deepwatch

Manufacturing **Case Study**

The Customer

Industry: Manufacturing

Security Team Size: 22

Revenue: $5 Billion

Endpoints: 40,000

The Challenges

- Multiple Discrete SIEM Solutions
- Inconsistent Data Categorization
- Lacking Security Oversight
- Lacking Proactive Security Measures
- Weak Understanding of Security Posture and Maturity
- Security Talent
- 24x7x365 Alert Monitoring
- Security Maturity Roadmap

The Goal

The customer, a global manufacturing conglomerate with five distinct business units, had been working with a Managed Security Service Provider (MSSP) that didn't meet the level of service and accuracy in delivery that they required to defend their network from cyberthreats. Each business unit had its own Splunk Enterprise Security environment that had been set up and managed independently. The customer needed to normalize data ingestion across all five business units and combine five Splunk instances into one that could effectively monitor, manage and detect security events, validate them, and promptly respond to them. In order to enhance their security posture the customer needed a partner with whom they could:

- Combine their five Splunk Security Incident and Event Management (SIEM) instances into one for holistic security monitoring and response
- Normalize all log and data sources for consistent ingestion and SIEM actioning
- Fully outsource a Security Operations Center (SOC) to establish 24x7x365 security monitoring capabilities consistently across all business units
- Ensure the SOC monitors, validates, and triages alerts properly to notify and enable the internal security team of incidents to remediate
- Collaborate with the MSSP to build a security maturity roadmap and enhance security capabilities over time
- Utilize Cyber Threat Intelligence (CTI) to enrich threat landscape understanding and quality of context delivered for incident response (IR)

The Criteria

The CISO and his team initiated a bid process and met with over a dozen MSSP's to evaluate their capabilities and find the provider that would best meet their criteria. Following are their key requirements in a new partner:

- Deep Splunk Enterprise Security engineering and monitoring expertise
- Cloud-first Security Operations (SecOps) model
- Responsive team of analysts to collaborate with and learn their particular threat landscape
- Fully managed 24x7x365 SOC
- Trusted partner to work with to enhance security maturity over time
- Application and sharing of Cyber Threat Intelligence (CTI) for enhanced incident context delivery to the Incident Response team
- Dedicated, proactive threat hunting

Outcomes

The customer selected deepwatch to normalize and standardize log and data ingestion across all five business units and combine it all in one overarching Splunk environment. The deepwatch team began the engagement by evaluating each business unit's security posture utilizing the deepwatch Maturity Model. Once a base maturity score was set for each business, and the conglomerate as a whole, the team went to work. Within 45 days the customer was fully onboarded and their named squad of deepwatch Managed Detection & Response (MDR) Service security analysts were protecting their network on a 24x7x365 basis.

The CISO, an experienced cybersecurity veteran, understood the need to stay ahead of the threats impacting their business. One of the core criteria in selecting deepwatch was the threat hunting activities embedded in the MDR service. The CISO and his security directors meet with their deepwatch threat hunting team on a monthly basis to review the MITRE ATT&CK framework and assign particular Tactics, Techniques, and Procedures for the deepwatch team to focus on. Fueled by Digital Shadows and open-source CTI, the threat hunter and his squad uncovered dormant threats on the customer network, provided rich context around active threats, and helped the customer's IR team resolve incidents before the business incurred any damage to its network, customers, or reputation.

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