Case Study

Electricity provider finds value in threat hunting partnership with Binary Defense

Business

Electricity provider in the US with approximately 100,000 customers

Challenges

Small staff tasked with overseeing security for a co-op organization

Saw the importance of threat hunting but unable to fully implement due to competing priorities

Results

Binary Defense Threat Hunting gives the company an extension of their team to complement their existing security solutions

The threat hunting team was able to proactively search their network for suspicious activity after a major third-party breach

"Having Binary Defense focused solely on threat hunting has been a huge advantage and help for us, and it also makes us feel like we have a better idea of what's going on."
-senior cybersecurity specialist

Utility companies must stay compliant while fighting cyber threats

Utility companies, including electricity providers, provide a valuable service to their customers. If a cyberattack were to disrupt or knock out electrical power, it could have wide impact beyond leaving people in the dark. This could lead to a utility company doing whatever it takes to get their systems back up and running—including paying a ransom to a hacking group. In 2015, the electric grid in the Ukraine was hit by a cyberattack, impacting over 250,000 customers. This event was eye-opening to the utility industry in general. In 2021, a hacker attempted to poison the water supply of a Florida town[1], failing because of safeguards in place, but nonetheless shining a light on how vulnerable infrastructure is to an attack.

In addition to combating threats from cybercriminals, utility companies must comply with the North American Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) rules which took effect in 2020[2], which affects cybersecurity for these providers. It's of utmost importance to these organizations to have the right tools and staff in place to protect their businesses from threats and stay compliant. Only about two-thirds of utility companies feel they currently have the adequate combination of technology and expertise to stay cyber safe[3]. And, over half of critical infrastructure providers have reported attacks that have attempted to control their systems.

Cybersecurity solutions to keep utility companies protected against cyberattacks can include endpoint detection and monitoring, Security Information & Event Management (SIEM) solutions, and threat hunting if an organization has the previously-mentioned layers of security in place. Threat hunting is an emerging practice where experts proactively explore a mature network's security logs to find hidden threats. These threats evade security technology because threat actors are constantly updating their techniques. The information uncovered in a threat hunt can then be used to update the alerts in a customer's environment, leading to faster detection time.

Provider turned to Binary Defense for Threat Hunting

A Binary Defense client is a regional electricity provider in the US serving just under 100,000 customers. This company had security technology in place to protect them from cyberattacks. They had even begun to look into doing threat hunting on their own. With a three person staff, however, they realized they couldn't keep up with the monitoring piece. When they spoke to Binary Defense about their threat hunting service, "it was an immediate YES," said the cybersecurity supervisor. "It escalated our desire to start a threat hunting program." Although the team is interested in threat hunting, as a small staff, they need to prioritize their time. "Having Binary Defense focused solely on threat hunting has been a huge advantage and help for us, and it also makes us feel like we have a better idea of what's going on," said a senior cybersecurity specialist on the team at the energy company.

The threat hunting engagement began in the fall of 2020. The organization had invested in technology including Microsoft Defender ATP, as well as the

Binary Defense Threat Hunting

Proactive service for organizations with security fundamentals in place

Experts seek out hidden threats and vulnerabilities on a company's network and use this information to update detection rules

Regular, ongoing hunting ensures the latest attacks are detected

Microsoft Azure Sentinel SIEM, which the Binary Defense Threat Hunting Task Force experts are skilled in using for threat hunting. Immediately, the company saw value. "We have skilled, experienced threat hunters watching and creating new detections for our environment at all times. We wouldn't be able to afford that level of talent at an energy company of our size. They feel like they are an extension of our team."

As with many organizations that pivoted to remote work when the COVID-19 pandemic hit in 2020, this organization relies upon a team chat application to stay in constant communication with one another. The Binary Defense threat hunters have been added to the chat with the security team, and are active participants, which helps bolster a feeling of teamwork between the two companies. "It allows us to share ideas, bring them up to speed on our environment and the value they bring to the table," noted a security engineer at the energy company. "The team supervisor added, "I've had a lot of security companies tell me that they want to be an extension of our team. But those promises come up short in many situations. This is the one time that that's not the case."

Threat hunting team goes above and beyond after Solarwinds attack

The team noted that when an incident involving threat actor group Emotet emerged on their system, the threat hunters at Binary Defense were able to do a thorough investigation, aided by the fact that a Binary Defense threat researcher has done extensive analysis on this particular group. When the late 2020 Solarwinds breach happened, the Binary Defense threat hunters proactively reached out to the utility company, knowing they were a customer of the technology provider. "The news dropped on Sunday, and we woke up to it first thing Monday morning. The Binary Defense team had already searched our environment and didn't find anything. That meant a lot to our team," the supervisor explained.

The Binary Defense threat hunters also noticed suspicious activity which was actually a penetration test in progress. "That was one of the better outcomes we ever could have hoped for with a pen test," the supervisor said. "I feel confident in saying that with that attacker simulation we would not have had as positive an outcome without their team helping us," the security team said.

The value of threat hunting to this organization has been invaluable, and they recommend threat hunting services to any mature organization. "We've been able to add resources to handle security incidents occurring inside of our organization without adding new FTE's," the supervisor noted. "If companies have the fundamentals in place already, there's tons of value to be had. To build this yourself would take many years, and a big expense to build out the infrastructure, not to mention hiring the expertise."

"The tools are important but having the right people dedicated on both sides—both Binary Defense and our internal team—is a requirement for success. If they weren't engaged, that would be detrimental," the supervisor added.

[1] https://www.scmagazine.com/home/security-news/network-security/security-gaps-in-operational-tech-exposed-with-hacker-attempt-to-poison-florida-city-water

[2] https://www.darkreading.com/attacks-breaches/nerc-updates-may-force-utility-companies-into-better-cybersecurity-/d/d-id/1337323

[3] https://www.utilitydive.com/news/utilities-say-they-are-prepared-to-meet-cyber-threats-are-they/572080/