CASE STUDY

University of Wisconsin-Superior Secures their Campus Network with AlienVault™ USM

Founded in 1893, the University of Wisconsin–Superior (UW-Superior) is a public university located in Superior, Wisconsin. UW–Superior grants bachelor's, master's, and specialist's degrees. The university currently enrolls about 2,450 undergraduates and 150 graduate students from over 40 different countries. Ranked as 23rd by U.S. News and World Report's "Best Online Bachelor's Programs/Best Online Programs," UW-Superior strives to ensure their record of 96% of graduates who join the workforce or continue their education.

There are approximately 1200 computers and 50 servers on the UW-Superior campus for faculty, staff, and lab use. Roughly 500 students living in the residence halls on campus also have access to UW-Superior's network services for their daily use.

In early 2015, UW-Superior's IT team was looking to replace their outdated intrusion prevention system. As a result of budget restrictions, however, they needed to find a cost-effective security solution that would still meet the needs of their large network.

Tom Janicki, Technology and Infrastructure Services Director at UW-Superior, was tasked with updating the campus's intrusion detection system (IDS). However, he soon realized that finding an IDS system at a price that met his limited budget was proving to be a challenge.

Company name: University of Wisconsin–Superior

Industry: Education

Headquarters location: Superior, Wisconsin

Employee count: 132

Website Link: www.uwsuper.edu

START YOUR FREE TRIAL ▸

"The replacement quote from the IDS vendor we had been with forever was around $100,000 dollars. There was absolutely no way we would be able to get that approved. We also have an aging phone system that we needed to replace so I couldn't justify such a high cost for a new IDS. I felt extremely helpless and asked myself, 'What am I going to do to protect my campus? Our intrusion prevention system is end-of-life.' The next quote that came in was closer to $200,000 dollars," said Janicki.

> "I believe we were very lucky to discover and acquire such a feature rich product at such a low cost."
>
> *–Tom Janicki, Technology and Infrastructure Services Director, UW-Superior*

While researching alternative IDS solutions, Janicki came across AlienVault's Unified Security Management™ (USM) platform. "I read a review in SC Magazine and decided to go through a self-guided demo. Afterwards, I spoke with a sales rep and was floored by the price he quoted," said Janicki.

After a full evaluation, UW-Superior decided to leverage AlienVault USM to meet their IDS needs. They then quickly began the process of deploying it in their campus network with professional services provided by AlienVault.

"We had opted for professional support to deploy USM but I wasn't sure what that

would entail. At the time I believed the support would simply be working through the setup on my own and calling in if I had problems. I didn't realize it was going to be separate from standard AlienVault support. I was pleasantly surprised to have an actual dedicated engineer who was assigned to help me out the whole way. I didn't have to open a single ticket. The engineer reached out to me and the whole system was extremely fast and easy to set up. We were up and running within a matter of days," said Janicki.

As Janicki and his team became familiar with using AlienVault USM as their intrusion detection system, they began to implement the other tools that make up the USM platform. During this process, Janicki was pleased to realize that because so many security features were already included in USM, like behavioral monitoring, SIEM and vulnerability assessment, he would not have to purchase additional security tools that he previously thought he would require.

"With AlienVault USM, we're able to share a lot of security-related information with our chief business officer. She and others have been floored by the amount of malicious traffic that is being generated towards our network."

–Tom Janicki, Technology and Infrastructure Services Director, UW-Superior

"We definitely got a lot of bang for our buck with USM. What I found amazing was the enormous amount of information from different sources that it could gather, correlate, and store. The engineer would ask me if there were any other assets I would like to monitor and we just kept adding them to the USM platform. Every switch, server, and several other specialized devices on our campus are logging to it and it has been running very smoothly, and I wasn't even looking to add a SIEM. So we got the intrusion detection piece of it, we got the SIEM piece that we're using, and we're even using it as an information security ticketing system, which is extremely helpful in many ways," said Janicki.

Currently there are a total of three security people on Janicki's team that are using USM. They all wear multiple hats and each of their roles are evolving as they learn more about the AlienVault USM platform. Recently, UW-Superior purchased an additional remote sensor that they've deployed outside of their firewall. This additional layer of security has already begun to provide them with detailed information about the malicious actors that are trying to gain access to their environment.

"With AlienVault USM, we're able to share a lot of security-related information with our chief business officer. She and others have been floored by the amount of malicious traffic that is being generated towards our network. We haven't detected

Key Benefits:

#1 - UW-Superior has greatly increased the security of their campus network with all five of AlienVault USM's core features.

#2 - By adding an additional AlienVault sensor outside their firewall, UW-Superior has been able to gain a great deal of information about malicious actors that are trying to gain access to their environment.

#3 - AlienVault professional support allowed UW-Superior to deploy AlienVault USM on their network quickly and easily.

START YOUR FREE TRIAL ▸

any breaches yet, but as with security in all other organizations, you can never be sure. That's why we decided to deploy an external sensor, so that we can report in greater detail on attempted attacks toward our network," said Janicki.

Once the external sensor was deployed, the UW-Superior security team was very surprised to see the amount of attacks attempting to break into their network. For instance, they recently detected a Shellshock attack that was targeting a backup system for the campus radio station. Janicki explained that the attack involved malicious actors who were attempting to place scripts on the radio station's server that would download files from a compromised website.

"This exploit wasn't successful, but we were able to get a lot of insight into what the hackers were trying to do because AlienVault USM provides us with much more visibility. Also, AlienVault's data correlation has allowed us to flush out a lot of false positives. Even though we may not be getting intrusion alarms, we still want to provide reports on activity so we can better understand our risks," said Janicki.

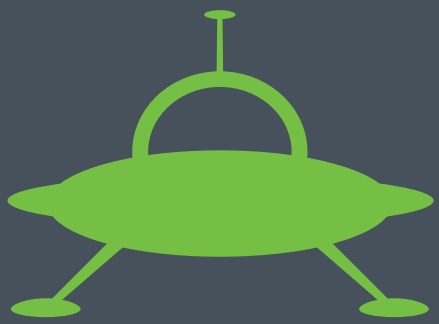
In addition to his full time role as the Technology and Infrastructure Services Director at UW-Superior, Janicki also teaches level 1 and level 2 classes on Cisco and will also start teaching a new networking and security class at Lake Superior College. He said that he has actually incorporated the AlienVault USM platform into some of his course lectures.

"In my Cisco class, I use the AlienVault platform to show my students examples of attempted attacks. For example, I once gave a demonstration of an exploit attempted on our main web server. You could actually see the location of the source of the threat and then how that was connected to the location of our server being targeted. The visual was really cool. Then I drilled down on the threat and was able to show my students the SQL statements that the hackers were running to try and harvest passwords off of our Web server. The students were really interested and it helped them visualize how threats can be detected," said Janicki.

The team at UW-Superior also expressed how AlienVault USM has made their security process far more efficient.

"I like to tell people about how cost effective USM is and about all the success we've had with the platfrm. I also tell them how much ground you can cover with it if you are really taking advantage of all it has to offer. In our network, I'm really impressed with how well USM operates and that it can keep up with everything we're using it for," said Janicki.

Overall, the team at UW-Superior has been able to create a much more secure environment for their faculty, staff and students. They have successfully implemented USM's IDS feature, are improving security event documentation through the ticketing system, and are using the SIEM functionality throughout the network. In addition, UW-Superior recently completed the deployment of behavioral monitoring, host based file monitoring, and vulnerability assessment. "I believe we were very lucky to discover and acquire such a feature rich product at such a low cost," said Janicki.



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).