SOLUTION BRIEF

Automating Regulatory Compliance with FortiSOAR

In today's rapidly evolving cybersecurity landscape, staying compliant with government and industry regulations and urgent advisory updates is vital, although time-consuming, for security and IT teams. Multiple agencies and regulations increasingly demand timely vulnerability management, threat intelligence processing, indicators of compromise (IOC) advisory actions, SLA adherence, and complete reporting.

The dilemma facing security teams is that these time-intensive activities are typically assigned to the same personnel tasked with investigating and responding to attacks in real time. Fortunately, FortiSOAR can centralize and automate compliance activities and end-to-end processing, ensuring timely compliance while allowing analysts to focus on attack investigation and response.

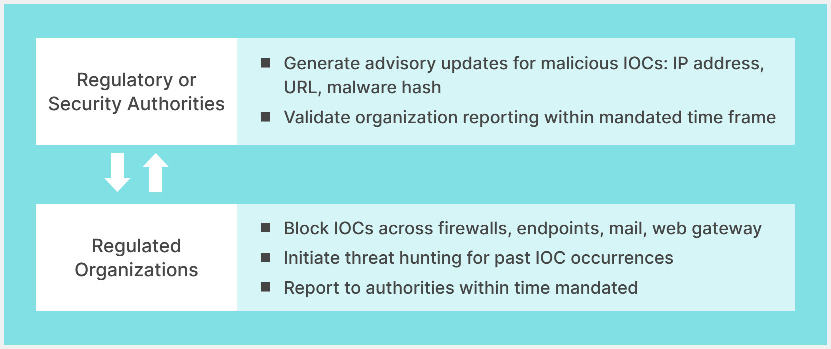
From hours to minutes, again and again

FortiSOAR automates frequent compliance activities, such as:

- Vulnerability management
- IOC advisory updates
- Threat intel processing
- Threat hunting
- Tracking and reporting

Automating Security Advisory Updates

Government and regulatory agencies increasingly issue time-sensitive security advisory bulletins specifying IOCs that must be identified and blocked at enforcement points across the security infrastructure. Manually processing, tracking, and reporting on these frequent bulletins is error-prone and costly for already overburdened teams. FortiSOAR can automate the entire process, providing timely protection and keeping you compliant while saving dozens of hours per week of SOC and IT team time.



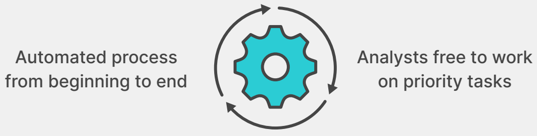
Regulatory or Security Authorities
- Generate advisory updates for malicious IOCs: IP address, URL, malware hash
- Validate organization reporting within mandated time frame

Regulated Organizations
- Block IOCs across firewalls, endpoints, mail, web gateway
- Initiate threat hunting for past IOC occurrences
- Report to authorities within time mandated

Before Automation
Hours to days of manual processing

- Parse email/communication to extract IOC list
- Determine new additions to make
- Manually add to each security product blocklist
- Initiate threat hunting for IOCs across products
- Validate completion, correct errors
- Manually generate report, send to authorities

With FortiSOAR
Immediate execution of entire process


Automated process from beginning to end
Analysts free to work on priority tasks

Savings of dozens of hours per week

Figure 1: Processing advisory updates can consume dozens of hours of precious analyst time per week.

Automating IT/OT Compliance Activities

Security compliance is multifaceted and requires continuous effort. Beyond automating advisory update compliance, FortiSOAR can centralize and automate many other compliance requirements and best practices with minimal analyst effort.

Vulnerability management

FortiSOAR integrates with threat intelligence sources and vulnerability scanning systems to provide a central point for processing KEV and CVE information, identifying vulnerable systems, and assigning, automating, and tracking vulnerability management activities. It also lets you view vulnerability status by asset and asset risk.

Compliance validation and reporting

FortiSOAR provides specialized tracking, dashboards, and IT/OT compliance management reporting for a variety of regulations, including GDPR, HIPAA, US BOD 22-01, US NERC CIP, and more. FortiSOAR asset management, vulnerability management, SLA tracking, and other features are extended to support mandatory alerts and actions necessary for compliance adherence.

Threat intelligence management

FortiSOAR automatically ingests, aggregates, normalizes, and curates a wide range of IT/OT threat feeds, including Fortinet FortiGuard Labs threat intel data. Intel automatically enriches alerts and can launch actions such as threat hunting. As a complete threat intelligence platform, FortiSOAR supports IOC exporting via STIX, TAXII, and CSV, a dedicated threat intel management workspace to facilitate research, collaboration, and sharing.

FortiSOAR Benefits

FortiSOAR centralizes, standardizes, and automates IT/OT security and NOC operations. With broad integrations across Fortinet and multivendor environments, rich use-case solutions, hundreds of prebuilt playbooks, and full SecOps management features, FortiSOAR is the SOC automation foundation for leading enterprise and MSSP organizations worldwide.

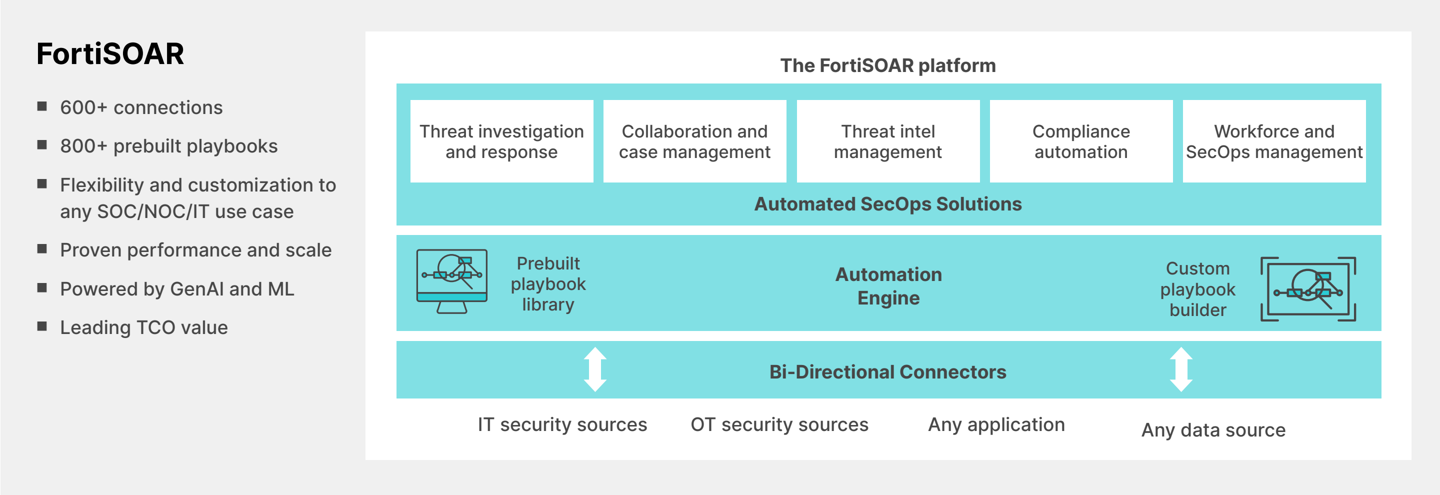


Figure 2: FortiSOAR centralizes, standardizes, and automates any process.

Learn more about FortiSOAR, or contact your local Fortinet account manager or channel partner.