White Paper

Analytics & Big Data

Intelligent Security Operations: An Investigation Guide

MICRO FOCUS

Table of Contents

SecOps focuses on security event detection and routine housekeeping tasks of the overall security organization such as reporting or addressing end user questions around issues such as spam or phishing attempts. Among them, security investigation and analysis is the front-line defense against increasing cyber threats from multiple actors.

By conducting efficient and effective security investigations, organizations can minimize the potential damage of a security breach. The knowledge gained through security investigation is also used to optimize detection rules and to fix vulnerabilities.

Overview

It is impossible to put an estimate on the importance of protecting organizations' data, customers' privacy, and brand. Virtually 100% of organizations are victims of cyber crime. Damage to any of those areas can cost organizations' money, trust, and reputation. The average annual loss per company in the US is $17 million. The threat landscape is constantly evolving and Security Operations (SecOps) Centers (SOCs) must keep pace protecting the overall operational health of business.

SecOps focuses on security event detection and routine housekeeping tasks of the overall security organization such as reporting or addressing end user questions around issues such as spam or phishing attempts. Among them, security investigation and analysis is the front-line defense against increasing cyber threats from multiple actors.

Security analysts need to conduct security investigation to identify the nature and scope of security issues, arrive at a sound conclusion, and have proper remediation processes started. There are technologies, tools, and best practices available that can help support security analysts with the process.

Objectives of Security Investigation

Security investigation identifies threats and determines the nature and scope of security issues. As part of the detection role of SecOps, security analysts are expected to investigate events, which means they must accurately analyze suspected intrusion events and determine the next steps. When skilled security analysts are able to make informed decisions based on reasonable evidence, it can protect the enterprise, including intellectual property, data, and the brand. The evidence includes analysis of massive amounts of data and patterns of behavior.

No software solution does everything required to perform security detection and investigation, and there is no perfect defense against cyber threats. Security investigation helps to bridge this gap. Security software generates security alerts that indicate something might be wrong; however, the alerts don't provide enough information to determine the scope and severity of that threat. Security investigation determines what the root cause is, which systems are affected, how severe the damage is, and if the attack is still propagating. By conducting efficient and effective security investigations, organizations can minimize the potential damage of a security breach. The knowledge gained through security investigation is also used to optimize detection rules and to fix vulnerabilities.

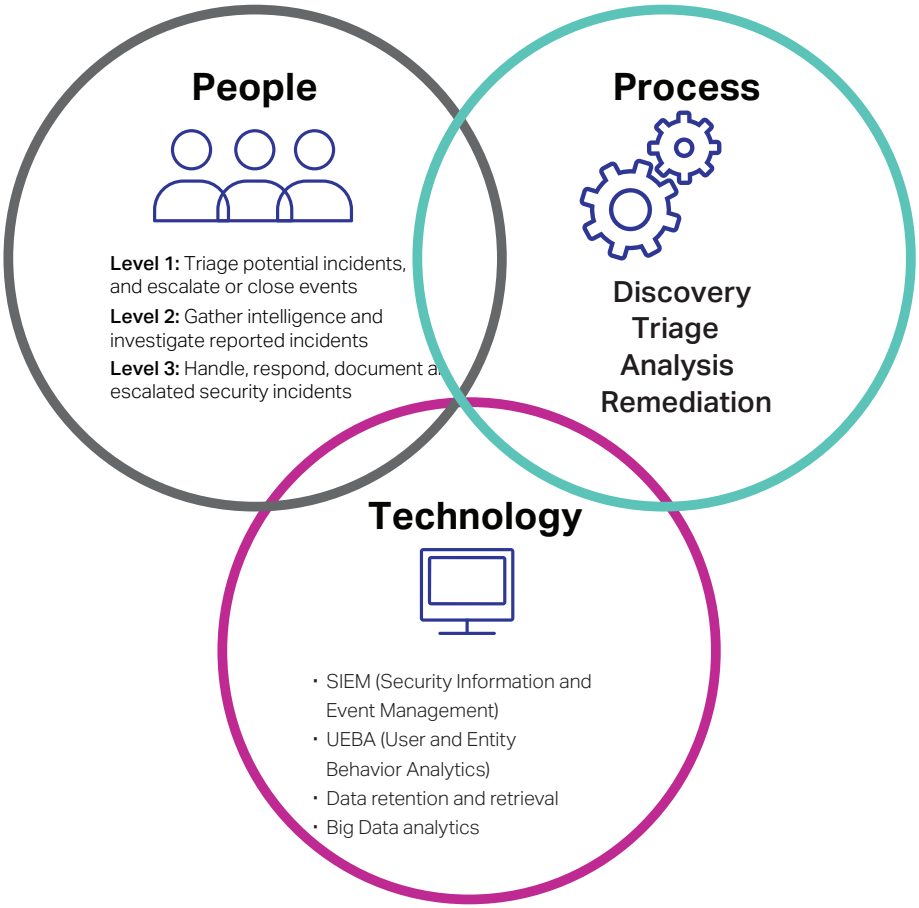

Figure 1. Three pillars of security investigation

Security Investigation Process

Appropriate policies should be established before any investigation takes place. For example, these policies should cover data confidentiality together with established incident response procedures that consider potential litigation and the preservation of evidence. Using these policies, security investigation broadly follows a set of steps from discovery to the conclusion of investigation, handoff to remediation, and restoration of a system to its original state.

Once the entry point of the threat is identified—and the case is escalated from the triage stage— the security analyst begins to collect and analyze relevant data to investigate the case further. The more information you can make available to your security analysts for their investigations, the more successful the investigation.

Discovery

A threat is typically discovered based on rule-based algorithms, dashboard activity, obvious damage, or threat intelligence. This process is similar to how fire is detected. The initial sign that analytics tools are constantly looking for is smoke—any indication in the data that something might be wrong somewhere. When any suspicious activity is detected, investigation begins.

Triage

In the triage phase, the security analysts are expected to make a determination about how severe the threat is and how to handle it. For example, whether to assign an engineer to update detection rules, to escalate incident response, or to close the event as a false positive. Industry and organizations have different sets of priorities (A defense contractor will differ from a retailer.). Analysts must follow their organization's established internal guidelines to quickly identify indicators of compromise and to escalate it to the next phase.

Data Gathering and Analysis

Once the entry point of the threat is identified—and the case is escalated from the triage stage— the security analyst begins to collect and analyze relevant data to investigate the case further. The more information you can make available to your security analysts for their investigations, the more successful the investigation.

Two main points of focus in security investigation include:

- Grouping common events for analysis
- Understanding the attack by gathering information about the full context of the potential attack. This process involves answering the following five questions where possible:
  - **Who conducted the attack?** Identify the IP address to determine where the attack originated and any associated user IDs to determine if the source of the threat is internal or external.
  - **What did they try to accomplish?** Identify the signature names, what the signature definitions are, what a specific Windows event ID means, and which broad category the events fit into—web, OS, application, SQL. The alert will identify what type of attack—for example, if it was web-based or a SQL injection—and this will drive the investigation to the next steps.
  - **When did they make the attempt?** Identify the attack timeline—how fast or how slow—and the time of day in the source IP time zone. Time zone and location will give you more information, and the time stamp helps security analysts determine in which timeframe to look for additional data.
  - **Where did they attack?** Identify the IP address and purposes of the targeted system—for example, external, internal, or demilitarized zone (DMZ); applications; open ports; vulnerabilities; and user names. If it is a potential insider threat, security analysts must determine where the targeted system is located geographically.
  - **Why did they attempt the attack?** Identify the purpose of the attack—for example, admin access, reconnaissance, or web defacement—and whether it was targeted or random. Sometimes this is difficult to determine and it can take a long time to reveal the intention of an attack.

Remediation

At the end of investigation, there should be a clear conclusion that provides the information necessary to make a decision about how to remediate the threat. These steps include shutting down the attack, stopping the data loss, and recovering the system to its original state. The information should be shared with multiple business groups such as IT operations or a regional incident response team to allow them to take appropriate action. Remediation and recovery could take anywhere from minutes to months based on the complexity of the attack and the systems involved. The remediation workflow should be documented internally to facilitate collaboration of cross-functional teams in order to minimize response time. If potential vulnerabilities or risks are identified through the investigation, the information should be reported to management level and business decisions addressing the issues should be made.

The remediation workflow should be documented internally to facilitate collaboration of cross-functional teams in order to minimize response time. If potential vulnerabilities or risks are identified through the investigation, the information should be reported to management level and business decisions addressing the issues should be made.

Skills and Talents

Security threats are uncovered through analysis of huge amounts of data that contain clues about misuse or attacks. To build an effective and efficient security investigation program, your security analysts must be trained to use security technologies and tools correctly, and understand the trend of cyber attacks and framework of decision-making. This includes what type of data to pull to reveal information about intrusions and how to make informed decisions based on sometimes insufficient evidence.

People

Who are the security analysts who perform security investigation and what challenges do they face? In a SOC, no one person can do everything, and many roles are needed to respond to threats. The following are descriptions of the tasks that are typically performed by different levels of security analysts in a SOC:

- **Level 1 security analyst**
  - Perform initial investigation, triage potential incidents, and escalate or close events as applicable. Look at events and assess relevance
  - Monitor incoming event queues for potential security incidents
  - Document investigation results, ensuring relevant details are passed to tier 2 for final event analysis
- **Level 2 security analyst**
  - Ensure Level 1 events are addressed in a timely manner using available reporting and metrics
  - Approve, and if necessary, further investigate Level-1-escalated events
  - Manage SOC event and information intake to include gathering intelligence reports, monitoring ticket queues, investigating reported incidents, and interacting with other security and network groups as necessary
- **Level 3 security analyst**
  - Handle, respond, and document all events or incidents that require escalation from Level 2 or Level 1 security analysts
  - Analyze and review escalated cases until closure. This includes investigating and recommending appropriate corrective actions for data security incidents, which includes communicating with the implementation staff

Who are the security analysts who perform security investigation and what challenges do they face? In a SOC, no one person can do everything, and many roles are needed to respond to threats.

When security analysts move to a new organization or adopt new tools, they should spend a significant amount of time just to learn how to use the new solutions. To lower requirements for IT training by implementing an investigation solution providing simple and intuitive user experience can help increase productivity of valuable talent working in security operations.

To learn more about the roles and responsibilities of SOC staff, see Intelligent security operations: A staffing guide business white paper.

SOC security investigations are generally a trade-off between the bandwidth of the security analyst and the depth required for the investigation. Larger enterprises typically use a tiered system of Level 1 security analysts who perform the initial triage and Level 2 or high-level security analysts who perform more in-depth investigations. Unfortunately, smaller organizations often don't have the staff to use this type of tiered system.

Skills and Training

Your security analysts need to be trained in multiple areas:

- Computer science including data structures, databases, operating systems, and networks.
- SecOps including defense in depth, data loss prevention, insider threats, and kill chain analysis.
- Attacker motivation such as hacktivism, cyber crime, cyber war, espionage, and terrorism.
- Vulnerabilities and attacker tactics, techniques, and procedures.
- Investigation tools, including the capabilities and limitations of the tools and which tool is best suited to accomplish investigation needs. If analysts do not know which tool is best suited to accomplish their investigation needs, this can produce disheveled and ineffective investigations.
- Evidence collection and handling, including what to document in an investigation—Not every investigation will go to court, but each one needs to be treated as if it may.
- All local laws and regulations to be in compliance with privacy laws or any other pertinent regulation.
- Communication skills—presentation and writing—to clearly and accurately impart findings and complex concepts that can be understood by management and customers, and that may be used in court.

When security analysts move to a new organization or adopt new tools, they should spend a significant amount of time just to learn how to use the new solutions. To lower requirements for IT training by implementing an investigation solution providing simple and intuitive user experience can help increase productivity of valuable talent working in security operations.

Technologies and Tools

Security analysts always need more information. The amount of data and how to sort through that data are key elements to investigation. How analysts perform their investigation is largely determined by the type of event and by the tools that are available for the analyst to use.

Many tools are currently needed to effectively perform security investigation. Security analysts need to access multiple tools to get the information needed to complete their investigations. Moving from a window

to another is not efficient and delays the investigation process. Having one pane of glass for security analysts is ideal but the integration of tools is in its infancy. These software products focus on real-time correlation, user behavior, data retention and retrieval, and data manipulation. However, none of these are sufficient on their own. Typically, SOCs use a number of tools to strengthen their security posture and to increase the success of investigations.

Security information event management (SIEM) products provide real-time visibility into security events, event correlation, investigation, and case management. Real-time correlation is a core capability of SIEM, which enables automatic detection.

SIEM

Security information event management (SIEM) products provide real-time visibility into security events, event correlation, investigation, and case management. Real-time correlation is a core capability of SIEM, which enables automatic detection. Without a SIEM and its correlation engine, your analysts will be expected to tie events from multiple sources in different log formats, which software does instantly and much more accurately than people do manually. SIEM solutions create alerts based on correlation rules and detect known threats as they occur. Constantly finetuning those rules is important to improve the efficiency of SecOps. This is because generic rules generate too many false positive alerts while detailed rules produce too many false negatives. Micro Focus® ArcSight ESM is a comprehensive security information and event management solution that identifies and prioritizes threats in real time so you can respond and remediate quickly.

User and Entity Behavior Analytics

User and entity behavior (UEBA) analytics brings profiling and anomaly detection—based on machine learning—to security. It detects unknown threats by creating a baseline of normal user and entity behavior and identifies anomalies associated with users and entities as they occur. By aggregating activities and multiple indicators of compromise for users, entities, and their peer groups, UEBA identifies high-risk users and entities. Alerts that are generated from UEBA complement SIEM alerts, which focus on events and log data, and together they enable more precise threat detection.

Data Retention and Retrieval

Implementing solid data retention and retrieval technologies in your IT environment is a foundation of SecOps. One solution for data retention and retrieval is using a data lake. This method of data management stores massive amounts of data—including many different types of data—in a central location. Another common solution is using log management tools to collect, parse, and store logs. Some of these solutions contain the ability to not just store data but to analyze data as well. For security operations, it is critical to have a single repository of structured data ready to use for threat detection and investigation. Without it, it is hard to have a holistic view of security events to track multi-stage attacks or identify repeated patterns.

Big Data Analytics

Security analytics and business intelligence (BI) tools are software solutions that are used to analyze current and historical data to derive insights for investigation. BI tools are versatile and flexible enough to be used for different kinds of business operations in addition to SecOps, but security analytics tools are optimized to understand data in a security context. These products allow sophisticated analysis including a statistical modeling and immediate visual representation of data analysis facilitating speedy decision-making.

When dealing with cyber attacks, every second counts. Ideally, an investigation will occur immediately when a threat is discovered. However, the reality is that investigations may take anywhere from days to months to complete, while damaging behavior continues unabated.

Current Roadblocks

When dealing with cyber attacks, every second counts. Ideally, an investigation will occur immediately when a threat is discovered. However, the reality is that investigations may take anywhere from days to months to complete, while damaging behavior continues unabated. This can occur because there is so much data to analyze—and the data is spread across so many systems—to identify the true nature of security issues. Therefore, analysts must perform time-consuming manual tasks accessing multiple tools to collect and analyze data. Additionally, the quality and speed of a security investigation is highly dependent on security analysts training, expertise, and discipline during investigation. When they fail to connect the dots in a security context or miss any key indicator, the source of the threat may take a long time to isolate.

Automation—though extremely important for analyzing large amounts of data—can't perform the critical decision-making process that human analysts can. Relying on individual expertise and discipline to interpret the data is still critical in investigation. Therefore, hiring skilled and talented resources to perform robust investigations is an industry-wide issue. The expertise, training, and knowledge of the analysts—which can vary greatly—and this variance in skill and expertise can make it hard for companies to count on consistent quality of investigation outcomes. Because the systems and IT environments are different based on industry and from organization to organization (Threats to a banking organizations are different from threats to government or a manufacturer or public utility.), some of the skills and experience analysts gain in one organization is hard to be transferred to the other.

Security analysts need tools to perform any investigation, but a strong security posture also requires an internal support framework to augment investigation, regardless of the size of an organization. To increase effectiveness, employ best practices that guide your security analysts' process and supplement their knowledge.

Guidelines for Best Practices

Security analysts need tools to perform any investigation, but a strong security posture also requires an internal support framework to augment investigation, regardless of the size of an organization. To increase effectiveness, employ best practices that guide your security analysts' process and supplement their knowledge. The following are best practices for a support framework:

Build and Update a Knowledge Base

A knowledge base is essential for all security analysts. They need a one-stop shop for information such as network architecture, IP ranges, host information, site contacts, and documentation of processes, procedures, and escalation mechanisms. Without readily available and accurate information, security analysts must use guesswork or operate using stale information. The internal knowledge base needs to be accessible by everyone in the security organization so that information can be updated and enriched when investigations are completed or when updated information is provided. For example, if a network segment has been changed to include Microsoft Windows systems when it previously only included Linux servers, events might be written off as a false positive by a security analyst. Having a knowledge base that is not up to date will inevitably lead to mishandled or misidentified events.

Get Triage Checklists Ready

Using triage checklists, your security analysts can perform accurate and consistent triage with confidence. Checklists are not meant to be the only way to handle events, but they can quickly provide guidance for the next steps in an investigation. Having checklists allows you to maintain consistency across all analysts and all shifts. This ensures that an event is triaged the same way at 2:00 a.m. Saturday as it was at 10:00 a.m. on Thursday. Every SOC has security analysts who are more experienced or knowledgeable than others. Sometimes their knowledge has not yet been shared, or a more experienced security analyst may not be available to field questions. Inconsistent triage using different criteria can cause security analysts to doubt and lose confidence in their analysis. You need to know that your security analysts can operate effectively day or night without skipping critical steps, which can result in a mishandled event involving a business-critical system.

Utilize an Effective Ticketing System

A ticketing system is used to track all the events from origination to close. By organizing the events in a ticketing or tracking system, you can ensure that investigations are not accidentally dropped. A ticketing or tracking system allows for a closed-look process for security events, as opposed to a flawed and sometimes splintered process such as tracking events in email. The ticketing system can also help you track metrics around the types of events your organization is facing along with metrics about security analyst performance. This can identify a good investigation, which can help improve programs and train new staff.

Enhance Insights with Threat Intelligence

Threat intelligence feeds enrich security device alerts. One good example is to use the information to correlate an event to a known malicious IP or domain name, providing one more piece of the investigation puzzle. Threat intelligence is also valuable to get insights about tactics, tools, and procedures (TTP). If a certain type of activity is identified, your security analysts can compare this with TTPs from threat intelligence and try to attribute this to a known type of attack from a known group or process.

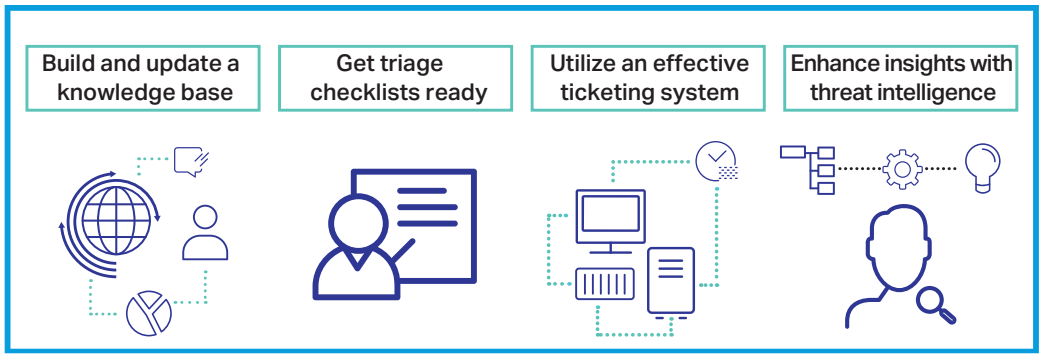

Figure 2. Tips for successful security investigation

Threat intelligence feeds enrich security device alerts. One good example is to use the information to correlate an event to a known malicious IP or domain name, providing one more piece of the investigation puzzle. Threat intelligence is also valuable to get insights about tactics, tools, and procedures (TTP).

To make sure that a SecOps program is healthy and forward-looking, it's important to evaluate whether the right tools and the right people are working together. Fortunately, development of security detection and analysis tools is continuing to move toward making the job more efficient and effective.

Conclusion

To make sure that a SecOps program is healthy and forward-looking, it's important to evaluate whether the right tools and the right people are working together. Fortunately, development of security detection and analysis tools is continuing to move toward making the job more efficient and effective. Ready-to-go analytical tools embedded in the main investigative process can reduce manual steps of data analysis and visualization, helping perform strong investigations in less time and lowering expertise and training requirements for security analysts to operate specific analytics tools. Easy access and management of Big Data can also improve the efficiency of the entire investigation process. SOCs should implement tools that can protect their enterprises from security breaches with fast detection and response and that can increases the efficiency of valuable talents. It is also important to ensure that your security analysts are trained to use the right tools and are up to date on the latest techniques and trends.

Learn More At
www.microfocus.com/secops
www.microfocus.com/espservices

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com