FORTINET

Strategies That Reduce Complexity and Simplify Security Operations

Table of Contents

FORTINET

Executive Overview

Two of the numbers that have grown the fastest in cybersecurity in recent years are the variety of threats and the number of point security tools designed to address them. Security architects are faced with a growing complexity that makes security operations difficult. However, three strategies substantially reduce this complexity: 1) centralizing and prioritizing threats, 2) simplifying audit and compliance, and 3) automating to speed response. These key strategies substantially improve an organization's security operations and security posture.

Up to 40% of new malware detected on a given day is zero-day or previously unknown.[1]

75 different security tools are in play at the average enterprise.[2]

Nearly 3 million security positions are unfilled worldwide today.[3]

Introduction: Too Much Useful Security Data

For security professionals, the numbers are discouraging: As cyber threats increase in volume and sophistication, organizations do not have enough security specialists available to address them.

The problem is not that security teams lack cybersecurity tools or valuable data from those tools to act on. There is simply too much. There are too many logs to correlate, consoles to manage, and alerts to evaluate. It is no surprise that 79% of security teams say they are overwhelmed by the volume of alerts.[4]

The takeaway is that security architects should consider several strategies to reduce complexity and simplify security operations.

01 Centralize Visibility and Prioritize Threats

Security monitoring should be centralized. Teams need a security approach that provides single-pane-of-glass visibility through a provided portal, or the capability to integrate security solutions with a popular visibility tool of choice.

The solution must provide an overview of anomalies across the extended digital enterprise, including on-premises, cloud, Internet-of-Things (IoT), and operational technology (OT) environments. An analytics-powered security and log management approach correlates data from multiple devices and combats alert fatigue by providing critical insight into threats. It pinpoints where an immediate response is required, enabling rapid response actions.

The solution should also enable zero-touch deployment of security configurations across the enterprise, minimizing human errors and misconfigurations. It needs to provide broad indicators-of-compromise (IOCs) visibility to security and operations teams, using machine learning (ML) to establish behavioral baselines, detect anomalies, and enable IOC identification. Additionally, it must receive new IOC updates gleaned from automated and human analysis of other environments around the globe that are provided by a threat-intelligence feed.

Having threat intelligence in one feed is important and actually heightens security risks. For example, in two recent global breaches, teams overlooked warnings because of alert fatigue.[5]

02 Simplify Audit and Compliance

When companies are too slow to implement critical security measures to protect their data, federal, state, and local governments step in. Globally, cybersecurity regulations are multiplying and becoming more demanding.[6] The European Union's General Data Protection Regulation (GDPR), which comes with stiff penalties and fines, is the biggest seen so far.[7] And with the California Consumer Privacy Act (CCPA) going into effect shortly, data privacy concerns will only increase for security architects.[8]

Security teams must seek an analytics solution that provides tools to map operations to industry best practices that are based on security standards from organizations such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). The solution should also generate reports that help prove compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS).

In addition, security leaders need to consider an analytics approach that answers three important questions of oversight:

1. Is the network set up properly? Can configuration problems be identified before they result in an incident?
2. What is the overall security posture? This should be summed up in a single measurement. It is a score that over time is useful in demonstrating the impact of security investments, and reporting on high-level trends to executive management and the board of directors.
3. What is proof of compliance? A solution can save hundreds of hours of manual analysis if it can analyze and report changes to network topology. It must simplify identification and remediation of high-risk and noncompliant devices and provide action plans and progress reports for both technical and management-level stakeholders.

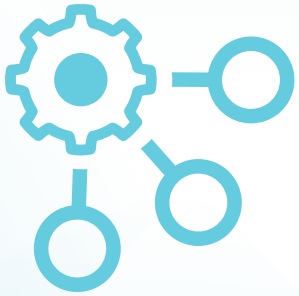
Answers to these questions can be formulated in an objective risk score, which needs to include comparisons against accepted benchmarks and peer organizations as well as actionable advice on how to achieve a better risk management posture.[9] The corresponding security rating score enables security architects to determine and prioritize which security components are requisite, while allowing security operations teams to allocate resources based on identified vulnerabilities and risk tolerance. Furthermore, the security operations team can use an easy-to-access trail of security issues and mitigation activities that they can leverage to proactively manage risk.[10]

"Technology risk metrics monitor the accomplishment of goals and objectives by quantifying the implementation, efficiency, and effectiveness of security controls; analyzing the adequacy of information security program activities; and identifying possible improvement actions."[11]

03 Automate to Speed Response

Network operations center (NOC) and security operations center (SOC) teams share the same goals of ensuring that services are available and protected—but they have different perspectives and tools. To help them collaborate, security architects must consider an analytics-powered security and log management approach that provides a consolidated view of operations and security. This enables NOC and SOC staff to align with one another and see integrated and cross-correlated NOC and SOC data. Analytics-driven threat detection identifies threats as high, medium, or low risk. Further, to make investigating a threat faster, an incident timeline view must show events in context.

This ascribed solution can also integrate with security information and event management (SIEM) and IT service management (ITSM) solutions, automating the workflow approval process between security and network teams for event responses and/or policy and settings recommendations. Security incidents are automatically passed to an ITSM solution, with analysts choosing from a catalog of responses, which can be implemented automatically from a central location. These capabilities reduce response times to minutes rather than days and enable limited staff to focus on expert-level decision-making rather than monitoring and information routing.[12]



Automation of security processes not only improves an organization's risk by reducing response times to minutes from days or weeks but it also can increase operational efficiencies.[13]

Conclusion: Cyber Risk Defines Our Era

A company may have billions of dollars of equipment at multiple facilities around the world, dispersed and well-secured physically. But in today's digital era, global operations can be brought to a halt silently and in minutes by a cyberattack, putting employee safety, revenue, and customer operations at risk, along with brand trust and reputation that may have taken decades to build. For example, NotPetya malware stopped operations at thousands of businesses worldwide, including a global shipping firm and a global pharmaceutical firm, for days. Worldwide losses were estimated at $10 billion.[14]

Facing the above advanced threat landscape, security architects must consider architectural changes to address incident response and event management. Organizations operate with about a one-in-three chance that a breach will occur in the next 24 months.[15] But experiencing a breach does not necessarily need to have a detrimental impact. As an underwriter at a specialty insurance risk company notes, "A breach alone is not a disaster, but mishandling it is."[16]

This is where a security architect can make a major difference, minimizing the time required for breach detection and remediation. An analytics-powered security and log management approach is a key element in achieving that goal. It can prioritize risks, speed investigations, and deliver answers faster in the event of a breach. Specifically, the ability to unify and correlate data from different security solutions and automate remediation workflows is key.

In One Year Across 65 Countries:[17]

2,216
reported data breaches

53,000
reported cybersecurity incidents

The average cost of a breach is $3.86 million, though organizations with fully deployed security automation can reduce that cost by $1.55 million.[18]

[1] According to internal data from FortiGuard Labs.

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

[3] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

[4] Greg Masters, "Crying wolf: Combatting cybersecurity alert fatigue," SC Magazine, June 9, 2017.

[5] Ibid.

[6] Jadzia Pierce, "Privacy and Cybersecurity: A Global Year-End Review," Inside Privacy, December 21, 2018.

[7] Juliette Rizkallah, "The Cybersecurity Regulatory Crackdown," Forbes, August 25, 2017.

[8] Mary K. Pratt, "State data privacy laws, regulations changing CISO priorities," TechTarget, April 2019.

[9] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, April 5, 2019.

[10] "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration," Fortinet, August 23, 2018.

[11] Mukul Pareek, "Standardized Scoring for Security and Risk Metrics," ISACA Journal, 2017.

[12] "Purpose-built Integrated NOC-SOC Management and Analytics," September 11, 2018.

[13] Marina Martin, "How Inefficiency Negatively Impacts Your Business," Dummies.com, accessed June 21, 2019.

[14] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, August 22, 2018.

[15] "2018 Cost of a Data Breach Study," Ponemon Institute, accessed October 18, 2018.

[16] "Phrases to help us think about cyberattacks…" The Cyber Rescue Alliance, accessed April 25, 2019.

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

[18] "2018 Cost of a Data Breach Study," Ponemon Institute, accessed October 18, 2018.

www.fortinet.com

402438-0-0-EN

July 3, 2019 4:30 PM

eb-cybersecurity-architect-fortianalyzer