binalyze!

From Security Alert to Action: Accelerating Incident Response

Navigating the Challenges of Comprehensive Investigation

Detection and investigation of security threats are fundamental components of the incident response process, with detection marking the beginning of a comprehensive process. Once precursors or indicators of a threat are detected, embarking on an investigative phase becomes imperative. In most basic terms, the output of the detection process are alerts that should be investigated. While the detection phase tells the analyst that something potentially malicious has happened, the investigation phase not only confirms this but provides the information to address appropriately.

And so, the investigation entails detailed scrutiny and analysis of identified threats to ascertain their characteristics, points of entry, extent, and the potential ramifications on the targeted systems or networks. This detailed investigation requires the acquisition and examination of evidence, as well as tracking the movements of the threat actors involved.

Detection versus Investigation

	Detection	Investigation
Objective	The objective of threat detection is to continuously monitor and analyze network activity to identify known anomalies and potential threats, ensuring timely identification and prioritization of cyber threats.	Once a threat is detected, the investigation aims to understand the nature, scope, and impact of the incident. It seeks to gather detailed information about how the breach occurred, the systems affected, and the data compromised.
Methodologies	Relies heavily on automated tools and systems like IDS (Intrusion Detection Systems), SIEM (Security Information and Event Management), and EDR (Endpoint Detection and Response) to monitor and alert on suspicious activities.	Involves a combination of automated tools and human expertise to collect digital evidence, analyze the data collected, conduct forensic analysis, and piece together the sequence of events that led to the incident.
Challenges	The main challenges include managing high volumes of alerts, reducing false positives, and ensuring coverage across all potential entry points in the network.	Challenges include collecting and preserving evidence without tampering, understanding complex attack vectors focusing on what matters in large sets of data, and accurately determining the extent of the damage.
Tools Utilized	Utilizes real-time monitoring tools, anomaly detection systems, and threat intelligence feeds to identify potential threats.	Employs forensic analysis tools, log analysis software, and threat intelligence platforms to gather and analyze data post-detection.
Outcomes	The immediate outcome is the identification of a potential security incident, which triggers an alert for further action.	Results in a comprehensive report detailing the incident, its impact, the root cause, and recommendations for preventing future occurrences. This phase is crucial for learning from the incident and improving security measures.

Deep Dive Investigations: Elevating Cyber Resilience

Quality investigations serve as a foundational element in the effective management and resolution of security threats, going beyond mere procedural formalities to significantly bolster an organization's resilience against cyber threats. Poorly conducted investigations can lead to a myriad of problems, weakening the organization's defensive posture. For example:

- **Delayed Reaction:** The lack of prompt and decisive action, especially in the face of fast-evolving threats like ransomware, can result in significant operational and financial damage.
- **Misguided Response Measures:** A superficial understanding of the threat could result in inadequate or misdirected response efforts, potentially leaving the organization exposed to repeated attacks due to unresolved weaknesses.
- **Missed Learning Opportunities:** Without deep investigative insights, organizations miss out on valuable lessons that could fortify their defenses against future attacks, improve detections, thereby amplifying the impact of breaches over time.
- **Recurring Security Incidents:** Ineffective investigations might not address the root cause of an incident, leading to a cycle of similar breaches that could have been prevented with a more thorough analysis.

Implementing a rigorous investigation framework is indispensable for uncovering the intricacies of each threat, enabling timely interventions, and fostering an environment of continuous improvement in security practices. By prioritizing comprehensive investigations, organizations can enhance their ability to withstand and recover from cyber incidents, ensuring long-term security and building cyber resilience.

Cyber Investigation Challenges

As highlighted above, the objective of an investigation is different to that of detection. While the output of detection is to generate an alert, the outcome of an investigation is to understand what happened to drive the best possible result. The intricacy of investigations is affected by numerous elements, such as the complexity of the attacker's methods, the availability and integrity of logs and data for scrutiny, the proficiency of the adversaries, and the complexity of the digital infrastructure in question.

As stated in NIST Computer Incident Handling Guide: "Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened."[1] The challenge is further amplified by the presence of sophisticated threats like advanced persistent threats (APTs) and their Tactics, Techniques and Procedures (TTPs), including tactics of encryption and obfuscation. The success of an investigation greatly relies on a combination of investigative tools and technologies available, the skill set of the security team, and their ability to integrate and interpret data from diverse sources to construct a clear narrative of the breach.

"Incident handlers are responsible for analyzing ambiguous, contradictory, and incomplete symptoms to determine what has happened."

1 NIST Computer Incident Handling Guide 800-61 r2

Investigation challenges grow and change based on investigation complexity but they include:

- **Lack of Situational Awareness:** Properly defining the extent of the incident and comprehensively understanding the environment and assets involved is crucial for an accurate response. In the most recent SOC Survey from SANS, respondents cited the "lack of context related to what we are seeing" as their number one challenge. This issue is particularly pronounced for third-party entities who are investigating environments that they are not familiar with, but also affects organizations with suboptimal governance or asset management structures. Proper scoping and investigation require an in-depth understanding of the environment.

- **Lack of Forensic Visibility** (during investigations): Challenges in obtaining the essential data for thorough investigations, including the absence of logs and inadequate or limited monitoring data. Add to that the common difficulties related to capturing and gathering forensic evidence and supplemental data from remote locations and within rapidly changing or diverse IT landscapes. More than half of the SOC teams are struggling to collect evidence from remote assets (50%) and evidence from diverse sources (50%).[2]

- **Lack of Efficiency in Triage:** The challenge of quickly and effectively triaging data across expanding data sets as the volume of information grows. Triage is the number one activity of the SOC.[4] 47% of the analysts find it too long to triage an alert.

- **Lack of Contextual Threat Intelligence:** Lack of contextual threat intelligence during investigations can significantly impact the effectiveness and efficiency of the response to cybersecurity incidents. Contextual threat intelligence refers to detailed information about threats that is relevant to a specific organization's environment, including the tactics, techniques, and procedures (TTPs) of threat actors, as well as indicators of compromise (IoCs) that are specifically tailored to the organization's infrastructure. Lacking contextual threat intelligence during the investigative process leads to prolonged response times, diminishes the effectiveness of identifying threats, and complicates the task of prioritizing them.

- **Fragmentation of Toolsets:** ESG's recent SOC Market Trends report finds that tool sprawl continues to slow down effectiveness across the SOC, with 93% of organization reporting several issues with using fragmented toolsets.[5] Using disjointed tools during investigations leads to constant switching between platforms, wasted time, a lack of a unified view, and difficulties in collaboration among teams. DFIR professionals are using 11-15 paid or open sources tools for investigation[6] and a third of SOC analysts use over 30![7] Most of those tools are not integrated. Spreadsheets and TXT files dominate the workflows.

- **Lack of Consistency in Processes:** The inconsistency in processes presents a significant challenge, as the lack of a uniform approach or strategy results in gaps, isolated efforts, and mistakes during investigation and response phases. The SANS Incident Response Survey highlights this issue, revealing that 32% of organizations recognize the need for enhancement in their incident response processes.[8] This data underscores the critical importance of establishing and adhering to a consistent methodology to streamline efforts, improve coordination, and reduce the likelihood of oversights in handling cybersecurity incidents.

---

2 SANS SOC Survey 2023
3 IDC State of DFIR 2023 Report
4 SANS SOC Survey 2023
5 ESG Report: SOC Market Trends Report, 2023
6 IDC State of DFIR 2023 Report
7 Voice of the SOC Analyst 20233
8 SANS Incident Response Survey 2023

- **Lack of Cross-Functional Expertise:** In many instances, comprehensively understanding the scope, reach and root cause of an incident relies on a team made up of diverse skill sets. According to the IDC State of Digital Forensics and Incident Response 2023[9] report "81% of respondents identified skills shortages (the lack of internal investigation expertise/skills) as the main challenge in managing incidents."

- **Limitations for Team Collaboration:** A cross-functional team is only as effective as its ability to share information and easily access to outputs and insights from malware analysis, security analysis, threat research, and hunting activities. Fragmented tool sets and processes continue to hinder cohesive response, leading to silos and an ability to coordinate workflows and knowledge share.

Enhancing Investigations

It's clear that there is a significant opportunity for improvement in how investigations are conducted. While the current technological landscape excels at detecting threats within vast and complex environments. Various sectors of the security industry focus on improving detection quality through technologies and methodologies such as Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM) systems, Data Lakes, and Data Pipelines. These tools aim to streamline the detection process, reduce the noise of false positives, and enhance the overall effectiveness of the Detection Process.

Their focus is not on the subsequent investigative process. The need for solutions specifically designed to enhance investigation capabilities cannot be overstated. Such tools would not only streamline the investigative process but also ensure a more thorough and accurate analysis of cyber threats. This gap in the cybersecurity toolkit highlights an urgent need for innovation and development, aimed at creating solutions that are as adept at investigation as they are at detection.

To truly enhance our investigative capabilities, a concerted effort must be made to develop technologies and methodologies that address the unique challenges of cybersecurity investigations. This includes overcoming obstacles such as the lack of relevant data, the difficulties in collecting and analyzing forensic evidence across diverse and remote IT environments, and the need for comprehensive context and intelligence. By focusing on these areas, we can develop a more cohesive and efficient approach to cybersecurity investigations.

Learn more about how Binalyze equips security professionals to swiftly and thoroughly investigate and respond to cyber threats.

Visit us at
www.binalyze.com

9 IDC State of DFIR 2023 Report

binalyze!

To find out more about our next-gen solution, visit us at Binalyze.com or start your free 14-day trial today.

Visit us at www.binalyze.com

Binalyze OÜ
Harju maakond, Tallinn,
Kesklinna linnaosa, Hobujaama
tn 4, 10151, Estonia