Unleash Your Security Fabric with FortiAnalyzer for Operational Technology

Modern industries depend heavily on operational technology (OT) and industrial control systems (ICS) to monitor and control physical processes. Unfortunately, previously isolated systems have become prime targets for sophisticated cyberthreats. OT organizations need a practical solution that can prevent, disrupt, and respond to potential threats while ensuring the continuity of their operations.

FortiAnalyzer for OT

The Fortinet OT-Aware Security Platform brings together integrated products and services tailored for OT environments. Part of the OT-Aware Security Platform, FortiAnalyzer for OT provides comprehensive network traffic analysis, log management, and automated threat responses. Through advanced threat detection, real-time insights, and seamless integration with the Fortinet Security Fabric, FortiAnalyzer ensures robust security for converged IT/OT environments.

Operational efficiency

FortiAnalyzer helps organizations streamline security operations by providing centralized logging and reporting. It eliminates the need for manual log collection and analysis, reducing the workload for security teams. FortiAnalyzer can also be integrated with other Fortinet products, such as FortiGate Next-Generation Firewalls and FortiSIEM security information and event management.

Network visibility and performance

FortiAnalyzer provides visibility into network traffic and connected devices. With the ability to monitor network performance and identify potential issues, organizations can better optimize network configurations and ensure that OT devices operate efficiently.

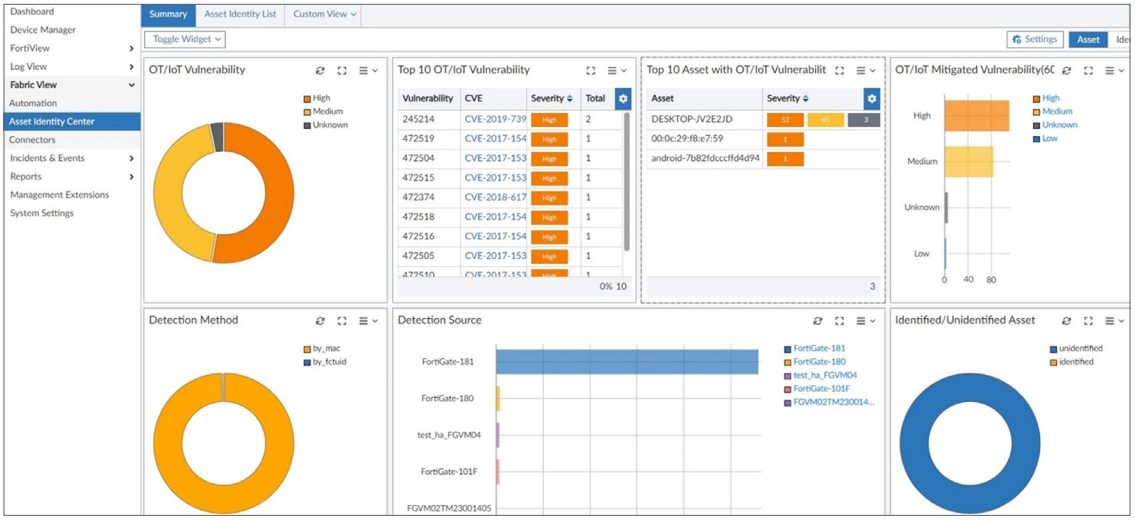

Figure 1: The FortiAnalyzer Asset and Identity Center consolidates IT/OT in a single view.

Threat detection and response

FortiAnalyzer collects logs and network traffic data from OT devices and analyzes them for potential security threats. It uses machine learning and threat intelligence to detect known and unknown threats and can identify patterns and relationships to help security teams detect and respond to complex, multi-stage attacks.

Compliance reporting

Many OT systems are subject to regulatory compliance requirements, such as North American Electric Reliability Corporation Critical Infrastructure Protection and International Electrotechnical Commission 62443 standards. FortiAnalyzer generates risk and compliance reports to help teams identify and address potential vulnerabilities and non-compliant configurations. These reports provide insights into the security posture of the OT environment, as well as recommendations for improving overall security and compliance.

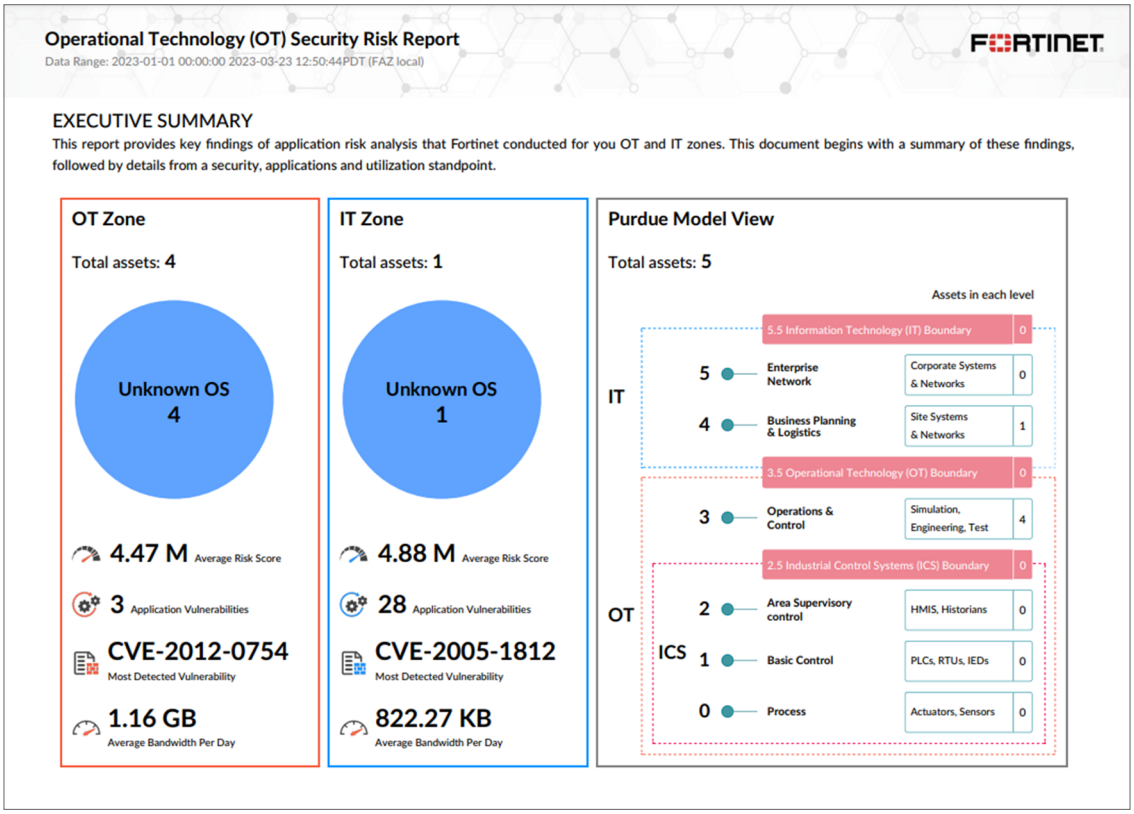

Figure 2: The FortiAnalyzer OT Security Risk Report detects risky applications for IT and OT zones, blind-spots, and maps assets to the Purdue model.

FortiAnalyzer for OT

FortiAnalyzer for OT goes beyond traditional cybersecurity measures with features that address the unique challenges posed by OT environments.

- **Unified IT/OT view:** A single, integrated dashboard shows where IT and OT data converge. This holistic view provides a comprehensive perspective that facilitates better threat recognition and incident response across the entire digital infrastructure.
- **OT networks mapped to the Purdue model:** A detailed OT perspective is structured using the universally recognized Purdue model. It shows the hierarchical layering from process control to enterprise zones, which helps improve situational awareness and makes it easier to pinpoint vulnerabilities.
- **MITRE ATT&CK framework for ICS:** The integrated MITRE ATT&CK framework is tailored explicitly for ICS and helps ensure real-time defense against known threat tactics and techniques.
- **Customized OT reports:** OT-centric reports provide analytics and in-depth insights into system operations, vulnerabilities, and compliance. These reports are designed to meet the demands of industrial environments.

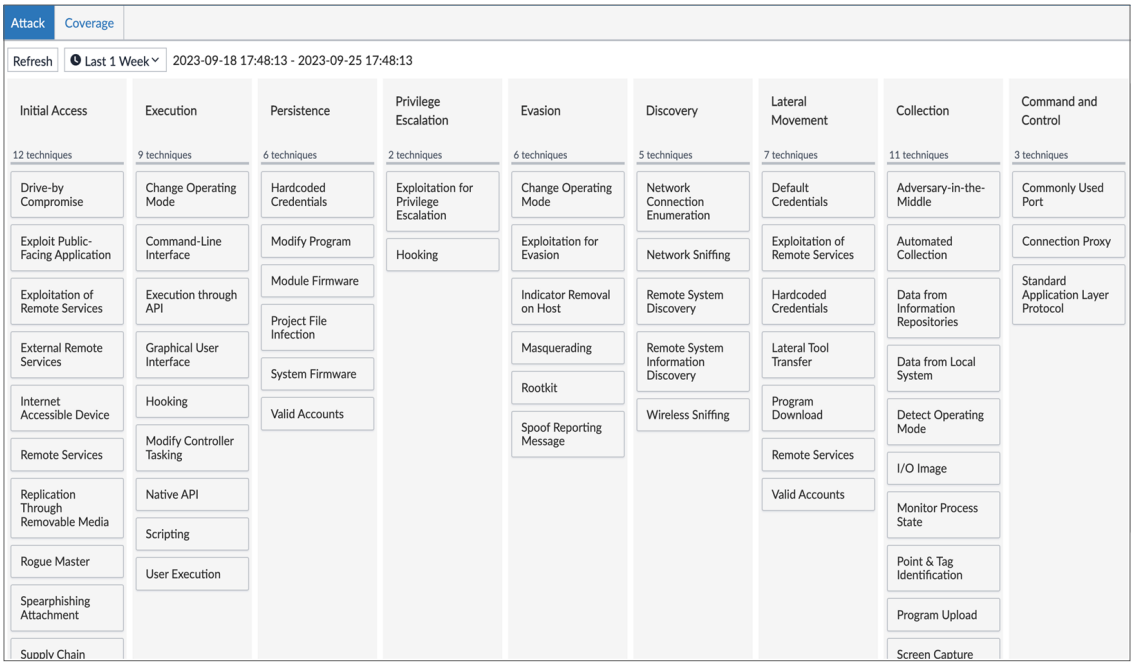

Figure 3: FortiAnalyzer speeds decision-making with MITRE ATT&CK frameworks for Enterprise and Industrial Control Systems (ICS).

A Consolidated IT/OT Solution for Today's Dynamic Threat Landscape

FortiAnalyzer for OT weaves cybersecurity into the fabric of operational technology. With a single dashboard, it offers a unified, real-time view of data across the Fortinet Security Fabric and other integrated systems, simplifying network management tasks and providing insights that can help speed identification, isolation, and remediation of threats across converged IT/OT networks.

Learn more about how FortiAnalyzer for OT helps elevate OT cybersecurity.

October 21, 2023 7:41 PM
2397373-0-0-EN