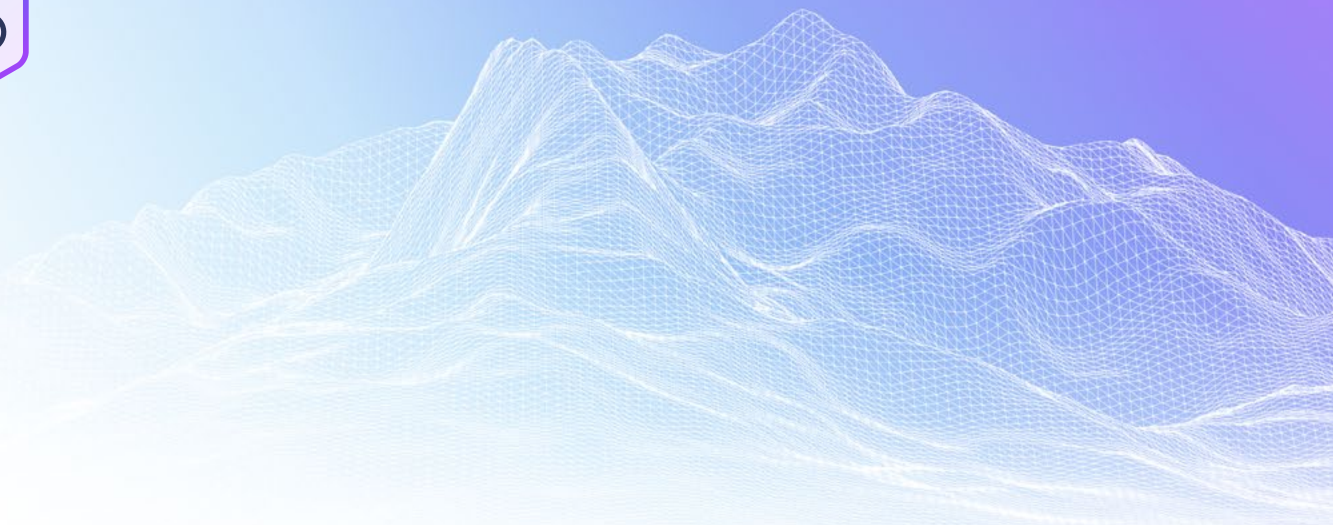
September 2024



Top Challenges in Cyber Investigations & Recommendations for SecOps Leaders

Research Report by Command Zero

Executive summary

This research report summarizes insights gathered from detailed interviews with three hundred and fifty-two (352) cybersecurity professionals (respondents) spanning fifteen (15) industries. It sheds light on the primary challenges encountered in cyber investigations including those stemming from alerts, insider threats, incident response, and threat hunting activities. These three challenges emerged:

Top challenges in cyber investigations

1 The universal talent gap in cyber hinders the ability to run investigations

The global skills gap in cyber is acute when it comes to security operations teams, impeding their ability to run investigations. 88% of respondents expressed concerns about operational issues related to the lack of skilled staff and high attrition rates.

Cloud environments continue to be an area where security operations teams lack the skills (74% of respondents). Visibility and traceability of an attacker across the stack also proved to be a challenge (72% of respondents). These seeds of doubt stem from limited data collection, cloud investigation expertise, investigation resources and technology specific skills.

2 Current SecOps tools are hard to operate and investigate

EDR/XDR, SIEM and SOAR are the most commonly used technologies for investigations. Security operations teams have few alternatives for collecting logs, generating cases and triaging alerts. Even though these technologies are powerful and the defacto standard, there is room to improve threat hunting and cyber investigations.

Respondents raised concerns about high cost of using SIEM, SOAR and EDR – in terms of license costs and the continuous operational labor required to get value from these systems. Blind spots were reported with SaaS applications (60% of respondents) and non-security data sources (72% of respondents).

3 Investigations lack consistency, documentation and auditability

Investigations are still mostly ad hoc manual processes and there's a lot of room for improvement. A lack of standardized collaboration during cyber investigations (92% of respondents), overly complex regulatory reporting (80% of respondents) and time-consuming reporting requirements (79% of respondents) are the leading challenges.

The dynamic and curious nature of analyses result in scope creep (72% of respondents) and most organizations (69% of respondents) lack a programmatic way to incorporate learnings from past investigations.

Command Zero's recommendations for SecOps leaders

Cyber investigations are the most significant bottleneck for security operations today.

To deliver better outcomes with current security operations investments, we need to transform complex analyses. We need a solution that keeps analysts in the driver's seat while reducing the manual toil of the process through automation. We can deliver the best investigation outcomes only if we can provide the subject matter expertise and access for all systems to all investigators. Democratizing these capabilities will increase the confidence of each investigator and build a path for standardized investigation processes.

We can build standard processes for cyber investigations by empowering all tier-2+ analysts (tier-2 and tier-3 analysts, threat hunters and incident responders) to deliver expert outcomes. These processes should include how to collaborate and communicate during analyses. Additionally, processes should outline approaches for reporting, collaboration, communications and scope creep issues.

Command Zero offers a novel way to address the common challenges above and more with the autonomous and user-led cyber investigations platform. **Please visit cmdzero.io to learn more.**

Contents

Introduction

Digital transformation has fueled human civilization to greater heights in the last 40 years, improving almost every aspect of our daily lives. So far, we've observed notable impacts with waves of digital innovation: networking, the internet, cell phones and cloud computing among many others.

Today, we're likely on the cusp of another remarkable wave with Artificial Intelligence (AI) and automation as powerful agents of change. While we're likely in the early chapters of a new era, these capabilities are already improving enterprise productivity and efficiency in ways previously unimagined. Just like with every other technology, the adoption of these complex computing trends raises significant cyber security challenges.

In recent years, the adoption of new and not fully understood technologies has changed the cyber game in already complex IT environments. Traditional tools and methods are challenged to keep up with detecting, investigating cases and recovering from cyber incidents. The current era of SaaS applications, multi-cloud, automation and AI clearly pushes all industries to rethink cyber strategies.

The state of security operations and cyber investigations

Regardless of industry or organization size, most security operations efforts follow a similar pattern:

Monitor activity, create alerts for potential cases.

Triage high volume of alerts and identify interesting cases. Escalate for investigation.

Investigate high priority cases, determine true positives and total impact.

Respond to the confirmed incident and incorporate learnings for the future.

As an industry, we've heavily invested in prevention and detection, yet cyber investigations along with response technologies remain as under-invested segments. Cyber investigations still require highly manual processes with deep subject matter expertise, direct access to data sources and administrator level technology knowledge on systems in question.

The combination of a lack of adequate investment, manual nature of these processes and a lack of skilled analysts makes investigations the most significant bottleneck of security operations. This is also known as the 'last mile problem' of security operations.

The 'last mile problem' of security operations

The 'last mile problem' refers to an organization's ability to conduct critical steps after a case is escalated for investigation. It includes the following fundamental steps:

1. Identify primary incident triggers
2. See impacted systems, isolate
3. Remediate the case
4. Retrieve detailed historic and informative context about the global situation
5. Scope of the breach beyond what is provided by existing security technologies (and their initial alerts)

Completing all of these steps, documenting the progress and doing so in a timely manner are critical for success. Making this process proactive and repeatable ensures that the organization can remain resilient in face of new threats.

The goal and key findings of this research

Command Zero focuses on solving the last mile problem through an expert cyber investigations platform that delivers autonomous and user-led capabilities. As a young startup, carving out the right path for Command Zero was key.

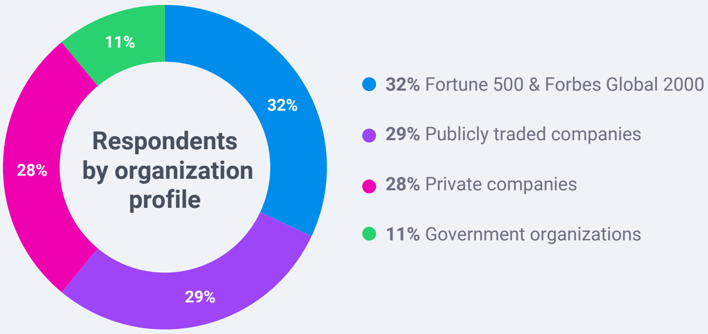
To better understand the current state of investigations, the Command Zero team conducted 352 interviews with security professionals including CISOs, security VPs, directors, managers, incident handlers and responders, legal counsels, and risk leaders.

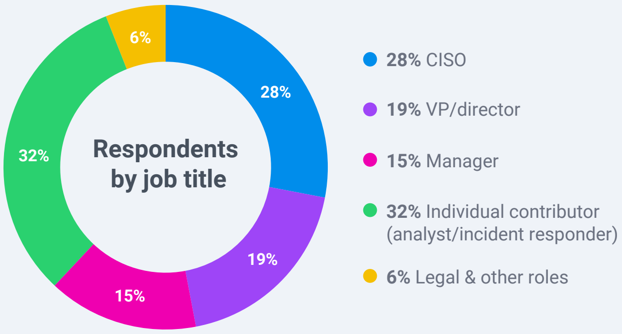
This report outlines some of the challenges facing cyber investigations teams and the learnings based on these interviews.

These interviews discovered patterns including challenges stemming from the complexity of conducting investigations in modern hybrid environments, shortcomings of widely adopted security operations tools, the shortage of skilled investigators, and the difficulty with collaboration amongst responders. This report covers these findings along with Command Zero's perspective on cyber investigations and suggested improvements.

Background and methodology

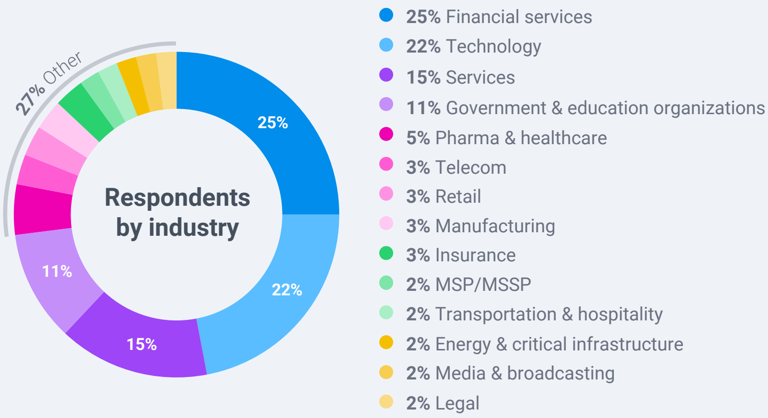
To better understand cyber investigation challenges, Command Zero conducted extensive interviews with 352 security professionals over 24 months (between June 2022 and June 2024). Each interview consisted of thirty to sixty-minute sessions in person and over Zoom. Interviews revealed important patterns about the state of cyber investigations and incident response.

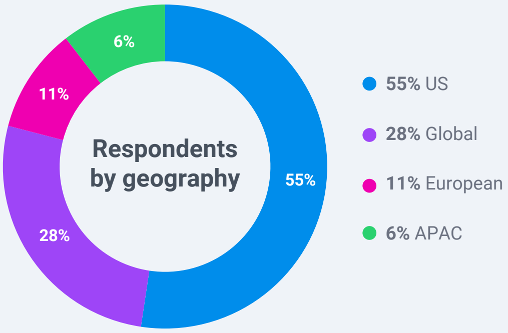




Respondent companies varied among corporate organizations with participation from Fortune 500 & Forbes Global 2000 **(32%)**, publicly traded companies **(29%)**, private companies **(28%)**, and government organizations **(11%)**.

Respondents consisted of cyber leaders and practitioners: CISOs **(28%)**, VPs/directors **(19%)**, managers **(15%)**, individual contributors – SOC analysts/incident responders **(32%)**, legal & other roles **(6%)**.





Respondents came from a wide range of industries including participation from financial services **(25%)**, technology **(22%)** and services **(15%)**, government & education organizations **(11%)** and other industries **(27%)**.

Respondent organizations were mostly representative of US organizations **(combined 55%)**, followed by global organizations **(28%)** and European organizations **(11%)** and APAC organizations **(6%)**.

The top challenges in cyber investigations

Every organization has different business priorities, IT infrastructure, cyber requirements and capabilities. Yet interview responses had surprisingly common themes. These are the top challenges based on the interviews:

1

Universal talent gap in cyber hinders the ability to run investigations

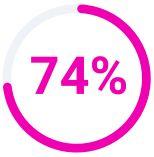
It is no surprise that a significant challenge for cyber teams is a pronounced skills shortage in the industry. The gap between the demand for experienced cybersecurity professionals and the available talent pool is widening for all cyber disciplines. This research indicates that this gap is even more acute for cyber investigations. This finding can be explained by the high skill requirements for investigators. Analysts who are tasked with resolving cases need to be subject matter experts in the analysis and have admin-level knowledge of data sources.

The scarcity of experts leads to situations where existing teams are often stretched thin grappling with the dual responsibilities. Namely, staying abreast of the latest cyber threats while also ensuring that day-to-day security operations run smoothly. This oversubscription creates room for potential oversights and burnout, undermining the effectiveness of overall security measures. Security teams must foster a culture of continuous learning and collaboration to navigate complex scenarios, yet this is challenging when teams are constantly in fire-fighting mode.

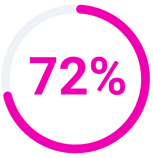
Before the wide adoption of cloud computing, servers, networks and data storage were deployed locally in on-premises environments and controlled data centers. The surge in SaaS and cloud computing adoption has created the need for cyber investigators to now perform across SaaS applications, traditional on-premises environments, cloud environments, as well as hybrid deployments. Similarly, the complexity of securing organizational assets has also increased. Beyond the complexity associated with modern environments, security operations teams find themselves in a relentless race to master a growing arsenal of specialized investigation tools.

Findings >>>

88% of respondents expressed concerns about operational issues related to the lack of access to skilled staff and high attrition rates. Undoubtedly, high attrition impairs institutional knowledge and processes for all organizations as a result.



Cloud environments are a significant part of enterprise IT infrastructure today and are projected to become an inevitable business necessity by 2028 (source: Gartner Says Cloud Will Become a Business Necessity by 2028). Yet, cloud environments are relatively new and not all analyst teams have the skills to run investigations in the cloud. **74% of respondents stated they felt their team lacked the skills in public clouds to perform high-quality investigations.** This is likely caused by a lack of cloud expertise and cloud security solutions, explaining the booming segment of cloud security and visibility.



Interview responses also showed that **72% of organizations were not confident about their ability to track an intruder through their environments within an incident.** The respondents cited reasons including a lack of data collection coverage, investigation expertise, investigation resources and technology skills. The responses indicated that most organizations are unsure if they're collecting the right data. Many organizations also lack the resources and skills to integrate all relevant data sources (especially when it comes to collecting critical SaaS logs).

Command Zero's perspective

Cyber investigations and incident response (IR) are innately challenging even in traditional IT environments where infrastructure, compute and storage are managed on premises or in fully controlled data centers. Security practitioners working in hybrid or cloud-born enterprises face not only these challenges but also additional issues. The absence of centralized control over the creation and monitoring of cloud tenants and assets can often lead to a complex infrastructure with vast data sprawl. Additionally, frequent, and relentless innovation in IaaS, PaaS, and SaaS technologies result in a persistent learning curve. Unfamiliarity with conducting cloud-based investigations further steepens this curve.

The situation is even more daunting and complex for hybrid environments consisting of both legacy infrastructure and cloud platforms. This added investigation challenge is not easily solved as existing security products typically focus on cloud or on-prem environments with little or no overlap or consistency between them.

The stark reality is that as an industry, we had not invented a scalable way for cyber operations for fully controlled environments. The widespread adoption of SaaS and cloud have only made the problem worse. As a result, defenders keep struggling with security operations fundamentals.

There is an obvious and significant shortage of seasoned investigators. Inexperienced analysts lack the expertise needed to navigate complex incidents and make use of large volume of security data. To make matters worse, budgetary restrictions result in understaffed teams, often leading to employee burnout and high rates of turnover. This is compounded by the fact that onboarding a new analyst to full productivity typically takes 6 to 12 months. Historically, finding skilled security personnel was already a challenge. Now, the need for expertise in both traditional systems, emerging cloud and SaaS technologies further increases the demand for skilled responders in an already deficient market.

Another consistent concern among respondents was **the heavy reliance on key individuals.** Organizations with a single point of personnel failure place their security program in a vulnerable position. In some scenarios, a single senior analyst is the only person on the team with unique knowledge and contextual understanding of the company's environment and security posture. At times, the key individual has developed bespoke tools specific to the organization and is the only one able to maintain and support the nuanced tool. Loss of a key analyst can lead to operational inefficiencies and even catastrophic security lapses.

The skills gap in cyber is a reality we've been living with for decades. However, the problem is more acute and damaging for advanced skill sets, such as incident responders (IR) and investigators. Cyber investigations are both art and science when the analysis process depends heavily on the individual skillset and tools, making the results hard to predict, report or review. Organizational investigation capabilities depend on keeping and growing individual talent, and the survey respondents reveal that as an industry, **we're unable to keep security operations talent at this time** (88% of respondents expressed concerns about operational issues related to the lack of access to skilled staff and high attrition rates).

Recommendations

- Investing in analyst career paths and continuous learning can improve job satisfaction.
- Improving the efficiency and job satisfaction of teams is critical for short- and long-term talent retention. Giving teams the expert tools and the content they need to operate within complex environments, adopting automation and AI capabilities where possible can reduce the burden on analysts.

2

Current SecOps tools are hard to operate and investigate

EDR/XDR, SIEM and SOAR are the three most widely deployed SecOps tools today. These technologies are foundational pillars of information security programs, used by SOC and IR teams across the industry. Although EDR/XDR, SIEM and SOAR are powerful, they incur significant costs due to deployment and management challenges.

EDR/XDR is a robust and powerful tool in capturing endpoint data. However, investigators begin to experience challenges when tasked with correlating network and cloud telemetry. An even bigger issue with EDR/XDR is the hefty price tag. Often, it is cost prohibitive to deploy EDR/XDR at scale in cloud environments. This in turn, can lead to visibility gaps.

Findings >>>

85% of respondents considered EDR as the most heavily relied upon investigation tool.

76% of respondents reported ingesting security relevant data to a SIEM for investigations and GRC purposes, with EDR data being the primary data source. However, respondents also stated that it was prohibitively expensive to use SIEM effectively to cover collection and retention of all security data.

59% of respondents expressed concerns about staffing costs associated with running their SIEM. While at the center of detection, correlation, alert escalations and investigations, SIEM and SOAR technologies have proven to be highly labor-intensive when it comes to implementation, customization and operations.

75% of respondents cited the lack of resources and skills required for integrating data sources into SIEM and SOAR. Most respondents also expressed they are using a third party or dedicated security engineering resources just to keep SIEM and SOAR systems operational.

Highly specialized skills are required to deploy, customize and maintain a SIEM. This involves the complicated process of developing rules and scripts that integrate event/data flow. Further, the financial cost of data retention is a significant and growing barrier due to the explosion of data across the enterprise environment. The SIEM is too costly to be fully deployed (across heterogenous cloud environments), adequately integrated with numerous data sources, and properly maintained.

The final security product which warrants discussion is SOAR. Contrary to the initial promise of the concept, SOAR is difficult to deploy, maintain and integrate. Respondents who utilize a SOAR all emphasized the need for specialized resources to script and automate playbooks. As a result, most SOAR investments are limited to using default playbooks or mildly customized playbooks that require a lot of manual work when it comes to investigating cases.

Investigation teams often encounter additional difficulty incorporating data from non-security products (such as Active Directory, source code repositories, case/ticket management, document management systems, etc.). This information is often needed for application, user, and data loss probes. In turn, this challenge leads to more manual efforts for analysis, resulting in lengthy and costly investigations.

Data collection, processing and retention surfaced as other main obstacles for security operations. **76% of respondents were unsure if they had collected all the data necessary to adequately investigate breaches across all their computing platforms.**

83% of respondents stated that access to SaaS log data is essential for incident response. However, less than 50% ingest SaaS logs into their incident response data platforms Business applications and core SaaS applications are increasingly becoming high value targets since they can host IP and other sensitive company data.

Blind spots in investigations are common due to the narrow focus on security alerts and logs. **Only 28% of organizations automate the integration of non-security data sources.**

Similarly, **90% of respondents consider network data a crucial factor in investigations. Yet less than half of the organizations surveyed collected network traffic flow data,** citing concerns over volume and retention times.

Command Zero's perspective

Despite the early and sincere focus on search/investigations, modern SIEM and SOAR capabilities have evolved to satisfy compliance/regulatory requirements. These technologies do not provide dedicated investigation tools and the right user experience for an effective flow.

Most SIEM features and engineering effort focus on collecting more raw logs and data retention in an economically feasible way, while pushing these logs to data lakes for long term storage and archiving. SIEMs do an excellent job at ingesting high volume of raw logs, normalizing, indexing and storing these logs while running static correlation rules to surface alerts. Due to storage limitations, cost and the difficulty of ingesting custom data, centralized logging on SIEMs is commonly limited to security devices only, generating gaps in visibility.

SOAR is a concept invented to overcome the flood of SIEM alerts and automate response to known threats. SOAR excels at static pattern matching via playbooks and improves the fidelity (aka true positive concentration) of the alert funnel. It does a good job at pattern matching the known alerts, but any minor change in the pattern breaks the rigid playbook structure and SOAR becomes useless for these alerts. In practice, SOAR fails to understand the full context of alerts and adapt to variants of alert patterns.

Although SOAR is not the best solution to cyber investigations, there are a lot of benefits to using SOAR. SOAR automates repetitive tasks, responds to known threat patterns in a programmatic way and improves overall security while reducing the effort for the security operations team. But this comes at a cost. The most consistent industry feedback is that SOAR platforms require advanced security engineering and developers to setup, customize and maintain. This leaves SOAR users restricted with the handful of default playbooks or investing in a full-time content/security engineering team to keep SOAR operational. This brings up the obvious question: With limited resources, **should security operations teams focus on engineering playbooks when they could be focusing on real security issues?**

Combined, SIEM and SOAR deliver a necessary service for security operations. They help continuously monitor the environment for alerts, adhere to compliance and regulatory requirements and can identify interesting alerts/cases that need further investigation. But when it comes to handling escalated investigations, they do not provide a clear path to follow actors across complex environments.

EDR/XDR technologies have come a long way with search and investigation capabilities, relying primarily on the data from endpoint agents. The issue with this approach is that EDR/XDR provide no value for systems that do not have agents installed. This means fundamental systems including Identity Providers (IDPs), cloud components and SaaS can be out of scope for investigations run on EDR/XDR. As of August 2024, some EDR/XDR vendors are adding SIEM/SOAR offerings to their portfolio. It is yet to be seen if these efforts can succeed or if they will carry the same design limitations of SIEMs.

Advanced training requirements for SIEM and SOAR mean that subject matter expertise will always be siloed within the team. Analysts running cases need to pull in other individuals to get full technical coverage. This also makes redundancy within the team more challenging since more team members need to get training on each platform. Additionally, platform user/admin training is a significant time investment.

Overall, security operations teams are left with SIEM, SOAR and EDR/XDR systems that do a satisfactory job collecting logs, generating alerts and triaging alerts. Yet, for escalated cases that require further investigation, tier-2+ analysts get little to no support. This means, investigators run investigations with a patchwork of open source, commercial and custom tools.

Recommendations

- Data collection and gaining visibility into your environment is key for security operations. Assume and accept that there won't be 100% coverage of all IT systems nor enough content for detection across all systems. Identifying the gaps you have and fixing them can help improve security. For example, knowing you're not collecting GitHub logs (or that bespoke web application) today, and creating a process for common GitHub investigation types in the future.
- Investing in conceptual and technology-based training for your security operations team will not only make them better at their job but will help with talent retention too.
- Implement layers of abstraction where possible to maximize the value received from individual solutions. Being able to build narratives using various data points across multiple platforms using a single solution is ideal to minimize technology expertise requirements for your team.

3

Investigations lack consistency, documentation and auditability

This is the age-old problem of getting teams to work together more effectively, in the context of investigations. There are very few (if any) security tools dedicated to managing a collaborative investigation process at most organizations. Instead, most teams rely on making things work with generic solutions such as Microsoft Excel, Slack or Google Workspace. Even dedicated ticketing/case management systems fall short when it comes to cross-team collaboration and covering intricate details of cyber investigations in flight.

Findings >>>

The interview process revealed well-known issues along with new patterns for enterprise investigations at scale. A lack of standardization in the investigation process, access to data and collaboration surfaced as agreed facts: **92% of respondents cited the lack of a standardized collaboration tool as a key challenge during cyber investigations.** Reliance on inadequate solutions leads to inefficiencies, miscommunications, and loss of data.

Project communication is particularly important in onboarding new team members to an investigation, handing-off investigations between analysts, collaborating with subject matter experts and asset owners. Getting everyone on the same page becomes even more challenging when coordinating with external personnel. Problems begin to compound when pressures mount internally from management or external parties for frequent updates on current cases. External pressure from press, law enforcement, or other regulators may continue to escalate the situation, resulting in errors during investigations.

80% of CISOs find tracking and complying with regulatory reporting overly complex. This was especially true for organizations operating in multiple jurisdictions. Not having a standard for the investigation process, output and outcomes are contributing factors to complexity. Challenges in getting traceability and auditability of past investigations is the intersection of GRC, security operations, identity management, etc. There's a lot of progress to be made on all fronts to truly overcome this chokepoint.

Reports are the standard medium to communicate the investigation process, outcomes and recommendations. Yet, building technically accurate reports that speak to technical and business audiences is a rare skillset. Conducting thorough and accurate investigations requires a deeply technical skillset. Whereas writing thoughtful reports of the technical process and its business impact requires social and writing skills which are not always common among technologists. This is why reporting is a daunting task for analysts of all levels. The research respondents confirmed this: **79% of respondents cited time-consuming reporting requirements and updating management (as well as other stakeholders) as a significant challenge.** As a result, reporting becomes a time suck for investigators, and report outputs may not meet expectations.

The dynamic and curious nature of investigations also comes with its own challenges: **72% of respondents found investigation scope creep problematic.** Keeping the investigation focused is a constant challenge as analysts must continually evaluate the relevance of new information. The scope of an investigation may expand rapidly as new data is discovered. This scope creep complicates building a clear and concise investigation narrative. To limit this effect, investigators must have well-defined practices when distinguishing between crucial data points and counterproductive rabbit holes.

At the individual level, we get better at things by accumulating experience through practice. At the organizational level, the only way to build institutional knowledge is by leveraging lessons learned in past activities to improve the process for future tasks. While this is common knowledge, implementing this for security operations does not appear to be common today. **69% of survey respondents did not programmatically link learnings from prior investigations.** Past incident data is invaluable as a reference for both future investigations and as useful case studies to train new investigators. A powerful practice for training new resources is the systematic review of prior incidents and associated investigations. These post-mortems not only help the analyst to learn the organization's environment, but also helps to teach investigative techniques. Through effective training, analysts will better understand common attack methods and the associated organizational protocols. All these elements are helpful both for training new investigators and refreshing the hands-on knowledge of the existing team. The result is better overall decision-making during a real incident for both inexperienced and seasoned investigators.

Command Zero's perspective

We live in a world where tier-2+ analysts need to be jacks of all trades to run complex investigations. They need:

- Administrator level technology expertise on all systems within scope.
- Direct administrator level access to all investigated systems.
- Advanced cyber investigations expertise.
- The current and historical context of the environment.
- Advanced written and verbal communication skills to communicate with teammates, other technical teams, business and legal teams.

Add in the complexity of enterprise IT environments and sophisticated attacks, and it's clear: cyber investigations need more structure to be repeatable and scalable. Best investigators are a rare breed who combine sophisticated technical and communication skills with excellent knowledge about the organization and the IT environment.

To get to the bottom of a complex investigation, an investigator needs 6-12 tools and 3-8 hours to reach a verdict on average (Source: ESG The State of the SOC). Experienced analysts are hard to find and harder to keep. Today's threat volumes and mature processes for detection result in more escalated cases. And each escalated case requires thorough investigations. As a result, many escalations end up without a deeper look. And many investigations that get started end up unfinished (without definitive verdicts within an acceptable timeframe).

So, how do the best investigators do it? For seasoned analysts, investigations are a manual process that combines manual controls, script bundles compiled over time and ad hoc communication. This is a model that works for that individual, but it is not repeatable, auditable and it certainly does not scale. The core of the process and the ever-growing knowledge is limited to experienced individuals and no institutional knowledge is built on past investigations.

Let's admit it, as an industry, we haven't advanced how we do investigations from the era of super admins. This was an era where all IT systems were kept in a single data center with total control, and a handful of super admins could know and access all systems within scope. The reality is that the IT systems and enterprise environments we investigate have evolved dramatically since then. Super admins as a concept is a thing of the past in today's hybrid world. All distributed systems have dedicated administrators who only cover parts of the IT ecosystem, likely without the access or expertise for adjacent systems.

To adapt to today's distributed IT environments, we need to shift how we do cyber investigations. We need a solution that keeps analysts in the driver's seat while reducing the manual toil of the process through automation. We can deliver the best investigation outcomes only if we can provide the subject matter expertise and access for all systems to all analysts. Democratizing these capabilities will boost the confidence of each investigator and build a path for standardized investigation processes.

SEC's recent Cybersecurity Disclosure mandates communication of cybersecurity incidents in four business days after the incident is determined to be material. The same statement also brings annual disclosure responsibilities for cybersecurity risk management, strategy, and governance. Being able to determine when there is an incident and documenting the analysis are important capabilities for all organizations. With this new statement, standardized, effective investigation practices and predictable documentation become regulatory requirements for public companies.

We can build standard processes for cyber investigations only if we can empower all tier-2+ analysts to conduct expert investigations. These processes can include how to collaborate and communicate during investigations. This approach would also solve for reporting, communications and scope creep issues noted about investigations above.

Recommendations

- Building detailed processes for cyber investigations is critical to success in complex organizations. As these processes develop, we need to consider three pillars that make an investigation:
  - **Technical investigation flow:** Cover the technical documentation, access protocols and the analyst qualifications. Add lessons learned from previous investigations and organizational context when applicable.
  - **Collaboration during an investigation:** Cover how multiple analysts, multiple business units and external parties can collaborate during an investigation. Defining how often they will communicate, and preferred communication methods are important.
  - **Reporting and communicating outcomes:** Cover best practices for reporting and sample reports showing what good looks like to guide analysts with the reporting process. A library of quality reports always comes in handy for analysts looking for inspiration.
- Look for ways to communicate lessons learned from past investigations in a structured way. Communicating high level flows, the decisions that affected the outcome, and identified areas of improvement with the analyst team helps foster a culture of sharing. Documenting these learnings and optimizing the process and system configurations (including detection, alerting, correlating and investigation tools) will drive continuous improvement. A weekly or monthly investigations office hour can be the right forum for these learnings, accompanied by a weekly/monthly written update.
- Keeping a list of compliance requirements and tagging investigations with the relevant compliance frameworks from inception is a best practice that will help gather the right information, present and communicate it in the right way. This proactive approach will save many cycles for the team as they can now run investigations to satisfy compliance/regulatory requirements.

Conclusion

Cyber investigations in modern environments are complex and labor-intensive.

The top challenges for security operations leaders are:

1. The universal talent gap in cyber hinders the ability to run investigations.

2. Current SecOps tools are hard to operate and investigate.

3. Investigations lack consistency, documentation and auditability.

To overcome these and future challenges, we must transform the way we do cyber investigations. Here are the recommendations to get there:

- **Implementing a unified investigations platform is key** to overcoming the many security operations challenges outlined in this report. Such a solution should be designed to ensure security teams have the tools and skills required to navigate both legacy infrastructure and cloud platforms. It should also streamline the integration of numerous data sources and align them to the investigation process.
- **Cyber investigators who focus primarily on security alerts must extend their focus** to gain a comprehensive understanding of a security incident – running across multiple alerts and systems. It is crucial to integrate various data sources beyond traditional security products to detection, investigation and response capabilities. For example, not having visibility into a high value target like a critical business application is a gap.
- **Automation is essential to enhancing data collection/analysis** from security and non-security tools as well as other data sources. This should improve overall efficiency as well as overcome the gaps in capabilities of tools like SIEM, SOAR and EDR/XDR.
- **To avoid burnout and attrition, SecOps teams need the right information and tools.** To overcome the skills shortage in cyber, organizations must continue to invest in ongoing training programs. Security leaders should encourage the acquisition of certifications, promote employee well-being through workload management strategies, and foster supportive work environments. These actions can reduce burnout while boosting morale and overall job satisfaction. We also need to reduce the repetitive low-impact work (gathering data, reporting, handing over to the next shift) with automation and tools to improve the quality of life for all analysts.
- **Fostering more effective collaboration and communication for investigations is essential.** Teams should implement a dedicated tool for cyber investigations which establishes clear communication protocols, implements strong management practices, and streamlines the consistent execution of inquiries and probes. This will minimize inefficiencies and keep the team focused on the main incident.

The challenges described in this report are ubiquitous among security operations teams across every industry and every company size. These are the exact conditions from which Command Zero was born.

The driving vision is a unifying platform which integrates data from a multitude of security tools, actively trains investigators, enhances team collaboration, and does so across traditional, cloud, and hybrid environments. Adoption of a unified investigations platform which solves for so many common problems will have a profound effect for every organization.

Command Zero is the industry's first autonomous and user-led cyber investigations platform. The platform supports SOC tier-2 and tier-3 analysts, threat hunters and incident response teams. Command Zero reduces the need for technology specific expertise; ensures consistent, repeatable, auditable investigations with automated reporting. As a result, all analysts can perform at their highest levels and deliver expert outcomes.

To learn more, visit
cmdzero.io