Energy Cooperative powers up to get better detection, visibility and response to network threats.

Case study

With Verizon Network Detection and Response, this mid-sized energy cooperative significantly reduced incidence response times and moved from a reactive to a proactive security approach.

Challenge

Chad is the sole manager of the cooperative's Security Operations Center (SOC) and the compliance manager for the North American Electric Reliability Corporation Critical Infrastructure Plan (NERC-CIP). His job is to ensure the integrity of the energy cooperative's corporate network, as well as monitor security for substations, transformers and other critical operational assets.

His goal was to operationalize the utility's cybersecurity. "I don't want reactive security tools," says Chad. "As a one man SOC, I need solutions that actively and pre-emptively address threats. Something that is more visually based, something that wasn't going to take up cycles that I don't have." He needed tools that would secure his network environment, ensure compliance with the NERC-CIP, improve threat identification, shorten the breach detection window, and make investigating and responding to threats faster and less time-consuming.

Solution

Chad was drawn to the solution's user interface (UI) and the Attack Spiral, a spinning nautilus based on the Lockheed Martin Cyber Kill Chain. The Spiral gives security pros a way to quickly identify the severity of threats and actively hunt them down.

"I'm a cyber kill chain guy. I like the idea of getting ahead of threats, quickly investigating and validating them, and responding. I like to know I have the chance to stop a threat in its tracks before it exfiltrates information."

The energy cooperative began a trial of the cloud-based solution. "The Verizon deployment model is appealing because it doesn't require us to buy any hardware. We were able to quickly deploy the sensor by just marrying traffic directly to a virtual machine that we had open. It was fast and painless."

The sensor captures full-fidelity network traffic, then compresses and stores it on the Verizon cloud platform for a client-determined amount of time. The cooperative chose to store their traffic for three months. "We didn't have full PCAP anywhere else and this is a requirement." notes Chad. "Verizon helps us meet this expectation."

Industry:
Electricity, Energy

Company:
Consumer-owned public utility. Headquartered in Amarillo, TX, its service area is larger than the state of Virginia.

Challenge:
Lean security staff needed a solution to quickly identify, validate and investigate security alerts and to ensure compliance with electric power industry regulations.

Solution:
Verizon Network Detection and Response

Outcomes:
Detected Shellshock exploit attempt ahead of E-ISAC alert

Shifted from reactive to proactive and automated detection of network threats

Reduced security staff man hours previously dedicated to forensic investigations

verizon

The network data is analyzed in real-time as well as retrospectively for threats. New indicators of compromise trigger automatic evaluation of historic network behavior for newly discovered, latent threats. “The automated retrospection really appealed to me,” says Chad. “New exploits and vulnerabilities are constantly appearing. I need to be able to tell my CIO whether or not we’ve been impacted.”

The energy cooperative is subject to twice-weekly DHS hygiene scans. “Before deploying Verizon, we didn’t have the visibility or the man hours to respond quickly if the scan found anomalies,” says Chad. “It could take weeks to find whatever threat or vulnerability DHS alerted us to. With Verizon I can login from anywhere, investigate quickly and knock it out. I can tell my boss exactly what is happening on our network and better yet, we can respond to DHS or other oversight bodies with validation of what took place on our network.”

Chad makes extensive use of the Verizon Network Detection and Response Visualizer,which provides advanced threat visualization. This feature takes the huge data stack of threat intelligence, prioritizes and correlates hundreds of thousands of security observations, and rolls them up into security events. Rather than being inundated with disparate security alerts, Chad is presented with actionable intelligence. “As a one man SOC, I need an intelligent tool that lightens my forensic workload. Alerts on my cell phone quickly prompt me to check out any priority events, and if I need to, I can quickly drill down to the observations. It’s an immense time saver.”

Outcomes

During the energy cooperative’s 30-day trial, a Shellshock exploit attempt appeared as a priority security event on the Visualizer’s heads-up display. With one click, Chad pivoted from the priority event to the Killbox to begin his forensic investigation. He saw that a critical external server had been connecting to an IP address in China, and observed various activities that progressed through the kill chain stages. This put the network at high risk of being compromised.

Chad was able to validate the event quickly by downloading the full PCAP where he saw a command asking the external server to download a malicious file. He addressed the issue and neutralized the threat before any damage was done. “This type of visibility and peace of mind is worth its weight in gold.”

Using Verizon Network Detection and Response, Chad was able to identify, hunt down, and kill the Shellshock exploitation, all before the Electricity Information Sharing and Analysis Center (E-ISAC) issued an alert on the threat.

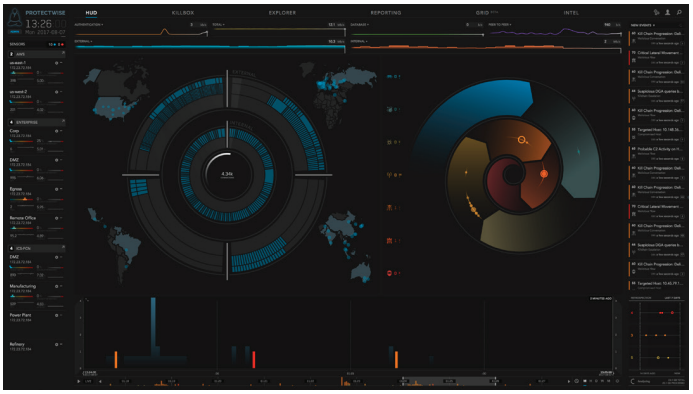
“As a one man SOC, I need an intelligent tool that lightens my forensic workload.”

About Verizon Enterprise Security

We have more than 25 years of industry experience, nine security operations centers, six forensics labs and one of the largest IP networks in the world. A recognized leader in managed security services, we monitor billions of security events (on average) each year to improve our threat library and inform our teams. Our world-class staff is ready to help you meet your security challenges. Our end-to-end cyber detection and response delivers broad visibility, actionable intelligence and adaptive response against potential threats. Our portfolio of services including our Cyber Security Incident Response Team, Rapid Response Retainer and custom SOC services can help keep you cyber resilient.

Learn more

Contact your Verizon sales representative for more information or visit enterprise.verizon.com/networkdetectionandresponse



Verizon Network Detection and Response dashboard

verizon