

SOLUTION BRIEF

# Amplify Security Operations Efforts and Accelerate Response With FortiSOAR

## Executive Summary

The evolving threat landscape and organizational complexities are creating obstacles for security operations center (SOC) teams and potentially leaving organizations exposed to attack. Many organizations have added point solutions, but the increased security complexity contributes to a number of problems. Security teams are faced with too many vendors to manage, too many alerts to investigate, manual processes that slow response times, and a lack of trained staff to manage the expanding workloads.

The addition of security orchestration, automation, and response (SOAR) capabilities to the security architecture can help alleviate these pressures. Using FortiSOAR, security operations teams can improve collaboration, control, and SOC automation through out-of-the-box connectors or customizable frameworks that pull together all of the organization's security tools while reducing alert fatigue. FortiSOAR centralizes tools and amplifies the efforts of SOC teams, empowering them to rapidly respond, automate tasks, and execute actions across the organization's security stack.

## Disjointed Security Increases Risk

Security analysts are currently overwhelmed by the number of security alerts they face each day. In a recent survey, 42% of responders reported suffering from cybersecurity fatigue, and 93% of those individuals are experiencing 5,000 or more alerts per day.<sup>3</sup> Attacks are more sophisticated and analysts face increasingly complex and fragmented security infrastructures with too many point products from different vendors.

Although the sheer volume of alerts is a big part of the problem, tracking, investigating, and trying to remediate alerts from many different sources requires a great deal of manual effort as well. And while alerts, vulnerabilities, and cyber threats demand attention, other aspects of improving an organization's security posture are important too.

At the same time, when it comes to security operations, organizations are struggling with a worldwide cybersecurity skills shortage. As of 2021, almost 3.5 million cybersecurity jobs remain unfilled and it's unlikely companies will successfully secure the additional talent needed to fully staff their security operations initiatives.<sup>4</sup> In fact, nearly two-thirds (65%) of companies currently lack the skilled staff they need to maintain effective security operations.<sup>5</sup> The combination of the skills shortage, security fragmentation, and overwhelmed analysts increases the chances of a breach going undetected.

A SOAR solution helps security teams integrate their security tools. It allows separate components to communicate and work together in a defensive coordination. With SOAR, security operations teams can automate the tedious and repetitive elements of workflows while maintaining human authority. The best SOAR solutions enrich and contextualize threats to help analysts quickly triage cases according to the severity of the risk, sensitivity, or the critical nature of the threatened business functions.

Breaches with a life cycle less than 200 days were, on average, \$1.22 million less costly than breaches with a life cycle of more than 200 days (\$3.34 million vs. \$4.56 million, respectively).<sup>1</sup>

The SOAR market is in such a demand for SOC teams, it is projected to grow to reach nearly \$1.8 billion at a CAGR of 15.6% from 2019 to 2024.<sup>2</sup>



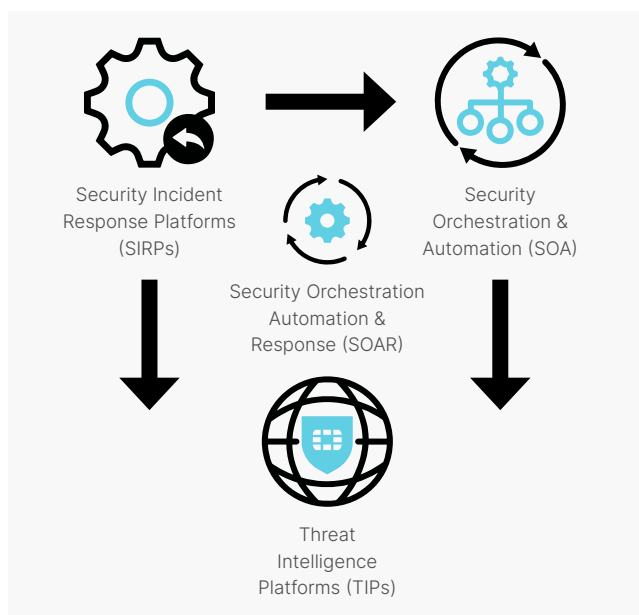


Figure 1: SOAR is the convergence of three key technologies that are necessary for timely threat identification and mitigation.

### FortiSOAR Integrates Security and Automates Responses

FortiSOAR aggregates and enriches alerts from a wide range of security products. It simplifies orchestration and management by leveraging well-defined playbooks, which helps eliminate time-consuming manual workflows. Consistently executing processes reduces the chance of operator error. In fact, FortiSOAR Customer Secure Cyber Defense reported that the response times to perceived threats dropped from 45 minutes to 2 minutes in some cases, which demonstrates how FortiSOAR can help analysts optimize their time. Instead of performing monotonous tasks, analysts can focus on finding threats before they occur.

Figure 2 shows how FortiSOAR can help SOC teams reduce incident response time by replacing a series of manual, inefficient, and error-prone steps. Steps that cumulatively could take as long as 15 hours, FortiSOAR automated processes completed in an average of 20 minutes.

#### Incident Response Time: Manual vs. FortiSOAR

Steps	Manual	FortiSOAR
Enrich artifacts to identify indicator of compromise (IOC)	46 to 60 minutes	3 minutes
Perform triaging on events from SIEM	20 minutes	1 minute
Submit a zip file to the detonation engine	1 to 6 hours	1 minute
Isolate affected devices	10 minutes	1 minute
Analyze, create, and annotate an incident	60 minutes	5 minutes
Block IOCs on a firewall, such as a FortiGate	45 minutes to 2 hours	2 minutes
Remediation and incident response	60 minutes to 6 hours	5 minutes
Prepare and send an incident summary report	2 to 3 hours	2 minutes
Total	4.5 to 15 hours	20 minutes

Figure 2: FortiSOAR helps SOC teams reduce incident response time.<sup>6</sup>

As part of the integrated Fortinet Security Fabric architecture, FortiSOAR unifies security tools, which helps shift a team's workload by automating the majority of tier-1 processes, so SOC analysts can focus on more critical tasks. The following use cases demonstrate the immediate value FortiSOAR offers to struggling SOC teams.

### **Use Case 1: Unified Rapid Response**

SOC teams need solutions that permit them to be adaptive, collaborative, and streamline operations so they can respond quickly. FortiSOAR is vendor-agnostic and helps lessen operational roadblocks by integrating disparate point security solutions into a centralized orchestration system that can be deployed in virtually any environment. It includes more than 300 out-of-the-box connectors, so teams can orchestrate, automate, and respond with their legacy tools in real time. And in a crisis situation, teams can use a war room to quickly make decisions, visualize threats, and cross-functionally collaborate beyond an organization's SOC. This collaboration connects analysts to critical information and other teams such as HR, legal, or other key stakeholders.

Analysts can manage operational and critical tasks in real time from their mobile device (iOS and Android). Teams can operate FortiSOAR seamlessly with existing security solutions from other vendors and ingest alert information while providing a centralized point of visibility and control across the organization. This integration eliminates ecosystem fragmentation, simplifies security operations processes, and extends the useful life of existing tools to maximize the return on investment (ROI) for those purchases. FortiSOAR enables teams to centralize their entire security process and to respond with all their current tools, which results in faster real-time response.

### **Use Case 2: Dynamic Alert Triage Automation**

Due to lengthy incident response processes, it has become increasingly difficult for analysts to keep up with the pace of incoming alerts. FortiSOAR aggregates these alerts in one place while enriching them with added context to help speed resolution. FortiSOAR streamlines simple SOC tasks such as alert ingestion, prioritization based on severity levels, and assigning tasks. It also automates more complex exchange-to-exchange (E2E) tasks, such as triage, enrichment, investigation, and remediation, cohesively centralizing the security processes by automatically correlating alerts from across a security stack into a single incident.

The machine learning (ML)-driven recommendation engine in FortiSOAR also helps reduce the number of false-positive alerts and provides support for defining, guiding, and accelerating investigations. It cohesively centralizes security processes by automatically correlating alerts from across a security stack, which can provide insights into threats that might not have been captured if they were assessed independently.

These sophisticated integration and automation capabilities help to eliminate many of the common burdens associated with alert fatigue, so SOC analysts can focus on threat hunting. FortiSOAR helps reduce workloads and the windows of exposure to an active breach threat.

### **Use Case 3: Incident Response With Custom SOC Process Mapping**

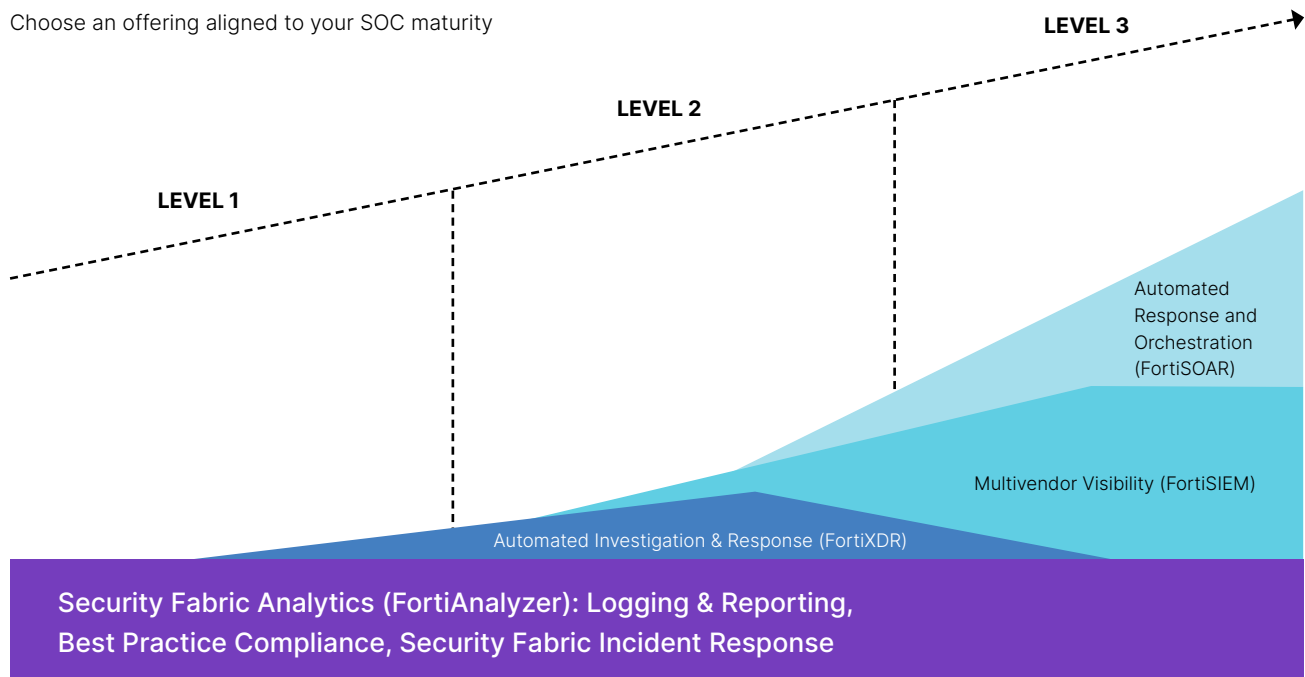
The existence of numerous manual workflows impedes alert investigations and increases time to resolution while increasing the risk of human oversights and errors. Organizations in this situation are not merely operationally inefficient; they are at increased risk of a breach. Security teams can increase efficiency by automating every task, change, or update according to the organization's needs. Instead of just automating a single entity, FortiSOAR can augment the entire SOC and improve overall security.

Going beyond investigation purposes, FortiSOAR can be used to improve efficiency where it is considered most essential for optimal incident response. Security teams can automate any response and subroutine to easily customize the solution around their internal framework on-demand. FortiSOAR can simplify custom connector, module, widget, and playbook building using guided templates that help expedite configuration. Where it makes sense, analysts can set threshold conditions at which FortiSOAR will immediately take an identity offline and use its built-in playbooks and connectors.



## Simplify Security Operations

SOCs can be classified into three levels of automation, as shown in Figure 3. Fortinet offers a range of components to improve the efficiency of security teams at each stage or level of maturity. Because of their different staffing levels and organizational structures, SOC teams at each of these levels have characteristically different challenges.



The Fortinet Security Fabric meets the challenges of each automation level with integrated offerings:

- FortiAnalyzer logging and reporting
- FortiXDR automated investigation and response across the fabric
- FortiSIEM security information and event management
- FortiSOAR orchestration and automation of security processes

At level 1, Fortinet Security Fabric customers can initiate their analytics and automation foundation with FortiAnalyzer. FortiXDR extends this foundation, by enabling automated incident detection, investigation, and response across the Security Fabric. At level 2, those organizations that require multivendor visibility and analytics benefit from FortiSIEM.

FortiSOAR is designed for automation level 3 enterprise teams that require full orchestration and automation of security processes across the Fortinet Security Fabric and in multivendor environments. It builds on the capabilities of FortiAnalyzer and FortiSIEM, adding more comprehensive workflow automation and orchestration, artificial intelligence (AI)-driven alert prioritization, and more built-in connectors for data ingestion and response coordination.

The powerful capabilities of FortiSOAR are most beneficial for experienced security teams with five or more analysts, well-defined security processes, and sizable security stacks. FortiSOAR is also highly effective for SOC teams that have been using multiple analytical or dedicated products similar to SOAR. These SOC teams are likely mature enough for SOAR itself, and FortiSOAR provides an effective and efficient upgrade.

## Managing Risk, Resources, and Results

Security operations teams face the dual pressures of an expanding attack surface and a lack of resources, which means they will continue to struggle to keep pace with growing risk exposure. An effective, fully featured SOAR solution can help teams address these difficulties while also enhancing, optimizing, and fortifying their organization's security processes.

FortiSOAR offers a nimble solution that helps security teams quickly adapt their response to an ever-evolving threat landscape. Teams can use the case management, automation, and orchestration capabilities in FortiSOAR to advance their entire incident response process. The outcome for organizations is a simplified security ecosystem, elimination of alert fatigue, accelerated response times, and a reduced burden on limited team resources, while maximizing team collaboration.

In addition, Fortinet offers simplified licensing for FortiSOAR through a user-based, predictable licensing model. Teams can leverage the efficiencies of FortiSOAR while staying within budget, regardless of the volume of incidents they handle. With an inherently scalable architecture, FortiSOAR delivers high availability for growing enterprise organizations. The solution can expand across growing and/or distributed organizations without having a serious impact on the resources needed for deployment and management at scale.

<sup>1</sup> ["2019 Cost of a Data Breach Report,"](#) Ponemon Institute and IBM Security, 2019.

<sup>2</sup> ["Security Orchestration Automation & Response \(SOAR\) World Markets, Outlook to 2024: The High Number of False Security Alerts Presents Lucrative Market Opportunities,"](#) Research and Markets, November 15, 2019.

<sup>3</sup> ["Cisco Cybersecurity Report Series 2020 CISO Benchmark Study,"](#) February 22, 2020

<sup>4</sup> Steve Morgan. ["Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021,"](#) Cybercrime Magazine, October 24, 2019.

<sup>5</sup> ["Strategies for Building and Growing Strong Cybersecurity Teams: \(ISC\)<sup>2</sup> Cybersecurity Workforce Study, 2019,"](#) (ISC)<sup>2</sup>, 2019.

<sup>6</sup> Internal Fortinet calculations.



[www.fortinet.com](http://www.fortinet.com)