MANDIANT®

CUSTOMER STORY

Multinational Energy Company Accelerates Security Transformation to Minimize Exposure

Mandiant Cyber Defense Operations Elevate Security Posture and SOC Team Effectiveness

FACTS AT A GLANCE

INDUSTRY

Energy

SOLUTIONS

- Mandiant Cyber Defense Operations

BENEFITS

- Significant increase in alert fidelity and accuracy across entire infrastructure
- Embedded Mandiant consultants elevated in-house skills and team effectiveness
- Rapid remediation of a situation that was inundating the SOC team with alerts
- Eliminated backlog of 2,000-3,000 endpoint-related events
- Alignment of tool capabilities to the revised incident response process

CUSTOMER PROFILE

The organization is a multinational energy company that generates and distributes electricity and gas across an infrastructure spanning two continents.

The Challenge

Securing an environment that is split across two continents is a massive and complex undertaking As part of ongoing efforts to continually evolve its cyber defenses, an industry-leading endpoint security solution was deployed across the utility company's extensive environment. However, a combination of initial configuration settings, coupled with the complexity and magnitude of the transcontinental infrastructure, resulted in the generation of thousands of alerts that quickly overwhelmed the in-house SOC teams.

The situation provided an opportunity to not only stem the barrage of alerts, but also improve alerting priorities and fully integrate response playbooks into their team processes.

The Solution

To expedite resolution of the unmanageable volume of endpoint-related alerts—and optimize internal processes and expertise around detection and response—the company engaged the Mandiant Cyber Defense Operations team.

Mandiant Cyber Defense Operations enable organizations to transform existing detection and response capabilities through hands-on operational support and coaching. The services leverage the extensive Mandiant frontline incident response experiences and expertise amassed from designing and running some of the world's largest cyber defense operations.

To fully optimize the speed and effectiveness of the operational transformation, the Mandiant team of experts were embedded in the organization, sitting alongside the detection and response team. A project plan was developed to baseline the existing state of security-related elements—including processes, technologies, capabilities and controls—at the energy company. The plan was created to address deficiencies discovered in aspects of the existing security environment with an emphasis on knowledge transfer and coaching for self-sufficiency

The objective of Cyber Defense Operations does not provide for long-term staff augmentation—because of this, an emphasis is always placed on knowledge transfer and coaching for self-sufficiency—consequently, building-out the capabilities of the in-house teams was included as an integral objective.

Phase One

For the energy company, the initial focus was to conduct a detailed assessment of the deployment and configuration of the existing endpoint security solution.

Phase Two

Once a detailed baseline was defined, the project's second phase concentrated on optimizing the parameters related to alert generation. Having determined the company's risk profile and security objectives, the Cyber Defense Operations consultants tuned the event triggers, and subsequently developed a series of guidelines for the SOC team for future endpoint security configuration and alert changes.

Phase Three

The third phase included operationalizing the newly created blueprint to address the endpoint security misconfigurations. The Mandiant consultants cleared all customizations and non-default configurations, and deployed the new settings across the company's two SOCs. A formalized sequence of knowledge transfer activities also was put in place.

A Clean Slate, A Fresh Start

The impact of erasing analyzing and tuning the endpoint security solution's non-default triggers and customizations was immediate and significant. By configuring the new pool of alerts for efficiency and fidelity, the Mandiant Cyber Defense Operations team was able to dramatically reduce the number of false positives and eradicate repetitious signals generated by low-value events. Custom indicators of compromise were developed and the methodology for remediation repeatedly practiced ensuring optimal response ahead of experiencing a significant compromise.

The focus on education and knowledge transfer elevated the SOC teams' ability to effectively and expediently detect and respond to alerts. Hands-on training was conducted in both the use of the product with real alerts and the collection and interpretation of artifacts supporting their analysis.

Tuning the endpoint security platform also resulted in deeper visibility and improved granularity across the entire infrastructure—the team is now optimally positioned to interpret the enhanced information and equipped to take immediate action. This has resulted in the creation of a more robust security posture across the company's extensive attack surface.

Another positive Cyber Defense Operations outcome was the alignment of tool capabilities to the organization's newly refined incident response process, with improved support for identifying relevant forensic artifacts for alert analysis.

The combination of the reconfigured endpoint security deployment, in conjunction with the SOC teams' heightened levels of skill and expertise, eliminated the accumulated backlog of 2,000-3,000 endpoint-related alerts. By tuning rules to minimize false positives, the number of alerts generated dropped from hundreds per week to just a few dozen.

The new capabilities also resulted in the discovery of latent malware, adware and unwanted programs, throughout the environment. These were quickly prioritized and addressed by the SOC team using the optimized set of processes and procedures.

Fast Pace, High Impact

By partnering with the Mandiant Cyber Defense Operations team, the multinational energy company gained visibility into the specific challenges it was facing. The national importance of its electricity and gas distribution networks dictated that deficiencies in processes and skills be immediately addressed. By the conclusion of the eight-week engagement, the company's cyber security professionals had acquired the skills, rigor, and process knowledge needed to build-out the capabilities to defend the company's assets in a competent, disciplined manner.

The security team spokesperson summarized, "The expertise of the Mandiant Cyber Defense Operations team accelerated our critically needed transformation and truly minimized the window of exposure."

For more information on how Mandiant Expertise On Demand can help you access flexible cyber security expertise for your organization, visit: **https://www.fireeye.com/mandiant/cyber-defense-operations.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®