Case Study

BINARY DEFENSE

Top-ranked university uses SIEM tuning and monitoring to help defend against hacking attempts

Business

Top-ranked university in the midwestern United States

Challenges

Small security team lacked ability for 24/7 monitoring

Had invested in a SIEM for the university but needed expert tuning to help cut down on the "noise" generated by alarms

Results

Unique partnership with Binary Defense has kept university safe

"It was easy to get the conversation started with Binary Defense. They were very flexible to figure out what was going to work best." – University CISO

Not just personal data, but proprietary research, makes colleges hacking targets

A top-ranked university in the midwestern US has received academic accolades from such entities as U.S. News and World Report, Princeton Review and Bloomberg Newsweek, just to name a few. With just under 10,000 students at the undergraduate, graduate, doctoral and online levels, this academic institution is a bustling hub of activity.

Which makes it a perfect target for cyberattacks.

In addition to the personal and financial information of its students and their parents, universities are ripe with proprietary research data. It's for this reason that hackers in countries like China have been stepping up their efforts to breach higher education institutions' cybersecurity measures.

Information security is of increasing importance at universities, ranking at the top of the list of critical IT issues in the higher education space[1]. A recent survey ranks education at the bottom of the list in terms of industries that are taking proper cybersecurity measures[2]. Thus, universities are looking for cybersecurity vendor partners that can help keep their information secure.

University Chooses to Partner with Binary Defense

The Chief Information Security Officer (CISO) began as the sole IT security staff member at the university, and thus had many duties. The university had invested in Splunk, a Security Information & Event Management (SIEM) platform, but had not done much of the tuning and setup that is needed for a SIEM to properly correlate and produce actionable data. A SIEM also requires around-the-clock monitoring or the alarms become irrelevant and nearly impossible to stay on top of, especially with a small team.

The university knew they needed a third-party Managed Security Services Provider (MSSP) to help guide them on the development, tuning and monitoring of the Splunk SIEM instance. They evaluated several providers, but most MSSPs wanted to bring in their own SIEM rather than work with the Splunk instance other existing security infrastructure. However, with Binary Defense, "it was easy to get the conversation started with them. They were very flexible to figure out what was going to work best," the CISO said.

Once a SIEM is tuned, organizations need a 24-hour-a-day Security Operations Center (SOC) to manage and monitor the SIEM 24/7 in order to be proactive and stay on top of alerts. The costs of hiring staff to work in multiple shifts may not be realistic for most organizations. Outsourcing a SOC to a third-party vendor is a simple solution that can be cost-effective in

Binary Defense SIEM Services

Deployment, tuning and 24/7 monitoring

Advanced detection technology that works with leading SIEM platforms

Security Operations Task Force analysts are an extension of your team

---

"With Binary Defense, we have a team that can look at our environment and give us thoughtful and insightful responses to what's happening. They're helping us improve our posture overall." – University CISO

comparison to building one in-house. This rang true for the university CISO as a one-person team, even as the staff grew.

A unique partnership

The CISO describes the relationship between his team and the team at Binary Defense as beyond a vendor relationship – it's a partnership. "We are a unique Splunk customer in the higher education market. With Binary Defense, we have a team that can look at our environment and give us thoughtful and insightful responses to what's happening," he said. "They're helping us improve our posture overall."

In addition, the CISO cites the team at Binary Defense as going above and beyond for him and his team. "Binary Defense met with our IT staff during National Cybersecurity Month [in October] to help promote our cybersecurity activities and talk about threats they are seeing and things we should be looking out for," he said. "They really go beyond the scope of just being a SIEM or a SOC."

Additional insights help improve security overall

Finally, the university security staff relies about the industry expertise Binary Defense shares with their customers. "The blacklist generated by Binary Defense has been very helpful," the CISO said. "We can see how to incorporate that into our environment or what bad actors are communicating with us. Threat intelligence is immensely valuable and something we could never get by trying to do it on our own." The team at the university subscribes to the Binary Defense Threat Watch newsletter and read it regularly.

"I tell people all the time, if you're looking at cybersecurity, you have to call Binary Defense," the CISO said.

[1] https://www.educause.edu/research-and-publications/research/top-10-it-issues-technologies-and-trends/2018

[2] https://edscoop.com/education-ranked-worst-at-cybersecurity-out-of-17-major-industries/