Don’t Wait for an Incident. Preempt Attackers by Optimizing and Maximizing Your Security Tech.

For security pros, it can sometimes feel like the only thing growing faster than the number of cyber threats is the catalog of tools to manage them. Many don’t even know if their solutions are effective.

Organizations must continuously mature their security environment if they want to stay ahead of hackers, who are as innovative as they are persistent. The best way to keep pace? A strategic shift towards programmatic, iterative improvement.

Source: Ponemon Survey for AttackIQ, July 2019

Optiv maturity services sessions can include:

<table>
<thead>
<tr>
<th>SIEM Services</th>
<th>Firewall Services</th>
<th>Secure Web Services (Netskope, Zscaler)</th>
<th>Endpoint Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Administration configuration and review</td>
<td>• Architecture and configuration review and recommendations</td>
<td>• Architecture and configuration review</td>
<td>• Solution health check</td>
</tr>
<tr>
<td>• Use case creation and tuning</td>
<td>• Advanced feature adoption</td>
<td>• Advanced feature adoption including:</td>
<td>• AV rules and signature updates</td>
</tr>
<tr>
<td>• Data source ingestion</td>
<td>• System update/upgrade recommendations</td>
<td>• Data loss prevention</td>
<td>• Alert tuning</td>
</tr>
<tr>
<td>• Custom parsers and dashboards</td>
<td></td>
<td>• Zero Trust network access</td>
<td>• Advanced feature adoption</td>
</tr>
</tbody>
</table>

Our maturity services extend well beyond basic implementation and optimization. We help you establish a proactive security mindset, reducing risk and getting you the most out of the technology you have.

Regular tuning delivers you from the chaos of reaction mode and allows you to prioritize applying critical adjustments and best practices.
How We Do It
Our security technology maturity program builds around a series of tailored weekly or bi-weekly fixed-fee sessions that begin with an extensive technology health check and use-case workshop or architectural review.

A regular cadence of optimization services rigorously assesses overall platform health and adjusts your current technology mix. This engagement matures your security footing, maximizes ROI and fortifies you against the environment’s inevitable evolution.

Why Clients Choose Optiv
Each of our engagements are customized to the client’s distinct technical, business and cultural dynamics. Our consultants are seasoned and tech-agnostic, informing a deep, objective view of your challenges.

Additional Technology Services

Migration and Implementation: Configure baseline capabilities or get help migrating to a new security solution

Health Check and Optimization: Ensure continued security technology effectiveness through review and remediation of identified issues so your security infrastructure is configured for optimal performance and protection

Authorized Support: Dedicated, 24/7/365 support from certified engineers with multiproduct expertise and industry best-practice savvy

Technology Management: Offload primary management responsibility for security devices or applications and ensure proactive, efficient upgrades and fault monitoring

Case Study
A supermarket chain with over 35,000 employees and hundreds of stores across the U.S.

Desired Outcomes
The client asked Optiv to review the health and maturity of its 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 potential cyber incidents or other underlying platform issues, we began weekly optimization and fine-tuning sessions to identify and implement recommendations for maturing 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
Consistent, best practice-driven methodology helps clients continually identify and document issues and prioritize improvements that align with their evolving operational requirements.

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.

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