Go beyond ‘one-and-done’ SIEM services

Security architecture has become increasingly complex. As an essential information security tool, security information and event management and user and entity behavior analytics (SIEM/UEBA) solutions make it easier for organizations to manage security by streamlining security investigations, filtering and prioritizing large amounts of security data, and enabling organizations to detect incidents that may otherwise go unnoticed.

How We Do It

Our SIEM/UEBA maturity program is a series of weekly or bi-weekly, pre-scheduled, fixed-fee sessions based on client requirements.

Our Maturity services help clients who do not have the in-house resources or expertise to confidently manage SIEM, and therefore struggle with low threat visibility and correlating security incidents to actionable intelligence. This partnership is designed to more effectively mature the SIEM environment and strengthen security posture as the threat landscape inevitably evolves.

Sessions can include:

**SIEM administration configuration and review**
- SIEM best practice configurations
- Health check and remediation

**Use case creation and tuning, including:**
- Correlation rules
- Dashboard creation
- Reports
- Playbooks/ Security Orchestration, Automation and Response (SOAR)

**Data source ingestion, including:**
- New data source onboarding
- Custom parsing and normalization

Optiv Solutions

With expertise in a wide range of top SIEM/UEBA solutions and industry best practices, Optiv provides professional service engagements designed to support clients wherever they are in their SIEM journey. From implementation and migration to regular tuning of and co-managing the SIEM environment, our expertise enhances security visibility across your enterprise.

Optiv’s SIEM Maturity service extends beyond base SIEM services to bring a more proactive approach to security visibility, ensuring protection against continuously developing threats.
Why Clients Choose Optiv

Optiv approaches all engagements with a client-focused process for assessing and reviewing security solutions. Our consultants have deep expertise in not just one security vendor or use case, but across the entire security stack. We also leverage our experience with requirements and capabilities as developed by vendor clients.

SIEM Services

- **Deployment and migration:** used for an initial deployment or migration of a client-selected industry SIEM, the engagement includes configuration of the SIEM environment, the collection and integration of critical data sources, initial tuning of correlation rules, creation of dashboards, searches and incident management playbooks.

- **Co-Managed SIEM:** with three service level options, co-managed SIEM services provide daily engagement around incident management, performance monitoring and SIEM optimization and tuning.

Case Study

A supermarket chain with more than 35,000 employees and hundreds of stores across the United States.

**Desired Outcomes**

Optiv was asked to review the health and maturity of the SIEM/UEBA platform, including hardware and software configurations, use cases, data sources and third-party integrations to improve data visibility and overall SIEM/UEBA platform effectiveness.

**Solution**

After an initial use case workshop and health assessment to prioritize any indicators of a potential cyber incident or other underlying platform issues, Optiv performed weekly optimization and fine-tuning sessions to identify and implement recommendations to mature the client’s SIEM/UEBA solution. This included reviewing data sources, improving log source visibility and parsing, providing use case recommendations and implementations, and integration of related tools into the platform.

**Client Benefits**

Through a consistent, long-term approach based on best practices, the partnership with Optiv is designed to continually identify and document issues and prioritize improvements that align with the client’s unique and changing needs over time.

**Secure greatness™**

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2022 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.