



JOINT SOLUTIONS BRIEF

Deepwatch & Splunk Joint Solution Brief

Security Incident & Event Management

OVERVIEW

At the heart of Deepwatch Managed Detection & Response (MDR) services is Splunk. Partnering with Splunk provides collection and telemetry of data sources, powering Deepwatch detection, investigation, and response services to empower enterprise observability and unified security in hybrid environments.

Splunk captures, indexes, and correlates data in a searchable container from which the Deepwatch SecOps platform performs contextual analysis of the security to allow Deepwatch analysts to detect, respond and offer guidance on cyber attacks.

USE CASE SUMMARY

SCALABILITY AND CONSISTENT DATA USEABILITY AND AVAILABILITY

Splunk hosts one of the largest groups of technology partners and development communities actively developing apps to aid data ingestion and normalization with their platform. This leads to easy ingestion of data from the outset, without the need for engineering resources to spend their time creating new data parsers for common data sources. This combined with their Common Information Model (CIM), allows for easy ingestion of data and ability to search across the Enterprise and scale, a necessity for mature security organizations.

The architecture of Splunk allows Deepwatch to support a broad variety of organizations, both those with less than a 1,000 employees to the global Fortune 500 businesses with terabytes of data. With Deepwatch and Splunk, SecOps teams scale with a common, integrated platform that improves usability of data and your team's ability to communicate risk throughout the organization.

CONTEXT RICH ALERT, TRIAGE, AND RESPONSE

Deepwatch's content engineering team develops new detections, leveraging the power of Splunk to normalize events across disparate data sources and to perform complicated correlations to detect threats. In this way, important artifacts for detecting and responding to threats can be correlated no matter whether an individual workstation or a cloud application.

DEEPWATCH'S THREAT HUNTING AND THREAT INTELLIGENCE TEAMS

Deepwatch's Threat Hunting team performs proactive threat hunts across our customer base using intelligence from our customers and from our Adversary Tactics and Intelligence (ATI) team, which includes our Adversary Intelligence and Adversary Response teams. This cross-team partnership enables Deepwatch to rapidly hunt our customers' environments for evidence of real and likely threats to their business.

Additionally, Deepwatch's ATI team produces a weekly cyber intelligence brief (CIB) for our analysts and customers alike to stay up-to-date with changes in the cybersecurity threat landscape and enact that intelligence in our alerting and our hunting.



Splunk Inc. (NASDAQ: SPLK) turns data into doing with the Data-to-Everything Platform. Splunk technology is designed to investigate, monitor, analyze and act on data at any scale.

BEST PRACTICES THROUGH COMBINED ENGINEERING AND SECURITY EXPERTISE

Lessons learned across hundreds of customer Splunk environments makes Deepwatch an ideal MDR partner, helping you maximize your Splunk deployment. We work closely with engineers and architects to establish a shared understanding of your assets, your critical data, and security outcomes.

CUSTOMER MATURITY AND USE CASE SOPHISTICATION GROWTH

As SecOps teams mature or add capabilities, Deepwatch helps them communicate value and impact. With Splunk and the Deepwatch SecOps platform, teams can quickly show use cases for visibility and risk mitigation. The Deepwatch Maturity Model creates a baseline for your team's growth based on industry peers. With frameworks like MITRE ATT&CK integrated into the Deepwatch platform, we help you establish a roadmap for a successful cybersecurity journey.

MORE RAPID RESPONSE

Faster detection through Deepwatch and Splunk leads to faster response. Shared tools and expertise, and the US-based team of dedicated Deepwatch Squad members maximize your Splunk investment and lead to better security outcomes.



deepwatch™

ABOUT DEEPWATCH

Deepwatch, a leader in managed detection and response (MDR) services, protects our customers from ever-increasing cyber threats 24/7/365. Powered by curated threat intelligence produced by our Threat Intel Team, our cloud-based security operations platform provides the industry's most comprehensive detection and automated response to cyber threats. In addition, dedicated experts provide our tailored guidance to mitigate risk and measurably improve security posture. As a result, hundreds of organizations, from Fortune 100 to mid-sized enterprises, trust Deepwatch to protect their business.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550

Tampa, FL 33607

www.deepwatch.com