Elements of Security Operations

Security operations (SecOps) is a necessary function for protecting our digital way of life, for our businesses and customers. SecOps requires continuous improvement in operations to face fast-evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats. All of this, though necessary, can be very overwhelming for organizations building out a SecOps function or modernizing an existing SOC.

To increase confidence in the ability to quickly stop stealthy attacks and adapt defenses to prevent future attacks, a SecOps function requires the right set of building blocks. These building blocks include the people, process, and technology aspects required to support the business, the visibility that is required to defend the business, and the interfaces needed with other organizations outside of the SOC. By utilizing these elements to build a SecOps function, operations can be improved by increasing automation and accelerating investigations.

SecOps consists of six elements including:

- **Business** (goals and outcomes)
- **People** (who will perform the work)
- **Interfaces** (external functions to help achieve goals)
- **Visibility** (information needed to accomplish goals)
- **Technology** (capabilities needed to provide visibility and enable people)
- **Processes** (tactical steps needed to execute on goals)

All of the elements tie back to the business itself and the goals of the SecOps organization.

Security Operations Processes

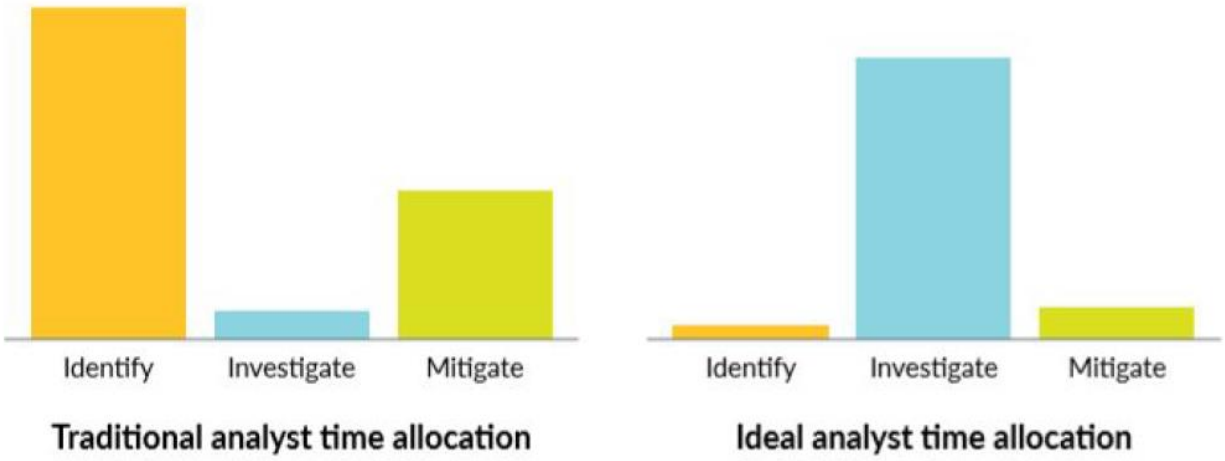
SecOps can be broadly defined as a function that identifies, investigates, and mitigates threats. If there is a person in an organization responsible for looking at security logs, then that fits the role of SecOps. Continuous improvement is also a key activity of a SecOps organization. The four main functions of SecOps are:

- **Identify** – Identify an alert as potentially malicious and open an incident.
- **Investigate** – Investigate the root cause and impact of the incident.
- **Mitigate** – Stop the attack.
- **Improve** – Adjust and improve operations to keep up with changing and emerging threats.

Identify

Security Operations Analysts spend a majority of their time in the identify phase due to false positives and low-fidelity alerts that they must weed through. Correctly implemented prevention-based architectures and automated correlation help reduce the time needed for this phase. A lot of time is also spent in the mitigation phase. This is driven by the lack of automated remediation, and complex or lacking interfaces with teams outside of the security operations organization that need to be involved in halting the attack (see Figure 4-1).

Figure 4-1 *The purpose of security operations is to identify, investigate, and mitigate threats.*



Alerting

Alerting is how an event is determined to be important enough to become an actionable incident. The alerting function has a high opportunity to utilize automation. When automation is used to surface alerts, then how these automated efforts will be validated for accuracy or missing events must be defined. The alerts themselves are generally created and maintained by the content engineering team. The quality of alerts is extremely important for presenting high-fidelity alerts to analysts and reducing false positives.

Content engineering

Content engineering is the function that builds alerting profiles which identify the alerts that will be forwarded for investigation. The content engineering team and the SecOps team need to be tightly interfaced with feedback continuously flowing between the teams.

An interface agreement needs to be put in place identifying how often content updates will be made, how they will be vetted, and the feedback process. It should identify how the SecOps team and threat hunting team make requests for new alerts or modifications to existing alerts. Properly configured alerts will allow the SecOps team to focus on important alerts that require further investigation.

Initial research

Initial research is a set of high-level processes that are utilized by an organization to begin an investigation into a suspicious alert. The results of the initial research assist by providing context around an incident to help in gathering information to triage, escalate, and determine if further investigation is needed or if the alert is malicious or benign.

When an alert is triggered, the SecOps team needs an easy way to gather the information required to determine the severity of an incident and build the foundation for an investigation. Many platforms offer automated severity recommendations and the data required for an analyst to quickly perform the initial review of alerts. Technology should be in place to allow for “right-click” or simple drill-down capabilities to access the context around the alert for the analyst to perform the initial research.

Severity triage

Severity triage defines the event prioritization based on impact to the business to help guide the analyst’s actions through the incident response lifecycle. When automation is utilized to assign an initial severity, the analyst reviews that severity assignment and then validates it against the uniqueness of the organization. This is done to verify or modify the severity and prioritization of the incident against other priorities.

Each business must determine its own risk tolerance and severity classifications. A 1-5 severity system is generally recommended: 1-Critical, 2-High, 3-Medium, 4-Low, and 5-Informational. Critical typically indicates a breach of some sort. The exact descriptions and impacts will vary from business to business. Some organizations add a severity 0 to indicate an ongoing breach where the attacker is attempting to exfiltrate, encrypt, or corrupt data.

Escalation process

Escalation is a set of guidelines that enable the SecOps team to increase the organization’s awareness of a potential issue and receive the necessary support. An interface agreement should be put in place to define what severities require increased awareness from the business. Escalation and communication plans need to be developed, documented, and socialized with all stakeholders. Stakeholders may include:

- IT Operations
- Governance, Risk Management and Compliance (GRC)
- Legal
- Corporate Communications or Public Relations
- Support

An escalation matrix should be developed to include specific scenarios and the associated escalation steps. These plans can quickly become obsolete due to revolving staff, so regular reviews are necessary to ensure accuracy and relevancy. Backup contacts and procedures to address slow or inadequate responsiveness are recommended as well.

Investigate

During the investigate phase, Security Operations Analysts perform a detailed analysis of an incident and collect forensics and telemetry data.

Detailed analysis

Detailed analysis is a deeper investigation into an incident to determine if it is truly malicious, identify the scope of the attack, and document the observed impact. It is a manual process to answer the questions: what, where, when, why, who, and how. Additionally, a detailed analysis helps to confidently determine if an incident is a true incident. In the event of a false positive, feedback should be provided to the content engineering team so they can tune alerts, or to the security engineering team so they can update controls, as needed.

The procedure developed describes the detailed analysis which is conducted as part of the modular incident response plan. The procedure presumes that initial research has concluded, and all respective pieces of information have been gathered accordingly. This procedure closes any remaining gaps that were left after the initial research. In addition, affected IT assets and business services are identified. The appropriateness and efficacy of available containment measures are evaluated and provided as input to the mitigation procedures. Detailed analysis ensures that all relevant information is gathered, including:

- The potential impact of the security incident
- The affected assets
- The adversary's objective
- The potential impact of containment measures

Only after these essential pieces of information have been investigated can an informed decision about the containment and mitigation strategy be made.

Forensics and telemetry

Forensics and telemetry provide the data needed to perform the different types of investigation from severity triage to detailed analysis and hunting.

Telemetry is a broad range of activity gathered in real-time from a given source. It is inclusive rather than selective, and rarely collects the contents of an item. Examples of network telemetry would be session and packet headers, rather than packet contents. Endpoint telemetry would include process execution details, file and memory reads and writes, but not their contents. Telemetry is consistently recorded, which makes it more useful than a log that collects prescribed information only when triggered by a specific event; it is also more accessible than forensics due to the wider coverage area and speed of collection.

Forensics is a commonly misused term, mostly referred to as "the act of collecting raw data needed to complete the detailed analysis for an investigation." Raw data capture requires specific tools and tends to be slow due to its size and method of collection. In the case of network data, raw data would be capturing whole packets or netflow logs, and for endpoint data, it may include a memory dump,

whole executable or operating system files, or even whole hard drives. The true use of the term forensics is to define the method an expert witness uses to prepare evidence. For electronic (or computer) evidence to be admissible in a court of law, it must be repeatable and defensible, the process undertaken by an expert must not modify any of the original data in any way, and the results must be factual and not tainted by whichever party is funding the work. The true use of forensics defines this method, and raw data capture is an integral component.

The use of both telemetry and forensics is a necessity for every security team. Telemetry from network and endpoint activity, and cloud configurations will provide readily available information necessary to triage and investigate the majority of alerts and incidents. Forensic data capture, while slow, will supplement telemetry and provide the information needed to conclude the small number of high priority or difficult incident investigations that often lead to breach identification. Should a breach be validated, all data and results will be required by government and regulatory bodies; however, the forensic data will be of most use to their investigators because of the way it is collected and the depth of its contents.

Types of data include:

Event: Any action performed by a person or technology

Alert: Notification of an event

Log: Details of an event

Telemetry: Activity consistently gathered electronically and in real-time from a given source

Forensic (raw): The complete contents of an item, without change or modification

Mitigate

Key processes in the mitigate phase include executing a mitigation strategy, performing preapproved mitigation scenarios, breach response, change control, and defining interface agreements.

Mitigation

Once an incident has been validated, a mitigation strategy must be executed. The mitigation strategy is comprised of a set of processes and interface agreements to contain the security incident. This typically includes documentation of any actions taken by the security team and temporary controls that can be implemented to quickly stop an attack, which should lead to permanent controls to prevent future attacks.

Preapproved mitigation scenarios

Some mitigation processes are easily automated for preapproved mitigation scenarios. These are a set of parameters that allow for the immediate containment or prevention of a security incident without further approvals. An example would be to block an infected laptop from the network to prevent the spread of malware. Another example is to create a dynamic process to block against specific IOCs (such as known bad URLs, domains, or IP addresses) without requiring a security commit invoking a change window. The process followed for each scenario by an analyst, when executing the mitigation process, should be documented.

Breach response

A true breach requires a plan separate from standard mitigation. It defines how to effectively respond during a critical severity incident. The first piece of this plan is to identify the cross-functional stakeholders, including corporate communications, legal teams, and third parties as appropriate. Then assign a timeline of when each stakeholder should become involved and how they will initially be notified. Details of the information to be collected and shared by the SecOps team should be defined, as well as the SOC commander responsible for providing the information to the stakeholders. Also included should be information about the frequency of updates, method of updates, and communication processes (emails, collaboration tools, a war room, etc.). Training and policies should be created to prevent leaks of breach details beyond the breach response team. Breach response plans should be periodically tested, typically a few times per year, and at least once without the security team having prior knowledge of the test.

Change control

In cases of both manual and automated mitigation, a change control process must be in place to monitor, document, and control changes being made. A good change control process ensures alterations to the environment have a minimized impact to business and are well documented in case a look-back review needs to be performed. The information required for this documentation should be identified and ideally contained in a formal template. This process should have timelines for reviewing and rolling back temporary changes. Also included, should be who can request changes, the steps needed to initiate change, any prerequisites or change windows available for the modification, backout and communications plans, and who can approve changes.

All changes should be:

Deemed necessary to the business

Consistently documented (even when automated)

Planned and scheduled to minimize downtime or disruption

Interface agreements

Interface agreements define how the SecOps team and other teams will interact with each other. These agreements list the teams involved and detail the scope of work and responsibilities for each team. SLAs and operational-level agreements (OLAs) should be referred to, as well as change request processes and escalation, in cases where an interface agreement is not being upheld. Communication paths and tools used between the teams should be identified. A regular review of all agreements should occur, and the intervals of reviews set and stated clearly.

Improve

Continuous improvement includes turning, process improvement, capability improvement, and quality review.

Tuning

Tuning refers to adjustments made to the alerting procedures regarding security incidents based on the outcomes of security investigations. It is an important step in reducing false positives and low-fidelity alerts in the SOC. An analyst may determine, during the course of a security incident, that there is a better way to detect the incident to increase visibility at the SIEM. When this occurs, the analyst will engage the tuning process to improve that visibility for future incidents. General tuning should be based on metrics collected from systems in the SOC. This includes a process to retire alerts when they are stale or ineffective.

The tuning process should define:

- Who or what triggers tuning efforts
- Thresholds for those triggers
- A review process for existing alerts
- The steps to request modifications to existing alerts (to increase visibility of future security incidents based on the outcome of a security investigation)

Alerts should be reviewed, at a minimum, on a quarterly basis with a monthly review of alert metrics.

Process improvement

Adjustments must also be made to the incident response lifecycle based on the results of security incidents and new threats. New technologies introduced to the SOC and the business may also require incident response process updates. The process should include information about who can update the incident response processes (this person must be a qualified resource knowledgeable in incident response). Changes need not be made daily, so it should define how often processes should be reviewed, which will vary by process. All improvements should be reviewed and then operationalized and socialized with affected groups.

Capability improvement

Capability improvement is rooted in revisiting prior incidents and asking how these incidents can be better prevented or mitigated in the future. This results in adjustments to the alerting profile, prevention posture, and automation techniques. Sometimes the goal is to prevent an attack; at other times, it is to stop a breach faster or gather the appropriate information needed for quicker investigation. Ideally, this effort should be ongoing and follow every investigation. In most cases this is not possible, so a monthly review of incidents should occur to identify opportunities for capability improvement.

Goals of capability improvement include:

- Prevention of future attacks
- Faster identification and stopping a breach
- Gathering of necessary data for investigation of specific incidents
- Quicker investigations
- Automated remediation

Quality review

As new tuning measures, processes, and capabilities are implemented, a thorough peer evaluation of the changes should be carried out to ensure effectiveness and value to the business. Additionally, incident workflows and documentation should also be reviewed. This is to confirm consistency within the incident response process which will result in a higher level of capability from the SecOps organization.

Identifying who is responsible for reviewing changes, as well as closed cases, must be documented along with a cadence for the review process. This resource must be given time to perform these reviews outside of their normal duties. A process should be created to define what severity cases require review, what items in the case will be reviewed, how feedback will be provided, and what training opportunities arise from the reviews. Then, that training must be delivered to the SecOps team (and sometimes beyond the SecOps team) to improve the overall efficiency and efficacy of preventing breaches.