Managed XDR with SIEM/SOAR

Solution Brief

Managed XDR with SIEM/SOAR

Our Global Managed Services team for XDR with Managed SIEM supports (MXDR) Check Point, Microsoft Sentinel and Microsoft Defender for XDR solutions. The scope of our managed services covers SIEM and event ingestion management, analytics and threat detection tuning, expert threat hunting, incident handling led by security analysts, and troubleshooting.

Check Point IGS Managed Services also offers a tight integration with Check Point Horizon MDR for advanced and rapid Detection and Response Services. We also offer a SIEM-as-a-Service option for XDR that includes 200 MB of daily SIEM-as-a-Service event ingestion per device or user.

Comprehensive Scope Coverage

1

Configured to work alongside Check Point and 3rd party products

2

Native Integration with Microsoft 365, Azure and Defender for XDR

3

Configuration, Programing, and 3rd party product event ingestion

4

Incident Handling and Advanced Product Support

5

Co-authored runbook, communication plan and Ticketing Integration

6

Assigned Teams with primary engineer and Service Delivery Coordinator

Managed XDR with SIEM/SOAR

Delivery

The first step is to understand the specific needs of the organization. This involves evaluating the current cybersecurity, compliance and SIEM requirements, identifying pain points, and determining the organization's goals and budget.

Our team will then work with you to integrate with existing security operations and configure the XDR and SIEM solutions to ensure they are functioning effectively and securely.

Integrated Visibility

Security visibility across an organization's entire network (endpoints, cloud infrastructure, mobile, etc.).

Rapid Time to Value

Out-of-the-box integrations and pre-tuned detection mechanisms across multiple different products

Improved Productivity

Eliminates the need for security analysts to switch between multiple dashboards and manually aggregate security data.

Rapid Unified Detection and Response

Centralized and unified incident response capabilities across all environments composing an enterprise network.

Improved Overall Attack Understanding

Gathers and aggregates signals from multiple sources, strengthening them and enabling an organization to detect and respond to attacks that may have otherwise been overlooked.

Managed Services

CPTS-MSS-MDR-ADV-1Y Managed XDR with Managed SIEM - per device or user, for 1 year (Minimum Qty 100)	**CPTS-MSS-MDR-ADV-S-1Y** Managed XDR with SIEM-as-a-Service - per device or user, for 1 year (Minimum Qty 100)

Learn more about Infinity Global Services