SERVICE BRIEF

Azure Sentinel Co-Managed SIEM

A Bird's-Eye View Across Your Enterprise

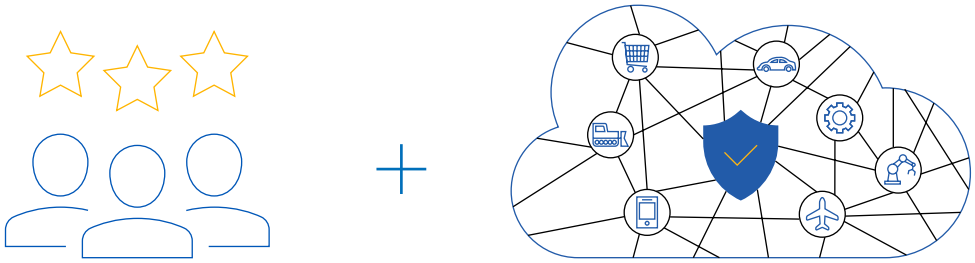
Effectively managing and monitoring your SIEM technology requires an intricate balance of people, processes and technology. This challenging task is made even more difficult with an increasing volume of threats across an expanding attack surface, evolving compliance demands, talent shortages and tight budgets.

Optiv's Co-Managed SIEM services are delivered by the Optiv Security Operations Center (SOC) to provide clients with collaborative service components to ensure preventive and ongoing real-time operational measures. With our co-managed SIEM services, clients can expand their security program capabilities allowing for a scalable and repeatable way of operationalizing procedures with management and monitoring of your Azure Sentential SIEM technology.

Azure Sentential has reinvented SIEM for today's digital world by making your threat detection and response capabilities smarter and faster with artificial intelligence (AI). Together, we empower your organization to classify, prioritize, investigate and resolve security threats to stop breaches.

Optiv + Microsoft Partnership Advantage

- 40+ Certified Microsoft Experts
- 140+ Solution Architects
- 100+ Global Security Advisors
- All Optiv Services in the One Communications Platform (OPC) Catalog
- 350+ Technology Integrations on Azure



OPTIV'S SECOPS TEAM + **AZURE SENTINEL**

Expected Outcomes

Achieve improved risk awareness, accelerated responses, proactive defenses to meet your security needs—while reducing costs.

Release Management
Maintains software currency

Change Management
Implements changes to configuration and security policies

Incident Management
Delivers device health and performance monitoring

Security Alert Monitoring
Provides monitoring, alerting and reporting of security events

Advanced Analytics
Delivers customized dashboards, visualizations and deep insights into data sources

Comprehensive Threat Hunting
Proactively and continuously searches to detect and isolate advanced threats

Why Clients Choose Optiv for Azure Sentinel Co-Managed SIEM

Dedicated Technical Project Manager throughout service integration

Designated Client Success Manager advocates for the client to ensure maximum value is being derived from our services

Certified experts drive operations, shape policy and lead response efforts for our clients leveraging threat intelligence from Optiv's gTIC (Global Threat Intelligence Center)

Future-proof planning to help clients develop a straetgy that maximizes and communicates the effectiveness of their security program

How Optiv Delivers Co-Managed SIEM and Security Monitoring Services

From start to finish, our threat analysts triage alerts and provide actionable results for every alert.

Alert Ingestion
Threat analyst acknowledges and reviews security alert within the portal's prioritized alert queue that is monitored 24x7x365

Alert Triage
Threat analyst uses intelligent queries, history and SIEM events to determine need for further investigation or if it's non-actionable/a false positive.

Incident Closure
Optiv SOC staff closes incident upoon client confirmation that the incident has been resolved.

Alert Analysis
Security alerts are investigated using human analysis and automation.

Alert Remediation Support
Optiv SOC staff collaborate with client in support of remediation efforts.

Alert Escalation
Alerts containing suspicious or potentially malicious activity that could impact client may be escalated for further investigation.

What's Next?

To get started, ask your local Optiv representative how Optiv and Azure Sentinel can help you prevent, detect and respond to today's challenging security threats.

Microsoft Partner
Microsoft
Gold Cloud Platform
Silver Application Development

Member of Microsoft Intelligent Security Association
Microsoft

OPTIV

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

Secure your security.™

Optiv is a security solutions integrator – a "one-stop" trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.