CASE STUDY

No Security Operations Analyst Required

Little green aliens help City of Lewiston protect their network

Founded in 1861, Lewiston, Idaho is the second-largest city in northern Idaho and ninth largest in the state with a population of 31,894 as of 2010. The city's official website contains a wealth of information on city departments, upcoming events, visitor questions and much more. The IT department for the city consists of five full time employees. Daniel Santiago is the System Administrator for the city and a large part of his job has become ensuring that his network is secure.

Because it is a city network, Santiago and his team are responsible for the security of all the public Wi-Fi spots in the city. In addition, the City of Lewiston is responsible for the security of the county network, however that network is managed by a separate IT team. Santiago's team is also responsible for maintaining the availability and security of online bill pay for municipal services like water, garbage and other public services.

When he first started at City of Lewiston, Santiago was using Spiceworks' free software to monitor his network and help him detect threats. He said it was here that he first learned about AlienVault's security feature integrated into Spiceworks. "One day while I was at work I noticed that my Spiceworks installation was reporting that a machine I was monitoring was communicating with a known 'Bad IP.' There was a little green alien face next to the alert that I had never seen before," said Santiago. After noticing the alert, he clicked down to the AlienVault Open Threat Exchange (OTX) page to find the attack history relating to the offending IP. He then blocked the IP before it could do any potential harm to his network.

Customer Profile

Company: The City of Lewiston

Industry: City-Local Government

Country: United States of America

Employees: 400+

Website: www.cityoflewiston.org

START YOUR FREE TRIAL ▸

"It's pretty incredible that AlienVault USM has truly allowed us to perform the work of a security operations analyst. The overall experience has been stellar and I have highly recommended AlienVault to everyone I come across"

-Daniel Santiago, System Administrator
City of Lewiston

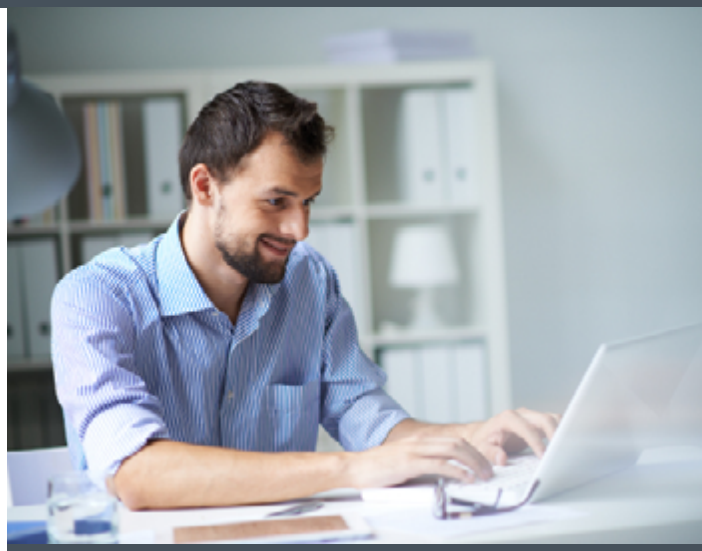
The little green alien face that alerted Santiago to a potential malicious IP was part of AlienVault's free threat alert tool that comes built in with Spiceworks software. It detects connections with known malicious hosts based on threat data from the AlienVault Open Threat Exchange (OTX).

After using AlienVault's threat tool for some time, Santiago said he began considering a paid security product with more functionality built in. "We looked at other companies that reported to be a SIEM as well. We were not as interested in log management and correlation as we were the SIEM side of things. We looked at Splunk and a few others, but ultimately realized the majority of the tools we considered required someone with the skills and training of a security operations center analyst to use them properly."

Being IT generalists, Santiago and his team didn't have the time or training to make sense of the data they were being provided by the tools they trialed. "For example, when we were demoing Splunk we found that it acts as a log gathering and index tool first. Then it requires you to spend all of your time looking at the logs to find patterns and problems where you can then create the alarm rules based off of what you find."

Although many of the products he reviewed had predefined rules, Santiago said it was still a challenge to update them and determine what exactly they were looking at in each log. "During the Splunk demo, every single 'attack' they were showing us in the test environment involved the host going through a minimum of 4-6 pages and clicks to drill into a problem and see what it was referencing," said Santiago. "I had my entire team look at the screen and log what was being shown and none of us had any real grasp of what we were seeing or how it would be bad." After many similar demos, Santiago and his team came to the conclusion that those products would only benefit them if they hired a security operations center analyst to implement and maintain the product. The high cost of hiring a security operations analyst and the additional training required for the tools they passed on convinced them that they needed to find a different approach. "The cost of an additional staff member trained in security that would be capable of doing the work would cost us around $50-70K a year in salary not including benefits," said Santiago.

Santiago said that when his team was shown a demo of AlienVault they got a different feeling than their experience with the competitors. They determined that with AlienVault they would be able to get a lot of value out of the product without having to hire a security operations center analyst. "We saw AlienVault as cutting out the middleman and possible 'telephone game' in our security."



Key Benefits:

#1 - City of Lewiston saw AlienVault as cutting out the middleman and possible "telephone game" in their security.

#2 - After only a few days of turning on AlienVault, City of Lewiston was able to discover that a former employee was attempting to regain entry to their network.

#3 - City of Lewiston found that, unlike other products, their team would be able to secure their network without the need to hire a security operations center analyst.

START YOUR FREE TRIAL ▸

Santiago and his team decided to run a proof of concept (POC) with AlienVault in August of 2014. “When we first turned on the Virtual Appliance for the POC we discovered after a few days of auditing that a former employee who left, under not the best of terms, was attempting to regain entry via the Exchange Server. We got the logs and information and that allowed us to get the police involved to rectify the problem,” said Santiago.

Because of the success of the proof of concept, Santiago and team were able to acquire funding for the AlienVault appliance in February of 2015. The team found that the general setup was very easy and simple to walk through. When they first deployed the appliance they found that their Exchange Server was under attack and discovered that a severe firewall hole was allowing RDP Connection through from anywhere unmonitored. Luckily no breaches took place but Brute Force Attempts were in progress from several countries.

START YOUR FREE TRIAL ▸

Since the deployment, Santiago and team have also been able to uncover:

- Where patches were needed for critical vulnerabilities like Heartbleed & Poodle
- Orphaned services accounts that needed to be shut down
- A brute force attack on ERP server via 3rd party software needed for ERP

About AlienVault

AlienVault has simplified the way organizations detect and respond to today’s ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault’s Open Threat Exchange, the world’s largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures.

For more information visit www.AlienVault.com or follow us on Twitter (@AlienVault).