Improve Security Operations Across the Security Fabric

Table of Contents

Executive Summary

During 2020, it was reported that 65% of companies currently lack the skilled staff they need to maintain effective security operations.[1] Many organizations' security teams are struggling to keep up with operational complexities such as too many consoles and alert overload. And these problems are worsened by layers of manual processes. The impact of COVID-19 has presented new challenges and 76% of organizations indicated that remote work would increase the time to identify and contain a potential data breach.[2]

The Security Operations Center (SOC) Automation Model is designed to help security teams identify appropriate Fortinet security products for their SOC, based on their existing investment in people and processes. Fortinet offers a range of components to improve the efficiency of security teams at each stage of a SOC's maturity. Because of differing staffing levels and organizational structures, SOCs at each level of maturity have distinct requirements. Using the SOC Automation Model, SOC teams can determine the solutions they need to maximize their ability to protect the organization.

Simplifying 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, processes, and products. Within each area, an organization can be classified at a maturity level 1–3 based upon their security posture. For example, an organization that is level 1 in all categories has a small IT team with no security staff (people). They have limited incident response playbooks (processes) and no dedicated security solutions (products). 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 security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions.

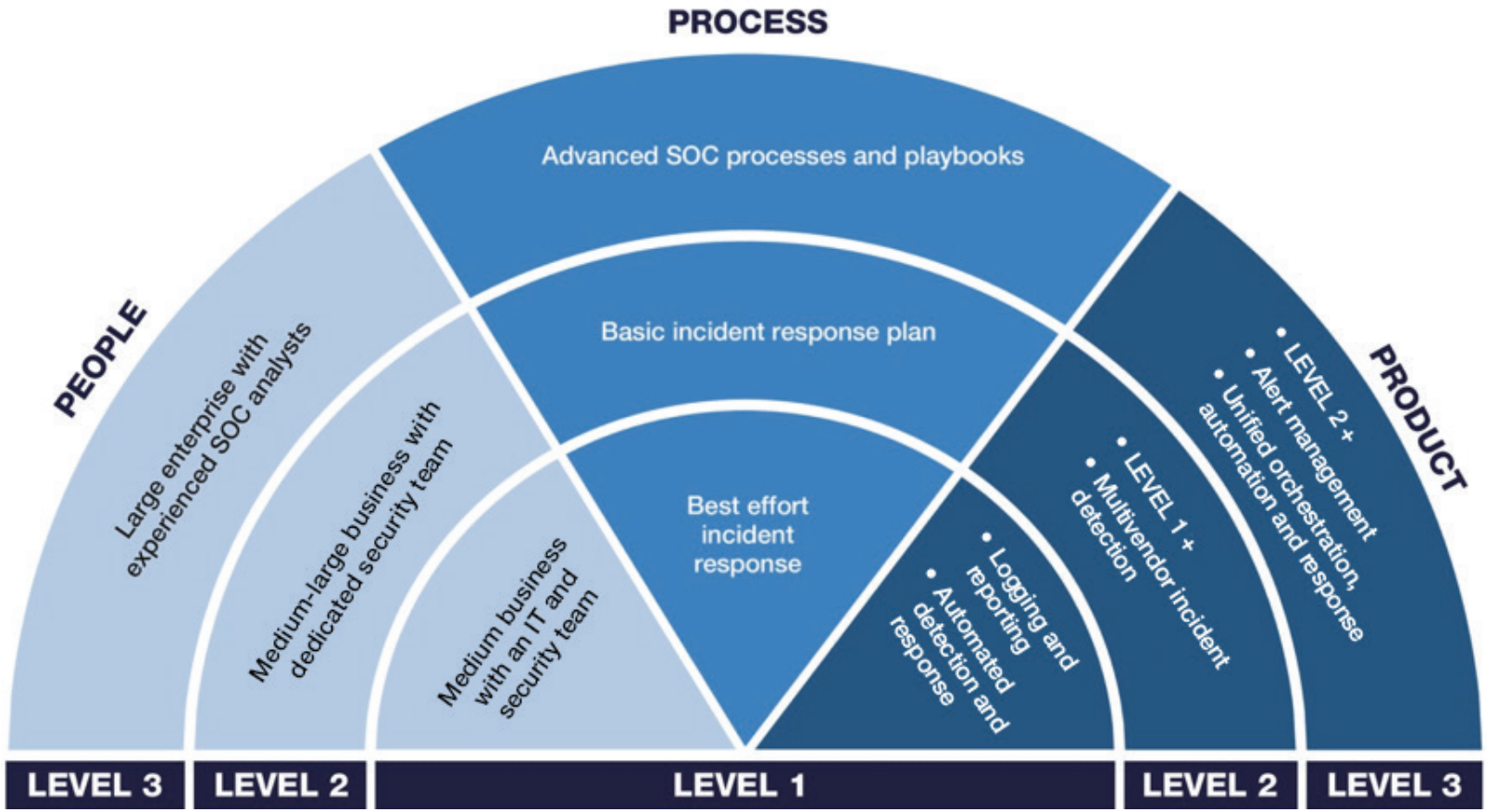

Figure 1. SOC automation maturity levels.

With a cybersecurity skills gap that is estimated at 3.5 million cybersecurity jobs unfilled in 2021 and growing, improving the people component of an organization's SOC automation maturity may not be feasible.[3] However, by implementing the correct processes and selecting the right products, an organization may be able to compensate for an understaffed security team.

The average enterprise receives 5,000 alerts per day.[4]

Level 1: Achieve Visibility and Identify True Threats

At level 1 of the SOC Automation Model, a security team has no dedicated security personnel or processes for addressing potential incidents. At this level, 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 of the log data must be manually collected and correlated before any analysis can be performed. Many level 1 SOC staff lack the knowledge or the resources to identify true threats, which puts the organization at risk.

Security Fabric Analytics

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, which provides valuable context to security analysts. By analyzing this data using machine learning (ML) and indicators of compromise (IOCs) provided through a global threat-intelligence feed, FortiAnalyzer can help even the smallest security team to pinpoint and rapidly respond to threats within their network. Smaller teams also can accelerate their maturity with the FortiSOAR container, which supplies a version of SOAR within FortiAnalyzer.

Extended Detection and Response

Many organizations are concerned about the dynamic cyber threat landscape, but are constrained by limited staff and processes. Their small, multifunction teams need to be selective about the products they have within their technology stack. As the first artificial intelligence (AI)-based extended detection and response (XDR) solution, FortiXDR extends the SOC Automation level 1 foundation. It enables automated incident detection, investigation, and response across the Fortinet Security Fabric.

Designed for a consolidated approach using existing technologies in the Fortinet Security Fabric, FortiXDR applies curated analytics to FortiAnalyzer, which converts raw alerts into high-fidelity incident detections. It uses AI to automatically investigate those incidents and 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.

The average time to identify and contain a breach is 280 days.[5]

Level 2: Maximize Multivendor Visibility With SIEM

As new threats evolve, to counter the sophistication of attackers, organizations deploy a multitude of technologies. This type of multivendor infrastructure often lacks visibility among the products within the security stack. Although each of the solutions may provide valuable intelligence about potential network threats, they often lack the context needed 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 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 Center for Internet Security (CIS). In this way, FortiSIEM expands on the visibility that FortiAnalyzer brings to the Fortinet Security Fabric.

Level 3: Automate Response With SOAR

To accelerate and expand the reach of their attacks, cyber criminals have been shifting their focus to include automation. Although extensive visibility into the network can help detect potential threats, the response to these threats can be fragmented because of lengthy manual workflows. Without the benefit of advanced security processes, security teams are often operating at a disadvantage, which increases an organization's risk. But with SOAR solutions, an organization's security team can speed incident response through automation.

Building on the capabilities of FortiAnalyzer and FortiSIEM, FortiSOAR is located at the peak of the SOC Automation Model. By creating an advanced automated framework coupled with comprehensive case management, an organization can pull together their complete security architecture. During a response, teams are enabled to respond cohesively and collaboratively with infrastructure security tools. As a result, security operators can accelerate incident response, decrease alert fatigue, and minimize the potential for overlooking vital information that could be hidden in the volume of alerts. FortiSOAR helps optimize security processes through well-defined security playbooks that automate repetitive tasks and responses to frequent threats. With FortiSOAR, security teams can become proactive, instead of reactive, giving analysts more time for more critical tasks.

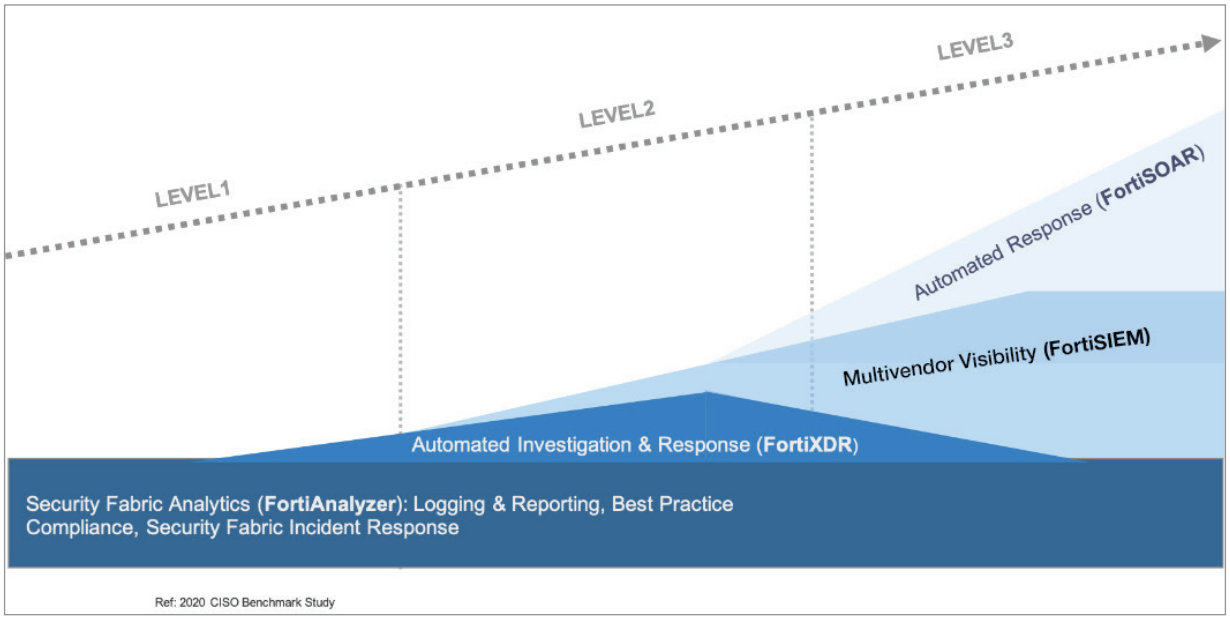

Figure 2. Best practice compliance.

Address Complexity With the SOC Automation Model

The cybersecurity threat landscape is quickly evolving, yet many organizations are not able to adapt at the rate it's growing. They may face operational complexities and limited resources and skilled personnel. To keep up with accelerating cyber threats, organizations need security solutions that help shift the cybersecurity workload off of overburdened and understaffed security teams. The SOC Automation Model helps security architects determine their current level of maturity and the steps that they must take to reach the next level.

Fortinet solutions, such as FortiAnalyzer, FortiXDR, FortiSIEM, and FortiSOAR, are designed to simplify the transition to each level. By using intelligent security automation, these tools not only reduce mean time to detection (MTTD) and mean time to response (MTTR) but they also decrease an organization's exposure to cyber threats and improve operational efficiency.

[1] "2020 Cost of a Data Breach Report," IBM, 2020.

[2] Ibid.

[3] Steve Morgan, "Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021," Cybercrime Magazine, October 24, 2019.

[4] "Cisco 2020 CISO Benchmark Report," Cisco, 2020.

[5] "2020 Cost of a Data Breach Report," IBM, 2020.

www.fortinet.com

May 3, 2021 12:04 AM

ebook-soc-automation

972314-0-0-EN