SOC Fundamentals

A SOC is defined primarily by what it does: cyber defense. Adapting the definition from the Committee on National Security Systems (CNSS), cyber defense is "the practice of defense against unauthorized activity within cyberspace, including monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities."

A SOC is a team, primarily composed of cybersecurity specialists, organized to prevent, detect, analyze, respond to, and report on cybersecurity incidents. All SOCs provide services to a set of customers referred to as a constituency which is a bounded set of users, sites, IT/OT assets, cloud assets, data, networks, and organizations. A constituency can be established according to organizational, geographical, political, technical, or contractual demarcations.

For an organization to be considered a SOC, it must:

- Provide a means for constituents to report suspected cybersecurity incidents.
- Provide incident handling assistance to constituents.
- Disseminate incident-related information to constituents and external parties.

Some SOCs will also have the skills and resources to perform more specialized activities, such as detailed forensics on compromised systems. Others, however, must call on partner SOCs or external resources when in-depth forensics must be performed.

SOC Functional Categories and Functional Areas:

- Real-Time Alert Monitoring and Triage. Performing triage and short-turn analysis of potential security incidents generated by near-real-time security alert feeds.

- Incident Reporting Acceptance. Receiving and processing reports of potential security incidents from constituents, other SOCs, and third parties. These reports may come through written (e.g., email) or verbal means.

- Incident Analysis and Investigation. Performing in-depth, detailed analysis of suspected incidents. This includes identifying details such as the origin, extent, and implications of an incident, and characterizing the confidence of these conclusions.

- Containment, Eradication, and Recovery. Performing activities supporting incident/adversary containment, damage management, adversary eviction, and system recovery to reduce current impact and move to a state that will prevent future incidents.

- Incident Coordination. Performing information gathering, information distribution, and notification in support of an ongoing incident. Directing and/or coordinating response in partnership with constituents, incident response stakeholders, other SOCs, and third parties.

- Forensic Artifact Analysis. Examining media samples and digital artifacts (hard drives, files, memory) to draw detailed observations and conclusions about suspected activity, such as content analysis and timeline reconstruction.

• Malware Analysis. Examining suspicious files to understand the provenance, pedigree, functions, and intent of suspected malware samples.

• Cyber Threat Intelligence Collection, Processing, and Fusion. Collecting cyber threat intelligence products, including CTI feeds and reports. Processing and integrating CTI into SOC systems and parsing and filtering information for further consumption by the SOC and its constituency.

• Cyber Threat Intelligence Analysis and Production. Utilizing analytic techniques to track, trend, and correlate adversary behavior over time, and support risk decision making. This includes creating and producing CTI reports describing specific adversaries, their TTPs, and campaigns.

• Cyber Threat Intelligence Sharing and Distribution. Sharing CTI and incident reports with parties outside the SOC, including partners, other SOCs, and the broader cybersecurity community.

• Threat Hunting. Performing proactive operations to identify potentially malicious activity, outside the scope of established SOC alerts, based on hypotheses that the adversary is operating in or against the constituency.

• Sensor and Analytics Tuning. Performing curation, tuning and optimization of detections, analytics, signatures, correlation rules, and response rules deployed on SOC detection and analytics systems, such as EDR, SEIM, and SOAR.

• Custom Analytics and Detection Creation. Using knowledge of adversary TTPs and constituency systems to create detections and analytics to detect and understand various activity in SOC sensors and analytic systems.

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.

Among the data sources a SOC is likely to ingest, the most prominent are host sensors such as endpoint detection and response (EDR) capabilities, network traffic metadata, and various log sources such as application or operating system (OS) logs.

Combined with security audit logs and other data feeds, this data will then be sent to a variety of systems within the SOC such as security information and event management (SIEM) or security orchestration, automation, and response (SOAR) technologies or specialized capabilities for performing functions such as malware analysis.

A typical SOC will collect, analyze, and store anywhere from millions to tens of billions of security events every day. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Events do not necessarily indicate good or bad behavior; they simply are things that happened.

An event is “any observable occurrence in a system and/or network”. In contrast, the term alert is typically used to reference an event that generated with the implication it may be a potential attack.

Intrusion detection systems (IDS) and SIEM systems are typical generators of alerts. An alert is a technical notification that a particular event, or series of events, has occurred.

Alerts will often come in two forms, signature-based and anomaly detections. Signature-based detection is where the system has prior knowledge of how to characterize and therefore detect malicious behavior, such as with an indicator of compromise (IOC) matching. IOCs are forensic artifacts from intrusions that are identified on constituency systems at the host or network level. They are discrete pieces of information, such as IP addresses, hashes/checksums, or malware characteristics. Anomaly detection is where the system characterizes normal or benign behavior and alerts whenever it observes something that falls outside the scope of that behavior.

Both events and alerts are nothing more than data; both must be evaluated within the context of the system(s) they occurred on, the surrounding environment, supported mission, relevant cyber intelligence data, and other sources of data that can confirm or repudiate whether there is any cause for concern.

Just because the SOC receives an alert, that does not necessarily mean something bad happened. It just that a pre-defined set of criteria was met. It takes human analysis, the process of evaluating the meaning of a collection of security-relevant data, to establish whether further action is warranted. This is typically performed with the assistance of specialized tools and automation.

No matter how severe it may seem, a single alert generally does not provide sufficient evidence that an incident occurred. Context can come in many forms. It can include business related information, such as knowing if the constituency should be expecting connections from foreign countries.

Analysts will start with initial indicators (such as a high-priority alert or analytic trigger) and use a combination of automation, rote process, and their own experience to gather additional contextual data. In cybersecurity operations, triage is the process of sorting, categorizing, and prioritizing incoming events and other requests for SOC resources. Confidence in this data can be enhanced and volume lowered through techniques such as filtering, deduplication, alert enrichment, cyber threat intelligence fusion, ML-based prioritization with the SOC's big data analytic platform, SIEM and SOAR.

The threshold at which an event or alert is escalated can be defined according to various types of potential "badness" (type of incident, targeted asset or information, impacted mission, etc.). In such an arrangement, the time span the triage analyst examines each alert is usually measured in minutes; this depends on the SOC's escalation policy, concept of operations (CONOPS), number of analysts, size of the constituency, and alert volume.

There is an enduring need for human analysts to reason about alerting, events and analytics that cannot otherwise be fully automated. Until a SOC analyst has evaluated the disposition of an alert, the SOC cannot be certain there is a confirmed incident or not. Automation assists, but does not fully replace, the judgment of advanced human analysts.

A cyber incident is defined as: "actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein."

Even with all the techniques at their disposal, the SOC cannot always be 100% certain they have the complete picture of what occurred. This is often due to incomplete, inconclusive, or ambiguous data. Given this, the SOC may not always deploy countermeasures at the first sign of an intrusion. The SOC wants to be sure that it is not blocking legitimate activity, for example.

There are cases where a set of indicators is correct often enough that certain response actions can be automated, leading to use of automated response at the asset and network level, or orchestrated through SOAR tools.

High-maturity SOCs typically build several layers of alert correlation, enrichment, and automation on top of alerts generated from such platforms. However, there is always the chance that a positive indicator will turn out to be incorrect. Given this, the decision to automate responses must include the risk calculation of the increase in the speed of the response vs the risk of taking the wrong action.

Historically, SOCs focused their efforts on detecting an incident while the adversary is performing reconnaissance, or during direct attack. By contrast, today the SOC must expand its situational awareness far beyond this focus. Indeed, in an ideal circumstance, the SOC will be part of a larger cybersecurity effort that understands the adversary well enough so that they can prevent or mitigate attacks before they occur, or at least detect an incident before significant damage is done.

Continually feeding timely CTI into SOC monitoring tools is key to keeping up with adversaries. In a given week, the SOC likely will process dozens of pieces of CTI that can drive anything from sensor detection updates to emergency patch pushes. A SOC must discriminate among the data that it harvests; CTI must be actionable, timely, relevant, and accurate about the incident, vulnerability, or threat it describes.

The SOC strives to detect and respond to adversaries, not just when they deliver their attack to a target, but also “left of hack” and “right of hack.” Left of hack includes actions the adversary performs prior to trying to get into the environment. These actions help an adversary prepare for an attack and potentially increase their chances of success. Examples include searching for information on a potential victim, developing technical capabilities such as malware, and active scanning of targeted victim environments. These left of hack actions can be more difficult to observe but are critical to a proactive defense. Right of hack includes all the actions an adversary might take after they have a foothold. This may include trying to gain additional access, collecting data and exfiltrating it, or taking actions to create an impact such as destroying information.

Some SOCs also allocate resources to look for all the unstructured indicators of incidents in addition to the routine detections and alerting that are processed every day. This is usually referred to as threat hunting–starting with different hypotheses of adversary presence in the constituency and using various analytical techniques to prove or disprove that hypothesis. A mature, structured hunt program builds on, and further enhances its CTI, routine alert handling, and response functions.

The best SOCs stand out in a number of ways, but a high operations (ops) tempo is one of the most prominent. Specifically, it is the SOC’s ability to both comprehend its constituency, and act in timescales relevant to the timescales of the adversary that will set it apart. Both require skill and sophistication in analytic tooling and tradecraft, and the right people and processes to act decisively. The key to effective security operations is having the people, process, and technology to enable the SOC to detect, understand, and respond to the adversary rapidly, both proactively and reactively.

Strategy 1: Know What You Are Protecting and Why

Very few businesses, government agencies, or private sector organizations have cybersecurity operations as their primary business function. Even for those that do, such as a company that offers security services like a Managed Security Services Provider (MSSP), the protection of their own systems and data is not their core mission.

Instead, cybersecurity operations must serve as mission enablers supporting the goals of their constituency. For the SOC, that means having the needed context for the data that it sees and the actions it takes. This is especially true given that most SOCs receive more data than they can possibly act upon and will need to prioritize their decision making.

The general definition of situational awareness can be extended to cyberspace: "Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future" For the SOC, gaining and using situational awareness follows the observe, orient, decide, and act loop (OODA Loop). The OODA Loop is a self-reinforcing situational awareness decision cycle.

Whether the analyst realizes it or not, they follow the OODA loop while carrying out various elements of the SOC mission, from the tactical to the strategic: when performing alert analysis, during hunting, and while assessing the impact of a vulnerability incident.

SOC Operating Context:

- Business/mission: This area is focused on understanding a constituency's reason for being and how it operates. This includes the products and/or services offered and primary customers.

- 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.

- Users, user behaviors, and service interactions: This area includes understanding typical patterns of behavior, including user to service and service to service interactions. The focus is on understanding normal behavior and then looking for deviations from that baseline.

- Threat: This includes understanding the various types of threats (hacktivists, criminal, nation state, etc.) likely to be of particular concern to the constituency, how they operate, and how that should affect the constituency's defensive posture.

Having mature cyber situational awareness allows the cyber defender to answer questions like: • What is our security posture? • What are the consequences of a successful attack, including the consequences for upstream or downstream services? • From which adversaries is the constituency facing imminent threat of attack? • How are they attacking us and what are they after? • What is our best course of action in

response to these attacks? • What is the patch status of the constituency? Which patches need to be prioritized? • To which systems should I apply a given set of security controls, thereby rendering the best mitigation? • What is changing about the threats faced by the constituency? • Who is acting outside their typical lines of behavior, and is this cause for concern?

The SOC should be able to put any cyber event it observes into constituency context so that it can effectively prioritize its actions. However, as vital as situational awareness is, SOCs have long struggled to achieve this understanding and context and to encode it in a way that is both durable and not siloed to specific individuals in the SOC.

Understanding the constituency mission means knowing what functions need high confidentiality, integrity, or availability, even during a cyber attack. Understanding the mission means knowing if the SOC is primarily trying to protect against the theft of intellectual property, support secure financial transactions, enable commerce, or something else.

When it comes to understanding what the SOC is protecting, systems and data are often the first thing that come to mind. Ideally the SOC will have access to robust information about:

- Location of constituency digital assets:
  - The geographic footprint of the IT and OT environment.
  - Number, type, location, and network connectivity of IT and OT assets, including laptops, servers, network devices, mobile devices, and internet of things (IoT) devices.
  - Network topology, including physical and logical connectivity, boundaries that separate differing zones of trust, and external connections
  - Asset, network, and application architecture (including authentication, access control, and audit)
  - Where data is stored relative to system assets such as in a closed network, in the cloud, or on mobile devices

- The relative importance of constituency digital assets:
  - The most important types of data and where are they located and processed
  - What systems perform essential functions for the constituency and what data requires high confidentiality, integrity, and/or availability

- The state of constituency digital assets:
  - What normal state looks like across major network segments and hosts
  - Changes in that state, such as changes in configuration, host behavior, ports and protocols, and traffic volume
  - The vulnerability of hosts and applications, and countermeasures that mitigate those vulnerabilities

The SOC's mission, and that of the larger cybersecurity apparatus, can be greatly enabled by an accurate, comprehensive, and current accounting of the constituency's cyber assets: on-prem, cloud, mobile, and so forth. This is essential to any sort of activity where the security org wishes to drive cybersecurity hygiene and compliance in a consistent and scalable manner.

In a large enterprise, the SOC is likely to leverage several sources of asset data: • Machine and user directory services such as Lightweight Directory Access Protocol (LDAP) and Windows Active Directory • Dynamic Host Configuration Protocol (DHCP) logs and lease databases • Inventory databases owned and operated by parties outside the SOC • Cloud resource/asset inventory • Mobile device management

(MDM) and EDR • Network scanners and mapping • Vulnerability scanners • Security correlation and analytic platforms that automatically generate asset lists • System management, patch management and software distribution

Aggregating and evolving a picture of digital assets can be one of the most daunting of endeavors for the SOC or the larger cybersecurity organization. However, it serves as the foundation for so much of what the SOC does, and for those who do it well, it serves as the foundation of almost every cybersecurity function performed.

Things that the SOC will want to be aware of:

- The meaning of activity on constituency networks and hosts in the context of the mission
- The role, importance, and public profile of major user groups, such as:
  - System administrators
  - Executives and their administrative staff
  - Those with access to sensitive information (intellectual property, finance)
  - General constituency user population
  - Users external to the constituency
- Baseline metrics for how systems and data, particularly critical ones, are accessed by users over time
- Inter-organizational and Inter-business zones of trust and trust dependencies

Developing a baseline of user behavior can be done through user entity behavior analytics (UEBA). This can be as straightforward as looking at access logs for suspicious connections to utilizing advance machine learning algorithms to identify unexpected activity. Common areas to focus on include tracking administrator access and behaviors, monitoring file shares, and monitoring access and use of critical systems. UEBA tracks not only user activity but communications between and among servers, routers, endpoints, and IoT devices.

Understanding the SOCs operating context would not be complete without understanding the threat to the constituency. If there was not a threat the SOC would not need to exist! To help contextualize the threats to the constituency the SOC will want to be aware of:

- What about the constituency might be of interest to an adversary: the adversary might be interested in something very targeted such as specific intellectual property or financial information.

- What are the types or groups of adversaries likely to target the constituency: Understanding if the constituency is more likely to be targeted by random hackers, hacktivists, criminals, or APTs can help the SOC bring in the right cyber threat intelligence to inform cyber defense practices.

- What historical cyber incidents have happened within the constituency: Understanding both the type of systems and data targeted and the impact and consequences of previous incidents can help the SOC prioritize efforts.

The SOC does not have to develop awareness in all the operational context areas on its own, or all at once. Senior management, legal, and IT operations will all have an important role to play in helping the SOC gain awareness. The SOC should prioritize gaining insights on mission critical systems and data and then iterate over time to add to their knowledge.

Strategy 5: Prioritize Incident Response

NIST defines a cyber incident as, “Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein”. In other words, anything the incident responders take action to determine, find, or analyze falls into the scope of incident handling.

Building on the CERT/CC list of activities included in incident handling, these activities may include: • Conducting log review and forensics to identify scope, depth, and source of intruder activity • Working with system, network, device and cloud resource owners and users to assess alerts and logs in context • Altering security controls to contain or eradicate an adversary • Filtering web, network, or other incident-related traffic • Resetting passwords, certificates, and other service principles • Applying relevant advisory and alert solutions

The SOC will be prepared for most response efforts if it has the following in place: • A workforce with strong technical, analytic, and communication skills • CONOPS, SOPs, and escalation procedures that guide the SOC’s actions • Means to coordinate analysis and response activity among members of the SOC • Established POCs with whom to coordinate response actions • Established and ad hoc artifact collection and analysis tools sufficient to establish the facts about incidents • The authorities to enact swift and decisive response actions when called for

What to include in an incident response plan: • Roles and responsibilities: Who is in charge of the incident and who is performing the IR. • Communications, coordination, and contacts: Who needs to be informed, coordinated with, and when and how • References and procedures: SOPs, reporting guidelines, policies, and other documentation. • A summary of the tools, technologies, and physical resources: Including what the SOC has and how to access them. • A list of critical network and data recovery processes: Including step by step plans.

Large and mature SOCs build up sizeable incident handling guidance codified as a “living” set of SOPs or playbooks staff are expected to know and routinely access. The purpose of these is to establish a) clear expectations for staff and b) repeatability in handling of most incidents.

Well defined SOPs and playbooks are also a key factor in being able to incorporate automation activities into the SOC. Without clear guidance on what actions need to be taken in what scenario automation tools cannot be programmed to take the appropriate actions.

A playbook is likely to include the following: • Title •Intent • Scope/who it applies to • Stimulating conditions, meaning under what circumstances it should be used • Procedures, steps, and expectations to be followed.

There has to be a balance of capturing enough detail so that less experienced cyber responders will understand how to respond to an incident and more experienced responders are consistent in approach. Too much and specific detail, and the playbook becomes obsolete quickly, and may stifle analysts’ ability to act on their own intuition and adapt to the incident at hand.

A cornerstone of effective playbooks are checklists. Checklists can be adopted and assimilated from various places and are useful for all responders, from inexperienced to expert. A good place to start developing checklists and ultimately SOPs and playbooks is to examine various types of playbooks available, and tailor and adapt good practices from them.

Initial incident reports can come into the SOC from e-mail, phone calls, IT service desk ticketing, partner organizations, and alerts from the SOC's own tools, among others. Cyber defenders then triage these incoming signals or make an initial determination on what the next steps are.

Some tips for triaging incidents include:

• Choose categories of incidents based on response: For example, successful cross-site scripting (XSS) and Structured Query Language (SQL) injection attack responses likely differ from a malware infection clean-up which is different from a DoS attack.

• Establish guidelines for triage: Ensure analysts do not spend "too long" analyzing one incoming alert, while others grow stale. Oftentimes, a SOC will apply time boxes for initial triage, to ensure all incoming alerts are handled in a timely manner. One way to help support this is to have a pooled set of users responsible for triage, with backups in place to share load.

For incident analysis, the following techniques can aid in ensuring the right conclusions are derived from the data:

• Check the assumptions: Ensure anyone participating in the analysis is aware and careful of making assumptions. Be wary of filling in gaps that satisfy a hypothesis, for example, without the data that confirms the activity.

• Seek more data: If there are apparent gaps in the activity that present barriers to conclusions, seek data that will augment the analysis. This may include identifying data sources that might be outside of the SOC purview.

• Analyze indicators: The most common technique of SOCs is to examine all observable pieces of information, including malware hashes, hardcoded/reused adversary passwords, IP addresses (with caution), web traffic, NetFlow, etc. to piece together the TTPs of what happened, when dealing with human adversaries.

• Create timelines of events: A sequence of dates and time when adversary activity occur provide insight into how long an adversary stays in one account/system/network, what occurred first, and can give investigators ideas on when an intruder moved from one network to another.

• Do not rely solely on IOCs: Discrete indicators of compromise, such as IP addresses or file hashes/checksums are easy for an adversary to change. IOCs are important and useful in an initial incident investigation to provide hints and determine where and what to search for but it is important to look beyond them.

• Be aware of bias: Once investigators have some experience with incidents, one incident might look very much like another in the data. It is important to treat each incident as a new one, and correlate them with other incidents only with hard, indisputable facts.

Most incidents are not detected at the initial entry point. Most SOCs find attacks “right of hack,” or after the successful initial entry. Example incident activities to look for include upgrading or escalating privileges, moving laterally across user accounts, or downloading exploits or tools.

The best data for confirming incidents originate from end hosts or systems and other user account data. While network data is commonly used and is a great starting point and useful to assist in pinpointing likely hosts, confirming malicious activity and finding details are better coming from affected host data.

Examples of considerations for investigation include: • File system and files: Unexpected files the user did not create or new hidden directories • Running processes: Unexpected or hidden processes or those do not perform as usual • Scripts, executables: Mysterious or unaccounted for programs and apps • File checksums and signing certificates: System file hashes that do not match expected hash or signing certificate that do not match the correct certificate authority • System logs: Unexpected user accounts, privilege changes, trusted hosts • Network, VPN activity: Unusual network (current and recent), VPN, tunneling, and other communication connections, including RDP, SSH, and other connections that could signify a backdoor

Part of the analysis process is determining the nature of the alert while understanding reasons the alerts may not be telling the full story. Each alert that detection tools generate falls into one of four categories:

- True positive: Something bad happened, and the system caught it.
- False positive: The system alerts, but the activity was not actually malicious.
- False negative: Something bad happened, but the system did not catch it.
- True negative: The activity is benign, and no alert has been generated.

False positives outnumber true positives in most detection systems. Continual tuning, strong context enrichment, and automation are critical to understand effectively and efficiently what is truly of value.

Before acting, incident responders investigate the situation to determine about what action is truly required. Routine incidents are usually straightforward, requiring little analysis, whereas a potential breach that starts with a subtle anomaly, such as an unexpected log in time, requires more.

Talk to Users, Service Owners, and System Admins. Users are familiar with their account activity. One of the best sources for identifying potential breach incidents, which are often subtle, is the user community. Users are familiar with their file structures, with their profiles, and their activity or non-activity, and may notice when something is not as they left it.

Put it in context. Determine what the observed activity means in the context of the service and any other events. What are the factors around the activity? Are there other activities and is there a sequence or timeline that can be formed?

Avoid premature conclusions and assumptions: It takes a skilled analyst to correctly interpret what a set of security logs, network data, or media artifacts convey. It is better to err on the side of conservative judgment, pending more data, then to jump to a conclusion that is incorrect, which can cost valuable time, money, and political capital.

Do not focus on attribution, but do consider adversary association. It can be helpful to associate current activity with previous activity or adversarial groups as this may give defenders additional context for understanding and investigating an incident. However, creating connections too quickly and without sufficient evidence can lead to incorrect hypothesis that harm the investigative process.

When the SOC explains an incident to stakeholders and upper management, the bottom line is not about bits and bytes, it is about mission, dollars, and, sometimes, lives. The SOC must translate technical jargon into business language. There are four questions that should be answered: (1) what (or who) was targeted? (2) was the adversary successful? (3) who is the adversary and what is their motivation? and (4) how to continue the mission?

Determining when to respond (to stop the exfiltration or damage being inflicted) vs. gathering more intelligence (to understand what the adversary is interested in) is a judgment of trade-offs. There is a natural tension between watching adversary activities to understand what is next and taking action to stop them from further damage.

Post incident response or post incident review (PIR), also known as after-action review (AAR), involves capturing and reviewing the lessons learned and action analysis for future incidents. Spending quality time on PIRs improves the SOCs response capabilities, as well as other areas such as detection.

Strategy 6: Illuminate Adversaries with Cyber Threat Intelligence

Cyber Threat Intelligence provides actionable knowledge and insight regarding adversaries and their malicious behaviors. In SOC environments, CTI can augment defenses by informing the following:

- Identifying unwanted actors in networks
- Tuning sensors and analytic systems/frameworks for better monitoring
- Prioritizing resources
- Providing context to incidents
- Anticipating adversary activities in more advanced SOCs
- Preventing or slowing down imminent attacks

Cyber Threat Intelligence refers to the collection, processing, organizing, and interpreting of data into actionable information or products that relate to capabilities, opportunities, actions, and intent of adversaries in the cyber domain.

To decide what cyber threat intelligence to use, consider the following criteria for evaluation:

- Actionable: Can the SOC do something constructive with the information, such as correlate with other data, create threat hunting scenarios or actions, or enact preventative protections? Is the CTI specific enough for the SOC to operationalize? Does it come in a format that is consumable and enrich a decision, while not complicating it?
- Timely: Are events recent (in days, hours, minutes for streams, or weeks for analysis)? Are there stale data?
- Relevant: Does it apply to the organization and reveal unknown and possible threats? Does it come from a reputable source? Is the data volume manageable? How is the CTI ingested or analyzed? Are there application program interfaces (APIs) for feeds and platforms?
- Accurate: Does the content correctly describe what happened? Did the CTI include spurious or wrong data about the original attack?

Tactical CTI comprises the contextual specifics about attacker methods and operations, as well as TTPs. It is the most common CTI in SOC environments and is used in writing, tuning and refining detections and analytics. Effective tactical intelligence is actionable and is used to develop defenses that are comprehensive for classes of attacks, rather than specific to indicators such as IP addresses or malware hashes.

The context of events provides a basic understanding of who is targeting a constituency, why, and what could happen as a result. Analysis helps to understand what has already happened and what is happening now. Action answers critical questions related to where and how something is happening and what can be done about it.

A common element to cyber analysis is that it usually consists of tracing activity from various sources and systems across various moves and sequencing events over time. Some of the activities my include:

- Discovery of new IOCs and TTPs, developed through a combination of digital artifact examination, static code analysis and reverse engineering, runtime malware execution, and simulation techniques.
- Mapping and analysis of adversary TTPs, to understand adversary activity of existing and potential threats to the constituency, as well as developing familiarity with sophisticated adversaries or criminal activity from reporting.
- Trending and reporting on activity and incidents attributed to more advanced threats to include sophisticated adversary activity or criminals.
- Tracking the evolution of adversaries and campaigns over time.
- Fusing and correlating locally derived and externally sourced cyber threat intelligence into signatures, techniques, and analytics intended to detect and track adversaries in coordination with other analysts in the SOC.
- Operating and populating threat knowledge management repositories, allowing SOC analysts to connect disparate but related adversary activity, incidents, indicators, and artifacts.

Above all, it is important to realize that context and specificity to the business or mission, the intellectual property, and the environment are key to getting good at analyzing present adversaries and moving toward anticipation.

The SOC's defensive strategies can be greatly improved by focusing on who is targeting the organization and why. The more the SOC evolves adversary understanding, the better it is positioned to anticipate what the adversary might do.

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. Adversary association is less rigorous than full attribution yet is useful for adversary anticipation and is good enough for SOC work in most cases.

Adversary association includes linking adversaries to likely attributes, such as IOCs, behaviors, and TTPs across the kill chain, which can then provide clues about what else the adversary has done and start to identify why. Patterns of behavior such as frequency, tools, targets, locations, and sectors can be identified to assist in anticipating adversaries' movements.

Some best practices in use of CTI include the following:

- Have a good feedback loop: Is the CTI actionable such that it can be integrated into the various SOC tools? Is it yielding useful results to the SOC team?
- Quality control: If the data is inaccurate, feedback should be used to adjust the SOC reliance.
- Define and maintain standards for attribution/association: Attribution is difficult, adversary association is more attainable: know ahead of time what is "good enough" for the SOC.

Cyber threat reports put context around the incident artifacts and data. They discuss information about attempted or successful intrusion activity, threats, vulnerabilities, or adversary TTPs, often including specific attack indicators and vectors.

Cyber Threat Analyst Artifacts:

- Cyber threat intelligence reports can range from monthly to annual and often summarize cyber threat activities for the constituency, specific enterprise, or for a business sector
- Formal incident write-ups: Particularly notable incidents may deserve formal documentation or presentation outside the scope of what is captured in the case management tool.
- Adversary trends: Cyber threat analysts are tracking the bigger picture of adversaries and incidents across an enterprise, and therefore are in the position to conduct trend analysis, pattern recognition, and make associations across activities that responders may miss.
- Indicator lists: Analysts aggregate, correlate, and associate various indicators of compromise (suspicious IP addresses, domains, email addresses, etc.) from external cyber threat intel reporting and its own malware reverse engineering. These indicator lists are primarily used to generate signatures and other detection content in the SOC's tool set.
- Sensor and analytics enhancements: CTI analysts will frequently write or enhance SOC detections and analytics themselves or pass off technical details to a team member to create them.

The point of CTI is to look beyond exact signatures, hashes, IP addresses, or other static and easily changed characteristics of an adversary's actions. If too much CTI is streaming into the SOC, there may not be enough analyst time to review and process the information, and it may introduce more "noise" than assistance to SOC analysts. CTI should provide clarity, not just more traffic. The SOC should shape its CTI ingest and focus around those relevant to its constituency.

Strategy 7: Select and Collect the Right Data

Gaining visibility into cyber activities requires thinking strategically about the data and feeds that best render a complete picture of those activities. This strategy focuses on the sensor and log data collected by network and host systems, cloud resources, applications, and sensors, wherever they may reside. The goal of this strategy is to gather the right data in the right amounts from the right places in the enterprise, with an economy of effort and expense.

Common Security-Relevant Data Sources:

- Host-based activity. Fields of interest: Process name, file name, action taken (allow/block)
- File integrity: Fields of interest: File name, hash.
- Anti-Malware: Fields of interest: File name, virus name, user name, action taken.
- Data-loss prevention. Fields of interest: User name, removable storage ID, device used.
- User activity monitoring. Fields of interest: User name, file name, process name, action taken.
- Network traffic: Source and destination IPs, ports, bytes, urls.

There are two classic approaches that SOCs may take in selecting and tuning data sources: tune up from zero or tune down from everything. This section also includes a third, somewhat orthogonal approach: leverage data in place. No matter which of the tuning approaches is taken, one of the first things to do is to tune out any data that is known to have a lower value.

Table 14. Approaches to Tuning Data Sources

Approach	Pros	Cons
Start with the entirety of a given data feed and tune down to a manageable data volume that meets common needs.	• Requires little foreknowledge of the data being gathered. • Easiest to implement. • Enables SIEM tools to leverage full scope of data features and event types offered.	• May overwhelm tools and analysts if data feed is too voluminous. • If methodology is used for many data feeds, poses exponential risk of "data overload." • "Default open" filtering policy toward data collection may pos long-term risk to data aggregation systems as feeds change over time.
Start with a candidate data feed, and tune up from zero, focusing only on what is deemed useful or important.	• Keeps data volume low. • Focuses systems and analysts only on what is deemed to be of interest. • Less problematic for SOCs with limited budgets.	• Carried to its extreme, limits value given time/ effort granting SOC access to given data feed. • Analysts blind to features of data feeds not explicitly set for input into data collection systems. • Approach may require more labor to implement.

An important point: Do not log just the "denies"; the "allows" are often more important. Failure events include users typing in the wrong password or being blocked from visiting a website. Failures mean a security control did its job: it stopped someone or something from doing what it should not do, which is usually a good thing. Successes, such as file modification granted, file transfer completed, and database table insert, are often where the SOC is most interested when performing investigation and analysis.

An “allow” is either a legitimate transaction, or it is an attacker or unwanted activity that got past some access controls. Consider situations in which “allows” are often more important than “denies” such as malware beaconing, RATs, data exfiltration, and insider threat. With only failure attempts logged, the SOC will not understand what happened. Failure, block, and deny events are frequently an analytic dead end. Successes events are necessary for both investigation and correlation.

Constituency systems and services are constantly being installed, upgraded, migrated, rebooted, reconfigured, and decommissioned; with cloud computing, this rate of change tends to be even more pronounced. These changes frequently present blind spots in monitoring coverage. One of the most important aspects of monitoring the enterprise is: Sensors and log feeds require their own routine monitoring to ensure they are performing as expected.

Check data feed status daily or every shift. Just because an agent is green does not mean the data feed is online. It may just mean the agent software has not crashed. Consider performing regular checks against feeds from high-value targets to ensure no interruptions.

Many SOC sensing technologies follow a similar basic pattern at their core:
• Knowledge of the environment and the threat is used to formulate detection policies and mathematical models that define known good, known bad, normal, or abnormal behavior.
• Feedback from the events generated will inform further tweaks to the detection policy, known as tuning.

There are two classical approaches to intrusion detection:
• Misuse or signature-based detection: Where the system has a priori knowledge of how to characterize and therefore detect malicious behavior, such as with IOC matching.
• Anomaly detection: Where the system characterizes what normal or benign behavior looks like and alerts whenever it observes something that falls outside the scope of that behavior.

Each of these approaches have pros and cons. In practice, finding tools that rely exclusively on one approach or the other is rare; most modern monitoring and detection products integrate both techniques.

Advantages and Disadvantages of Intrusion Detection Elements:

Behavior-based detection can detect previously unknown attacks and misuse within a session, prior to a specific attack being publicly known (e.g., with “zero days”). Disadvantages: • They are complex and prone to false positives. • They may require longer ramp-up times to learn baseline system behavior. • Networks or systems with frequent changes and activity surges may be difficult to profile.

Signature-based detection is fast and sometimes has a lower false-positive rate than behavior-based detection. It can find known attacks immediately. Disadvantages: • They can only alert on known attacks. • If signatures are not updated, new types of attacks will most likely be missed. • They may be especially prone to circumvention by content obfuscation or protocol encryption.

A **network sensor** can monitor a large range of systems for each deployed sensor and is invisible to users. Disadvantages: • A network sensor can miss traffic and is prone to being attacked or bypassed. • A network sensor often cannot determine the success or failure of an attack. • In absence of SSL/TLS “break and inspect” decryption, network sensors cannot examine encrypted traffic.

A **host sensor** will not miss attack traffic directed at a system due to packet loss or encrypted obfuscated traffic, assuming the detection is based on locally observed host behavior. A host sensor can help determine the success or failure of an attack and it can identify misuse by a legitimate user. Disadvantages: Host monitoring software could be disabled or circumvented by a skilled attacker using rootkits.

Intrusion Prevention (IPS) can prevent or reduce damage by a quick response to a threat or attack. Disadvantages: IPS require careful tuning in order not to block or slow legitimate traffic or host activity.

Passive Intrusion Detection (IDS) react by sending alerts or alarms; they have comparatively less risk to deploy. Disadvantages: requires operator intervention for all alerts.

With the expansion and maturation of host-based monitoring, along with the proliferation of network traffic encryption, emphasis has shifted to host-based instrumentation and prevention. In general, if you are trying to positively confirm an attacker was successful in hacking an account, generally data retrieved from end point sources, such as EDR, will be more effective than network traffic sources such as NetFlow.

In contrast, network traffic can be better than EDR at providing hints such as “where else do I have a problem” and “which end nodes to I look at first” in a situation where EDR coverage is incomplete. Data from an endpoint is generally more informative than network traffic data for confirmation of intrusion.

Host Observables:

- From mounted file systems and any other storage:
  - OS version, installed service pack(s), and patch level
  - Installed applications
  - Resident files, modification times, ownership, security permissions
  - Browser history, cache, cookies, and settings

- From system memory and processor(s):
  - Application process identification number (PID), creation time, parent (spawning) process
  - Executable path, execution syntax with arguments
  - User whose privileges it is running under
  - RAM contents and memory map

- From attached devices and system input/output (I/O):
  - Content of network traffic
  - Actions from input devices including keyboard and mice
  - Connected devices, potentially including details such as device type, driver info, serial number

To paint a complete picture of what is happening on the host, SOC analysts frequently examine all three described elements (on disk, in memory, and attached device I/O). For instance, focusing on just the local file system will blind an analyst to malware operating exclusively in memory.

Techniques leveraging a hardware-based root of trust, such as with trusted platform module (TPM) and trusted boot help ensure both the OS and other components match expected code. Gatekeeper

in macOS and AppLocker in Windows can be used to limit which users use what programs, and with which permissions. For Windows, a more extreme security control of application allow listing component is CodeIntegrity.

Generally, application allow listing and deny listing are most successful for high-risk users that have a finite software baseline and/or stick to software from a known set of publishers or app stores without much divergence.

Tripwire is used on end hosts to detect changes to key configuration files and can alert on changes that may be an indicator of malware or a malicious user. Changes that are detected in monitored files and settings can be detected and reversed by the administrator.

For many constituencies, there is significant concern about the exfiltration of sensitive data from the enterprise. No matter how implemented, the host is often the only place where the SOC can expect to clearly see this activity (e.g., through network traffic, clipboard, file copy, print activity and system call observables).

Alternatively, some adversary engagement and deception products can leverage techniques like honeytokens, or bogus records, datasets, or other data of no value, are often set to entice intruders. When altered or exfiltrated, alerts are sent to the SOC.

Network-based monitoring technologies can sometimes be the most cost-efficient and simplest means by which SOCs can gain visibility and attack detection coverage for a given enclave or network, especially in cases where they have no other visibility.

Attacks detected by NIDS, NIPS, such as exploits executed across the network (most notably remotely exploitable buffer overflows), no longer comprise the majority of initial attack vectors. Client-side attacks, such as phishing, have long become far more prevalent, giving way to the content detonation and analysis devices. Further compounding this, many cloud-based services consumed by many enterprises do not support the deployment of traditional NIDS/NIPS due to their network topology.

There is a high false-positive rate associated with IDS technology; NIPS administrators are justifiably cautious. Consider that each false alarm results in blocked traffic. If not careful, the NIPS administrator can inflict a very serious DoS. As a result, many SOCs will be careful about which NIPS signatures they turn to block, doing so only after several days or weeks of use in alert-only mode.

Like any other detection technology, a good NIDS/NIPS will provide rich contextual data to the analyst or operator. Having access to raw signatures is highly desirable, as this, married with full session PCAP, gives the user clarity on why an alert fired, and how prone that detection is to false positives.

Whereas some sensors examine entire contents of network traffic, it can also be useful for the SOC to have a capability that succinctly summarizes all network traffic. One data source complementary to sensor alerts are NetFlow records.

NetFlow record collection and analysis is regarded as an efficient way to understand what is going on across networks of all shapes and sizes. It is critical to understand that NetFlow records do not generally contain the content of network traffic above OSI layer 4. By combining flow records,

knowledge about the constituency, and NetFlow analysis tools, an experienced SOC analyst can find a variety of potential intrusions without any other source of data.

When analyzing a serious incident such as one that requires active response or legal action, the SOC requires concrete proof of what happened. This confirmation comes from host data. Having a complete record of network traffic can also be helpful, especially when host telemetry is not available or untrustworthy.

Malicious files will usually behave in suspicious ways like making privileged system calls, beaconing out for command and control, or downloading additional malicious packages. Malware detonation systems look for this sort of activity, but generally without sole reliance on signatures that define a specific attack or vulnerability. As a result, they are better tuned to ongoing detection of zero-days and specially crafted malware. While the attack vectors may change, the outcome does not, and that is the focus of detonation.

Generally, on-prem content detonation systems come in two varieties:
• Offline: The first type accepts file uploads by users in an "offline" manner. This capability can automate several hours of manually intensive malware reverse engineering. Best-of-breed products will provide specifics on system calls, network connections made, and files dropped.
• Real time: The second type is a device that can scan network traffic (usually Web or email) in real time, pull out malicious files, and detonate them fast enough to block the malicious content from reaching the victim user or system.

An enterprise's Internet-facing gateways are typically a first choice for sensor placement. This sensor placement at these locations meets most of the goals discussed: (1) mission-critical systems usually connect through it, (2) a large proportion of the entire enterprise's traffic passes through, (3) systems on the other side of gateways are untrusted, and (4) it is expected that many enterprise systems will expose various vulnerable services through it.

Zero trust, or the practice of not trusting users or endpoints, regardless of whether they are inside or outside the enterprise (gateway perimeter), consists of reauthenticating at various points. There are different ways of configuring zero trust, and typically, micro segmentation is used. Micro segmentation is breaking up networks into smaller zones to control more granularly what is secured in applications and user access.

In summary, the SOC should consider the following when choosing where to place sensors, and which log feeds to gather:
• What is the mission of the systems being considered for monitoring and what is its criticality (monetary, lives, etc.)?
• How much trust is placed in users of the system(s) and hosted services?
• What is the assessed or perceived level of integrity, confidentiality, or availability of the system(s), data, and services?
• What is the perceived and assessed threat environment? How exposed are systems to likely adversaries?
• Are the systems (or their audit data) under legal, regulatory, or statutory scrutiny, outside of those directly related to the SOC?
• Where in the architecture do assets sit?

Strategy 8: Leverage Tools to Support Analyst Workflow

It seems like every new set of technology promises centralization and a "single pane of glass" for SOCs. However, experience tells us this is rarely the reality. Rather, reducing the number of panes of glass, and providing integration between them is the best strategy with an emphasis on automation and integration for repeated tasks, escalation, and incident handling.

When an analyst starts their workday, they will typically start in one of three places:

- Incoming fresh alert triage in the SIEM or EDR tool
- New threat intel and news found in the intel/indicator management platform
- New or updated cases in the case and workflow management platform

From there, they will have several options on what to do next:

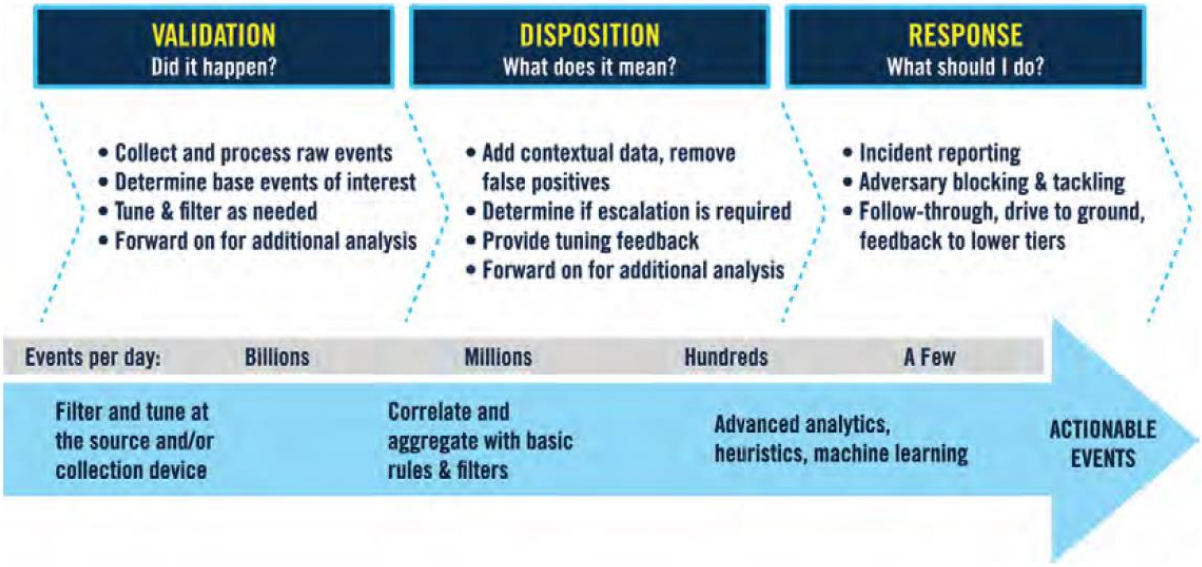
- The analyst can pivot based on entity to drill down in EDR platform, looking at detailed process execution trees and file changes on the end host
- The analyst can pivot to network metadata capture to see what is known about that hosts' communications
- Using either, the analyst may take information about processes or files and look them up in the threat intel management platform
- If available, a file captured from the host or unencrypted traffic can be moved to a malware detonation chamber to see if the file is malicious
- Queries can be executed using analytic notebooks, executing various predefined, curated queries in a couple minutes
- Information on involved users and hosts may be retrieved from asset and entity knowledgebases;
- Finally, the analyst can record this information captured in a case management tool for further action

SIEM collects, aggregates, filters, stores, triages, correlates, and displays security-relevant data, supporting both real-time and historical review and analysis. The purpose of SIEM is to enable the analyst to turn information collected by the SOC into knowledge that can be acted upon in a timely fashion. Modern best-of-breed SIEMs can support many compelling use cases:

- APT detection: Including piecing together disparate data indicating lateral movement, remote access, command and control, and data exfiltration
- Incident analysis and log forensics: Including retention and investigation of historical log data
- Workflow and escalation: Tracking an event and incident from cradle to grave, including ticketing/case management, prioritization, and resolution
- CTI fusion: Integration of tippers and signatures from CTI feeds
- Trending and threat hunting: For analysis of long-term patterns and changes in system or network behavior
- Perimeter network monitoring: Classic monitoring of the constituency for malware and external threats
- Insider threat and audit: Data collection and correlation that allow for detection and monitoring for profiles of suspicious internal threat activity
- Configuration monitoring: Alerting on changes to the configuration of enterprise servers and systems, from password changes to critical Windows registry modifications
- Cyber Situational Awareness: Enterprise-wide understanding of threat posture

Some SOCs struggle to realize the value proposition of SIEM, in large part due to their complexity, as effective correlation rule writing and upkeep can be resource-consuming.

From left to right in the diagram, the event lifecycle "inverted funnel" goes from billions of events to a handful of potential cases. In this process, SIEM moves from automation on the left, through correlation and triage, to workflow support and enabling features such as event drill-down, case management, and event escalation on the right.



The SIEM will generally support two or three approaches to analytics and detections:

- A near-real-time alerting and correlation engine: Supports alerting on single event matches (known as atomic rules) and sets of events, potentially utilizing a state machine (e.g., "true" multi-event correlation)
- An analytic engine that executes analytics against data persistent on disk: Sometimes referred to as "query on a timer" that executes on a schedule defined in each analytic
- A machine learning (ML) engine: For more advanced SIEMs (and SOCs), the ML engine can run on data in-memory as it streams in and/or against data persisted on disk.

The perennial challenge for SIEM owners is in the months and years after initial acquisition. Any analytic platform, SIEM or otherwise, is a long-term investment, and many have opined at these challenges. Custom analytic creation and post-installation tuning enables the SIEM, and thus the SOC, to reach maximum effectiveness. A SIEM, SOAR, UEBA or big data platform without custom content, use case, workflow, and other tuning, usually offer little value to its users; this is where most such installs go wrong.

The star of the SIEM show is the content crafted by its users. That includes detections, analytics, reports, dashboards, queries, notebooks, and the like. The SOC should dedicate resources to not only creating this content but managing it. That typically manifests as a routine cadence for content review and vetting, along with one or more analysts designated as "content managers."

It is necessary for the SOC to designate analysts or leads to ensuring cases and alerts are driven to closure in a timely and orderly fashion, and they are not left in an untidy, orphaned, incomplete, or lost state.

The initial setup of an on-prem SIEM is largely straightforward and can usually be accomplished in a day or two; cloud-based SIEMs are deployed in minutes. In a few weeks, the first few data feeds can be hooked up and tuned, with content created that provides quick wins. However, outfitting the system with the right data, tuning it, writing content for the constituency, training users, and integrating it into operations can take several months. Out-of-the-box content serves as a good start for most SOCs, but the best content is customized for the constituency.

The SOC has a handful of prominent requirements and use cases for case management that should be considered:

- Allows consistent and complete information capture across incidents for each state of the incident life cycle—alert triage, in-depth analysis, response, closure, and reporting
- Can record both structured information from analysts (incident category, time reported), semi-structured data (impacted users, impacted systems) and unstructured information (analyst narrative), along with time-stamped notes
- Supports trending, metrics, and feedback: Including mean/median time to acknowledge, respond, eradicate, and close; and as a feedback loop to inform detections and analytics tuning.
- Allows analysts to capture information about specific entities (particularly users and hosts) that can be referenced and correlated with other cases, thereby providing continuity across disparate analysts and cases.

Some observations and suggestions concerning case management system:

- New, less mature, and small SOCs may wish to consider a ticketing system that is cloud-based, the same solution as the IT helpdesk, or built into one of its other tools like a SIEM or EDR, to minimize timelines and acquisition and sustainment costs.
- The SOC may find that it will naturally gather information not only on constituent systems and networks, but about adversary actors and campaigns. When making a choice regarding case management, the SOC should evaluate whether it expects to capture this information principally inside its case management system, or in a separate threat intelligence management platform.
- Ensure alert deduplication/aggregation and throttling is put in place to avoid a phenomenon known as ticket storms.
- Enabling triage analysts to “squelch” or temporarily pause a busy detection that would otherwise overwhelm them with unwanted cases.
- Automate alert enrichment and frequent emails sent to constituents, such as through email templating.

SOAR are a set of products and features that, as their name implies, enable the security operations user to quickly and efficiently design and leverage repeatable processes common to the SOC. Leveraging SOAR, the SOC can:

- Gather incidents from disparate systems, presenting a single pane of glass view for alert triage and alert management.
- Enrich and prioritize alerts, integrating threat intelligence and knowledge of entities involved in an alert.

- Execute automated queries or other information gathering activities when an alert fires, like sending a file to malware detonation chamber, gathering vulnerability scanner results, or looking up a user's HR data.
- Run a series of frequently used queries against a log repository.
- Perform routine constituent interactions, such as sending alert details to a constituent, asking for confirmation or repudiation, "was this expected" or "was this really you?"
- Automate response actions like terminating network connections or disabling user accounts.

There are many reasons for the SOC to harness SOAR capabilities:

- Too many alerts and not enough time to manually analyze all of them
- Bring better, more prioritized, and enriched data to the analyst
- More repeatability and consistency in triage and investigation
- Enabling junior analysts to "snap to" procedures codified in workflows by more senior staff
- Improvement in quality of life for the analyst, meaning fewer manual tasks to accomplish
- Faster triage time (mean/median time to acknowledge and investigate)
- Faster response time (mean/median time to contain, respond, and eradicate)

The idea of automatically closing out incidents and responding to the adversary can be very compelling. However, for a SOC that does not already have firmly established processes in place, this can also add risk. Avoid high-risk workflows until both the SOC has reached strong maturity in its incident handling, and executed low-risk integrations. When implementing high-risk workflows: ◦ Avoid active blocking actions against firewall, VPN, or identity solutions in the first three to six months of using a SOAR product. ◦ Ensure reversibility is built in.

Knowledge of what monitoring tools are in use might allow the adversary to mount direct attacks against them or, more often, shape its attacks to avoid detection. A SOC can execute its mission in part because the adversary does not know where or how monitoring and response capabilities operate.

A key recommendation is: Limit exposure of SOC monitoring infrastructure, sensors, analyst workstations, or any other SOC equipment from the general constituency's domain. The SOC is considered the "inner keep" of the constituency castle and should be the least likely asset to be compromised. As a result, the SOC must be even more vigilant in securing its systems against compromise.

The SOC should consider several questions when planning the approach and degree to which the SOC should insulate itself against constituency breach:

- What proportion of the user population has local administrator on their desktops, thus making privilege escalation and lateral movement by the adversary a further-elevated risk?
- What kinds of logical separations are already in use, and can they be trusted?
- What is the security hygiene of network management, meaning can it be trusted to offer insulation from the general user population?

Typically, each analyst will have at least two desktops: one desktop for SOC monitoring and analysis, and one standard enterprise desktop/laptop for email, Web browsing, and business functions. Maintaining this separation introduces some inconvenience for the SOC analyst, but this is usually outweighed by maintaining the highest level of integrity.

Strategy 11: Turn Up the Volume by Expanding SOC Functionality

Having a solid incident response and detection function, along with basic CTI capabilities, is necessary but not sufficient for most SOCs given the adversaries' ease of hiding and shifting of techniques. Therefore, the SOC may find it necessary to incorporate additional functions which are designed to augment more routine detection and prevention techniques.

These additional functions include:

- Looking for the adversary in new ways through threat hunting
- Testing and enhancing the SOCs 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 SOCs knowledge of adversary actions, techniques, and tools through malware and digital forensic analysis
- Improving SOC operations through the use of tabletop exercises

Cyber threat hunting is a proactive security search through networks, endpoints, services, and data to discover malicious or suspicious activities that have evaded detection by existing, routine tools and monitoring.

Threat hunting is an active and proactive process that relies on skilled, intuitive experts to engage in detective and analytic activities not yet reduced to routine practice by the SOC. To be effective, threat hunters create hypotheses based on adversary behavior, and search to validate by using intuition, logic and reasoning, and forensics. Perhaps most important, hunters take an assume breach mindset; they assume an adversary is already entrenched in the enterprise, so they are primarily interested in searching for evidence of identifying the adversary "right of hack".

Hunters need context, and more than just network or system data, they need visibility into mission areas, to see what adversaries might be doing across missions. Threat Hunting is one of the best ways for a SOC to find adversaries that elude ordinary, routine detections and alerting.

Some of the business reasons of why SOCs find threat hunting of value include:

- Confirming and denying suspicions the adversary is on the network
- Conventional means of detection are proving unsatisfactory
- Another organization provided a lead requiring a deeper look than what routine detections did not find
- CTI indicated an adversary may be targeting or interested in the constituency mission or data
- Vulnerabilities known to be in the constituency are being actively exploited
- Growing analytic techniques that can be feed back into routine operations

Hunting is not the same as routine incident investigation. Generally, analysts should have specific objectives and/or hypotheses for a given hunt. Sources for inspiration of hunt activities include incidents within the enterprise, CTI, and adversary behavior experienced by others.

To start hunting, most teams form an adversary scenario or hypothesis. This hypothesis could correlate to most any part of the kill chain or ATT&CK matrix: how an adversary might target the constituency, their lateral movement, what their actions on objectives might be, and so forth. Based on the scenario, hunters develop TTPs and hypothetical values to use for forensic and other searching.

Sample steps involved in hunting:

- Plan the hunt: The hunt team should clarify the hypotheses, goals, scope, timeline of the hunt, and nominate who will be involved in the hunt.
- Gather and gain access to necessary data: The hunter should bring together the data nominated in Step 1. If the SOC is already gathering, curating, or has access to the data in question, this step is very quick.
- Perform iterative analysis: This is the core execution of the hunt. During this state, hunters will write and execute various analytics against the data.
- Respond or provide findings to the IR team.
- Share results and synchronize operations.

No matter how hunt teams are activated or designed, here are some tips for success in carrying out hunts:

- Focus on a specific hypothesis: Develop a single or small related set of TTPs to start. Be clear on scope and avoid inadvertent scope creep.
- Be curious: Curious analysts are the most effective hunters. Technology can be taught, curiosity cannot. The subtlest of indicators can lead to big discoveries.
- Choose scenarios based on perceived mission interest to an adversary.

For hunting, the team might pick one of the tactics and one of its associated techniques, based on the adversary, and the likelihood to see in the enterprise, or based on understanding SOC defenses and monitoring. Once a set of TTPs is chained together, the hunt team can then derive the data necessary to detect the TTP activity.

Threat hunting is often analyzed in three dimensions:

- Timing: When an event occurs including the sequence and duration of events.
- Behavior: What events are occurring including relationships/correlation.
- Terrain (cyber environment): The systems, processes, applications, and networks in context of SOC monitoring and adversary movement/exploitation.

Some of the network, EDR, and other data queries that might be developed to provide attributes, hints, and further leads to explore include the following:

- Failed logins
- Hosts with new logins
- New users
- Uncommon processes (bottom 10 percent or so)
- Powershell downloads
- Windows: Recycle bin contents (malware, suspicious tools, files, etc.)
- Publicly facing Web site vulnerabilities and configuration weaknesses
- Compare DNS logs to CTI

In general, threat hunters need the ability to see network and host activity in detail. Being able to identify vulnerabilities, such as through vulnerability scanning results, may also help. The majority of a hunter's time is likely in designing and conducting various queries and correlations.

Cyber Threat Hunting Tools:

- Logs and SIEM: Any hunt team should start primarily with logs (system, proxy, DNS, web, etc.), and the tools to query them.
- Scripting and command line tools assist in many ways including analyzing logs and categorizing and describing classes and instances of malware (utilizing binary or text patterns).
- Packet capture software: Enables hunters to view traffic, and aggregate, summarize, trend network traffic. It is indispensable in identifying insecure hosts and apps, dissect protocol traffic. Examples include Wireshark.
- Intrusion detection systems: Used to observe traffic across the network. Its usefulness is in the detailed logs. Example includes Zeek.
- Vulnerability scanner results assist hunters in identifying where the designated TTP or log queries/results might turn up with successful adversaries; it is useful to know what vulnerabilities are actively exploited. Example includes OpenVAS.
- Persistence analysis and host information gathering: invaluable for analyzing new and suspicious processes, persistence mechanisms (autoruns) and for malware analysis. Examples include procmon, Sysmon, OS Query.

To become proficient in threat hunting for a specific environment, it is important each team member develops skills in the following areas:

- Train on malicious TTPs
- Develop and test hypotheses
- Learn how environments are instrumented, such as through sensoring and log collection
- Learn what normal activity is (usually means working with system administrators, detection analysts, and savvy system owners)

Table 28. Evolution of a Cyber Threat Hunt Team

Phase Description	Output
Learn the enterprise environment	Augments existing enterprise understanding such as Internet-facing connections, important mission apps or platforms, cloud environments, isolated and not isolated hosts, new devices, IoT, Wireless Access Points, etc.
Learn about adversary TTPs	Understanding various threat actors, from basic to sophisticated, and which might target the enterprise. Understanding TTPs and basics for detection and alerts.
Identify gaps in data collection, including sensor detection, alerts	Recommendations for detection alerts, new sensors, tweaks on type of detection, such as anomaly or by TTPs.
Reuse others' adversary attack scenarios.	Identify incidents not previously detected by enterprise, but detected by other organizations, existing TTPs from others but applied to enterprise, detection configurations.
Develop original adversary attack scenarios	Identify new incidents, malicious actors, adversaries, TTPs, or detection strategies.