ROCK THE SOC 101

Building an Aware, Scalable, and Actionable Security Operations Center

WHITE PAPER

NETWORK AND SECURITY TRENDS

Today's distributed and rapidly blurring network boundaries are challenging organizations' abilities to track and manage data collected from nearly any device, process and store that data virtually anywhere on the planet, and scale and redistribute resources to meet new demands. The proliferation of IoT devices, cloud computing, mobile consumers, and online applications are accelerating this change. As the network edges continue to blur and expand, the potential sources, frequency, and types of threats organizations are facing are expanding and becoming more prevalent and sophisticated as well.

The result is that the potential of a security breach is now higher than ever. High-profile attacks have caused C-level executives and boards to adopt the mantra that "all business initiatives must have an associated security initiative component" in order to manage risk and better ensure success. Unfortunately, legacy security methods, technologies, and procedures for managing threats and responding to breaches are no longer viable or sustainable strategies for protecting today's highly dynamic and distributed networking environments.

Organizations that are slow to adopt the new security postures and technologies needed to manage today's risks are learning the hard way that simply conforming to regulatory compliance standards does not necessarily provide the comprehensive or cohesive security operations strategy or solution their network requires. In spite of unprecedented investments in security devices, breaches continue to be commonplace, including for those organizations whose networks are considered to be "compliant" with regulatory standards. This is driving the realization that today's new networks require new leadership, new thinking, new tools, and new processes.

For many organizations, this has been the driving impetus to either build or enhance their security operations center's (SOC) capabilities, while others are moving to outsource their security efforts to a managed service provider (MSP).

SOC AS A STRATEGY

Managing security operations against today's threats requires adaptive visibility, along with collecting and correlating local and global intelligence in order to anticipate both current and future threats. Just as critical are deeper and more contextual analytics to more rapidly detect and respond to those threats.

If your organization is building a SOC for the first time, you're going to want to clearly understand some of the challenges current SOCs deal with in order to minimize them as much as possible:

- Threats are growing in sophistication and volume. For many security teams, monitoring this environment can easily create a scenario of information

overload. There are just too many alerts and no easy way to prioritize them.

- It is impossible to reliably protect everything.
- Due to the division of responsibilities between IT teams, dynamically changing networks, and piecemeal security infrastructure, most SOCs have limited visibility into critical company assets and processes.
- Many SOCs have developed organically over time, and they also have developed ad hoc processes, tools, and methodologies, most of which are performed manually. Limited automation reduces the ability to respond to threats rapidly enough to prevent compromise.
- They have a limited understanding of their security adversaries.
- The growing security skills gap makes this environment complex to manage, leaving networks more vulnerable.

THE SECURITY OPERATIONS CENTER

There are three interrelated de facto standard components that make up a SOC: People, Process, and Technology.

People—People are the core of the SOC. You can have all the latest technology and processes, but that can only take you so far. You need skilled SOC members to run it and make it effective. In addition to having technical skills, it is crucial that they interact well with management, understand staffing structure requirements, and exhibit people skills. To retain good people, you will need to provide training and a satisfying career path. This also includes the people who touch the network, such as employees, customers, and suppliers.

Process—Properly defined processes are just as important to the SOC as people are. Good processes drive efficiencies and effectiveness, and they need to be defined and regularly tested for effectiveness in the analytics and efforts of managing against business, technology, operations standards, and key performance indicators (KPIs).

Technology—Equally important is the technology being used to enable the SOC. You need to consider what products, event data types, correlation capabilities, and additional contextual sources of information are needed for better detection capabilities.

Let's look at each of these components in detail:

PEOPLE

One of the first things to consider here is the line of business management constituents and stakeholders, as they will need to be involved with the overall security program and its performance against strategic initiatives. They will need to make key decisions about what is important to them, the business, their employees, and their customers, and will be a key ally in reporting up the chain on the effectiveness of the SOC. It is therefore critical to keep them involved through continuous updates.

Depending on the size of your SOC, team members will play different roles. In a large SOC, team members need to be skilled in their positions and understand how to triage and who to triage incidents to. For smaller SOCs, team members will most likely wear multiple hats. Defining their roles will help ensure that no aspect of managing the SOC is overlooked. You will need to assess their skills in order to understand what role would be the best fit. This will help provide a road map for individual training plans.

Keep in mind working in a SOC can be very demanding, and many people get burned out quickly or lose their sharpness. Regular training and cross-training is essential to keep team members sharp and motivated. It also is important to make sure SOC members have a clear path to advance their career.

Below is an example of various roles and positions a typical SOC may require. The titles may vary and roles are often combined, but this should give you an idea of what you will need to cover.

TITLE	ROLE
SOC Manager	Responsible for the overall management of the SOC, incident validation, metrics, and SOC resource and skills review.
Threat Intelligence Analysts	Focused on the collection and analysis of threat intelligence. It is often outsourced in smaller organizations.
Vulnerability Analyst	Analyzes scans and tests to identify vulnerabilities. Vulnerability scans and penetration testing should be performed once a year by a third-party entity.
SOC Operator	Usually a Tier-1 analyst responsible for incident identification, case/ticket creation, initial notification, and escalation.
Incident Analyst	Typically a Tier-2 or Tier-3 analyst responsible for incident validation, ongoing investigations, response actions, trending, and tuning.
Malware/Forensic Analyst	Analyzes malware to determine intent, and researches new threats, malware variants, and techniques used, including evasion techniques and payloads. Many organizations supplement this role with sandboxing technology or outsource it to consultants.

PROCESS

The SOC requires specialized processes for business, technology, operations, and analytics.

Business Processes

Business processes drive the overall direction of the SOC. In this phase, you map out the mission and goals, and define what priorities and functions the SOC will perform. This is typically completed before building even takes place. Critical business processes include the following:

A Project Sponsor: The sponsor's primary objective is to promote the creation of a SOC to management and other departments through educational workshops, training sessions, etc. Without management support, your chances of standing up a SOC are slim. Critical to the buy-in process is to establish a written mission or "a reason for the SOC to exist."

Mission and Objectives: The mission and objectives should include responsibilities, specific tasks, and customers. A sample mission may state, "provides a 24/7 service responsible for increasing the entire organization's security posture through continuous monitoring to proactively identify, contain, and manage security incidents to reduce the risks and impact of potential cyber threats. The function will also include the management of all security and networking devices including endpoints and systems."

Goals/Objectives: SOC goal and objective examples include detecting cyber incidents and security violations, proactively responding to security incidents, providing situational awareness to management, and enabling continuous improvement through lessons learned.

Functions: SOC functions ensure that the mission and business objectives are achieved. Example SOC functions include incident detection, compliance monitoring, configuration management (such as FW/IPS rule changes), and patching vulnerable systems.

Tasks and Responsibilities: These define the day-to-day details associated with each function and map back to the job descriptions of the SOC staff. For example, compliance monitoring may include creating and monitoring SIEM compliance dashboards, building and reviewing compliance reports, and ensuring that assets are properly configured.

It's almost impossible to monitor or protect everything in your environment. Because of this, you will need to establish priorities around key critical business processes, the assets those processes require, and which data is sensitive or has regulations tied to it.

Threat Actors: Once you understand what sorts of data reside in your environment, you can get a better idea of what sort of threat actors will be motivated to steal that data. Who are they? What is their motivation? What are their capabilities and tactics?

Threat actors include state- or industry-sponsored cyber spies, organized crime, hacktivists, malicious insiders, opportunistic hackers, vandals, script kiddies, and even user error.

Metrics: To determine the effectiveness of your SOC, you need to define performance and risk indicators. Metrics need to be specific, measurable, actionable, relevant, and timely. A high-level task list for creating your metrics should include determining KPIs, understanding where to collect data, establishing a baseline for normal network behavior, establishing target ranges, defining how KPIs will be calculated, and determining frequency reporting.

Technology Processes

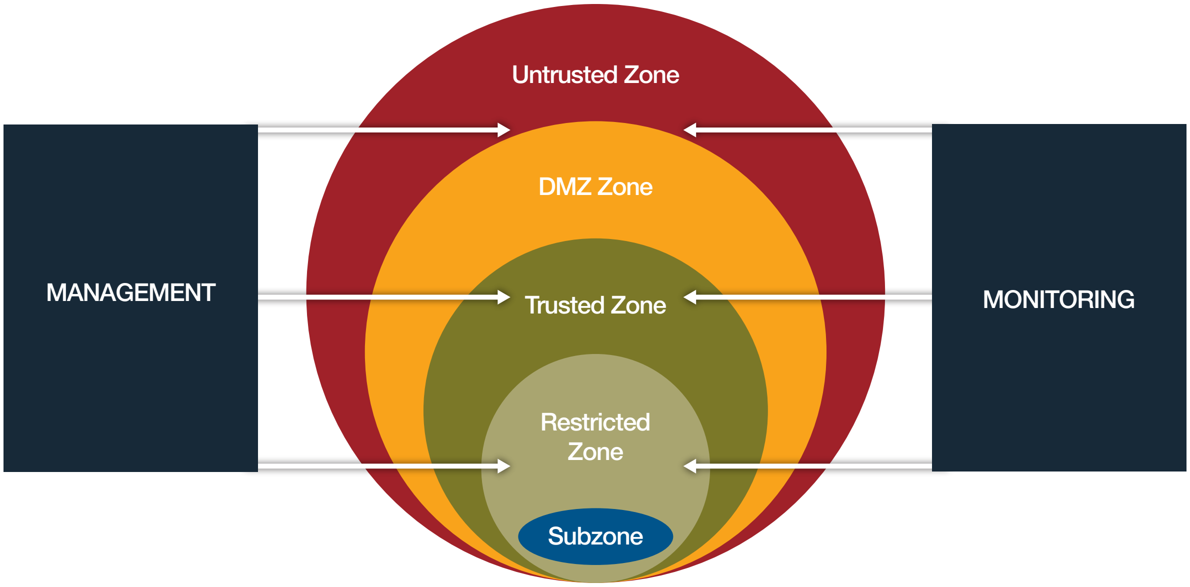
Many products are never installed or managed correctly, which means you never realize the full ROI on your technology investment. Establishing technology processes will help ensure that technology is configured, managed, and administrated effectively throughout its life cycle.

Network Design and Segmentation: Understanding how your network is designed, especially how devices are connected, and where data flows and resides is becoming increasingly difficult because of the growth of cloud networking, data virtualization, remote sites, mobile workers and devices, business partner connections, and Shadow IT.

Mapping your network and data flows will help you identify potential attack paths. This becomes your blueprint for deploying sensors, data collection points, and management and analysis tools. It also helps you to effectively segment your network into logical traffic or security zones.

Here is a simple network segmentation example:

- *Untrusted Zone*—Contains unknown and uncontrolled systems, such as devices on the Internet.
- *DMZ*—A secured area that can be reached by unknown and uncontrolled devices seeking access to network assets. It is important to filter and track traffic to and from these devices.
- *Trusted Zone*—Internal known enterprise systems. This zone contains such things as email and file servers and network devices.
- *Restricted Zone*—This area contains known systems that are restricted to certain users due to their critical nature or data sensitivity. Often, these areas are governed by compliance regulations. Servers in this zone should not have access to the Internet.



- *Subzones*—You can get even more granular by creating subzones within your restricted zones. Remember, as you create these zones you need to ensure proper management and monitoring within each zone.

Configuration Management: Many network breaches occur because of improperly configured devices. Device configurations may start off secure, but after time things like change requests can open vulnerabilities. That's why it's critical to manage the configuration process, monitor changes, and understand if changes are authorized and comply with corporate policy. Your change-control process should have well-defined tasks, including documenting current network device configurations and the purpose and details of any changes, maintaining an archive of older configurations to reset devices to known secure settings, and implementing policies to control the rate of change and who is authorized to perform changes and back-out plans.

Operational Processes

Attacks happen quickly, and the malware involved is usually automated, which means your SOC has to quickly detect and respond to these threats. Establishing operational processes and procedures helps standardize day-to-day processes to increase the effectiveness of the SOC. Where possible, use technology to automate many of the SOC's repeatable tasks.

Staff Turnover Procedures: Whether your SOC requires multiple tiers of analysts or only a few analysts operating at the same level, it's important to build and maintain turnover procedures. These procedures can include things like shift turnover procedures, such as logs and updates, shift scheduling and resource staffing, visitor procedures, and secure lock-up procedures. Some of these procedures, such as incident ticketing systems, should leverage vendor technology.

Incident Response Plans: Incident response (IR) procedures ensure the proper resolution, documentation, and reporting of all responses and findings for any security incident. They must also enforce proper identification, documentation, and the collection of evidence. If the need arises to report an incident to law enforcement, the members of the IR team should act as a liaison between the corporation and any external investigation team.

Resource Plans: Resource planning is essential to ensure that you have the appropriate staff resources available to handle threat volumes. Selecting and implementing appropriate technology can help solve the resource and budget issues by helping prioritize incidents to make the process more efficient and to minimize the staff needed to support the SOC.

Physical Access: The SOC is a critical resource, so physical access needs to be tightly controlled through such things as keycard access, cypher locks, or biometrics. Physical access tools should maintain audit logs of personnel entering and leaving the SOC.

Analytical Processes

It is critical to minimize costly mistakes and errors related to identifying and resolving security incidents. To accomplish this, most organizations establish a formal documented process for analysts to follow, including how and when management will be informed of detected incidents. Analytical processes to consider creating include reporting, management, and intrusion and malware analysis.

Reporting: One of the most important services the SOC provides is situational awareness, which means always seeing and understanding high-priority risks and threats. This requires generating appropriate reports to the staff and management. Most reports should be generated automatically, tailored to a specific audience, and incorporate trending analysis to help identify anomalies that would normally not be seen.

Malware Analysis: To understand the context of any incident, your SOC analysts need to have the tools and skills necessary to analyze any malware or forensic evidence found. Most teams aren't fortunate enough to have the funding and skilled resources necessary for a malware analysis lab. Instead, many leverage sandbox technology to automate the malware analysis process, and extend detections to enforcement technologies such as firewalls, endpoints, and mail systems. Ideally, your SOC team should have a combination of skilled resources available and the latest sandbox technology.

TECHNOLOGY

In addition to people and processes, your SOC requires security technology. These tools are crucial in protecting, detecting, and responding to threats. While an array of security devices is critical to securing your network and enforcing policy, an effective SOC also requires the collection and analysis of event data, contextual information, an understanding of malicious behavior, and the ability to effectively correlate intelligence collected from local devices and global threat feeds.

Security Devices: Undoubtedly, your organization has already deployed security devices across your network. It is critical to take an inventory of existing resources and identify any gaps you may have based on the threat actors targeting your business, the sensitivity of the data you process and store, any regulations you are required to comply with, and your ability to leverage these existing tools to collect threat intelligence and coordinate a synchronized response to detected threats.

The critical nucleus of any SOC is a Security Incident and Event Management (SIEM) solution. All other security solutions need to be able to report to this technology. In addition to a SIEM, an effective SOC needs to include many or all of the following security tools: Next-Gen Firewall, IPS, WAF, Database Protection, Web and Email Security, Host Protection and Endpoint Detection and Response (EDR), Data Loss Prevention (DLP), Mobile Device Security (MDM), Host Forensics, Network Access Control (NAC), Vulnerability Scanners, Identity Management (IdM) Systems, Asset Management, Database Monitoring, and other emerging technologies leveraging security analytics.

Keep in mind security technology should not only be chosen for its protection features. To respond to today's sophisticated and distributed threats, you need to develop a holistic architecture built around open solutions that can interact and share intelligence, automatically react to a locally detected breach, as well as participate in a centrally orchestrated threat response.

Event Data: Your SIEM solution needs to see and gather information from the various technologies in your network to provide situational awareness. To do this effectively, it's important to understand what type of data your SIEM requires in order to provide the clearest picture, including alerts/logs, session data, full packet information, and statistical data. Better visibility equals better analysis.

Contextual Information: This includes things like user, application, and vulnerability data, anomaly information, and asset classification or importance. Having this additional contextual information helps prioritize which alerts are most important to look at first.

Threat Intelligence Feeds: Once you have good visibility into your internal network, you may want to subscribe to a threat intelligence feed. These feeds usually consist of bad IP addresses, URLs, domains, hashes, or even processes and registry changes. Your SIEM technology should be able to consume these feeds and cross-reference them with your local data to determine if a device is communicating with a known threat actor or compromised system.

Correlation: Tying all of your collected information together is the central function of any SOC. Typically, the more information you have, the better correlation rules you can create and better detections you will make. Fortunately, most SIEM technologies provide preconfigured correlation rules that can be tuned to your unique network. In addition, your SIEM should also provide use cases, which are the logical, actionable reporting component of the SIEM. A use case can be a rule, report, alert, or dashboard to solve a set of needs or requirements. Building use cases will be a continuous process that you will refine over time. These can include hosts communicating to bad hosts, tracking configuration changes, user authentication tracking, and malware detection.

AN INTEGRATED SECURITY OPERATIONS SOLUTION

Building a SOC starts with understanding your business, including: What are your current corporate initiatives? How critical is each to the success of the business? What needs to be measured and monitored, and what are the targets for performance? What future initiatives need to be considered and enabled? What current and future risks need to be monitored and managed, and what is the level of risk the business is willing to take to ensure success?

At Fortinet, we start with the **Fortinet Security Fabric**, a holistic security framework designed on a common operating system and integrated solutions, enabling it to dynamically adapt to your evolving IT infrastructure needs and defend its rapidly evolving and unpredictable attack surface. The Fabric enables organizations to intelligently and transparently segment and microsegment their networks, and integrate advanced protections against sophisticated threats deep into the distributed environment. Because Fortinet and partner tools are built around a common set of open standards, each security element in the fabric is aware of each other, allowing them to share and push policies, integrate threat intelligence, understand application flow information, and automatically synchronize a coordinated response to detected threats.

Key Fortinet Security Operations components include:

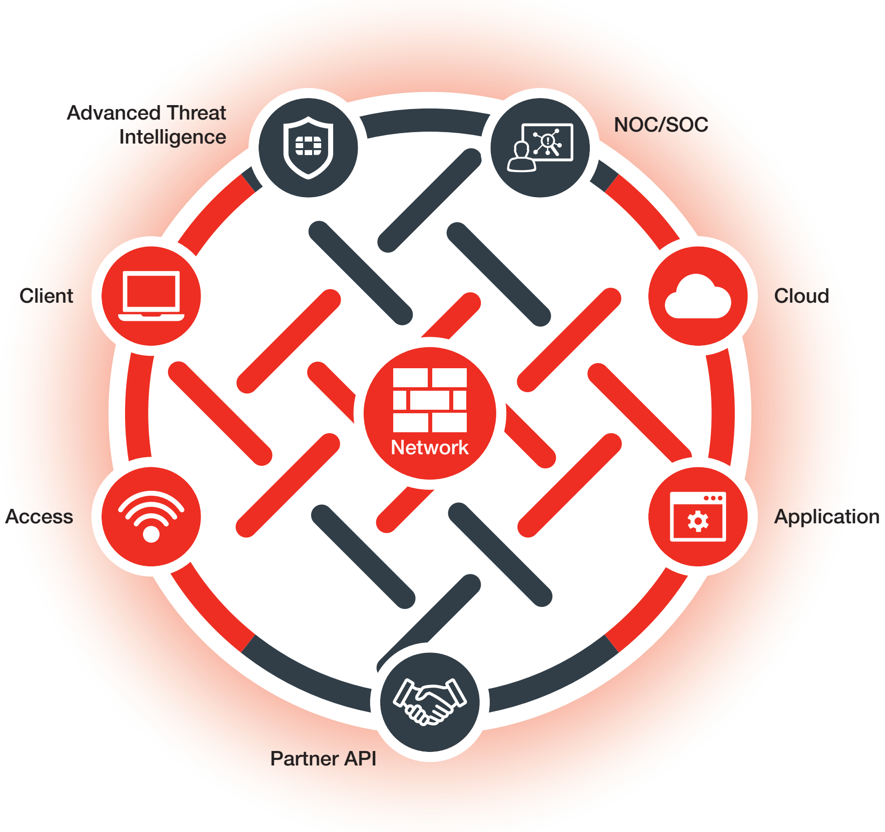
FortiAnalyzer—Provides centralized threat analysis of data collected from security and network devices distributed across the network, enabling much faster and more accurate threat detection.

FortiManager—Enables SOC and network operations center (NOC) personnel to initiate and synchronize a coordinated response to a detected threat across Fortinet devices, no matter what part of the network is being compromised. In addition, a growing number of Fortinet technology partners are an integral part of this distributed security framework.

FortiGuard Threat Intelligence—Dynamically adds global threat intelligence to your attack profile to ensure current and accurate detection of real-time threats.

FortiSIEM—FortiSIEM provides SOC teams with the centralized visibility that is needed to better manage a variety of rapidly changing security, performance, and compliance environments and business needs. It provides industry-leading and patented threat-detection technology that cross-correlates, in real time, both NOC and SOC analytics, enabling any SOC deployment to better understand the greater context of its environment.

FortiSIEM's virtual appliance format enables a simple and rapid solution deployment that automatically integrates hundreds of operations and network and security hardware devices, including those outside of the Fortinet family. Its unique ability to discover network-attached devices and self-learn their configurations allows it to create a dynamic centralized management database (CMDB). It can then establish event context and analyze collected threat intelligence with integrations from both



FortiGuard Threat Intelligence and third-party threat intelligence feeds.

It also provides prebuilt reports for all common needs, including regulatory compliance standards and the management of business applications. FortiSIEM also supports a multi-tenant architecture for reporting on separate network segments and virtual and logical environments. All this can be managed and monitored through its single-pane-of-glass console that reduces the complexity and time it takes to detect threats. And its highly scalable design ensures that organizations are able to process their ever-increasing volume of log and event data without interruption.

This combined solution set, woven together into a dynamic and responsive Security Fabric, integrates security monitoring and management from the endpoint, access layer, applications, network, data center, and cloud into a single, cooperative security solution that delivers the adaptive visibility, control, and analysis required by even the most challenging SOC environments.

FORTINET®

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
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

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

December 23, 2016