Hands-On Lab: AlienVault OSSIM

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; AlienVault OSSIM

Table of Contents

[Introduction 2](#_Toc76733660)

[Objective 3](#_Toc76733661)

[Estimated Completion Time 3](#_Toc76733662)

[Materials Required 3](#_Toc76733663)

[Minimum System Configuration 4](#_Toc76733664)

[Data From Your Instructor 4](#_Toc76733665)

[Setting up AlienVault OSSIM 4](#_Toc76733666)

[Downloading and Installing VMware Workstation 16 Player 4](#_Toc76733667)

[Downloading and Installing AlienVault OSSIM 5](#_Toc76733668)

[Starting AlienVault OSSIM 7](#_Toc76733669)

[Web UI Access 8](#_Toc76733670)

[Configuring and Using AlienVault OSSIM 10](#_Toc76733671)

[Self-Reflection and Response 23](#_Toc76733672)

[Instructor’s Response 23](#_Toc76733673)

# Introduction

Many organizations have come to rely on security information and event management (SIEM) as a central element to empower a security operations center (SOC) to identify and react to the many events, incidents, and attacks against their information systems. SIEM’s roots are in the UNIX syslog approach to log file aggregation; for years, organizations and security professionals have sought ways to leverage existing systems and have them work together to maintain situation awareness, identify noteworthy issues, and enable response to adverse events.

A SIEM system supports threat detection and informs many aspects of threat intelligence. It is also instrumental in managing aspects of compliance and vulnerability management. It often plays a pivotal role in an organization’s security incident management through data collection and analysis by enabling near real-time and historical analysis of security events. It integrates data from multiple sources, including local events and contextual data sources. SIEM systems are derived from legacy log file monitoring systems and procedures.

AlienVault OSSIM (Open Source SIEM) provides a feature-rich, open source tool complete with event collection, normalization, and correlation. The software was created by security engineers because few open-source products were available to serve a critical need.

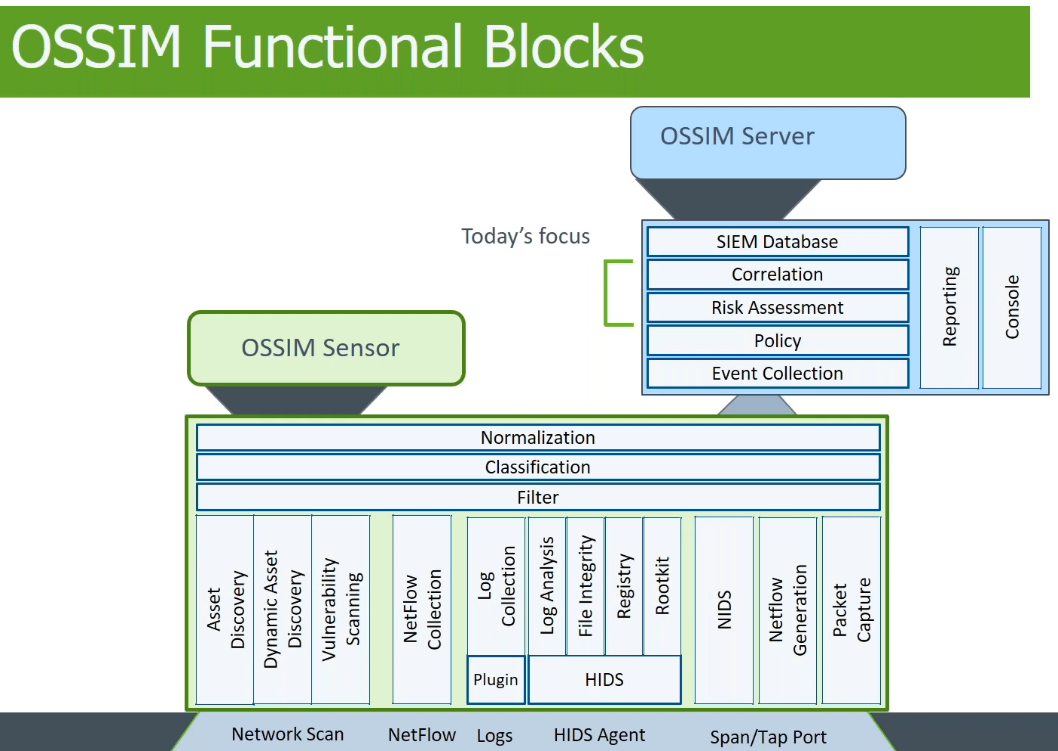
AlienVault OSSIM addresses the challenges faced by security professionals with a unified platform that provides essential security capabilities, including the following:

* Asset discovery
* Vulnerability assessment
* Intrusion detection
* Behavioral monitoring
* SIEM event correlation

The OSSIM environment shown in Figure L09-1 would be a typical setup in a corporate setting. In this example, a sensor is used to collect multiple data sources. It then organizes the data through filtering, classification, and normalization before the information is sent to the OSSIM server. This type of deployment is typical because it allows the enterprise to do the following:

1. Place the sensors close to the source of data to speed up processing.
2. Offload the processing between the two system components to prevent overloading.

Note the various types of processes performed and information collected at the sensor. The sensor is responsible for network scanning, NetFlow collection, log collection, host intrusion detection system (HIDS) collection, and raw network traffic captures (NIDS). Once these data sources are collected and processed based on the setup, they will be forwarded to the OSSIM server for further enrichment based on the policies and rules that have been applied. These policies and rules should place context around events and allow the collected data to be interpreted more accurately.



**Figure L09-1** OSSIM functional blocks

(Source: https://cybersecurity.att.com/forms/webcast-thank-you/getting-started-with-ossim)

This lab uses a proof of concept (POC) deployment in a virtual environment that combines the server and sensor in a single system. This setup is fine for purposes of the lab but should never be deployed in an enterprise environment except for testing.

## Objective

Upon completion of this activity, you will be much more knowledgeable about the AlienVault OSSIM software and how to install, configure, and operate it. You will use the software more extensively in a subsequent lab.

## Estimated Completion Time

If you are prepared, you should be able to complete this lab in 2-3 hours.

## Materials Required

Completion of this lab requires the following software to be installed and configured on your workstation prior to beginning the procedure steps:

* Microsoft Windows 10, or another operating system version as specified by the lab instructor
* VMware Workstation 16 Player (or similar version)
* Internet access to download the specified software

## Minimum System Configuration

To complete the labs included, it is recommended that you operate them from a computer system (desktop or laptop) that is running Windows 10 and has:

* Intel i5 or better CPU
* 8 GB RAM (minimum) - 16 GB RAM (recommended)
* 1 TB Hard Drive with at least 250 GB free (minimum) - 350 GB free (recommended)
* Microsoft Windows 10 or latest version

## Data From Your Instructor

Your course instructor or lab supervisor will provide these details:

|  |  |
| --- | --- |
| **Data** | **Value:** |
| A static IPv4 address assigned to their virtual OSSIM system |  |
| The subnet mask to use on the local network |  |
| The IPv4 address of the local network gateway |  |
| The IPv4 address of the DNS server |  |
| Root password (Created during installation) |  |
| Local time zone (Chosen during setup) |  |
| Administrator password (Chosen during setup and used through Web access) |  |

# Setting up AlienVault OSSIM

Work through the steps in the following sections to install and explore the AlienVault OSSIM software.

## Downloading and Installing VMware Workstation 16 Player

In the following steps, you will download and install a virtual host platform. If your lab instructor has provided you with instructions to use another version or another application, please follow those instructions.

1. Use a web browser to search for “VMware Workstation 16 Player download”. Locate the download link and download the free installer for your computer operating system. Run the installer allowing the permissions for it to be installed as it progresses. You may be asked to reboot your computer.

## Downloading and Installing AlienVault OSSIM

In the following steps, you will download AlienVault OSSIM, install it, and perform initial configuration setup for the software.

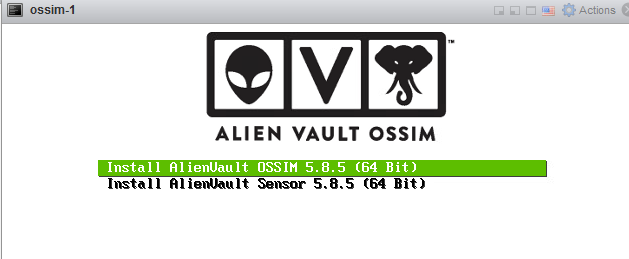
1. Go to <https://cybersecurity.att.com/products/ossim> and click the blue **Download AlienVault OSSIM ISO** button.

After you have downloaded the AlienVault OSSIM ISO file, you will install it to your virtual machine.

1. Start VMware Workstation Player and click the Create a new Virtual Machine link.
2. Choose the Installer disc image file (iso) option and click Browse.
3. When the navigation window opens, navigate to the folder where you saved the OSSIM ISO file, select the file, and then click Open.
4. When the navigation window closes, click Next.
5. In the Select a Guest Operating System window, click the Linux button, select Debian OS instance in the Version menu, and then click Next.
6. Give your virtual image a name, such as “OSSIM.”
7. Verify that the location is correct. If it is not, select the desired location.
8. Click Next.
9. Set the maximum disk size to 500 GB. Do not change the default option, “Split virtual disk into multiple files.” Click Next.
10. Click Customize Hardware.
11. In the left pane of the window, click Memory. Change the “Memory for this virtual machine” value in the right pane to 8192 MB.
12. Next, in the left pane, click Network Adapter, change the Network connection setting from NAT to Bridged, and then click Close.
13. Click Finish to complete the configuration of features in your virtual system.
14. To power on your virtual machine, click the Play virtual machine link.
15. If you are asked to download VMWare Tools for Linux, select Remind Me Later.
16. If you are using VMware Workstation as the host virtual machine, here is a recap of the needed parameters:

* Operating System (OS): Linux Debian 8 x 64
* Processors: 2 CPUs
* Memory: 8 GB
* Hard Drive: 500 GB (thin provisioned)
* CD-ROM: ISO File—point to the OSSIM ISO file you downloaded
* Network Interface Cards (NICs): Add three more NICs for a total of 4 NICs

1. When you have created the VM guest instance and initiated the Debian OS instance, select **Power on** in your virtual machine environment to launch the OS installation. In the installation screen shown in Figure L09-2, select **Install AlienVault OSSIM (64 Bit)** and press **Enter**.



**Figure L09-2** AlienVault OSSIM installation screen

1. The installation will take you through a series of setup options. Select appropriate options for the following settings. (The options used for testing are in parentheses.)

* Select Language: (English)
* Select Location: (United States)
* Keymap to use: (American English)

The installation then loads the necessary components and detects hardware settings.

1. Next, configure the network by assigning the following settings. (Your instructor may provide these addresses to you.)

* Choose the primary network interface. There should be four options; use **ETH0** for the primary interface.
* IP Address: Select an IP address on the network that you have been assigned by your instructor. If using your own network, choose an address that is not in use.
* Netmask: Usually 255.255.255.0
* Gateway: The IP address for the network router/gateway (for example, 192.168.1.1)
* DNS Server Address: Usually the network router/gateway

The IP address you provide will be the Web address you use to access the Web user interface (UI) for AlienVault OSSIM later in this lab.

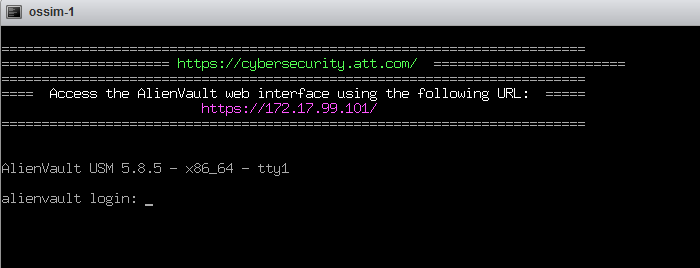
**Note**: Record these addresses for future reference.

1. The installer will have you set up the root password. This will be used for the root login account in the AlienVault OSSIM OS. A separate account will be set up for console access. Record your OS password.
2. When prompted, set up your time zone.

The installation proceeds. It could take 35 minutes or longer, depending on machine resources.

## Starting AlienVault OSSIM

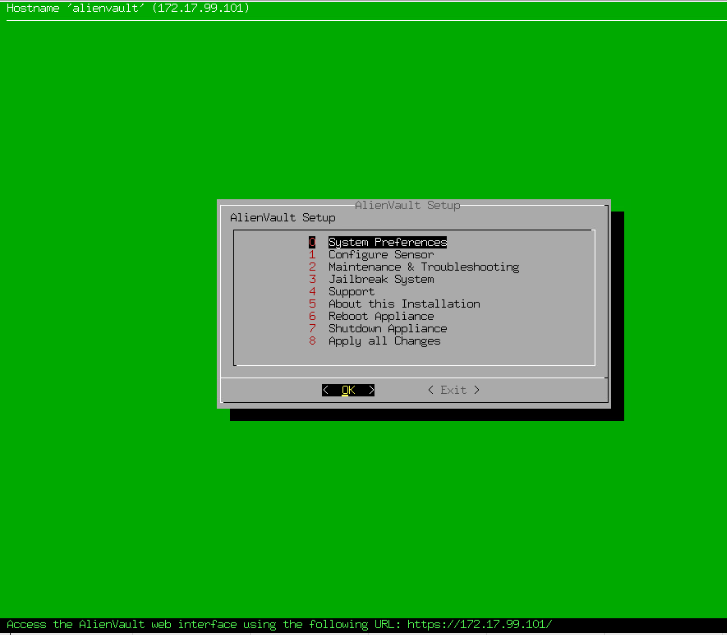
When the installation has finished and the system has rebooted, you should see a login screen like the one in Figure L09-3.



**Figure L09-3** Login screen that appears after installation

1. Log in to the system by using the root account and entering the password you designated during OS setup in the preceding section.

In the upper-left corner of the next screen, you should see the IP address assigned during installation (see Figure L09-4). The OSSIM console should display several options, but no further configuration should be required from this screen.



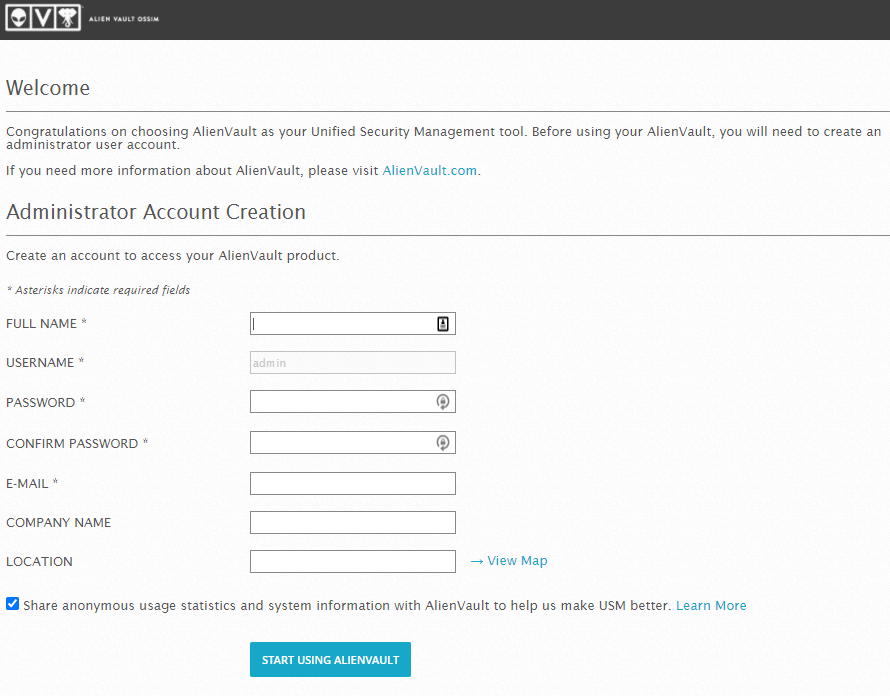
**Figure L09-4** AlienVault login management screen

## Web UI Access

The next step is to access the Web UI and set up your administrator account for console access.

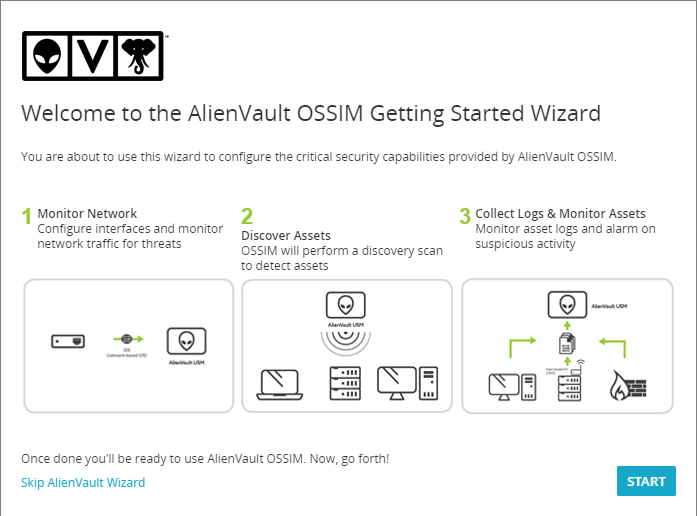
1. Open your web browser. In the navigation bar, enter the IP address you selected earlier in the setup process.

If the browser displays a connection privacy warning, click **Advanced** and then click **Proceed to *<the IP address you entered>***. You should see the page shown in Figure L09-5.



**Figure L09-5** Administrator account creation

1. Create an administrator account on the Welcome page by filling in all the fields that have an asterisk (\*) next to the field names. The username should be “admin.”
2. When you have completed the screen shown in Figure L09-5, a login screen appears. Log in to the system using **admin** as the username and the password created in the preceding screen.
3. Click **Login** to enter the Web UI. The program’s Getting Started Wizard appears, as shown in Figure L09-6.

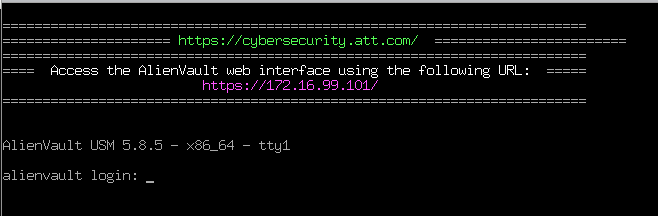


**Figure L09-6** AlienVault OSSIM Getting Started Wizard

1. Take a screen shot of this screen to submit to your instructor to show completion of the setup.
2. In the lower-left corner of the window, click **Skip AlienVault Wizard**. The system is ready to use.

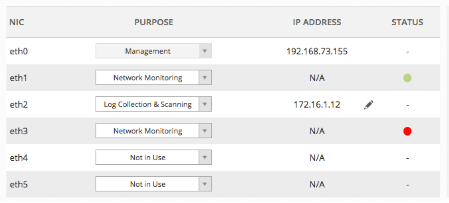
# Configuring and Using AlienVault OSSIM

1. If it isn’t already running, start the AlienVault OSSIM server in the virtual environment that was installed in the Module 7 lab. The system might take a few minutes to start completely. When the system is running, the virtual machine should display a login prompt, as shown in Figure L09-7.



**Figure L09-7** AlienVault login prompt

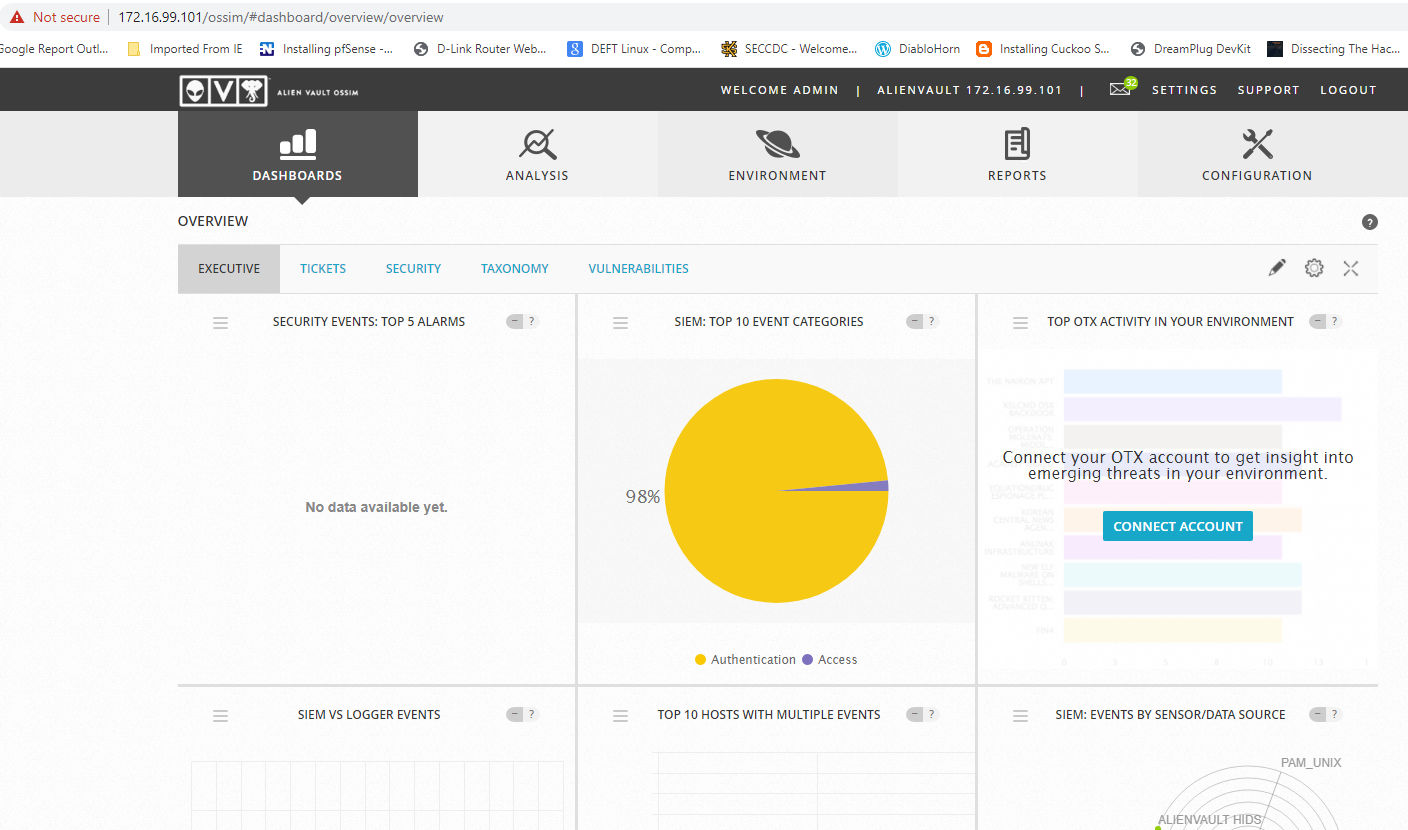
1. Open a web browser on the local machine and navigate to the IP address you used in the previous lab by entering **https://** followed by the IP address. A login screen should appear. If the browser displays a connection privacy warning, click **Advanced** and then click **Proceed to *<the IP address you entered>***.
2. Log in through the web browser using **admin** as the username and the password you used previously.
3. When you first log in to OSSIM via a web browser, the OSSIM Getting Started Wizard appears. This wizard is the easiest way to get a system up and running. You will not use the wizard in this lab but note that it provides the easiest way to configure multiple network interfaces for the OSSIM. Figure L09-8 shows how multiple network interfaces may be configured for various components of the SIEM system.



**Figure L09-8** Network interfaces

The primary interface eth0 will be the management interface; this interface was set up during the initial installation in the previous lab. The IP address is the same one you used to log in through the web browser. Another IP address is used to collect log files for ingestion. In this case, administrators can forward syslog files from a firewall or other devices of interest to OSSIM using that IP address. Also, two network cards are configured for network monitoring. The interfaces would either collect raw packet data (sniff) or be connected to a device that sniffs network traffic, like a terminal access point (TAP). To collect this information, the network cards must be in promiscuous mode. Monitoring network traffic at this level requires special permissions from the network owner; in a virtual environment, it also requires a special configuration in VMware.

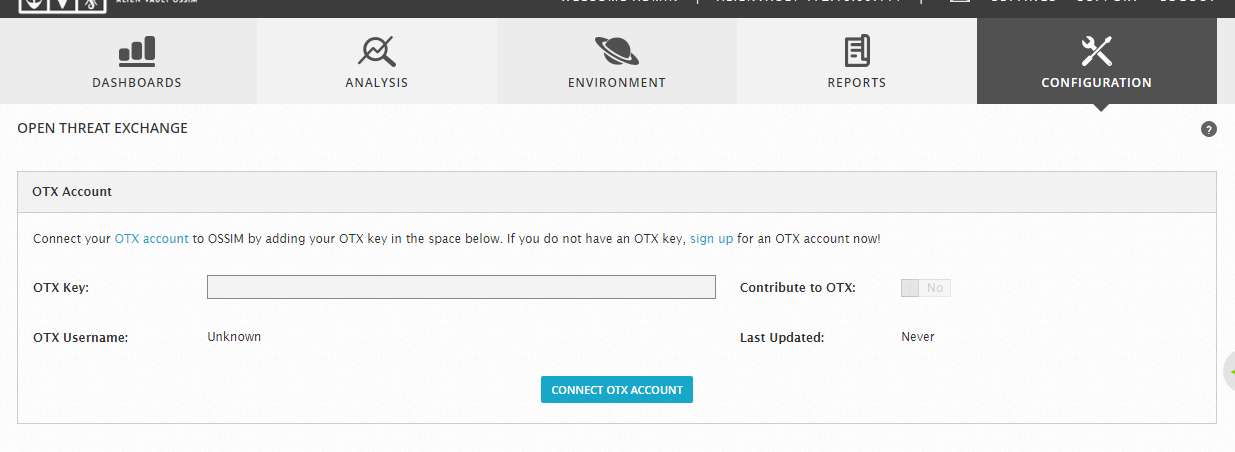
1. If the OSSIM Getting Started Wizard does appear, click **Skip AlienVault Wizard** in the lower-left corner.
2. Take a moment to examine the next screen that appears (see Figure L09-9). The top part of the screen displays who is logged in, the IP address the system is using, the internal system e-mail, a Settings menu, a Support menu, and a logout option. The Support menu provides a wealth of information about OSSIM setup and use. The next part of the screen displays five tabs—Dashboards, Analysis, Environment, Reports, and Configuration—that can be used to configure, monitor, and report on the environment.



**Figure L09-9** AlienVault OSSIM dashboard

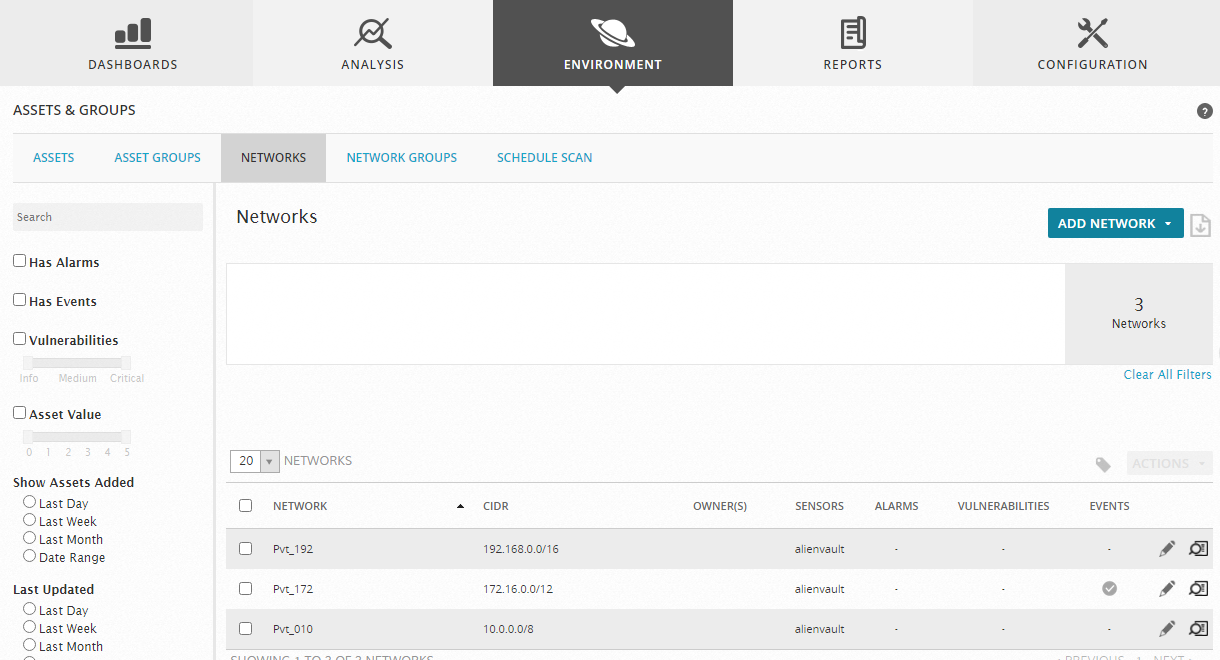
1. AlienVault OSSIM is designed to interface with the AlienVault OTX (open threat exchange). This service includes both free and paid subscriptions that provide open-source intelligence (OSINT) to Alien Vault OSSIM and can provide information and further context around malicious traffic and alerts in the environment. Analysts can sign up for this service, but it is not required in order to complete the lab assignment.

If an analyst signs up, he or she will receive an API key that can be applied to OSSIM to allow OTX to interface with the system. Click the **Configuration** tab and then click **Open Threat Exchange**, as shown in Figure L09-10. You can add the API key and choose whether you want to share information with OTX from your environment. If you have registered for an account with OTX, you can add the key here or register and get a key.



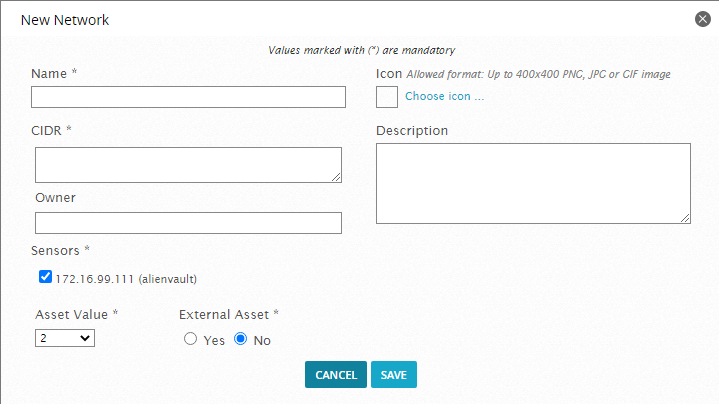
**Figure L09-10** AlienVault OSSIM open threat exchange

1. The next step is to define your network and perform an asset discovery. Click the **Environment** tab, click **Assets & Groups**, and then click the **Networks** tab, as shown in Figure L09-11.



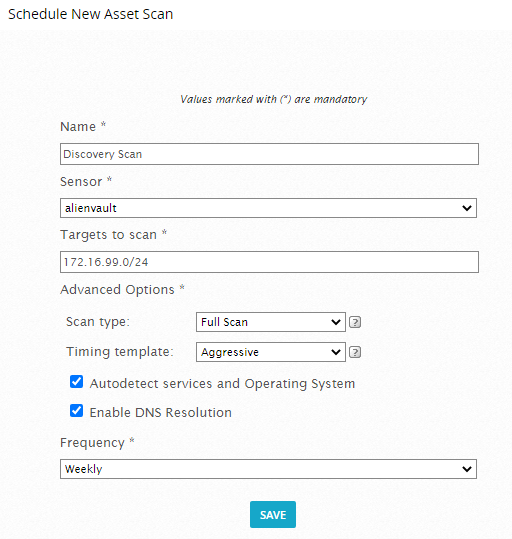
**Figure L09-11** AlienVault OSSIM Environment tab

1. You should have your network defined via CIDR notation in this tab. If you need to add a network, click the **Add Network** button on the right side of the page. You should see the window shown in Figure L09-12. For example, to capture a 192.168.1.0 network, you should enter 192.168.1.0/24; for the full range, enter 192.168.0.0/16. Other metadata can also be added, such as asset value, which allows for more emphasis to be placed on higher-value network assets (1 is the lowest value and 5 is the highest).



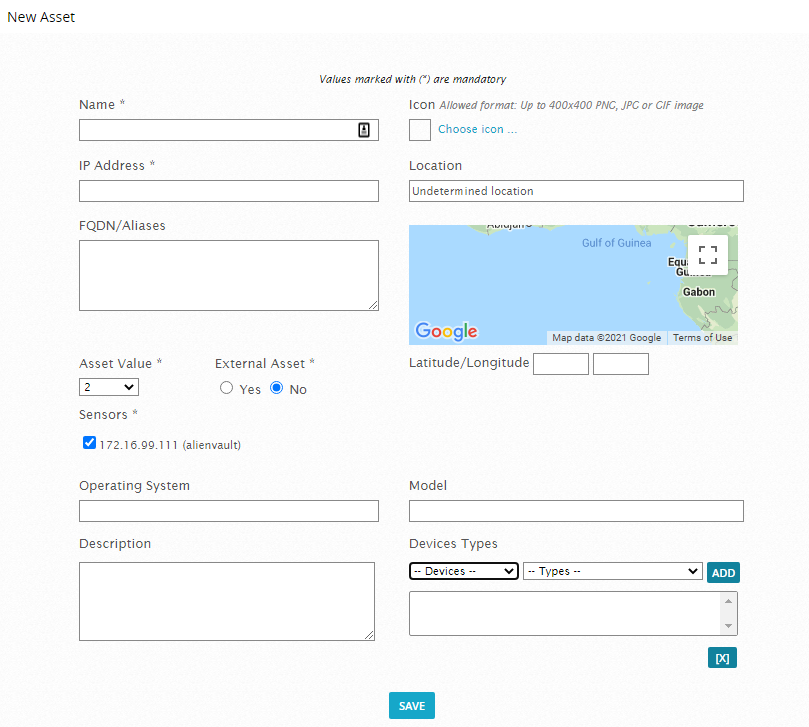
**Figure L09-12** AlienVault OSSIM new network entry

1. Still in the Assets & Groups menu, click **Schedule Scan** to see a list of scans set up in OSSIM. (Note that OSSIM uses Nmap for scanning and asset discovery.) To create a new scan, click **Schedule New Scan** on the right side of the window. The window shown in Figure L09-13 appears. Provide a name, sensor, targets to scan, scan type, timing template, and scan frequency. The Nmap tool will begin to scan when these settings are saved.



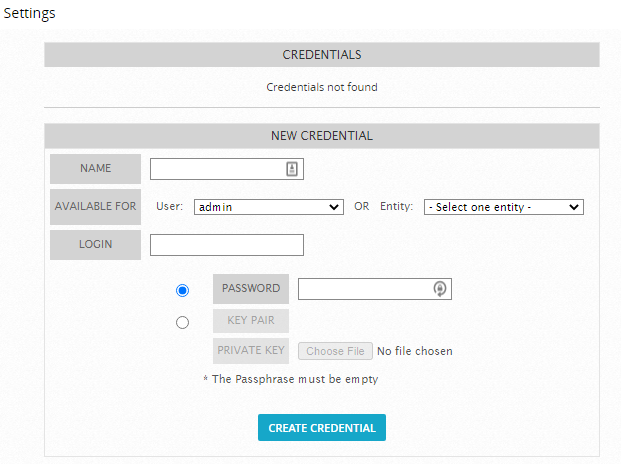
**Figure L09-13** AlienVault OSSIM new asset scan

1. To see what assets have been discovered, click the **Assets** tab under the Assets & Groups menu. You can also click the **Add Assets** button on the right side of the screen to add more assets. Figure L09-14 shows the New Asset window.



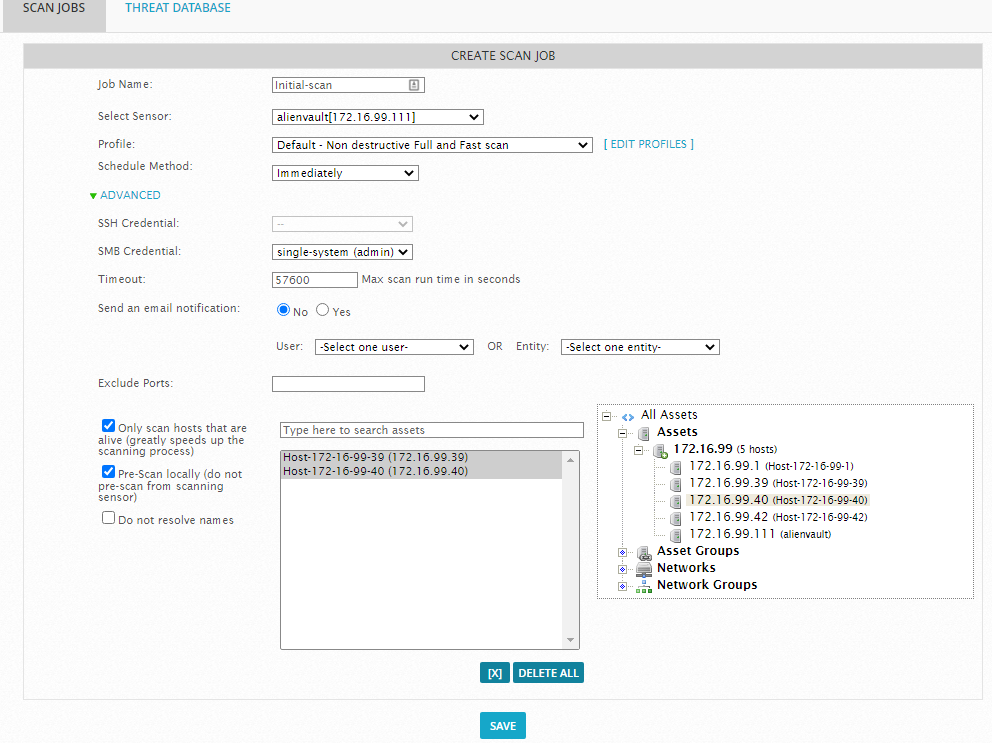
**Figure L09-14** Adding new assets

1. Next, you configure a vulnerability scan for the environment. Click the **Environment** tab at the top of the screen and then select the **Vulnerabilities** menu. OSSIM uses the Open VAS vulnerability scanner.
2. When scanning for vulnerabilities, it is preferred to use valid credentials, but not required. You can skip this step, but note that an analyst could click the **Settings** button on the right side of the screen and then enter a credential set into the system, as shown in Figure L09-15. For example, an analyst could enter credentials for one Windows system and scan one system in the environment.



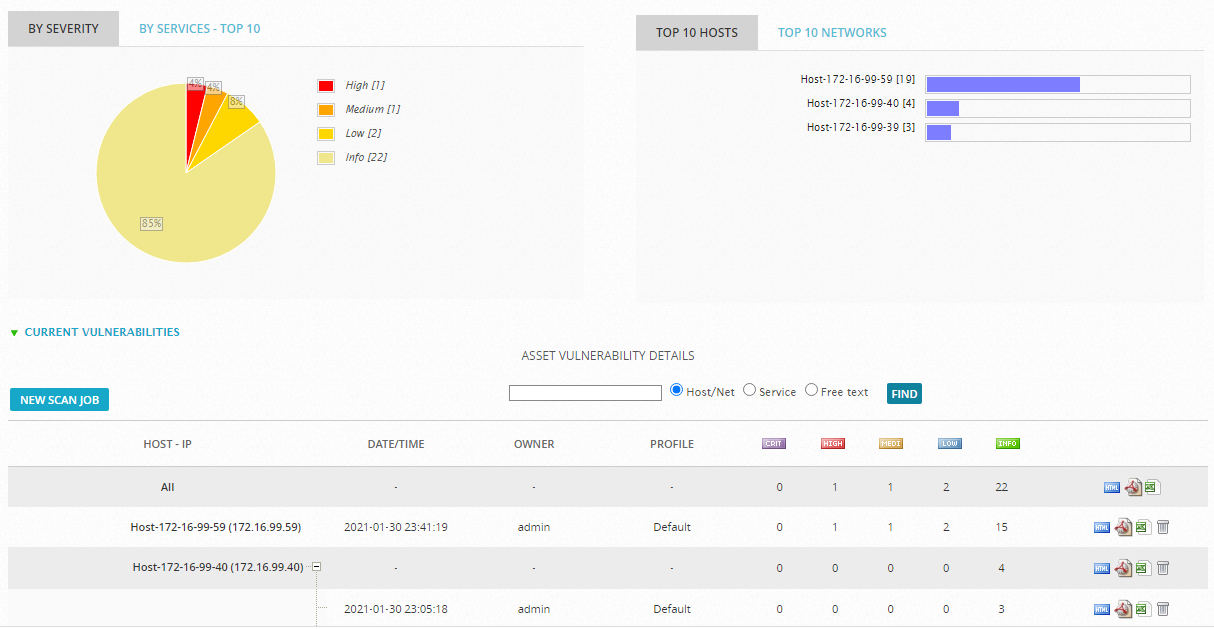
**Figure L09-15** New credentials entry in AlienVault OSSIM

1. Still under Vulnerabilities, click the **Scan Jobs** tab and then click the **New Scan Job** button on the left side of the screen. Provide a job name, select a sensor, choose the default profile, and schedule the scan to occur immediately. You can also choose particular assets to scan from the tree on the lower-right side of the screen, as shown in Figure L09-16. Click **Save** when you finish. The scan should start in a minute or so. Be patient; it will take a while to complete.



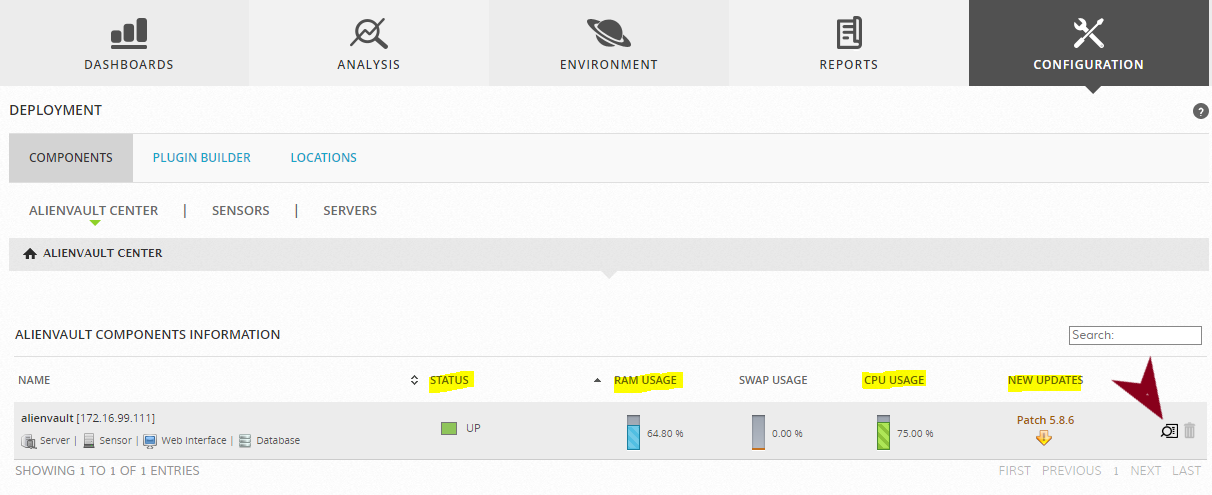
**Figure L09-16** Creating a scan job in AlienVault OSSIM

1. Once the vulnerability scan is complete, click the **Overview** tab to see the scan results. Figure L09-17 shows an example of information from a vulnerability scan. OSSIM provides a view of the overall vulnerabilities in the environment and a list of vulnerabilities found for each machine. Reports are available in HTML, PDF, and CSV format.



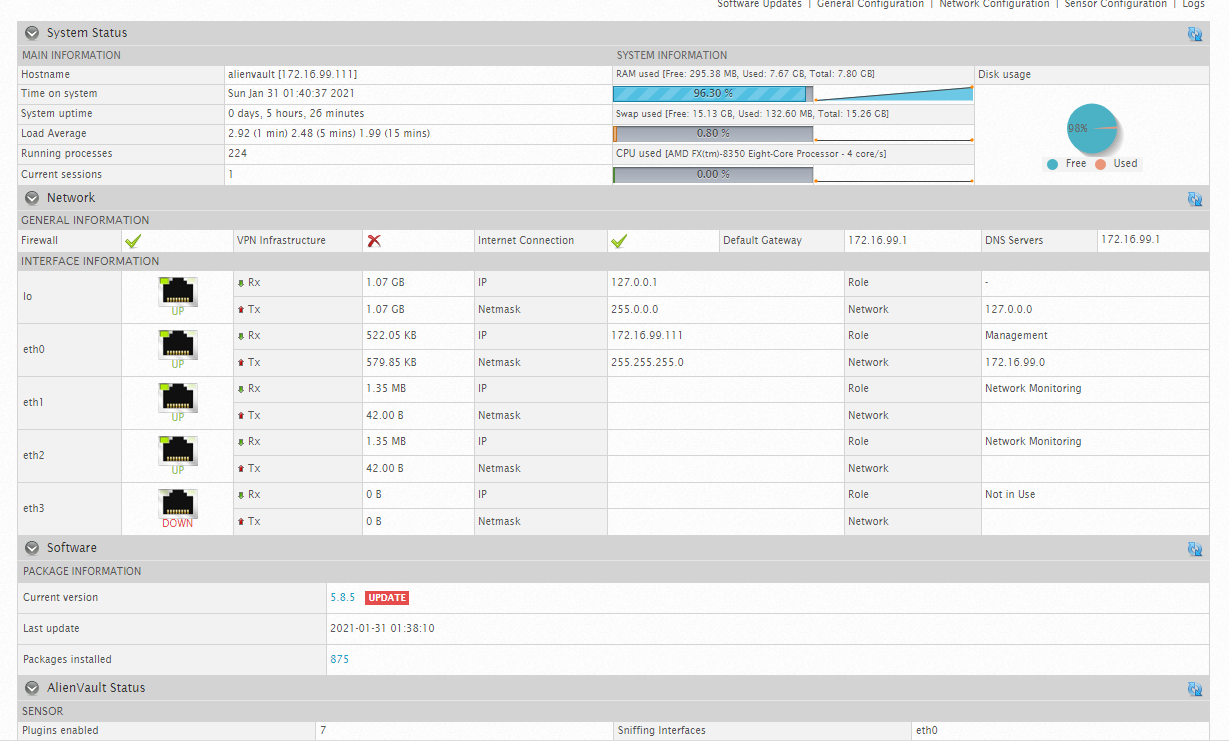
**Figure L09-17** AlienVault OSSIM scan results

1. This lab comes with a report from a Windows 7 system that should clarify what the scanning tool can do. Open the **LM8-Vulnerability-AV-OSSIM-ScanResult.pdf** file and review the report.
2. Next, you will review the network intrusion detection system (NIDS). Click the **Configuration** tab and select **Deployment** from the menu to see the window shown in Figure L09-18. This window provides detailed information about system status, RAM usage, CPU usage, and new updates that are available.



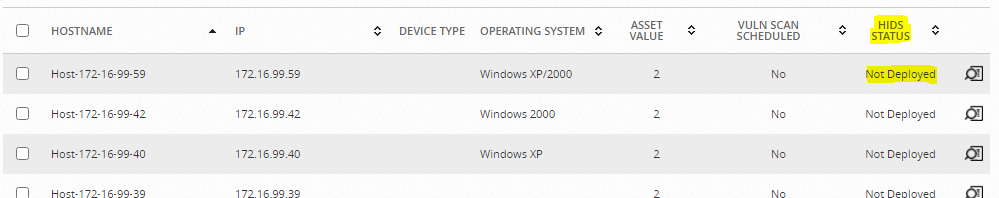
**Figure L09-18** AlienVault OSSIM Configuration tab

1. To get a more detailed view of the current system, click the **spyglass** icon indicated by the arrow in Figure L09-18. (*Do not* click the trash can icon.) The detailed view of the system status page is shown in Figure L09-19. Current RAM and CPU usage is displayed in addition to the assigned values of network cards and how much traffic they are receiving. You can use this view to check that NIDS devices are receiving traffic.



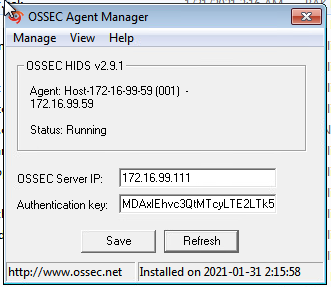
**Figure L09-19** AlienVault OSSIM system status view

1. OSSIM also has a host intrusion detection system (HIDS) component and several versions of agents ready to deploy. Click the **Environment** tab again and select **Assets & Groups** from the menu. Examine the individual devices on the resulting page, as shown in Figure L09-20. OSSIM shows whether an HIDS agent has been deployed to each device. Select the **spyglass** icon next to Not Deployed to open the Assets Details page.



**Figure L09-20** HIDS status

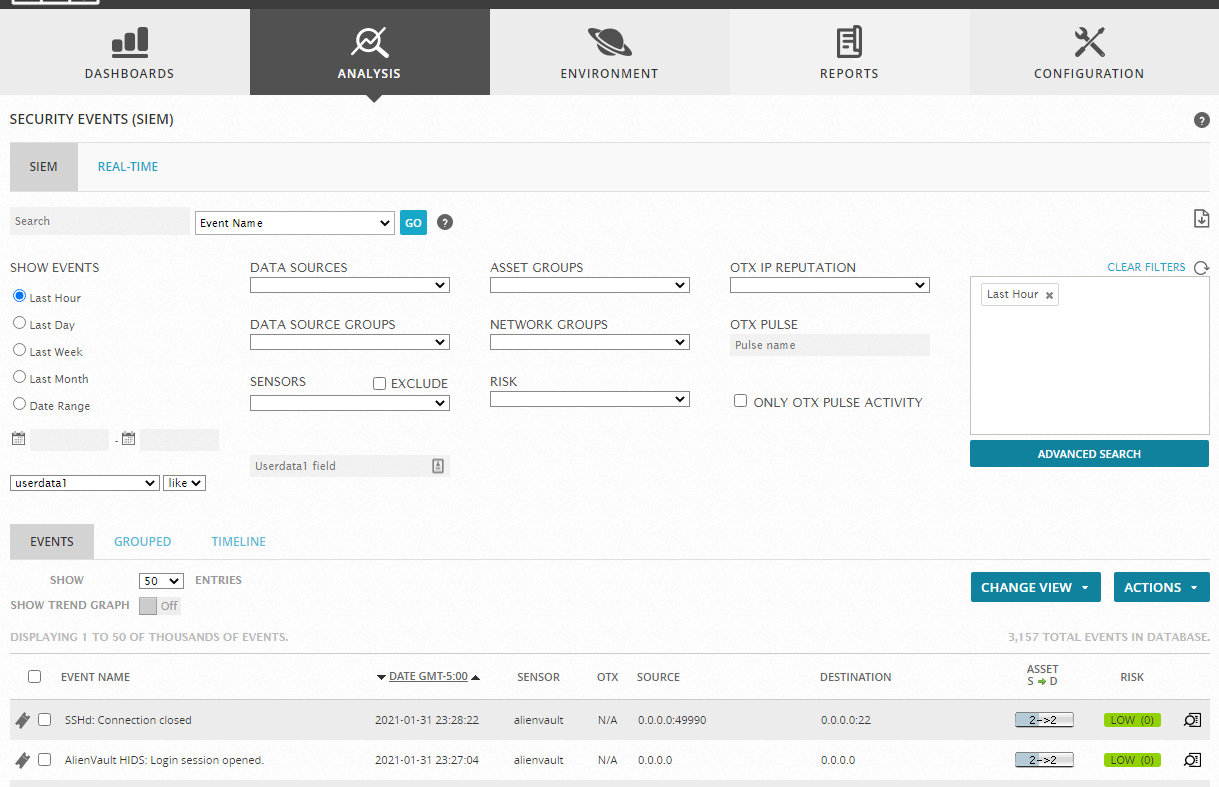
1. On the right side of the window, click the **Action** button and then choose the last option, **Deploy HIDS Agent**.
2. The Deploy HIDS window appears. Enter the correct username and password for the selected system, and enter the domain name if the system is within an enterprise. An HIDS agent will be deployed, although the process will take a few minutes. When the agent has finished installing without error, you can check the target system files under C:\Program File (x86)\ossec-agent\ to confirm the installation. If you see the directory, you can look for a file named **win32ui.exe** and launch the application. Compare your results to those in Figure L09-21 to see if the installed service is running. If the ossec-agent directory is missing, a manual installation is required.



**Figure L09-21** Deploying HIDS agent credentials in AlienVault OSSIM

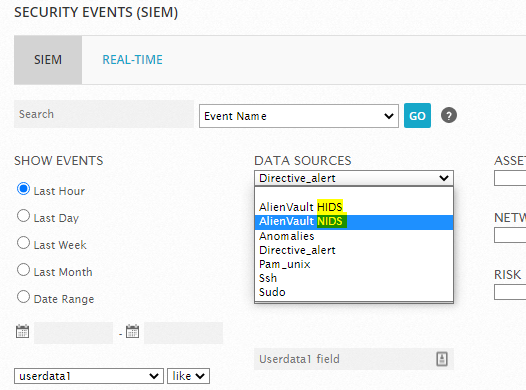
You have completed the basic setup routines for AlienVault OSSIM. However, there are many more functions to consider when working in an enterprise environment. For example, you did not learn about specific plug-ins for other devices that assist in processing incoming data, such as logs.

1. When the SIEM system is processing the required data, you can go to the area of the software where analysts will spend most of their time. In the OSSIM console, click the **Analysis** tab and then choose **Security Events (SIEM)** from the menu to see the window shown in Figure L09-22.



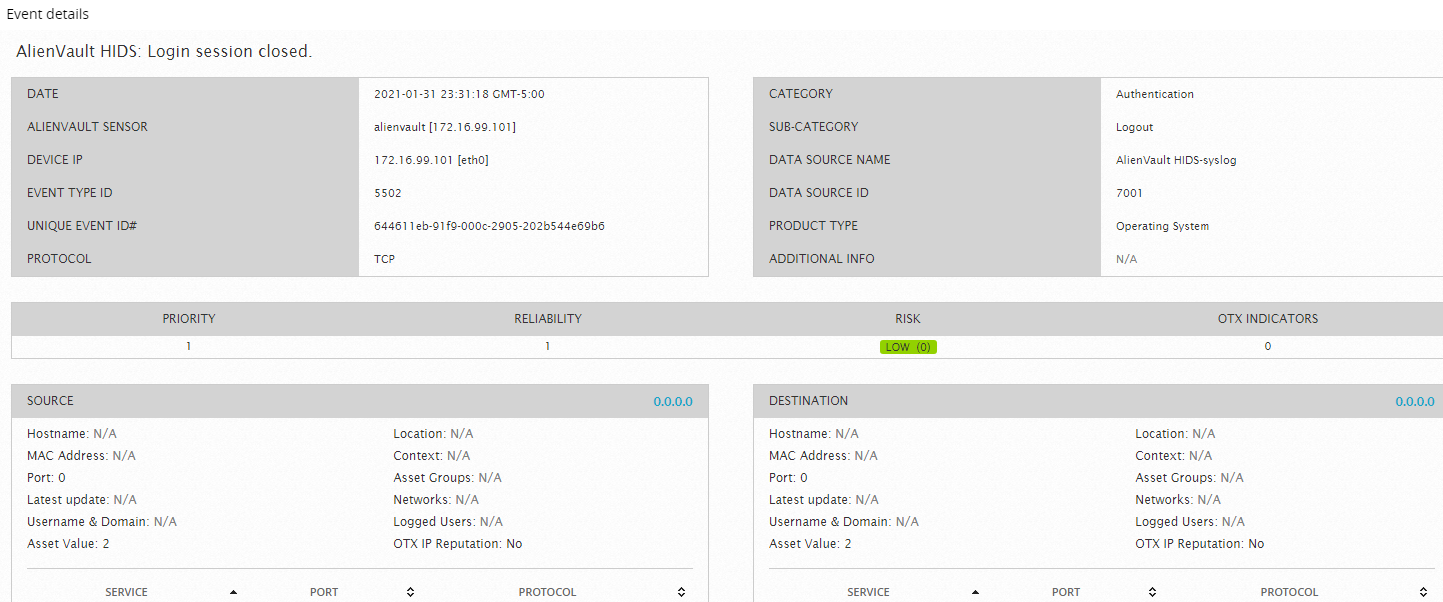
**Figure L09-22** AlienVault OSSIM Analysis tab

1. Note the various drop-down menus and ways to look at the information from the SIEM system. There are multiple ways to track down events. There are prebuilt time filters on the left side of the screen as well as custom dates and times that you can set. The bottom of the screen presents individual events as they are processed. The Data Sources menu includes multiple options for sorting events, most notably from HIDSs and NIDSs, as shown in Figure L09-23.

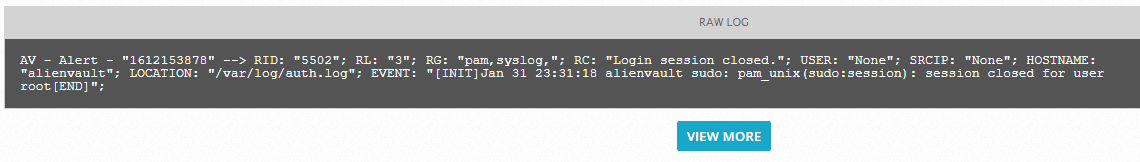


**Figure L09-23** AlienVault OSSIM data sources

1. An analyst can also click an event of interest to see more details about it. Scroll down to the bottom of the detailed event view (Figure L09-24) to see the raw event log that generated it (Figure L09-25).



**Figure L09-24** AlienVault OSSIM event details



**Figure L09-25** AlienVault OSSIM raw log file

You have completed a basic walk-through of the OSSIM console and its configuration. Many more components, plug-ins, and modifications can be added to tune the OSSIM system for better reporting and performance. Consolidating the large amounts of data required in an enterprise is always complicated. The more accurate the SIEM system’s reporting is, the less time is wasted tracking down meaningless alerts.

# Self-Reflection and Response

Attach the screen shot taken at completionof OSSIM setup or insert it here.

Were you able to complete the setup, configuration, and use of OSSIM?

|  |
| --- |
|  |

If you were not able to complete the setup and configuration, explain what went wrong.

|  |
| --- |
|  |

## Instructor’s Response

|  |
| --- |
|  |