deepwatch + splunk>

deepwatch and Splunk Joint Solution Brief

SECURITY INCIDENT & EVENT MANAGEMENT

Joint Solution Overview

After stringent testing and customer feedback, deepwatch chose Splunk as its only Security Incident & Event Management (SIEM) platform to deliver Managed Detection & Response (MDR) services to our customers.

Splunk enables deepwatch to protect and defend customer networks by fully managing their threat detection and response capabilities. Splunk serves as deepwatch's main platform to deliver customers leading Security Operations Center (SOC) capabilities. deepwatch has fully integrated Splunk with our Cloud SecOps Platform and our Security Orchestration Automation and Response (SOAR) technology for reliable security event monitoring and response.

JOINT SOLUTION BENEFITS

- **Leading threat detection, alerting and response fueled by rich context**
- **Unmatched customer data usability, enrichment, and availability**
- **Customer-specific deployments and security use case execution**

deepwatch and Splunk Use Case Overview

LOG, DATA, AND CYBER THREAT INTELLIGENCE INGESTION (CTI) FOR CONTEXT RICH TRIAGE, ALERTING, AND RESPONSE

With the Splunk platform, deepwatch is able to ingest logs, data, and CTI, and index those on a continuous basis, regardless of the source type. Armed with context rich alerts deepwatch security analysts and threat hunters are able to properly triage, escalate, and respond to security events. Ensuring that our customers only need to focus on real threats to their business and are armed with rich context for rapid response.

SCALABILITY AND CONSISTENT DATA USABILITY AND AVAILABILITY

deepwatch leverages Splunk's industry leading scalability, high availability, and disaster recovery capabilities to ensure quick new data source ingestion and coverage, as well as consistent MDR customer service delivery and data portability. Our customers know they are protected and can mature their security operations quickly and easily.

SUPERIOR CUSTOMIZABILITY TO MEET UNIQUE CUSTOMER REQUIREMENTS

deepwatch customizes each customer's Splunk deployment to ensure that it meets their unique criteria, security use cases, and environment. We monitor and alert what is critical and unique to your environment.

CUSTOMER MATURITY AND USE CASE SOPHISTICATION GROWTH

As customers grow their security capabilities and maturity, deepwatch is able to accommodate and meet new security use cases quickly utilizing the Splunk platform and its rapid data ingestion and visibility capabilities.

splunk>

ABOUT SPLUNK

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.

deepwatch

ABOUT DEEPWATCH

deepwatch secures enterprises via its unique, highly automated cloud based SOC platform backed by a world class team of experts that protect your network and digital assets 24/7/365. deepwatch extends your team and proactively improves your cybersecurity posture via our proprietary maturity model. deepwatch's managed security services are trusted by leading global organizations.

CONTACT US

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