Security Operations

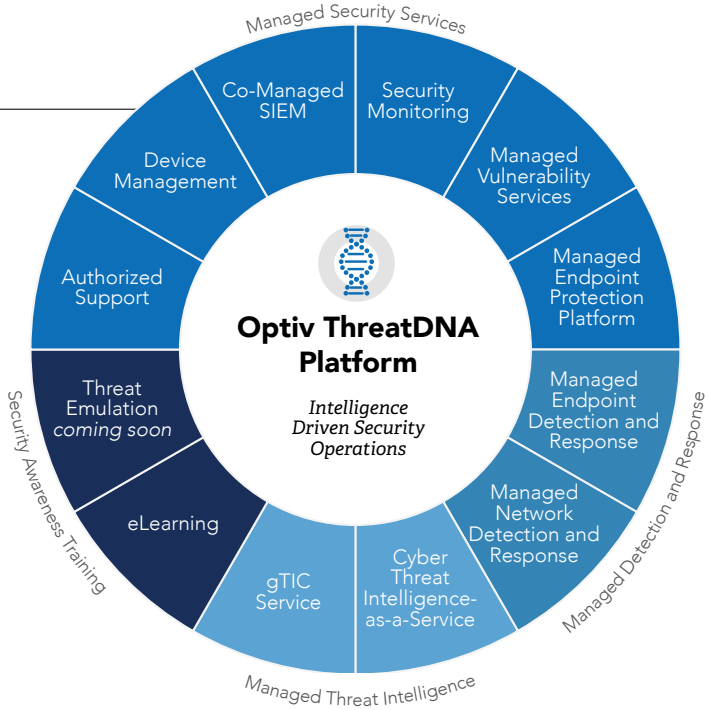
Flexible and Scalable Solutions to Improve Your Security Capabilities

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 choice between your budget and your risk. With the right partner, you don't have to choose.

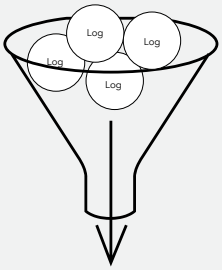
Optiv's Managed Security Services (MSS) are enabled by teams of analysts, security engineers and world-class security practitioners from multiple centers to support your organization on-demand 24x7x365. Optiv MSS provides solutions that help you to achieve more by expanding your security program and 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



24 x 7 x 365
Operations

200+ Experts, 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.

MANAGED THREAT INTELLIGENCE

Global Threat Intelligence Center

Goal

Access to latest global threat intelligence to stay ahead of potential attacks specific to your company and mission.

Overview

Optiv's Global Threat Intelligence Center (gTIC) develops security alerts and bulletins surrounding high-value, industry affecting threats and vulnerabilities. In addition, the gTIC staff monitors global events and disseminates threat reports in conjunction with potential campaigns that could affect Optiv clients.

Service Components

- Daily Situation Report
- Weekly Intelligence Summary
- Monthly Threat Landscape
- Quarterly Intelligence Briefing
- Critical Advisories
- Threat Feeds

Cyber Threat Intelligence-as-Service

Goal

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

Overview

Optiv's Cyber Threat Intelligence-as-a-Service 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

- Workbook Development
- Alert Monitoring
- Alert Investigation
- Reporting
- Remediation/Take-Down

MANAGED DETECTION AND RESPONSE

Managed Network Detection and Response

Goal

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

Overview

Optiv's Managed Network Detection and Response service uses data analytics and full packet capture technology to deliver 24x7 threat monitoring, alert investigation and event and file analysis. Our experts co-manage your packet capture platform to deliver on change requests, data source classification and groupings, native reporting, platform incident management, problem management, health checks and release management.

Service Components

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

Managed Endpoint Detection and Response

Goal

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

Overview

Optiv's Managed Endpoint Detection and Response (MEDR) service augments your next-generation endpoint solution's detection capabilities by continuously monitoring incidents and shortening your response times. Our expert threat analysis team uses advanced 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

MANAGED SECURITY SERVICES

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

- Aruba, Check Point, F5, Fortinet, Juniper Networks, McAfee, Palo Alto Networks, Pulse Secure, Symantec (Blue Coat)

Device Management

Goal

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

Overview

Our Device 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)

Supported Platforms

- Firewall, Next Generation Firewall, Unified Threat Management, Network Intrusion Detection and Prevention, SSL VPN, Web Application Firewall, Load Balance, Web Proxy

Co-Managed SIEM

Goal

Leverage your existing SIEM investment to provide management and monitoring 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

Security Monitoring

Goal

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

Overview

Our Security Monitoring 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

Managed Vulnerability Services

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 Managed Vulnerability Services help 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

Managed Endpoint Protection Platform

Goal

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

Overview

Our Managed Endpoint Protection Platform 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

SECURITY AWARENESS TRAINING

eLearning

Goal

Simplify your training initiatives, providing a cost-effective, easy-to-use solution that helps you meet compliance, maximize data security and ensure training best practices are in place.

Overview

Optiv offers engaging, interactive eLearning courses that cover a range of security topics including security awareness, compliance, secure coding and application development.

Service Components

- Security Awareness featuring CyberBOT
- Security Awareness Circuit Training
- Credit Card Handling
- Introduction to PCI
- Secure Coding Java/NET
- OWASP Top 10
- Application Security
- Mobile Security Top 11
- Web 2.0 Secure Coding

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com