MANDIANT

CUSTOMER STORY

GLOBAL MANUFACTURER ADDRESSES POTENTIAL GAPS IN SECURITY POSTURE

Mandiant Cyber Defense Operations enhances MITRE ATT&CK coverage with creation of tailored use cases

FACTS AT A GLANCE

Industry
Manufacturing

Solution
- Mandiant Cyber Defense Operations

Benefits
- Created a company-specific threat profile—that identified threat actors and favored methods of attack—to enhance the company's detection and remediation capabilities
- Developed 60 use cases for ingestion into the SIEM
- Added coverage for 40+ previously exposed MITRE techniques and refined many existing techniques to further improve overall efficacy

Customer Profile
The company is a high-profile multinational engineering and manufacturing corporation and is the market leader in many of the business sectors in which it operates. It is a member of the Global Fortune 500.

The challenge

This company represents a rich target for cyber criminals looking to gain access to personal, financial and operational information, as well as intellectual property that could be exploited on the black market.

Being a perpetual, highly visible target for online criminals, the company continually refines its security posture to ensure that its cyber assets and critical data always remain protected. The organization has made sizable investments in its defenses and attached significant strategic importance to cyber security enabling it to attract and retain top-tier talent and expertise from across the security industry. Their security team established a robust set of defenses that have been effective in securing the environment against a wide range of mainstream attacks.

The company is a long-time user of the MITRE ATT&CK framework to validate its security architecture and to support the development of specific threat models and methodologies. They wanted assistance identifying and addressing any potentially obscured or nuanced vulnerabilities in its defenses.

The solution

The company engaged the Mandiant Cyber Defense Operations team to develop a series of highly detailed use cases that would be used in the SIEM to elevate its detection and response capabilities and further fortify the engineering giant's multinational attack surface.

Phase 1

The Mandiant team began by creating a tailored threat profile for the company and its industry, Mandiant Threat Intelligence. One of the deliverables Mandiant consultants generated in the initial phase of the engagement was a list of global threat actors deemed to have a high probability of aggressively targeting the company's digital assets.

Phase 2

Having established this foundation, with the Mandiant Threat Intelligence team, the Mandiant Cyber Defense Operations consultants then focused on the creation of custom use cases explicitly aligned to address specific gaps uncovered during the investigation phase. Every use case included a set of meticulously documented detection criteria to facilitate the rapid identification of each newly profiled compromise attempt.

Example use case categories included:

- Specific malware strains favored by named threat actors identified by Mandiant experts
- MITRE ATT&CK exploitation techniques associated with named adversaries
- Detection capabilities for open source techniques known to be used by actors targeting companies in the industry

Phase 3

TAs they refined each use case, the Mandiant team wrote detection logic pseudocode (using a Sigma-compatible format) before submitting the completed packet for ingestion into the company's SIEM. After assimilation into the SIEM portfolio, each use case was tested and further tuned to ensure optimal effectiveness.

The use of preconfigured templates ensured that each use case followed the same coding methodology and taxonomy, and the entire collection was optimally aligned to address the specific, advanced threats that the company was likely to face from the cadre of sophisticated attackers that had previously been identified.

Results

Because each use case was mapped to individual elements of the MITRE ATT&CK framework, integrating detection logic into the SIEM gave the company the ability to quantify measurable enhancements to their detection and remediation capabilities.

The Mandiant Cyber Defense Operation engagement lasted approximately eight weeks and resulted in the creation of 60 new use cases comprised of almost 800 individual detection objects. This addressed over 40 MITRE techniques that were previously uncovered prior to the project's launch, a solid double- digit percentage uplift in the number of enterprise techniques deployed at the company. In addition to the newly implemented use cases, the detection capabilities of more than a dozen existing MITRE techniques were further enhanced using information directly sourced from the engagement.

Due to the positive impact of the original engagement, the company signed an annual agreement to work exclusively with Mandiant to further accelerate use case development and ensure ongoing enhancements.

Learn more at **www.mandiant.com**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.

MANDIANT