Defend Your SCADA Devices and Data from Attack

Operational technology (OT) devices are fast becoming foundational components for effective digital transformation. Their addition to IT environments allows for improved data utilization, better technology management, increased output and reduced costs and downtime.

But the addition of these new devices and data sources fundamentally alters your organization’s threat landscape. Their sheer number and broad distribution create new vulnerabilities. Traditional network security typically can’t detect OT connections or provide adequate visibility across your expanded threat surface.

Optiv’s Harden and Connect workshop offers the knowledge, expertise and guidance you need to address your security needs and balance them with your business objectives. Optiv takes a different approach aligned to your unique business requirements and delivers an experience and outcomes that you won’t get from other providers.

☑️ Measurable, verifiable results
☑️ Radically stronger security programs
☑️ Optimized and rationalized security strategies

Using this proven collaborative process, you’ll identify, segment and protect OT devices in your distributed environment—along with the data they produce—to create an actionable plan to get you on the path to success.

Benefits of Optiv’s IoT Security Workshop

Expertise
Leverage Optiv’s OT security expertise

Objectivity
Navigate the complex vendor landscape objectively

Business Alignment
Align plans with business and technical needs

Action Plan
Develop security strategy covering people, process and technology
How We Do It

Plan For Success
We collect relevant documentation, including but not limited to business information, existing malware defenses, endpoint types, appropriate controls and staffing information.

Alignment With Business Goals
We assist with defining business and technical requirements, use cases, existing malware defenses and staffing plans based on your company’s unique needs.

Collaborative Workshop With Key Stakeholders
We work with various teams and stakeholders within your company to discuss specific recommendations for people, process and technology decisions.

Plan For Next Steps
Optiv offers additional services to get your endpoint strategy on track.
• Implementation or migration services
• Health check and optimization services

Summary and Recommendations
Your documented endpoint security strategy includes business endpoint use cases, defense category mapping, a technical requirements matrix and a roadmap to move forward.

Harden Schedule

<table>
<thead>
<tr>
<th>Workshops</th>
<th>Deliverables</th>
<th>Outcomes</th>
<th>Project Readout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kick-Off</td>
<td>Workshop</td>
<td>Harden Deliverables</td>
<td>Project Readout</td>
</tr>
<tr>
<td>• Introduction and expectations</td>
<td>• 3-day “tabletop” discussion</td>
<td>• Detailed threat and risk model</td>
<td>• Two-hour session to discuss findings</td>
</tr>
<tr>
<td>• Outcomes and deliverables</td>
<td>• Driven by two OT SMEs</td>
<td>• Gap assessment</td>
<td>• Delivery of executive summary</td>
</tr>
<tr>
<td>• Standards selection</td>
<td>• Using DHS’s CSET &amp; Optiv metrics</td>
<td>• Project scorecards</td>
<td>• Deliverables handoff</td>
</tr>
<tr>
<td>• Document requests</td>
<td>• 9–12 functional topic categories</td>
<td>• Prioritized roadmap</td>
<td></td>
</tr>
</tbody>
</table>

Workshop Details

Process
• Align IT and OT teams with one set of goals
• Assess and analyze proposed architecture
• Identify security policy gaps
• Establish programmatic area of improvement

Deliverables
• Risk assessment
• Current and future state
• Gap analysis
• Prioritized road map
• Project scorecards

Outcomes
• Recommended people, process and technology investments
• Gap assessment with priority scoring
• Cost, complexity and effectiveness analyses

Workshop Details

Process
• Align IT and OT teams with one set of goals
• Assess and analyze proposed architecture
• Identify security policy gaps
• Establish programmatic area of improvement

Deliverables
• Risk assessment
• Current and future state
• Gap analysis
• Prioritized road map
• Project scorecards

Outcomes
• Recommended people, process and technology investments
• Gap assessment with priority scoring
• Cost, complexity and effectiveness analyses

Why Clients Choose Optiv

Outcomes That Support Your Business
• Visibility of all devices connected to your network
• Reduced attack footprint
• Connect devices safely on-premises or in the cloud
• Accelerated time to market through better decision making

Certified Professionals
NERC-CIP, CISSP, IEC 62443, API 1164, GICSP and more

16+ Years
The average experience of Optiv’s Digital Transformation team

Partnerships and Awards
CyberX | Security Matters | Fortinet | Check Point Software | ARIMS
Partner of the Year 2020 | Palo Alto Networks: Cyberforce Partner of the Year (2019)

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.