WHITE PAPER

Automate Security Operations with the Multilayered Fortinet Automated SOC Solution



Executive Overview

As the threat landscape becomes more complex, organizations struggle to keep up with increasing risk. The security operations center (SOC) is expected to defend against unrelenting, ever-more sophisticated cyberattacks. However, according to a recent study, more than half of respondents believe that the security operations environment has become more difficult to manage over the last two years.[1]

Unfortunately, these difficulties come at a time when the cybersecurity skills shortage is worsening. Another study found that 3.4 million additional workers are needed globally to secure assets effectively—a year-over-year increase of 26%.[2]



81% of organizations believe that their security operations have been negatively impacted by the skills shortage.[4]

It's important for enterprise security leaders to have a comprehensive toolset that includes:

- Behavior-based sensors that can be deployed across the digital attack surface for early detection and response
- A centralized platform for analytics and synergistic response
- Outsourcing and consulting services for operational readiness, staff augmentation, and assisted response

Fortinet can help fill the skills gap with all the necessary components for automated security operations. Organizations that fully deployed artificial intelligence (AI) and automation had a mean time to detect and contain that was 74 days faster, with an average cost of a breach that was $3M less than those with no AI and automation.[3]

The Automated SOC: Keeping Pace with a Constantly Evolving Cyber-Threat Landscape

The cybersecurity threat landscape is rapidly evolving, and many companies are not able to adapt quickly enough. Depending on the organization, this can be due to a limited number of skilled personnel, operational complexities, or inadequate technology—or a combination of the three. Fortifying against accelerating cyber threats demands security solutions that shift workloads away from overburdened and understaffed SOC teams while empowering them to achieve more.

By using intelligent security automation, these tools not only reduce mean time to detection (MTTD) and mean time to response (MTTR) but also improve operational efficiency. The result is that security teams can provide more robust protection, reducing risk without increasing headcount.

Optimizing security operations without adding staff

Given the growing cybersecurity skills gap and the general staffing challenges that organizations continue to grapple with, the people component of security operations may be the hardest to improve. Even if financial resources are plentiful (which is rarely the case), it is difficult for organizations to build a SOC team that is adequate for the processes and products they currently have.

With Fortinet, organizations can implement best-practice processes and roll out technology that provides both robust security and SOC automation—actions that can help mitigate staffing challenges while improving the overall security posture.

Behavior-Based Sensors for Early Detection

Behavior-based sensors can detect early signs of threat activity when deployed at the endpoint, network, and data repository, both within the organization and outside of it. The whole ecosystem leveraged by threat actors can be monitored, enabling faster detection and therefore faster response. Fortinet offers the most detection sensors of any available solution as part of the Fortinet Security Fabric.

Endpoint protection with rapid remediation

FortiEDR endpoint detection and response helps organizations identify and stop breaches in real time automatically and efficiently. Security teams are saved from the typical slew of false alarms and disruptions to business operations with FortiEDR, one of the most innovative endpoint security solutions available. It proactively reduces the attack surface, prevents malware infection, detects and defuses potential threats in real time, and can automate response and remediation procedures with customizable playbooks.

Virtual security analyst: on-premises next-generation AI

FortiNDR network detection and response accelerates threat intelligence to machine speed to keep pace with the advanced threat landscape. Our network detection and response solution learns and adapts to new attacks on a specific organization over time, continually improving and optimizing the threat-protection life cycle. It supports security operations staff by identifying and analyzing network anomalies in fileless and file-based malware and identifies compromised systems across the organization with 100% certainty—all in less than a second.



A recent study found that AI and automation reduced the average mean time to detect by 54 days.[5]

FortiNDR uses AI technology to examine attacks and make decisions as if a human security analyst was manually investigating. The AI performs many tasks including:

- **Detection of network anomalies** by processing large amounts of north-south and east-west traffic at the perimeter and in the data center. It uses machine learning (ML) to profile traffic and detect anomalies and threats, such as encrypted attacks, malicious web campaigns, botnet-based attacks, intrusions, and more.
- **Investigation and classification of the attack** by tracking the original source of the infection with a time stamp. Then, it provides full visibility of the lateral spread from patient zero to all subsequent compromised systems.
- **Malware analysis** determines the type of malware based on features observed by the FortiNDR deep neural network (DNN) and provides an event timeline for each infection event. This is akin to a miniature kill-chain model that describes in scientific terms what the threat tried to do in a step-by-step fashion, including techniques employed.

A Centralized Platform for Security Analytics and Synergistic Response

Many organizations lack adequate technology products that can help them manage security operations across myriad IT tools and security point products. Teams may be using outdated log aggregation tools or may still rely on a member of the IT team to manually collect and correlate event data and context from disaggregated security tools. Both methods are time consuming, and other tasks may take precedence and delay this manual work. The result is a complete lack of visibility into potential threats before they cause damage.

This means that smaller, multi-function teams need to be selective about the products they have in their cybersecurity technology stack. According to Gartner, 80% of organizations are either currently or planning to consolidate security vendors to provide an integrated security architecture for an expanded attack surface—while improving efficiency.[6] As many organizations have learned from experience, adding another disconnected tool to the stack makes security operations more complex.

Centralizing Security Fabric analytics and reporting

FortiAnalyzer is an easy-to-deploy solution for centralizing visibility and threat detection across an organization's entire Security Fabric, including both on-premises and cloud deployments. FortiAnalyzer correlates log data from multiple Fortinet devices, providing valuable context to security analysts. By analyzing this data using ML and indicators of compromise (IOCs) provided via a global threat-intelligence feed, FortiAnalyzer can help even the smallest security team pinpoint and rapidly respond to threats within their network.

Bolstering Security Fabric detection and response

FortiXDR provides the first AI-based extended detection and response (XDR) solution, enabling automated incident detection, investigation, and response across the Security Fabric. Designed for a consolidated approach utilizing existing technologies of the Security Fabric, FortiXDR:

- Applies curated analytics to FortiAnalyzer that convert raw alerts into high-fidelity incident detections
- Leverages AI to automatically investigate those incidents
- Provides a simplified framework to predefine common response actions

In doing so, it enables a more hands-off approach for overstretched teams that lack the time or expertise to keep up with threat and alert volume.

Bringing security information together

The FortiSIEM security information and event management (SIEM) system is the logical solution to the complexity caused by a multivendor security architecture. It ingests log data collected from all security tools and performs automated correlation and analysis to provide a clearer picture of the overall status of the protected environment. FortiSIEM allows security teams to map operations to industry best practices and security standards, such as those published by the Center for Internet Security (CIS). In this way, FortiSIEM expands on the visibility that FortiAnalyzer brings to the Fortinet Security Fabric.

Going beyond the "known bad" events that are based on threat intelligence and triggered correlation rules, FortiSIEM also applies ML and statistical techniques to the monitored behaviors of users, endpoints, network flows, and other entities on the network to establish baselines of what is "normal" and what is suspiciously anomalous. Referred to as user and entity behavioral analytics (UEBA), this technology detects unknown attacks automatically, without adding additional burden to the SOC team. Detected events within FortiSIEM are automatically mapped to the MITRE ATT&CK framework tactics and techniques, a curated knowledge base of the most widely used attack methods. In all these ways, FortiSIEM expands on the visibility that FortiAnalyzer brings to the Fortinet Security Fabric.



84% of companies report that security alerts are becoming increasingly overwhelming as more security tools are added to the mix, and nearly half of all companies believe consolidated platforms will be the most effective approach to security over the next decade.[7]

Bringing full automation to security response

Although extensive visibility can help organizations quickly detect potential threats, their response tends to be fragmented and slow, thanks to lengthy manual workflows. But security orchestration, automation, and response (SOAR) solutions enable security teams to use automation to speed incident response and reduce risk.

Building on the capabilities of FortiAnalyzer and FortiSIEM, FortiSOAR helps an organization optimize its security processes by leveraging well-defined security playbooks. It automates repetitive tasks and responses to frequent threats and uses ML to eliminate false positives so that teams can focus on the alerts that matter. As a result, security teams can become proactive rather than reactive, freeing up analyst time for more strategic tasks.

Teams with more modest SOAR requirements that are using FortiAnalyzer can access the FortiSOAR container, which supplies a version of the Fortinet SOAR technology within FortiAnalyzer. This adds tighter orchestration and an automated threat response functionality with the convenience of an out-of-the-box deployment.

Readiness and Response Services to Help Teams Prepare Proactively

A recent study found that organizations with an incident response (IR) team that tested their IR plan incurred $2.66M less in the event of a data breach.[8] Fortinet offers security leaders two types of incident response services: Managed Detection and Response (MDR) Service and FortiGuard Incident Response and Readiness Service. These two services enable security operations teams to stop breaches and improve incident detection, investigation, and response capabilities, which in turn reduce operational costs and disruptions.

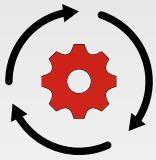
Incident Response Services: an extension of your team and technology

With FortiGuard Incident Response Services, organizations can easily achieve continuous monitoring as well as incident response and forensic investigation. The FortiGuard Services team is staffed with professionals who have years of training and experience in malware hunting and analysis, reverse engineering, multiple scripting languages, forensics, incident response processes, and the tactics, techniques, and procedures of bad actors.

The MDR Service is designed for customers of the FortiEDR advanced endpoint security platform. MDR provides organizations with 24×7 continuous threat monitoring, alert triage, and incident handling by experienced analysts and the platform. MDR is designed to help organizations defeat even the most advanced attacks.

To do so, Fortinet experts monitor the alerts produced by FortiEDR for customers. This team reviews and analyzes every alert, proactively hunts threats, and takes actions on behalf of customers to ensure they are protected according to their risk profile. Additionally, the FortiGuard team provides guidance and next steps to incident responders and IT administrators.

While many incidents can be addressed by FortiEDR and the MDR Service, sometimes organizations will need more customized services, which are available through the FortiGuard Incident Response and Readiness Service. This FortiGuard service assists customers with the analysis, response, containment, and remediation of security incidents to reduce the time to resolution, limiting the overall impact on an organization. In addition to serving FortiEDR customers (whether or not they have subscribed to the MDR Service), FortiGuard Incident Response and Readiness Service can also help organizations that have not deployed FortiEDR for a specific incident or breach investigation.



90% of organizations currently automate at least some security operations processes, and 35% plan to purchase security operations tools to automate and orchestrate security operations in the next 12 to 18 months.[9]

Flexible SOC Automation Solutions to Fit Any Gap or Need

Fortinet's portfolio of SOC automation solutions has been carefully designed to work with any size organization at any state of SOC capability and maturity. The solution is ideal whether building a complete technology stack managed by an in-house team, completely outsourcing the SOC function through one of Fortinet's service delivery partners, and everything in between. Most organizations today continue to have many manual and repetitive SOC processes that are automatable, while also missing out on advanced capabilities such as earlier, upstream detection. Fortinet's SOC automation solutions can help you detect earlier, respond faster, and avoid the fatigue that comes with too many alerts and too many monotonous and repetitive tasks.

[1] "SOC Modernization and the Role of XDR," ESG, October 24, 2022.

[2] "2022 Cybersecurity Workforce Study," (ISC)², accessed November 7, 2022.

[3] "Cost of a Data Breach Report 2022," IBM Security, July 2022.

[4] "SOC Modernization and the Role of XDR," ESG, October 24, 2022.

[5] "Cost of a Data Breach Report 2022," IBM Security, July 2022.

[6] Peter Firstbrook, et al., "Top Trends in Cybersecurity 2022," Gartner, February 18, 2022.

[7] "2023 State of Security Report," Cybersecurity Insiders, accessed November 9, 2022.

[8] "Cost of a Data Breach Report 2022," IBM Security, July 2022.

[9] "SOC Modernization and the Role of XDR," ESG, October 24, 2022.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

January 14, 2023 10:28 PM

1824543-0-0-EN