ALIEN VAULT

CASE STUDY

Overcoming Challenges of IT Security in K-12 Environments

Council Rock School District is the 12th largest district in Pennsylvania. It includes 18 buildings, 5 municipalities, and 10 IT employees supporting over 13,000 users, including students and employees. For the security aspect of IT, Council Rock School District relies on a one-man team: Matthew J. Frederickson. Matthew is CISSP certified and has more than 25 years in IT. Being solely responsible for the security of over 13,000 users, Matthew has encountered many challenges and has had to adapt the way he approaches keeping Council Rock School District secure.

Since most K-12 IT teams are under budget and understaffed, Matthew originally tackled his job with open source tools. Soon he realized that he was using an unmanageable number of single point products for the different tasks he needed to accomplish. That's when Matthew started browsing the Internet to find a better solution.

"I was doing a web search, looking for something like Security Onion but with a better UI," said Matthew. "That's when I found AlienVault's free Open Source SIEM (OSSIM). It was perfect because it included all the open source tools I was using all in one dashboard, instead of point products on their own."

Company name: Council Rock School District

Industry: Primary: School District

Secondary: N/A

Headquarters location: Southeastern Pennsylvania

Employee count: ~1,000

Website Link: www.crsd.org

START YOUR FREE TRIAL ▸

"I didn't fully realize how much value I would get out of USM until I started using it.

–Matthew J. Frederickson, Security Officer Council Rock School District

OSSIM provides essential security capabilities like asset discovery, vulnerability assessment, intrusion detection, behavioral monitoring and SIEM built into one unified platform. Standing on the shoulders of the many proven open source security controls built into the platform, OSSIM is one of the fastest ways to make the first steps towards unified security visibility.

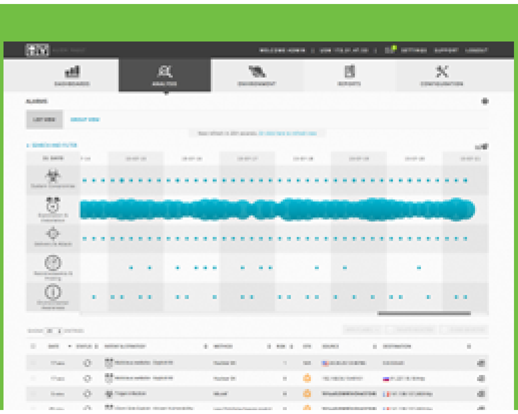
AlienVault provides ongoing development for OSSIM so that anyone can have access to sophisticated security technologies; this includes the researchers who need a platform for experimentation, and the unsung heroes who can't convince their organizations that security is a problem.

Matthew used OSSIM for about 2 months and really liked what he saw. However, he realized he needed a fully supported product so he could get answers to his questions quickly rather than waiting for others in the community to help.

"I wanted to see if OSSIM was good enough before considering a paid solution," said Matthew. "After that was proved, I decided I needed something that was fully supported. That's when I decided to upgrade to AlienVault USM."

The transition from OSSIM to USM was straightforward. Matthew worked on it a little each day over about 3-4 days, spending about 4-5 hours in total. He didn't try to integrate any previous data, just started fresh. Through trial and error he was able to complete the migration without even having to contact support.

"I didn't fully realize how much value I would get out of USM until I started using it," said Matthew. "The reporting in USM is awesome, it's been a big benefit for me. And, having a fully supported solution means I can get answers to my questions much more quickly than before. My favorite USM feature is the cyber kill chain screen. It makes it really easy for me to prioritize and investigate alarms. I believe those features are what really allowed me to justify to management why we should go with a paid solution."



> "Suddenly, I'm the go-to guy for security. With so many products/services out there, it's hard for people to know where to start and where they can get the most bang for their buck. OSSIM was a great starting point for me, and migrating to USM has brought even more value."
>
> – Matthew J. Frederickson, Security Officer
> Council Rock School District

Instead of having to research and write correlation directives for each new security threat that emerges, Matthew now relies on the threat intelligence provided to USM by AlienVault Labs. AlienVault Labs is a team of world-class security experts that analyze, validate and curate global threat data collected by the Open Threat Exchange (OTX)—the world's largest open source repository of threat data.

The AlienVault Labs team has become an extension of Matthew's security monitoring program. They evaluate and translate threat data into integrated security intelligence that is updated weekly in USM via a coordinated set of advanced correlation rules—meaning Matthew can detect emerging threats without needing the expertise to research and write correlation directives himself.

Since migrating to USM, Matthew finds himself logging on at least once a day to look at machines that show alarms and rule out any false positives. He also now shares his experience with OSSIM and USM with the IT staff from other school districts in knowledge sharing workshops. "Suddenly, I'm the go-to guy for security. With so many products/services out there, it's hard for people to know where to start and where they can get the most bang for their buck. OSSIM was a great starting point for me, and migrating to USM has brought even more value."

Key Benefits:

#1 - Instead of researching and writing correlation directives for each new security threat that emerges, Council Rock School District relies on threat intelligence provided to USM from AlienVault Labs.

#2 - Council Rock School District started out by using AlienVault's Open Source SIEM (OSSIM) and soon after migrated to AlienVault USM for it additional functionality.

#3 - The cyber kill chain screen is used by Council Rock School District to easily investigate and prioritize alarms.

START YOUR FREE TRIAL ▸

View all AlienVault case studies at www.alienvault.com/resource-center#content_case-studies