the GIAC Enterprises fortune submission and review infrastructure (web server and database server). However, the AMI Linux distribution (based on RHEL) rsyslog client, used for the web server and database server, performs logging using TCP/514 as installed. As a result, either the OSSIM instance or the RHEL platforms had to be adjusted to allow rsyslog to work. After a short amount of research, it became apparent that changing the OSSIM configuration would be the easier of the two options. In addition, because TCP is a connection-oriented protocol with reliable delivery, it is more suitable for the purposes of securing the GIAC Enterprises environment.

5.2. Setup

The OSSIM logging capability collects data from practically any source and performs correlation. The OSSIM correlation activity is not only accomplished on the raw logs it receives, but also between its multiple sources of security data, which is known as cross-correlation. As the OSSIM looks for patterns of malicious activity, if it finds anything that is identified as malicious, it will issue an alarm (i.e. alert) via multiple media (i.e. SIEM Dashboard, email, text, etc.) (AlienVault, Inc., n.d. h).

There are two major pieces that need to be in place before logging can be configured between a device and the OSSIM: the first piece is the OSSIM needs to be configured to receive logs and the second is the asset that’s sending logs needs to be “seen” or “discovered” by the OSSIM asset discovery function (covered in a previous section). The technical details of the GIAC Enterprises pilot implementation log...
configuration between the rsyslog client (on the Linux servers) and server (on the OSSEC sensor) can be found in the corresponding section of the appendix.

5.3. Plugins

Once the OSSIM interface is configured and the assets are discovered, plugins need to be enabled for the respective application and/or operating system that is the target for log collection. Plugins are the software components of the OSSIM logging architecture that ingests and prepares the log data through context and normalization, making it useful for the OSSIM Server. There are 2 types of plugins, detector plugins and monitor plugins. For this discussion we will be focusing on detector plugins.

There are 2 main functions of plugins: collecting and normalizing log data. Plugins make the log data useful by parsing out fields needed for correlation and tying events to security-specific metadata. The metadata is what allows for the categorization of the log data to the proper event type and subtype. This categorization, in turn, allows for the creation of alerts. Log collection will not happen without the enablement of the proper plugins. Below is graphic displaying how the normalization process works:

![Log Normalization Process](image-url)

Figure 11: Log Normalization Process (AlienVault, Inc., g)
It’s important to note that there may be times when OSSIMs default plugins do not meet the exact needs for a particular log source. In such cases, custom plugins can be created or existing plugins can be modified to meet the situation’s needs. However, before you begin the development process, AlienVault asks that you initially submit a request directly to them. The following locations describe how to modify existing plugins or create your own, respectively:


A single endpoint may have multiple plugins associated with it to accommodate the various applications that are the target of log collection. There can be a total of 10 plugins per endpoint. Once the plugins are enabled on the OSSIM, the respective endpoints need to be configured to forward their logs to the OSSIM. These instructions are provided within the Log Management Confirmation page of the OSSIM by clicking on a hyperlink titled “Instructions to forward logs”. Once logs are being received by a respective plugin this is indicated within the Log Management Confirmation page when the Receiving Indicator turns green. Below is an example of this interface:

<table>
<thead>
<tr>
<th>ASSET</th>
<th>TYPE</th>
<th>PLUGIN ENABLED</th>
<th>RECEIVING DATA</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host:192.168.73.2 (192.168.73.2)</td>
<td>Cisco ASA Adaptive Security Appliance</td>
<td>✔️</td>
<td>☐️</td>
<td>Instruction to forward logs</td>
</tr>
<tr>
<td>Host:192.168.73.2 (192.168.73.2)</td>
<td>Citrix NetScaler</td>
<td>✔️</td>
<td>☐️</td>
<td>Instruction to forward logs</td>
</tr>
</tbody>
</table>

**Figure 12: Plugin Status (AlienVault, Inc., g)**

The current list of plugins can be found here: [https://www.alienvault.com/docs/data-sheets/usm-plugins-list.pdf](https://www.alienvault.com/docs/data-sheets/usm-plugins-list.pdf). If a plugin is not available, the following knowledgebase article explains how to submit for the addition of the needed plugin: [https://www.alienvault.com/documentation/usm-v5/kb/2016/03/how-to-request-a-new-plugin-or-updates-to-an-existing-plugin.htm](https://www.alienvault.com/documentation/usm-v5/kb/2016/03/how-to-request-a-new-plugin-or-updates-to-an-existing-plugin.htm) (AlienVault, Inc., n.d. g;
5.4. OSSIM Log Management

Though the OSSIM doesn’t contain the Logger feature of USM for long term log storage, there are still log management considerations. The primary logs that need to be considered are the logs received directly from managed devices. These logs are normalized on the sensor component of the OSSIM and sent to the server component of the OSSIM for event and alert creation. However, the pre-normalized logs are still retained on the sensor and will quickly fill up available storage, preventing further collection.

For the GIAC Enterprises pilot implementation, the environment has been configured to rotate these logs every seven days. This rotation periodicity allows for uninterrupted operations for the OSSIM deployment. Another logging feature that should also be considered is those logs generated by OSSIM itself. These can be managed by the logrotate service. AlienVault recommends referencing the rsyslog and logrotate MAN for configuring these services. The technical details of these configurations within the GIAC Enterprises pilot implementation can be found in the respective section of the appendix (AlienVault, Inc., n.d. i, AlienVault, Inc. n.d. j, & AlienVault, Inc., n.d. k).

6. Correlation & Alerting (Alarms)

6.1. Correlation

After logs are converted into events, the events are normalized in preparation for the next key process in the OSSIM workflow -- the correlation of the events. Correlation is the crux of the SIEM value proposition since it creates an overall picture of an environment. This macro view enables security teams to accurately identify and efficiently respond to security alarms. Correlation is executed by a correlation engine, which is part of the OSSIM server. The correlation engine identifies security events by
looking for behaviors patterns across all the events and identifying commonality between them.

AlienVault describes an Event as a “single line of data that describes a particular system or user level activity that took place” (AlienVault, 2016). Once the OSSIM server receives normalized events from the OSSIM sensors, the server first analyzes the events against correlation directives. Correlation directives contain correlation rules, which are applied to events to determine if events should be connected. Correlation rules take these individual lines of data and bring them together, along with information about risk and asset value, reliability and numbers of events, source and destination data and patterns of behavior to determine whether to raise an alarm (AlienVault, 2016). If an alarm is generated, it should be reviewed by the security team.

It’s possible for correlation to create a new event with increased priority and/or improved reliability. These events are then sent through the correlation engine as a new event. Correlation directives are the component of the correlation process that manages relating events (AlienVault, Inc., n.d. l, AlienVault, Inc., n.d. m, AlienVault, Inc., n.d. n.). Below are several graphical representations of the correlation process, application of correlation rules, and a resulting alert:

![Figure 13: Plugin Status (AlienVault, Inc., m)](image-url)
6.2. Reducing False Positives

It is easy for security analysts to get overwhelmed by the onslaught of alerts coming out of a SIEM in a busy network (Boland, 2013). By reducing false positives, analysts are able to react more quickly to potential threats (Lenaerts-Bergmans, 2015).

OSSIM users have several options for reducing false positives, including disabling or reducing the risk level of a particular correlation rule, customizing plugins, or changing OSSIM policies to remove events from a particular source (AlienVault, 2016).

In the GIAC Enterprises environment, multiple alarms reported OSSIM vulnerability scans coming from the OSSIM scanner as malicious activity. During the
pilot, the security team created a policy to reduce the event priority for any event with source and destination of the OSSIM scanner to 0. This allows these events to still be created, but they won’t create alarms.

![Diagram](image.png)

**Figure 16: GIAC Enterprises False Positive Tuning**

### 6.3. Tickets

Alarms, along with findings from a vulnerability scan with severity above a configured threshold opens tickets within the system. In many cases, ticket descriptions contain information about the vulnerability and how to mitigate or investigate further, as this information exists in the Threat Intelligence Knowledgebase (AlienVault, 2016). An analyst is able to update status or priority, re-assign tickets, create additional description or action, attach files, link to existing tickets, or mark as a false positive.
6.4. Investigating Alarms

OSSIM also categorizes events using the assumed “intent” of the attacker. The “intent” categories correspond to the phases of attack described in Lockheed Martin’s “Cyber Kill Chain” model (AlienVault, 2016). The Cyber Kill Chain model corresponds to the patterns used by cyber attackers when attempting to compromise a victim (Terala & Cole, 2015). In OSSIM, these phases correspond to the following intent categories:

- Environmental Awareness
- Reconnaissance & Probing
- Exploitation & Installation
- Delivery & Attack
- System Compromise

Understanding the intent of the attacker gives an analyst a starting point for prioritizing and investigating the resulting alarms. While Reconnaissance & Probing alarms may be frequent, they are not the highest priority for investigation; perhaps an analyst would add the source IP to a list of external IPs to watch out for, as described above. For Exploitation or Attack alarms, however GIAC might choose to investigate immediately, by sending those threats to an external alias for paging.
7. Vulnerability Scanning

The OSSIM sensor contains a built-in vulnerability scanner that can alert based on a combination of the severity of a vulnerability (Serious, High, Medium, Low, Informational) and the criticality of the asset. Initial configuration of the scan is as simple as configuring an asset group for the scan and creating a one-screen schedule as shown below.

![Figure 18: GIAC Enterprises Vulnerability Scan Example](image-url)

Beyond this simple scan case, OSSIM offers the ability to run both authenticated (credentials configured in the “settings” screen) and unauthenticated scans, and to customize both the contents of the scan jobs. Thresholds can be customized for alerting based on the vulnerability scans. Unfortunately, the threat database must be updated manually in OSSM, from the SSH interface. It’s hard to complain about this inconvenience, given that this feature is available, at all, in a free product.
7.1. Reporting on Vulnerability Scans

Built-in reporting on vulnerabilities is somewhat limited, with one stock report and no trending. The system does allow for a side-by-side comparison of two reports, allowing a view into new vulnerabilities that have appeared in between runs. Vulnerability descriptions include CVSS scores, reference and version information for easy follow-up. Details of the GIAC configuration can be found in the appendix.
8. Open Threat Exchange

Another valuable feature of AlienVault OSSIM that increases the reliability of event data is its Open Threat Exchange (OTX). OTX is an open information sharing and analysis network that’s free for participating organizations. Enabling OTX allows for the sharing of anonymous threat information within the OTX community, which is updated every 30 minutes. (OTX) acts as a source of current threat information that can be correlated with security events in OSSIM to alert on potentially malicious activity. With thousands of users, OTX leverages the security community to provide a breadth of data from across the Internet (Murphy, 2016).

Participants in OTX create threat descriptions known as “pulses” that contain Indicators of Compromise for threats seen in the wild, including IP addresses, domains, file hashes and URLs (AlienVault, 2016). The following type of data are shared: source and/or destination IP address of an event; name of the event; number of times such event occurred. In order to connect to OTX, one needs to create an account and enter a specified key. After signing up for an account on AlienVault’s OTX website, users will receive an “OTX Key”, which is used to register the OSSIM with OTX.
Once registered, users can subscribe to “pulse” data about a particular threat or to a user’s pulse feed. Pulses are tagged and can be searched for threats related to relevant software and operating systems; other users can vote for useful pulses and see which users have subscribed to a particular feed. Events that match an OTX pulse will give information about the matching feed, as well as information on the attacking IP or domain (AlienVault, Inc., n.d. o). Below is an example of the OTX registration page and a pulse matching an event within the GIAC Enterprises OSSIM environment, respectively.

![Figure 22: GIAC Enterprises OTX Registration Screen](image1)

![Figure 23: GIAC Enterprises OTX Pulse Matching Events](image2)
9. Issues and Weaknesses

9.1. OTX

AlienVault’s Open Threat Exchange clearly has the power to be a very valuable resource, but the pulse model makes it difficult to leverage the community threat intelligence effectively. Tens of thousands of users have created “pulse” threat feeds, but there is almost no information to be had about the best pulses or users to follow or enough metadata to understand targeted industries. While it is possible to search tags for an operating system or piece of software involved in a threat, subscribing pulse-by-pulse is inefficient and there’s no sort functionality to find the most popular feeds, those with the most votes, or those created by people or companies that have good threat information. OTX seems like a potentially great source of data, but the format makes it difficult to use.

9.2. OSSIM Performance

GIAC Enterprises had only a small number of servers involved in its OSSIM pilot. Even with two Linux and Two Windows servers contributing log information, the OSSIM control node, with two CPUs and 8 GB of memory was frequently showing high CPU and memory utilization and the configured sensor frequently crashed.

Figure 24: GIAC Enterprises Crashed Sensor Node after several hours of received logs
9.3. Long Term Log Storage

The OSSIM installation provides no built-in mechanism for long-term storage of logs, making it difficult to use for audit or regulatory purposes. AlienVault does provide instructions for using the “Jailbreak” console to configure external log storage, an option GIAC is considering exploring in a future proof of concept.

10. Next Steps

10.1. Tandem AlienVault OSSIM and ELK Deployment

OSSIM was chosen for several reasons. First, it is a well-supported open-source SIEM solution that is able to parse a wide variety of event sources through its plugin system. In addition, the OSSIM solution allows an administrator to write custom plugins for event sources that are not supported. This solution also provides an upgrade path to a commercial solution in AlienVault USM.

The most cited difference between the open-source OSSIM and commercial USM solution found during research was support for long term log storage and correlation. Without the ability to perform long term analysis, some attacks may be missed due to the speed at which they are carried out.

A novel solution to this issue discovered during research was to perform a tandem deployment. In order to perform short term correlation and analysis of events the researchers employed OSSIM as discussed in this guide. In addition, to address the long-term analysis shortcoming of OSSIM, the researchers deployed an ELK stack. ELK is the combination of ElasticSearch, LogStash, and Kibana software to create a flexible and highly scalable analysis platform.

The ELK stack was configured to collect and perform long-term analysis on the same sources. The shortcoming of ELK stack as a SIEM is that it requires significant customization to perform this role. It is not built solely for the purpose of being a SIEM. This could provide a next-step opportunity for analysis and correlation on a longer term basis after OSSIM is deployed and tuned properly.

In addition, while there was a wealth of “buzz” about ELK as a SIEM, there wasn’t much in the way of practical implementation guidance. This may indicate a possible
trend toward ELK-based SIEM products and greater support. As a result, it may be worth making the effort to integrate ELK into the GIAC Enterprises environment as an open-source investment strategy.

10.2. Additional Hardening

AlienVault supports granting root terminal access to the OSSIM sensor; however this appears to be deterred through the use of the OSSIM console menu seen below. The “Jailbreak System” term carries with it a negative connotation that may deter administrators from wandering into root shell access.

Figure 25: GIAC Enterprises OSSIM Console Window

The secondary notice seen below doesn’t help matters any either.

Figure 26: GIAC Enterprises OSSIM Console Secondary Notice
Having this access can be valuable for configuring a number of features. First, SSH public key authentication may be desired over password authentication. This configuration eliminates the possibility of password-based attacks. Also, during the process of configuring rsyslog, the IPtables firewall configuration had to be adjusted in order to allow communication over TCP/514 from the AMI Linux hosts. While inspecting the configuration, several recommended rules were identified within the OSSIM firewall_include configuration file as seen below.

```
# This file includes custom rules to the ossim_firewall file after
# ossim-reconfig is run
#
# Rules starting with -A (append) get added after the default ossim rules
# Example to allow port 5666:
# -A INPUT -p tcp -m state --state NEW -m tcp --dport 5666 -j ACCEPT
#
# Rules starting with -I (insert) get added before the default ossim rules
# Example to ignore all new incoming connections except for network
# 192.168.0.0/16
# -I INPUT -m state --state NEW -s ! 192.168.0.0/24 -j DROP
#
# Be careful with DENY and DROP rules, as functionality might be affected and
# you could loose the connection to the host administrative interface. It is
# recommended to add the following line at the end of this file to always
# permit remote administration from one host or network:
# -I INPUT -s [administration IP or network] -p tcp -m state --state NEW -m multi
# port --dports ssh,http,https -j ACCEPT
#
# -A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
```

**Figure 27: GIAC Enterprises OSSIM IPTables Configuration**

Configuration of the OSSIM firewall is not possible within the web interface. Additional rules may be used to restrict access to the sensor itself. In the first highlighted block above, the example rule is used to restrict communication (all protocols) to a particular network. In the second block, the example rule is used to restrict access for administration of the OSSIM sensor. Both rules provide additional defense in depth for an important detective countermeasure.

Finally, it is desirable to configure rsyslog to operate over SSL/TLS. Logging information has been known to contain sensitive information which may include credentials, verbose error messages, and details that may assist an attacker in executing
an attack. This information should be protected commensurate to its sensitivity from both insiders and would-be attackers.

10.3. Network Flow Data Collection

With the GIAC Enterprises resources deployed as virtual server instances in AWS there were limited opportunities to configure network flow collection from the OSSIM sensor. Network flow is a method to summarize network transfers into statistical information useful for analysis. This information can be particularly useful in identifying data exfiltration. Multiple successive or persistent connections from the same host and large transfers are potential indicators of compromise that should be monitored. Despite lack of support and control from Amazon, it is possible to collect network flow data from hosts using host-based network flow generation software such as Netflow-Generator-for-Linux (https://github.com/vamshireddy/Netflow-Exporter-for-Linux). At the very least, this software should be deployed on the web and database servers that support the GIAC Enterprises fortune collection application.

11. Conclusion

GIAC Enterprises, a small to medium size business, has grown to a point where their current manual log analysis process is no longer efficient or effective. Thus, the GIAC Enterprises growth mandated the need for the automated analysis and correlation of system logs. As such, GIAC Enterprises was forced to look for a SIEM solution that automates the correlation and analysis of system logs. GIAC Enterprises had a significant financial constraint, which required them to focus their investigation on several open source solution options. After researching all the available OSS SIEM options, AlienVault’s OSSIM solution best met the needs of GIAC Enterprises.

OSSIM was chosen for several reasons. It not only met the needs from a log analysis and correlation capabilities perspective but also from a scalability and support perspective. OSSIM is a stable and well-supported open-source SIEM solution that is able to parse and correlate a wide variety of event sources through its plugin system. In addition, the OSSIM solution allows an administrator to write custom plugins for event sources that are not supported, further increasing its ability to scale for log collection.
AlienVault also provides a path to upgrade OSSIM to its commercial solution, AlienVault USM, which supports long-term log storage and additional alerting indicators.

Once the security analysts settled on OSSIM as the solution of choice, a pilot environment was developed. The pilot installation revealed that OSSIM has the capability to scale with organizational growth and the capability to scale in terms of additional security analysis capabilities (i.e. vulnerability scanning, endpoint security, commercial version, etc.). The additional security analysis capabilities increase the ability for OSSIM to improve the efficacy of its alerts from log correlation. The only significant drawback that was found in OSSIM is its ability to support long-term log storage. However, as the next steps section explains, there are potential options available for addressing this shortcoming. Overall, OSSIM was found to be an excellent OSS SIEM option for implementation within the GIAC Enterprises business.
REFERENCES


## 1. Solution Selection Matrix

<table>
<thead>
<tr>
<th>Product</th>
<th>Linux Support</th>
<th>Windows Support</th>
<th>AD Integration</th>
<th>RBAC</th>
<th>Log Correlation</th>
<th>HIDS</th>
<th>NIDS</th>
<th>Long Term Log Storage</th>
<th>Real-Time Search</th>
<th>Tagged Elements</th>
<th>Active Development</th>
<th>Threat Feeds</th>
<th>Reporting Dashboards</th>
<th>Compliance Reports</th>
<th>Community Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSSEC</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td>no</td>
<td>Not a SIEM. OSSEC integrates with SIEMs (i.e. OSSIM).</td>
</tr>
<tr>
<td>ELK</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>Not robust enough for a complete solution.</td>
</tr>
<tr>
<td>ELSA</td>
<td>yes</td>
<td>yes</td>
<td>ldap</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>?</td>
<td>no</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>Doesn't include all the need functionality.</td>
</tr>
<tr>
<td>Graylog</td>
<td>yes</td>
<td>yes</td>
<td>ldap</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>Doesn't include all the need functionality.</td>
</tr>
<tr>
<td>OSSIM</td>
<td>yes</td>
<td>yes</td>
<td>ldap</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>Can pay for commercial version if needed.</td>
</tr>
<tr>
<td>OpenSOC w/ Apache Metron</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>Not mature enough.</td>
</tr>
<tr>
<td>Prelude</td>
<td>Free version doesn't support large environments.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Onion</td>
<td>Richard Bejtlich already wrote a full book on monitoring with Security Onion; no need to repeat this work</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIDO</td>
<td>Not mature enough.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOGalyze</td>
<td>Not mature enough.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Primary Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Archiving</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prelude</th>
<th>Free version doesn't support large environments.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Onion</td>
<td>Richard Bejtlich already wrote a full book on monitoring with Security Onion; no need to repeat this work</td>
</tr>
<tr>
<td>FIDO</td>
<td>Not mature enough.</td>
</tr>
<tr>
<td>LOGalyze</td>
<td>Not mature enough.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Primary Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Archiving</td>
</tr>
</tbody>
</table>
2. OSSIM Image Installation

2.1. Building and Installing the Virtual Machine Image

To begin, VMWare Workstation 11 must be started as seen below.

![VMWare Workstation Interface](image1.png)

Once the VMWare interface is opened select File > New Virtual Machine.

![New Virtual Machine Wizard](image2.png)

This will open the “New Virtual Machine” wizard. We will make some simple hardware adjustments at the end of our build so we can select the “Typical” option.
With the typical option selected, click the next button. On the next screen, we must select the ISO file which was downloaded from the AlienWare website. This will serve as the installation media for the OSSIM virtual machine.

Select the “Installer disc image file (iso):” radio button option, click the “Browse…” button, and select the downloaded ISO file. Click Next.

On the next screen the virtual machine must be named. Based on the node that is being built; call the virtual machine “OSSIM Control Node” or “OSSIM Sensor Node” as necessary.
Click Next.

The wizard will request that the disk size be specified. The Control Node should be allocated a 64 GB virtual hard disk while the Sensor Node is allocated 32 GB. Leave the “Split Virtual Disk Into Multiple Files” setting selected.

Click Next.

On the next screen, the hardware for the virtual machine must be customized to ensure that it meets our specifications.
Click the “Customize Hardware…” button. This will present the Virtual Machine hardware configuration. Select the “Memory” option first. Both virtual machines will be allocated 8 GB of RAM.

*Note: If possible, more RAM can be allocated if physically available. This is recommended, since the USM documentation recommends 15 GB of RAM for control node installation.*
Next, select the Processors node. The USM documentation recommends 2 processor cores for the Control Node. We will configure both the Control and Sensor nodes with the same processor characteristics. Select “2” in the “Number of Processors” drop down and leave all of the other options with their default selections.

![Hardware Configuration](image)

Next, select the Network Adapter node. Rather than using NAT, we will specify a bridged network connection which allows the appliance to get an IP address not issued by the host operating system. In addition we will avoid two potential levels of Network Address Translation. Select the “Bridged” radio button and leave all other options default.
Finally, our OSSIM instance will require two network adapters. One adapter will be used to collect data for analysis while the other will be used for management of the Control and Sensor nodes. Click the “Add…” button found at the bottom of the node list. On the ensuing page, select the “Network Adapter” node and click the Next button.
Configure the network adapter in “Bridged” mode similar to the first network adapter instance. Leave all of the other options default and click the “Finish” button.
Click the “Close” button to complete the virtual machine configuration changes. Then click “Finish” to complete the virtual machine configuration and power on the OSSIM instance.

The OSSIM ISO will boot to the node selection window seen below. Depending on the instance that you are building, select the appropriate node from the menu.

The image above depicts the build for the OSSIM Control Node so we will select the “Install AlienVault OSSIM 5.2.2 (64 Bit)” option. Select the appropriate language for the installation on the next screen seen below and click the “Continue” button.
Select the appropriate location and click the “Continue” button.

Select the appropriate keyboard language layout and click the “Continue” button.
The OSSIM installation will progress through several installation steps before prompting for the next set of input.

When prompted for the primary network interface, select an interface that has internet connectivity and click the “Continue” button.
Next, specify an IP address that can be used for internet connectivity and click the “Continue” button.

Input the appropriate network mask for the target network can click the “Continue” button.
Input the appropriate IP address for the network gateway and click the “Continue” button.

Input name servers for the OSSIM installation to perform host resolution and click “Continue”.
Specify a secure root password for the OSSIM installation and click “Continue”.

Select the appropriate time zone for the installation and click “Continue”.
The installer will format the disk and begin installing the OSSIM components. This will take several minutes to complete.

The wizard will complete, reboot the virtual machine, and start the AlienVault OSSIM operating system.
When the book sequence completes a logon prompt is presented along with the URL for the OSSIM web interface.

Before shutting down the OSSIM node an administrator account must be created. Open the OSSIM web interface at the specified URL. This initial visit will prompt to create an account to administer the OSSIM instance. Fill out the form, select a strong password (not the root password), and click the “Start Using AlienVault” button.
This will get us far enough along in the process to shut down the virtual machine and convert to an AWS AMI instance.
Close the web interface and log onto the console of the OSSIM appliance. Once logged on, the menu below will be presented. Select option 7, Shutdown Appliance and click the OK button.
Once the virtual machine has shut down, we can convert it to an AMI instance.

2.2. Converting the Virtual Machine

In order to import the virtual machine into AWS, it must be checked for compatibility and converted to an OVA file. To accomplish this, the AWS Command Line Interface must be installed on the computer used for conversion (Amazon, n.d.). Installing the AWS Command Line Interface is a straightforward process. Simply download the appropriate installer, execute it, and accept all of the default options.

VMware Workstation only exports virtual machines in OVF format. AWS requires that virtual machines be in VMDK, VHD, RAW or OVA format. Luckily, VMware also makes the VMware OVF Tool available for use. This tool must also be downloaded in order to convert the virtual machine to OVA format (VMware, n.d.). This tool is supported across multiple platforms including Windows, Linux and OSX. Install the OVF Tool by executing the downloaded installer, accept all of the defaults on the installation wizard, and click finish.

Once both tools are installed, convert the virtual machine by changing into the “C:\Program Files\VMware\VMware OVF Tool” directory and then run the following command:
C:\Program Files\VMware\VMware OVF Tool>ovftool.exe  \
"c:\users\[username]\Documents\Virtual Machines\OSSIM Control Node\OSSIM Control Node.vmx" c:\Users\fletch\Downloads\OSSIM-Control-Node.ova

The tool will identify the source and destination files and indicate the progress of the conversion as seen below.

Once conversion of the virtual machine has completed, the OVF Tool will indicate as such and you will find the output OVA file in the target directory as seen below. Despite having specified a 64 GB VHD and 8 GB of RAM the output OVA file is only 2 GB in size.

With the VMX formatted virtual machine converted to OVA format, the virtual machine can be imported into AWS using the AWS Command Line Interface.

### 2.3. AWS Image Import

The first step in converting the newly-created VMX image for use in AWS is to upload the image to Amazon Storage. If there is no existing storage bucket in S3, create one in the region where you’ll be converting the AMI:
Upload the .OVA image to the bucket:

Log into an AWS instance (launch a new one, if needed) running Amazon Linux in a region co-located with your S3 bucket. The AWS command line interface tools should come pre-installed on these images.

Run `aws configure` and enter the correct access key and secret key, as well as the region where the S3 bucket was created.

```bash
$ aws configure
AWS Access Key ID [None]: 1234
AWS Secret Access Key [None]: 5678
Default region name [None]: ap-southeast-2
Default output format [None]:
```

Create the following three files, customized for the region, bucket and image name:

Role-policy.json

{  
   "Version":"2012-10-17",  
}
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": [
      "arn:aws:s3:::lyssanr-6100-ossim"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": [
      "arn:aws:s3:::lyssanr-6100-ossim/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:ModifySnapshotAttribute",
      "ec2:CopySnapshot",
      "ec2:RegisterImage",
      "ec2:Describe*"
    ],
    "Resource": "*"
  }
]
}

trust-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vmie.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
Then run the following commands to do the conversion:

```bash
$ aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
$ aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
$aws ec2 import-image --description "OSSIM Control Node" --disk-containers file://containers.json
```

The image may take some time to convert. Once it finishes, it will be available in “My AMIs”.

### 2.4. Launching from the AMI

With the new AMI created, you can launch an instance.
Choose an instance type that matches the hardware specified when creating the OVA file:

Choose the subnet that matches the IP used to create the OVA file and enter that IP in Network Interfaces:
Configure security groups to match the needed ports (1514 for OSSEC traffic, 514 for syslog, HTTPS and SSH):
We have not given the OSSIM control node a public IP, so you’ll need to use an SSH tunnel through a bastion host to get to the web interface:

```
$ ssh -L 8443:192.168.2.130:443 ec2-user@52.91.54.98
```

### 3. Configuring Networks and Asset Discovery

Before adding the monitored networks, the default networks should first be removed. Navigate to the Environment > Assets & Groups option, then select the Networks tab.

On this tab, the networks identified below will appear. To perform the deletion, select the check box next to the Network header (which selects all subsequent networks).
After the networks have been selected, navigate to the Actions menu and select the Delete Option.

Finally, confirm the deletion by clicking the Yes button.

With the default networks removed from the sensor, the production networks can be added. For each network identified in the table above select the Add Network > Add Network option.

Use predetermined asset values supplied in the table above to fill out the ensuing form that loads as seen below. Since the GIAC Enterprises deployment is small, only the default sensor exists. If OSSIM expansion occurs ensure that the appropriate sensor is selected. Optionally, an icon to identify the monitored resource can be selected and a description can be added. Once the form is complete click the Save button to complete the network add operation.
Once the network has been added, it will appear within the OSSIM interface similar to the screen grab seen below.

After all monitored networks have been added to the OSSIM sensor Asset Discovery Scans should be configured for each. The Asset Discovery Scan settings are accessed by navigating to Environment > Assets & Groups and selecting the Schedule Scan tab.
For each monitored network a scan should be scheduled by clicking the Schedule New Scan button. This will cause the Schedule New Asset Scan form to be displayed. Each scan’s characteristics should be configured as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Targets to Scan</th>
<th>Sensor</th>
<th>Type</th>
<th>Timing</th>
<th>Auto-detect OS</th>
<th>Rev DNS</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIAC Enterprises DMZ Scan</td>
<td>192.168.0.0/24</td>
<td>Default</td>
<td>Full Scan</td>
<td>Normal</td>
<td>Y</td>
<td>Y</td>
<td>Daily</td>
</tr>
<tr>
<td>GIAC Enterprises Internal Scan</td>
<td>192.168.2.0/24</td>
<td>Default</td>
<td>Full Scan</td>
<td>Normal</td>
<td>Y</td>
<td>Y</td>
<td>Daily</td>
</tr>
</tbody>
</table>

The Name, Targets to Scan, and Sensor are all parameters that we’ve already used before. The Type, Timing, Auto-Detect OS, and Reverse DNS options can be thought of as parameters to an Nmap discovery scan. Since we are scanning our own network segments which contain sensitive information we want to perform a comprehensive scan. We therefore select the Full Scan option. If the number of assets on the network segment grows significantly it may become impractical to use the Full Scan. The scan should be monitored for completion time and storage.

Everything on these networks is connected at LAN speed and our scans do not need to be covert so we select Normal timing. If new networks or assets are added over WAN links, it may be wise to consider selecting a slower timing value. Auto-detect OS and Reverse DNS are both easily understood options. Finally, the frequency will be set to Daily since we are monitoring highly controlled environments. As a matter of corporate policy, we will NOT engage in external resource scanning. The purpose of OSSIM is to inform GIAC Enterprises on potential incoming attacks or malicious activity. It will not be used as a platform for “Hacking Back” or gathering intelligence useful for informing this activity.

An example of a completed “Schedule New Asset Scan” form can be seen below. Once the form is completely filled out the save button can be clicked to make the change permanent.
4. Deploying HIDS Agents

4.1. Windows Agents

In order to push the Windows agent, assets must exist and have the correct Windows operating system associated. Assets can be discovered automatically using an asset scan as described in the “Asset Discovery” section, or can be added manually. Choose the asset or group of assets for deployment and send using “Deploy HIDS Agent” from the Actions menu. The installation will prompt for a Domain, Username, Password for install on the target system.

In the event that the HIDS agent cannot be pushed automatically from the OSSIM console, the pre-configured binary can be downloaded from the Environment -> Detection -> Agents screen, using the download button and distributed automatically via tools such as SCCM or copied manually over to the target system for installation.
If some agent installations are unsuccessful, errors and suggestions regarding troubleshooting can be found by looking in the “Asset Details” for the particular asset that failed. The right-hand side “SUGGESTIONS” menu should have logs for each installation attempt, with more details on the failure.
4.2. Non-Windows Agents

To install the Linux based agents in the GIAC Enterprises environment, the following steps need to be executed:

1) Install proper compiling tools
2) Download and extract the installation package
3) Run the install script (included with the installation package)
4) Associate the agent with the OSSIM instance

The command below installed the proper tools for compiling (Step 1):

```bash
sudo yum groupinstall "Development Tools" -y
```

```bash
sudo yum install kernel-devel -y
```
NOTE: All installation processes required the commands to be run in administrative mode (i.e. “su” or “sudo”).

The commands below downloaded and extracted the agent package (Step 2):

“sudo wget –U ossec http://www.ossec.net/files/ossec-hids-2.8.2.tar.gz”

The screenshot below shows this download in progress:

Once the download was completed the package needed to be extracted.

The command below was run to initiate the installation script, which completed the install (Step 3):

“bin/bash ./install.sh”

Once the script was executed, the only choices that needed made were what language to support (English), the software to install (agent instead of server), and the IP address of the OSSIM sensor.
Once the installation is complete, you simply need to press Enter to complete the installation, and you’re provided with the screen below.
The next step in the process is to add the installed Linux HIDS agent to the OSSIM (Step 4). Following the instructions available here from the AlienVault Deployment Guide:

Switch to the OSSIM instance and complete the following steps:

1. Navigate to **Environment > Detection**.
2. Navigate to **HIDS > Agents > Agent Control > Add Agent**.
3. On New HIDS Agent, select the host from the asset tree.
4. Click **Save** (The new agent should be added to the list of agents)
5. Next extract the authentication key for the agent by clicking the ![key icon] button in the Actions column, and then copy the key that displays.
6. Login to the Linux host, run `/var/ossec/bin/mange_client`, and then enter `I` to import the key you copied in the previous step.
NOTE: To edit the IP address of the OSSIM sensor you can edit /var/ossec/etc/ossec-agent.conf on the respective endpoint.

NOTE: The follow command can restart the OSSEC agent: service ossec-hids restart

Below you can see what an active status looks like under the status column.

5. Logging & Plugins

In order to configure the OSSIM server to support rsyslog over TCP an administrator must connect to the server via ssh. Once connected, the following menu will appear.
Manually editing configuration files on an OSSIM sensor is not authorized by default. In order to make changes to the system the Jailbreak System option must be selected. Upon selecting this menu option a prompt is displayed requesting feedback on the desired features that aren’t present through the user interface.

Select the Yes option and press enter. This will exit the setup menu into a root shell prompt as seen below.
With root access to the system obtained, the appropriate configuration files can be edited. To confirm that the sensor is not listening on TCP/514 the netstat command can be used as seen below.

```
    allenvault:~ netstat -na | grep 514
    udp  0 0 0.0.0.0:514 0.0.0.0:*
    udp6 0 0 :::514 ::::*
    allenvault:~
```

Based on the output, the rsyslog service is not bound to the TCP port. In order to make this change, the the `/etc/rsyslog.conf` file must be edited. Within this guide the vim editor is used but any command line editor will work to complete this process.

Near the top of the configuration file there are two sections that relate to the transport protocols supported. By default, the TCP option is commented out since hash marks appear at the beginning of lines 20 and 21. Enabling the TCP 514 listener is as simple as deleting the hash marks at the beginning of each line.

```
1 # /etc/rsyslog.conf  Configuration file for rsyslog.
  
2 # For more information see
  # /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
  
3 #
4 #
5 #
6 #
7 #
8 #
9 #
10 #
11 #
12 #
13 #
14 #
15 #
16 #
17 #
18 #
19 #
20 #
21 #
22 #
23 #
24 #
25 #
26

# provides TCP syslog reception
$ModLoad tcp Sob
# Provides support for local system logging
$ModLoad imuxsock
# Provides kernel logging support
$ModLoad immark
# Provides --MARK-- message capability
$ModLoad imudp
# Provides UDP syslog reception
$InputTCPServerRun 514
# Provides TCP syslog reception
$InputTCP 514
```

A properly modified configuration file can be seen below.
Save and close the file to complete the change. It is not enough to just edit the configuration file to start the listener. The service must be restarted so that the new configuration is loaded into the running daemon. Restart the rsyslog daemon by issuing the “service rsyslog restart” as seen below.

One the restart is complete the netstat command can be used to confirm the listening state of the service. Output from this command can be seen below.

Two new lines should appear in the output indicating that IPv4 TCP and IPv6 TCP are both in a listening state and bound to all active IP addresses.

Now that the service is running, we must ensure that the Linux AMI clients can connect to the OSSIM sensor over this port. The default OSSIM configuration has an iptables firewall configuration that only allows a minimum number of services to access the server. Since rsyslog over TCP is not configured by default, this service must also be allowed through the iptables firewall.
Changing the iptables configuration requires that the `/etc/ossim/firewall_include` file be edited to add the necessary rules. Before doing so, it is a good idea to review the current firewall rules by running the `iptables -L` command. Output similar to that seen below will be produced by the server.

```
*filter
::

Chain INPUT (policy ACCEPT)
target     prot opt source               destination          icmp-timestamp-request
DROP       icmp -- anywhere             anywhere
ACCEPT     icmp -- anywhere             anywhere
ACCEPT     all -- anywhere              anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:ssh
ACCEPT     tcp -- localhost             anywhere            state NEW tcp dst:syslog
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:syslog
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:44001
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:44002
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:44004
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:440079
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:http
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:https
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:44003
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:8001
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:3226
ACCEPT     udp -- anywhere              anywhere            udp opt:1514
ACCEPT     udp -- anywhere              anywhere            udp opt:1514
ACCEPT     tcp -- anywhere              anywhere            state NEW tcp dst:9590
ACCEPT     udp -- anywhere              anywhere            udp opt:9595
ACCEPT     udp -- anywhere              anywhere            udp opt:9595
ACCEPT     udp -- anywhere              anywhere            udp opt:9595
ACCEPT     tcp -- localhost             anywhere            state NEW tcp dst:6380
REJECT     all -- anywhere              anywhere            reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
REJECT     all -- anywhere              anywhere            reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination      icmp-timestamp-reply
```

The `iptables -L` output should be reviewed to understand the rules that are currently in-place on the sensor. Once this information is understood, the configuration file can be edited to allow rsyslog to communicate. An already edited `firewall_include` file can be seen below.

```
# This file includes custom rules to the ossim_firewall file after
# ossim-reconfig is run

# Example to allow port 5666
-A INPUT -p tcp -m state --state NEW -m tcp --dport 5666 -j ACCEPT

# Example to allow port 514
-A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
```

- Be careful with DROP and DENY rules, as functionality might be affected and
you could loose the connection to the host administrative interface. It is
recommended to add the following line at the end of this file to always
permit remote administration from one host or network:
```
-A INPUT -s [administration IP or network] -t tcp -m state --state NEW -m multiport --dport
```

- A INPUT -p tcp -m state --state NEW -m tcp --dport 514 -j ACCEPT
Each of the rules is inserted into the firewall configuration. Since the default OSSIM firewall configuration ends with a deny all rule, appending them would be ineffective. The first two rules restrict access to the OSSIM sensor to the two protected networks. The next rule allows new inbound connections on TCP 514 enabling log collection using rsyslog over TCP. A TCP established rule already exists in the default configuration so it is not necessary in this instance.

Once the firewall_include file has been updated, save the configuration and issue the ossim-reconfig command to the sensor. The following progress window will appear as the sensor is reconfigured.

Once the reconfiguration is complete, a root shell prompt will appear at the bottom of the window. This prompt is easy to overlook and an administrator may believe that the sensor has stopped responding.
After reconfiguring the sensor it is a good idea to review the iptables configuration to ensure that the new rule appears in the running configuration. This output can be seen below with the new rule highlighted indicating that configuration was successful.

As recommended in the configuration file, additional rules should be added to further restrict access to the OSSIM sensor. This portion of the guide is specifically concerned
with configuration of the rsyslog service. Security enhancements to the sensor will be discussed in another section of the guide.

Type exit at the root shell and hit enter twice. This will return to the OSSIM console interface. Select the Exit option to disconnect the console session.

Access to the rsyslog service can now be tested from the client to ensure that the service can be accessed prior to enabling remote logging. Log onto one of the clients which will be forwarding logs to the OSSIM sensor. Once logged on, use the netcat tool to ensure that the port is open and responding.

As long as the netcat tool does not respond with an error (like no route to host or connection refused) and connects to the sensor then the service is running. An example error message can be seen below.

```
[ec2-user@ip-192-168-0-184 ~]$ nc -vv localhost 514
nc: connect to localhost port 514 (tcp) failed: Connection refused
[ec2-user@ip-192-168-0-184 ~]$ 
```

Next, rsyslog must be configured on the client to forward log events to the OSSIM sensor. The /etc/rsyslog.conf file must be edited similar to the OSSIM server. Open the rsyslog.conf file on the AMI Linux instance in your preferred editor and navigate to the
forwarding section of the configuration file. This is located around line 60 of a default AMI Linux host.

By default, the entire log forwarding section of the configuration file is commented out. To enable forwarding, uncomment the lines that correspond to lines 68-73 below without editing. After that, uncomment the line corresponding to line 75 in the output below. Then replace the text remote-ip with the IP address of the OSSIM sensor. After completing these changes, save the file and exit your editor.

```
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding rule. They belong together, do NOT split them. If you create multiple forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is down, messages are spooled to disk and sent when it is up again.
$WorkDirectory /var/lib/rsyslog # where to place spool files
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
$ActionQueueMaxDiskSpace 1g # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList # run asynchronously
$ActionResumeRetryCount -1 # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
.* @192.168.2.130:514
# ### end of the forwarding rule ###
```

As with the OSSIM sensor, the rsyslog configuration must be reloaded for the configuration to take effect. Issue the service rsyslog restart command as seen below. The service will restart and begin forwarding logs to the OSSIM sensor.

One final configuration step is required to ensure that rsyslog information that is forwarded to the OSSIM sensor gets processed properly. To make this configuration change, the OSSIM web interface must be accessed. Log into the web interface using the administrator account and navigate to Environment > Assets & Groups and select the Assets tab.
For each AMI Linux installation that must have rsyslog configured, perform the following operations.

Click the asset details button at the end of the row for the AMI Linux computer that is to be monitored.

The asset details form will appear as seen below. Navigate to the lower portion of the page when it loads. This area has a number of “tabbed” options. Select the Plugins tab.
Once the Plugins tab is active, click the Edit Plugins button to add the plugin to the instance. This will load the Edit Plugins page seen below.

Click the Add Plugin button to add the syslog plugin. When the button is clicked, a new row of drop down lists will be added to the form. Simply select the syslog entry in the Vendor field. The Model and Version fields will automatically populate.
Finally, click the Save button to save the plugin configuration. Once this is complete, monitor the asset details page to ensure that new syslog entries are being added to the Events count. Once syslog data has been reflected in this output the syslog configuration is successful.

5.1. **Adding non-plugins from the console**

Some plugins cannot be configured directly from the web interface and need to be enabled from the console instead. To enable SSH into OSSIM Control Node as root:

```
[ec2-user@ip-192-168-0-184 ~]$ ssh root@192.168.2.130
root@192.168.2.130's password:
Linux alienvault 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt20-1+deb8u3 (2016-01-17) x86_64

==========================================

=   =

=   =

=   =

==========================================

http://www.alienvault.com

Access the AlienVault web interface using the following URL:

https://192.168.2.130/

You have new mail.
Last login: Wed Apr 6 20:59:01 2016 from ip-192-168-0-184.ec2.internal
```
Choose option 1 for “Configure Sensor” from the menu and then choose option 4 for “Configure Data Source Plugins”:

Access the AlienVault web interface using the following URL: https://192.168.2.130
There is an extensive list of plugins available, including many open-source security tools and common infrastructure solutions such as: apache, bit-9, clamav, cisco asa and vpn, exchange, dhcp, bind, and honeyd. Space bar will add or remove each selection. During configuration, the GIAC team found that adding more than a handful at a time caused the server to freeze up during the Apply phase.

Hit enter for “OK” and then choose option 8 to “Apply All Changes”.

Access the AlienVault web interface using the following URL: https://192.168.2
5.2. Configuring the ‘moodle’ plugin:

Certain plugins cannot be enabled or configured directly from the web interface and must instead be enabled from the console using the “jailbreak” feature. The ‘moodle’ plugin is one example of a database plugin that requires configuration from the Jailbreak console.
Locate the configuration file in /etc and edit:

```
source=database
source_type=mysql
source_ip=
source_port=3306
user=
password=
```

Enter the appropriate IP, port, username and password to connect to the mysql database.

```
source=database
source_type=mysql
source_ip=
source_port=3306
user=
password=
```

db=moodle

sleep=2
6. Alarms, False Positives, & Tickets

6.1. Alarms

Alarm list:
6.2. Reducing False Positives

During GIAC testing, multiple false positive alerts showed up for scans conducted by the OSSIM scanner. OSSIM offers the option of configuring policy to remove these false positives or change rules or risk ratings based on environment.

To adjust policy configuration, Go to Configuration -> Threat Intelligence -> Policy.

Create a new policy in the default group, with the OSSIM Scanner IP as the source:
Lower the event priority to 0:

Reload to use the new policy:
Delete all existing alarms for these events:
6.3. Tickets

Ticket resulting from a vulnerability scan finding with risk 5. Contains information on vulnerability and how to mitigate:

**Vulnerability Detection Result:**

It was detected that the host implements TCP timestamping.

**Vulnerability:**

TCP timestamping was introduced with a delay of 1 second between:

- TCP SYN, and
- TCP SYN+ACK, with

```
    seq no 1 0 1 1 2 3
    timestamp 0 0 0 0 0 0
```
Ticket Update:

**DESCRIPTION:**

- Updated kernel parameters.

**ACTION:**

- Updated kernel parameters.
7. Configuring Vulnerability Scans

Vulnerability scans get run against a particular asset group. To configure an asset group, choose “Asset Groups” from the “Assets & Groups” dropdown in the “Environment” heading:

Create New Group:
Add Assets to the new group from the existing list:
Then set up the scheduled scan, choosing an existing profile or creating a new profile with custom rules, if needed. Configure the schedule and associate with the chosen asset group. If authenticated scans are needed, authentication credentials must be associated with particular assets or asset groups in the Configuration -> Administration menu, under “Users”.

Sample Vulnerability description from a vulnerability scan finding. Most checks provide useful information and links regarding mitigation strategies for the vulnerability.
MySQL Authentication Error Message User Enumeration Vulnerability
Risk: High
Application: mysql
Port: 3306
Protocol: tcp
ScriptID: 802046
Vulnerability Detection Result:
The following users could be enumerated:
root
admin
test
Impact:
Successful exploitation allows attackers to obtain valid
usernames, which may aid them in brute-force password cracking or other attacks.
Insight:
Mysql server will respond with a different message than Access
Denied, when attacker authenticates using an incorrect password with the old
authentication mechanism mysql 4.x and below to a mysql 5.x server.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A
Summary:
The host is running MySQL and is prone to user enumeration vulnerability.
Affected Software/OS:
MySQL version 5.5.19 and possibly other versions
MariaDB 5.5.28a, 5.3.11, 5.2.13, 5.1.66 and possibly other versions
Solution:
For MariaDB upgrade to 5.5.29, 5.3.12, 5.2.14 or later.
For updates refer to https://mariadb.org/
For MySQL apply the updates from vendor, http://www.mysql.com/
References:
http://osvdb.org/88067
http://securia.com/advisories/51427
http://www.exploit-db.com/exploits/23081
https://mariadb.atlassian.net/browse/MDEV-3909
<table>
<thead>
<tr>
<th>Course Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>