CASE STUDY

A Night Vision Equipment Company Stalks its Invisible Enemies

Bad actors strategically hunting for Department of Defense (DoD) information prefer to target smaller suppliers who feed into the largest DoD contractors rather than attempt to prey directly on huge companies such as Lockheed Martin, Northrop Grumman and Raytheon. As a result, smaller firms are now major targets for cybercriminals who continuously attempt to breach their infrastructures and gain access to their customers' classified information.

Trustwave®

Client Spotlight

A DoD contractor, specializing in producing thermal imaging infrared cameras, components and sensors for military, law enforcement and commercial use, embeds its products in Apache helicopters and other military equipment. A successful cyberattack could threaten its eligibility for work on classified government systems, threaten its intellectual property, and endanger its largest revenue stream. Accordingly, the company employs leading-edge cybersecurity solutions to anticipate, hunt and respond to threats.

The Challenge

A global leader in the infrared imagery industry recently underwent a network upgrade and security improvement across its seventy global locations. Deploying new technology was critical to enhancing the company's security posture and ensuring it met stringent DoD guidelines; the new systems also generated an overwhelming amount of data.

> *"Trustwave SpiderLabs' expertise in threats targeting military and manufacturing clients, along with Trustwave's partnership with Palo Alto, sealed the deal."*
>
> – IT Services Firm that Recommend Trustwave to the client

The company did not have enough in-house security staffers to effectively monitor, respond and correlate that volume of data. Limited resources within a larger IT budget and a dire industry-wide shortage of trained cybersecurity experts made the idea of building out its own security operation center unrealistic. To further complicate the situation, the company had spent a considerable sum of money implementing Palo Alto Networks firewalls and security tools such as Cortex XDR and required a partner that could leverage its existing assets and security tools.

> *"Our client doesn't just want to know about a breach, it needs an immediate response, too. That's why the Trustwave MDR ability to take action was so important."*
>
> – IT Services Firm that Recommend Trustwave to the client

The Solution

The company engaged a national IT services firm to assess its needs and options. After considering several major providers, the firm recommended implementing a host of Trustwave services, including Managed Detection and Response (MDR), Digital Forensics and Incident Response (DFIR) and Consulting and Professional Services (CPS). Because the client had already invested in Palo Alto Networks Cortex XDR detection and response platform, they would benefit from Trustwave's alignment with Palo Alto Networks. Leveraging the Cortex XDR platform, Trustwave provides deeper visibility into their data lake allowing powerful enrichment, investigation, hunting, and strong orchestration for incident response so the client can view Cortex XDR insights directly within Trustwave Fusion. Moreover, the professional services team at Trustwave delivered a turnkey setup and configuration, as well as continuous fine-tuning, to eliminate any transition-related complications.

Today, the company's security logs and data points from Cortex XDR are fed to Trustwave SpiderLabs Fusion Center, an elite security command center that identifies and tracks vulnerabilities and adversary tactics. The client was especially pleased that Trustwave SpiderLabs ethical hackers specialize by industry, so the experts assigned to the company's team possessed deep military manufacturing expertise. With this background, the Trustwave team was able to skip the ramp-up period and immediately identify advanced attacks.

Industry Threat

Cybersecurity risks pose a severe threat to the defense industry and the national security of the U.S. government, as well as its contractors, partners, and allies. In February 2020, the Defense Information Systems Agency, part of the DoD, reported that it that may have compromised personal information of about 200,000 people, with several previous breaches exposing millions of others. This prompted the Pentagon to create a new framework, the Cybersecurity Maturity Model Certification (CMMC), which was introduced in 2020. CMMC requires all members of the defense industrial base to implement and practice certain cybersecurity requirements based on maturity level, and be certified by a third-party assessor. Still, the fight against cyber criminals continues: In April 2020, the Government Accountability Office released a report noting that the DoD is years behind on several internal cybersecurity initiatives.

Trustwave®