deepwatch™

CUSTOMER SUCCESS STORY

Manufacturing Case Study

ABOUT DEEPWATCH

Deepwatch is the leading managed security platform for the cyber resilient enterprise. One of the fastest growing cybersecurity companies, we operate as an extension of our customer's team by providing 24x7x365 comprehensive security management for unparalleled visibility, precision response to threats and the best return on your security investments. With a customer base growing at nearly 75% annually, many of the world's leading brands, including John Deere, GPC, Grainger, New Balance, and Wawa rely on the Deepwatch platform to reduce risk, improve their security posture and give them peace-of-mind cyber resiliency.

CUSTOMER

This Deepwatch customer, a global manufacturing conglomerate with five distinct business units, had been working with a managed security service provider (MSSP) that did not meet the level of service and accuracy in delivery required to defend their network from growing threats.

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:

CHALLENGE

- 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

ENTERPRISE DETAILS

Industry: Manufacturing

Security Team Size: 22

Revenue: $5 Trillion

Endpoints: 40,000

- **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**

- 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)
- 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)

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
- Trusted partner to work with to enhance security maturity over time
- Cloud-first Security Operations model
- Application and sharing of cyber threat intelligence for enhanced incident context delivery to the Incident Response team
- Fully managed 24x7x365 SOC
- Dedicated, proactive threat hunting

OUTCOMES

The CISO, an experienced cybersecurity veteran, understood the need to stay ahead of threats impacting their business. One of the core criteria in selecting Deepwatch was the threat hunting activities embedded in our MDR service. Today 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 (TTPs) for the Deepwatch team to focus on. Fueled by Digital Shadows and open-source CTI, a 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.

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. Our team began the engagement by evaluating each business unit's security journey utilizing the Deepwatch Security Posture Score. Once a base security posture score was set for each business and the organization as a whole, the team went to work. Within 45 days the customer was fully onboarded and their named squad of Deepwatch MDR security analysts began work protecting their network 24x7x365.

deepwatch™

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

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com