## AlienVault

# Unified Security Management

AlienVault, the company with the cool logo, has really outdone themselves with the Unified Security Management Platform (USM). This is a next-generation product at a low-end SIEM price. The version we evaluated came pre-loaded on a server, but you can put it in your virtual environment with no trouble. You can download the VM for a 30-day free trial as well. It appears that AlienVault has coined a new class of product: the USM. Functionality is excellent and includes traditional SIEM, discovery, vulnerability assessment, intrusion detection and behavioral monitoring. It pulls all of these pieces together and applies sophisticated analytics to pinpoint threats and problems that may have started to occur on the enterprise. It is an excellent example of the marriage of SIEM and UTM.

The product comes mostly configured with host and network IDS that look in both directions. This can pinpoint malicious communications from a piece of malware to its command-and-control (C2) mothership. The host IDS reads Windows logs adding context to the overall threat picture. AlienVault provides its own brand of threat intelligence with a bit of a twist: A crowd-sourced web portal called the AlienVault Open Threat Exchange (OTX). Here members of the forum upload indicators of compromise (IOC). These are useful even if you do not have an AlienVault implementation since the IOCs are applicable to any threat hunt.

The tool provides traditional syslog consumption from just about any device that generates syslogs, as well as NetFlow consumption for anomaly detection and validation of suspicious behavior. All of these sources are fed to the threat correlation engine which provides coordinated threat management – taking advantage of threat feeds, vulnerabilities, discovered threats inside the enterprise and context from such sources as OTX and NetFlow data.

We hooked up the product to our test bed and network and without any trouble and logged into the appliance. The first step is the usual configuration with a console. This allows you to set up network parameters that will allow remote web-based access for the rest of the setup process.

Once we had the device online, we started with it discovering our test bed and gathering data. There is a lot you can do to get at the real power of the product, but it is very useful to be able to start with a known working environment before you start adjusting it for your enterprise. Documentation is superior, easily accessible and covers all of the aspects of setting up and using the tool. Support is good and price is unbelievably low given the power of the product. This is a very good value and it lives up to all the positive responses you may have heard about AlienVault. – *Peter Stephenson, technology editor*

## DETAILS

**Vendor** AlienVault

**Price** $5,050 for virtual appliance.

**Contact** alienvault.com

| | |
|---|---|
| Features | ★★★★★ |
| Performance | ★★★★★ |
| Documentation | ★★★★★ |
| Support | ★★★★★ |
| Value for money | ★★★★★ |

**OVERALL RATING** ★★★★★

**Strengths** Significant, mature next-generation blend of SIEM and UTM capabilities at a very reasonable price. Outstanding customer relationship building.

**Weaknesses** None that we found

**Verdict** For its powerful, mature feature set, performance and superior value we make this our Best Buy.

ALIEN VAULT
**1875 S. Grant Street • Suite 200**
**San Mateo, CA 94402**
**+1 650 713-3333**
**www.alienvault.com**