Enhancing Your Organization’s Security Posture

In today’s unpredictable threat landscape, Security Operations Centers (SOCs) must be ever-vigilant and continuously monitor real-time threat intelligence, enhance protection capabilities, perform threat hunting and support other advanced capabilities. As cyber actors continue to grow in both numbers and sophistication, SOCs are the first line of defense for organizations to prevent, detect and respond to threats.

In addition to an evolving threat landscape, enterprise networks continue to grow more complex by integrating cloud capabilities, mobile devices, IoT, etc. Therefore, SOCs are required to broaden their security visibility and ensure that their people, processes and technology are capable of defending, detecting and responding across the larger enterprise.

Optiv’s Security Operations Assessments recognize these challenges and support the reduction of enterprise risk through a comprehensive evaluation of your organization’s capability to adapt to threats and business evolutions while simultaneously supporting the defense of your critical business operations and data.

Optiv’s Security Operations Assessment Benefits

We understand the challenges faced by your organization and strive to improve your security posture and mitigate risks. Optiv will provide detailed findings and key recommendations to support security operation improvements and benefit your overall cybersecurity program.

Optiv’s Security Operations Assessments will support your organization through:

- Reduced impact of security incidents
- Reduced risk of a broader cyberattack
- Improved security event visibility
- Reduced response time

*Gartner, Selecting the Right SOC Model for Your Organization, 2018.*
How We Do It

Optiv’s assessment framework includes a comprehensive, phased approach that enables Optiv subject matter experts to conduct a comprehensive analysis of your organization’s Security Operations. Our approach includes the following phases:

1. **Initiate Assessment**
   - Includes the collection of security documentation, interviews, security procedure observations and conduct interviews.

2. **Assess Security Operations**
   - Evaluates the governance, protection capabilities, detection coverage and response processes that support your organizational security across industry standards.

3. **Assessment Report**
   - Provides a comprehensive report on all assessment domains with maturity assessment, key findings, recommended improvement areas, and a project plan with actionable steps to remediate gaps, enhance your security operation capabilities, and mature your security posture.

Optiv’s SOA Methodology is aligned with industry standards, such as NIST and MITRE, and takes a holistic approach to examine your existing security operations by evaluating and enhancing the domains aligned to your people, process and technology.