11 STRATEGIES OF A WORLD-CLASS CYBERSECURITY OPERATIONS CENTER

We Are Indian We Are Great

What is the SOC and why is it important?

This booklet provides a brief overview of the 11 Strategies of a World-Class Cybersecurity Operations Center. It offers a window into the 11 strategies discussed in the book, with the hope that the reader will be enticed to download the freely available full version of the book or to acquire the e-book or a print version.

Ensuring the confidentiality, integrity, and availability of the modern digital enterprise is a big job. It encompasses many parallel and related efforts, from robust systems engineering to effective cybersecurity policy and comprehensive workforce training. One essential element is cybersecurity operations: monitoring, detecting, analyzing, responding, and recovering from all measures of cyber attack. The operational focal point for incident detection, analysis, and response is the cybersecurity operations center (CSOC, or simply SOC).

Who is this book for?

If you are part of, support, frequently work with, manage, or are trying to stand up a SOC, this book is for you. Its audience includes SOC managers, technical leads, engineers, and analysts. Portions of *11 Strategies* can also be used as a reference by those who interface with SOCs on a routine basis to better understand and support security operations. Students and individuals transitioning into cybersecurity operations from other fields may also find it useful.

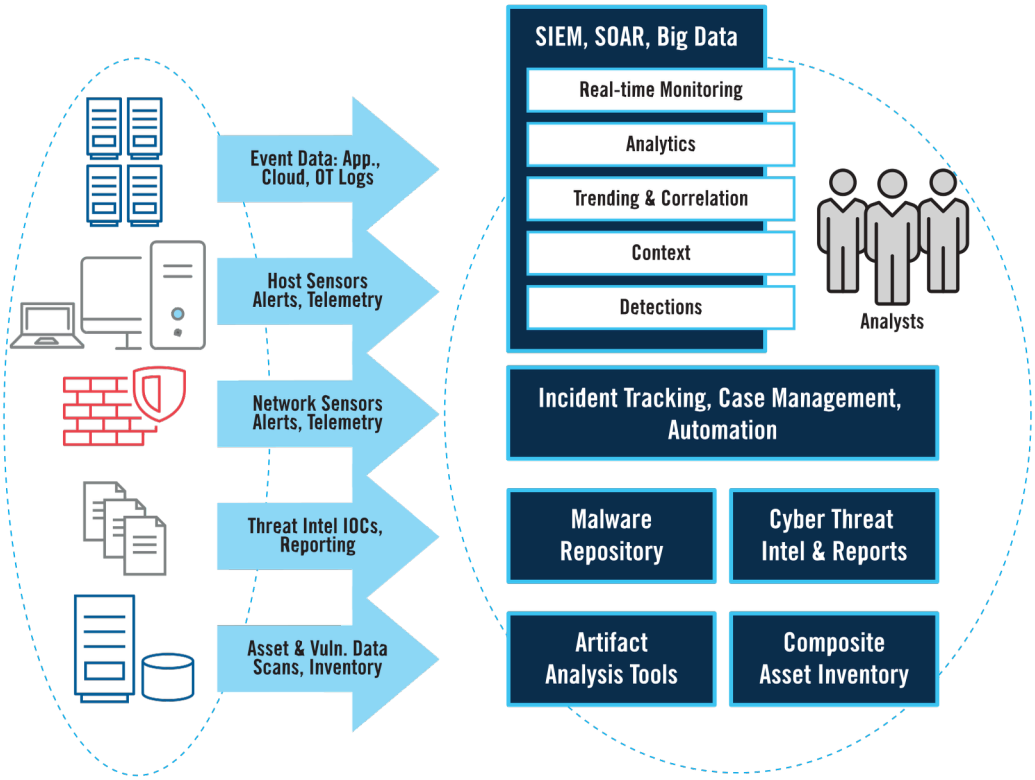
Table of Contents

SOC Fundamentals

The operational focal point for incident detection, analysis, and response is the cybersecurity operations center (CSOC, or simply SOC). A SOC satisfies the constituency's cyber monitoring and defense needs by performing a set of functions for its constituency.

SOC FUNCTIONAL CATEGORIES AND FUNCTIONAL AREAS
• Incident Triage, Analysis, and Response
• Cyber Threat Intelligence, Hunting, and Analytics
• Expanded SOC Operations
• Vulnerability Management
• SOC Tools, Architecture, and Engineering
• Situational Awareness, Communications, and Training
• Leadership and Management

- SOCs accomplish their mission in large part by being purveyors and curators of copious amounts of security-relevant data.
- They must be able to collect and understand the right data at the right time in the right context.
- Virtually every mature SOC employs several different technologies, along with automation processes, to generate, collect, enrich, analyze, store, and present tremendous amounts of security-relevant data to SOC members.



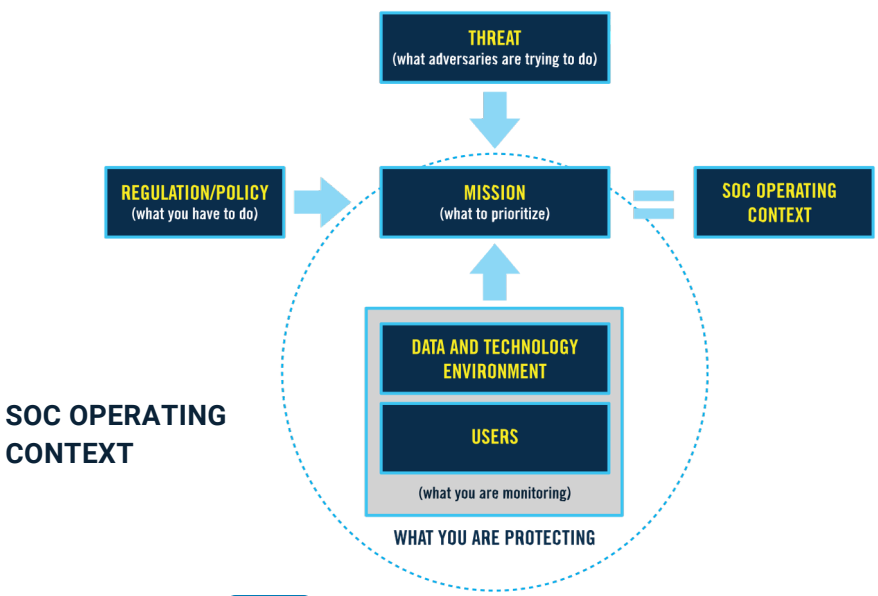
TYPICAL SOC DATA AND TOOLS

CHALLENGE: Cybersecurity operations exist to support their organizations' missions, so they need context for the data that they see and the action they take.

STRATEGY 1: Know What You Are Protecting and Why

Develop situational awareness across five areas over time:

- **Business/mission:** This area is focused on understanding a constituency's reason for being and how it operates.
- **Legal and regulatory environment:** This area includes government laws and industry regulations that are pertinent to cybersecurity operations such as reporting requirements or privacy regulations.
- **Technical and data environment:** This area includes understanding the number, type, location, and network connectivity of IT and OT assets along with the status of those assets (e.g., patch status, vulnerability status, or up/down status). This also includes knowing the constituency's critical systems and data, the connection and value of that data to the business, and the location of that data (on-prem systems, cloud, partner IT, etc.).
- **Users, user behaviors, and service interactions:** This area includes understanding typical patterns of behavior, including user-to-service and service-to-service interactions.
- **Threat:** This includes understanding the various types of threats (hacktivists, criminal, nation state, etc.) likely to be of particular concern to the constituency.



CHALLENGE: SOCs are on the front line in defending a constituency's cyber assets. Where they are in the organizational structure, and how they are funded, directly impacts their ability to fulfill their mission.

STRATEGY 2: Give the SOC the Authority to Do Its Job

A SOC charter—written guidance that grants a SOC the authority to exist, procure resources, and enact change—is an important component of building and operating a SOC.

- Elements should include the SOC's function, scope, and authorities along with expectations for partnering with other parts of the constituency. The SOC requires support and enablement through other cybersecurity and IT governance.
- The SOC should take an active role in developing and reviewing other existing constituency policies that support execution of their functions.

The SOC draws its authorities, budget, and mission focus from the organization to which it belongs.

- The SOC can be housed in many places within an organization, each with its own pros and cons.
- The most common placement is under the Chief Information Officer (CIO) or Chief Information Security Officer (CISO). Other options include under the Chief Operations Officer (COO), under the Chief Security Officer (CSO), under IT operations, or inside a specific business unit.

An effective SOC has a charter and set of authorities, signed by constituency executive(s), which enable it to advocate for needed resources and gain cooperation to execute its mission.

CHALLENGE: There are thousands of SOCs around the world and no two are organized exactly alike. What's appropriate for one organization may not work for another; there are many models to build from.

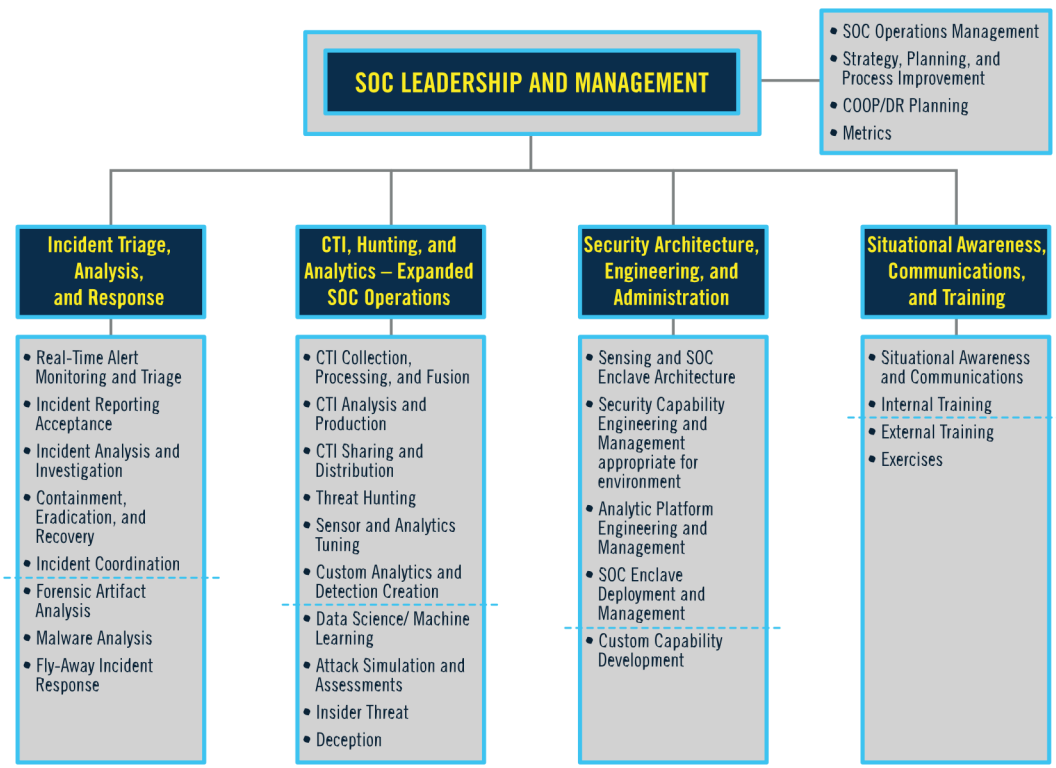
STRATEGY 3: Build a SOC Structure to Match Your Organizational Needs

Structure SOCs by considering the constituency, SOC functions and responsibilities, service availability, and any operational efficiencies gained by selecting one construct over another.

- The size of the constituency is a key driver in determining the appropriate type of SOC organizational structure.

Dimensions of a SOC organizational model include both the internal SOC structure (mapping of functions to roles) and the overarching model of how the SOC is placed within the constituency and its overall objectives.

SOCs will incorporate some or all of the SOC Functional Areas described in the Fundamentals section according to their constituency needs.



NOTIONAL CENTRALIZED SOC

Different SOC organizational models help the SOC support consistencies of dramatically different sizes and shapes. The primary SOC organizational models include:

Organizational Model	Example Organizations	Remarks
Ad Hoc Security Response	Small businesses	No standing incident detection or response capability exists.
Security as Additional Duty	Small businesses, small colleges, or local governments	No formal SOC organization. However, SOC-like duties are part of other duties.
Distributed SOC	Small to medium-sized businesses, small to medium colleges, and local governments	A decentralized pool of resources housed in various parts of the constituency.
Centralized SOC	Wide range of organizations including medium to large-sized businesses, educational institutions (such as a university), or state/province/federal government agencies	Resources for security operations are consolidated under one authority and organization.
Federated SOC	Organizations with distinct operating units that function independently of one another	A SOC that shares a parent organization with one or more other SOCs, but generally operates independently.
Coordinating SOC	Large businesses or government institutions	A SOC responsible for coordinating the activities of other SOCs underneath it.
Hierarchical SOC	Large businesses or government institutions	Similar to the Coordinating SOC structure; however, the parent organization plays a more active role.
National SOC	Country-level governments	Responsible for strengthening the cybersecurity posture of an entire nation.
Managed Security/SOC Service Provider	Organizations of all sizes	Provides SOC services to external organizations via a business/fee-for-services type relationship.

CHALLENGE: People are the most important aspect of operating a world-class SOC. Ensuring you have qualified staff—through training and recruitment—is key.

STRATEGY 4: Hire AND Grow Quality Staff

Staffing is one of the biggest challenges for a SOC; it is also one of the most important factors in the success of the SOC mission.

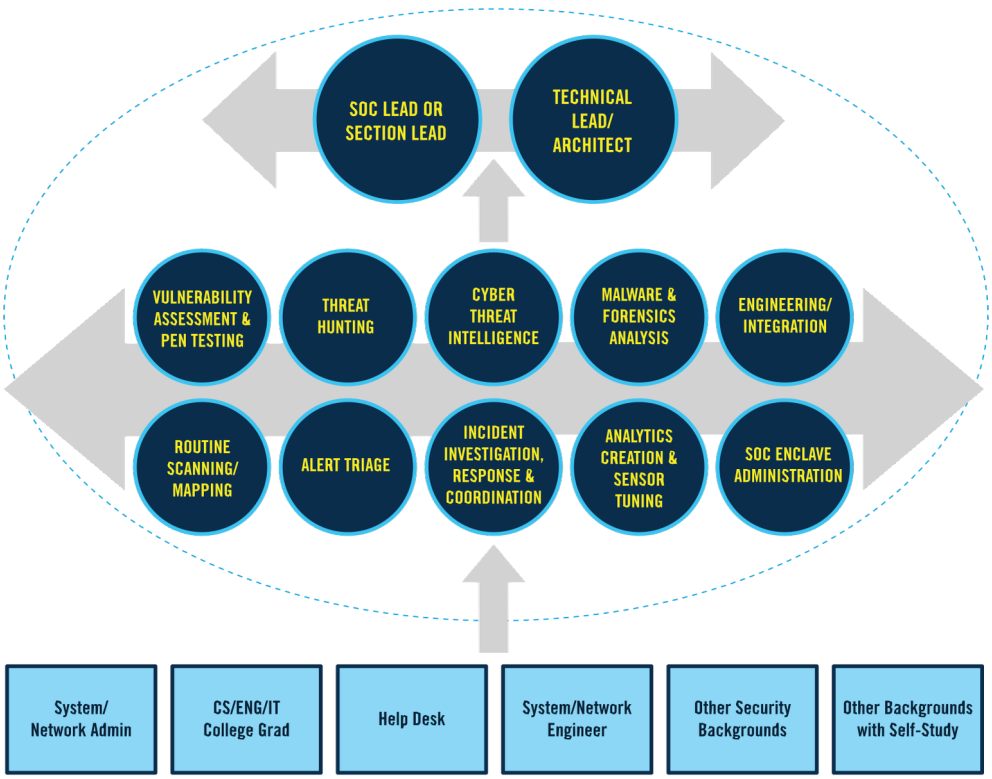
- When hiring, passion for the role is a key indicator of success.

There are not enough cybersecurity professionals available. Each SOC must also grow talent internally, and support career progression.

SOCs must also create an environment that encourages staff to stay by paying fair market value, creating a sense of belonging through communication and sharing among the SOC team, and supporting a diverse and inclusive work environment.

Staff turnover is a reality for most SOCs.

- Pre-plan for departures by formally capturing institutional knowledge to help address this issue and support overall SOC process execution.



SOC CAREER PATHS

CHALLENGE: As long as there have been computers and networks, there have been cyber incidents. Typically, a SOC's effectiveness is determined by how and when it responds.

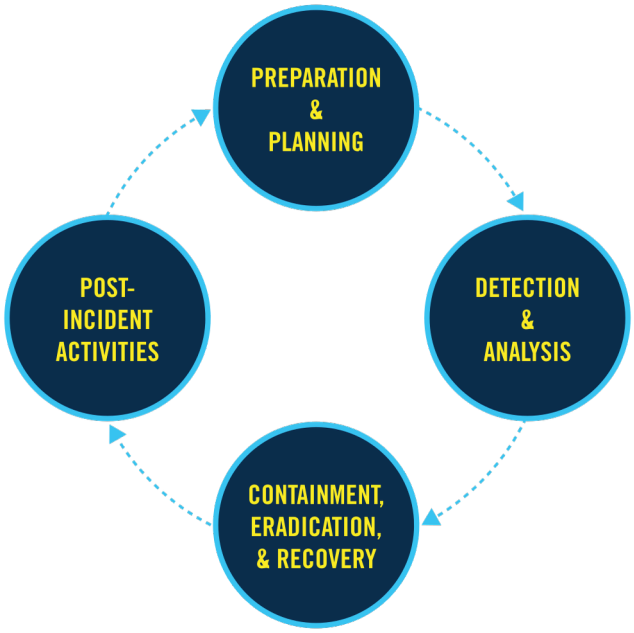
STRATEGY 5: Prioritize Incident Response

Prepare for handling incidents by defining incident categories, response steps, and escalation paths, and codifying those into Standard Operating Procedure (SOP) and playbooks.

Determine the priorities of incidents for the organization and allocate the resources to respond.

Team members must be given enough structure to ensure that expectations such as consistency, timeliness, and the removal of analytic bias are met, while also being given the freedom to act on their intuition and experienc.

Execute response with precision and care toward constituency mission and business.



NIST INCIDENT RESPONSE LIFECYCLE

CHALLENGE: Finding malicious activity and other traces of adversaries can be challenging. SOCs need to be proactive and identify threats before they enter their constituency's environment.

STRATEGY 6: Illuminate Adversaries with Cyber Threat Intelligence

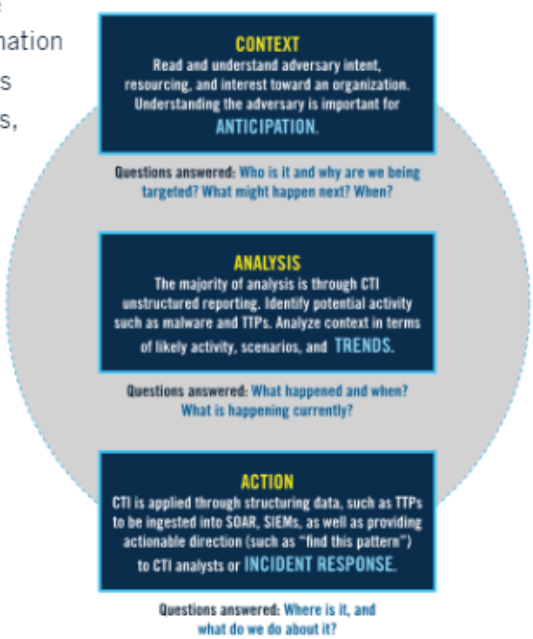
Tailor the collection and use of cyber threat intelligence by analyzing the intersection of adversary information, organization relevancy, and the technical environment to prioritize defenses, monitoring, and other actions.

Consider using MITRE ATT&CK to help inform and categorize adversary tactics, techniques, and procedures (TTPs).
Actionable Cyber Threat Intelligence (CTI) requires integrated analysis of adversary information, the constituency technical environment, and the business or mission context.

SOCs cannot predict attacks without adversary association. Adversary association is defined as the action of linking malicious activities to likely adversaries, or known groups of behavior, for defensive purposes without requiring absolute certainty that a specific person or group perpetrated the activity.

SOCs cannot predict attacks without adversary association. Adversary association is defined as the action of linking malicious activities to likely adversaries, or known groups of behavior, for defensive purposes without requiring absolute certainty that a specific person or group perpetrated the activity.

Using CTI effectively is an iterative process and evolves as more information is understood. The process includes understanding the context of events, performing analysis, and taking action.



CTI KEY COMPONENTS

CHALLENGE: Most constituencies generate more digital data than an SOC can possibly process and act upon.

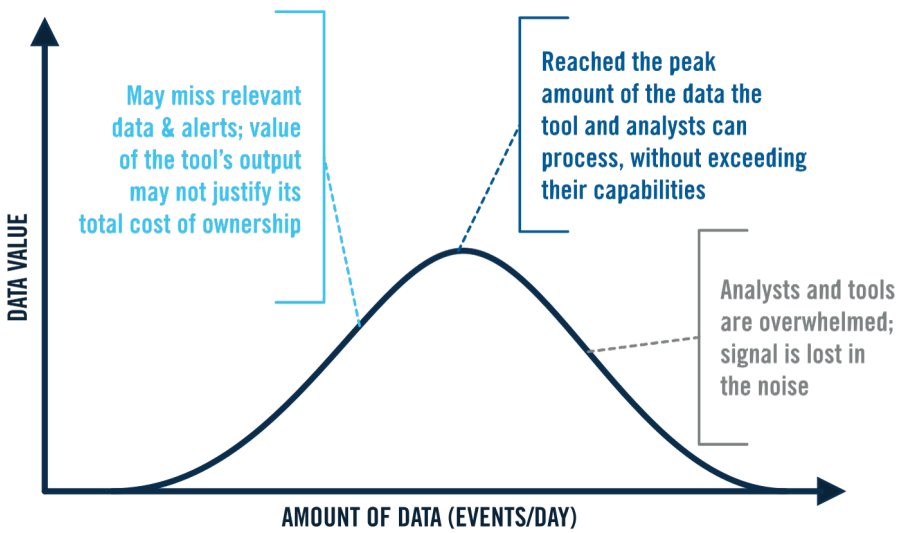
STRATEGY 7: Select and Collect the Right Data

Choose data by considering the relative value of different data types such as sensor and log data collected by network and host systems, cloud resources, applications, and sensors.

Consider the trade-offs of too little data (and therefore not having the relevant information available) and too much data (such that tools and analysts become over whelmed).

For both detecting and confirming intrusions, data and instrumentation from endpoints are generally considered more informative and provide more clarity than data from network traffic.

SOCs should collect data from all relevant environments including on-site data centers, cloud environments, mobile infrastructure, and operational technologies.



BALANCING DATA VOLUME WITH VALUE

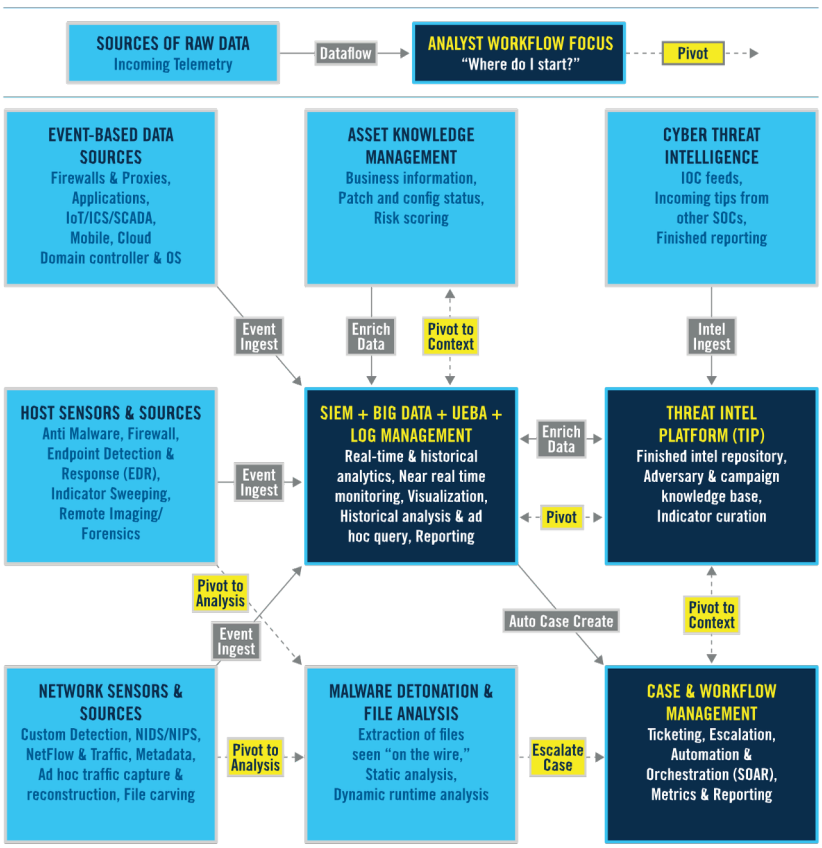
CHALLENGE: SOCs bring vast amounts of disparate data together into an information architecture. Analysts need to be able to quickly evaluate the data, turn the data into information, and use the information to fulfill their mission.

STRATEGY 8: Leverage Tools to Support Analyst Workflow

Consolidate and harmonize views into tools and data and integrate them to maximize SOC workflow.

Consider how the many SOC tools, including Security Information and Event Management (SIEM), User and Entity Behavior Analytics (UEBA), Security Orchestration, Automation and Response (SOAR), and others fit in with the organization's technical landscape, to include cloud and operational technology environments.

Each SOC brings to bear a different set of tools, capabilities, and integrations in support of their analysts. This figure shows one example architecture.



SOC TOOL INTEGRATION AND PIVOTING

CHALLENGE: No matter how well-funded or well-staffed a SOC is, it can never know everything about the cyber threat and vulnerabilities the organization faces. Collaborations—both internal and external—can provide valuable insight.

STRATEGY 9: Communicate Clearly, Collaborate Often, Share Generously

Engage within the SOC, with stakeholders and constituents, and with the broader cyber community to evolve capabilities and contribute to the larger cybersecurity ecosystem.

Improving communication, collaboration, and sharing should begin within the SOC itself.

- Everyone in the SOC should be given the opportunity to be an active participant in these areas, as only then can the SOC fully leverage its most valuable resource, its people.

Being able to express clearly and succinctly what the SOC is doing and what the SOC needs will go a long way toward building strong relationships with the SOC constituency and maximizing the SOC's effectiveness within the organization.

EXAMPLES OF COMMUNICATING, COLLABORATING, AND SHARING WITH DIFFERENT GROUPS

	Inform and be informed	Collaborate	Share
Within the SOC	Pass information from one shift to another.	Bring together incident responders and the CTI team to create a new analytic.	Mentor a colleague.
With Stakeholders and Constituents	Provide risk summaries and recommendations to stakeholders and executives.	Pre-plan with constituents how to respond to incidents and jointly publish guidance.	Hold a lunch and learn about the latest cyber threats and how they might impact the business.
With the Broader Cyber Community	Provide incident TTPs, IOCs, detection tactics to other SOCs, and receive some back.	Compare best practices, chosen joint activities such as hunt.	Hold cross training with other SOCs; incorporate and hold lessons learned sessions.

Partnering and sharing with others creates a stronger cyber defense community for everyone.

CHALLENGE: SOCs succeed when they fulfil their mission and protect the constituency's cyber assets. As technology changes and new threats emerge, SOCs need to understand what is working well and where improvements would be most beneficial.

STRATEGY 10: Measure Performance to Improve Performance

Determine qualitative and quantitative measures to know what is working well and where to improve. A SOC metrics program includes business objectives, data sources and collection, data synthesis, reporting, and decision-making and action.

Metrics can be broken up into three groups:

- Those that are meant for internal SOC consumption.
- Those that describe the SOC's value and operating status to stakeholders.
- Other things the SOC learns about the constituency's cybersecurity status that fall outside the SOC mission.

Not all measures result in positive outcomes. Choosing and monitoring the "wrong" measures can lead to wasted time or worse, a focus on harmful practices. Seek team consensus, compensating quality checks, and balance in metrics to emphasize not only basic service delivery, but growth in capabilities and a culture of transparency.

SOC METRICS PROGRAM

CHALLENGE: Cyber adversaries are continually evolving, and technology changes rapidly. SOCs need to keep pace.

STRATEGY 11: Turn up the Volume by Expanding SOC Functionality

Once incident response is mature, amp up a SOC's ability to detect and defend against more sophisticated attackers who often hide and quietly move in a constituency.

These additional functions include:

- Looking for the adversary in new ways through threat hunting.
- Testing and enhancing the SOC's ability to detect the adversary through red teaming, purple teaming, and breach and attack simulation.
- Concealing networks and assets, creating uncertainty and confusion, and/or influencing and misdirecting adversary perceptions and decisions through deception.
- Advancing the SOC's knowledge of adversary actions, techniques, and tools through malware and digital forensic analysis.
- Improving SOC operations through the use of tabletop exercises.

Threat hunting is one of the best ways for a SOC to find adversaries that elude ordinary, routine detections and alerting.

Enjoy Learning!
Thank You ☺

Bhaskar Soni