Utility Leader Builds Cybersecurity Powerhouse

One of the top 10 energy and utility companies in the United States has become a recognized leader in cybersecurity—and not just in that market sector.

The organization carefully and methodically matured its cybersecurity posture over a 4-year period. The move repositioned their strategy from a reactive model, increasingly ineffective against devastating cyberattacks, to that of predictive—understanding the attackers and their goals before new threats launch. Today, this company shares threat intelligence throughout the industry, helping others combat advanced threats targeting the market.

The transformation into a cybersecurity leader began in 2009, when they became the target of a large-scale advanced persistent threat (APT). At the time, perimeter defenses like antivirus scanners and firewalls served as network protection. They discovered the APT early, quarantined the damage and mitigated the threat. However, the fact that it was discovered after breaching the network perimeter alerted the utility to the need to improve its cybersecurity posture. Among the things needed was a security operations center (SOC) to bring together intelligence and activities for analysis and action against emerging advanced threats..

How does a utility company with static perimeter defenses become a world leader in cybersecurity in just a few years?

How did they do it?

The utility engaged Leidos Professional Services to transform and build their cybersecurity infrastructure. Executive management teams provided total buy-in to the process and were involved at every step along the way. The process required the company to upgrade its cybersecurity footprint in the areas of people and processes as well as technology.

leidos

THE SOLUTION

The foundation of any mature cybersecurity organization is people. In addition to executive-level support, this organization needed front-line teams to handle the dayto- day work of identifying and responding to advanced threats. Automated tools would handle the routine tasks of blocking known threats. Leidos collaborated with the organization to design a foundational nucleus of threat monitoring and incident response teams-one of the first efforts of this scale within the energy sector. Several specialty teams trained in areas such as focusing on intelligence fusion, mitigations and countermeasures, and dedicated malware analysis.

Training focused on the Cyber Kill Chain® methodology, using a defined set of steps that attackers use to find and access the data they want on a network. Understanding the chain allows defenders to challenge the notion that attackers only have to be right once, and aligns defenses across phases. Attackers must be successful in all phases to achieve their desired objectives, and it doesn't end there. When the threat is blocked, it is analyzed to determine who the attackers are and what data they're trying to target. Identifying an adversary does not necessarily mean identifying an individual, but distinguishes a criminal attack from a nation-state or terrorist attack. Knowing the location of the bad actors can help to understand their goals and methods. That information is used to create defenses specifically to see and block future threats from those same attackers, pushing them further up the chain and away from the target.

The more attempts an attacker makes to breach a network, the more information the security operations team is able to collect and use to improve defenses and create proactive countermeasures.

This was a new way of thinking in 2009 when cutting-edge efforts to improve cybersecurity were just beginning.

Creating a world-class environment in cybersecurity meant the organization needed to foster a completely new, innovative way of thinking about security that was far advanced from what anyone else in the industry was doing at the time.

An evolution to the concept of Intelligence Driven Defense® integrative services was gradual, using simulations and drills to ensure that teams retained information.

An evolution to the concept of Intelligence Driven Defense® integrative services was gradual, using simulations and drills to ensure that teams retained information.

IMPLEMENT POLICIES

In addition to a trained workforce, effective cybersecurity requires developing the proper policies, procedures, and practices.

The next step taken by this organization defined the roles, teams, and missions for the SOC staff as well as actions to take after threat detection. Those procedures included highly advanced concepts such the analysis of captured threats, and provided actionable intelligence to allow the SOC to improve the organization's overall security posture continuously.

Cybersecurity organizations throughout the industry embraced this unique concept of turning threats around for use as a defensive advantage.

leidos

INTRODUCE TECHNOLOGIES

The third essential element in effective cybersecurity is the technology. Most organizations have at least some of the necessary tools in place. The expertise of a professional partner in the field can help a team take full advantage of existing tools to identify and fill the gaps in technology. This organization built a knowledge and intelligence management system to track security resources and their associations, coordinate the tracking of threats, enable communication, and direct remediation in the wake of any incident. It could also analyze the contex tual indicators of threats so that actionable intelligence compared to previous attacks. That information helped protect against future actions by threat actors, and made this system the backbone of the entire security architecture.

The knowledge and intelligence management system works with existing security tools, allowing central management from the SOC. Any single security program might not detect some threats, especially APTs with traditionally light footprints. However, this system combines and normalizes data from multiple sources to help analysts spot suspicious or malicious activity that otherwise could have been missed. Trained teams within the SOC view a holistic and complete picture of network health. Collected threat data is stored in an enriched database to use against future attacks or help identify attackers by their previous and preferred methods of attack.

EMERGE A LEADER

This energy and utility organization is responsible to protect the critical infrastructure that it owns and operates, and the SOC works with the entire enterprise to defend against all types of cyberattacks. It also helps to ensure the company's compliance with government and industry regulations such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

The organization now actively shares information it gathers about threats and their creators with others in the industry. They have come a very long way since finding that original APT within a network back in 2009. Today, thanks to their proactive and cutting-edge efforts, the organization is recognized universally as an expert in cybersecurity.

In fact, the utility has become such a leader in cybersecurity that they no longer need support from Leidos in the day-to-day operations of their SOC. As the utility's cybersecurity posture matured, the partnership matured as well. Leidos continues to be a collaborative partner and sounding board, advising on threats, technologies, and trends that face the organization.

Implementing a world-class cybersecurity infrastructure ensures this organization has comprehensive coverage against modern threats. Even advanced threats are detected and analyzed before they can do damage and before the attackers reach their goals. This fully sustainable approach to cybersecurity continually improves the organization's defensive posture and their competitive position in the market.

FOR MORE INFORMATION
855-56-CYBER / cyber.security@leidos.com
cyber.leidos.com

XX-LH:V0