CASE STUDY

Securing the Infrastructure So People Can Go Skiing

ORDA (New York's Olympic Regional Development Authority) is a state authority, established after the 1980 Olympics to manage two ski resorts and several Olympic sites as facilities for public recreation and world-class sporting competitions. I joined ORDA about 7 years ago, and I'm the focal point for information security. As Information Security officer, I'm the only person in our eight member IT Department dedicated to security. This puts me in charge of user awareness and security training, managing preventative technologies, and monitoring for anomalies and indicators of compromise. ORDA is a great place to work; I occasionally arrange my schedule so that I can take a long lunch on skis (cellphone in hand, of course).

Our business is seasonal, so we hire quite a few employees in the fall. This provides the opportunity for special security indoctrination for new employees, and security training for the rest of ORDA's staff. To reinforce this, I send written security updates to employees, reminding them to be vigilant. I encourage employees to contact me if they see something suspicious. There's no point in belittling users or blaming victims for clicking on a malicious link. The last thing I want is for a user to click a malicious link, realize that it was a mistake, and want to hide the fact for fear of reprisal. I want users to alert me so that I can address security issues as soon as possible.

"As for preventative measures, we have standard perimeter firewalls and anti-virus, but it's not enough to ensure our security."

-Kevin Geil, Security Officer, NYS ORDA

Company name: New York State Olympic Regional Development Authority (ORDA)

Industry: Primary: State Government

Secondary: Ski resort, Olympic development

Headquarters location: Lake Placid, NY

Employee count: N/A

Website Link: www.orda.org/corporate/

As for preventative measures, we have standard perimeter firewalls and anti-virus, but it's not enough to ensure our security. When we acquired a third ski resort in 2012, we made some changes to the way we handled credit cards, and were required to implement a log management solution in order to be PCI compliant.

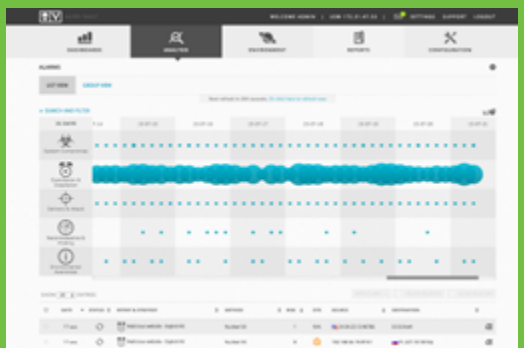
We did a full competitive comparison of log management tools. We reviewed AlienVault, LogRythm, Splunk, HP ArcSight and Solarwinds Log and Event Manager. We chose AlienVault Unified Security Management (USM) because it offered more than the other products, at a similar (or better) price. In addition to log file management, AlienVault includes a whole set of integrated capabilities that we continue to roll out over time.

We purchased AlienVault in 2012, and started rolling it out in the fall. We started with implementing OSSEC host intrusion detection. This enables me to watch Active Directory changes with a keen eye toward privileged account use, escalation, and group membership changes. With OSSEC, I can drill down to see which administrator

did what on which machine. Privilege escalation and group membership changes can be indicative of suspicious behavior, and sometimes leads to further investigation.

One of AlienVault's powerful features is the Network Intrusion Detection (IDS), using Snort and Suricata that comes with USM. It relies on packet sniffing to spot exploited vulnerabilities and indicators of compromise. I'm in the process of tuning it for my environment, and have been expanding its deployment from my first site to all locations this spring. I also use the behavioral monitoring capability with Netflow on two of my four remote sensors.

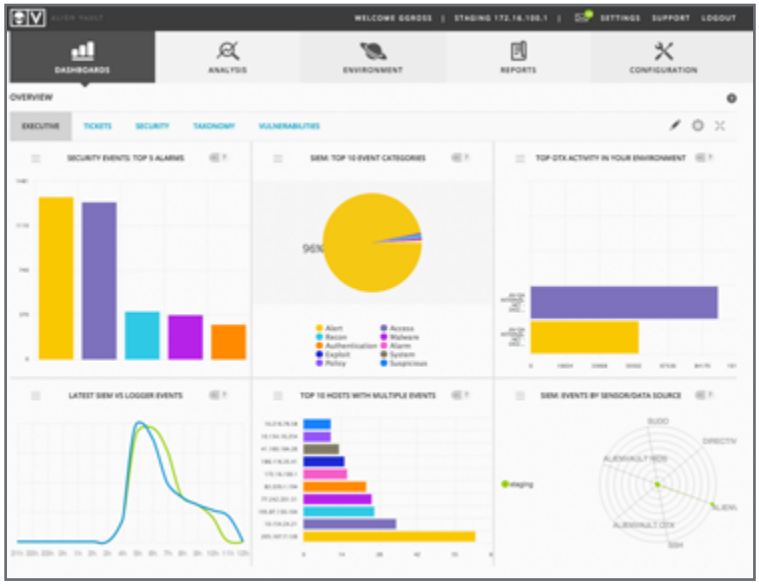
Open Threat Exchange (OTX) is very useful, primarily when investigating potential incidents and indicators of compromise. I'm not yet monitoring ORDA's IP addresses with it, but that's on my list for the near future, perhaps even this afternoon.



"We chose AlienVault Unified Security Management (USM) because it offered more than the other products, at a similar (or better) price."

– Kevin Geil, Security Officer, NYS ORDA

As the "lone security ranger," there are a lot of things that keep me up at night. Foremost is the potential for a credit card data breach. I'm also concerned about malware getting on our systems, and I'm glad I have USM to provide the ability to detect malware and help us stay PCI compliant. After all, I like to have time to hit the ski slopes now and then!



Key Benefits:

#1 - NYS ORDA began reviewing security products when they made changes to the way they handled credit cards and were required to implement a log management solution in order to be PCI compliant.

#2 - OSSEC host intrusion detection allows NY ORDA to watch Active Directory changes with a keen eye toward privileged account use, escalation, and group membership changes.

#3 - NY ORDA finds AlienVault's Open Threat Exchange (OTX) very useful when investigating potential incidents and indicators of compromise.

START YOUR FREE TRIAL ▸