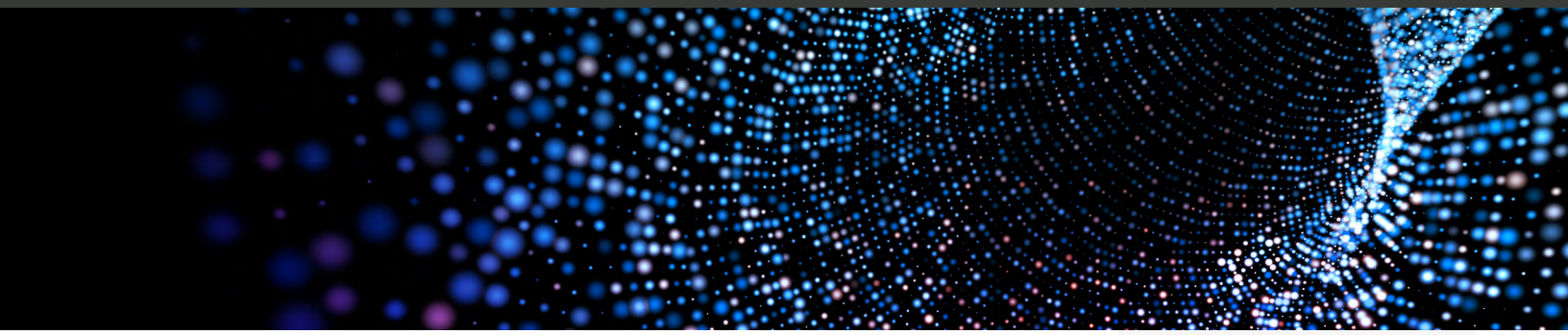

PARTNER SERVICE BRIEF

# Azure Sentinel Deployment and Migration Services

## A faster, more successful, more secure and more integrated approach for Azure Sentinel

Security architecture and infrastructure has become increasingly complicated. Securely deploying and migrating technology into your unique environment is critical for mitigating threats and reducing risk. Optiv provides professional service engagements focused on the migration, implementation and initial configuration of Azure Sentinel solutions into your environment. Our expertise and services enhance security visibility within your enterprise and assist with streamlining security investigations.

### OPTIV + MICROSOFT PARTNERSHIP ADVANTAGE

- **40+** Certified Microsoft Experts
- **140+** Solution Architects
- **100+** Global Security Advisors
- **Gold:** Security
- **Gold:** Cloud Productivity
- **Gold:** Cloud Platform
- **Silver:** Datacenter
- **Silver:** Application Development
- All Optiv Services in the **One Communications Platform (OPC)** Catalog
- **350+** Technology Integrations on Azure

Microsoft Partner — Gold Security, Gold Cloud Productivity, Gold Cloud Platform, Silver Datacenter, Silver Application Development

Member of Microsoft Intelligent Security Association

Microsoft

## Our Implementation and Migration Services include:

- Detailed assessment of your current SIEM
- Collection and integration of critical data sources
- Initial tuning of analytic rules
- Creation of workbooks
- Hunting queries
- Basic incident management playbooks
- Knowledge transfer for all tasks completed by Optiv's consultant

OPTIV

# Why Clients Choose Optiv for Azure Sentinel

- Dedicated Technical Project Manager
- Designated Client Success Manager
- Certified Experts
- Future-Proof Planning

## How Optiv Delivers Deployment and Migration Services for Azure Sentinel

### PROJECT PLANNING PHASE

**Deployment:**
Identify critical data sources and plan out collection strategy including agent deployment best practices. Create a prerequisite guide for data source onboarding.

**Migration:**
Detailed review of current SIEM to identify critical data sources and use cases to be migrated to Azure Sentinel. Architecture workshop to plan out data source collection strategy including agent deployment best practices. Create a prerequisite guide for data source onboarding.

**Implementation and Data Source Onboarding:**
Enable Sentinel within client's Azure environment following Microsoft best practices. Deploy agents where required and onboard identified critical data sources. Review data ingestion of each data source.

**Content Optimization and Tuning:**
Enable Sentinel Analytics rules based on onboarded data sources and tune rules to lower false positives. Enable Sentinel workbooks to provide visibility into critical data sources. Create hunting queries based on customer use case requirements. Enable Playbooks to automate and respond to incidents.

**Project Deliverables and Closeout:**
Create a detailed summary of work performed and recommended next steps to mature the Sentinel environment.

### DEPLOYMENT AND MIGRATION SERVICE DELIVERABLES

**A Project Summary Report** containing a high-level description of the work performed, and the solution's configuration in the following:

- Summary of work performed
- Architecture diagram
- Configuration settings
- Data source details
- Recommendations and next steps

**Integrate Log Sources:**
Integration of supported Azure Service logs, as well as Authentication, Endpoint, Perimeter, Network and Email logs. Unsupported log sources may require additional time to integrate.

**Analytics Rules:**
- Enable up to 30 out-of-the-box Analytics rules
- Create up to 10 custom Analytics rules
- Tune rules to lower false positives

**Workbooks:**
- Enable out-of-the-box Workbooks associated with onboarded supported data sources
- Configure two (2) custom Workbooks

**Hunting Queries:**
- Create up to five (5) Hunting Queries

**Playbooks:**
- Enable two (2) community-supported Playbooks

**Entity Behavior (UEBA):**
- Enable Azure Entity Behavior

**WHAT'S NEXT?**

For more on Optiv's SIEM Tuning service, see www.optiv.com/explore-optiv-insights/downloads/optimization


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, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more costefficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are modernizing cybersecurity to enable 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.