Unveiling the Hunter-Gatherers: Exploring Threat Hunting Practices and Challenges in Cyber Defense

Priyanka Badva, Kopo M. Ramokapane, Eleonora Pantano, and Awais Rashid, *University of Bristol*

https://www.usenix.org/conference/usenixsecurity24/presentation/badva

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Open access to the Proceedings of the 33rd USENIX Security Symposium is sponsored by USENIX.

Unveiling the Hunter-Gatherers: Exploring Threat Hunting Practices and Challenges in Cyber Defense

Priyanka Badva
University of Bristol

Kopo M. Ramokapane
University of Bristol

Eleonora Pantano
University of Bristol

Awais Rashid
University of Bristol

Abstract

The dynamic landscape of cyber threats constantly adapts its attack patterns, successfully evading traditional defense mechanisms and operating undetected until its objectives are fulfilled. In response to these elusive threats, threat hunting has become a crucial advanced defense technique against sophisticated and concealed cyber adversaries. However, despite its significance, there remains a lack of deep understanding of the best practices and challenges associated with effective threat hunting. To address this gap, we conducted semi-structured interviews with 22 experienced threat hunters to gain deeper insights into their daily practices, challenges, and strategies to overcome them. Our findings show that threat hunters deploy various approaches, often mixing them. They argue that flexibility in their approach helps them identify subtle threat indicators that might otherwise go undetected if using only one method. Their everyday challenges range from technical challenges to people and organizational culture challenges. Based on these findings, we provide empirical insights for improving threat-hunting best practices.

1 Introduction

Investigating a security breach can be daunting, complex, and time-consuming for security experts. In 2020, a security analyst at Mandiant[1] responded to what seemed like a routine security alert, unaware of what would unfold in the following weeks and months. Soon after, the team discovered that the hack had been active for weeks, undetected by the tools meant to raise alerts. While they could see the intruder's activities, they could not determine how the attack had occurred. But after weeks of intensive investigations, they traced the source to a tool supplied by SolarWinds [2] [49]. According to multiple sources [17, 29, 40, 49], the SolarWinds or *Sunburst attack* [3] is believed to be the biggest and most advanced attack to date. Its discovery was not straightforward; it was through trial and error and a series of separate and loosely connected activities.

Security attacks, e.g., *Sunburst attack*, require the expertise to proactively seek them out from an organization's networks or systems before they could cause significant damage or compromise sensitive data. However, their discovery highlights the complex nature of threat hunting and the challenges it poses to security experts. Despite an increasing number of threats being detected in the wild, the processes and practices of threat hunting remain poorly understood and undocumented. Prior research on threat hunting has largely focused on understanding attacks [18, 23, 31], improving detection [4, 14, 47] and mitigation techniques [20, 26, 33], improved policies around breach disclosures [41], and building effective tools [7, 13, 45], but very limited on the analyst who do the job. Another body of research [1, 3, 8, 32, 37–39, 42] has primarily focused on Security Operations Centers (SOCs) to improve their functioning and the well-being of experts within them. However, despite threat hunting largely falling under SOCs, there remains a significant lack of understanding of the daily practices and challenges threat hunters face.

Understanding these factors is essential for establishing best practices, streamlining threat-hunting procedures, enhancing tool usability, and identifying skill gaps and areas for improvement in the field. To bridge this gap, we interviewed twenty-two (22) threat hunters to gain deep insights into their daily practices, constraints, needs, and experiences with current processes and tools. We asked two primary questions:

RQ1: Who performs threat-hunting activities, and what methods and processes do they use? We aimed to understand the requirements for becoming a threat hunter, including the necessary skills and experience in the field. Moreover, we sought to understand the various approaches used for threat hunting and the factors influencing their adoption. This analysis would enable us to identify skill gaps and areas of focus

[1] Mandiant is an American cybersecurity firm and a subsidiary of Google. www.mandiant.com

[2] SolarWinds Corporation is an American company that develops software for businesses to help manage their networks, systems, and information technology infrastructure. www.solarwinds.com

[3] Sunburst Attack disclosure mandiant.com/sunburst

for recruitment while streamlining threat-hunting efforts by understanding the preferred methods.

RQ2: What challenges do threat hunters face, and what strategies do they employ as best practices to overcome them? Through RQ2, we aimed to explore the challenges faced by threat hunters, their resolutions, and the practices they found essential and effective. Addressing RQ2 will provide valuable insights into the areas where improvement efforts are needed and which practices should be standardized across the industry for effective threat hunting.

Our analysis suggests that threat hunting is performed by various experts with diverse skills and experiences. However, it also requires tacit knowledge, making training essential for new beginners. We unearthed three broad threat-hunting approaches commonly used in the field: use-case/hypothesis-based, intel-based, and random-based hunting. The innovation of threat hunting lies in seamlessly combining these methods to suit needs, available resources, skills, and organizational requirements. Though planning might vary, the core process remains constant - collecting data, identifying and validating threats, and instrument remediation and reporting. Threat hunters encounter various challenges, technical complexities, interpersonal dynamics, and organizational issues. For instance, they face difficulties in building hunting hypotheses due to the ever-evolving threat landscape, with new tactics emerging regularly. Consequently, adaptability is highly emphasized in their approach to address these unique challenges. Our results offer valuable insights into the specific daily experiences of threat hunters. In summary, our contributions to the field are as follows:

- **Comprehensive Understanding of Threat Hunters' Practices**: We provide the first empirical evidence on the daily practices of threat hunters in the wild. We highlight the prevalent methods and how they are used to tackle cyber threats. Additionally, we shed light on the required skills, qualifications, and experience needed for threat hunting.
- **Addressing Challenges and Suggesting Improvements**: Our study offers insights into the most common challenges in threat hunting and the strategies that threat hunters employ to overcome them. By doing so, we identified recommended practices for improving threat-hunting processes.

2 Background and Related work

The concept of threat hunting has evolved over the years, primarily driven by the growing sophistication of cyber threats and the realization that traditional security measures alone are insufficient to safeguard against these advanced threats. Threat hunting is typically classified as an essential element within Cyber Threat Monitoring and Analysis [33]. It can be defined as a proactive and iterative process aimed at searching for and identifying potential cyber threats and malicious activities within an organization's network or systems [28, 36]. Threat hunting can be broadly categorized into two main approaches: proactive and reactive. Proactive hunting involves the utilization of threat intelligence to formulate hypotheses or use cases, enabling security teams to actively search for potential threats before they can cause harm. On the other hand, reactive hunting focuses on conducting forensic investigations and responding to alerts indicating threats after they have been detected [33]. According to SANS 2018 threat hunting survey[4], 60% of respondents reported engaging in proactive threat hunting, with 43.2% conducting it continuously and 16.7% performing it at regular intervals. Our study aims to investigate this further and understand the threat hunting practices in the wild.

Threat hunting is widely recognized as a complex and cognitively demanding process. Consequently, ongoing efforts have been made to automate various aspects of the threat-hunting process. Previous works [3, 11, 33, 36] argue that automation in threat hunting can offer numerous benefits, such as reducing response times, resolving repetitive tasks, requiring less technical knowledge from analysts, and reducing their cognitive load. However, it is also acknowledged that complete automation may not be feasible, as certain aspects of the process require human analysts to make critical decisions. Most analysts rely on their domain knowledge and experience to make decisions, often without deeply considering specific cases [19, 22, 50]. Chen et al. [10] have argued that experts' critical knowledge is often lost and have advocated for tools that can retain expert knowledge to reduce their workload and address their blind spots. We expand this knowledge area by investigating the role of automation in threat hunting and hunters' experience influences their efforts.

While the consensus is that complete automation is not achievable, significant progress has been made in automating specific parts of the threat-hunting process. For example, hypothesis generation [36], data collection, threat detection [27, 48], data triaging [50], malware classification [6, 28], and other aspects of the process. Despite the advances in automation, prior studies have not focused on understanding how these tools impact threat-hunting investigations. In addition to tools, threat hunting heavily relies on intelligence (e.g., threat reports), analysts depend on it for investigations and to ensure the security of their systems. Threat reports are typically based on analyzed and remediated attacks, offering reactive advice [12, 34]. Outside academia, vendors such as Symantec, McAfee, Trend Micro, FireEye, Cyveillance, and Kaspersky regularly publish threat intelligence for multiple government and commercial organizations. Our current study provides valuable insights into how threat analysts use intelligence in their everyday hunting processes.

Other studies [1, 3, 8, 32, 35, 37–39, 42, 46] related to analysts focus on SOCs, primarily aiming to understand the well-being of security analysts. For instance, previous works [35, 37] investigated the factors contributing to analysts leaving the

[4] https://www.malwarebytes.com/pdf/white-papers/sans_report-the_hunter_strikes_back_2017.pdf

field. Another line of work on security workers has primarily focused on bug bounty hunters [2, 5, 43, 44]. For example, Votipka et al. [44] compared how testers and hackers discover software vulnerability techniques. They concluded that the discovery experience, knowledge of underlying systems, availability of access to the development process, and motivation play a crucial role in each step of vulnerability discovery. Our study builds upon these investigations by examining factors that are influential in identifying threats. Additionally, we provide insights about other security workers, specifically threat hunters.

3 Methodology

3.1 Study Design

To gain insight into the practices and challenges of threat hunters in real-world scenarios, we designed and conducted an online semi-structured interview study. Our interview script was divided the script into five sections: introduction, data collection, threat identification, threat analysis, and conclusion. The introductory section aimed to establish rapport and obtain information on participants' role and responsibilities. The subsequent sections, data collection, threat identification, and threat analysis, were designed to delve into the details of the threat hunting process. Lastly, the conclusion had questions that sought to gather suggestions from participants on improving the process and concluded the interview. Demographics were gathered using a separate form.

To validate the effectiveness of our interview script, we conducted pilot studies with two members of our research group who had experience working in SOC. The rationale behind this was twofold: to assess the clarity of our questions and whether they could elicit responses that addressed our research questions and ensure that the interview could be concluded within a reasonable time. Based on the outcomes of the pilot study, we refined our script by reducing the number of questions and supplementing follow-up questions in each phase of the threat hunting process. The pilot study data was excluded from the final analysis.

3.2 Ethics and Participant Recruitment

We obtained ethics clearance from our University of Bristol Ethics committee before beginning our study. Utilizing our personal, industrial, and academic connections, we recruited diverse participants through social media, word-of-mouth, Slack, and academic and industry conferences. Our objective was to identify and recruit professionals whose daily work could be described as threat hunting or involved some aspect of threat hunting and who had a minimum of 2.5 years of experience in the field. This was to ensure that our sample included the necessary expertise and familiarity with the problem space, particularly in identifying, analyzing, and managing cyber incidents. Once interested, we sent them the information sheet (PIS), the demographics form, and consent form. The PIS explained the purpose of the study, anonymization, what participation entailed and the withdrawal process. The consent form was seeking consent to participate, audio recording of the session. Respondents who completed and sent the consent form were further contacted for scheduling a session. We did not conduct any further screening of our respondents since our recruitment material explicitly requested participants with over 2 years of experience. However, to ensure suitability, we asked them to clarify their roles and daily activities during the interviews.

Similar to other works on security workers (e.g., [4]), targeting such a unique and specialized group presented a significant challenge. Some potential participants chose not to participate in the study due to concerns about being recorded and directly quoted or about disclosing their company's operational practices. Given the sensitive nature of the subject matter, participants were allowed to participate without sharing their cameras. Moreover, SOC personnel, for example, are typically occupied with responding to severe incidents, and their willingness to participate in academic studies may not be motivated by financial incentives. To overcome these challenges, we employed a snowball sampling technique to increase our sample size. We targeted professionals leading threat hunting teams and asked them to encourage their colleagues and other professionals they know to participate. We also encouraged those who participated in our study to share our research with their colleagues.

3.3 Participants

In the end, we successfully recruited 22 participants from various countries. The majority were from the UK (7) and the US (9), while the remaining six participants were from Qatar, Australia, Singapore, Germany, India and UAE. These participants were employed by leading multinational companies, five participants were from companies that provided in-house threat hunting services only, while eleven participants were from Managed Security Service Providers (MSSP). The remaining six were from companies that provided both in-house and external threat hunting services. While some participants shared the same company affiliation, most worked in different countries and states serving diverse clients around the world. Only P1 and P3 were based in the same office, while P4, P5, P9, P10, and P11 worked for the same company but across different offices in the US. As for their roles, participants held a variety of positions, including analysts, consultants, red team specialists, and security engineers. They also had diverse educational backgrounds and held various security certifications, such as the CISSP. Table 1 provides a summary of the demographics, a more detailed summary of our participants' demographic and professional backgrounds can be

Table 1: Participants demographics details "-" : Prefer not to answer

ID	Job Role	Country	Experience	Education	Company	Type of Service	Recruitment Method
P01	Senior Cybersecurity Analyst	UK	10-15 years	PhD	Company 1	In-house	Industry Connection
P02	Security Consultant	Australia	15-20 years	MSc	Company 2	MSSP	Industry Connection
P03	Threat Intelligence Analyst	UK	5-10 years	Bachelor	Company 1	In-house	Industry Connection
P04	Associate Director Threat Hunt	US	10-15 years	-	Company 2	MSSP	Industry Connection
P05	Threat Hunting Team Lead	US	-	-	Company 2	MSSP	Industry Connection
P06	Digital Forensics Specialist	UK	5-10 years	Bachelor	Company 3	MSSP	Industry Connection
P07	SOC Analyst	US	10-15 year	Bachelor	Company 4	In-house + MSSP	Industry Connection
P08	Director for DFIR	Singapore	10-15 years	MSc	Company 2	MSSP	Industry Connection
P09	Consultant	US	15-20 years	Bachelor	Company 2	MSSP	Industry Connection
P10	Lead SOC Threat Hunter	US	5-10 years	High School	Company 2	MSSP	Industry Connection
P11	IT Security Engineer	US	15-20 years	Bachelor	Company 2	MSSP	Industry Connection
P12	SOC Analyst	India	10-15 years	Bachelor	Company 4	In-house + MSSP	Snowball
P13	Security Analyst L3	UAE	5-10 years	-	Company 5	In-house + MSSP	Slack
P14	Program Lead Adv Sec Analytics	US	15-20 years	-	Company 6	In-house	Slack
P15	Threat analyst	UK	5-10 years	High school	Company 7	MSSP	Slack
P16	Cybersecurity Technical Specialist	UK	10-15 year	Bachelor	Company 3	MSSP	Snowball
P17	SOC Head	UK	10-15 years	MSc	Company 8	MSSP	Industry Connection
P18	Security Research Lead	UK	15-20 years	Bachelor	Company 9	In-house + MSSP	Snowball
P19	Cybersecurity Engineer	Germany	15-20 years	-	Company 10	In-house	Snowball
P20	Lead Cybersec Engineer	US	10-15 years	MSc	Company 5	In-house + MSSP	Slack
P21	Manager, Incident Handling	US	10-15 years	MSc	Company 11	In-house	Snowball
P22	Senior Incident Response Consultant	Qatar	10-15 years	MSc	Company 9	In-house + MSSP	Snowball

found in Table 2 in the Appendix 8.1.

3.4 Interview Procedure

At the beginning of each interview session, participants were reminded of the purpose of the study, their expected involvement, and the withdrawal process. They were also asked to confirm their willingness to participate. After obtaining consent, we initiated the audio recording and began the interview. Our first questions were about roles and responsibilities in their workplaces. We then proceeded to ask about their threat hunting practices, guided by their responses. While we had a script, we did not rigidly adhere to it in all cases, but we ensured that all relevant questions were covered by the end of each session. The interviews concluded with exploring potential areas for improvement in the threat hunting process. Participants were then thanked for voluntary participation in the study, and no financial compensation was provided. On average, each interview session took between 40 minutes to 1hr 15 minutes. Due to time differences with some participants, some interviews took place in the early hours or late evenings of our local time. Our complete interview protocol can be found in the Appendix 8.3.

3.5 Data Analysis

Once data collection was complete, we utilized a professional transcription service that adhered to our university policy and GDPR complaint to transcribe all our interview recordings. After transcribing all the audio files, we began the coding process. We inductively coded [9,30] the scripts using the conventional line-by-line method to identify key themes, methods, processes, tools, and attitudes relating to threat hunting. Two researchers independently coded the first two transcripts to identify key themes, methods, processes, tools, and attitudes related to threat hunting. Following this, they met and discussed their findings to create a codebook. Discrepancies between the coders were resolved using the "arguing to consensus" method [21]. The codebook was then shared with other researchers for review and validation before finalizing. After developing the codebook, two researchers proceeded to code an additional three transcripts and calculated the inter-coder reliability. The inter-coder reliability score using Cohen's Kappa Coefficient was 0.81, indicating substantial agreement in applying the codebook [24]. Then, the first author proceeded to code the rest of the scripts. High level codebook attached in Table 4 in the Appendix 8.4.

3.6 Limitations

While we attempted to diversify and enhance our sample using snowball sampling, we acknowledge some common limitations associated with studies that have employed this technique as a recruitment method. Firstly, snowballing can perpetuate power imbalances; some participants may have participated in the study because they were recruited by individuals in higher positions, feeling obligated to participate. To mitigate this, we emphasized to participants the voluntary nature of their involvement and their right to withdraw at any point, ensuring they felt no external pressure to participate. Secondly, samples recruited through snowballing often lack representativeness. For instance, our sample is biased towards participants from large companies that primarily offer managed security services. This bias may stem from participants sharing the study among their peers or personal networks limited to such companies. Moreover, some participants even

came from the same large corporations. However, while they may have been affiliated with the same large companies, they were situated in different countries, serving a diverse array of clients and dealing with various challenges and circumstances. This diversity instilled confidence in us that our sample has provided a broad spectrum of perspectives.

Other limitations of our study include lack of generalizability. As prior studies [3, 4] have reported, SOCs and organizations are unique, and other salient factors could influence the daily experiences of threat hunters that we may not have captured in our study. Moreover, our results may be skewed towards companies that provide managed security services than those with their own in-house dedicated threat hunting teams. We conducted recorded interviews, which might have influenced participants' responses. Some threat hunters declined to participate due to concerns about recording sessions, which could have led to under-reporting or giving answers that they believe are socially or professionally acceptable. To mitigate this social desirability bias, we emphasized that we were interested in their opinions on processes rather than specific sensitive issues. However, it remains essential for the security community to explore alternative methods that protect participants' identities or their organizations while still obtaining valuable insights.

4 Findings

4.1 Who performs threat hunting?

Our analysis suggests that threat hunting is performed by analysts with various skills and qualifications, who may either belong to dedicated teams or have other responsibilities within their organizations. Participants engage in threat hunting both for their own organizations and as consultants for external entities. From our sample, those who had dedicated teams performed threat hunting for their organizations and also provided external consultations: *"I have 9 staff working for me. We have staff in the US, India... It's a dedicated service, when a client signs up, we assign a dedicated analyst to that particular client."* P04

Teams are often formed randomly, with their structure and size depending on the organization's size and requirements. Threat hunting teams in some organizations can consist of one person or a team that leads the efforts and receives assistance from other teams or departments within the organization. For instance, P7 explained that their threat hunting is part of a SOC, where they have a monitoring team, and others perform threat investigations. *"I work around the SOC, which also has threat intel, threat hunting, [Incident] response, all of that. The organization is global in the sense that we have office in possibly every country on this planet. [...] We run our security operations centre from two geography's and do cover 24 [countries] across seven services. There is a threat intel function which works for big organizations, the other companies, the other big organizations in the United Nations family and so on."*

Regarding skills and qualifications, we found that threat hunting teams consisted of analysts with various skills and knowledge (captured in Table 1 and 2). However, many participants with teams explained that they either received or provided training for their new team members. For instance, one participant explained that their team comprised individuals with forensic and penetration testing backgrounds, but they had to provide training to cross-train the team members in threat hunting. P05 said *"I have a team of 8 people, most of them actually started on our forensic team, and I've kind of poached people from the forensic team... pentest team to form the threat hunt team. I had to cross-train the forensics guys and the pen-testers."*

This finding is further supported by the skills and qualifications of the participants in our sample. They have various skills and qualifications. Other teams started with one member, and later were joined by others. P10 explained: *"Our company had one dedicated threat hunter, [name]. He's also a science instructor. He kind of worked on threat hunting but he didn't work in the SOC doing the day-to-day job, [he did] informal type of threat hunting stuff. Me and a few others started doing threat hunting on our own and we proposed a threat hunting program."* P10

> **Take Away.** Threat hunting is carried out by analysts with diverse qualifications who may be part of dedicated teams or have other organizational responsibilities. Since there are no specific entry qualification requirements for threat hunting, organizations invest considerable time and resources in training their staff to excel in hunting for threats.

4.2 How do they perform threat hunting?

Our analysis revealed that threat hunters employ various methods when conducting threat hunting in the wild. These methods are often combined based on specific needs and available resources. For easy explanation, we have categorized them into three broad groups: use-case hunting, signature or intel hunting, and random hunting.

In the first approach, **use-case hunting (n=17)**, threat hunters use predefined scenarios or patterns of suspicious activities to identify and investigate known threats and attack patterns. These use cases are based on the threat hunters' knowledge of threat actors, the systems they own, and the typical attack patterns. The second category, **intel-based hunting (n=7)**, involves leveraging technical threat intelligence, such as known indicators of compromise/attacks (IoC/IoA), to guide the hunting process. This method relies on up-to-date threat intelligence to proactively detect potential threats. The difference between these two methods is that in use-case based hunting, hunters rely on pre-defined scenarios or cases to hunt for threats, while intel-based hunting relies on

the threat intelligence they receive to investigate and identify threats. For example, under intel-based hunting, hunters may use malware signatures they have received to search for threats. Under use-case based hunting, hunters formulate or create scenarios to guide their efforts, and sometimes these scenarios are informed by threat intel. For instance, a scenario may include the behavior of malware which was provided as intelligence. The third category, **random hunting (n=6)**, encompasses methods where participants conduct hunts without prior knowledge of specific indicators of compromise or a predefined plan. This approach involves being alert to potential threats during regular responsibilities or while conducting other specific hunts, such as onboarding new clients or responding to incidents initially considered benign.

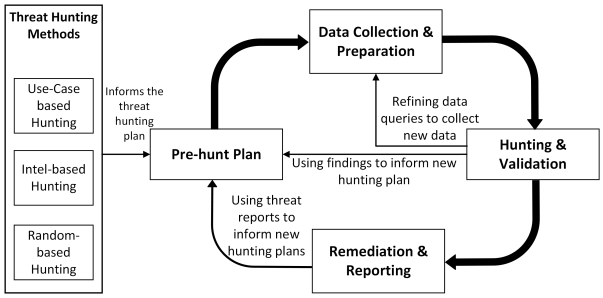

Figure 1: Threat Hunting Process

Our analysis indicated that the choice of approach is influenced by several factors, including available resources (e.g., malware lab), data availability (including external threat intelligence), the skills and experience of the hunter, and organizational requirements. Despite their differences, these methods share a similar approach involving planning, data preparation, threat identification, and remediating and reporting the findings. Figure 1 shows the relationship between various processes involved in threat hunting.

4.2.1 Pre-hunt Plan

Our analysis indicated that most threat-hunting activities begin with a dedicated planning phase. During this stage, hunters gather to formulate a plan that outlines the specific areas they intend to investigate. Participants emphasized that having a well-defined plan enables them to assume control over the exercise and effectively allocate resources. They also explained that having a plan helps keep the entire team involved. *"We try to plan all that stuff out at the beginning. It's planning, getting together in the beginning with everyone involved. And, then just let the system run, and then if something comes up later, you deal with it as a team."* P19

Pre-hunt plan for **use-case-based hunting** involved defining the scope of the hunt, determining the type of threat to pursue, and identifying the required data sources based on the use cases and hypotheses they have developed. Participants stated that they create use cases based on Tactics, Techniques, and Procedures (TTPs), particularly leveraging the MITRE ATT&CK framework, historical incidents, threat intelligence, their knowledge of the infrastructure in question, or the specific requirements of their organization. *"Using my experience of having worked in many environments and I look at how unlikely an attacker would target one of those individual systems. Then we build a threat mod el that goes from the outside in using info that is publicly available for the initial compromise. But then my experience comes in, how does a breach of [the] main frame look like, what data would they try to steal, what would they do if they got access to a PLC."* P18

Once the use case is finalized and the approach is outlined, participants explained that they would determine or compile a list of the necessary data for the hunt and identify the relevant sources. This is to ensure that the data is readily available when needed. *"It's really important that you identify the data sources before you do an investigation, so you can onboard them, normalize that data, so when you need to do any type of hunting activity, it's readily available."* P14

Participants who consulted for other organizations mentioned that the planning phase included assessing the client's infrastructure to understand normal behavior and whether their existing resources and methods could be applied to the client's case. P04 said: *"When a client signs up for our service, we assign a dedicated analyst specifically for that client. This allows the analyst to become familiar with the client's environment, understand what is considered normal in that context, and identify abnormalities."*

Intel-based planning is primarily influenced by the intelligence or indicators of compromise (IoCs) hunters receive. This intel may come as hash values, filenames, registry keys, IP addresses, domain names, malware, and host or network activities associated with malicious activities. Participants explained that detailed and specific planning begins when they receive such intel. Consequently, they rely on getting the latest threat intel. Participants received intel from various sources, primarily external sources such as mainstream vendors and open-source intelligence platforms. They shared that they also actively participate in various security communication groups on platforms such as Slack, LinkedIn, and Twitter, while others are public and private security exchange groups. *"We start by looking at what's available open source; blogs and reports that other vendors have produced, maybe where they have only mentioned a particular piece of malware or CnCs [Command&Control]. We then take those CnCs, analyze them further, and try to build a bigger picture. We also get intelligence from other partners in the community, closed intelligence exchanges, not open to the public, just between security vendors or other companies in that kind of space. We have our tracking as well. We've paid for services like VirusTotal, an online malware repository service, and we pay to put certain kinds of tracking in place on those sites, various services such as the known groups we track. We can say if it*

satisfies this rule, it will alert us, and we can stay on top of things that way as well." P16

Once intelligence is received, hunters review and try to understand it; its origins, the systems that can be affected, and how the threats can be identified and mitigated. P03 stated: *"The idea is that once we have that, we would then run that information through other data sources that we [have] purchased or have access to, and kind of enrich it."*

For **random hunting**, we observed that there is minimal planning involved. These hunts are more ad hoc, happening spontaneously and sometimes driven by curiosity or a hunch. For instance, a threat hunter may impulsively investigate old 'benign' logs without a predefined plan or specific objectives.

> **Take Away.** Threat hunters use various methods in their hunting activities, which they often combine based on their specific needs, skills, knowledge, and available resources. Most activities start with a dedicated plan, where hunters define the scope of the investigation, assess threat intelligence, generate hypotheses or use cases, identify relevant data sources, and allocate resources based on their chosen approach.

4.2.2 Data Collection and Preparation

Once the pre-hunt plan is complete, participants indicated they would collect and process the necessary data from various systems. Threat hunters collect data from various sources, including firewalls, antivirus, network systems, Endpoint Detection and Response tools (EDR), and proxy servers, and these data are based on specific time frames or behaviors of the systems. Participants emphasized the importance of selecting the hunting approach before initiating data collection. For example, P09 stated, *"Before you even get to data collection, you talk about the frame of where they are approaching it from. [...] People will see something on Twitter and say, 'That's a great idea; let me go and hunt for it,' but they don't really bring a rigorous approach to it."*

After gathering all the required data, they curate and prepared it for their hunts. The data preparation process involves cleaning, filtering, consolidating, and transforming the data into a usable format. This is often within a single location or system such as a SIEM (Security Information and Event Management) solution, which also aids in the hunting process. Other steps included normalizing, parsing, and restructuring the data. Filtering was typically performed to remove benign activities from suspicious events, based on time frames, patterns, and thresholds defined during the planning phase.

For participants using **use case hunting**, data collection was aligned with the goal of the hunt. They would determine what the hunt needed and then search for the logs supporting those detections. They would then build rules or triggers to detect threats, even those that may not be easily noticeable.

Participants who utilized the **intel-based approach** stated that once they understood the campaigns or the intel, they would plan how to implement or run the IoCs in their systems. This process involved collecting relevant data and preparing the testing environments such as malware labs, to handle the received indicators. Hunters also used the intel to develop new use cases or hypotheses for threat-hunting activities.

Those who engaged in **random hunting** used various data logs for their hunts, often selecting sources based on what was available or what they found interesting at the time.

We found that threat hunters generally prioritize gathering as much data as possible. Participants argued that it could significantly improve the quality of the hunt. For example, P04 stated, *"We collect as much data as we can because the more data you have, the better. Sometimes, you might search for an ID, which might appear on three different devices, allowing you to trace how it entered the network. The more we can do on the SIEM, the better, rather than having scattered devices."*

> **Take Away.** Threat hunters tailor their data collection to align with their hunting goals and collect as much data as possible to maximize their effectiveness in detecting and responding to security threats.

4.2.3 Hunting and Validating

Our analysis indicates that threat hunters hunt and validate threats through an interactive and connected process. Threat hunters move between hunting and validating as needed, often collecting more data/intel or creating new scenarios.

For **use case hunting**, hunters deploy the rules they have built on the collected and filtered data. When specific conditions related to threats are met, alarms are triggered, prompting the hunters to investigate further. P02 explained, *"We create use cases - if the rule is being triggered, we identify the specific behavior, whether that's coming from an IP address or a process."*

For **intel-based hunting**, IoCs are fed into relevant systems to trigger alerts and identify potential compromises. Hunters compare their own data or logs against signatures or patterns of known indicators of compromise associated with specific tactics, techniques, and procedures (TTPs). When a match is found, it suggests a potential compromise or the presence of a specific TTP. P22 elaborated, *"if our threat intelligence profile tells us that we need to look for a specific binary name in the Windows system32 folder, then we're going to search for that."*

On the other hand, **random hunts** tend to occur unplanned and are often initiated by hunches or when the hunter observes something that looks malicious. Participants described situations where, based on their knowledge of the normal state of the system, they occasionally discovered patterns of malicious behavior. P09 stated, *"I could be looking at something and think that looks weird. To me, that is an identification. An analyst looking at data and saying, 'That does not quite look right' is absolutely identification."*

After an investigation is triggered, threat hunters manually search for threats or use tools to understand the alarms. They employ tools such as Splunk, VirusTotal, or ReliaQuest/GreyMatter to validate whether they deal with threats or false alerts. Threat validation includes further investigations (using additional hypotheses) and may involve inviting other team members to confirm the findings. Threat identification is a process that requires knowledge and experience. P09 emphasized, *"I think it requires more knowledge and keeping up-to-date with stuff. We would discuss it as a team, 'Does this look suspicious? This doesn't seem quite right to me."'*

In addition to team discussions, participants mentioned that they refer back to previous incidents or notes to confirm whether the behavior is normal or if the suspicious pattern has been encountered before. P20 explained, *"The first thing I usually do is look back on my own notes and things and see if I recognize them. If it's a URL or a pattern, I look back on past incidents and any notes I have to see if it's familiar to me to jog my memory. If I can't recall it, then I usually go to open sources first, and secondly, I'll go to places like VirusTotal, input the domains, and see what comes back."*

Take Away. Threat identification and validation are interconnected processes. Threat hunters employ various tools and manually search and validate indicators of compromise. In most cases, validation is a team process.

4.2.4 Remediation and Reporting

Once threats are validated, the remediation and reporting process is initiated. Participants described these processes as interconnected and often addressed them together. Depending on the case, remediation can either be carried out by the threat hunting team or passed on to other teams in the SOC or the client to decide. *"If we do identify threats, and we prove our hypothesis to be correct, we'll inform the customer and move to emergency response."* P22

They emphasized the critical importance of severity and time in remediation and reporting. For severe issues, immediate action is taken, and relevant parties are contacted promptly on how to proceed. In cases where they have permission or authority to act on behalf of the client, they contain the situation. However, if authorization is needed, they would contact relevant people immediately suggesting some remediation steps. *"...depending on the severity, we contact the client; it could be a phone call or an email. Then we check with them and tell them some remediation steps they can take."* P02

Sometimes, the remediation process involves collaboration with other teams, requiring thorough communication. In such cases, participants emphasized the need for detailed reporting to ensure everyone understands what took place, what actions were taken, what was discovered, how the situation was contained, and any further recommendations to prevent future occurrences. *"For the breaches, the idea is pretty much that we wanna give a report, we want to tell a story, we want to be able to say this is how it actually started. So and so got a phishing email, they called the number on the phishing email..."* P05

The reporting process also includes lessons learned. Participants stated that this part of the report includes detailed information about how the detection mechanisms missed the threat or specific steps to configure a system properly. These lessons are valuable for future reference and can provide new intelligence on threats. P13 said, *"As I said, in the lessons learned part, we will be giving them more detailed information about how to enhance their detection analytics to fix where they failed to alert."*

Moreover, participants recognized the value of thorough reporting as it allows them to demonstrate the value of their hunt to the organization. By providing a detailed post-action report, they can show how they addressed deficient posture in the organization, helping prevent potential damage or further threats. *"For me, the hunt starts with that framework of a plan and post-action report to help capture the value because then we can show the organization we have this posture improvement report that came out of our hunt, and we helped to address deficient posture in the organization before it caused damage or allowed damage to occur."* P09

Take Away. Threat validation, remediation, and reporting are interconnected and vital stages of threat hunting. They are crucial for ensuring that threats are effectively addressed, lessons are learned, and necessary actions are taken to enhance the organization's security posture.

4.3 Threat Hunting Challenges

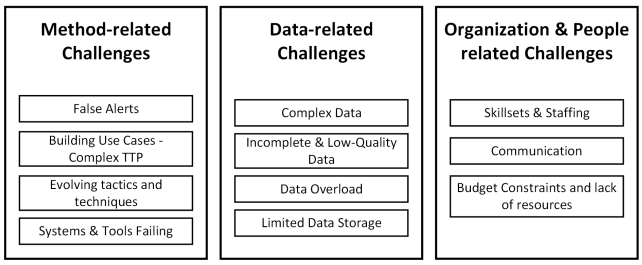

Figure 2: Threat Hunting Challenges regarding Method, Data, Organization and People

Participants revealed various challenges they face as threat hunters. We categorize and present these challenges in three groups as shown in Figure 2

Method-related challenges: These are participants' most common issues while attempting to identify, verify, and remediate threats.

False alerts One common challenge reported by all our participants is dealing with false alerts or false positives. They explained that many hunting activities are prone to trigger alerts that are non-malicious. However, despite being false, participants explained they cannot be ignored and require thorough investigations, which often takes time and need resources. Participants further indicated that several factors maybe contribute to false alerts, such as vague detection rules, new devices joining the network, and internal users using pirated or banned tools or accessing malicious sites. P08 mentioned, *"Yeah, there are many false positives, especially on the PowerShell side. We built a usecase to block PowerShell in the network, and it sometimes flagged it. When we ask about it, we received responses like, 'No, we're not using PowerShell,' but it turned out there's one admin who is very proficient with PowerShell and who used it. We thought, 'Oh, what's happening here?' The analysts said, 'No one's using PowerShell,' but there was a senior guy who was actually using it."*

Moreover, participants pointed out that verifying these anomalies can be particularly challenging, especially when users have flexible working conditions like working from home or during outside normal working hours. P19 further explained that it is even be more complex when the company operates globally; reaching an individual to verify alerts can be even more challenging: *"We're a global company and there are people working in different time zones. If people are working on a Sunday, and they've turned off their phones because they're not technically supposed to be working, trying to catch up, we may not be able to reach them when they've triggered the alerts. Sometimes that's a big challenge."*

Participants also discussed false alerts as a challenge when automating processes. They explained that automation sometimes results in false alerts or causes tools to miss out on detecting threats. They also pointed out that due to the speed at which threats constantly evolve, automation may struggle to keep up with newer threats, leading to countless false negatives. *"False negatives, that's a silent killer. Not understanding that, it's tough...There are dozens of cases that I can think of where I looked at something and was like, hey, I don't see anything and I go back to the business owner and we look at it together and then we're like, hey yes, these things right here, that should never happen. The system should never do that, even though to me they first looked benign."* P14

Building use cases - Complex TTP. Participants (n=5) also discussed building use cases or hypotheses for threat hunting as one of their biggest challenges. They explained that TTPs are complex, making it difficult to formulate and focus on specific usecases for each client. They also stated that the complexity arises from each usecase requiring its own unique data set, which limits the possibility of reusing certain use cases. Some participants specifically emphasized the challenges they face when using the MITRE ATT&CK Framework to build use cases, noting that its broad scope poses difficulties in application. *"The biggest challenge we have is going through all the tactics and identifying what we can look for in particular client's environments because the MITRE ATT&CK Matrix is very broad, there's so much data there that you have to go through and understand what data sources are needed for a particular techniques to focus on."* P08

Furthermore, some participants highlighted the difficulty in determining what to hunt for when they are not even a victim or aware of what is happening outside their companies. They find it challenging to identify what they should be monitoring without any leads, leading them to rely on information from other sources. *"If you are not a victim or an incident responder with access to active attacks, you have to rely on other people to say, 'Oh, we were just attacked by this. Here's the information,' that's different from a SOC where you're the one being attacked. You have the information. We wait on other people to present the information to us. That is a challenge. Trying to find things of interest is always a challenge, but fortunately, there's a lot of security researchers out there who are constantly blogging things, so we get by."* P16

Evolving tactics and techniques. Participants (n=10) mentioned that one challenge in the threat identification process is from the ever-changing threat landscape. They explained that from time to time they encounter evolving threats and actors as technologies change or advance, new threat actors and threats are discovered. Moreover, some participants explained that threat actors also adapt the way they operate, making threats increasingly challenging to understand. *"The biggest challenge would be changing TTPs, when you have groups that change the way they operate. You can't go in knowing that CONTI does this or APT28 does this ... you can't really be used to that much because they could change tactics... Groups change their tactics all the time so that's probably the biggest thing is involving tactics."* P05

Participants commonly described these tactics as a moving target, which some said it is overwhelming and hard to keep up with. They explained that the problem with these constant changes is that threat can sometimes evade their existing detection methods; actors refusing to comply with predictable patterns-*"not playing according to their wishes."* Evolving nature of threats demands continuous changes to approaches and budget to threat hunting. *"Big contenders of challenges, first of all, are adversaries are not rolling over and playing dead for us. They are specifically interested in evading detection. We are dealing with a moving target and that moving target has interest to succeed, the ability to evade our detections which means they are developing evasions."* P09

Systems and Tools failing. We also found that tool performance poses many challenges. Participants (n=7) described various situations in which the tools or system they were using failed to deal with their request. For instance, a tool crashing

because it is dealing with large amounts of data or queries. *"Because we do correlation, some searches take more time and CPUs than others, so we need to optimise so that one search does not crash all the system. We try to do that but the issue is, in the lab we only have few rules and only running when we want them to run, whereas for a big production you have a thousand of rules all running in parallel together. So, when we create a rule we have to make sure that it will fit in the big production without crashing everything else"* P02

> **Take Away.** Building relevant use cases or hypotheses is a big challenge because attacks constantly evolve. Dealing with false alerts, whether positive or negative, poses many challenges, including time and team effort. While tools play a significant role in hunting, they sometimes fall short.

Data-related challenges: These are the most common challenges threat hunters face concerning data for threat-hunting purposes.

Complex data. Participants (n=7) also highlighted that dealing with complex data poses various challenges. While having a lot of data available is considered a good thing, the task of getting these data into a usable format presents many challenges. They explained that logs of various systems come in various formats or containing different bits of information. Furthermore, technological advancements can also lead to changes in logs, which is challenging to keep up with. As P07 explained: *"it's very challenging to keep up with technology and available options, logs often change their format, the way they appear. The way they parse. So, what that mean is that the detection that we burn is based on what the logs looked like a year back. They're not really what it is today."*

To make use of this data effectively, participants explained that they must first get it into a standard and usable format. This involves filtering, normalizing, and transforming it into a format that is appropriate for analysis tools. But, in most cases, these processes require time and effort. P01 said: *"The challenge is to get the data in a good shape. For instance, if you have email logs where you have one that is odd, for this message ID, you have different indicators, the subject, sender, the recipients. Then you have another thing that says the file attachments are this big. You have all these logs, and they all intermingled, so you need to do a lot of work on the data just to get one line of the email. That's a challenge because you need to be like a data scientist and programmer just to get the information you need before you even do your analysis as a security person, so that's definitely a challenge."*

Incomplete and Low-Quality Data. Participants (n=11) also highlighted the significant challenges they face when dealing with incomplete or low-quality data; data lacking critical points or information required for threat-hunting investigations. They said data full of noise or data missing some information is of little value for effective threat hunting. We identified several factors contributing to data quality issues, including the lack of knowledge among data collectors, limited resources for long-term data storage, and excessive noise in the data. Participants noted that data collection decisions, particularly by external companies, can be ill-informed. This can result in unnecessary or incorrect event logging, which are common issues that lead to data not being useful for threat hunting. Moreover, storage limitations, where companies fail or do not have enough resources to retain logs for extended periods was commonly mentioned. Regarding the lack of visibility due to missing data points, P18 stated: *"Another thing that becomes apparent is when you expect the data to be there, but it's not. You should have had 30 days of logs, but when you check, there are only 7. What happened there? I think these are the basics for obtaining data, and some people would call this visibility. I need visibility into these things in order to do it."*

Other participants argued that the low visibility of devices or systems in the logs was sometimes caused by logs collected in various places rather than in one location. Some participants said this challenge is sometimes caused by not having access to relevant systems or devices to collect data. Example of P17 explaining that they had to revisit a device because it was missing from the logs: *"The data in the logs sometimes doesn't give us enough information to go on and hunt, what's presented in front of the analysts is quite hard to use to make a decision. You end up having to spend extra time actually going to the originated device to see what happened. So, we can't pull back PCAPs [Packet capture], things like that, we're solely based on what the logs present to us and they're defined by IS defenders so that can be quite tricky."*

Participants who cited noise in the data as a problem explained that it forces them to spend significant time filtering through irrelevant information. *"You're digging through large data sets you're always going to have limitations and time... You don't get instant results for any query or analysis that you're doing. Again the volume of data that you have to go through is so much data... it's overwhelming sometimes how much you have to dig through ... As you scale the data it just gets harder and longer and more difficult."* P04

Regardless of the specific cause of low data quality or visibility issues, all participants emphasized that missing data or data gaps create blind spots, making it difficult to identify threats (from benign events) or determine the duration of an ongoing attack.

Data overload. Participants(8) also reported that the sheer volume of data they have to deal with can sometimes pose challenges. They explained that going through all the data to identify threats takes time and is complex. Some highlighted that it can be an overwhelming experience which may affect the hunter's ability to spot obvious indicators of compromise. Another challenge mentioned concerning the abundance of

data was querying. Participants explained that having too much data makes querying difficult and time-consuming. We found that failing to promptly and effectively retrieve the necessary data slowed their efforts and made hunting challenging. *"To make sense of the data, we have a lot of it and to get something interesting from it is a big challenge. You end up with loads of results that are useless in the data set. It's hard to filter out new threats. It's very challenging and it takes time to adjust the query to get the right data."* P15

Limited data storage. Some (n=7) face challenges around data storage. They explained that they usually have limited storage capacity, which means they sometimes do not have sufficient data to conduct thorough investigations. Participants also explained that the issue of data storage is challenging because it is also hard to know how much data is needed to be stored just in case it needs to be used for investigations. The participants who conducted external threat hunting stated that most of their clients usually do not keep much data because they do not have the infrastructure to do so. They explained that this leads to challenges when investigating threats or understanding how long the systems have been compromised. *"Acquiring the data is the difficult part because they might not have storage for that stuff. It's ridiculous. The security solutions that are out there are not made to store data, they're basically made to do things with it and then remove it quickly. The problems I've seen, is that people don't think about what happens when you need the forensics? What happens when there's compromise? You need 30 days of logs or 60 days or 180"* P22

> **Take Away.** Threat hunting relies extensively on the availability, usability, and quality of data. However, this crucial aspect presents a significant challenge. The difficulty arises from (1) obtaining the required data for investigations due to poor logging (visibility) and storage practices within organizations, and (2) the complexity and overwhelming nature of the data, making it challenging to analyze with the available tools and/or knowledge.

People and Organizational-related Challenges These include issues around organizational culture and interpersonal skills of individuals. Participants reported facing significant challenges in identifying and recruiting skilled staff, establishing effective communication channels, and managing constraints around budget and resources.

Skillsets and staffing. Participants (n=11) highlighted various challenges related to their staffs' necessary skillset for effective hunting, including technical, communication, and analytical skills. They emphasized that threat hunting requires more than just technical expertise; it demands a specialized set of skills and critical thinking. As a result, they explained that they need to provide training to every new hunter to ensure they possess the right skills for the job, but this process takes time and requires resources. *"Our main challenge is that not a lot of IT people we encounter are well-versed in security and incident management, so we have to give them step-by-step instructions on what to do, and it takes time, and even if you do, sometimes they don't understand. 'Oh, what is happening? Why do we need to do this?' We have to let them understand it, otherwise they are going to make mistakes"* P08

In addition to skillsets, attracting and retaining skilled personnel emerged as another problem. Participants described the difficulty in finding individuals with skillsets that strike the right balance between broad enough for various threats and specific enough for effective threat hunting. Furthermore, retaining staff posed challenges as threat hunting can be demanding, making it crucial to maintain long-term commitment from employees. P02 elaborated on the staffing challenges, and said; *"Yeah. I will start with the people. People is finding people and retaining people especially with Level 1s because they work on shifts, they work at night, then when you work online looking at the logs, again it's a bit big. So, make sure they can see the end of the tunnel. We can keep them interested and they can move on to the next level of analyst."*

Communication. Participants (n=7) also reported that communication within teams, management and clients can sometimes be challenging. Some participants explained that some threat hunters have difficulty communicating threats or risks they find during hunts. Poor communication or unclear reporting protocols (or channels) may lead to other team members underestimating the impact of the threats or the management not understanding what is needed or how to respond. They emphasized the critical importance of communication, especially since they work with various teams (e.g., legal), some of which may not possess the technical expertise to understand and assess cyber attacks. P03 highlighted the significance of effective communication: *"There's no point having threat intelligence if you can't communicate it to someone in the proper way, so someone who is very skilled at reports who can create a lot of information. Communication is quite useful to the people that are working on the board and things like that and who don't understand cyber, presenting the threats to them in a way that they can understand it, that's useful."*

Budget constraints and lack of resources. Participants (n=9) also emphasized the significant challenge posed by budget constraints on security and threat-hunting efforts within organizations. They stated that the lack of budget affected several crucial aspects, including acquiring necessary resources, availability of skilled workforce, dedicated teams, and time allocation. Some participants argued that this is due to the management not understanding the importance of proactive security response. Most participants shared that threat hunting

and security are underfunded, making it difficult to acquire the right equipment for storage or analysis, as it is often expensive. *"Cost is one of the biggest issues because the technologies that companies need are expensive. I've been in threat hunting for almost 20 years one form or another as well as exploited all kinds of stuff, we have to do the best job possible with a lack of information and a lack of technology at the client."* P05

Some participants also associated operational issues like bad performance, time constraints, and lack of dedicated threat-hunting teams with insufficient budgets. The shortage of financial resources often forces threat hunters to perform other duties unrelated to threat hunting because the company does not have enough security personnel. This affected their threat identification performance, ability to learn and tune their threat detecting rules, and response time to alerts and investigations. *"Another [challenge] is having time, being able to dedicate – not just time, but continuous time, where you can continually tune the rules that we have, and actually go back and continually review the results of the rules that we have. So, I would say time is the biggest issue outside of data collection. Time and dedicated man hours to threat hunting. With respect to that, I guess having one person dedicated to threat hunting would definitely be useful but I always say there's a saying, if you give me six hours to cut down a tree I will spend four hours sharpening my axe"* P10

Furthermore, we found that budget constraints posed challenges in fostering a culture of innovation and continuous improvement among threat-hunting teams. Some participants were concerned that low or no budget could hinder analysts' exploration of new techniques and experimental approaches. The lack of allocated time and flexibility for hunting duties affected their ability to stay at the forefront of evolving threats and identify potential security risks effectively.*"The challenge is that our organizations are telling the analysts don't be smart, don't spend the time to learn new techniques, don't spend the time to experiment, don't spend the time to try things that might not work. That's exactly what the organization is telling people when they take away the time allocation from hunting and flexibility. That's the big pressure on us as to why we're not good at [threat] identification."* P09

Participants stated that budget constraints also their clients. They said budget constraints affected what they could do or recommend for their clients. For instance, P04 explained that their clients cannot collect all the necessary data they need due to budget constraints. *"I think the biggest challenge is usually client budgets because you know it's always kind of [affect] the amount of data that goes to the SIEM [because] that's how they get charged by EPS. The more data they send in there, the higher their bill. You know budget constraints seem to be the biggest barrier to collecting the data we really need in order to do the kind of threat hunting that they would want us to do."* P04

Take Away. Threat hunting's effectiveness is intricately tied to the skills and experience of the threat hunters. However, finding and retaining qualified staff in this field presents a significant challenge. Furthermore, threat hunting is frequently underfunded, exacerbating the challenges faced by security teams, like getting the right tools.

4.4 Best Practices Strategies

To address the various challenges, participants shared several strategies they used and practices they perceived to be the most effective in improving threat hunting processes. We only discuss the most reported strategies.

Strategy 1: Re-analysing, Re-tuning, and Collaborating. Firstly, to address false alerts participants emphasized conducting thorough analysis of the cases against historical data to identify patterns or common characteristic of previous attacks. This method helped them distinguish genuine threats from false positives more accurately. Secondly, some explained they constantly fine-tune their approaches; refine detection rules, use cases, and algorithms. Refining these approaches helps in reducing false positives. Participants also highlighted that relying only on rules for identifying threats might lead to false negatives, especially when dealing with new and emerging threats (e.g., zero-days). To overcome this, they randomly conduct further analysis on logs that may have initially passed without triggering alerts. This active approach helps them uncover potential threats that might have been missed by the existing rules or tools. Other participants emphasized the importance of collaboration and shared learning to mitigate false negatives. They explained that when an IoC is missed, and later found, they come together to discuss and understand the reasons behind the oversight. This collective effort helps them identify gaps in their detection capabilities and implement necessary changes to avoid similar false negatives in the future.

Strategy 2: Automating Repetitive Tasks. Other participants reported that automating certain activities helps to scale the search and improve its effectiveness. By streamlining repetitive tasks, they can free some time and focus on other strategic and analytical aspects of threat hunting. Moreover, they stated that automation also helps to ensure consistency and accuracy around data collection and analysis. We also found that automation also help reduce the burden on threat hunters; reduces the risk of errors that might result due to manual analysis of larger datasets.

Strategy 3: Refining data collection strategies. To mitigate issues around data collection, some participants reported that they work on their data collection strategies, identifying and collecting only info that is needed, and also using

efficient methods of collecting and storing logs. Other participants explained that they encourage best practices around data collection and also by following best policies. For instance, some argued for more centralization of data. They reasoned that having all the data in one place improves the overall visibility of the data and the infrastructure being investigated. While others stated that having centralised data was useful for use case generation; they explained that it made use case generation easier as one can clear visibility of what they have and what they do not have.

Strategy 4: Being flexible and Open minded. Participants said one way of making threat hunting easier is not following a rigid and repetitive process. They explained that, as threats constantly evolve, one needs to be creative and find new ways of hunting for threats. Being strict in approach or not adapting the process could lead to missing new or emerging threats. They explained that approaching threat hunting with an open mind however helps to break routines and norms that develop within teams over time. With an open-minded approach, threat hunting teams can promote an environment where fresh ideas and perspectives are valued which may eventually lead to new novel techniques to threat hunting.

Strategy 5: Keeping up with current threats. Some participants emphasized that staying informed about the latest threats is crucial for enhancing threat hunting practices. They recommended providing threat hunters with continuous learning opportunities to keep them updated on current threats and how to identify and respond to them. Other participants suggested that this could be achieved through training and research efforts. While some participants had specific suggestions like having frequent training, others stressed on enhancing the complexity of the training. In addition to training, other participants suggested documenting and reporting new threats as part of the learning and keeping up with new threats.

Strategy 6: Asking for better budget allocation. Almost all the participants discussed budget in one way or another particularly how it can improve threat hunting activities. For example, acquiring tools and organizing and conducting trainings. Participants suggested that having adequate budget allocation is critical to facilitate effective threat hunting activities and enable teams to have access to necessary resources and tools that can detect and mitigate threats.

5 Discussion

Humans, Machines, and Collaborations. Our findings reveal that threat hunting is a multifaceted process that demands creativity, attentiveness, and the utilization of appropriate tools. These results align with existing literature [15, 36, 48, 50], emphasizing the significance of human-machine interaction in hunting. From our results, it is clear that machines have a significant role to play in threat hunting, but alone, without humans, they are limited. For instance, they may struggle to detect zero-day attacks or other new and emerging attacks, which may require human involvement. Our findings also suggest that threat hunting requires dynamic reasoning, such as intuition, creativity, and strategic thinking, which cannot be fully replicated by tools alone. Moreover, like hackers and testers [44], we found that experience plays a significant role in threat hunting. Some threats have been discovered solely because of experience (Tacit knowledge). Also, some hunters have found threats due to their curiosity, personal creativity, and persistence. Future efforts could investigate how these workers could collaborate to build morale, exchange ideas, and bring creativity to the field.

In-House vs. Providing Services. Our sample represent various companies, with some conducting in-house hunting and others outsourcing their services. We observed significant similarities between both groups, particularly in how they apply each method. However, there were a few notable differences (Table 3), for example, reporting. Participants expressed frustrations about reporting while providing services to other companies, highlighting unclear reporting lines than in-house which they believe affect the remediation of identified issues. Regarding challenges, though they face similar issues, the manifested differently. For example, both groups faced challenges with data, but those offering services to outside companies emphasized issues such as unusable data and missing data points. This discrepancy is perhaps unsurprising, as companies typically have more control over their in-house operations compared to external entities.

Lack of standardization. While we categorized threat hunting methods in our paper, in practice, they are borderless, and not one size fits all. Hunters combine them for better output. While this flexibility may be beneficial in some cases, it could also lead to undesirable practices and outcomes. For example, hunters may choose to prioritize certain activities while neglecting others (e.g., skipping pre-planning), which may be critical in the entire threat hunting process. There is a need to standardize these methods to prevent the loss of critical processes and promoting best practices. Moreover, the establishment of industry standards outlining how each threat hunting approach should be executed may lead to greater consistency, and minimization of errors. Furthermore, this could lead to the development of specific training materials to assist practitioners, such as detailed case studies that could be used worldwide. Future work should look into these methods and identify which ones are prevalent in the wild and the activities that should form the base of threat hunting framework.

Beyond Traditional SOC Boundaries. Beyond Traditional SOC Boundaries: Our findings indicate that threat hunting is expanding beyond traditional SOC boundaries. Some participants reported that their threat hunting efforts began outside the SOC, while others mentioned that members of their threat hunting teams had additional responsibilities in their companies and conducted threat hunting outside the SOC. Hunting outside the SOC may have both positive and negative aspects. In some cases, it may democratize threat hunting and engage everyone. However, it may also introduce additional privacy and security risks or require extra measures to be put in place, which might increase costs. Also, during the pandemic, there were discussions about virtual SOCs (or metaverse SOCs), which would enable practitioners to connect to SOCs remotely or integrate several SOCs virtually in real-time. As spatial computing becomes more popular, virtual SOCs are feasible, and threat hunting outside physical SOCs might become common. We believe virtual threat hunting warrants further exploration to determine how it can be achieved securely. Moreover, research should further investigate current practices of threat hunting outside SOC settings and how it can be made effective and secure.

Budget and Staffing. Similar to other works on security workers (e.g., [5, 16, 25]), recruiting and retaining skilled personnel is also a challenge in threat hunting. This is a multifaceted problem, involving low budgets, lack of motivation, excessive responsibilities, and cognitive demands. We believe there is no single solution to these issues, but management should work on certain improvements. For example, removing additional non-hunting responsibilities, as they may indicate a lack of appreciation for proactive security measures. Moreover, this could maximize hunters' time and effort. We also acknowledge that hunters may take on other roles because they see no clear career progression in threat hunting. Consequently, there is a need for clear career paths in threat hunting, so hunters can envision themselves in these roles for the long term. Investing in threat hunting may also address some of these issues; for instance, providing training could ensure an adequate number of personnel and boost team motivation, which is crucial in this field, as highlighted in previous studies [2, 44] on bug hunters. The research community should also emphasize the importance of investing in proactive security rather than relying solely on reactive measures, as this is paramount to the success of threat-hunting initiatives.

6 Conclusion

In this work, we investigated threat hunters' practices in the wild, including who conducts the hunts, how they conduct them, the challenges they face, and the strategies they employ to address these challenges and improve hunting processes. We found that threat-hunting activities are not standardized; various security experts can perform threat-hunting and use different methods based on needs and resources. The challenges they encounter are not just technical but include organizational challenges. Our results not only provide empirical evidence on threat hunters' daily practices but also have the potential to strengthen Cyber Defense Strategies and improve decision-making in SOCs. Future studies could investigate the unique challenges and opportunities for threat hunting in specific areas, such as gaming.

7 Acknowledgement

We thank all the security experts who took part in our interviews, without their time and expertise, the publication of this paper would have not been possible. We would also like to thank the reviewers and shepherd for their valuable feedback to the paper. This work is supported in part by EPSRC CDT TIPS-at-Scale.

References

[1] Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, and Pete Burnap. Towards a framework for measuring the performance of a security operations center analyst. In *Int. conference on cyber security and protection of digital services*, pages 1–8. IEEE, 2020.

[2] Omer Akgul, Taha Eghtesad, Amit Elazari, Omprakash Gnawali, Jens Grossklags, Michelle L Mazurek, Daniel Votipka, and Aron Laszka. Bug hunters' perspectives on the challenges and benefits of the bug bounty ecosystem. In *32nd USENIX Security Symposium.*, 2023.

[3] Olusola Akinrolabu, Ioannis Agrafiotis, and Arnau Erola. The challenge of detecting sophisticated attacks: Insights from soc analysts. In *Proc. of the 13th Int. Conf on Availability, Reliability and Security*, ARES 2018, NY, NY, USA, 2018. Association for Computing Machinery.

[4] Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic. 99% false positives: A qualitative study of SOC analysts' perspectives on security alarms. In *31st USENIX Security Symposium*. USENIX Association, 2022.

[5] Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman. "You've got your nice list of bugs, now what?" vulnerability discovery and management processes in the wild. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[6] Saed Alrabaee, Paria Shirani, Mourad Debbabi, and Lingyu Wang. On the feasibility of malware authorship attribution. In *Foundations and Practice of Security: 9th Int. Symposium, FPS 2016, Québec City, QC, Canada*, pages 256–272. Springer, 2017.

[7] Abdulellah Alsaheel, Yuhong Nan, Shiqing Ma, Le Yu, Gregory Walkup, Z Berkay Celik, Xiangyu Zhang, and Dongyan Xu. Atlas: A sequence-based learning approach for attack investigation. In *USENIX Security Symposium*, pages 3005–3022, 2021.

[8] Louise Axon, Jassim Happa, Alastair Janse van Rensburg, Michael Goldsmith, and Sadie Creese. Sonification to support the monitoring tasks of security operations centres. *IEEE Transactions on Dependable and Secure Computing*, 18(3):1227–1244, 2021.

[9] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[10] Po-Chun Chen, Peng Liu, John Yen, and Tracy Mullen. Experience-based cyber situation recognition using relaxable logic patterns. In *IEEE Int. Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, pages 243–250. IEEE, 2012.

[11] Peter Clay. A modern threat response framework. *Network Security*, 2015(4):5–10, 2015.

[12] Stephanie de Smale, Rik van Dijk, Xander Bouwman, Jeroen van der Ham, and Michel van Eeten. No one drinks from the firehose: How organizations filter and prioritize vulnerability information. In *IEEE Symposium on Security and Privacy (SP)*, 2023.

[13] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. In *Proc. of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1272–1289, 2018.

[14] Feng Dong, Liu Wang, Xu Nie, Fei Shao, Haoyu Wang, Ding Li, Xiapu Luo, and Xusheng Xiao. Distdet: A cost-effective distributed cyber threat detection system.

[15] Anita D'Amico, Laurin Buchanan, Drew Kirkpatrick, and Paul Walczak. Cyber operator perspectives on security visualization. In *Advances in Human Factors in Cybersecurity: AHFE Int Conf on Human Factors in Cybersecurity, Walt Disney World®, Florida, USA*, pages 69–81. Springer, 2016.

[16] Anita D'Amico and Kirsten Whitley. The real work of computer network defense analysts: The analysis roles and processes that transform network data into security situation awareness. In *VizSEC 2007: Proc. of the workshop on visualization for computer security*, pages 19–37. Springer, 2008.

[17] FireEye. Highly evasive attacker leverages solarwinds supply chain to compromise multiple global victims with sunburst backdoor. https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor, 2020. Accessed on May 2023.

[18] Stefan Gast, Jonas Juffinger, Martin Schwarzl, Gururaj Saileshwar, Andreas Kogler, Simone Franza, Markus Köstl, and Daniel Gruss. Squip: Exploiting the scheduler queue contention side channel. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 468–484. IEEE Computer Society, 2022.

[19] Robert S Gutzwiller, Sunny Fugate, Benjamin D Sawyer, and PA Hancock. The human factors of cyber network defense. In *Proc. of the human factors and ergonomics society annual meeting*, number 1. SAGE publications Sage CA: Los Angeles, CA, 2015.

[20] Xinfeng Li1 Xiaoyu Ji, Chen Yan1 Chaohao Li, Yichen Li, Zhenning Zhang, and Weyuan Xu. Learning normality is enough: A software-based mitigation against inaudible voice attacks. 2023.

[21] Barbara Johnstone. *Discourse analysis*. John Wiley & Sons, 2017.

[22] Benjamin A Knott, Vincent F Mancuso, Kevin Bennett, Victor Finomore, Michael McNeese, Jennifer A McKneely, and Maria Beecher. Human factors in cyber warfare: Alternative perspectives. In *Proc. of the Human Factors and Ergonomics Society Annual Meeting*, volume 57. SAGE Publications Sage CA: Los Angeles, CA, 2013.

[23] Piergiorgio Ladisa, Henrik Plate, Matias Martinez, and Olivier Barais. Taxonomy of attacks on open-source software supply chains. *arXiv preprint arXiv:2204.04008*, 2022.

[24] J Richard Landis and Gary G Koch. The measurement of observer agreement for categorical data. *biometrics*, pages 159–174, 1977.

[25] Chanel Macabante, Sherry Wei, and David Schuster. Elements of cyber-cognitive situation awareness in organizations. In *Proc. of the Human Factors and Ergonomics Society Annual Meeting*, volume 63, pages 1624–1628. SAGE Publications Sage CA: Los Angeles, CA, 2019.

[26] Michele Marazzi, Flavien Solt, Patrick Jattke, Kubo Takashi, and Kaveh Razavi. Rega: Scalable rowhammer mitigation with refresh-generating activations. In *44rd IEEE Symposium on Security and Privacy*. IEEE, 2023.

[27] Vasileios Mavroeidis and Audun Jøsang. Data-driven threat hunting using sysmon. In *Proceedings of the 2nd Int. conf on cryptography, security and privacy*, pages 82–88, 2018.

[28] S Naveen, Rami Puzis, and Kumaresan Angappan. Deep learning for threat actor attribution from threat reports. In *2020 4th Int. Conf on Computer, Communication and Signal Processing (ICCCSP)*, pages 1–6. IEEE, 2020.

[29] Lily Hay Newman. Russia's fireeye hack is a statement—but not a catastrophe. https://www.wired.com/story/russia-fireeye-hack-statement-not-catastrophe/, 2020. Accessed on April 2023.

[30] Lorelli S Nowell, Jill M Norris, Deborah E White, and Nancy J Moules. Thematic analysis: Striving to meet the trustworthiness criteria. *Int. journal of qualitative methods*, 16(1):1609406917733847, 2017.

[31] Antonio Pecchia, Domenico Cotroneo, Rajeshwari Ganesan, and Santonu Sarkar. Filtering security alerts for the analysis of a production saas cloud. In *IEEE 7th Int Conference on Utility and Cloud Computing*. IEEE, 2014.

[32] Akalanka Perera, Shanith Rathnayaka, N. D. Perera, W.W. Madushanka, and Amila Nuwan Senarathne. The next gen security operation center. In *2021 6th Int. Conf for Convergence in Technology (I2CT)*, pages 1–9, 2021.

[33] Rami Puzis, Polina Zilberman, and Yuval Elovici. Athafi: Agile threat hunting and forensic investigation. *arXiv preprint arXiv:2003.03663*, 2020.

[34] Sagar Samtani, Ryan Chinn, Hsinchun Chen, and Jay F Nunamaker Jr. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4):1023–1053, 2017.

[35] Jordan Shropshire and Christopher Kadlec. I'm leaving the it field: The impact of stress, job insecurity, and burnout on it professionals. *Int. Journal of Information and Communication Technology Research*, 2(1), 2012.

[36] Xiaokui Shu, Frederico Araujo, Douglas L Schales, Marc Ph Stoecklin, Jiyong Jang, Heqing Huang, and Josyula R Rao. Threat intelligence computing. In *Proc. of the 2018 ACM SIGSAC conference on computer and communications security*, pages 1883–1898, 2018.

[37] Sathya Chandran Sundaramurthy, Alexandru G Bardas, Jacob Case, Xinming Ou, Michael Wesch, John McHugh, and S Raj Rajagopalan. A human capital model for mitigating security analyst burnout. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pages 347–359, 2015.

[38] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G Bardas, and S Raj Rajagopalan. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*, pages 237–251, 2016.

[39] Sathya Chandran Sundaramurthy, Michael Wesch, Xinming Ou, John McHugh, S Raj Rajagopalan, and Alexandru G Bardas. Humans are dynamic - our tools should be too. *IEEE Internet Computing*, 21(3):40–46, 2017.

[40] Joe Tidy. Solarwinds: Why the sunburst hack is so serious. https://www.bbc.co.uk/news/technology-55321643, 2020. Accessed on April 2023.

[41] Swaathi Vetrivel, Veerle Van Harten, Carlos H Gañán, Michel Van Eeten, and Simon Parkin. Examining consumer reviews to understand security and privacy issues in the market of smart home devices. In *32nd USENIX Security Symposium*, 2023.

[42] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 2020.

[43] Daniel Votipka, Seth Rabin, Kristopher Micinski, Jeffrey S Foster, and Michelle L Mazurek. An observational investigation of reverse {Engineers'} processes. In *29th USENIX Security Symposium*, 2020.

[44] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, and Michelle Mazurek. Hackers vs. testers: A comparison of software vulnerability discovery processes. In *IEEE Symposium on Security and Privacy*. IEEE, 2018.

[45] Maurice Weber, Xiaojun Xu, Bojan Karlaš, Ce Zhang, and Bo Li. Rab: Provable robustness against backdoor attacks. *arXiv preprint arXiv:2003.08904*, 2020.

[46] Rodrigo Werlinger, Kasia Muldner, Kirstie Hawkey, and Konstantin Beznosov. Preparation, detection, and analysis: the diagnostic work of it security incident response. *Information Management & Computer Security*, 18(1):26–42, 2010.

[47] Chong Xiang, Alexander Valtchanov, Saeed Mahloujifar, and Prateek Mittal. Objectseeker: Certifiably robust object detection against patch hiding attacks via patch-agnostic masking. 2022.

[48] Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel, and Engin Kirda. Panorama: capturing system-wide information flow for malware detection and analysis. In *Proc. of the 14th ACM conf on Computer and communications security*, pages 116–127, 2007.

[49] Kim Zetter. The untold story of the boldest supply-chain hack ever. https://www.wired.com/story/the-

untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/, 2024. Accessed on May 2024.

[50] Chen Zhong, John Yen, Peng Liu, and Robert F Erbacher. Learning from experts' experience: toward automated cyber security data triage. *IEEE Systems Journal*, 13(1):603–614, 2018.

8 Appendix

8.1 Participants demographics details showing their skills and certifications

Table 2: Participants' skills and certifications

ID	Job Role	Certification(s)
P01	Senior Cybersecurity Analyst	-
P02	Security Consultant	CISSP, CISM, CCSP, GICSP,Fortinet NSE7 Firewall, NSE 7 OT, NSE7 SD WAN. Fortinet NSE5 FortiAnalyzer, NSE5 FortiManager, Fortinet NSE4
P03	Threat Intelligence Analyst	-
P04	Associate Director Threat Hunt	GSIF, GCIH, GCFE, GREM, GMON, GSEC, GPEN
P05	Threat Hunting Team Lead	-
P06	Digital Forensics Specialist	-
P07	SOC Analyst	-
P08	Director for DFIR	CISA, CISM, CISSP, GSE, GIAC x12
P09	Consultant	CISSP, GSEC, GCIA, GCIH, GCFA, GPEN, GMOB, GPYC, GASF, GXPN, GREM
P10	Lead SOC Threat Hunter	SANS (GDAT, GREM), CCNA,Security+, CEH
P11	IT Security Engineer	MTA Sec Fundamentals, Comptia Security+, Comptia CySA+,GIAC, GCIH
P12	SOC Analyst	-
P13	Security Analyst L3 -	-
P14	Program Lead Adv Sec Analytics	GPYC (Python Coder), AWS Security
P15	Threat analyst High school	-
P16	Cybersecurity Technical Specialist	-
P17	SOC Head	-
P18	Security Research Lead	-
P19	Cybersecurity Engineer	-
P20	Lead Cybersecurity Engineer – SOC and Blue Team	GCIH
P21	Manager, Incident Handling	-
P22	Senior Incident Response Consultant	-

8.2 In-house Vs Outsourcing services

8.3 Interview Protocol

Q1. Please tell us about job role/position/level
Q2. Please tell us about your work responsibilities within the company?
Prompt: What do you have to do in your day-to-day job role?
Follow-up: Are you working in a team or individually?
Q3. Could you please tell me about your approach of threat hunting? Prompt: How do you perform threat hunting?

Study Intro: This study is divided into three parts:
1) Data collection 2) Threat Identification 3) Threat Analysis

Data\Log Collection

Aim: To identify and understand the data collection process, various sources of logs and address the challenges linked with the collected data.

Q1. How do you do data collection?
Follow up: Can you tell us about the types of information you collect?
Follow up: How often do you collect logs for analysis?
Q2. How do you get your logging information ? (event logs/ Cyber Threat Intelligence)
Follow up: What are the security devices or methods you use to collect logs? (Source of the logs: Where does the data come from?)
Q3. After collecting all your logs, what do you do next?
Follow up: Do you use any parser or tools for the analysis?
Follow up: How much data do you keep and for how long?
Q4. How do you do log aggregation?
Q5. What kind of challenges do you normally face during data collection?
Q6. How do you think the challenges can be mitigated?
Follow-up: Any suggestion for improvement of the current approach?

Threat Identification

Aim: Gain insight into the practical aspects of threat hunting and identify challenges when extracting threats from extensive event logs. Additionally, explore how analysts cope with uncovering advance threats while encountering the challenges in the data collection process.

Q1. What is your process of hunting the threats/IoCs out of the logs?
Follow-up: What procedure you follow for threat hunting? Is this process automated or manual, or reported?
Follow-up: What sort of tools and techniques do you use?
Follow-up: Do you use any specific tool or technique to identify thyreats?
Q2. How do you prioritise threat and threat validation?
Q3. How is the severity of incidents defined?
Follow-up: Who defines the severity of incidents?
Q4. What kind of challenges do you face during hunting process?
Q5. Threat hunting sometimes includes false alarms, do you also face such false positive alerts?
Follow-up: How do you deal with false positive?
Follow-up: What do you do in case false negative?
Q6. Based on your experience, What can be done to improve the process?

Analysis of Threats:

Aim: Now that you have cultivated a good amount of evidence indicating anomalies, the next step would be, analysis of threats or anomalies. We want to understand the challenges in the threat analysis part.
Note: The person identifying threats also analyzing the threats?

Q1. Once IoCs are identified, how do you analyse the threats?
Prompt: Is this automated or manually?
Follow-up: What challenges do you face while analysing threats?
Follow-up: Do you have labs or simulation environments to test out the particular executable behavior?
Follow-up: What challenges do you face when testing or simulating these behaviours?
Q2. How do you resolve the identified incidents?
Prompt: Once the incident source has been identified, what are actions taken to resolve it?
Follow-up: Is this process based on severity measurements?

Suggestion/Scope of improvement:

Q1. In general, as a person who works in SOCs or deal with identifying threats, what kind of challenges in terms of people, process and technology?
Follow-up: the processes involved in threat hunting?
Follow-up: the technologies used for threat hunting?
Q2. What would you like to change in this whole threat hunting process?
Q3. What tools and technologies do you think can benefit threat hunting process?

8.4 Codebook

Table 3: In-house Vs Outsourcing services

Threat Hunting Process	In-house	Outsourcing services
Pre-hunt Plan	Have deeper knowledge of the network, systems, and data being collected.	Cannot only rely on the client's in-house team, they must learn the systems themselves from scratch
	Have defined communication line so they know who to communicate with during planning about data and devices.	Communication is usually challenging because sometimes it is not clear who oversees what.
	Flexibility to adapt and refine planning	Services are for limited time, and they must follow standardize process.
	Priority issues (analysts may have other work responsibilities)	No priority issues, as this is a dedicated team
	Other local teams and management usually understand scope of the threat hunting	Keeping everyone on the same page as sometime client have different expectations.
Data Collection and Preparation	Have direct access to data/logs makes the process easy	Limited data access and availability because sometimes the logs are not even collected or have been collected but deleted.
	They are usually part of the team that decides which logs needs to be collected and retention period.	Lots of time can be spent on trying to understand logs. Data sometimes is missing
Hunting and Validating	Misunderstanding threats may lead to false negative alerts	Limited access to data and lack of data source results in false negative
Remediation and Reporting	Due to direct access to internal team can promptly respond to threats and start remediation actions	Must wait and be advised on how to respond to threats.
	Can communicate directly with other teams during remediation	Communication can be challenging which may delay the threat response process
	Reporting channels are clear	Reporting can be cumbersome

Table 4: Codebook

Theme	Code	Subcode	Description
Threat Hunting Practices	Threat Hunting Method	Use case-bases Hunting	Participants describing a process of threat hunting that involves building cases or scenarios on possible attack patterns, tactics, techniques, and behaviors that adversaries might employ.
		Intel-based Hunting	Participants explaining they leveraged threat intelligence feeds, open-source intelligence, or vendor-based intelligence for threat hunting.
		Random-based Hunting	Participants describing a method of hunting that is random, possible based on suspicion or knowledge from past events.
	Threat Hunting Process	Pre-hunt Plan	Participants describing a process in which they carefully plan for the hunting process. This includes defining the objectives, scope, choosing network or system logs to investigate, and determining the tools and techniques and who will carry out the search.
		Data Collection and Preparation	Participants describing an approach for collecting data from various sources such as network, tools, and other security devices deployed to collect data within the organizations.
		Hunting and Validating	Participants describing the hunting process and the validation process they follow to identify and verify threats.
		Remediation and Reporting	Participants explaining the process they follow when they have discovered and confirmed a threat or indicator of compromise including how they report it and to whom.
Threat Hunting Challenges	Method-related Challenges	False Alerts	Participants explaining sometimes they receive potential threat alerts that turn out to be false or benign.
		Building Usecases - Complex TTPs	Participants explaining that building use cases requires deep understanding of potential attacks tactic and technique, also highlighting that this is not easy.
		Evolving tactics and techniques	Participants explaining that because threat actors continually adapt and innovate their approaches to bypass security measures and avoid detection, then threat hunting is more challenging.
		System & Tools failing	Participants explaining that systems and tools sometimes fail to provide the services required.
	Data-related Challenges	Complex Data	Participants explaining that data being extracted can come in diverse formats, sometimes even challenging to understand.
		Incomplete & Low-Quality Data	Participants explaining that data is sometimes incomplete or of low quality leading to inaccurate assessments or provide insufficient insights on potential threats
		Data Overload	Participants explaining that identifying threats from large volume of data is complicated and challenging.
		Limited Data Storage	Participants explaining that their challenge is having limited storage which affects their threat hunting efforts.
	Organization & People related Challenges	Skillsets & Staffing	Participants discussing challenges around finding people with the right skills to perform threat hunting.
		Communication	Participants explaining that communication is one of their challenges in threat hunting.
		Budget Constrains & Lack of Resources	Participants explaining the constraints that they have in threat hunting due to lack of budget and having the right resources.
Threat Hunting Strategies	Best Practices Strategies	Re-analysing, Re-tuning, and Collaborating	Participants describing how they address false alerts.
		Automating Repetitive Tasks	Participants explaining how they use automation to address some of the challenges they face.
		Refining data collection strategies	Participants explaining that they continuously refine their data collection strategies to have useful data for threat hunting.
		Being flexible and Open minded	Participants explaining that they approach threat hunting with an open mind to ease the tasks.
		Keeping up with current threats	Participants describing the importance of continuous learning to keep up with threats.
		Asking for better budget allocation	Participants explaining how better budget would solve majority of their challenges.