AlienVault®

Unified Security Management™ (USM™)

We have been using the AlienVault tool in the SC Labs for over a year. It is already an SC Lab Approved product and we will be looking back at it in our One Year Later segment in a future issue. As a UTM, this is one of the top tools we've come across. We use it to monitor some of the more exotic tests that we do. Setup is very straightforward and we had it online in about a half-hour, completely configured and taking data.

This is a very good example of a UTM that starts with a very good broad picture and lets you drill down as far you want. But this is really something more than a UTM. The functionality it provides is asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and SIEM log management. There is integrated threat intelligence and it takes and provides feeds from and to the community through the Open Threat Exchange™ (OTX™). We have found the OTX extremely valuable on a variety of levels. Because it provides indicators of compromise, it gives valuable input to the appliance on a continuous basis.

There also are some excellent SIEM functions as well, including log consolidation for syslogs, Windows event logs, CEF, MySQL, MS SQL, and NetFlows. It comes complete with host and network intrusion detection – which can be agent-based or agentless. For threat correlation, AlienVault uses 3,500 built-in "correlation directives," each of which consists of one or more correlation rules. These are constantly being updated through the Threat Intelligence Subscription.

There is an excellent incident management system and, although we don't use it in the SC Labs, it includes a first-rate ticketing and workflow management system. What we do use in the SC Labs is its forensics capability. In addition to providing excellent analytical resources, everything is encrypted and forensically preserved.

There is a virtual appliance version that can run VMware or Hyper-V. There also is a software version that can be deployed on server.

We are especially impressed with AlienVault support. As we were getting ready to review the product, we found that we needed to upgrade our device. We followed the instructions in the excellent documentation and next morning the sliding "busy" bar still was sliding happily back and forth. That didn't make us quite so happy though, so we called support expecting a long drawn-support call. We were escalated immediately to a higher-level support engineer who logged into our appliance through a screensharing session and in well under an hour we were up and running, with upgrade completed, problem identified and escalated to engineering team.

– Peter Stephenson, technology editor

DETAILS

Vendor AlienVault

Product Unified Security Management (USM) Appliance

Website alienvault.com

Price Starts at $5,595 for SMBs.

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

OVERALL RATING ★★★★★

Strengths Solid correlation of events, first-rate forensics and loads of features at a very attractive price.

Weaknesses None that we found

Verdict Not much to say here besides that this product is SC Lab Approved and that is our highest designation. This is one of the best UTMs we've tested and over long periods of use it has delivered very well. We make it SC Lab Approved for another year.

AlienVault, Inc
1875 S. Grant Street
Suite 200
San Mateo, CA 94402
www.alienvault.com
Tel: +1 650 713-3333