

MOVING BEYOND MDR: THE NEXT STEP

Open Security Data Architecture (OSDA)

The Open Security Data Architecture enables Deepwatch to have more flexibility in supporting technology choices of the future.

THE NEED FOR MODULAR CYBERSECURITY SOLUTIONS

Security tooling, visibility, and logging requirements continue to expand in both scope and complexity, resulting in increasing costs and the creation of blind spots and detection limitations due to budget constraints.

As an industry, we have to realize a more modular approach to our tooling, data collection, detections, and response capabilities, else our expected outcomes will not fully materialize. Modularity in this sense is based on the flexibility to utilize data and logging where it resides while maintaining best-of-breed detection and response capabilities across a range of security tools or platforms.

This balance can be achieved through active management of tooling, selective ingestion and processing of signal flows, data standardization, and active responses, coupled with both GenAI-led analysis and Security Expert guidance.

DEEPWATCH PAVING THE WAY TO CYBER RESILIENCE

Deepwatch knows the challenge of adding or changing security technologies and getting value out of them as quickly as possible. OSDA will enable Deepwatch to support multiple SIEMs, XDR, Endpoint, Identity, Cloud, Exposure, and Vulnerability to utilize these technologies to secure assets and maximize security spend.

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 not only addresses cost concerns but also enhances detection and response capabilities without compromise.

Benefits

- ✓ Flexibility - Customers are no longer dependent on monolithic SIEMs/one source
- ✓ Better ROI - Optimization of your costs and tool effectiveness
- ✓ Scalability - Adapt to the growing complexity of cybersecurity challenges

Cyber Resilience

OSDA provides the ability to continue to mature security operations with Deepwatch regardless of the choices of where to log, aggregate, and store security data.

This is the beginning of Deepwatch laying out an exciting future of possibilities for our customers in expanded data flexibility, coordinated responses, and updated operational capabilities.

