SOLUTION BRIEF

FortiSOAR: Optimize OT Security Operations

Executive Summary

The convergence of operational technology (OT) and information technology (IT) infrastructures continues to accelerate. And as publicized attacks and industry warnings increase, organizations must now prioritize securing their OT assets and infrastructure. But this process cannot happen in isolation. Years of IT security operations center (SOC) experience have clearly shown the critical need to centralize, standardize, and automate security operations (SecOps) top to bottom. Security orchestration, automation, and response (SOAR) software is designed to fulfill this need, enabling SOC teams to efficiently process all security alerts, investigate threats, and rapidly respond to attacks.

OT security presents similar operational challenges and requires a similar approach to fully protect the organization. FortiSOAR has extended its industry-leading IT SecOps features to fully encompass unique OT needs with features such as risk-based asset and vulnerability management, MITRE ATT&CK ICS views, OT threat remediation playbooks, and full OT ecosystem integration.

Whether you're extending your SOC to protect OT or growing the cybersecurity capabilities of your OT control center, FortiSOAR is key to your OT security posture, threat responsiveness, and SecOps efficiency.

600+
integrations

800+
playbooks

400+
enterprise and MSSP customers

Fortinet named a leader in the KuppingerCole Leadership Compass for SOAR, 2023 & 2024

OT Security and Automation

As digital innovation advances, OT assets have become more open and dependent on network communications and increasingly connected to the larger corporate network. As a result, they are now potentially vulnerable to outside attacks ranging from sabotage to ransomware. Specialized cybersecurity products provide protection and detection across OT operational levels and at the OT/IT network boundary, but monitoring, investigating, and responding to alerts from this array of products is complex and prone to error.

OT security centers that suffer from alert overload and analyst burnout, delayed threat recognition, or inadequate response open the entire enterprise to unacceptable risk. FortiSOAR is the answer to the need for OT security operations.

OT Automation at Work

Standardize proactive security measures by automating risk-based OT monitoring, threat intelligence gathering, vulnerability management, and asset management procedures.

Respond immediately to OT alerts by automating alert triage and investigation and triggering real-time and permission-based mitigation procedures, such as firewall updates, asset isolation, and ticket generation.

Protect OT assets from outside attack by ensuring OT security solutions and procedures are immediately updated when an intrusion is detected elsewhere in the corporate network.

Figure 1: Track OT asset status using the Purdue model.

Solution Overview

FortiSOAR enables organizations to centralize, standardize, and automate SecOps, IT, OT, and any critical enterprise operation. With broad integrations, rich use-case functions, prebuilt workflows, and simple playbook creation, FortiSOAR can help companies dramatically improve their cybersecurity posture, threat responsiveness, and the efficiency of any operation.

Key Features

Automation
500+ integrations and 800+ playbooks along with robust features and use-case solutions support SOC, NOC, and IT/OT automation.

GenAI assistance and automation
FortiAI uses natural language and GenAI to guide, simplify, and automate FortiSOAR analyst activities, such as threat investigation, response, and playbook building.

Built-in threat intelligence
Enrich investigations and power actions with built-in FortiGuard Labs global intelligence and your preferred public sources.

Content hub and community
Ever-growing connectors, playbooks, solution packs, best-practice videos, and community contributions help drive continued benefits.

No/low-code playbook creation
Patented playbook design experience provides visual drag-drop and rapid development modes to create custom playbooks with ease.

Flexible deployment options
FortiSOAR can be deployed on-premises, as a Software-as-a-Service (SaaS) solution, as cloud software, or managed by a managed security service provider (MSSP), all with the same robust functionality.

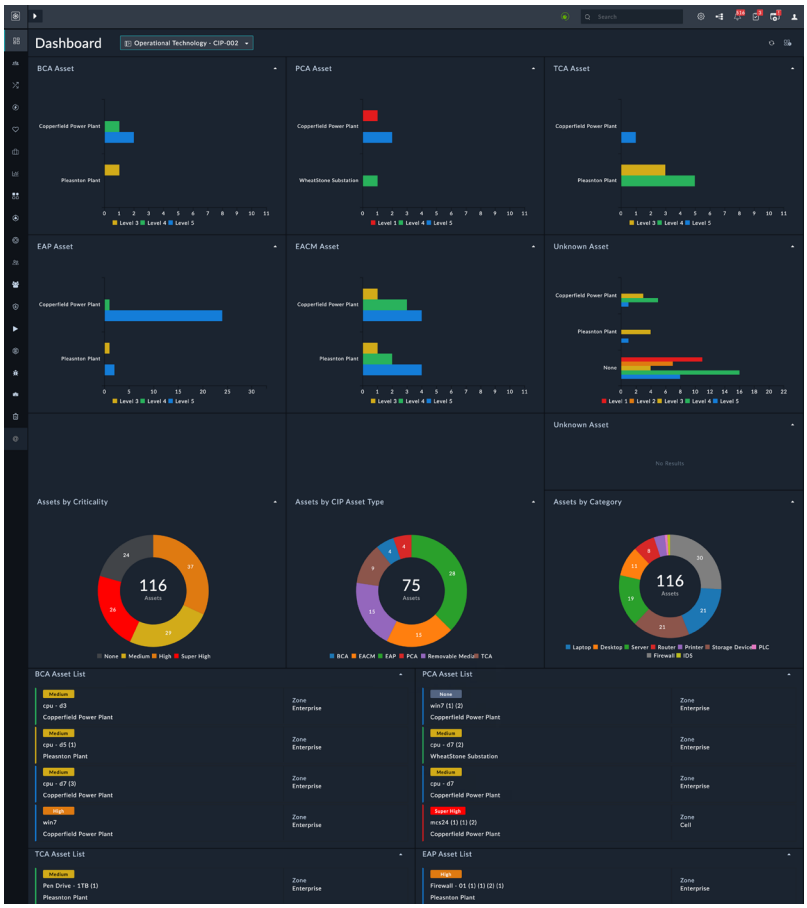
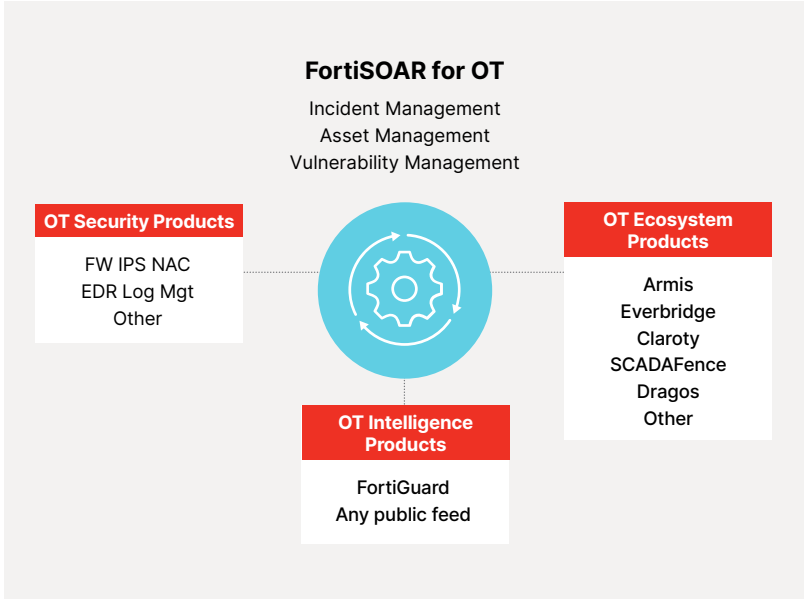


Figure 2: Track OT asset alerts by type and severity.

FortiSOAR for OT

Beyond the standard capabilities suitable for any type of operation, FortiSOAR provides additional rich features, content, and integrations tailored to meet OT needs. Whether you are focused solely on automating OT cybersecurity or a modern converged IT/OT SOC, FortiSOAR delivers the OT security automation capabilities you need in a single solution. FortiSOAR OT features include:

- Connection to OT protection products
- Integration with OT ecosystem solutions
- OT threat intelligence management
- OT incident management and playbooks
- OT asset management solution pack
- OT vulnerability management solution pack



OT Automation Use Cases

Central OT security visibility
Take full charge of your security posture

Manage OT security using rich dashboards featuring OT asset distribution, risk, and vulnerability status based on the Purdue model. Track open incidents, analyst activities, and threat response SLAs. Easily create custom dashboards.

OT incident investigation and response
React immediately to maintain continuity

Automatically triage, enrich, and assess alerts from OT cybersecurity products and applications. Group alerts to incidents, map to MITRE ATT&CK ICS framework, and execute prebuilt mitigation playbooks or initiate a war room investigation.

Vulnerability management
Continually protect against new OT CVEs

Evaluate, categorize, and prioritize OT vulnerability scanner results using the Cybersecurity and Infrastructure Security Agency risk-based framework. Assign tasks and execute end-to-end playbooks to patch or mitigate critical vulnerabilities.

Asset management
Keep up with the dynamic asset life cycle

View and report on OT asset inventory along with detailed identification, criticality, vulnerability status, and alert status. Assign, manage, and automate asset change activities and standard procedures. and community contributions help drive continued benefits.

Compliance automation and reporting
Automate advisory updates and compliance activities

FortiSOAR automates advisory updates and overall compliance activities with automation playbooks, specialized tracking, dashboards, and IT/OT compliance management reporting for regulations, including GDPR, HIPAA, US BOD 22-01, US NERC CIP, and more. FortiSOAR asset management, vulnerability management, SLA tracking, and other features support mandatory alerts and actions necessary for compliance adherence.

Threat intelligence management
Leverage the latest intel at every step of the way

Use FortiGuard Labs and any standards-based OT intelligence source to automatically enrich alerts and power investigations. Curate and manage feeds to stay current with cybersecurity researchers and attacker trends.

Custom playbook creation
Optimize any workflow with automation

Build custom playbooks leveraging the rich content hub library and patented playbook design experience. Utilize the unique low/no-code process to rapidly develop playbooks of any complexity without technical coding skills.

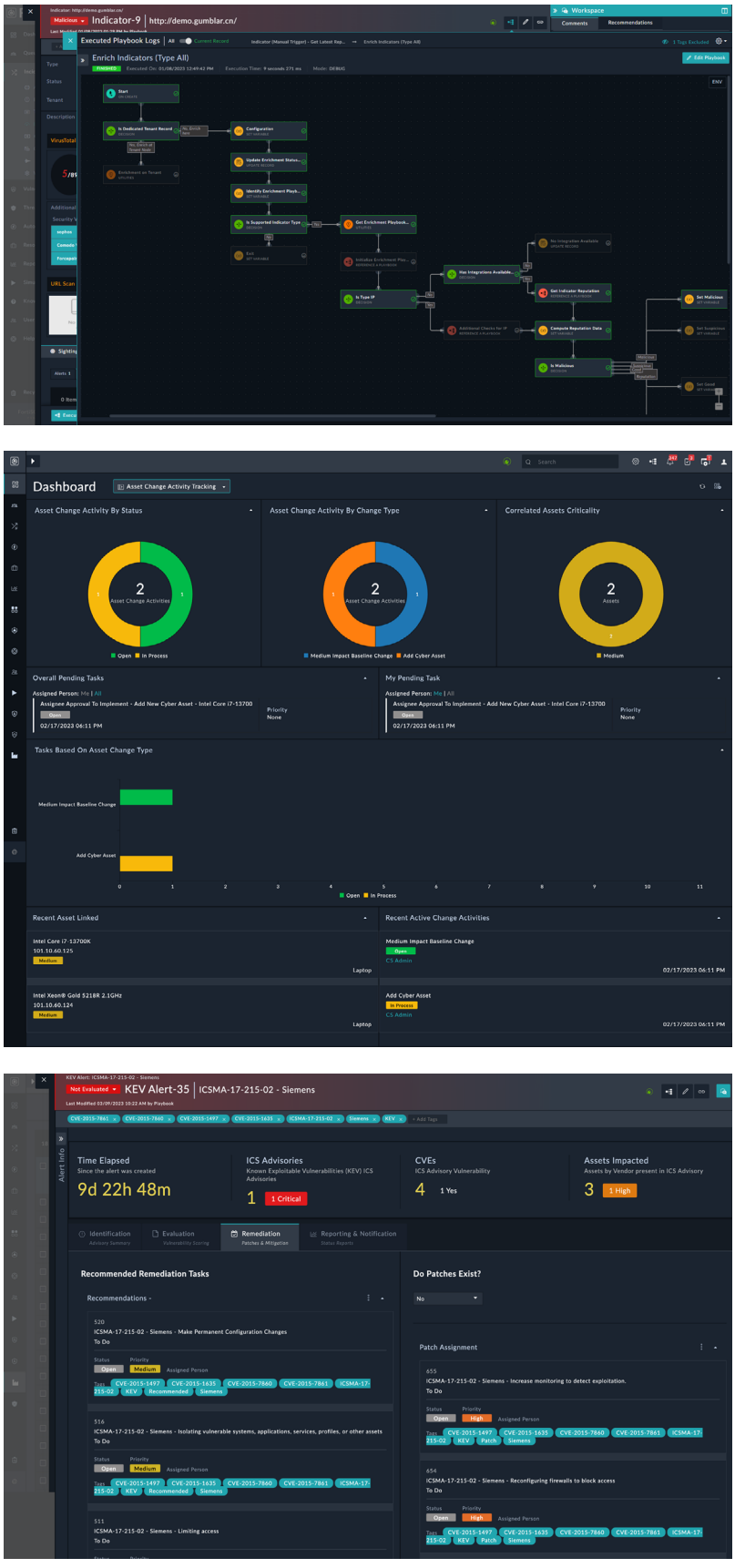


Figure 3: FortiSOAR offers visualizations for playbook creation, asset tracking, and alert investigation.

The FortiSOAR Content Hub and Community

The FortiSOAR Content Hub provides a large and growing library of ready-made product content and useful knowledge via an intuitive web-based and in-product portal. You can easily add valuable new use cases to your solution by leveraging its hundreds of connectors, playbooks, dashboard widgets, and complete solution packs built by the Fortinet team or contributed by the user community. Demo and how-to videos deliver tutorials and best practices to get the most from your automation initiatives.

The FortiSOAR Community Portal keeps you in touch with your peers and the latest FortiSOAR news. A moderated discussion board and idea exchange give you immediate access to peer group Q&A, helpful insights and practices, as well as a direct link to Fortinet expert staff.

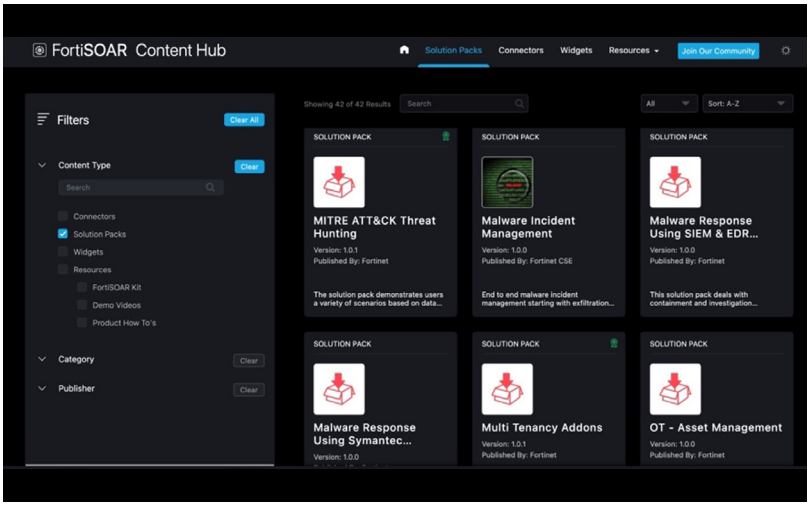


Figure 4: The FortiSOAR Content Hub offers easy management.

Fortinet Solutions for OT Security

FortiSOAR is part of the Fortinet portfolio of enterprise security products that ensure the end-to-end protection of converged IT/ OT operations. FortiSOAR is available as a SaaS solution, on-premises or cloud-ready software, and as an MSSP service.

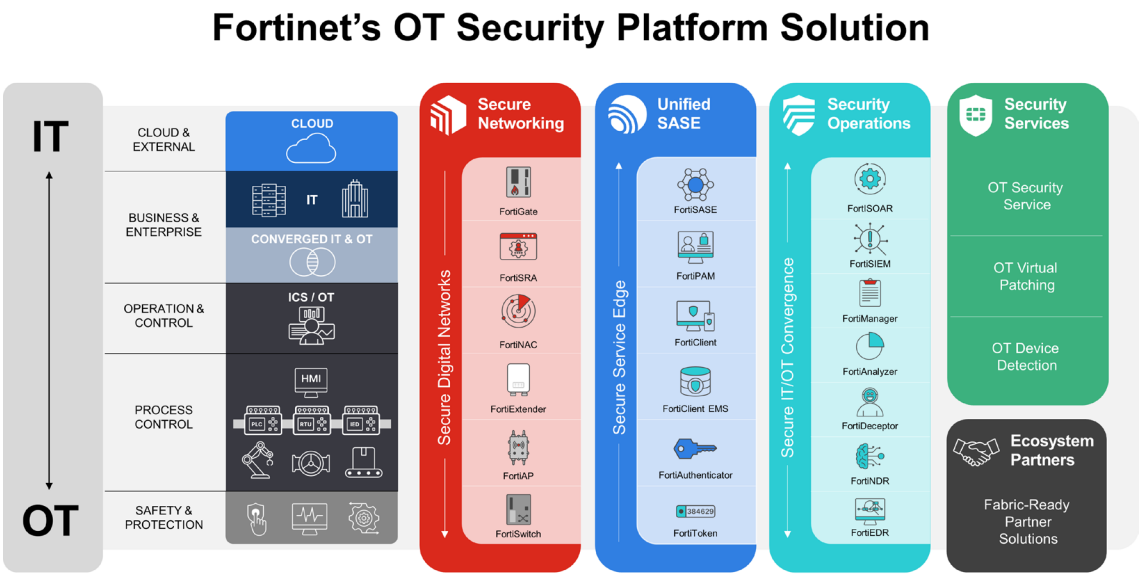


Figure 5: Fortinet offers multiple solutions for OT security.

[1] 2024 State of Operational Technology and Cybersecurity Report, Fortinet, June 12, 2024.

[2] Ibid.

FORTINET

www.fortinet.com

September 29, 2024 12:58 PM / 2039566-A-0-EN