SOLUTION BRIEF

Optimize Security Operations with FortiSOAR

Automate Threat Investigation and Response

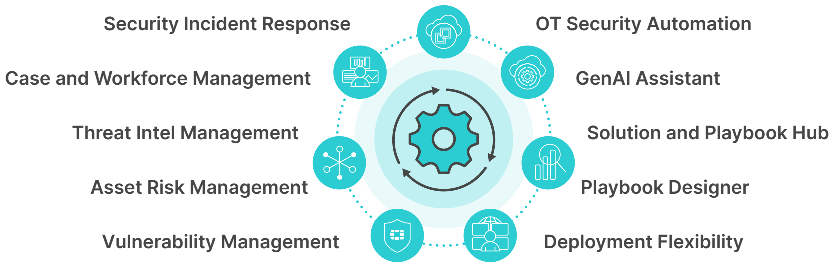
Executive Summary

Security operations center (SOC) teams everywhere are overloaded with investigating alerts and responding to threats, stitching together data from dozens of tools to investigate and remediate incidents. Most teams struggle to keep pace, slowing their ability to discover serious attacks. Network operations center (NOC) and operational technology (OT) teams face monitoring and maintenance challenges, furthering security risks. Leading organizations and managed security service providers (MSSPs) use FortiSOAR security orchestration, automation, and response to unify and optimize these critical workflows, ensuring better security while driving efficient IT/OT operations.

FortiSOAR enables organizations to centralize, standardize, and automate IT/OT security operations and critical enterprise functions. With broad integrations, rich use-case functions, hundreds of prebuilt workflows, and simple playbook creation, FortiSOAR supports best-in-class procedures tailored to your specific needs. FortiSOAR is the security operations hub that connects tools and automates processes to help protect your organization from attack.

FortiSOAR

Centralize, standardize, and automate IT/OT security operations



Security Incident Response

OT Security Automation

Case and Workforce Management

GenAI Assistant

Threat Intel Management

Solution and Playbook Hub

Asset Risk Management

Playbook Designer

Vulnerability Management

Deployment Flexibility

The Automation Imperative

Security teams are overloaded with too many tools to manage, too many alerts to investigate, and too many manual or repetitive processes—all of which slow down response times. Despite analyst efforts and SOC budget spending, typical incident detection and response performance remains inadequate to protect organizations against today's attackers.

Automation via FortiSOAR can dramatically change this dynamic by augmenting staff efficiency and enabling analysts to refocus on high-value activities. But automating repetitive or mundane tasks is only a fraction of the potential value organizations gain from FortiSOAR. Centralizing and standardizing complete

FortiSOAR

600+
integrations

800+
prebuilt playbooks

400+
enterprise/MSSP customers

Fortinet named a leader in the KuppingerCole Leadership Compass for SOAR, 2023 & 2024 investigation and response workflows that leverage AI, the latest available threat intelligence, and a rich analyst toolset can make the difference between attack deterrence and breach recovery.

FortiSOAR includes robust IT/OT functions for managing threat intelligence, threat hunting, risk-based assets, vulnerabilities, and more—all integrated into a single security operations hub. NOC and OT integrations, playbooks, the ability to automate anything, and the ease of customization make FortiSOAR an ideal operations hub.

The FortiSOAR platform is truly enterprise-grade with proven reliability, scalability, flexible deployment options, and high-availability configuration support. Rich reporting and compliance capabilities track your security posture, forensic-level activities, and complete operations service-level agreements (SLAs). Whether you are looking for turnkey Software-as-a-Service (SaaS) automation, a mission-critical operations platform, or an MSSP value-added service, FortiSOAR is the right choice.

FortiSOAR Key Features

FortiSOAR delivers essential security orchestration, automation, and response features in a single platform.

- **Security incident response**: FortiSOAR offers centralized and automated alert triage, enrichment, investigation, collaboration, and incident response actions. The solution includes hundreds of integrations and playbooks, robust features, and use-case solutions to support SOC, NOC, and OT efficiency.
- **Case and workforce management**: Teams get a complete solution for managing and tracking task assignments, work queues, and shift calendaring.
- **Asset and vulnerability management**: FortiSOAR combines risk-based asset views, vulnerability status, task management, and mitigation playbooks.
- **Compliance automation and reporting**: FortiSOAR offers task automation, tracking, and reporting for IT/OT compliance management.
- **OT security management**: Extended integrations and functions meet OT-specific monitoring and playbook automation requirements.
- **Generative AI assistance and recommendations**: The FortiAI and Recommendation Engine combine to inform and speed analyst investigation, response, and more.
- **Built-in threat intelligence**: Enriched investigations and threat hunting are powered by built-in global intelligence from FortiGuard Labs as well as additional public sources.
- **FortiSOAR Content Hub and Community**: An expanding library of connectors, playbooks, solutions, videos, and community contributions offer continued benefits.
- **No- and low-code playbook creation**: Patented design experience provides visual drag-and-drop and rapid development modes to easily create custom playbooks without technical coding skills.
- Flexible deployment options: Choose from SaaS, on-premises, public cloud hosting, or trusted MSSP partners, all with the same robust functionality.

“FortiSOAR has advanced our threat detection and response capabilities by five years. It gives us this tremendous Swiss Army knife of functionality that we are excited to capitalize on.”

CEO, Secure Cyber Defense

“FortiSOAR is the champion product when it comes to automation and having the ability to maximize existing tools.”

Alejandro Leal
KuppingerCole Leadership Compass for SOAR, January 30, 2023

FortiSOAR Use Case Spotlight

Critical use cases for FortiSOAR include:

SOC threat investigation and response

FortiSOAR is designed to be the central hub for threat management, automatically assessing, triaging, and enriching alerts from virtually any security product. Routine alerts are automatically handled and closed. Priority alerts are mapped to the MITRE ATT&CK framework and intelligently grouped into incidents for deeper investigation. Recommended playbooks augment rich investigation features, suggest actions, and execute complete remediation steps. Escalated incidents can activate a full war room that facilitates collaboration and includes detailed forensic logging. Analysts can take action anywhere and anytime via the FortiSOAR secure mobile application.

Asset and vulnerability management

FortiSOAR integrates with asset management and vulnerability scanning systems to give you a complete risk-based picture of your IT/OT assets, including identification, criticality, vulnerability status, and alert conditions. Analysts and managers can use this information to launch automated remediation or other playbooks and assign and track tasks. Alert and incident investigation is enriched and accelerated by having complete asset profiles at hand without the need to access other systems or tools.

OT security operations

Increasing convergence with IT exposes OT assets to risks that demand comprehensive security protection. FortiSOAR enables you to fully monitor and manage OT SecOps, with features such as risk-based OT asset and vulnerability management, MITRE ATT&CK industrial control system (ICS) views for threat investigation, OT threat remediation playbooks, and full OT ecosystem integration.

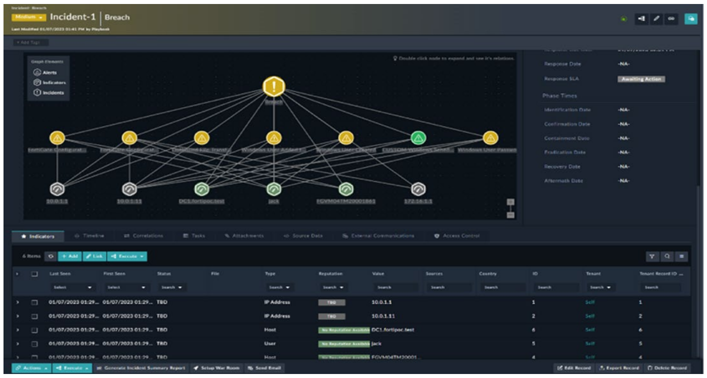
The design approach of FortiSOAR for OT is based on best practices aligned with Cybersecurity and Infrastructure Security Agency (CISA) operational directives.

Compliance automation and reporting

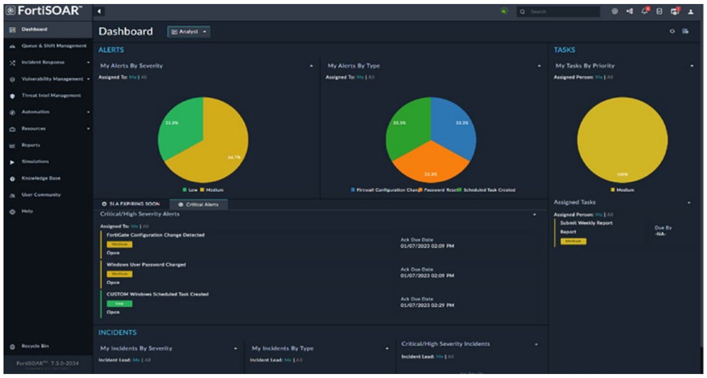
FortiSOAR automates advisory updates and overall compliance activities. It also provides specialized tracking, dashboards, and IT/OT compliance management reporting for regulations, including GDPR, HIPAA, US BOD 22-01, US NERC CIP, and more. FortiSOAR asset management, vulnerability management, SLA tracking,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

Playbook creation

The patented playbook design experience provides a visual drag-and-drop graphical user interface (GUI) and a low-code rapid development mode that allows users of all types to easily create custom playbooks. The FortiSOAR Content Hub contains hundreds of prebuilt playbooks and automated actions to use as building blocks, while the FortiSOAR Recommendation Engine provides inline step guidance. Even the most complicated playbook flows do not require technical coding skills. The designer function includes full versioning control as well as a simulation engine for testing.



	Last Seen	First Seen	Status	Type	Reputation	Value	ID	Tenant	Tenant Record ID
	01/07/2023 01:29...	01/07/2023 01:29...	TBD	IP Address	TBD	10.0.1.1	1	Self	1
	01/07/2023 01:29...	01/07/2023 01:29...	TBD	IP Address	TBD	10.0.1.11	2	Self	2
	01/07/2023 01:29...	01/07/2023 01:29...	TBD	Host	No Reputation Available	DC1.fortipoc.test	6	Self	6
	01/07/2023 01:29...	01/07/2023 01:29...	TBD	User	No Reputation Available	jack	5	Self	5
	01/07/2023 01:29...	01/07/2023 01:29...	TBD	Host	No Reputation Available	FGVM04TM20001...	4	Self	4

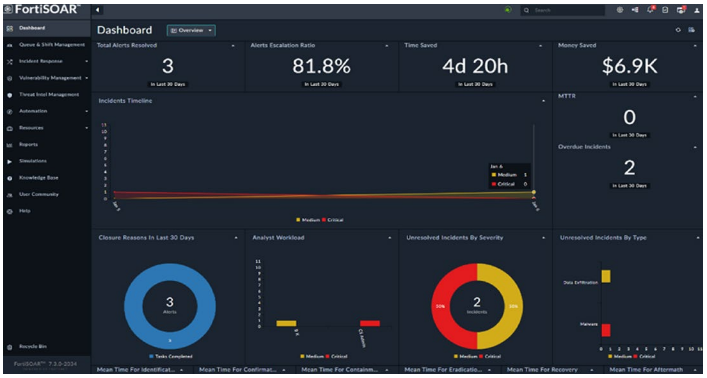


FortiGate Configuration Change Detected — Medium — Open — Ack Due Date 01/07/2023 02:09 PM

Windows User Password Changed — Medium — Open — Ack Due Date 01/07/2023 02:09 PM

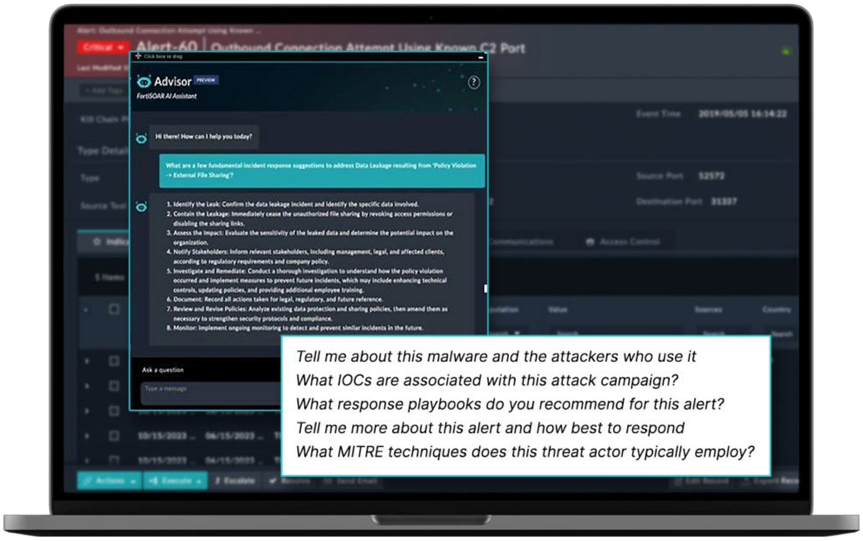
CUSTOM Windows Scheduled Task Created — Low — Open — Ack Due Date 01/07/2023 02:29 PM

Submit Weekly Report — Medium — Due By -NA-



MSSP operations

FortiSOAR is designed to uniquely enable the flexible and sophisticated deployment models demanded by MSSP operations. Shared and dedicated tenant models supported by on-premises agents allow hierarchical, global, and regional SOC deployments and enable bespoke customer requirements. FortiSOAR also offers global and per-tenant playbooks and a full range of tenant-specific functions, such as SLA tracking, alerts, incident views, reports, and dashboards. In addition, the FortiSOAR concurrent user licensing model helps MSSPs control costs and offer attractive customer pricing.



Hi there! How can I help you today?

What are a few fundamental incident response suggestions to address Data Leakage resulting from 'Policy Violation -> External File Sharing'?

1. Identify the Leak: Confirm the data leakage incident and identify the specific data involved.
2. Contain the Leakage: Immediately cease the unauthorized file sharing by revoking access permissions or disabling the sharing links.
3. Assess the Impact: Evaluate the sensitivity of the leaked data and determine the potential impact on the organization.
4. Notify Stakeholders: Inform relevant stakeholders, including management, legal, and affected clients, according to regulatory requirements and company policy.
5. Investigate and Remediate: Conduct a thorough investigation to understand how the policy violation occurred and implement measures to prevent future incidents, which may include enhancing technical controls, updating policies, and providing additional employee training.
6. Document: Record all actions taken for legal, regulatory, and future reference.
7. Review and Revise Policies: Analyze existing data protection and sharing policies, then amend them as necessary to strengthen security protocols and compliance.
8. Monitor: Implement ongoing monitoring to detect and prevent similar incidents in the future.

Tell me about this malware and the attackers who use it
What IOCs are associated with this attack campaign?
What response playbooks do you recommend for this alert?
Tell me more about this alert and how best to respond
What MITRE techniques does this threat actor typically employ?

GenAI-Driven Assistance, Recommendations, and Automation

FortiAI uses natural language and augmented GenAI to guide, simplify, and automate FortiSOAR analyst activities, such as threat investigation, response, and playbook building. The recommendation engine uses ML to power automation and decision-making for threat investigation and response workflows, task assignments, playbook recommendations, and playbook-building guidance.

Content Hub and Community

The FortiSOAR Content Hub provides an extensive and growing library of ready-made product content and valuable knowledge via an intuitive, web-based, and in-product portal. You can easily add critical new use cases to your solution by leveraging the 600+ connectors, 800+ 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 help you 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 provide immediate access to peer group Q&As, helpful insights, best practices, and a direct link to contact Fortinet experts.

www.fortinet.com

September 30, 2024 4:18 PM
2048834-B-0-EN