FORTINET

Accelerate Efficiency of Security Operations Across the Security Fabric with Rapid Response

Table of Contents

Executive Overview

In 2019 alone, over $124 billion was spent on cybersecurity;[1] however, many organizations' security teams are struggling to keep up. Challenges include too many consoles, alert overload, a reliance on manual processes, and a shortage of cybersecurity personnel.

The Security Operations Center (SOC) Maturity Model is designed to help security teams identify the capabilities in the Fortinet Security Fabric based upon their existing investment in people and processes in their SOC teams; hence, guiding enterprises with the solutions required to solve the challenges faced by organizations at each level of maturity.

Fortinet solutions, such as FortiAnalyzer (Security Fabric analytics and automation), FortiSIEM (security information and event management), and FortiSOAR (security orchestration, automation, and response), leverage security automation to address the key challenges faced by security architects and advance their SOC Automation. The Security Fabric links all of these solutions together, enabling lean security teams to maximize their ability to protect the enterprise.

Introducing Security Automation Across the Security Fabric

Operational complexity is a challenge for security teams of any size. The SOC Automation Model helps an organization's security team to identify their current maturity level and choose the Fortinet security solutions that are the most appropriate for their environment.

The SOC Automation Model is broken up into three key areas: people, process, and product. Within each area, an organization can be classified at a maturity level 1-3 based upon their security posture in that area. For example, an organization that is level 1 in all categories has a small IT team with no security staff (people), best effort incident response playbooks (process), and no dedicated security solutions (product). At the other extreme, an organization may have a large security team with experienced SOC analysts, well-defined playbooks, and have not only deployed but also measure the effectiveness of their SIEM and SOAR solutions.

With a cybersecurity skills gap of over 4 million and growing,[2] improving the people component of an organization's SOC Automation may be infeasible. However, by implementing the correct processes and selecting the right products, an organization can compensate for an understaffed security team.

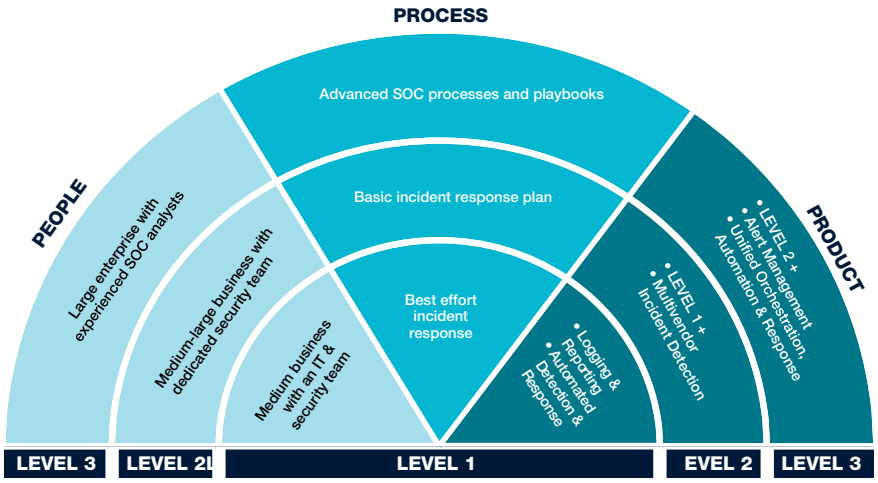


Figure 1: The SOC Automation Model.

Level 1: Achieve Visibility Leveraging Security Fabric Analytics

At level 1 of the SOC Automation Model, a security team has no dedicated security personnel or processes for addressing potential incidents. Additionally, the average enterprise receives over 10,000 alerts per day,[3] meaning that SOC analysts are overwhelmed and have little time for identifying and remediating true threats to the network.

Without dedicated solutions, an organization's security team lacks visibility into potential threats to their network. All log data must be manually collected and correlated before analysis can be performed. Many level 1 SOCs lack the knowledge or the resources to identify true threats, leaving the organization at risk.

FortiAnalyzer is an easy-to-deploy solution for centralizing visibility and threat detection across an organization's entire Fortinet 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 machine learning (ML) and indicators of compromise (IOCs) provided via a global threat-intelligence feed, FortiAnalyzer can help even the smallest security team to pinpoint and rapidly respond to threats within their network.

Level 2: Enhance Multivendor Visibility with SIEM

The average enterprise has 75 different point security solutions deployed on their network.[4] While each of these solutions provides valuable intelligence about potential threats to the organization's network, they often lack the context required to differentiate between a true threat and a false positive. Additionally, an array of standalone security solutions makes it difficult to enforce consistent security policies and maintain compliance with strict new data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

A SIEM system is the logical solution to the security complexity caused by a multivendor environment. A SIEM solution ingests data collected from products created by multiple different vendors and performs automated correlation and analysis to provide a clearer picture of the overall status of the protected environment.

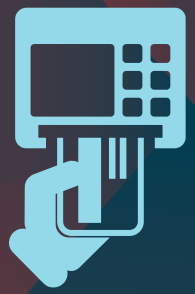
FortiSIEM allows security teams to map operations to industry best practices and security standards, such as those published by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). In this way, FortiSIEM expands on the visibility that FortiAnalyzer brings to the Fortinet Security Fabric.

Level 3: Incorporate Automated Response with SOAR

The cyber-threat landscape is accelerating as cyber criminals increasingly rely upon automation to speed up their attacks. While single-pane-of-glass visibility speeds up the rate at which a security team can identify a potential threat, a reliance on manual incident response processes means that defenders will always be a step behind the attackers.

SOAR solutions enable an organization's security team to leverage automation to speed incident response. By creating an automated framework to tie together an organization's complete security architecture, defensive actions can be taken by multiple different systems in concert. This minimizes the context switching required of security personnel, decreasing alert fatigue and speeding incident response.

FortiSOAR also enables an organization to optimize its security processes by leveraging well-defined security playbooks. By automating repetitive tasks and responses to common threats, FortiSOAR enables a security team to focus their efforts and limited resources on higher-level tasks.



Automation can reduce response times to minutes rather than days.

Leverage the SOC Automation Model to Intelligently Address SOC Complexity

The cybersecurity threat landscape is accelerating, yet many organizations suffer from a lack of adequate resources and skilled personnel. Defending against growing cyber threats requires security solutions that shift workload off of overburdened and understaffed SOC teams.

The SOC Automation Model helps security architects identify their current level of maturity and the steps that they must take to reach the next level. Fortinet solutions, such as FortiAnalyzer, FortiSIEM, and FortiSOAR, are designed to help make this transition.

By leveraging intelligent security automation, these tools reduce mean time to detection (MTTD) and mean time to response (MTTR), decreasing an organization's exposure to cyber threats.

In one year across 65 countries:[5]

- **2,216 reported data breaches**
- **53,000 reported cybersecurity incidents**

[1] Lawrence Pingree, et al., "Forecast: Information Security and Risk Management, Worldwide, 2017-2023, 3Q19 Update," Gartner, October 3, 2019.

[2] "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide," (ISC)², November 6, 2019.

[3] "How Many Daily Cybersecurity Alerts does the SOC Really Receive?" Bricata, October 2, 2019.

[4] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO, March 14, 2016.

[5] Gil Press, "60 Cybersecurity Predictions For 2019," Forbes, December 3, 2018.

www.fortinet.com

616492-0-0-EN

May 8, 2020 3:08 AM

ebook-FA-accelerate-efficiency-of-security-operations-across-the-security-582020