

FORTINET®

- /Administration
- /Human Resources
- /Legal
- /Accounting
- /Finance
- /Marketing
- /Publicity
- /Promotion
- /Research
- /Business
- /Development
- /Engineering
- /Manufacturing
- /Planning


BRIDGING THE NOC-SOC DIVIDE

**UNDERSTANDING THE KEY
ARCHITECTURAL REQUIREMENTS
FOR INTEGRATION**


TABLE OF CONTENTS




EXECUTIVE SUMMARY




SECTION 1
NEW PERSPECTIVE ON SOC
AND NOC OBJECTIVES



SECTION 2
WHAT DOES INTEGRATED
NOC-SOC LOOK LIKE?



SECTION 3
ADDING COMPLIANCE
TO THE MIX



SECTION 4
END-TO-END AUTOMATION
HELPS SECURITY SCALE



CONCLUSION



EXECUTIVE SUMMARY

Enterprise IT organizations can view their global network assets in seconds. They can deploy new cloud servers in minutes. They can even have a new appliance delivered to a branch office in a few hours. But it takes them 197 days on average—more than half a year—to identify a data breach.¹ Considering that the average cost of a data breach has reached \$3.86 million, security leaders need more expeditious ways to detect and remediate threats before they wreak havoc.²

Bridging the gap between siloed network operations centers (NOCs) and security operations centers (SOCs) goes a long way to meet this need. It doesn't require any major infrastructure or organizational change. With appropriate technology, security architects can reach across the NOC-SOC divide to provide much-needed agility, scalability, and better use of limited technical resources. This eBook outlines the kinds of tools and processes that architects should consider.

¹ ["2018 Cost of a Data Breach Study: Global Overview,"](#) Ponemon Institute LLC, July 2018.

² Ibid.



01: NEW PERSPECTIVE ON SOC AND NOC OBJECTIVES

Security architects who follow the Cybersecurity Framework from the National Institute of Standards and Technology (NIST) will recognize that network security stretches across five key threat management stages: identification, protection, detection, response, and recovery.³ Though these stages are defined as discrete processes, in reality, they are often performed both continuously and concurrently.

What makes this difficult is the fact that some of the processes, such as identification and detection, are typically handled in the SOC, while others, such as response and recovery, are in the purview of the NOC. Each team uses its own tools to collect and manage data on network assets. Sharing data between the teams is a manual process, which especially drains limited technical resources when data is found to be out of date. It is also too slow—allowing threats to inflict damage and proliferate.

ASSESSING THE NOC-SOC DIVIDE

Addressing all five NIST stages continuously and iteratively requires a coordinated perspective that simultaneously gives an operational context to the SOC and security awareness to the NOC. Achieving that coordinated perspective first requires changing the silo mindset.

³ [“Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,”](#) National Institute of Standards and Technology, April 16, 2018.

To do so, it is helpful to reevaluate the roles and objectives of NOC and SOC teams (even if the two groups remain organizationally distinct). In a traditional siloed IT environment, NOC-based network engineers optimize for operational efficiency. That means leveraging SNMP/Syslog-based network monitoring, ticketing, and reporting systems to maintain continuous availability and throughput of servers, storage systems, networking equipment, firewalls, and any other IP-based devices.

Security analysts in the SOC, on the other hand, strive for intelligence efficacy and a defensible security posture. To achieve these objectives, SOC analysts may determine that certain network assets or links need to be further secured—for example, with SSL inspection, application control, or endpoint security software—even at the expense of throughput. And when they detect an emerging threat, SOC experts may recommend quarantining a networked asset until the threat can be resolved.

In sum, while the NOC is focused on throughput and availability metrics, the SOC evaluates its performance based on the number of threats its systems have detected, and their response to those threats. Worse, because of their separate areas of focus, the NOC and SOC may not develop efficient means of sharing information that is vital in the event of a data breach. Staff in the SOC may be aware of impending threats, but they need NOC data on systems and devices across the network in order to effectively mitigate the threats.



**NOC and SOC must work together
for the organization to respond
effectively and efficiently to attacks.**

EASING INTO INTEGRATION

The inherent conflict between the NOC's focus on operational efficiency and the SOC's emphasis on security efficacy must be resolved at the executive level; every organization will arrive at its own optimal balance. But once that balance is determined, it can be implemented only when the NOC and SOC have the same operational objective in view. For example, instead of just measuring NOC and SOC success in terms of network throughput and detection rates, respectively, the teams can be measured in terms of a common measure: **secure throughput**. Success against this metric would require the NOC to monitor the status of security measures along with network throughput. Meanwhile, the SOC would need to monitor not only security effectiveness but also metrics such as network throughput that indicate how security measures affect the organization's operations.

When both SOC and NOC teams view secure throughput as their objective—and define their SLAs in those terms—they can avoid much conflict between their teams.





In their throughput assumptions, network leaders will factor in security processes such as firewalling, antivirus checks, secure sockets layer (SSL) inspection, intrusion prevention system (IPS), and application control, all of which introduce some measure of latency. This is especially important when network operations specifies technology that incorporates security, such as software-defined WAN (SD-WAN) or secure web gateways.

At the same time, considering security in the context of operations encourages security architects and other IT security decision-makers to prioritize network performance as they design threat detection and response policies and select technologies such as firewalls, application control, and endpoint security. It gives them some accountability for any downtime in the name of security processes. Operationally appropriate security technology is designed for minimal impact on network throughput, a fact that should be reflected in the hardware and software specifications.

How can an IT function make this happen? Organizational restructuring may not be in the cards, but some reasonable technology improvements can instigate and support the change. To start, NOC-SOC collaboration is much easier through a single pane of glass, with integrated NOC and SOC dashboards and workflows that streamline operations and make security insights readily available.

02: WHAT DOES INTEGRATED NOC-SOC LOOK LIKE?

A decade ago, when there were fewer than 50 threat actors, security professionals had to contend with 1,000 or fewer alerts per day. Now, the number of threat actors has increased 20-fold, and analysts are inundated with more than 1 million alerts and indicators of compromise (IOCs) per day.⁴

A broader attack surface and a more advanced threat landscape are hard to combat. Enterprise firms, on average, report 20 successful intrusions in the past two years.

⁴“2018 Security Implications of Digital Transformation Report,” Fortinet, July 2018.

To make sense of such a huge volume of incidents, and to scope and prioritize their responses, analysts need the up-to-date network context: which parts of the network are really affected? Which applications and devices are actually impacted? This context can be provided by overlaying the alerts and IOCs on a network map in the

security dashboard. The map should be the same one the NOC team uses to manage the network, so that it presents the latest network status. The security team’s dashboard should also indicate the likelihood that each threat will spread and what network changes, if any, are needed to effectively contain or stop it. Armed with this information, the SOC team is in a better position to advise their peers in the NOC.

Meanwhile, in the NOC, if the operations team gets a report of network or server slowdown, their dashboard should indicate any security incidents that may be contributing to the slowdown. Because the SOC team is working with the same information, it is easier for the teams to consult with each other and decide on a course of action quickly. For some types of alerts, the teams may agree to automate the response, eliminating human-related delays while further reducing the administrative burden and associated costs.

⁴ Dave DeWalt and David Petraeus, “[The Cyber Security Mega Cycle Aftermath](#),” Optiv, September 7, 2017.

03: ADDING COMPLIANCE TO THE MIX

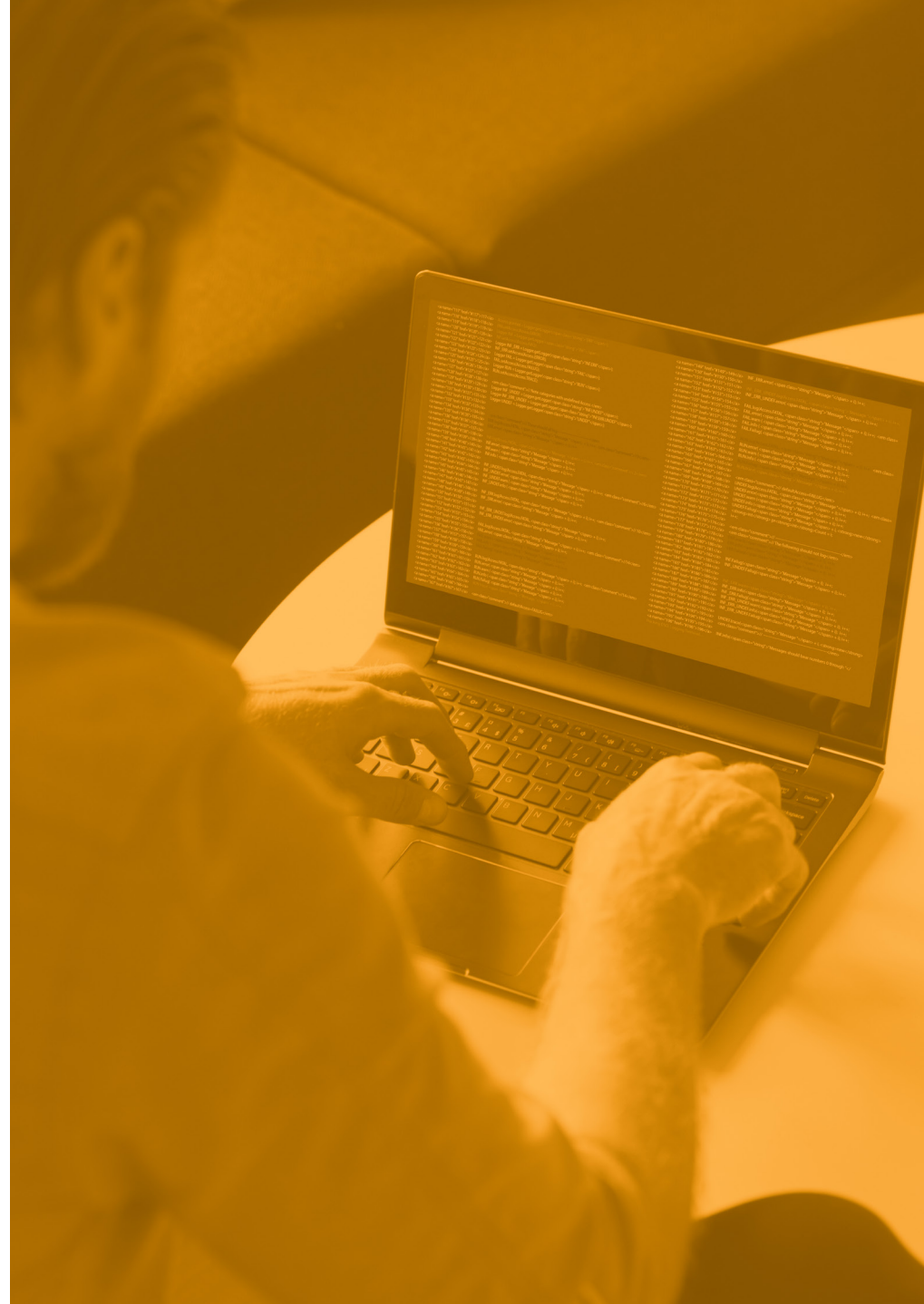
Regulatory compliance is placing a growing burden on security architects and their teams. In addition to the NIST framework, organizations are committed to compliance with ISO 27001 risk management, Control Objectives for Information and Related Technologies (COBIT), and the Committee of Sponsoring Organizations (COSO) framework for battling corporate fraud. Industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) for the healthcare sector, may also be in the purview of the security operations team.⁵

Each of these standards comes with its own set of best practices, and it can be difficult for staff to stay up to date. Managing and sharing best practices expertise within the organization is also a challenge. What's needed is a security metric that encompasses the most relevant best practices, and a software solution that outputs a single score which can be tracked over time and documented. Indeed, mapping the security score against the timeline of threat outbreaks is important, as is comparing the enterprise's security score with the industry average. These comparisons provide a basis for estimating security risk, essential information both for security architects and their CISOs or CSOs.

⁵ Taylor Armerding, "[How to write an information security architect job description](#)," CSO Online, July 20, 2017.

Monitoring the organization's performance on a single overarching security score requires a tool that bridges the NOC-SOC divide. The most efficient way to incorporate real-time threat information and composite security score data is with a direct intelligence feed into the NOC-SOC management system. The solution should produce reports that show both the organization's overall score and the breakdown of best-practice deficiencies according to their criticality for network security, with the ability to click through to details on what is holding the NOC or SOC (or both) back.

When security is quantified in this way, security architects can more easily prioritize resource allocations based on their security impact, which enables them to maintain the best security posture for the organization as a whole. Not only that, but they will have an easy-to-access trail of security issues and mitigation efforts that they can bring to bear should a compliance situation require that information.



64%

**of organizations feel
that adherence to
compliance requirements
is either very effective or
extremely effective.**

"The 30 cybersecurity stats that matter most," TechBeacon, March 22, 2018.

04: END-TO-END AUTOMATION HELPS SECURITY SCALE

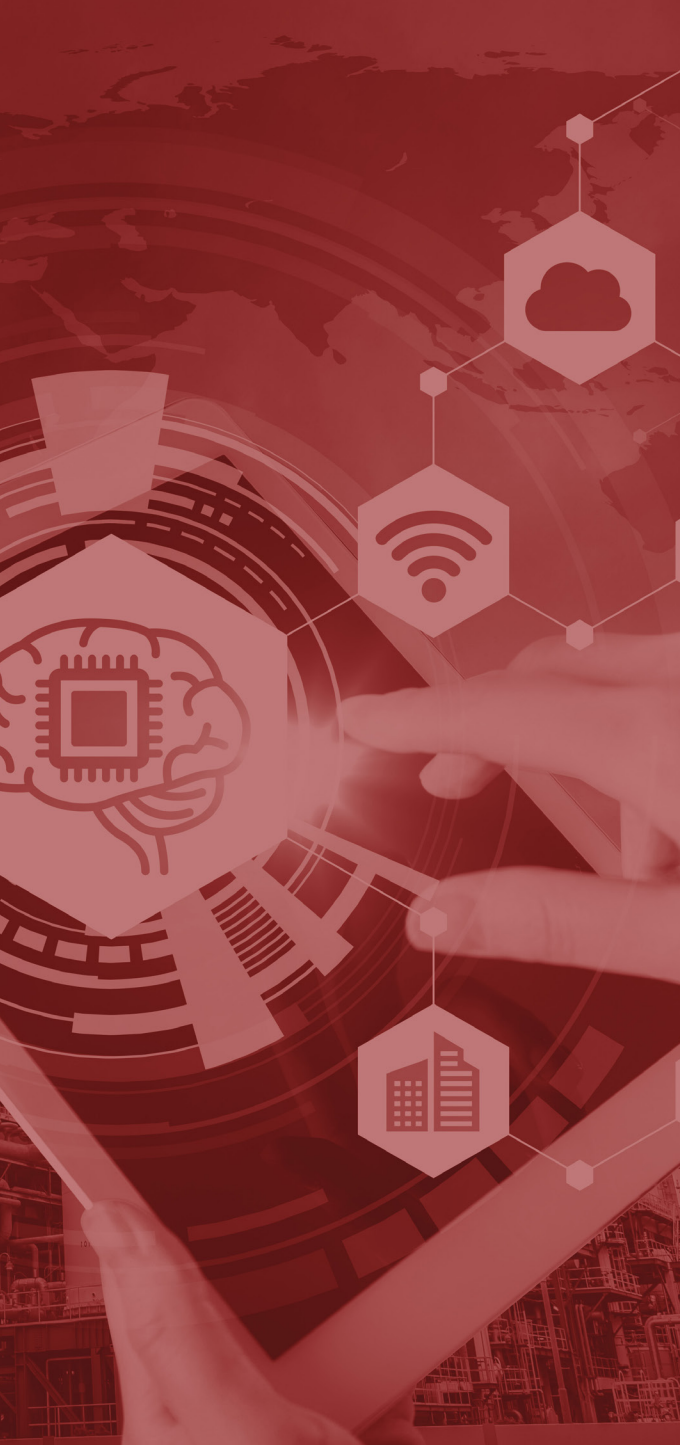
Providing an integrated perspective helps the SOC and NOC teams work better together, but human teamwork is not enough to keep up with the accelerating pace of threats. For one thing, there's a global shortage of security experts, and constrained SOC and NOC budgets are a challenge for many organizations. But even an army of experts is no match for the exploding population of threat actors.

Security architects can help security scale at the pace of threats with two interventions. First, they can streamline processes. Typical handling of security incidents involves multiple steps and touchpoints: the security analyst in the SOC, the internal or external IT service management (ITSM) team, and finally the NOC staff. A NOC-SOC technology solution can provide the deep integration needed to automate detection and response across the NOC, SOC, and ITSM silos. Such automation enables limited staff to focus on expert-level decision-making rather than monitoring and information routing. But more important for the security architect, it enables more effective security.

The average organization can reduce the cost of a breach by \$1.55 million by fully deploying security automation.

"2018 Cost of a Data Breach Study: Global Overview," Ponemon Institute LLC, July 2018.





To be of practical use, any automation capability should not require ripping and replacing security management and ITSM tools or extensive retraining. Rather, existing tools should be able to share information and processes.

Second, security architects should consider the intelligence of automation the organization deploys. It is one thing to configure the security management system with rules for responding automatically to known types of incidents, behaviors, and user profiles. It is quite another thing to enable the system to learn and adapt to new behaviors. Machine-learning technologies exist that autonomously collect, analyze, and classify threats, and then quickly develop highly accurate defensive signatures. Because this technology is new, caution is a virtue. These technologies will eventually be part of any NOC-SOC management system, but before deploying machine learning, security architects need to make sure the solutions will provide trustworthy information, which may require more maturity in the market.

CONCLUSION

Getting the NOC and SOC to work together involves transforming people and processes, which can be a challenge. In some organizations, certain security and network operations are outsourced, further complicating organizational integration. Still, security architects can greatly improve their security posture while supporting their organization's digital transformation by mitigating the impact of siloed operations. The technology changes proposed here offer a long lever for boosting both security and operational value.





GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapore 038988
Tel: +65-6395-7899
Fax: +65-6295-0015

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

Copyright © 2018 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. 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.