deepwatch

Retail Industry **Case Study**

Retail Business Selects deepwatch to Provide Managed Detection & Response Services Across Business Units

The Customer

Industry: Retail

Security Teams: 10

Total Security Team Size: 42

Revenue: $15 Billion

Endpoints: 57,000

The Challenges

- Multiple Business Units Across International Geographies
- Multiple Leadership Teams
- Multiple Security Teams
- Extremely Large Attack Surface
- Lacking Value from Existing MSSP
- Security Talent
- Shared Data Analytics Platform Between Cybersecurity and IT Operations

The Goal

As a consolidated conglomerate of ten international retail business units, the customer has a broad attack surface to monitor and defend. This includes various endpoint technologies such as Point of Sales Devices, Mobile phones, Computers, Servers, Inventory Management Systems, and more. These systems range from physical devices that are operated at franchise locations, data centers, warehouses, and office locations, to Cloud-based systems and applications that are used by telecommuters. Each business unit operates as its own independent entity, with support from shared services organizations, which include Information Technology Operations and Security. In 2015 the business hired a Managed Security Service Provider (MSSP) to manage network log correlation, threat detection, and response. The MSSP did not provide them with the promised return on investment and left the various business units to fend for themselves. Between 2015 and 2019 the company had to remediate and repair a variety of breaches stemming from PoS malware campaigns and phishing attacks. Consequently, the business decided to replace its current MSSP with one that they could partner with to secure their businesses together, collaboratively.

The goal for establishing a relationship with an MSSP was to:

- Have a single shared service Security Operations Center (SOC) with named security analysts that could understand the security needs of each independent business unit and security team, while collaborating to share best practices and Indicators of Compromise (IOCs) for comprehensive detection and response
- Fully outsource security capabilities to establish 24x7x365 security monitoring, vulnerability management, and endpoint detection & response capabilities
- Ensure network traffic and alerts across all discrete business units are monitored, validated and triaged properly to remediate incidents quickly
- Grow their understanding of their threat landscape in close collaboration with the MSSP partner

The Criteria

The corporate Chief Information Security Officer (CISO) and his divisional security peers collaborated to arrive at a list of criteria needed to derive maximum value from its MSSP service. They met with several MSSP's to evaluate their capabilities and find the provider that best met their criteria. The selected MSSP needed to:

- Provide a team of responsive security analysts who would manage, monitor, validate and triage alerts across all the business units in a single platform
- Equip the MSSP security team to be an extension of their security operations team who would learn from attacks, events, and incidents targeted at one business unit, and would apply IOC's, detection signatures, etc. for a proactive defense to the security technologies belonging to the other business units
- Deliver a fully enabled 24x7x365 SOC to reduce cyber risk exposure, secure each business unit, and reduce the attack surface
- Serve as a trusted partner to enhance security maturity over time
- Possess deep technology expertise with best-of-breed solutions and IP that's tuned to stay ahead of relevant threats to the business' network
- Have a team located in the continental United States to ensure ease of collaboration and communications
- Deliver competitive pricing to assist in containing the overall security investment, while optimally configuring security technologies and driving economies of scale

Outcomes

After a detailed evaluation and analysis, the CISO and his divisional counterparts selected deepwatch to deliver its Managed Detection & Response service across all 10 business units. deepwatch was selected based on its ability to deploy within a compressed time frame, its high-touch Squad Delivery model, its US-based team, its ability to ingest logs from all sources into its Security Operations (SecOps) Platform, and its Maturity Model that numerically indexes how well they are defending their network from threats, while providing a roadmap to enhancing their security posture over time.

deepwatch deployed its SecOps Platform across all 10 business units and began delivering validated and triaged alerts to the businesses in less than 30 days. The named deepwatch squad has built strong relationships with various security stakeholders across the conglomerate and continue to collaborate to grow and enhance each business' security posture. The business continues to grow and expand its security presence and physical footprint and leans on deepwatch to continue to ingest and tune additional logs on an ongoing basis. Since bringing deepwatch in to detect and respond to security alerts, the business has seen its maturity index steadily improve.

ABOUT DEEPWATCH

deepwatch delivers data-driven managed security services while extending customers' cybersecurity teams and proactively advancing their SecOps maturity. Powered by our innovative cloud-native platform, deepwatch is trusted by leading global organizations to provide 24/7/365 managed security services.

CONTACT US

sales@deepwatch.com
7800 E Union Ave, Suite 900 Denver, CO 80237
855.303.3033

deepwatch.com