MANAGED SECURITY SERVICES

Flexible and Scalable Solutions to Improve Your Security Capabilities

OVERVIEW

Security threats continue to rise each year and are increasing in sophistication and malicious intent. Unfortunately, security operations teams are constrained by the lack of qualified staff and limited budgets. This creates a dilemma between selecting the correct security programs or enhancing your security environment. With the right partner, you can do both.

Optiv's Managed Security Services (MSS) are enabled by teams of threat analysts and security engineers from multiple operations centers to support your organization on-demand 24x7x365. Optiv MSS provides solutions that help you to achieve more by expanding your security program and improve detection through continual monitoring. Our services are designed to enhance your ability to detect and respond to threats and serve as a remote extension of your security staff. We do this by providing the following suite of turnkey solutions to answer your complex information security challenges.

FLEXIBLE SOLUTIONS

Platform Management
Receive release, device incident, problem and change management.

Authorized Support
Quickly and proficiently resolve Tier 1, 2 and 3 technical support issues when they arise.

Cyber Threat Intelligence-as-a-Service
Monitor and respond to threats facing you from the clear, deep and dark web.

Enhanced Threat Analysis
Receive managed detection, response and remediation of malware threats.

Co-Managed SIEM
Leverage existing technology investments and restrict what data leaves the client premises.

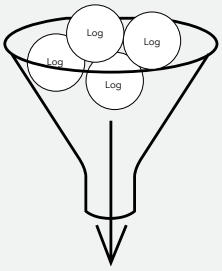
Hosted SIEM
Receive log management, monitoring, alerting and reporting.

Vulnerability Management
Run scans to identify exposures and see tempered results.

Endpoint Management
Ensure your systems are deployed, up-to-date and optimally configured.

24 x 7 x 365
Operations

140+ Engineers and Analysts



70 Billion
Logs per Day

All MSS offerings are delivered through our three Security Operations Centers (SOCs), located across the United States. Our SOCs are state-of-the-art facilities designed specifically for security operations.

Co-Managed SIEM

Goal

Leverage your existing SIEM investment to provide monitoring and management using best practices.

Overview

Our co-managed SIEM offering leverages your existing investments and restricts what data leaves your premises. Our certified team of SIEM engineers performs ongoing management while threat analysts triage your security events and deliver actionable findings.

SERVICE COMPONENTS

- Release Management
- Change Management
- Problem Management
- Incident Management (DHPM)
- Alert Triage

SELECT PARTNERS

- IBM, LogRhythm, McAfee, Splunk

Hosted SIEM

Goal

Provide you with a system for log management and monitoring, alerting and reporting using a hosted multi-tenant solution.

Overview

Our Hosted SIEM offering reduces the complexity of deploying an on-premise solution by leveraging Optiv's own multi-tenant solution. Our certified team of SIEM engineers perform ongoing management while threat analysts triage your security events and deliver actionable findings.

SERVICE COMPONENTS

- Log Management
- Log Monitoring and Reporting
- Change Management
- Problem Management
- Incident Management (DHPM)
- Alert Triage

SELECT PARTNERS

- LogRhythm

Authorized Support

Goal

Deliver expert support services for quick remediation when you encounter technical problems.

Overview

Our Authorized Support service helps your organization resolve technical problems through efficient and trustworthy technical support. Optiv's certified experts are equipped with deep product knowledge and will provide timely response and issue remediation.

SERVICE COMPONENTS

- Incident Management
- Return Merchandise Authorization

SELECT PARTNERS

- Check Point, Cisco, F5, Fortinet, Juniper Networks, McAfee, Palo Alto Networks, Pulse Secure, Symantec

Platform Management

Goal

Manage your security devices and monitor their health and performance to improve your security posture.

Overview

Our Platform Management service optimizes your security technologies through continuous issue discovery and resolution. With experience supporting and managing thousands of devices, our certified security professionals quickly respond to your device issues and help improve your security posture.

SERVICE COMPONENTS

- Release Management
- Change Management
- Problem Management
- Incident Management (DHPM)

SELECT PARTNERS

- Check Point, Cisco, F5, Fortinet, HP, IBM, Juniper Networks, McAfee, Palo Alto Networks, Pulse Secure, Symantec

Supported Platforms

FIREWALLS	NETWORK IDS/IPS	UTM	SSL VPN
› Cisco, Juniper Networks, Palo Alto Networks, Fortinet, Check Point	› Check Point, Cisco, HP, Fortinet, Juniper Networks, McAfee, Palo Alto Networks	› Check Point, Fortinet, Juniper Networks, Palo Alto Networks	› Pulse Secure
WAF	**FIREWALL MANAGEMENT**	**LOAD BALANCING**	**PROXY**
› F5	› Firemon	› F5	› Symantec

Vulnerability Management

Goal

Provide ongoing vulnerability scans and deliver tempered results to help you understand which vulnerabilities are being exploited in the wild so you can prioritize patches.

Overview

Our Vulnerability Management service helps your organization remain confident that its network and applications are secure. Using proven methodologies, our highly trained staff identifies vulnerabilities and validates findings.

SERVICE COMPONENTS

- Deployment and Integration
- Asset Discovery and Asset Management
- Scan Management
- Vulnerability Reporting and Guidance

SELECT PARTNERS

- Qualys

Endpoint Management

Goal

Deliver day-to-day management and monitoring of your endpoint technology.

Overview

Our Endpoint Management service is designed to help clients deploy, operationalize and ensure they are getting the most value out of their endpoint technology.

SERVICE COMPONENTS

- Release Management
- Change Management
- Problem Management
- Incident Management (DHPM)
- Alert Triage

SELECT PARTNERS

- McAfee

Enhanced Threat Analysis

Goal

Identify the real threats in your environment and provide context and actionable steps to help you eliminate them.

Overview

Optiv's expert threat analysis team uses advanced tools and techniques to help investigate incidents 24x7x365. Static and dynamic analysis of your malicious samples accelerates your response times and helps you contain malicious threats more effectively.

SERVICE COMPONENTS

- Alert Investigation
- Incident Notification
- Sample Analysis
- Hunting and Containment
- Intelligence Integration

SELECT PARTNERS

- Carbon Black

Cyber Threat Intelligence-as-a-Service

Goal

Monitor and respond to threats facing you from the clear, deep and dark web.

Overview

This solution provides you with an advanced "beyond the perimeter" capability as a part of your cyber security program. Our team of CTI professionals use a fully automated threat data collection and analytics platform to prioritize alerts regarding your adversaries' tactics, techniques and procedures (TTPs).

SERVICE COMPONENTS

- On-Site Workshop
- Workbook Development
- Alert Monitoring
- Alert Investigation
- Reporting
- Remediation/Take-Down

SELECT PARTNERS

- IntSights