Securing industrial operations in the age of interconnectivity

Industrial sectors like manufacturing, energy, and transportation are prime targets for ransomware and espionage attacks. Attackers may exploit the significant financial and logistical damage caused by even brief disruptions, increasing the likelihood of a payout. Operational Technology (OT) and Internet of Things (IoT) environments are particularly vulnerable due to outdated equipment and maintenance challenges.

The fourth industrial revolution is driven by connecting OT with IT applications, allowing for vast data processing and storage in data centers or the cloud. This convergence of traditionally isolated OT and IT networks can create new security challenges.

To address these potential challenges, Verizon proposes a six-phase security framework that can be tailored to your organization's maturity level.

A phased approach to OT Security.

Ongoing OT Operation (asset management, asset sementation, OT policy rules)

Phase 1
Increase IT/OT Environment Visibility

Phase 2
IT/OT Network Segregation

Phase 3
(Micro)-Segmentation

Phase 4
Automation and Lifecycle Management

Phase 5
Secure Remote Access

Phase 6
Behavior-Based Traffic Analysis

verizon business

Phase 1: Increase IT/OT Environment Visibility

Verizon's Cybersecurity Consulting Services can help you understand the interconnected devices in your industrial environments. Through comprehensive asset discovery and assessment, Verizon can provide visibility of your OT/IoT devices and their associated risks.

Our Operational Technology and Controls Systems (OTACS) assessment evaluates your operational security against industry best practices to help identify gaps in your defenses by examining people, processes, and tools.

Phase 2: IT/OT Network Segregation

By implementing physical or virtual firewalls, Verizon can segregate your OT network from your IT network. Essential security controls like threat prevention, anti-malware, Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) and DNS protection can be activated.

Our certified consultants can implement these controls, and our Security Operations Centers (SOCs) can manage them. From this phase onward, Verizon utilizes partnerships with leading security vendors to help implement necessary hardware and robust management.

Phase 3: (Micro)-Segmentation

Following the Purdue Model, experienced Verizon consultants can establish micro-segmentation within the OT environment. This involves creating standardized and repeatable security blueprints with distinct security zones and policies across your facilities, which our consultants can implement on existing security controls.

Phase 4: Automation and Lifecycle Management

Verizon develops OT-specific playbooks to help streamline the creation and updating of security rules, using your existing tools or through script development. Verizon can manage the lifecycle of devices to keep them aligned with required security controls and placed in an extra security zone when no proper maintenance is possible.

This phase can also include the implementation of a Security Orchestration, Automation, and Response (SOAR) platform from leading security vendors to help streamline incident management and response.

Phase 5: Secure Remote Access

Verizon facilitates modern, zero-trust remote access for suppliers and employees with specific access controls, including agent-based and browser-based solutions. Our SASE (Secure Access Service Edge) Management solution combines network access with cloud-delivered security services, offering a unified model that supports zero-trust network access. This service includes change management, incident management, and health monitoring.

Phase 6: Behavior-Based Traffic Analysis

To enhance visibility, Verizon uses AI-powered security controls like Data Loss Prevention (DLP), Intrusion Prevention Systems (IPS), and User and Entity Behavior Analytics (UEBA). This phase can include monitoring, threat intelligence, and incident response.

Verizon's Managed XDR Extended Detection and Response with Accenture provides a cost-effective, tailored solution for offloading security operations with near real-time visibility and automated response. Additionally, our Verizon Security Operations Service offers a standardized monitoring solution to help identify and respond to threats.

Why Choose Verizon?

With a deep understanding of the evolving cyber threat landscape, Verizon leverages insights from our global network and security operations centers, as well as over a decade of producing the Data Breach Investigations Report. Verizon has extensive experience delivering OT-specific solutions for:

- Asset discovery
- Network segmentation
- Vulnerability management
- Detection and response

Based upon our global presence and many years of security experience, Verizon is well equipped to help design, operate, manage, and automate your OT security environment.

Learn more

To discover how Verizon can help protect your business, please contact your Verizon Business Account Manager or email us: otsecurity@verizon.com

verizon business