deepwatch™

THE NEXT STEP IN OSDA

Open Security Data Architecture + Microsoft Sentinel

A new Deepwatch capability to further support our customers and provide unmatched cyber resilient solutions.

WHY DEEPWATCH + MICROSOFT SENTINEL

Microsoft Sentinel is a security information and event manager (SIEM) whose presence and capabilities are growing constantly. While Microsoft Sentinel is an incredibly powerful SIEM for Mircosoft tools and products, it is still a SIEM with all the complexities, ingestion, normalization, investigation, and search concerns of any other SIEM.

Deepwatch provides years of experience and understanding of the Microsoft ecosystem to enable effective operationalization alongside expansion.

These years of experience allow Deepwatch Security Experts to provide ongoing guidance around logging and visibility needs, content packs, event code tuning, and standard and modified detection capabilities. This is accomplished through:

Data Source Selection and Management

- ✓ Security Logging vs Operational Logging
- ✓ Event Codes and Content Packs
- ✓ Security Index qualified sources

Advanced Detection Management

- ✓ SOC Best Practices Tuning
- ✓ Currated Threat Hunting
- ✓ KQL Detection Optimization

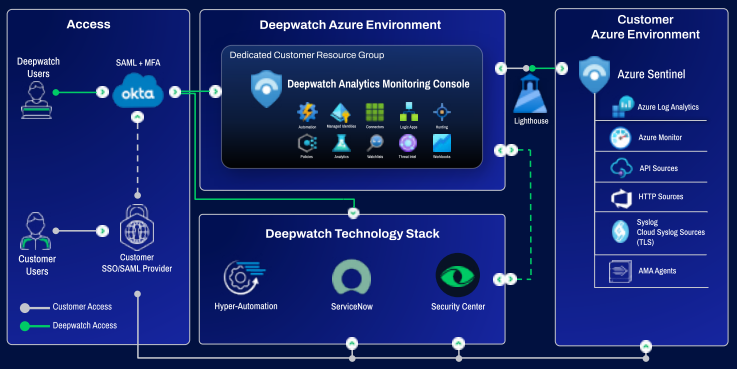
Operational Resilience

- ✓ 24/7 Security Operations Management and Monitoring
- ✓ Sentinel Health Monitoring
- ✓ Zero to Retainer Coverage

www.deepwatch.com

Benefits

- ✓ Flexibility - Customers have guided support on the implementation, migration, and optimization of Microsoft Sentinel
- ✓ Increased Value - Guidance and control over the ingestion possibilities and costs associated with MS Sentinel
- ✓ Scalability - Understand where to go next and when with MS Sentinel capabilities



deepwatch™

DEEPWATCH OSDA SUPPORTS EXISTING MICROSOFT SENTINEL INSTANCES:

- Natively augments and extends Microsoft Sentinel detection and alert capabilities to enable more holistic Security Operations
- Extends correlation and enrichment capabilities to log sources and tools outside of the Microsoft ecosystem or to those not yet supported
- Enables precision responses within the Microsoft tool stack, such as MS Defender
- Allows customers to move data and logs to other storage options in their Azure cloud and still can utilize the information for investigation, triage, enrichment, and validations
- Active management of the Microsoft Sentinel instance
- Includes Deepwatch ATI curated threat intelligence and threat hunting

DEEPWATCH EXPERTS

Deepwatch is at the forefront of cybersecurity solutions, particularly in Microsoft Sentinel expertise. Our team of experts possess decades of combined Security Operations experience and understand not only the day-to-day alerting and response, but also the visibility, engineering, and daily engineering requirements necessary to empower cyber resilient enterprises. Coupled with a deep understanding of Microsoft Sentinel and Microsoft Azure (AZ-500 and SC-200 certified), our experts ensure customers receive comprehensive support tailored to their specific needs. This expertise is especially beneficial for businesses deeply entrenched in the Microsoft ecosystem, offering enhanced security measures to combat evolving cyber threats effectively.

DEEPWATCH PAVING THE WAY TO CYBER RESILIENCE WITH OSDA

The Deepwatch Open Security Data Architecture enables Deepwatch to support multiple SIEMs, XDR, Endpoint, Identity, Cloud, Exposure, and Vulnerability data sources and to utilize these technologies to secure assets and maximize security spend. The challenges of changing or adding security technologies are ever-present, and getting value as quickly as possible is critical. OSDA solves that.

Deepwatch OSDA empowers customers with flexibility in security tooling, data aggregation, and storage. By alleviating the constraints of relying on a single security data repository, OSDA will enable better utilization of native analysis capabilities across a diverse range of already deployed security tools. This migration away from expensive SIEM ingestion and storage models addresses cost concerns and enhances detection and response capabilities without compromise.

deepwatch™

ABOUT DEEPWATCH

Deepwatch is the leading managed security platform for the cyber resilient enterprise. Our platform combines comprehensive threat management capabilities, expert practitioners, and precise automated actions. Embrace preventative actions to improve your security posture and enhance your speed of response. Join leading global brands relying on Deepwatch for cyber resiliency and security peace of mind.

CONTACT US

GET STARTED

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

www.deepwatch.com