Cyberspace Vigilante or Security Sleuth: Understanding the Threat Hunter Persona

by

Samantha Hill
B.Sc., University of Victoria, 2022

A Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Computer Science

We acknowledge and respect the Lək̓ʷəŋən (Songhees and Esquimalt) Peoples on whose territory the university stands, and the Lək̓ʷəŋən and W̱SÁNEĆ Peoples whose historical relationships with the land continue to this day.

Cyberspace Vigilante or Security Sleuth: Understanding the Threat Hunter Persona

by

Samantha Hill
B.Sc., University of Victoria, 2022

Supervisory Committee

Dr. Margaret-Anne Storey, Supervisor
(Department of Computer Science)

Dr. Yvonne Coady, Committee Member
(Department of Computer Science)

ABSTRACT

Threat hunters are essential to cybersecurity. Anticipating, identifying, and intercepting potential threats makes threat hunters an indispensable part of an organization's security strategy. Though essential, the human aspects of threat hunting are often overlooked, leaving threat hunters to face difficult challenges in an intense environment. Through a qualitative study, involving interviews with 20 threat hunters, I aimed to better understand who threat hunters are, how they work, and the challenges they face. I identified 17 key dimensions of threat hunters and constructed four unique threat hunter personas that capture the lived experiences of threat hunters. I discuss the findings in the context of the literature, the implications of the novel findings, the adaptability the threat hunting role in response to an evolving threat landscape, the utility and drawbacks of personas for supporting threat hunters, and recommend directions for future work. By providing a comprehensive understanding of the human aspects of threat hunting and humanizing the role, this research lays the foundation for the design of user-centered support tools that will ultimately improve the well-being of threat hunters and cybersecurity strategies as a whole.

Table of Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

I would like to thank:

Dr. Margaret-Anne Storey, thank you for guiding me through this process, for your confidence in me, and always providing me with encouraging words and support in the difficult moments.

The team at OpenText, thank you for your support throughout this project. Your help with recruiting threat hunters and invaluable feedback was so important to the success of this research.

Alessandra, thank you for all your advice, shared struggle, and friendship. Your support on the threat hunting project is irreplaceable.

Threat Hunting Project group, Enrique, Arty, Marcus, Callum, Norman, and David, thank you for all your hard work on this project and for all the support you provided me throughout my time on the project.

Mum and Dad, thank you for your unwavering and unconditional support, I hope this thesis makes you proud.

My friends, Hana, Mekensie, Sofi, and Emma, thank you, seriously could not have done this without all of your support and distractions, love you!

My research presented in this thesis is a contribution to UVic CHISEL group research project in collaboration with OpenText. Research on this project was funded through Mitacs Canada in partnership with OpenText Corporation and through the Natural Sciences and Engineering Research Council of Canada (NSERC)

DEDICATION

For anyone who has ever felt stuck, may we dig ourselves out piece by piece and be proud of the path we build.

Chapter 1

Introduction

Today, cyber threats and attacks are increasing in number, severity, and complexity [29, 28]. In 2023, 2,365 cyber attacks[1] in the United States affected over 300 million victims and the number of data compromises[2] increased by 72% [28]. Organizations that face these attacks have complex networks of interconnected hardware, software, and people that are susceptible to the dynamic threat landscape. They employ security controls such as firewalls, multi-factor authentication, and public education, to protect themselves from cyber attacks and their repercussions.

Threat hunting is a critical role in cybersecurity [20]. Threat hunters monitor how data, systems, and networks are accessed and traversed in order to build hypotheses about potential threats, with the ultimate goal of anticipating, identifying, and intercepting threats to the systems they protect [20, 17, 51]. Many companies today rely on them as the first line of defence in keeping their infrastructure, systems, and users safe [51]. Threat hunters are a vital security control. Without threat hunters as a proactive security control, companies risk incurring, on average, $200,000 dollars per breach [27]. With increasing numbers of cyber threats, it is not sustainable for companies to operate without such a critical control [28, 27].

Like many other roles in cybersecurity, the environment in which threat hunters work is intense and often has them splitting their attention between multiple tasks [20]. 76% of threat hunters still have responsibilities outside of threat hunting leaving only 24% dedicated to threat hunting full time [19]. Threat hunters face information over-

[1]Cyber Attack - "involve compromising an electronic information system using software or computer technology." [28, pp. 39]

[2]Data Compromise – "the overall term used to refer to events where personal information is accessible by unauthorized individuals and/or for unintended purposes. This includes data breaches, data exposures, and data leaks." [28, pp. 4]

load on a daily basis and many of the tools they use exacerbate the fatigue caused by information overload [13]. Factors such as information overload and attention splitting make the threat hunter role highly demanding, cognitively challenging, and exposes threat hunters to an increased risk of burnout [13, 19]. In particular, demanding job tasks, poor work-life balance, low role clarity, and reduced recognition and support from their teams and management contribute to burnout in threat hunters [38]. Burnout can lead to lower performance, decreased well-being, and increased negative effects on mental health in threat hunters, ultimately leading to high turnover, increased risk of security breaches and loss of skilled professionals [40, 38].

Threat hunting is also a very new job title in the field of cybersecurity. In 2019 the SysAdmin, Audit, Network and Security (SANS) institute reported that "threat hunting is still very much in its infancy" [20, pp. 2]. Since the role is new, the tasks associated with the title "threat hunter" still overlap with other job titles in cybersecurity such as "Security Operation Center (SOC) Analysts" or "Security Analyst".

Since 2019 much of the literature related to threat hunting is comprised of white papers and technical reports with a technical focus on tools and processes [20, 26]. Organizations have been more focused on improving Security Information and Event Management (SIEM) tools and putting in place sophisticated processes than on understanding and improving the experiences of threat hunters [20]. Limited research has explored understanding the humans behind the work of threat hunters [20, 26]. However, the 2023 SANS report states that threat hunters are "crying out for more training, education, and support from management" [19, pp. 2]. Some researchers have studied the implications of technology and processes on the threat hunter experience and their effectiveness [40, 20, 38], but much of this work is based on stale assumptions that do not account for the emergent nature and increasing demands of the role.

Despite the critical nature and importance of the threat hunting role, it is a role that is not well understood or supported. What is not known from the literature are the personal attributes and characteristics of threat hunters. The threat hunting community, both academic and professional, lack insights on who threat hunters are, their backgrounds, and their working practices. These insights are critical for providing them with better supports for their work.

One way to capture and document the human and social characteristics of threat hunters is to create "personas". Personas are a well-cited tool used to develop understanding of the primary attributes of user groups [24, 9, 23, 45, 8]. Personas can be

used to step into the minds of users and facilitate the user-centered design of tools that better support their needs. This is especially important for overcoming the ego-centric intuition fallacy, the idea that what is true for the designer must also be true for others [45, 30]. Personas are often constructed from user characteristics called "dimensions" [21, 45, 24], so understanding who they are, how they work, and what challenges they face is essential. Equipped with a better understanding of who threat hunters are, researchers, threat hunters, and organizations can collaborate to build better support tools that serve the unique cognitive needs of threat hunters.

1.1 Research Goal, Questions and Contributions

The **goal** of my research is to understand threat hunters, who they are, how they work, and the challenges they face, in order to encourage further collaboration between researchers, threat hunters, and industry partners and inspire action towards building towards building better tools that support the needs of threat hunters.

1.1.1 Research Questions

In order to understand threat hunters, my research team and I (team member roles and contributions can be found in Appendix A) conducted 20 interviews with threat hunters across the globe, analyzed their responses using thematic analysis, and created personas that embody the characteristics of the threat hunters we interviewed.

To achieve the goal of this study I pose the following three **research questions**:

RQ1. Who are threat hunters?

RQ2. How do threat hunters work?

RQ3. What challenges do threat hunters face?

1.1.2 Contributions

The **contributions** of this thesis are:

Contribution 1: A description of who threat hunters are and how they work.

Contribution 2: A description of the challenges threat hunters face.

Contribution 3: A set of 17 dimensions of threat hunters.

Contribution 4: A set of four distinct threat hunter personas.

Contribution 5: Recommendations for future work and how to use the findings of this work.

The findings and contributions of this research are intended to be used as a foundation for developing cognitive support tools that address the challenges faced by threat hunters.

1.2 Thesis Structure

To elaborate these contributions, answer the research questions, and meet the goals of my research I will describe the qualitative study my research team and I conducted (Appendix A), present the findings, and discuss the implications of the results using the following structure:

Chapter 2–Background and Related Work: presents background information and related work on what is already known about who threat hunters are, how they work and the challenges they face, and introduces personas as tools for design and how they are currently used in cybersecurity and threat hunting.

Chapter 3–Methodology: describes the study design and methods used to investigate the research questions.

Chapter 4 – Findings: presents the findings, organized by research question, from the study conducted.

Chapter 5 – Personas: presents the personas and threat hunting dimensions that emerged from the study conducted.

Chapter 6 – Discussion: discusses the findings in the context of the literature, the implications of the novel findings, the affects of the dynamic threat landscape, the benefits and drawbacks of personas, and the assessment of the validity of the study conducted.

Chapter 7 – Conclusion: provides the conclusions of the study.

Chapter 2

Background and Related Work

Threat hunting is a critical role in cybersecurity [20]. However, the literature surrounding this role is primarily comprised of industry white papers, research with a highly technical perspective, or research with a focus on threat actors and the public. There is little focus on the socio-cognitive aspects of threat hunting. Personas are a useful tool that are used to summarize socio-cognitive needs of software users. However, the use of personas in cybersecurity for understanding threat hunters is sparsely explored by existing research. In the following sections I will review what is known about threat hunters (Section 2.1) and what is known about the use of personas in the cybersecurity context (Section 2.2).

2.1 What Do We Already Know About Threat Hunting?

In this section, I summarize what is known about the role of threat hunting. I briefly describe the existing literature related to the workflows (Section 2.1.1), tools (Section 2.1.2), information resources (Section 2.1.3), skills and characteristics (Section 2.1.4), and collaboration (Section 2.1.5) in threat hunting. In each section, I also elaborate on some of the related challenges threat hunters are known to be facing as described in the literature.

2.1.1 Workflows - Tasks, Processes, and Strategies

Threat hunting is a role primarily dedicated to the active defence of threats within a system [31]. Active defence is defined by Lee and Lee as "the process of analysts monitoring for, responding to, and learning from adversaries internal to the network" [31, pp. 4]. Threat hunters hunt by anticipating, identifying, understanding, intercepting, and preventing potential threats and threat actors [17, 51, 20]. They use their domain expertise and experience to extract anomalous behaviours in massive datasets of system and network telemetry [51, 17]. Following a hypothesis-driven, iterative process, threat hunters first triage and prioritize leads that build the hypotheses, then work to disprove, validate, or refine them [20]. Examples of daily tasks for threat hunters include reviewing the logs from the previous night, "scanning the Internet for news of the latest attacks, vulnerabilities, and IDS signature updates" [22, pp. 342], and updating the intrusion detection signatures [22]. They also respond to anomalies and occasionally do incident response [42]. Additionally, for threat hunters to anticipate potential threats, they develop hunting expertise and build experience [22, 20, 51].

Many threat hunting tasks overlap with other roles such as *security operations center (SOC) analyst*, *security analyst*, or even *threat intelligence analyst*. Threat hunters' attention is often demanded by many tasks at the same time and they struggle to cope with context switching between tasks [17, 53]. This challenge is exacerbated by the copious amounts of data generated by their tools. As Endsley and Garland state "more data does not equal more information" [14, Ch. 1, pp. 4]. Information overload is detrimental to the productivity, effectiveness, and decision making capabilities of threat hunters [40, 38]. Threat hunters are also relying on their memory in the process of combining information, interpreting it, and making predictions to support critical decision making [14]. Information overload and stress impact threat hunters' memory [40, 38], ultimately reducing their capacity to make effective decisions.

Situational awareness is another important strategy for threat hunters that supports critical decision making and the anticipation of threats [14, 17]. Situational awareness is the cycle of gathering information to develop a sense of what is happening in an environment, including the cyber landscape [14, 17]. Information overload is also a challenge for threat hunters as it impedes the development of good situational awareness [14].

To support these key tasks and strategies, and standardize the methodologies

used to threat hunt, frameworks and processes have been introduced into threat hunting [35]. Maxam defines frameworks as a way to organize information related to threat hunting and processes as a way to organize threat hunting tasks over time [35]. Using Maxam's definitions, some of the frameworks that exist include the MITRE ATT&CK framework, Pyramid of Pain, and Cyber Kill Chain. Other types of frameworks for critical decision making have been adopted from other areas such as Boyd's Observe, Orient, Decide, Act (OODA) loop, adopted from military operations research [5]. Processes such as van Os *et al.*'s Targeted Hunting integrating Threat Intelligence (TaHiTI) methodology [52], Maxam's TH process diagram [35], and Gunter and Seitz's Threat Hunt Model [25] have started to be used more and more [18].

The existing literature focuses on concrete tasks associated with finding and eliminating threats. There has been a small shift in the industry towards standardized methodologies. However, the focus of these frameworks and processes are on the technical capabilities of the tools. There is still a need for more research focused on the lived experiences of threat hunters, what cognitive processes they use and what makes their work difficult.

2.1.2 Tools

Day to day, threat hunters use an array of different tools. Log viewers, threat detection systems, malware analysis platforms, software center configuration management tools, and command line-based utilities are some examples [17]. Security analytic systems and intrusion detection systems (IDS) provide telemetry and analysis capabilities to threat hunters [7, 42]. Alerting and reporting tools provide notification of suspicious network activity and potential threats [20, 53]. Unmet tooling needs currently include a need for tools to provide more comprehensive data [20], a need to keep humans in the loop with automated tools [4], and a need to improve data analysis metrics [51]. Additionally, there are few tools available that support building situational awareness and the existing tools that do support building situational awareness still need to be more dynamic (updated in real-time) and scalable [16]. Some recognition in the literature exists surrounding the use of less technical tools, such as communication channels (email, text, video chat, and phone calls), whiteboards, and source control repositories [22, 53, 51]. However, there is a lack of focus on the human aspects of threat hunting, especially when it comes to tools that support non-technical aspects of the role such as communication, situational awareness, and memory.

Security Information and Event Management (SIEM) tools are the primary tool used by threat hunters to collect and interpret data [17, 42, 20, 51]. SIEM tools monitor network data for anomalous behaviours, alerting when those behaviours are detected, and generating a report detailing the the severity and count of the event [33]. Contemporary SIEM systems use Artificial Intelligence (AI) and Machine Learning (ML) such as User and Entity Behaviour Analytics (UEBA)[1], to identify threats [43]. Shaukat *et al.* describe how AI based systems perform better than less automated tools when it comes down to the detection error rate, predicting attacks correctly, and counting false positives[46]. Despite their capabilities, these systems have certain drawbacks. As Lee and Lee state, "threats are human" [31, pp. 2] because adversaries are human. Threats are therefore inherently unpredictable and AI and ML algorithms still generate false positives because they cannot always account for all the variables introduced by human actions [46]. Consequentially, human oversight remains a key countermeasure for unique attack techniques from adversaries [4].

2.1.3 Information Resources

There is little academic research on how threat hunters use information resources. However, the grey literature uncovers some of the types of resources threat hunters use including blogs (from vendors and independent), commercial intelligence providers (third party), internal research, OSINT providers, government, and industry peers [18]. The 2023 SANS report showed that most threat intelligence is provided from third-party sources [19] and the 2024 report confirms that the primary sources of information that threat hunters use to stay up to date on attacker techniques are vendor blogs and papers [18]. Fuchs and Lemon further describe how understanding who created the content of these resources is critical and must be trusted [18]. They argue that even though vendors are trustworthy they may provide intelligence with bias [18]. Both industry and academia have a need for a better understanding of where threat hunters are going to find information, who is providing this information, and how trustworthy these sources are.

[1] AI and ML based SIEM tools from companies including: Elastic, Exabeam, LogRhythm, and IBM QRadar

2.1.4 Skills and Characteristics

Skills required for threat hunting include general analysis and forensic capabilities for logs, networks, endpoints, malware, memory, and threat intelligence [20, 51]. Understanding what typical network communication, activity, and behaviour look like is a critical skill [20, 51]. For instance, familiarity with typical endpoint user behaviour and application behaviour is key to spotting abnormal and suspicious behaviour [51]. Developing a strong investigative instinct is also vital for threat hunters and is honed over time [20]. While the literature predominantly addresses technical skills, other abilities and characteristics such as communication, curiosity, and passion are equally important and warrant further exploration [22, 51, 31]. There is a need to deepen the understanding of the non-technical skills and characteristics threat hunters have.

2.1.5 Collaboration

Within organizations, threat hunters work alongside stakeholders such as fellow threat hunters, security operations center (SOC) teams, incident response teams, IT specialists, human resources departments, legal departments, managers, and executives [20, 53]. Externally, they engage with security technology vendors, external IT firms, external experts, and end-users [53]. Nevertheless, there is a recognized gap in the research related to how this collaboration is happening between threat hunters and what tool supports for collaboration exist [20, 53, 19]. Prior research has identified some challenges that threat hunters face at the organizational level, such as a lack of security culture, security not being a core part of the business, lack of involvement from senior leadership, or distributed IT management [53, 19]. Moreover, collaboration challenges related to situational awareness tools, and breakdowns in communication between team members [26] have been described. However, there is a need to study the behavioural, cognitive, and collaborative aspects of threat hunters that are currently underserved by the literature [20].

2.2 Personas in Cybersecurity

Supporting threat hunters is increasingly important because they face high-pressure tasks and there is a shortage of skilled practitioners. Developing better tools can help alleviate some of their challenges and capturing and understanding the lived

experiences of threat hunters in these high-pressure roles is critical to improving security as a whole.

Personas are a widely used tool in user-centred design [24, 3, 45, 8] that remind us as researchers, designers, and developers that the users we service are human. According to Goodwin, personas serve as "archetypes" that are used to "encapsulate and explain the most critical behavioral data in a way that designers and stakeholders can understand, remember, and relate to" [23, Ch. 11, pp. 229]. The universal nature of personas is essential for the collaborative design of tools, they allow designers and users to build a shared understanding of the human experience the tools are aiming to capture.

However, personas are not without some limitations. Since personas are archetypes [23] they can be abstract, impersonal [34], or promote stereotypes [8] if not created with consideration for the population they represent. Efforts can be made during the persona creation process to incorporate details from the users on which they are based, making the personas more personalized and concrete. For example, including quotes from real people as part of the personas or including data from user studies with personas should be considered. Furthermore, because personas are abstract, they can perpetuate stereotypes, especially related to gender [8]. Designing diverse personas that reflect the diversity of the users they represent and promote increased diversity is important. Personas are often created using qualitative methods that involve user studies [23, 44] which presents other limitations such as scalability, cost, and becoming obsolete over time (expiring) [44]. These limitations are not always solved by adjusting how we create personas. However, creating highly customizable personas, as suggested by Burnett *et al.*, allows for personas to be adjusted based on the context in which they are used [8].

Despite these limitations, personas in cybersecurity have been used to understand both end users and attackers in the context of cybersecurity systems [37, 12]. For example, Morrison *et al.* developed personas of older adults to aid in the creation of security solutions [37]. They used their qualitative data to construct the common characteristics of older adults to inform their personas [37]. On the other hand, Dev, Rashidi, and Garg explored attacker personas to create customizable privacy models for threat categorization and interception [12]. These personas were used by security practitioners to understand the patterns of threat actors [12]. Another study by Sander and Hailper concentrated on cybersecurity professionals [45]. They created five personas for users of Threat Information Sharing Platforms (TISP) to

create design requirements for new and better TISPs. Using ethnographic methods and interviews, they derived patterns and observations that formed their personas. These studies illustrate the use of personas in cybersecurity and show the value and richness personas bring to designing better tools. However, there is a lack of research focused on understanding the threat hunter role through the development of meaningful personas that support the improvement of threat hunting tools. Therefore, my research focuses on closing this gap by developing personas that capture who threat hunters are and their needs.

Chapter 3

Methodology

My goal was to understand who threat hunters are and to learn about how they use their tools, what their workflows look like, what tasks they complete, and what challenges they face. My team of researchers and I (Appendix A) conducted semi-structured interviews with 20 threat hunters that resulted in the elucidation of 17 dimensions of threat hunters and the construction of four threat hunter personas. The methodology we used for this research is visualized in Figure 3.1 described in the following sections: industry partnership (Section 3.1), interviews (Section 3.2), data analysis (Section 3.3), and persona creation (Section 3.4). The roles that each researcher performed is described in Appendix A. The study protocol was reviewed and approved by the University human research ethics board, ethics protocol number **21-0601** (certificate of approval can be found in Appendix C).

3.1 Industry Partnership

My work was conducted in partnership with OpenText, a global market leader for information management that offers cybersecurity consulting and technology services, including "an advanced threat-detection tool that uses user entity behavior analytics (UEBA) and 100%-online, unsupervised machine learning (ML) to detect behavioral anomalies across the organization and empower threat hunters" [1]. The team at OpenText provided validation and feedback at many stages of the study, supported the recruitment process, and provided the incentives for the interview participants. OpenText Corporation, NSERC Alliance, and Mitacs Canada provided financial support for this project.

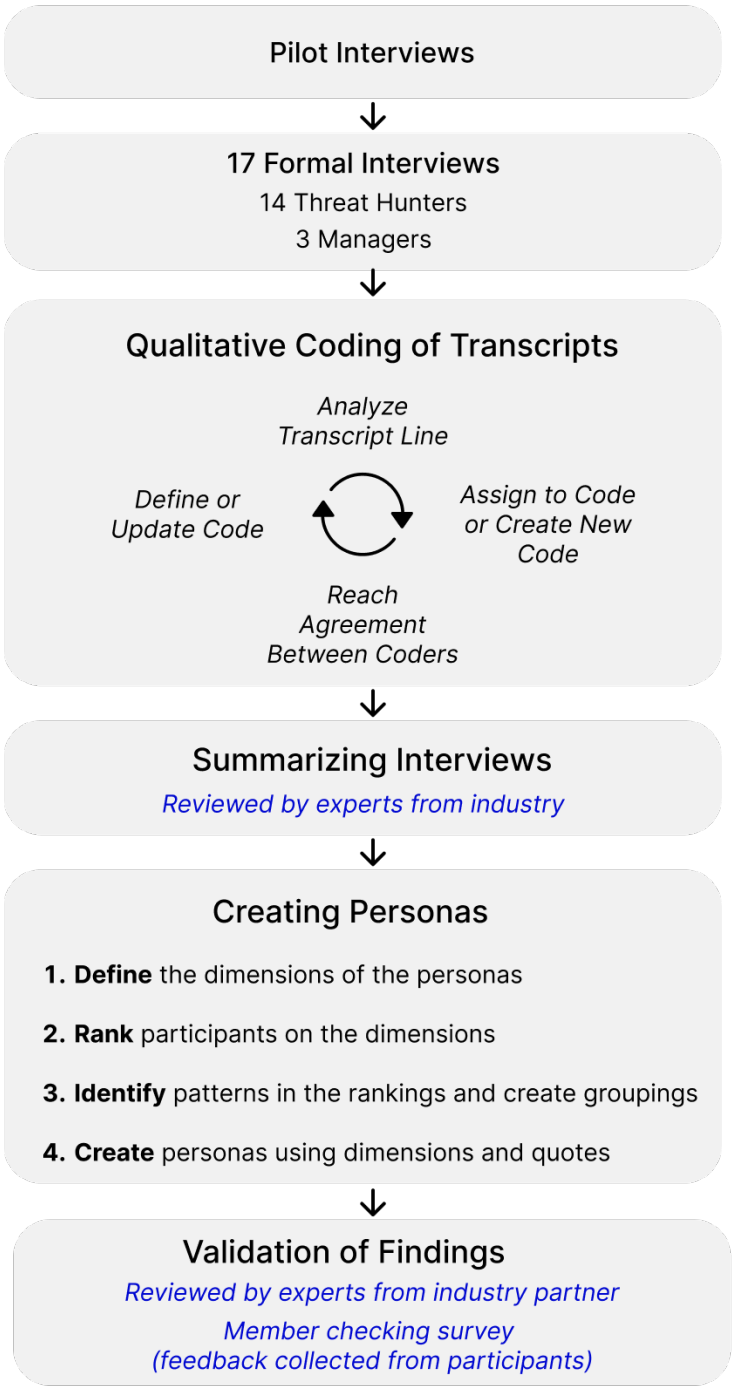


Figure 3.1: Workflow of the methodology

3.2 Interviews

Given the difficult nature of recruiting security professionals who are working in a fast-paced, high-pressure, and time-pressured environment where information sharing is done rarely and cautiously [49], we carefully constructed our study design to ensure a level of trust was fostered between the researchers and participants.

3.2.1 Protocol

The interview questions were created by an experienced researcher team member (Appendix A) who began by conducting a literature review of previous studies related to threat hunting. Through this review, some categories of what made up the role of threat hunting emerged and a gap in the literature related to the behavioural aspects of threat hunting was identified. The categories that emerged from the literature review were used to structure the interview questions. This researcher used their previous experience in conducting interview studies in cybersecurity and the main findings of the studies from the literature review, to create the questions. The initial script was then reviewed by myself, another researcher and the team at OpenText to validate the correctness, quality, and estimated length of the protocol before being used in the pilot studies. Any questions deemed not useful or unclear by the reviewers (myself, another researcher, and OpenText team) were omitted or re-worded for clarity.

3.2.2 Participant Recruitment

Our initial recruitment for the pilot interviews was done in collaboration with our industry partner. We provided OpenText the recruitment criterion that the threat hunters they recruit are security threat hunters who have at least two years of professional experience (professional experience in security or related area). The team at OpenText provided connections with six threat hunters from within their organization or a personal contact of a team member. Three we interviewed in the pilot sessions, and three we recruited for the formal interviews. Data from one participant from the first three formal interviews was discarded because they did not work as a threat hunter.

We used LinkedIn as the primary tool to support the recruitment process for the remaining participants. First, we posted the study invitation (Appendix B) on

LinkedIn to recruit some initial participants and initially we received over 40 responses. We completed one interview from this set of invitations. However, we found that the answers provided were vague and indicative of fraudulent behaviour (i.e., the participant opted not to divulge details of their workflow or experience and could not provide any reliable proof of threat hunting experience). Due to this unforeseen issue, we decided to change the recruitment approach.

Ultimately, we decided to recruit participants by searching for threat hunters and reaching out to them directly. We did a comprehensive search on LinkedIn, targeting individuals from 18 different countries with "threat hunter" in their job titles. This search yielded 1,991 relevant profiles. Sifting through the first 196 profiles allowed us to develop the loose selection criteria based on how complete the profile was (i.e., Did they include their recent work history? Is threat hunting their current or very recent role?) and their work experience (security related experience, and threat hunting experience). Given these criteria, we extended participation invitations to 104 individuals, of which eight agreed to our interviews. The response rate was as expected, given the demanding nature of the role of threat hunting [49]. In addition to the LinkedIn invitations, we also employed some convenience sampling [15]. We leveraged the personal professional networks from participants we already interviewed.

The participants completed a demographic survey that also included the consent form (Appendix B). We collected consent and demographic information verbally from pilot interview participants and the first two formal participants (P1 and P2). Participants from within the partner organization voluntarily participated in the interviews as a part of their work day and participants outside of the industry partner organization that completed the interview were offered 100 US dollars as an incentive. Recruitment took place in parallel with interviews was driven by reaching saturation in the coding process described in the next sections. We concluded recruiting new participants when we reached theoretical saturation of the data. In total, our final pool of interviewees comprised 17 threat hunting professionals (not including the three pilot interview participants).

3.2.3 Pilot Interviews

Two other researchers and I (Appendix A) conducted the pilot interviews with the primary goal of gathering feedback to enhance the interview questions. Following each pilot interview, participant input and experiences were carefully assessed to determine

the most relevant questions, with a focus on streamlining interviews to encompass essential information while minimizing duration. For example, if a participant seemed to not understand a question, we re-worded the question to clarify. As a result of the pilot phase, the alterations made to the interview script made it more balanced, clear, and comprehensive. Additionally, these changes and the practice interviews helped us to reduce the length of the protocol to ensure that our research was not impeding on the threat hunter's busy schedules as recommended by Sundaramurthy *et al.* [49]

3.2.4 Interviews

We conducted the 17 semi-structured online interviews via Zoom, with each interview lasting around 70 minutes. The participants completed the pre-interview survey to confirm their informed consent (Appendix B). The final interview script had 52 questions (Appendix D). Each interview involved two roles: the interviewer and the note-taker (the full description of who completed the roles can be found in Appendix A). The notes taken by researchers were mainly focused on capturing any key or new narratives and experiences of the participant to aid the coding process that followed. To stimulate richer discussion with participants, we encouraged participants to share recent encounters with security incidents and asked follow-up questions to elicit detailed responses.

We organized the interviews into sets of two or three to facilitate iterative segmented analysis (see Appendix A for role breakdown). We continued conducting interviews until achieving theoretical saturation, a concept elaborated by Strauss and Corbin [48], indicating the point at which sampling should cease because no more new information has emerged. Saturation in this study was driven by the coding process, once no new codes were emerging from the analysis, the recruitment of new participants stopped. We reached theoretical saturation after completing 17 interviews with threat hunting professionals. The recorded audio from each interview was transcribed using OpenAI's *Whisper*[1], then anonymized, and finally formatted into an Excel sheet for analysis.

[1]Whisper: `https://huggingface.co/openai/whisper-medium.en`

3.3 Data Analysis

The thematic analysis process was inspired by the inductive coding approach described by Cruzes and Dyba [11]. The process started with deductive [2] coding using a set of predefined codes derived from the interview questions (Appendix D). Then as coding continued, inductive [3] coding was used to update the codebook with new categories and codes [6].

The first two interviews were independently coded by myself and one other researcher (Appendix A) and were followed by multiple agreement sessions aimed at progressively constructing a cohesive codebook and assessing inter-coder agreement. The agreement sessions were conducted by going through both sets of codes created independently by each researcher, then when conflicting codes or new codes arose, we discussed the definitions and assignment of those codes. There were three possible outcomes for this: (1) one of the assigned codes was selected (no definitions updated), (2) one of the codes was selected and its definition was updated, or (3) an entirely new code was created and defined in the codebook.

After the first two interviews were coded, the remaining interviews were coded independently by me and one other researcher (Appendix A), while noting any codes we were unsure of or any new codes that emerged. We held agreement sessions to review any snippets of the transcripts that were unclear for coding and to review and confirm new codes that were added to the codebook. This process ensured that we had ongoing coder agreement and that we reduced coder bias as much as possible.

This process was repeated until saturation of the data was reached [48]. We evaluated the saturation of our data after each set of interviews was coded by checking if any new codes were added, any of the code definitions changed, or any new concepts emerged within the codes [10]. Once these criteria were met, the recruitment and interviewing of participants concluded.

After completing the thematic analysis, we validated the findings through member checking with study participants, as per the methodology outlined by Miles and Huberman [36], to validate the data and to ensure that we had captured information accurately. A technical report was disseminated to all participants by email and shared via LinkedIn to solicit informal feedback [4]. We used two member checking surveys to validate the findings of the technical report and the personas.

[2] coding using a set of predefined codes and fitting the data to the codebook [11]

[3] coding from scratch using no guides, letting all the codes emerge from the data [11]

[4] The technical report can be found at this link: `http://hdl.handle.net/1828/15969`

The first member checking survey (Appendix E) was a short anonymous post-interview survey that requested general feedback from participants. The survey included questions asking participants to indicate which findings resonate with them the most, if any of the findings surprised them, which persona they most closely identified with, and how they found the interview experience overall. The second member checking survey (Appendix E) presented each of the personas and asked participants to anonymously indicate how much they identified with each persona and which persona they identified with most. This second survey was used to validate the personas we derived and was created and disseminated to participants to encourage more engagement after a low response rate to the first survey. Additionally, validation was provided by experts at OpenText. The final report was shared with the team at OpenText and discussions with them in monthly meetings provided the necessary feedback for validating the personas. The feedback received from both participants and OpenText was reviewed ensure the accurate interpretation of qualitative data gathered from the interviews.

3.4 Constructing Personas

Building personas is an art that practitioners [21, 50] and researchers [23] alike, have developed methodologies for. Studies, such as those by Morrison *et al.* [37] and Burnett *et al.* [8], have used the concept of dimensions to create personas. Dimensions are key characteristics that emerge from participant data. In this study, I extracted the dimensions from the interview data. The dimensions can be mapped to the themes from the codebook and summarized findings. Dimensions can be either categorical (binary choice of values similar to a multiple choice) or continuous (values on a spectrum in between two extremes, more than a binary choice). A preliminary list of dimensions was evaluated in thorough discussions with other researchers and the industry partner team at OpenText. From those discussions, the most relevant dimensions for threat hunters and cognitive support tools were carefully selected to shape the personas.

Inspired by the approaches proposed by Goodwin [23], the Fluid Project [50] and Goltz [21], I used the idea that ranking each participant on a scale for each of the continuous dimensions would identify patterns [23, 50, 21]. Any patterns that emerge from this process are considered to be a grouping of characteristics that can be converted into a persona. This is a subjective process that I grounded in the

findings and the codebook.

After ranking each participant on the continuous dimensions based on the responses they provided in the interviews, I compared the patterns between participants to identify any potential groupings that could inform the personas. To do that, I first evaluated which participants were the most similar by counting the number of matching dimension rankings each pair of participants had. Secondly, I evaluated the most dissimilar participants by looking at the maximum difference in ranking between each pair of participants. Finally, to visually assess if there were any natural groupings or patterns across the participants, I created radar graphs (see Chapter 4). I made one graph of all the participants and one graph with four groups of participants created based on the similarity analysis I had done in the previous steps.

Using results for this more quantitative approach coupled with the insights from the data, I built the four personas. Specifically, I used the graph with the four groups of participants to determine the four types of threat hunter personas I would make. I assigned the dimension rankings for each persona based on the average for the group of participants. In the cases where the characteristics were similar for all four personas, I intentionally exaggerated the rankings of some dimensions so that overall the four personas were distinct. My experience of running the interviews gave me a strong understanding of what participants had shared. This helped guide my interpretation of the patterns, as well as allowed me to form the personas using my judgment that was grounded in the data.

In addition to the dimensions, other elements such as, a photo, a tagline, demographic information, and quotes were included, following the recommendations from the literature on persona development [23, 50, 21]. Goodwin [23] and Goltz [21] highlight the importance of using a narrative tone in the description of the persona and the use of quotes to make the personas more human. Additionally, Goodwin [23] explains that photos should be realistic and appear to exist in an environment that is contextually appropriate for the role of the persona. Finally, through feedback discussions with the team at OpenText and through the two member-checking surveys (see Appendix E) sent to participants, the final set of personas were validated.

I decided on creating four personas because this number of personas affords the breadth and detail needed to encompass the diverse characteristics of the main types of threat hunter while still providing distinct characteristics that make the personas identifiable [23]. Personas have some notable limitations including perpetuating stereotypes or biases [8], being difficult to scale [44], and becoming obsolete (ex-

piring) [44]. In the process of creating these personas, I made the effort to reduce stereotypes and biases by creating diverse personas whose identity attributes such as gender, ethnicity, and age were varied. To address the other limitations of scale and expiration (the proclivity to become obsolete), I created a template of the personas to allow for others to customize and expand on this work, echoing Burnett *et al.*'s call for customizability in personas [8]. Further discussion of the benefits and limitations of personas and how I mitigated them in this study can be found in Section 6.4.

Chapter 4

Findings

In this chapter, I present the rich findings of the interviews and qualitative coding. I summarize the findings to illustrate the demographics of the participants (Section 4.2) and to answer each of the research questions: RQ1 – Who are threat hunters? (Section 4.3), RQ2 – How do threat hunters work? (Section 4.4), and RQ3 – What challenges do threat hunters face? (Section 4.5). The summary I provide in this chapter contains the highlights of the most frequently reported and most interesting findings. For a more in-depth set of the results please consult the technical report published here: `http://hdl.handle.net/1828/15969`. The dimensions and the personas are presented later in Chapter 5.

4.1 Results of the Qualitative Coding

The interviews and qualitative coding I conducted with three other researchers (see Appendix A), yielded over 20 hours of transcribed conversations with threat hunters and 13 categories that summarize 54 codes. All 13 categories: *Experience*, *Environment*, *Work Flow*, *Skills*, *Improvements*, *Tasks*, *Collaboration*, *Tooling*, *Positives*, *Resources*, *Challenges*, *Identity*, and *Mistake*, and all 54 codes are represented in Figure 4.1. Figure 4.1 also shows how each of the categories of codes and the codes are related to one another. All the categories are parent nodes to the codes and the codes are the leaf nodes of the diagram. Some codes are linked to one another when one directly influence another. For example, *Interruptions* are linked to *Workflows* because interruptions to a threat hunters workday affects their workflow. The rules of coding and relationships of the interconnected codes and categories are outlined in

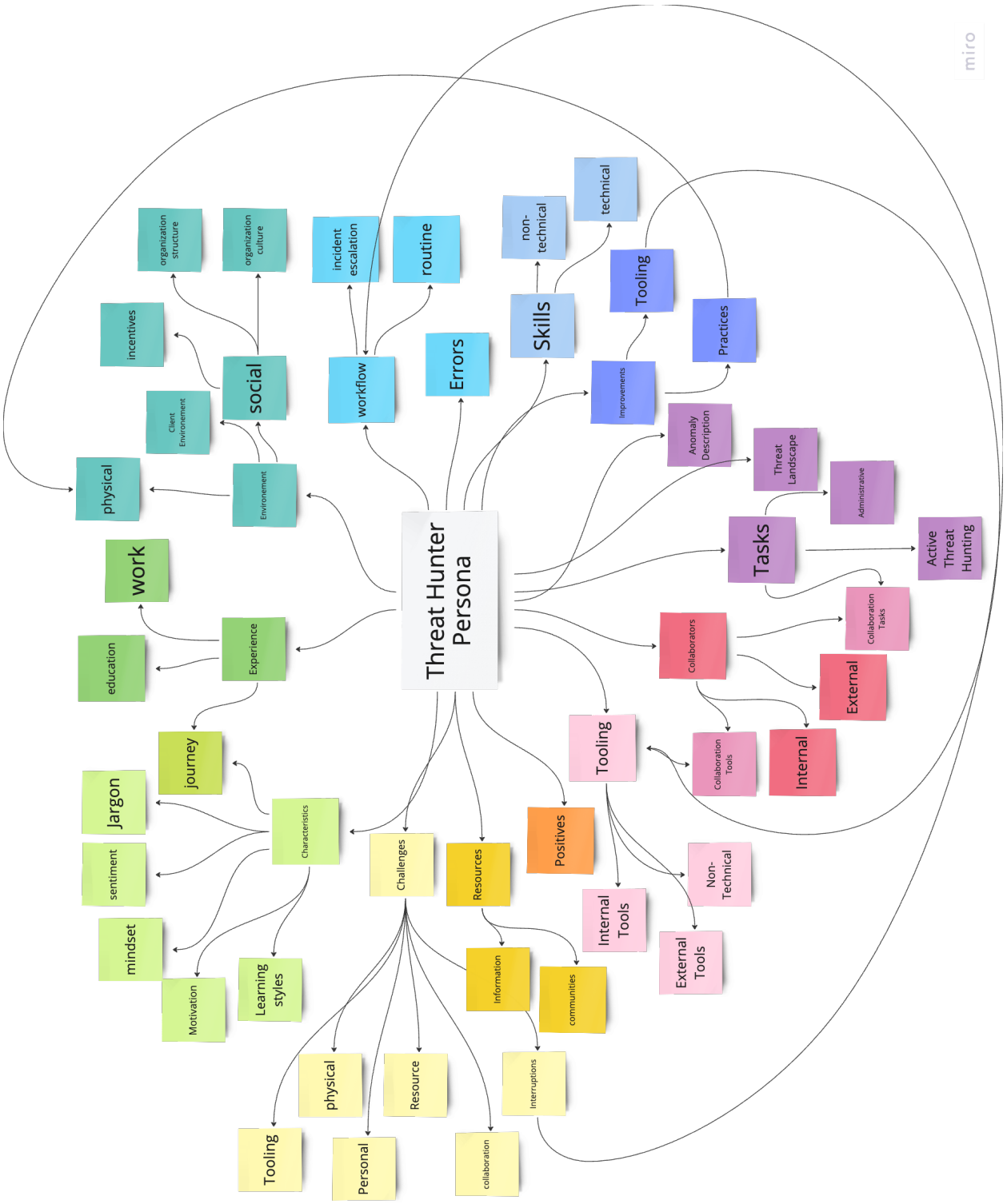


Figure 4.1: Graph of codes organized by category and subcategory, with links showing the relations between codes.

Appendix F. Additionally, the codebook (set of all the categories and codes with their definitions) and anonymized examples of coding are also available in Appendix F.

4.2 Participant Demographics

We coded the final pool of 17 interviewees into two categories threat hunters and managers, with 14 participants categorized as threat hunters (P1-P4, P7-P12, P14-P17) and three as managers (M5, M6, and M13). Table 4.1 summarizes the demographic information we collected from participants. The participants reported various job titles such as *threat hunter*, *senior threat hunter*, *lead threat hunter*, *threat researcher*, *senior threat researcher*, *lead threat research analyst*, *threat intelligence engineer*, and *senior threat response analyst*. All of the participants did threat hunting as a large part of their daily tasks. However, "threat hunter" was not always their job title. Other job titles the participants reported include: *senior cybersecurity consultant*, *security engineer tech lead*, *CEO/principal consultant*, *CISO*, and *platform engineer*.

The participants were from six different countries (Figure 4.2) and they reported working for organizations in six different countries (Figure 4.3). Participants worked in seven different industries (Table 4.1). Most participants (10 of 17) worked for companies with between five thousand and 50 thousand employees, three participants worked for companies with one thousand to five thousand employees, and one participant worked for a company with over five hundred thousand employees. The average team size for the participants was 11 people. However, the majority of participants worked on teams with less than five people. Eleven of 17 participants (65%) reported working remotely, while five reported working with a hybrid[1] modality, and one participant did not disclose their working style (Table 4.1). The educational background of the participants varied from high school education to PhD education, with most participants (11 of 17) having a bachelor's or master's degree (Table 4.1). Their professional experience spanned from one to 39 years, with a median of eight years of relevant work experience in cybersecurity (Table 4.1). 15 of the 17 participants have been in their current role five years or less (Table 4.1).

[1]Hybrid work is the combination of working some days of the week remotely and some days physically in the office [2].

Participant	P1	P2	P3	P4	M5	M6	P7	P8	P9	P10	P11	P12	M13	P14	P15	P16	P17
Educational Background																	
High School								●					●				
College					●				●							●	
Bachelor's Degree	●	●				●	●			●							●
Master's Degree			●								●	●		●	●		
Ph.D. or Higher				●													
Years of Work Experience in Security																	
0 to 5	●	●						●									
6 to 10			●				●			●	●			●	●		●
11 to 15									●								
16 to 20				●	●												
21 to 30												●	●				
31+						●										●	
Time in Current Threat Hunting Role																	
0 to 2	●	●	●				●	●		●	●	●	●	●	●		
3 to 5				●	●				●								●
6 to 10						●											
11+																●	
Industry																	
Information Services and Technology			●			●	●	●		●	●			●		●	●
Enterprise Software	●	●															
Financial Services, Banking and Insurance				●											●		
Government					●								●				
Cybersecurity									●								
Semiconductor												●					
Work Location																	
Remote	●	●	●			●		●	●	●	●	●		●	na		●
Hybrid				●	●		●						●		na	●	
Affiliation Type																	
Consultant	●	●	●		●	●	●	●	●	●	●	●		●		●	●
Internal													●		●		
Freelancer				●													

Table 4.1: Summary of participant demographics. "M" indicates a manager. "na" indicates no answer provided.

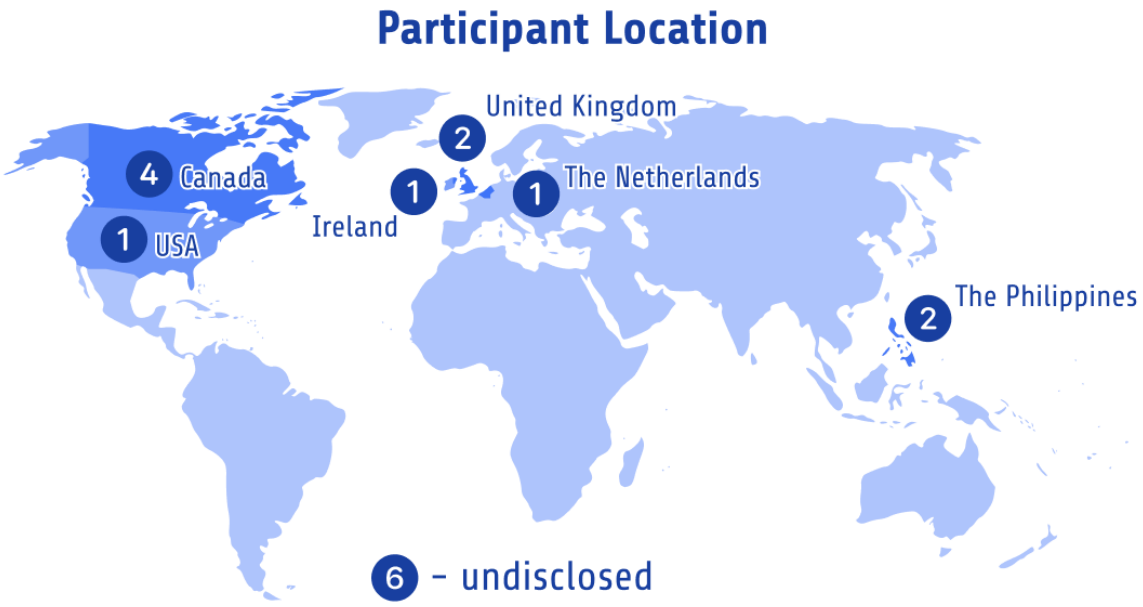


Figure 4.2: Home location of interview participants

Figure 4.3: Location of participant organization headquarters

We also asked the participants to self-report their level of threat hunting expertise on a scale of one to five, where one is basic, 3 is intermediate, and 5 is expert. Most participants (10 of 17) reported having more than intermediate level (4) of threat hunting expertise. Three participants reported having expert level (5) expertise and three reported having intermediate level (3) expertise. One participant reported having less than intermediate level (2) expertise.

4.3 Who Are Threat Hunters?

To answer the question of *who threat hunters are*, I summarize the findings related to threat hunter key characteristics (Section 4.3.1), motivations (Section 4.3.2), cultural factors (Section 4.3.3), and skills (Section 4.3.4).

4.3.1 Key Characteristics

Threat hunters have key characteristics that shape their mindset. They are inquisitive (P7, M13) and curious (P3,M5, M6, P9, P10) in nature helping them to be open-minded (P10). Threat hunters use creativity (P3, M5, P8, P10, P12), adaptability, and resilience to support their hunting in the unpredictable threat landscape. Threat hunters are proactive in how they approach hunting (P1, M5, M6, P10, P11, P12). Though threat hunters can be skeptical (P1, P12) and paranoid (M5, P14), such as P1 who said, *"I think we have this zero trust concept"*, threat hunters are passionate about what they do (P3, P17, P12, M13).

Staying informed about the threat environment and being constantly vigilant is critical to maintaining an effective threat hunting mindset. M5 highlighted that *"the typical mindset of a threat hunter is basically trying to go with the mindset of ... we're currently being hacked and I need to figure out where they are."* Threat hunters are constantly learning (P2, P15) and are constantly looking to collect threat hunting experience. As P15 aptly said, the threat hunter *"mindset needs to be kind of thirsty for knowledge."* Building experience was the most reported factor in building up threat hunter confidence (reported by 10 of 17 participants); other factors included learning about other threat hunters' experiences (P2, P16), making mistakes (P16, P17), and successfully identifying threats (P9, M13). However, many participants (P2, P3, P9, P17, M13) noted that it is difficult to ever feel fully confident given the dynamic nature of modern threats.

4.3.2 Motivations

Threat hunters are motivated to do their work by solving hard problems (P3, P4, P8, P11), protecting critical assets and their organizations (P3, P10, P17, M13), helping people (their peers and clients) (P3, P10, P11, P16, P17), and sharing knowledge both with their teams, with the public, and with the cybersecurity community (P3, P9, P15). As with other professionals, incentives such as financial bonuses, good performance on metrics, and recognition from management and peers, motivate threat hunters. The participants shared that metrics, including the number of identified threats or the delay before detecting an incident, are important for tracking the efficiency of threat hunting.

4.3.3 Cultural Factors

Threat hunters are influenced by cultural factors related to location, ethnicity, gender, age, and language in their day to day work. Language (M5, P7, P9, P11, P14, P15, P16) was the most reported factor to influence the work of threat hunters due to communications between threat hunters and collaborators often taking place over cultural and international boundaries. For example, three participants shared that English is the most common language used to communicate within teams and with clients (P7, P9, P11).

Team diversity in threat hunting was brought up by participants as an essential part of building teams with a breadth of perspectives (P3, M6). In particular, diversity of gender, ethnicity, and age were discussed by participants highlighting the difficult nature of diverse hiring. P3 described how their team lacked diversity: *"[large city] is super diverse. And it's not always reflected in the teams I'm in. ... Now that I work in a different team, ... I think we've only one or two women, it's very different. ... And it's the same with ethnic minorities. Like, I think it will be great to have more of [those folks], but ... they're hard to find."*. However, M6 shared that over the years there is starting to be some change: *"there's definitely ... a boys club problem. It's true of IT. It's even intensely true of cyber[security] just because of the environment. It doesn't attract its gender bias. It's that ego alpha male. Attraction. You know, the indispensable troubleshooter. So there's there's that bias that I think was really large 10 years ago that's starting to change."*.

4.3.4 Skills

Threat hunters are highly skilled professionals that have an arsenal of both technical and non-technical skills. Technical skills are related to hunting tasks, whereas non-technical skills are related to their cognitive and collaborative processes. For technical skills, participants reported that, having a strong understanding of operating systems (P2, P3, M5, P12, M13, P16), computer networks (P1, P2, M5, M6, P9, P11, M13, P15), how an attacker thinks (P3, M5, M6, P10, P17), and the typical behaviour of the systems they monitor (M5, P10), are crucial as a strong foundation of good threat hunting skills. Some threat hunters (P3, M5, P7) reported certification programs including SANS courses [2], OSCP (OffSec Certified Professional) [3], or CISSP (Certified Information Systems Security Professional) [4] as a way to develop threat hunting skills. Skills such as developing knowledge of the threat landscape (M5, P16) and of new AI and ML technologies (P12) are becoming more and more necessary for effective hunting.

The most important non-technical skill identified by participants was good communication (P1, P2, P7, P8, P9, P10, M13, P14, P15). Communication was emphasized for its importance in coordinating threat hunts involving multiple hunters and for providing clear and timely guidance for clients. Participants noted problem solving (M6, P7, P17), being independent (M6), and being organized (P12) as good skills for threat hunters to have. Also important to threat hunting are critical thinking (P1, P2, P3, P7, P17), situational awareness development (P10), being observant (P16, P17, M13), and analytical skills (P1, P2, P3, P7, P17). P1 highlighted storytelling as a unique skill of threat hunters: *"we just have to patch things together so that we could create the story out of it"*. Threat hunters learn fast (P8), know the right information to gather (P8), and are not afraid to ask for help or to find an expert that knows more (P3, P11). When learning quickly, mistakes can happen, as P9 said, *"You have to kind of make it a safe space to fail."*.

4.4 How do Threat Hunters work?

To answer my research question of *how threat hunters work*, I compiled the responses from the participants related to their tasks (Section 4.4.1), workflows (Section 4.4.2),

[2] `https://www.sans.org/cyber-security-training-overview/`
[3] `https://www.offsec.com/courses/pen-200/`
[4] `https://www.isc2.org/certifications/cissp`

tools (Section 4.4.3), information resources (Section 4.4.4), work environment (Section 4.4.5), common errors (Section 4.4.6), research and learning strategies (Section 4.4.7), and collaborative practices (Section 4.4.8).

4.4.1 Tasks

The core threat hunting tasks are related to investigating potential threats within the client's environment. Threat hunters create hypotheses (P10), triage alerts raised by automated processes (M5, P7), manually review and analyze data (P4, P9, P15), develop scripts to automate their repetitive tasks (P9, P11, P12), and create, update, and execute data queries to detect or track potentially malicious activities (P4, P11, P15). Threat hunters must review and verify security alerts generated by automated tools. These alerts not only provide starting points but also help prioritize higher-risk threat events. Manual data navigation gives threat hunters detailed control over search parameters, allowing them to gather better intelligence, identify indicators of compromise, and confirm automated alerts (P9, P15). Threat hunters often document and share their findings with colleagues and clients (M13, P14). They create hunting playbooks (M5, P14), write reports (P1, P2, P3, P7, P12, M13, P14), and give recommendations for the next steps after identifying a threat (P14, P15, P17).

4.4.2 Workflow

Threat hunters often use a cycle of creating a hypothesis and proving or disproving it to identify, confirm, and remediate a threat (P10, P12). However, participants primarily described their workflows in three steps: identifying and confirming a threat, assessing the severity or urgency of the threat, and taking the appropriate remediation steps to conclude hunting.

Threat hunters must initially confirm a security incident has occurred. They need to quickly gather information and build a complete understanding of the event. Incident escalation is a critical process that uses the gathered information to inform the appropriate collaborators (P1, P2, P3, P14). Logs provide the most valuable information for the comprehension of an incident (P8, P11, P15), with P10 highlighting the importance of knowing the incident timeline, the current phase of the attack, and the client's preferences for how the threats are handled. P11 adds that it is critical to assess the number of clients and machines that have been affected by the potential threat. P7 describes how they orient themselves to the data and asks question such

as: *"If we're dealing with ... compromised users or compromised computers on a network, then ... are we talking about a low-privileged user? Are we talking about an administrative user? ... Are we talking about one single compromised endpoint or multiple compromised endpoints? Are we talking about workstations or are we talking about servers?"*.

Once a security incident has been confirmed, its severity needs to be assessed. Many participants described a process of clarifying information and determining the urgency of response for the situation (P1, P2, P3, M5, P17). Some threat hunters need to manually quantify the severity of urgency of threats using conventions such as a two point scale (P1), a three point scale (P17), or a four point scale (P2, P3). For other threat hunters, their tools determine a severity score that they need to confirm (P2, P11, P14). Typically, currently ongoing attacks are given the highest priority (P1, P2), and all incidents are treated as high priority until proven to be less severe or urgent (P1, P11). Many threat hunters rely on their intuition or "gut feeling" to judge the severity of events (P3, P7, M5, M13). Other methods of assessing the severity include the value of compromised assets and privileges of compromised accounts (P7, P14, P15) and the type of attack (P7, P11, P15, P16). P11 emphasized that *"It's the impact on the environment [that] determines the ... priority."*.

After confirming and assessing a threat and its severity, threat hunters must determine what remediation steps are to be taken. They may be responsible themselves for fixing any vulnerabilities or they may create a report and send it off to the appropriate response team (e.g., SOC team, IR (incident response) team, etc., see collaborators in Section 4.4.8). A threat hunter's responsibility to fix a vulnerability — beyond identifying its potential existence — depends on the size of their organization and if response is a task assigned to them by their organization (P14, P17).

4.4.3 Tools

In total, the participants reported 95 different tools they use for threat hunting. Figure 4.4 shows the technical and non-technical tools reported by participants with the technical tools on the left and the non-technical tools on the right. I classified 60 of the tools as "technical". By technical I mean that the tools either provide threat data or a way to manipulate threat data, and they support technical or active hunting tasks. Thirty-five of the tools were non-technical meaning they provide support for non-technical tasks including communication, administration, or collaboration, and

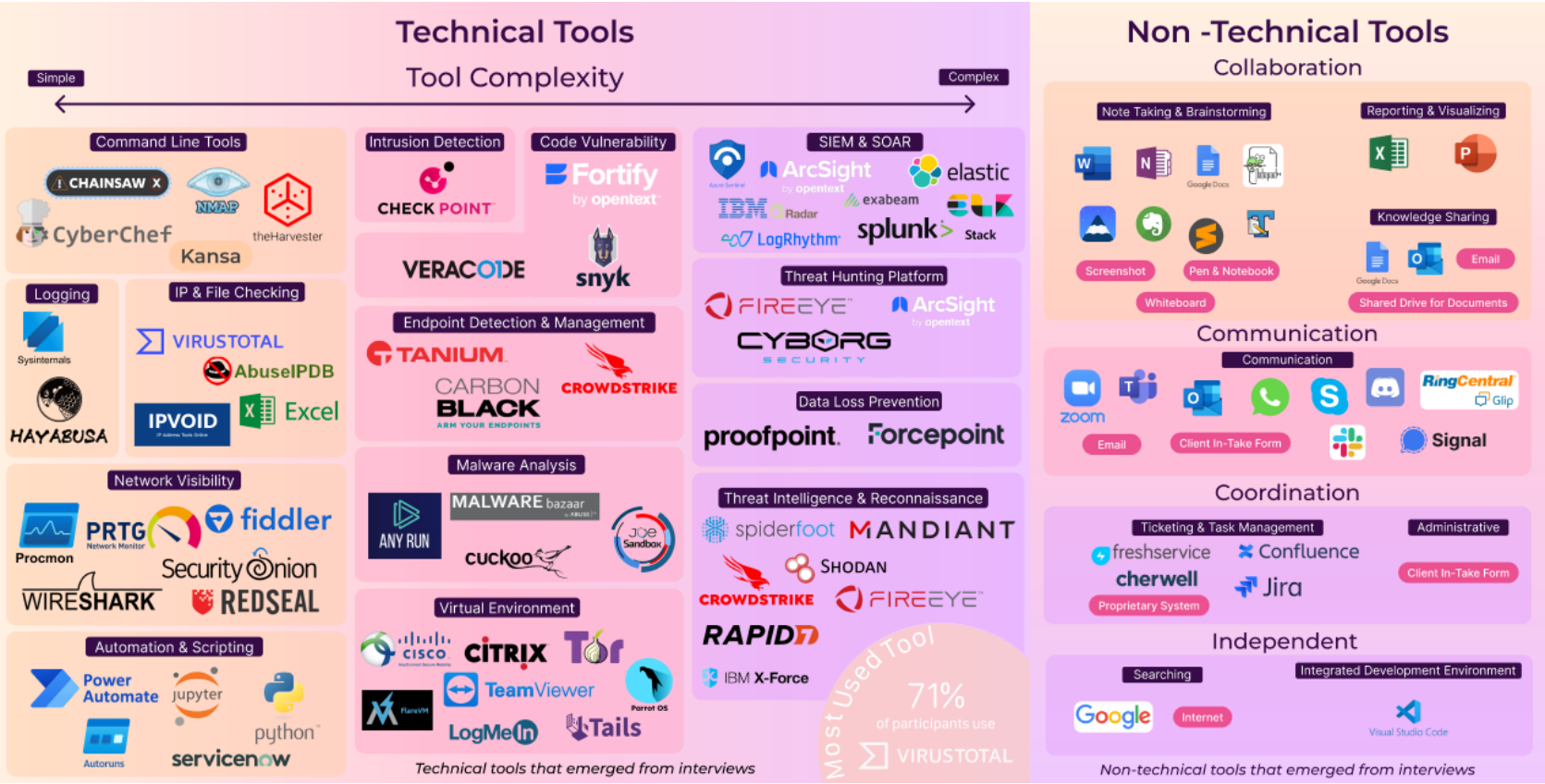


Figure 4.4: All tools reported by participant, technical and non-technical, organized by primary use case

are often used to manage the cognitive load of threat hunters.

The tools in Figure 4.4 are organized into categories based on their primary use as described by participants. There are 11 technical tool categories: *Command Line*, *Logging*, *IP and File Checking*, *Network Visibility*, *Automation and Scripting*, *Intrusion Detection*, *Code Vulnerability*, *Endpoint Detection and Management*, *Malware Analysis*, *Virtual Environment*, *SIEM and SOAR*, *Threat Hunting Platform*, *Data Loss Prevention*, and *Threat Intelligence and Reconnaissance* and nine non-technical categories: *Note-taking and Brainstorming*, *Reporting and Visualizing*, *Knowledge Sharing*, *Ticketing and Task Managing*, *Administration*, *Searching*, *Integrated Development Environment*, *Communication*. These categories were validated by industry professionals from OpenText. Some tools appear in multiple categories because they are the main tool for more than one type of activity.

The technical tools are also organized linearly from simple to complex (left to right). The tool that was the most reported by participants (12 of 17) was VirusTotal. Many of the tools that are more complex (on the right side of the technical tool figure, Figure 4.4) are used as the primary hunting tool, which threat hunters pair with some of the less complex tools (on the left) such as command line tools or IP and file checking tools. The non-technical tools are used mainly to complete administrative tasks such as documentation or sharing knowledge but they are also used to support the technical activities such as taking notes to remember an details for later in the hunting process. P12 describes their notebooks and whiteboard as, *"your throwaway [and] your long-term memory."*.

The collection of tools reported is not an exhaustive list of all the possible threat hunting tools that exist, but does represent the breadth of tools used by the participants we interviewed. Threat hunters use many of the tools they described in parallel, building a toolkit that they refine and customize for their personal hunting style.

4.4.4 Information Resources

Threat hunters reported 56 different information resources that are listed in Table 4.2. The reported resources range from online forums and newsletters to social media platforms and online communities, to internal intelligence. In the interviews we specifically asked threat hunters if they used the dark web as a resource of information. Four participants (P2, P4, P8, M6) shared that they occasionally used forums on the dark web to gather information for hunting. However, P2 shared that they do not

use their company computer to do this work. Three other participants (P7, P9, P11) shared that they use dark web information collected from a third party source or by their internal intelligence team.

Resources		
Anomali	Google	Slack channels
Articles	LinkedIn	SOC Prime
Blogs	Local cyber security group	SpiceWorks
Books	Mastodon	Stack Overflow
Business Continuity Plan	MISP	Third party dark web information
Cisco Talos	Mitre	Threat Intel feeds
Conventions	Newsletters	Threat Intel team
CrowdStrike reports	OSINT	Threat intelligence platform
CyberReason	OWASP	Tool manuals or documentation
Dark web (forums)	Palo Alto unit 42	Udemy
Digital Shadows	Password disclosure lists or breaches	Vendor websites
Discord servers	Peers in their degree program	Websites / Internet – unspecified
Facebook groups	Playbooks	X (Twitter)
Feeds from external researchers	Podcasts	X-Force
Forums	Reddit	YouTube

Table 4.2: Summary of resources used by threat hunters interviewed

4.4.5 Work Environment

Threat hunters tailor their physical work environments to the specific demands of their threat hunting activities. Typical elements of participant's work setups included a computer or laptop, complimented by one or more monitors and other devices such as iPads (P9) or raspberry Pis (used to automate their personal desk environment) (P9). Specifically, threat hunters noted having an additional computer for connecting to an *"air-gapped environment"* (M5) or a machine completely disconnected from any network to use for file testing (P17). Threat hunters also use networking hardware (P10), virtual private networks (VPNs) (M5, P15), and virtual machines (P9, P10, P16, P17) for conducting network simulations.

Threat hunters also find making their work environment comfortable especially important. Two participants (P3, P12) use standing desks to support physical well-being (P3), or to feel more proactive and get a *"better feeling ... of getting into ... work"* (P12). Two participants (P4, P12) shared how important it is to have music in their space. P4 said, *"descending [in]to music is really important"* for their hunting.

4.4.6 Common Errors

Threat hunters, like any other person, make errors. The most common errors reported by the participants included misidentifying suspicious activity (P3, P7, P12, M13, P17), overestimation of the severity of an anomaly and inappropriately raising the incident to the customer (P1, P2, P4), jumping to conclusions of what an event could mean (P15, P16), and cutting corners in the hunting process (P3, P16, P17, M6). In particular, P3 said that, *"if I can always try and automate [tasks], meaning I don't cut corners. Because it can be very tempting to just leave [hashes] or make a copy paste mistake, that sort of thing."*.

Managers reported other flawed approaches that threat hunters occasionally use. For example, M5 said that if, *"all [threat hunters] do is the same thing over and [over] then ... they're not being proactive at that point."*. Relying on a single tool and not considering the limitations, creating hypotheses too early, using tools to confirm bias, and not investigating an anomaly all the way to the root cause are other common potential errors identified by managers (M5, M6, P12)

4.4.7 Research and Learning Practices

Threat hunters need to stay up to date on the latest cyber threats and are continuously learning. Most of the participants reported that they learn through mentorship (P1, P2, P9, P10, P14) and hands-on experience such as learning by doing (P2, P7, P10, P12, P15, P17). Threat hunters learn from their peers, senior threat hunters, managers, and their community. Threat hunters learn hands-on through trial and error, practice, and by running simulations or drills with teammates (P12, P17) or through events such as *Hack The Box* [5] (P9). Other approaches that threat hunters use to learn and stay informed include: reading articles, newsletter, blogs, and reports (P1–P3, M5, P7–P11, P14, P15, P17), listening to podcasts (P2, P4, P9, P14, M13), and watching videos (P1–P4, P8, P14, P17, M5).

[5] `https://www.hackthebox.com/`

Threat hunters share information with their peers, managers, clients, and communities to anticipate future threats and implications, stay informed (P2, P10, P11, P15, P16), familiarize themselves with the client's environment (P3, P8, P9), make predictions based on technology and business trends (P15, P16), and review historical attacks to find patterns (P1, P11). They share information within their teams primarily through presentations (P1, P3, P7, P9, P11), during meetings or handover (P1, P2, P3, P14), and one-on-one with teammates (P1, P2, P7, P14). P7 highlights how casual weekly meetings with their peers helps them learn from one another: *"if somebody knows something and somebody else is particularly interested in it ... give[s] people the license [to] have that chat and like reach that same understanding."*. To share information outside of their teams, with the client for example, threat hunters present reports during weekly, monthly, or on-demand meetings (P1, P2). To share information, threat hunters use many non-technical tools such as email, *Slack*, *WhatsApp*, *Microsoft OneNote*, or internal documentation sites (e.g., *Confluence*).

4.4.8 Collaboration

Threat hunters collaborate with many groups of people both in their organizations (internal) and outside their organizations (external). Internal collaborators include teammates (P1, P2, P3, M5, P7, P10, P14, P17) and managers (P1, P2, P3, P4, P9, P11, P15, P17), as well as other security and engineering teams such as security operations centers (SOCs) (P1, P4, P11, P14, P15), data science teams (P1, P2, P7), threat intelligence (M5, P7, P10, P11,, P12, P15), red and blue teams (P11), software developers (P2, P4, M5, P12, M13), and product development teams (P12, P16). External collaborators are primarily the threat hunting clients (P1, P2, P3, M5, M6, P7, P8, P11, P12, P14) including their SOC teams and data centre analysts, but also cybersecurity insurance companies (M13), supply chain vendors (M5, M6, P14), the public (P7), and security researchers (P10). Threat hunters use many tools to collaborate and communicate as seen in Figure 4.4 (on the right).

Collaboration between threat hunters and collaborators takes the form of planned meetings, hand over procedures (P2, P3, M5, P7, P9, P16), and presentations (P7, P8, P12, P14) and ad hoc collaboration, which is primarily communication between collaborators (P1, P2, P4, M5, P7–P17). Daily (P8, P9), weekly (P1, P7, P9, P12, M13, P14, P15, P17), and monthly (P14) meetings were reported by threat hunters with daily and weekly meetings happening primarily with team members and monthly meetings

mostly with clients. Between shifts, some threat hunters hold handover meetings to brief the incoming hunter on the progress and findings of the outgoing hunter. Handover procedures minimize redundant efforts and ensure that suspicious activities are thoroughly investigated to conclusion, regardless of whose shift they occur during (P7, P16). P3 describes the handover process as *"a rolling log of things that the next person should be aware of"*.

During shifts threat hunters reported working together to tackle suspected or recognized attacks (P12, M13). Additionally, threat hunters are preparing reports and presentations that summarize the timeline of an attack, identify the resolution and consequences of an attack, and recommend improvements to protect against future threats to share with their collaborators. Other collaborative artifacts threat hunters reported include journals of activity during threat hunting sessions, concise reports on hunting activities, playbooks for responding to specific events, inventories of clients' digital assets, and network maps of clients' environments.

4.5 What Challenges do Threat Hunters Face?

Threat hunters reported challenges related to themselves and their peers (Section 4.5.1), their domain and landscape they hunt in (Section 4.5.2), their tools (Section 4.5.3), their information resources (Section 4.5.4), and collaboration (Section 4.5.5). Participants also shared some ways to mitigate the challenges they reported which I describe in the corresponding sections below.

4.5.1 Human Factor Challenges

Participants listed environmental challenges that lead to physical limitations such as tired eyes (P1), uncomfortable desk set-up (P7), and screen fatigue (P2, P15) as challenges they face while working. Interruptions and distractions including client messages (P11, P16), needing to document everything (P14), and task urgency getting mis-prioritized (P3), are challenges that threat hunters face. Interruptions introduce further challenges such as context switching between tasks (P1, P2, P3, P7, P8). P3 shared that often it is an administrative task, such as emails or creating presentations, that interrupt more critical threat hunting activities. P1 and P2 also note that switching between tools, especially when smaller tools are not integrated into their main tool, is challenging.

Information overload is a significant challenge for threat hunters, as P16 said, *"I think the biggest challenge really, I think for all of us is just digging through the noise"*. Specifically, parsing, isolating, organizing, and sharing the right information is difficult (M5, P7, P10, P16). M5 expressed *"... dealing with just data and logs and so on can be very overwhelming because there's like millions, billions of logs being done ..."*. Information overload and sheer number of incoming threats (P7, P14) makes staying up to date with information and the status of systems challenging (P3)

Some **mitigations** for challenges related to the human factors of threat hunting that participants shared include: taking breaks during work (P1, P2, P3), time blocking (P1, P2, P3), getting comfortable in their environment (P7), having a comfortable desk set-up (P7), not doing some of the more menial administrative tasks to avoid distraction (P3), and understand themselves and how they work (P17).

4.5.2 Domain and Landscape Challenges

Threat hunters operate in varied environments, facing unknown threats (zero-day threats (P11)) and conflicts between usability and security that makes users reluctant to adopt strict security measures (M13). The most reported domain limitation was poor visibility of client systems (P1, P2, P3, M5, P8, P11, P12, P16). P8 explained that *"... we never have enough access to the client's infrastructure and data and all the tools that we need."*. Client environments are diverse, P3 said, *"some of them are multinational, it's really hard to say what is normal and what isn't"*. Hunting for multiple customers on various systems requires context switching and learning a range of skills. P16 emphasized the challenge that is posed when client systems dictate the procedure threat hunters can use. Additionally, P9 remarked that there is no standardized way to hunt and that presents challenges with transferring knowledge.

Threat hunters suggested **improvements** for domain and landscape challenges such as communicating the repercussions of not implementing good security hygiene to stakeholders (P8), and escalating access challenges up the management chain (P8, P15).

4.5.3 Tooling Limitations

Even the best tools have limitations and the two most frequently reported challenges were false positives, data availability, and data retention. Tools are often reporting too many false positives and P8 shared their frustration saying *"to sanitize these*

returns is painful". Many participants also reported challenges related to insufficient data, not having the right data, and not knowing how long to retain important data. P3 noted that often *"the data you need to establish some sort of thing is not available"*. P10 shared that building the right query for the data you want to find is a challenge. Visualizations, performance issues, and general lack of cohesion in their tools were some usability challenges reported by participants. The existing visualizations are often not effective in helping threat hunters recognize patterns and detect anomalies (P2, M6, P17). Many participants shared their frustration with the lack of cohesion between all their tools and information resources (M5, P9, P11, P17).

Threat hunters shared some **solutions** to these tooling challenges such as automation of simple tasks (P3, P7, P14, P15), version or action tracking history (P1, P2), and making sure that threat hunters have access to the right tools (P10). The most reported solution was to integrate key features and tools that threat hunters are using often directly into their primary SIEM tools (P1, P2, P11, P14). Further exploration of these solutions are discussed in Chapter (Section 6).

4.5.4 Information Resource Challenges

The most significant challenge reported with information resources is determining which information is trustworthy and reliable (P7, P8, P9, P14). Threat hunters noted that many of their information resources are behind paywalls or confidential, making them inaccessible (P4, P15, P16). In particular, P16 remarked, *"not everyone's willing to share information"*. The effectiveness of an information resource is constrained by the threat hunter's ability to frame the right questions, the number of searches they can perform (P1, P10), and their ability to condense large amounts of information (P3, P10). Many of the available resources are not concise and the knowledge that threat hunters are looking for often needs to be distilled from a larger body of work (P3, P10). P3 also notes that the information they need for a hunt may be very specific and *"not everything is on the internet"*.

The dark web presents challenges for threat hunters using it as a resource, it can be costly and difficult to access. P2 explained that many useful forums for threat hunters are invitation-only and require time to build trust within the community. There are also significant risks associated with maintaining a presence on the dark web (M5, M6) and it takes a lot of work to maintain safe access (P12).

Threat hunters suggested several **improvements** to enhance the effectiveness of

their information resources, emphasizing better integration of resources into the primary hunting tool (P2, P11), and a way to verify the trustworthiness of information sources (P3, P11, P14). P3 also noted that accepting that some questions may remain unanswered is important. To improve knowledge sharing, P8 recommended ways to provide more detailed findings such as capturing the current context, critical questions, and the urgency of the situation, which are often missed in formal reports. Suggestions also included normalization and standardization of information (P9), and queries (P11). Enhancing accessibility (P14, P15) and reducing costs were highlighted, with a call for organizations to provide paid access to necessary resources (P15). Additionally, the use of AI to ingest and query organizational data was proposed as a new resource that could streamline threat hunting processes (M5).

4.5.5 Collaboration Challenges

The most frequently reported collaboration challenge is coordinating geographically dispersed teams, particularly across multiple time zones (P7, M13, P15). Participants highlighted the difficulty of tailoring communication to different audiences, such as clients or management (P3, P8, P9, P10, P12, M13, P14), with one manager noting that some teams struggle to communicate their work within the company (M5).

Threat hunters also find it challenging to distill collected information into a simple format (P8, P10) and sometimes need to convince their team that a threat is real and serious (P12). Communication with clients can be problematic, as clients may not implement recommended actions (P14). Additionally, varying learning styles, different levels of knowledge among team members (P1, P3, P16), and limited time for knowledge sharing (P7), add to the challenges. The absence of a local threat hunting community impedes threat hunters from learning from their peers (P2).

Organizational structures and processes present further challenges, with issues in large organizations not getting addressed promptly (P3) and inadequate support from companies (P4). P9 noted that some organizations have a culture of withholding information, *"they don't want to show you how messy their backyard is ..."*, and some do not prioritize security in their business models effectively to support threat hunting (P8).

To make collaboration better, participants suggested **improvements** such as standardizing the handover protocol (P9), having a centralized platform for communication (P1), having more automation available to support report generation (P14),

and organizations building better security hygiene practices (M13). P7 mentioned how virtual and in-person meet-ups with their team helped with collaboration, and they said, *"it made a big difference when I actually went out to one of the other regions and met ... some of the other threat hunters, ... interacting with them in person ... made me feel much like it was much easier to kind of just like ping them casually"*. Overall, more collaboration on threat hunting teams was recommended (P16).

The findings of our interview study are rich and uncover the human aspects of threat hunting. However, these findings are dense and perhaps unapproachable due to their level of detail. Therefore, the next chapter describes how I used the findings to construct personas that capture the essence of these findings and present them in an accessible way, that facilitates the understanding of who threat hunters are and the design of better support tools.

Chapter 5

Personas

The personas presented in this chapter are archetypal representations of threat hunters, serving a crucial role in humanizing and contextualizing threat hunters within cybersecurity. These personas act as a snapshot of the current state of the role of threat hunting by describing who threat hunters are, how they work, and the challenges they face. The dimensions introduced in this chapter emerged from 20 interviews with threat hunters and form the basis of the personas. Using the approach of ranking participants on each of the dimensions to identify patterns [23, 50, 21], I created personas that are grounded in the data. Ultimately, these personas bridge the gap between the technical and human aspects of threat hunting. In the following sections, I present the dimensions (Section 5.1) and the four personas (Section 5.3).

5.1 Dimensions

My experience of conducting the interviews coupled with expert insights from the team at OpenText and discussion within my research team, guided the process of extracting the key dimensions of threat hunters. Initially, 40 dimensions emerged from the interview data. This set of dimensions was analyzed thoroughly by all the team members (researchers and OpenText) to narrowed down the final 17 dimensions. The resulting set of dimensions consisted of six categorical dimensions and 11 continuous dimensions. All the dimensions are defined in this section. The categorical dimensions are labelled D1-D6 and the continuous dimensions are labelled D7-D17.

D1 Organizational Affiliation Type

Internal: threat hunter hunts for the organization by which they are employed.

External: threat hunter hunts for clients outside of the organization by which they are employed

D2 Affiliation Type

Freelancer: A threat hunter that does not belong to an organization and works primarily as a contractor.

Consultant: Threat hunter works for an organization that provides threat hunting services to clients.

Internal: Threat hunter works as part of a security team of an organization and hunts within the environment of that organization.

D3 Experience

1 - (1 - 4 years of experience)

2 - (5-9 years of experience)

3 - (10 - 19 years of experience)

4 - (20 + years of experience).

D4 Location

Remote: threat hunter works entirely from a non-office setting / from home.

Hybrid: threat hunter works both remotely and in an office setting.

Office: threat hunter works entirely from an office setting.

D5 Role

Threat Hunter: basic role of threat hunter with no responsibility to manage peers.

Senior Threat Hunter: Threat hunter with more experience and provides support for less experienced peers but has no responsibility to manage peers.

Team Lead: Head of team with responsibility to lead the team in hunting activities but does not manage the team outside of hunting.

Technical Manager: manages the team outside of hunting activities (administrative). Could also manage threat hunting activities. A technical manager can be a team lead but a team lead cannot be a technical manager.

D6 Learning Strategies

Self Taught: threat hunter learns primarily through teaching themselves from resources.

Trial and Error: threat hunter learns primarily by trying and failing in secure environment.

Formal Certification: threat hunter learns primarily through courses and formal training.

Mentorship and Collaboration: threat hunter learns primarily through working with peers or a mentor and getting feedback.

D7 Hunting Style

Proactive: threats are identified before an attack occurs that leverages the threat.

Reactive: response to attacks is done as they appear.

D8 Hunting Process

Ad Hoc: means the team or individuals hunt by following threats and the path they follow rather than a prescribed procedure.

Procedural: means that the hunting style is to follow a protocol on how to investigate specific threats (playbook).

D9 Cognitive Approach

Intuitive/Creative: means that the threat hunter uses gut feeling and intuition to navigate tasks and thinks outside of the box to solve problems.

Analytical/Methodological: means that the threat hunter has a process they follow when they navigate tasks and use logical reasoning to solve problems

D10 Collaboration Mode

Individual: hunting is done individually.

Team: hunting is done as a team.

D11 Validation of Findings

Peer-Peer: threat hunter validate their findings by checking with their peers.

Resources: threat hunter validates their findings by checking resources.

D12 Process Initiation

Hands-on: threat hunter is customizing their tools and writing their own queries and scripts to get what they want from their tools.

Tool-led: the threat hunter's workflow is derived from the existing tools functionality.

D13 Tool Quantity

One tool: hunts are conducted using only one tool.

10+: hunts are conducted using 10 or more tools.

D14 Tooling Landscape

Commercial: the tools being used are predominantly commercially produced threat hunting products.

Built-in house: the tools being used are built by the threat hunter or the team. (For THs that work for companies creating and using commercial software it would still be considered commercial)

D15 Availability of Resources

Open source: resources used by threat hunter are open source.

Private intel: resources used by threat hunter are from a private source.

D16 Formality of Resources

Casual: resources used by threat hunter are such as blogs, feeds, or social media and are not peer reviewed.

Formal: resources used by threat hunter is formal articles or literature often peer reviewed.

D17 Motivation

Intrinsic: threat hunter is motivated to do their work by intrinsic things such as a sense of accomplishment, helping others, or fighting for a cause.

Extrinsic: threat hunter is motivated to their work by extrinsic things such as salary or recognition.

5.2 Identifying Data Patterns For Personas

Figure 5.1 shows the ranking of each of the 17 participants on each of the 11 continuous dimensions. I used a four point scale, as recommended by Goltz [21], to simplify the ranking process and avoid neutral ratings that would reduce the uniqueness of the personas. I visualized the patterns in the rankings using colour value to create a heat map of the rankings. This visualization helps to identify some patterns between participants that were next to each other in the table however, it does not make it easy to compare multiple participants.

	P1	P2	P3	P4	P7	P8	P9	P10	P11	P14	P15	P16	P17
Less years of experience - More years of experience	2	3	3	4	3	1	4	3	3	3	4	4	2
Proactive - Reactive	1	2	1	1	3	3	2	1	1	4	4	2	2
Ad Hoc - Procedural	2	2	2	3	4	3	3	4	3	4	3	2	2
Intuitive - Methodological	2	2	3	4	4	3	3	2	2	1	3	2	1
Creative - Analytical	2	3	1	3	3	1	2	1	3	3	4	2	2
Individual - Team	3	3	3	2	3	2	3	2	3	2	2	2	2
Hands on - Tool led	4	3	4	2	3	4	2	2	3	3	2	2	2
One Tool - 10+ tools	1	2	1	4	3	3	3	3	2	3	3	2	4
Commercial - built in-house	1	1	2	3	2	2	2	3	1	1	1	3	2
Open source - private intel	1	2	1	3	2	2	1	1	2	3	1	1	2
Casual - Formal	1	1	2	3	1	3	2	2	3	3	1	1	2
Intrinsic - Extrinsic	1	3	2	1	2	2	2	1	3	2	2	1	1

Table 5.1: Ranking of participants on spectrum dimensions. Each column represents a participants ranking on the spectrum dimensions.

To facilitate the comparison of multiple participant rankings, I created two matrices that compared each of the participants to one another based on most similar rankings and most dissimilar rankings. To compare the most similar participants I counted the number of dimension rankings each participant had in common (exactly the same) as another participant using the formula:

=SUMPRODUCT(- -(participantRanking1=participantRanking2))

in Excel. Table 5.2 shows the results of this analysis, with the higher the value indicating higher similarity between participant rankings. The number of similar pairs are highlighted using a value scale, with a white background indicating lower similarity and a darker grey background indicating a higher similarity. I highlighted, in dark blue, the pairs of participants that had six or more of the 11 dimensions in common.

To compare the most dissimilar participants, I looked at the maximum difference in ranking values for each pair of participants using the formula:

=MAX(ABS(participantRanking1-participantRanking2))

	P1	P2	P3	P4	P7	P8	P9	P10	P11	P14	P15	P16	P17
P1	null												
P2	5	null											
P3	6	3	null										
P4	2	1	1	null									
P7	2	6	4	2	null								
P8	1	1	5	3	5	null							
P9	3	2	6	3	4	5	null						
P10	4	2	5	5	3	3	4	null					
P11	4	9	3	4	5	3	2	3	null				
P14	1	4	2	4	6	4	2	4	5	null			
P15	3	2	3	4	3	5	7	4	2	5	null		
P16	6	5	2	5	1	1	5	6	2	1	5	null	
P17	4	3	3	4	2	3	5	4	1	2	2	6	null

Table 5.2: The most similar participants based of rankings on threat hunting dimensions

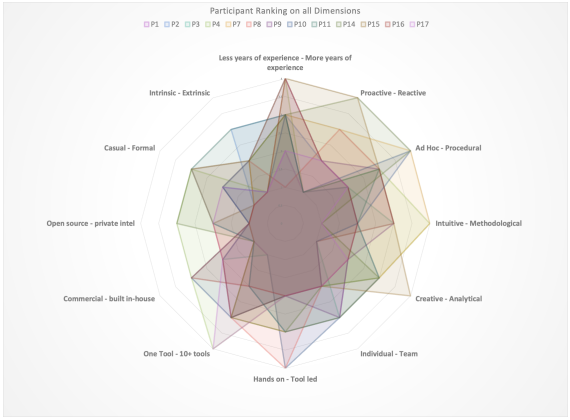
	P1	P2	P3	P4	P7	P8	P9	P10	P11	P14	P15	P16	P17
P1	null												
P2	2	null											
P3	1	2	null										
P4	3	2	3	null									
P7	2	2	2	2	null								
P8	2	2	2	3	2	null							
P9	2	1	2	2	1	3	null						
P10	2	2	2	2	2	2	1	null					
P11	2	2	2	2	2	2	1	2	null				
P14	3	2	3	3	3	2	2	3	3	null			
P15	3	2	3	3	1	3	2	3	3	2	null		
P16	2	2	2	2	2	3	1	2	2	2	2	null	
P17	3	2	3	3	3	2	2	2	2	2	2	2	null

Table 5.3: The most different participants based of rankings on threat hunting dimensions

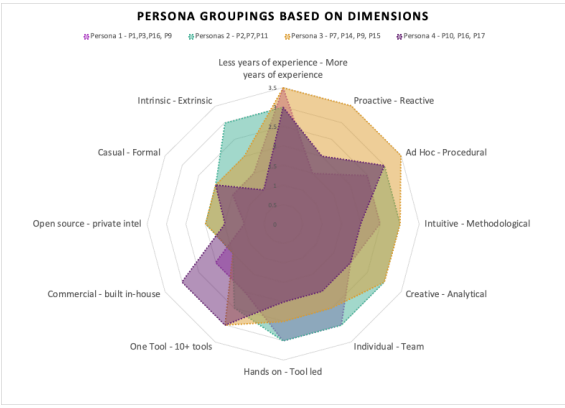
in Excel. Table 5.3 shows the result of this analysis, with higher values indicating a higher degree of difference between two participants. I highlighted, in red, the participants with the highest differences between rankings and the lowest difference.

Finally, I created radar graphs of the participant rankings of the dimensions to visually assess if there were any natural grouping or patterns across the participants. In Figure 5.1a I looked at all the participant rankings together. In Figure 5.1b, I first grouped participants based on patterns in the similarity analysis (Table 5.2) and the initial heat map (Table 5.1), then I averaged their rankings to create the groups visualized on the radar graph. The graphs with the grouped participants were more useful than the graph with all 17 participants because it was easier to see patterns. However, as the radar graph figures (Figure 5.1) show, strong patterns did not emerge.

The patterns illustrated in the heat map of participant ranking, the similarity anal-



(a) Radar graph of all participants rankings on each dimension.



(b) Radar graph of groupings of similar participants rankings on each dimension.

Figure 5.1: Radar graphs used to attempt to quantitatively identify patterns in participants to form groupings for the personas development.

ysis visualization, and the dissimilarity analysis visualization, provided inspiration for which dimensions each of the four personas embody. The groupings of participants in Figure 5.1b show weak patterns in some of the dimensions. These patterns were used to inspire a second approach to creating the personas. This approach combined these results and intentionally exaggerated some dimensions with the goal of building personas that are distinct and relatable.

5.3 The Threat Hunter Personas

I designed the personas template to mimic a LinkedIn profile for a threat hunter. Each persona profile has a headshot, name, pronouns, a text description of their role, experience, and some more personal details (hobbies and interests). Underneath the description of their role and personal details, I also included quotes that humanize the personas and give them a unique voice (Figure 5.2-A). The quotes included in the profile were taken directly from anonymized participant data. The threat hunting dimensions are included in the profile as either tags underneath their name to represent the categorical dimensions (Figure 5.2 D1-D6) or in the column on the right of the profile as scales with rankings to visualize the continuous dimensions (Figure 5.2 D7 - D17). I included other elements such as pain points (the specific challenges that persona faces) (Figure 5.2-B), the tools they use (Figure 5.2-C), and their best skills (Figure 5.2-E). Including these types of elements enriches the personas, bringing them

Figure 5.2: Elements of the personas

to life, and makes the personas relatable and human [23]. I present these next.

5.3.1 Olivia

Olivia embodies the proactive and creative team lead, known for her strong leadership capabilities in threat hunting. She has seven years of cybersecurity experience and has several SANS certifications, which she earned through her time in a mentorship program. As a senior member of her hunting team, she provides guidance and feedback to her peers. Olivia uses a small but carefully curated toolkit and adopts a proactive hunting style. Her approach is intuitive and creative, often working *ad hoc*. She primarily uses private information resources, such as intelligence gathered internally by her organization. Olivia is highly motivated by helping others and fostering a strongly connected team. However, her main pain points that limit her ability to hunt include managing diverse customer systems, frequent context switching, limited organizational support, and collaborating with various individuals who have very different personalities.

5.3.2 Jay

Jay is a novice threat hunter, recently graduated from an education track. Jay is equipped with exceptional analytical skills and a reactive approach to hunting. He holds a Master's degree in IT security and has been a threat hunter for two years. He has specialized skills in red teaming and automation and enjoys writing scripts to automate his repetitive threat hunting tasks. His hunting style is procedural and he uses his organization's ticketing systems to communicate with his team and clients. Jay uses a large range of tools to assist him on his tasks and is hands-on with the data when he is hunting. He is motivated by working hard, advancing his career, and financial incentives. The primary pain points that affect Jay are poor tool performance, information overload, diverse communication styles, and context switching.

5.3.3 Thomas

Thomas, the most seasoned threat hunter, works within a small team and relies on his intuitive hunting style. Thomas has over 25 year of experience as a security professional. He is involved in many online communities. He has a well-crafted toolkit of five to seven key tools. He hunts proactively and tries to be always one step ahead

of attackers. He uses many information resources to validate his hunting hypotheses and prefers to use tools he has built and customized himself. Thomas is motivated by keeping the organizations he protects safe and highly values educating clients and the public on proper security hygiene. The main pain points that affect him are screen fatigue, restricted data availability, and diverse client systems.

5.3.4 Ren

Ren is the manager persona, who oversees the coordination between the threat hunting team, clients, and the organization, even though they are not always directly engaged in the daily threat hunting activities. Ren works as a consultant for clients that are external to the organization they work for. They are a hands-on manager who works closely with their team and their clients. They work in a hybrid environment, coming into the office twice a week and to run quarterly meetings with their clients to report the critical findings that their team have uncovered. Ren is good at communicating highly technical information in an approachable way and takes pride in building diverse teams that are composed of driven and passionate individuals. Ren is motivated by achieving the goals set out by their team, clients, and organization. However, some pain points such as limited diverse personalities, overly complex tools, varied client systems, and context switching challenge them.

5.3.5 Member Checking

Throughout the qualitative analysis and development of the personas we consulted with the team at OpenText. They provided feedback during the analysis and reviewed the final dimensions and personas. Additionally, we sent out two member checking surveys (the second survey sent to encourage more engagement from participants), along with the final report to our interview participants. In the surveys, we asked participants to indicate which persona they identified with most and share any feedback they had (see Appendix E). In total, five participants responded to the anonymous member checking surveys. The feedback was positive, with one threat hunter indicating that the personas we created reflect the types of threat hunters they have on their team. Four identified most with Thomas and one with Jay. These results were expected given most of the participants we interviewed were not team leads or managers.

The dimensions and personas I devised embody the lived experiences of the 20 threat

hunters that were interviewed. They describe the key characteristics of threat hunters both related to tasks and behaviours, the skills they have, the workflows they prefer, and the challenges they face. Next, I discuss how the findings fit in the context of related literature, the implications of the novel findings, how the role of the threat hunter is evolving in response to the dynamic threat landscape, and the benefits and drawbacks of using personas in cybersecurity.

Figure 5.3: Olivia's threat hunter profile

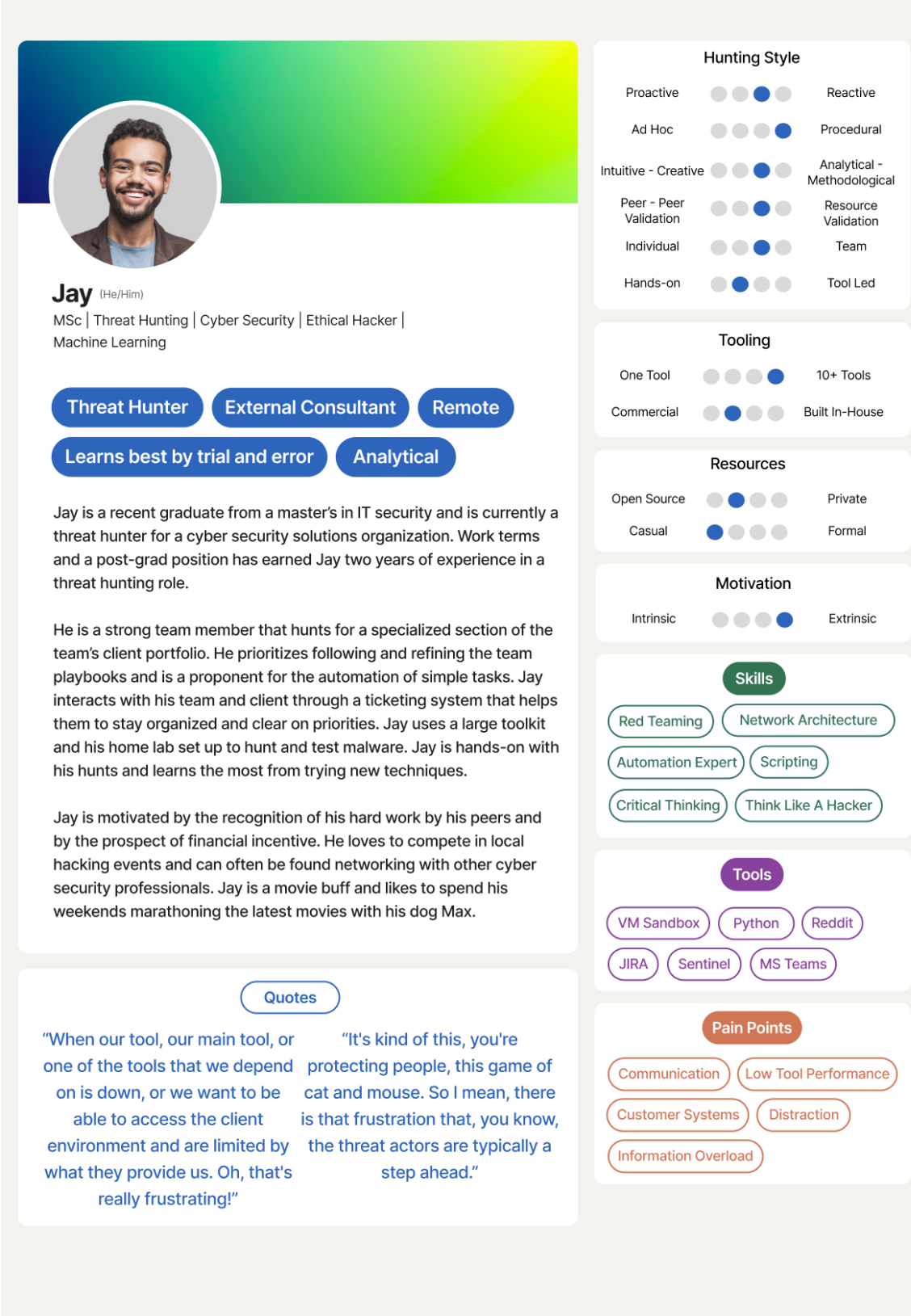


Figure 5.4: Jay's threat hunter profile

Figure 5.5: Thomas' threat hunter profile

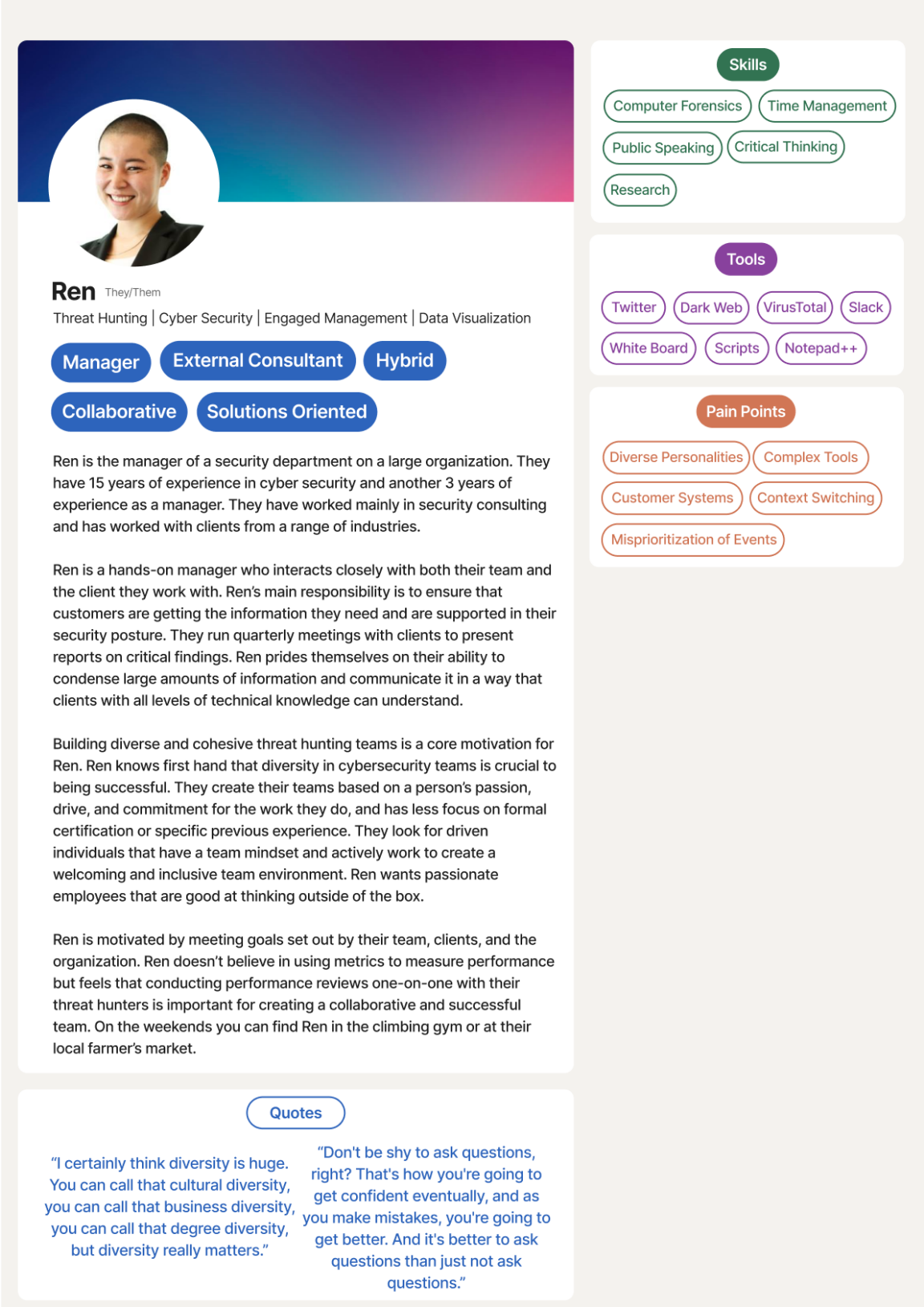


Figure 5.6: Ren's threat hunter profile

Chapter 6

Discussion

In this chapter, I discuss the findings from the research presented in my thesis and their implications. I begin by exploring what I learned from the participants and how these findings fit in the context of the existing literature. Next, I discuss the implications of the novel findings of this study. Then, I dive deeper into the critical nature of threat hunting and why the role is changing quickly. After, I discuss the benefits and limitations of personas and recommend ways of using them. Finally, I conclude with the threats to the validity of my research.

6.1 Confirming Known Aspects of Threat Hunters

The findings of my research confirmed several aspects of threat hunting recognized in the literature. Key traits such as communication skills [22], curiosity, and investigative instincts [20], emerged as critical to threat hunters, aligning with existing work that highlights these foundational qualities as essential for effective threat hunting. Specifically, Goodall *et al.* [22] describe the communication skills needed for threat hunting and Fuchs and Lemon [20] describe the need for investigative instincts both of which were noted by many participants (communication skills - (P1, P2, P7–P10, M13, P14, P15) and investigative instinct - (P7, P10, P14, P17)). Additionally, Trevelyan [51], and Fuchs and Lemon [20] describe curiosity as a key trait of threat hunters, while Lee and Lee [31] describe threat hunters as passionate and curious. These sentiments were echoed by many participants (P3, M5, M6, P9, P10, P12, M13, P17). These key traits directly informed the dimensions and personas created in this research and are crucial in understanding who threat hunters are and how they work.

The importance of experience, for developing threat hunting skills and strong intuition, was also confirmed by participants (P1, P3, P7–P10, P14–P17), corroborating the works of Goodall [22], Trevelyan [51], and Fuchs and Lemon [20]. In particular, Goodall *et al.* describes strategies security professionals use to develop their expertise and experience, listing "*learning by doing*" as a primary strategy and corroborating the reports of many participants (P2, P7, P10, P15, P17). I discuss in the next section, (Section 6.2) how experience also develops confidence in threat hunters and why that is important to understand for the development of new tools.

Moreover, high-stress work environments often lead to information overload and a significant risk of burnout for threat hunters [38, 13, 19]. The findings confirmed these risks, with reports of information overload (M5, P7, P10, P16) and other burnout indicators such as fatigue (P1, P2, P12, P15), frustration (P2, P3, P4, M13, P16), feeling overwhelmed (M5, P16), and feeling discouraged (P2). These factors are a crucial part of understanding threat hunters and offer insight into the kinds of supports that threat hunters need in order to improve the lived experience of their role.

Understanding and confirming these key characteristics, skills, and challenges of threat hunters lays an important foundation for the new findings to emerge from. The findings that this study confirms show that though we understand the technical aspects of threat hunting and some of the challenges threat hunters face that there is still a need for deeper understanding of the human aspects and that these aspects will guide the development of better supports for threat hunters.

6.2 Implications of Novel Findings

Threat hunters are motivated by solving hard problems, protecting assets, protecting people, sharing knowledge with their community, and being committed to continuous learning. P15 emphasized the need for a *"mindset [that] needs to be kind of thirsty for knowledge."*. Motivations are a key component of building useful personas because they influence how individuals behave [23]. Moreover, motivations influence how threat hunters collaborate, the workflows they use, and the tools they choose. Understanding threat hunter motivations and how they influence their behaviours is critical to the development of new tools, because with different motivations come different needs that should be supported by tools. For example, a threat hunter who is primarily motivated by continuous learning will require more integration of their information resources in to their tools. Whereas, a threat hunter primarily motivated

by helping others will need tool features that support clear and simple reporting and visualization, so they can easily share their work and implement change.

The idea that experience builds threat hunters' confidence (P1, P3, P7, P8, P9, P10, P14, P15, P16, P17) was also highlighted by the findings. Though this new insight might be intuitive, it is an important concept to understand especially in a field like cybersecurity where the turnover rate is high [40, 38] and rapid decision-making is critical [26]. Newer threat hunters require more checks, guidance, and collaboration from leadership to accomplish their highly intense and critical tasks. This means that novice threat hunters will have different workflows and therefore different tool support needs. For example, when a threat hunter notices some highly suspicious activity during their daily hunting tasks, a newer threat hunter would feel the need to bring this issue to their supervisor or manager to check their work, before raising the issue higher up in the organization. This is similar to what P1 describes: *"[threat hunters] will raise [suspicious events] to us, the seniors for checking, for double checking, and then, when found that it is malicious, we will be raising that to our manager ... and then, when confirmed [and we] agree that it is really a malicious activity, or an ongoing attack, [we will] notify the client about it."*. Whereas, an experienced threat hunter would be able to take the required action without the extra step of having their work checked. Tools need to be able to support the additional needs of new threat hunters, such as clear communication channels with managers, better data visualization in tools, history or version tracking so they or their managers can retrace their steps, and the ability to create storylines of hunts to be able to communicate what is happening effectively to stakeholders.

Another key finding is that threat hunters rely on their memories to build situational awareness during their hunts (P11, P12). Threat hunters rely on non-technical tools such as notebooks, whiteboards, or programs such as OneNote, to support their memory and document their mental models during hunts. This confirms what Gutzwiller *et al.* emphasized: there is a lack of support for building situational awareness in current cybersecurity tools [26]. It is important to first understand what mental models threat hunters are building and how they are building them in order to provide them with adequate support. Tools that allow threat hunters to externalize their mental models and thoughts, while still keeping this information integrated into their hunting tools will reduce their cognitive strain; ultimately lessening their risk of stress, fatigue, and burnout. Future work should explore what mental models threat hunters are building, how they are externalizing their thoughts and mental models,

and how new tools can support these processes. My research team (Appendix A) and I have conducted a second study that built on the dimensions and the personas of this research. We used observational case studies, with threat hunters at OpenText, to explore in-depth the workflows of threat hunters and how they are building their mental models. We propose a model for the process that threat hunters use to build, externalize, and share their mental models[1].

The the corroboration of existing literature and new findings emphasize the need for better support structures and tools to maintain the well-being and efficiency of threat hunters. Future research should delve deeper into the challenges faced by threat hunters, the strategies they use to mitigate these challenges, and how tools can better support them.

6.3 The Dynamic Nature of Threat Hunting

The increasingly complex dynamics of the threat landscape are driven by cultural, political, and environmental factors and require roles such as threat hunter to adapt and change. Globalization further amplifies the complexity of the threat landscape, as P12 describes: *"What looks [suspicious] in country A is not suspicious in country B. . . . you really have to think about that and think about the impacts"*. In response to these dynamics, threat hunting white papers document how the role of threat hunter has changed over time.

In 2019, Fuchs and Lemon describe how threat hunting is new and still developing [20]. Then in subsequent annual reports (2023, 2024), they describe how the role of threat hunter has matured over time. The role has matured through the standardization and adoption of new methodologies and changes in tooling choice by threat hunters to accommodate their needs [19, 18]. Since 2019, they noted a shift from a reactive approach to a proactive approach [20, 19], that is echoed by the six participants who reported using a proactive approach to hunting (P1, P10, P11, M5, M6, M12). Specifically, P11 said, *"we try to find the threats before they are able to be executed on the machine or find unknowns that are on the machine before they have an impact on the client."*. These findings and reports show that even over a short period of time, the role and needs of threat hunters are changing, presenting a big challenge for providing them with adequate tool support. For example, a tool

[1] https://doi.org/10.48550/arXiv.2408.04348

that supports a reactive approach will not have the same heuristics or features of a tool that is designed to support a proactive hunting approach. Tools designed for a proactive approach should allow threat hunters to make predictions and hypotheses about the threats they look for. Building tools that reflect the threat landscape and the dynamic roles they serve will improve the effectiveness of security and the lived experience of cyber security professionals.

The job market is also affected by the dynamic threat landscape. The increasing demand of threats on the landscape has created a deficit of skilled professionals in critical roles such as threat hunting [49, 47]. The intensity of the role of threat hunting, also exacerbated by the increasing number of threats, leads threat hunters to burnout, stress, and turnover [38]. These pressures are reflected in what participants reported on the challenges they face related to fatigue, information overload, and high job demand. Additionally, 11 of the 17 participants indicated that they have spent two years or less in their current role. This could be the result of higher turnover rates, or it could be due to the job title of "threat hunter" being new. Fuchs and Lemon reported in 2023 that over 75% of threat hunters do not work exclusively as threat hunters. Many participants had obligations to job titles outside of "threat hunter", similar to what Fuchs and Lemon reported, which included job titles such as, "Security Administrator", "Security Analyst", "SOC Analyst", "Security Manager", or "Security Director" [19].

The analysis of the findings revealed that it is not clear what tasks are unique to threat hunting and that the boundaries between threat hunting tasks and tasks associated with other security roles tend to overlap. Future studies should include observational case studies where researchers observe how threat hunters work, to gain a clearer understanding of which tasks are exclusively related to threat hunting and what strategies threat hunters are implementing to manage the intensity of their role.

6.4 Why Personas?

The of the most significant contributions of this study are the identification of 17 threat hunter dimensions and the development of four distinct threat hunter personas: Olivia, Jay, Thomas, and Ren. Each persona represents a unique set of threat hunter dimensions within the cybersecurity community and offer a nuanced understanding of the diverse ways individuals engage in this critical cybersecurity role. These personas and dimensions not only capture the technical and analytical skills, but also the varied

workflows and adaptive strategies used by threat hunters. This novel categorization provides a more detailed and human-centric view of threat hunters. In the following sections, I discuss the benefits and the drawbacks of these personas and how to use these personas to overcome common limitations.

6.4.1 Benefits

Personas are a useful tool that bring the humans behind the work to life. They can evoke empathy and understanding in processes, such as tool development, that are often highly technical [22] and "inject accurate information about real users into the chaotic world of product development" [3, pp. 97]. They can be used to communicate with collaborators and to design better tools for threat hunters.

Communicating with Collaborators

In the context of threat hunting, personas can serve as a communication device between collaborators, to communicate the needs and challenges of threat hunters to one another. Personas help establish a shared mental model between team members, managers, CEOs, and clients. For example, if the CEO of an organization knows the Olivia persona, they would understand how threat hunters like Olivia struggle with generating reports, potentially prompting investment in better reporting tools. Similarly, personas can be used as way of supporting new threat hunters in training and on-boarding, by exemplifying the tasks and skills of more experienced threat hunters. For example, a senior threat hunter resembling the Thomas persona might be tasked with training a new threat hunter who resembles the Jay persona. The two of them could use the personas as a way to find common ground and learn skills such as critical thinking or automation from one another.

The collaboration with OpenText has provided an opportunity to share this research within the organization and with the broader threat hunting community. The dimensions and personas created in this study were shared with other teams within OpenText such as the data science team and the marketing team. Additionally, we collaborated on sharing the technical report to OpenText's LinkedIn page and through a blog post [2] co-authored by my research team and the OpenText team.

[2]Blog post can be found at this link:`https://blogs.opentext.com/a-study-of-threat-hunters/`

Designing Better Tools

Threat hunter personas can also be used in the design of new tools to ensure that tools embody and support the experiences of their users. Personas can be used as heuristics to validate why certain tool features are necessary, or they can be used to illustrate how tool features can appear or behave, given a certain type of user. Personas can also be incorporated into the design process using methods such as *scenarios*, proposed by Nielsen [39], or *design maps*, proposed by Adlin and Pruitt. Both of these methods use personas as the main characters of a design story, centering the primary goals of the design on meeting the needs of the main character and solving their problems. Future work should use the four personas presented, for the ideation, design, and implementation of better support tools for threat hunters. My research team (Appendix A) and I are conducting a further study that build on the personas and the process of creating threat hunter mental models to create design requirements for new tools to support threat hunters. We plan to ideate and prototype promising ideas for further development.

6.4.2 Drawbacks

Regardless of the many benefits of personas, there are limitations to the use of personas. The related literature describes personas as difficult to scale, expensive, and become obsolete (expire) [44], and perpetuating stereotypes, especially related to gender [8].

Scalability, Cost, and Expiration

Even though the personas I created are ready to be used immediately by threat hunters and those who are developing tools to support them, these personas may be used in other contexts such as threat hunting in other industries (health, finance, etc.) or other roles in cyber security (SOC analysts, incident response professionals). Using these personas in other contexts can introduce issues of scaling, cost, and expiration (becoming obsolete) [44]. These limitations can be addressed by customizing personas for the context they are used in.

The persona template, in Appendix G, is a framework that can be used to customize these personas. For example, an organization wants to build better support tools for their threat hunters but do not want to incur the cost of developing per-

sonas. Their threat hunters work in a specific context: providing services for clients in the health and medicine sector. This organization could use the personas I presented here as they may save time, money, and resources. However, there may be some challenges or domain specific tasks that are not currently captured by Olivia, Jay, Thomas, and Ren. Therefore, this organization could consider creating a short survey for their threat hunters, using the dimensions and interview questions from this study (Appendix D), to learn about those context specific details and incorporate them into updated personas. The dimensions provided can be used as a starting point for understanding their threat hunters, but new context specific dimensions are likely to emerge and adding them to the personas will make the personas more useful for tool development. Additionally, as time goes on and threats become more sophisticated, this organization can repeat this process and update the personas to reflect the current state of the threat hunting role.

Other researchers, threat hunters, managers, developers, and designers should consider customizing the personas, Olivia, Jay, Thomas, and Ren, in their own tool development processes, to overcome some of the limitations of personas. They can also expand on these personas by using the methods described in this section to learn about their threat hunters or security professionals in different contexts. Specifically, case studies on threat hunters who hunt in specific sectors, such as health, finance, critical infrastructure, and government, would enrich the understanding of threat hunting tasks and characteristics, ultimately leading to improved support tools for threat hunters.

Stereotyping

As previously mentioned, a common stereotype in cybersecurity is that there is a lack of gender diversity [41], making it increasingly difficult to recruit diverse individuals for high pressure jobs such as threat hunting [47]. Shumba *et al.* hypothesize that the field of cybersecurity is less attractive to women and minority groups because it "is strongly aligned with a hacker-mentality and the military." [47, pp. 5]. However, threat hunters recognize the critical need for diversity and the removal of barriers that exist in their field (P1, P3, M6, M13). Specifically, P3 said, *"there's not enough women in my industry. And because there are not enough women, it's also really hard to attract women because they don't see any role models."* (P3). Personas in particular, can directly reflect or even amplify these stereotypes, but they can also be

used to challenge stereotypes by showing how diversity might appear [8]. Therefore, it is imperative that the tools researchers, developers, and designers create are actively considering the diversity of the threat hunters currently in the field, as well as the diversity threat hunters want to see in the future.

In constructing the four personas, Olivia, Jay, Thomas, and Ren, I considered carefully how to not only mitigate gender stereotypes, but also how to challenge them. Following Burnett *et al.*'s [8] recommendations, I created personas that encompassed a broad range of gender diversity, including a non-binary persona Ren, and ensured that the dimensions of each persona were selected independent of the gender identity of the persona. Participants shared in the member checking surveys that they resonated with the diverse personas. One participant anonymously shared *"the personas presented are representative of the team I work with, and it seems we all face many of the same challenges."*. By reflecting the diversity threat hunters want to see in personas we create, we can encourage a broader spectrum of people to become threat hunters.

6.5 Assessment of Validity

As Miles *et al.* describe, qualitative data emphasizes "people's lived experiences" [36, pp. 11] and the analysis of qualitative data can identify the "*meanings* people place on the events, processes, and structures of their lives and connect these meanings to the *social world* around them" [36, pp. 11]. Though this medium of inquiry is complex and rich, it is important to evaluate the "quality of conclusions" for trustworthiness, quality, and validity [36]. Miles *et al.* [36] use Lincoln and Guba's [32] theory of naturalistic inquiry as the basis for their approach to assessing the trustworthiness of qualitative analysis, describing five criteria: confirmability, dependability, credibility, transferability, and usability. In this section, I assess the validity of the research presented in my thesis using these five criteria: confirmability (Section 6.5.1), dependability (Section 6.5.2), credibility (Section 6.5.3), transferability (Section 6.5.4), and usability (Section 6.5.5).

6.5.1 Confirmability

Confirmability is the expectation of "relative neutrality and reasonable freedom from acknowledged researcher biases" [36, pp. 311]. The methodology and additional material in the appendices, such as the recruitment surveys, interview scripts, member

checking surveys, codebook and samples of coding, and the persona templates, provide the necessary information required to replicate this work. A replication package complete with sample data is not available due to the sensitive nature of working with cybersecurity professionals; security and privacy is critical to participants in this context. Despite the transparent, consistent, and rigorous approach, I acknowledge that different results would emerge from other researchers conducting the same protocols with the same data. In addition to providing all the supplementary materials for replication, careful care was taken to document each of the steps and decision made along the way. Notes were kept on key study design decisions to ensure that the methodology described in the research was clear, traceable, and useful for replication.

I encourage other researchers to replicate this work and to confirm my findings, to continue the discussion and to enrich the findings of this work with new data that emerge over time. Adding to this work will encourage a collaborative and human-centered approach for future threat hunting and cybersecurity research.

6.5.2 Dependability

Dependability is the idea that "the process of the study is consistent, reasonably stable over time, and across researchers and methods." [36, pp. 312]. The research questions of this thesis can be mapped directly to the interview questions, methodology and findings. During the analysis and synthesis of the data, regular inter-coder agreement and reviews by experts (both researchers and industry leaders from OpenText) were conducted to reduce any bias introduced by researchers in the process. Additionally, throughout the study design process, I kept notes in a journal on each study design decision made that was made and the whole research team participated in documenting the processes and analysis methods. This was done to ensure that there was always shared understanding and agreement on the research approach.

Despite the best effort for consistency in the methodology, attrition and turnover of participants occurred. This led to challenges with member checking such as low participation. Additionally, the research team changed over the period of this study (Appendix A). However, this was mitigated to the best of my team's ability, through the retrieval of documentation from parting members and the detailed on-boarding of new members. This ensured that the goals of the study and the methodological philosophy were shared by all the active members of the team.

I recommend to any researchers looking to repeat this work, to conduct analysis

as promptly as possible after the interviews to ensure that participants receive the member checking surveys as soon as possible.

6.5.3 Credibility

Credibility is the notion of *truth value* [32] and answers the question: "Are [the findings] credible to the people we study and to our readers?" [36, pp. 312]. The research team consisted of individuals with backgrounds in computer science and software engineering, with one researcher having experience conducting studies in cybersecurity. To make up for the limited cybersecurity experience, a literature review was conducted and introductory materials from OpenText were provided. I also completed a course that introduced cybersecurity theory and practices, that provided me with a foundation of understanding of the structures, processes, roles, and concepts in cybersecurity.

During the pilot sessions, an experienced researcher (with background in cybersecurity research) guided two other researchers through the process of conducting interviews. They shared techniques on how to ask follow up questions and probe participants for more detailed answers when appropriate. This mentorship allowed for all the researchers to quickly note the suspiciously vague answers from a preliminary participant, that ultimately identified an issue with recruitment and fraudulent behaviour that were later resolved.

Additionally, the study design, preliminary results, and the technical report were shared with the team at OpenText to validate the findings and assert their credibility. Participants also received the technical report to validate the findings. To mitigate challenges with the member checking sessions that I previously acknowledge (Section6.5.2), a second round of the survey was conducted after low participation in the initial round. The challenges could have been due to the time between the interviews and the member checking, but it is likely exacerbated by the limited availability of threat hunters due to the high intensity of the role [49]. Future work could consider validating the findings and personas with tool designers and developers to assess the credibility of the findings in their context.

6.5.4 Transferability

Transferability is the ability for the findings of the study to be generalized to new or different contexts [36]. In this study we conducted 20 semi-structured interviews

with threat hunters. This sample size is consistent with other studies using personas in cybersecurity: an average of 17 participants for one end user persona study [37] and slightly lower than another studies on human factors of threat hunting with 35 participants for a study on burnout in incident responders [38]. Threat hunters and cybersecurity professionals, that face high pressure roles, are known to be difficult to recruit for research studies due to their workload and stress [49]. However, through carefully considered recruitment, the 20 participants interviewed represent threat hunters from diverse educational backgrounds, industries, organization affiliations, use of technological frameworks, and work experience (as cited in the demographics in Section 4.2). Therefore, the findings and the dimensions are likely extendable to a broad spectrum of cybersecurity organizations. I do note that the sample of participants could have been more representative of threat hunters in manager roles such as technical manager, non-technical manager, or CISO (Chief Information Security Officer), and more representative of culture, gender, and geographic location. Future work could consider further exploration of the influence of culture, gender, or location on threat hunting practices.

6.5.5 Utilization

Utilization is the issue of understanding "what the study does for its participants– both researchers and researched" [36, pp.314] and the consideration for the harms and benefits of the research for participants, researchers, and readers alike [36]. All participants were compensated (by OpenText) for their time spent participating in this study and provided with the option to withdraw (themselves and their data) from the study at anytime. Effort was made by the entire research team to provide a welcoming, open, and safe environment for threat hunters in the interviews and subsequent contact for follow-up and member checking. This was especially important given the sensitive nature of the information shared about security, proprietary workflows, tools, and personal experiences or opinions. All the participants were provided with the technical report document. This document is easily accessible physically, through the provided link [3], and intellectually, through having clear writing and summarizing the extensive findings into short highlights. My hope is that the findings, especially the figures, dimensions, and personas, offer actionable insights to threat hunters, managers, CISOs, researchers, and tool designers. These insights should inspire ef-

[3]The technical report can be found at this link: `http://hdl.handle.net/1828/15969`

forts to develop better support systems for threat hunters that improve their lived experiences.

Chapter 7

Conclusions

The goal of my research was to understand threat hunters, who they are, how they work, and the challenges they face to encourage further collaboration between researchers, threat hunters, and industry partners and inspire action towards building tools for threat hunters that support their needs. Through 20 interviews with threat hunters and qualitative analysis the contributions of this work emerged: a description of who threat hunters are and how they work, a description of the challenges they face, 17 threat hunter dimensions, four threat hunter personas, and recommendations for future work and how to use the findings.

The **first contribution** is a description of who threat hunters are and how they work. This description fosters a deeper understanding of the needs of threat hunters and provide the basis for the dimensions of threat hunters and the threat hunter personas. Identifying the *who* and the *how* of threat hunting will encourage developers and designers to consider the needs of threat hunters in the design of new tools.

The **second contribution** is a description of the challenges threat hunters face. This description will guide the process of building solutions for threat hunters by highlighting the exact issues they are facing. The challenges threat hunters face will provide the basis for threat hunter persona pain points and for developing new tools for threat hunters that address real problems and improve their lived experience.

The **third contribution** is a set of 17 dimensions of threat hunters. These dimensions are used to build personas that are grounded in real threat hunter data. These dimensions can be used by others, in any context, to describe threat hunters past, current, and present, and provide customizability and flexibility in personas.

The **fourth contribution** is a set of four distinct threat hunter personas. These personas are design artifacts that document the needs, challenges, behaviours, skills,

tasks, and tools threat hunters use and illustrate the different combinations of dimensions threat hunters represent. These personas can be used as they are or as a foundation for new personas to support the development of better tools.

The **fifth contribution** is a set of recommendations for future work and how to use the findings of this work. These recommendations will inspire action towards developing better support tools for threat hunters and can guide the selection of methodologies in future work.

Together, these contributions answer three research questions: *Who are threat hunters?*, *How do they work?*, and *What challenges do they face?* and provide accessible design artifacts that will support the development of better threat hunting tools that solve the challenges threat hunters face. The findings and contributions of this research highlight the dynamic nature of the threat landscape and threat hunters' proclivity to adapt to it and change to meet its demands. It is up to researchers, organizations, and product designers to support threat hunters in meeting these demands. Researchers and organizations can use the presented dimensions and personas to understand threat hunters and their experiences. This understanding will lead to better tools that support the well being of threat hunters, ultimately creating a more resilient and effective cybersecurity workforce equipped to adapt to an ever-evolving digital landscape.

Bibliography

[1] OpenText ArcSight Intelligence. https://www.opentext.com/products/arcsight-intelligence.

[2] What is hybrid work? https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-hybrid-work.html.

[3] Tamara Adlin and John Pruitt. Putting Personas to Work: Using Data-Driven Personas to Focus Product Planning, Design, and Development. In *Human-Computer Interaction*. CRC Press, 2009.

[4] Bilal Al Sabbagh. *Cybersecurity Incident Response : A Socio-Technical Approach*. PhD thesis, Department of Computer and Systems Sciences, Stockholm University, 2019.

[5] John R Boyd. The essence of winning and losing, 1996.

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

[7] Anna L. Buczak and Erhan Guven. A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 18(2):1153–1176, 2016.

[8] Margaret Burnett, Simone Stumpf, Jamie Macbeth, Stephann Makri, Laura Beckwith, Irwin Kwan, Anicia Peters, and William Jernigan. GenderMag: A Method for Evaluating Software's Gender Inclusiveness. *Interacting with Computers*, 28(6):760–787, November 2016.

[9] Yen-ning Chang, Youn-kyung Lim, and Erik Stolterman. Personas: From theory to practices. In *Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges*, pages 439–442, Lund Sweden, 2008. ACM.

[10] Juliet Corbin and Anselm Strauss. Grounded Theory Research: Procedures, Canons and Evaluative Criteria. *Zeitschrift für Soziologie*, 19(6):418–427, 1990.

[11] Daniela S. Cruzes and Tore Dyba. Recommended Steps for Thematic Synthesis in Software Engineering. In *2011 International Symposium on Empirical Software Engineering and Measurement*, pages 275–284, 2011.

[12] Jayati Dev, Bahman Rashidi, and Vaibhav Garg. Models of Applied Privacy (MAP): A Persona Based Approach to Threat Modeling. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[13] Josiah Dykstra and Celeste Lyn Paul. Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. In *11th USENIX Workshop on Cyber Security Experimentation and Test (CSET 18)*, Baltimore, MD, August 2018. USENIX Association.

[14] Mica R. Endsley and Daniel J. Garland, editors. *Situation Awareness Analysis and Measurement*. CRC Press, June 2000.

[15] Ilker Etikan, Sulaiman Abubakar Musa, and Rukayya Sunusi Alkassim. Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1):1–4, 2015.

[16] Fabian Fischer. *Visual Analytics for Situational Awareness in Cyber Security*. PhD thesis, University of Konstanz, 2016.

[17] Lyndsey Franklin, Meg Pirrung, Leslie Blaha, Michelle Dowling, and Mi Feng. Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. In *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)*, pages 1–8, Phoenix, AZ, USA, October 2017. IEEE.

[18] Mathias Fuchs and Lemon Josh. SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos. Technical report, SANS institute, March 2024.

[19] Mathias Fuchs and Josh Lemon. Survey Threat Hunting: Focusing on the Hunters and How Best to Support Them. Technical Report 8, SANS, 2023.

[20] Mathias Fuchs and Joshua Lemon. SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters. Technical Report 4, SANS institute, 2019.

[21] Shlomo Goltz. A Closer Look At Personas: A Guide To Developing The Right Ones (Part 2). https://www.smashingmagazine.com/2014/08/a-closer-look-at-personas-part-2/, 2014.

[22] John R. Goodall, Wayne G. Lutters, and Anita Komlodi. I know my network: Collaboration and expertise in intrusion detection. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work - CSCW '04*, page 342, Chicago, Illinois, USA, 2004. ACM Press.

[23] Kim Goodwin. *Designing for the Digital Age: How to Create Human-Centered Products and Services*. Wiley, Wiley Publishing, Indianapolis, Indiana, 2009.

[24] Jonathan Grudin and John Pruitt. Personas, Participatory Design and Product Development: An Infrastructure for Engagement. In Thomas Binder, Judith Gregory, and Ina Wagner, editors, *Proceedings of the 7th Biennial Participatory Design Conference 2002*, page 8, Malmø, Sweden, 2002.

[25] Dan Gunter and Marc Seitz. A Practical Model for Conducting Cyber Threat Hunting. Technical report, SANS institute, 2021.

[26] Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. Gaps and Opportunities in Situational Awareness for Cybersecurity. *Digital Threats: Research and Practice*, 1(3), September 2020.

[27] IBM. Cost of a Data Breach Report 2023. Technical report, IBM, 2023.

[28] ITRC. 2023 Annual Data Breach Report. Technical report, Identity Theft Resource Center, 2023.

[29] FortiGuard Labs. Global Threat Landscape Report. Technical report, Fortinet, May 2024.

[30] Thomas K. Landauer. Behavioral Research Methods in Human-Computer Interaction. In *Handbook of Human-Computer Interaction*, chapter 9, pages 203–227. North-Holland, second edition edition, 1997.

[31] Robert M Lee and Rob Lee. The Who, What, Where, When, Why and How of Effective Threat Hunting. Technical report, SANS institute, February 2016.

[32] Yvonna S. Lincoln and Egon G. Guba. *Naturalistic Inquiry*. Sage Publications, Beverly Hills, Calif, 1985.

[33] Abdul Majeed, Raihan ur Rasool, Farooq Ahmad, Masoom Alam, and Nadeem Javaid. Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. *Journal of Ambient Intelligence and Humanized Computing*, 10(4):1509–1526, April 2019.

[34] Tara Matthews, Tejinder Judge, and Steve Whittaker. How do designers and user experience professionals actually perceive and use personas? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1219–1228, Austin Texas USA, May 2012. ACM.

[35] William P. Maxam. Discovering U.S. Government Threat Hunting Processes and Improvements. Master's thesis, Purdue University, West Lafayette Indiana, May 2023.

[36] Matthew B. Miles, A. Michael Huberman, and Johnny Saldaña. *Qualitative Data Analysis: A Methods Sourcebook*. SAGE Publications, Inc, 3rd edition, April 2013.

[37] Benjamin Alan Morrison, James Nicholson, Lynne Coventry, and Pam Briggs. Recognising Diversity in Older Adults' Cybersecurity Needs. In *Proceedings of the 2023 ACM Conference on Information Technology for Social Good*, pages 437–445, Lisbon Portugal, September 2023. ACM.

[38] Subigya Nepal, Javier Hernandez, Robert Lewis, Ahad Chaudhry, Brian Houck, Eric Knudsen, Raul Rojas, Ben Tankus, Hemma Prafullchandra, and Mary Czerwinski. Burnout in Cybersecurity Incident Responders: Exploring the Factors that Light the Fire. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1):1–35, April 2024.

[39] Lene Nielsen. *Personas - User Focused Design*. Human–Computer Interaction Series. Springer London, London, 2019.

[40] Calvin Nobles. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA – Journal of Business and Public Administration*, 13(1):49–72, July 2022.

[41] Bureau of Labor Statistics. Employed persons by detailed occupation, sex, race, and Hispanic or Latino ethnicity. Technical report, Bureau of Labor Statistics, 2023.

[42] OpenText. What is Cyber Threat Hunting? How it Works. https://www.opentext.com/what-is/cyber-threat-hunting.

[43] Paritosh. SIEM + AI Integration Exposes Shocking Threats! Don't Miss These Eye-Opening Insights!, December 2023.

[44] Joni Salminen, Kathleen Guan, Soon-Gyo Jung, Shammur A. Chowdhury, and Bernard J. Jansen. A Literature Review of Quantitative Persona Creation. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–14, Honolulu HI USA, April 2020. ACM.

[45] Tomas Sander and Joshua Hailpern. UX Aspects of Threat Information Sharing Platforms: An Examination & Lessons Learned Using Personas. In *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pages 51–59, Denver Colorado USA, October 2015. ACM.

[46] Kamran Shaukat, Suhuai Luo, Vijay Varadharajan, Ibrahim A. Hameed, and Min Xu. A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, 8:222310–222354, 2020.

[47] Rose Shumba, Kirsten Ferguson-Boucher, Elizabeth Sweedyk, Carol Taylor, Guy Franklin, Claude Turner, Corrine Sande, Gbemi Acholonu, Rebecca Bace, and Laura Hall. Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE Working Group Reports Conference on Innovation and Technology in Computer Science Education-Working Group Reports*, pages 1–14, Canterbury England United Kingdom, June 2013. ACM.

[48] Anselm Strauss and J. M. Corbin. *Grounded Theory in Practice*. Sage, 1997.

[49] Sathya Chandran Sundaramurthy, John McHugh, Xinming Simon Ou, S. Raj Rajagopalan, and Michael Wesch. An Anthropological Approach to Studying CSIRTs. *IEEE Security & Privacy*, 12(5):52–60, September 2014.

[50] Personas - Fluid - Fluid Project Wiki. Online, 2010.

[51] Matthew Trevelyan. Detecting the Unknown - A Guide to Threat Hunting. Technical report, United Kingdom Government, March 2019.

[52] R van Os, M Bakker, R Bouman, M D van Leeuwen, M van der Kraan, and W Mentges. TaHiTI: A threat hunting methodology. Technical report, 2018.

[53] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. Security Practitioners in Context: Their Activities and Interactions. In *Student Research Competition*, page 6, Florence, Italy, 2008.

Appendix A

Research Team

Figure A.1: Research team on this project and their backgrounds of expertise.

The research team I worked with on this research was comprised of 9 members (Figure A.1) in addition to the team at OpenText. The roles of each team member in the research consisted of (R3: thesis author):

- Creating the interview script: R2
- Recruiting participants: R5 + OpenText team
- Validating the recruitment process: R1, R3, R4, R5
- Validating and adjusting the interview questions: R2, R3, R4, R5
- Interviewing: R2, R3 (leading), R4
- Qualitative coding: R3 (leading), R4, R7
- Reviewing and validating the qualitative analysis: R1, R5, R6, R7 + OpenText team
- Summarizing interview data and extracting key quotes: R3 (leading), R7
- Writing the technical report: R3 (leading), R5, R7
- Creating the personas: R3
- Validating the dimensions and the personas (R1, R5, R6, R7 + OpenText team)
- Communicating with the OpenText team: R1, R3 (leading 2024), R5 (leading 2022-2023)
- Preparing presentations for meetings with OpenText team: All
- participating in meetings with OpenText team: All
- Writing of an pending academic publication: R1 - R7, R3 (leading)

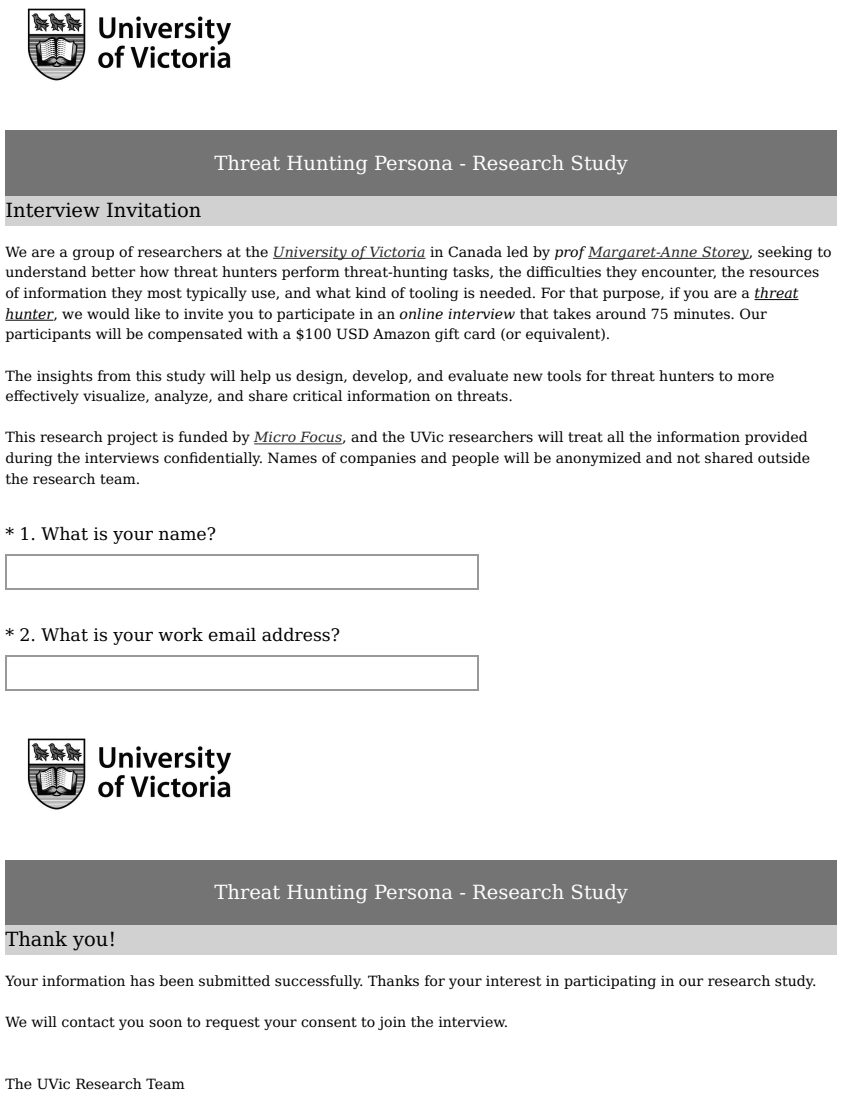
Specifically for the interviews, there were two roles, one interviewer asked the questions the other took notes. The breakdown of each of the interviews and who performed which are in the following table (Table A.1).

Interview	Led by	Notes by
1	R2	R3
2	R3	R2
3	R3	None
4	R3	R4
5	R3	R4
6	R4	R3
7	R3	None
8	R4	R3
9	R4	R3
10	R3	None
11	R4	R3
12	R3	None
13	R4	None
14	R3	None
15	R3	None
16	R3	None
17	R3	None

Table A.1: Summary of the researcher roles during the interviews

Appendix B

Recruitment and Consent Forms



University of Victoria

Threat Hunting Persona - Research Study

Interview Invitation

We are a group of researchers at the *University of Victoria* in Canada led by *prof Margaret-Anne Storey*, seeking to understand better how threat hunters perform threat-hunting tasks, the difficulties they encounter, the resources of information they most typically use, and what kind of tooling is needed. For that purpose, if you are a *threat hunter*, we would like to invite you to participate in an *online interview* that takes around 75 minutes. Our participants will be compensated with a $100 USD Amazon gift card (or equivalent).

The insights from this study will help us design, develop, and evaluate new tools for threat hunters to more effectively visualize, analyze, and share critical information on threats.

This research project is funded by *Micro Focus*, and the UVic researchers will treat all the information provided during the interviews confidentially. Names of companies and people will be anonymized and not shared outside the research team.

* 1. What is your name?

* 2. What is your work email address?

University of Victoria

Threat Hunting Persona - Research Study

Thank you!

Your information has been submitted successfully. Thanks for your interest in participating in our research study.

We will contact you soon to request your consent to join the interview.

The UVic Research Team

Figure B.1: Invitation to participate in interview study posted to LinkedIn

University of Victoria

Improving Cognitive and Collaborative Support for Security Threat Hunters

Consent Form

Thanks for your interest in participating in a study entitled "*Improving Cognitive and Collaborative Support for Security Threat Hunters*" conducted by a team of researchers at the University of Victoria led by prof Margaret-Anne Storey. [redacted]

Purpose and Objectives

This study aims to gain an in-depth understanding of the tasks threat hunters perform, the tools they use, the challenges they face, and how they collaborate with each other and with those in other roles. These insights will inform the generation of innovating analytics and tool supports that will help them do their job more “intelligently” and help keep Canadian systems and data more secure.

Importance of this Research

Today’s threat-hunting tools were developed quickly to meet urgent needs without an adequate understanding of how the tools should work. Furthermore, each threat-hunting activity is part of a larger organizational workflow, and how the many different stakeholder roles collaborate is still poorly understood. Improved tools that harness sophisticated analytics and cognitive support for humans are thus a pressing need.

Participant Selection

You are being asked to participate in this study because of your experience as a threat hunter.

Involvement

If you agree to participate in this research voluntarily, your participation will include an individual interview and a member-checking meeting. A member of the research team will conduct the interview. Then, once when the interview analysis is completed, you will be invited to join a member-checking discussion to validate the information collected.

Risks

Participation in this study may cause some inconvenience to you, including brief distractions from your current activities. The individual interview may last around 75 min however, we can schedule them for the duration of your choice. To avoid this inconvenience, the research team will coordinate with you for the best time to participate in the interview. Please note that this research does not collect information about individual performance in any way. We encourage you to not provide any identifying information that could represent a potential risk for you and your employer. We offer you the possibility of signing a non-disclosure agreement if necessary.

Benefits

The potential benefits of your participation in this research includes a better understanding of the threat-hunting persona, workflows, tasks, and challenges and how tools can provide threat hunters with better cognitive support and collaboration.

Voluntary Participation

Your participation in this research must be entirely voluntary. If you decide to participate, you may withdraw at any time without consequences or any explanation. If you withdraw from the study, your data will be not used in any research articles and will be destroyed. The notes from interviews will also be destroyed.

Anonymity

Apart from identifying information collected by the research team, your anonymity will be protected. The research team for this study will be the only people that have access to this information. We will not inform your managers whether you choose to participate in the study or not. The research team will maintain a way to identify each piece of the data collected to enable follow-up with participants in subsequent research phases. This identifying information will be protected and only in the possession of the research team.

Confidentiality

Your confidentiality and the confidentiality of the data will be protected by being kept electronically on password-protected computers in the CHISEL office at the University of Victoria. No one other than the researchers of this study will have access to information that identifies you within the research data.

Dissemination of Results

It is anticipated that we will share the results of this study with others in the following ways: presentations at scholarly meetings, published articles at conferences or journals, directly to participants in the form of reports made available to your company, and online in the form of a thesis. These reports will not provide information to identify the participants or company names. The researchers will provide publication drafts to the company if requested. The company reserves the right to obfuscate any company-sensitive material from any resulting papers or publications. Data from this study will be disposed of after three years.

Ethics Protocol Approval

In addition, you may verify the ethical approval of this study or raise any concerns you might have by contacting the Human Research Ethics Office at the University of Victoria [redacted]

* 1. Your name:

* 2. Your email:

3. I agree with

☐ I understand the above conditions of participation in this study. I have had the opportunity to have any questions answered by the researchers and consent to participate in this research project.

University of Victoria

Improving Cognitive and Collaborative Support for Security Threat Hunters

Threat Hunter's demographics

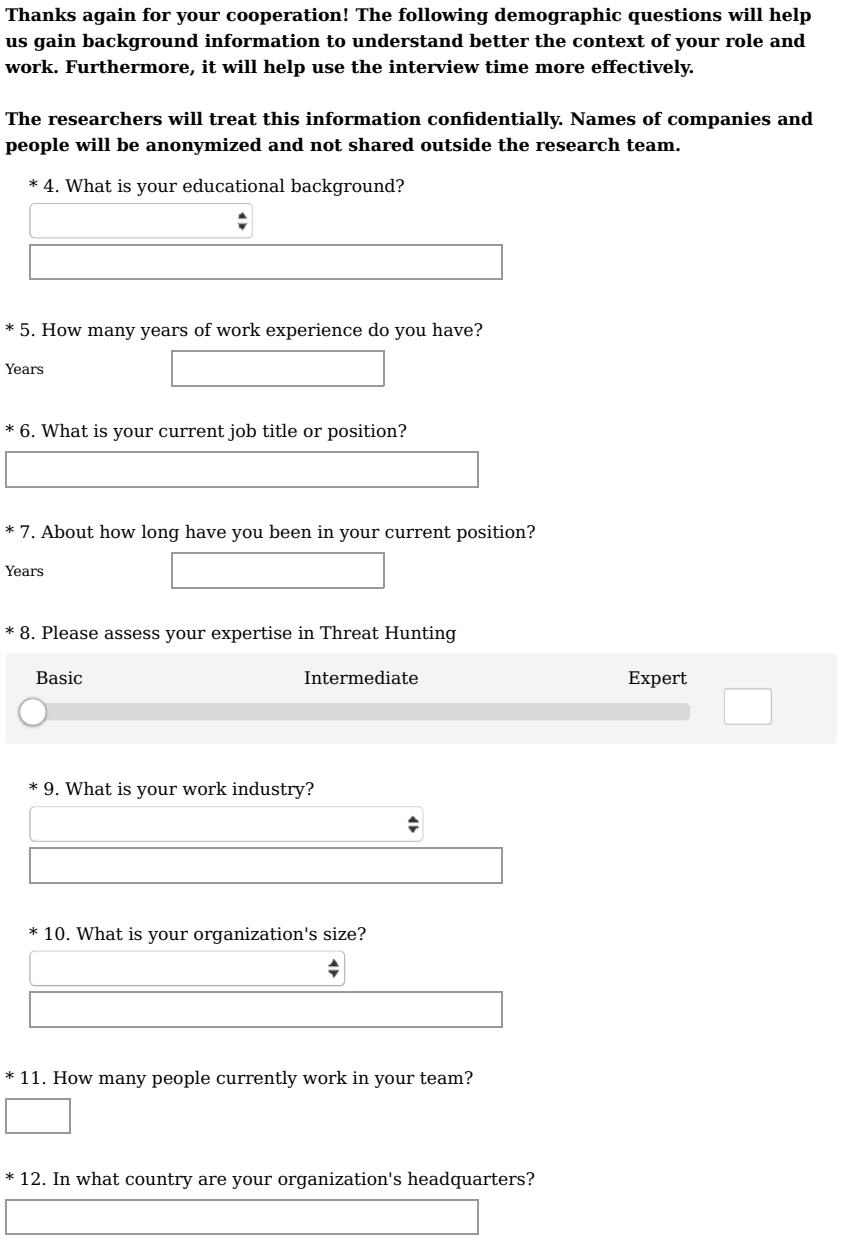


Figure B.2: Survey used to collect demographic information and consent from interview participants

Appendix C

Certificate of Ethical Approval

University of Victoria
Office of Research Services I Human Research Ethics Board
Michael Williams Building Rm B202 PO Box 1700 STN CSC Victoria BC V8W 2Y2 Canada
T 250-472-4545 I F 250-721-8960 I uvic.ca/research I ethics@uvic.ca

Certificate of Approval - Annual Renewal

PRINCIPAL INVESTIGATOR:	**Margaret-Anne Storey** (Supervisor)	**ETHICS PROTOCOL NUMBER:** Expedited review - delegated	**21-0601**
PRINCIPAL APPLICANT:	**Alessandra Milani** **PhD student**	ORIGINAL APPROVAL DATE:	13-Jul-2022
UVIC DEPARTMENT:	**Computer Science COSI**	APPROVED ON:	25-Jul-2024
		APPROVAL EXPIRY DATE:	12-Jul-2025

PROJECT TITLE: **Improving Cognitive Support for Security Threat Hunters**

RESEARCH TEAM MEMBERS:
Callum Curtis - Researcher, University of Victoria
Samantha Hill - Researcher, University of Victoria
Norman Anderson - Researcher, University of Victoria
Marcus Dunn - Researcher, University of Victoria
David Moreno Lumbreras - Researcher, Universidad Rey Juan Carlos
Cassandra Petrachenko - Researcher, University of Victoria
Enrique Larios Vargas - Postdoctoral student, University of Victoria
Arty Starr - Researcher, University of Victoria

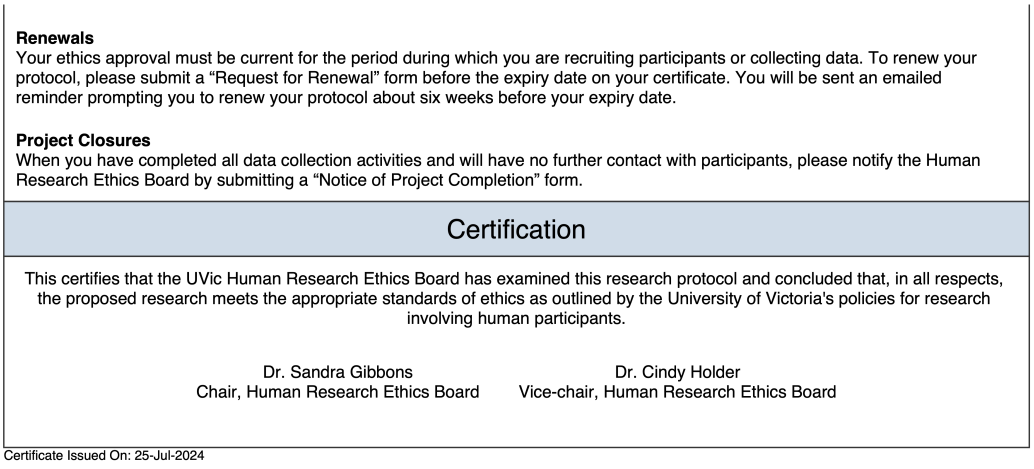
DECLARED PROJECT FUNDING:
NSERC, University of Victoria

DOCUMENTS INCLUDED IN THIS APPROVAL:
Interviews_invitation v1.1.pdf - 12-Jul-2022
FocusGroup_invitation v1.1.pdf - 12-Jul-2022
UserObservations_invitation v1.1.pdf - 12-Jul-2022
tcps2_core_certificate Samantha.pdf - 25-Oct-2022
tcps2_core_certificate Marcus.pdf - 25-Oct-2022
tcps2_core_certificate_Alessandra.pdf - 25-Oct-2022
tcps2_core_certificate Arty.pdf - 25-Oct-2022
Demographics data collection Survey v1.0.pdf - 03-Nov-2022
Interview Protocol - Target Group 1 - v2.0.pdf - 03-Nov-2022
Online interview invitation v1.0.pdf - 10-Nov-2022
Interview Questions - Target Group 2 v2.1.pdf - 23-Nov-2022
Participant Consent Form - Threat hunters v2.0.pdf - 23-Nov-2022
Online consent form and demographics data collection v2.0.pdf - 23-Nov-2022
callum_tcps2_core_certificate.pdf - 02-May-2023
Survey Post-Interview.pdf - 14-Nov-2023
PostInterviewSurvey_Invitationv1.pdf - 28-Nov-2023
Post-interview SurveyMonkey Consent.pdf - 28-Nov-2023
Post-Interview SurveyMonkey Questions.pdf - 28-Nov-2023
tcps2_core_certificate_david.pdf - 14-May-2024
tcps2_core_certificate_norman.pdf - 14-May-2024

Conditions of approval

This Certificate of Approval is valid for the above term provided there is no change in the protocol.

Amendments
To make changes to the approved research procedure in your study, please submit "Amendments" or "Annual renewal with amendments" form. You must receive research ethics approval before proceeding with your amended protocol.



Renewals
Your ethics approval must be current for the period during which you are recruiting participants or collecting data. To renew your protocol, please submit a "Request for Renewal" form before the expiry date on your certificate. You will be sent an emailed reminder prompting you to renew your protocol about six weeks before your expiry date.

Project Closures
When you have completed all data collection activities and will have no further contact with participants, please notify the Human Research Ethics Board by submitting a "Notice of Project Completion" form.

Certification

This certifies that the UVic Human Research Ethics Board has examined this research protocol and concluded that, in all respects, the proposed research meets the appropriate standards of ethics as outlined by the University of Victoria's policies for research involving human participants.

Dr. Sandra Gibbons
Chair, Human Research Ethics Board

Dr. Cindy Holder
Vice-chair, Human Research Ethics Board

Certificate Issued On: 25-Jul-2024

Figure C.1: Certificate of approval for human research ethics. Ethics protocol number: 21-0601

Appendix D

Interview Questions

Demographics

1.1 Could you please introduce yourself a little bit?

Tasks

2.1 What does it mean to be a threat hunter?

2.2 Could you describe your most recent working day? Is this a typical day? Why? Why not? How is your typical working day?

2.3 What was your most recent incident about?

2.4 What are your most common tasks as a threat hunter?

2.5 What are the most common mistakes threat hunters could potentially make?

2.6 How does the threat hunting team deal with a security incident when it is discovered? Is there any systematic process? What are the steps?

2.7 Do you hunt for multiple clients?

2.8 Do you have different techniques when working with clients in different industries? For which industries?

2.9 What are the challenges/barriers you face when performing threat hunting tasks? Have you ever felt frustrated when performing threat hunting tasks? What happened? (Organizational, technical/process, human stakeholders, tools, resources, learning, etc.)

2.10 How would you mitigate those challenges?

2.11 How often do you need to switch to a different task when performing threat hunting tasks? Why?

2.12 What are the causes of interruptions while you're performing threat hunting tasks?

2.13 What would you suggest to improve the productivity/effectiveness of threat hunters?

Tooling

3.1 Could you describe your work environment? (Hardware)

3.2 What technical and non-technical tools do you usually use in your threat hunting activities? Are they always available? Could you describe them? (Non-technical tools such as whiteboard with sticky notes, notebooks, wall maps, etc.) (Technical tools such as SIEM tools, open source tools)

3.3 Do the tools you have used during your threat-hunting activities provide some visualization techniques to support you? Which ones?

3.4 What are the advantages of using those tools? How do they facilitate your work?

3.5 Are there any disadvantages of using them? Which ones?

3.6 What would you suggest to improve those tools?

Resources

4.1 What resources do you usually use/access while performing threat hunting activities? (tutorials, sites, references, communities) Are they always available?

4.2 Could you describe them? How often do you use them? In which scenarios?

4.3 How do you use those resources? Are there any limitations?

4.4 *(If not mentioned in Q1 or Q2)* What resources (or communities) from the dark web do you usually use/access while performing threat hunting activities?

4.5 What would you suggest to improve the use of those resources?

4.6 *(If not mentioned in Q1 or Q2)* How often do you approach online communities? Why? (Forums, mailing lists, meetups, etc.)

Collaboration

5.1 Who are the internal collaborators you usually interact with as part of your threat hunting tasks? Are they usually available?

5.2 Who are the external collaborators you usually interact with as part of your threat hunting tasks? Are they usually available? (e.g., customers)

5.3 How do you collaborate with them? Is it an ad-hoc or systematic process?

5.4 How often do you collaborate with them?

5.5 What tools do you usually use for collaboration?

5.6 How do you hand over at the end of your shift? Can you describe the process?

5.7 How do you communicate information to your managers, specifically?

5.8 What will help you improve your collaboration with other peers?

5.9 How could your organization help you improve that collaboration?

Learning

6.1 What are the core skills (technical and not technical) needed to be a threat hunter?

6.2 What was your personal journey to become a threat hunter? (Mentors, role models?).

6.3 What practices do you usually follow to keep-up-to-date your cybersecurity knowledge? Could you describe your strategy for learning? (Learning by doing, self-taught, trial and error, on the fly education, etc.)

6.4 What does it take for a threat hunter to become confident in performing threat hunting tasks?

6.5 How is knowledge disseminated across threat hunting teams and other stakeholders?

6.6 Do you find it challenging transferring your expertise? Why?

Situational Awareness

7.1 When you are handling a security incident, what are the elements that you need to understand that incident?

7.2 How do you use the elements of your environment to understand the security incident?

7.3 *(If not mentioned in Q1)* How do you know the urgency of a security incident? and How do you differentiate between different security incidents? (How a threat hunter evaluates and differentiates between a critical attack in progress versus a standard script that is unlikely to go anywhere?).

7.4 How do you anticipate future threats and their implications? (individual's ability to project forward in time to anticipate future events, i.e., if the current sequence of suspicious events continues, and they are coming from the same source, then the next likely event will be of a specific type)

7.5 *(If not mentioned in Q2)* What criterion do you usually use when evaluating the urgency of different security incidents?

Behavioural

8.1 From 1 to 5 (5 is highly confident). How confident do you feel about performing threat hunting tasks? Why?

8.2 How would you describe the mindset of a threat hunter? (Analytical mindset, adept at solo work, satisfaction from being the last line of defence, inquisitive personality? etc.)

8.3 What are your motivations for being a threat hunter?

8.4 What are your personal goals as a threat hunter? What makes you a successful threat hunter? Which goals are most important to you? Why?

8.5 What types of rewards or incentives positively influence your work as a threat hunter? Does your organization have any metrics for measuring threat hunting capabilities? Which ones?

8.6 What type of cultural factors do you believe might influence your work as a threat hunter? Why? (Language, norms, values, ethics, attitudes, age, gender etc.)

Appendix E

Member Checking Surveys

Threat Hunting Personas Final Report Feedback

Consent Form

Thanks for your interest in providing feedback for the study "Improving Cognitive and Collaborative Support for Security Threat Hunters''. The study is being conducted by a team of researchers at the University of Victoria led by prof Margaret-Anne Storey. [redacted]

Purpose and Objectives

This survey aims to collect feedback from the participants of the study. These insights will confirm the validity of the findings presented in the Final Report shared with participants.

Voluntary Participation

Your participation in this research must be entirely voluntary. If you decide to participate, you may withdraw at any time without consequences or any explanation. If you withdraw from the study, your data will be not used in any research articles and will be destroyed. The responses from the survey will also be destroyed.

Anonymity

Apart from identifying information collected by the research team, your anonymity will be protected. The research team for this study will be the only people that have access to this information. We will not inform your managers whether you choose to participate in the study or not. The research team will maintain a way to identify each piece of the data collected to enable follow-up with participants in subsequent research phases. This identifying information will be protected and only in the possession of the research team.

Confidentiality

Your confidentiality and the confidentiality of the data will be protected by being kept electronically on password-protected computers in the CHISEL office at the University of Victoria. No one other than the researchers of this study will have access to information that identifies you within the research data.

Ethics Protocol Approval

In addition, you may verify the ethical approval of this study or raise any concerns you might have by contacting the Human Research Ethics Office at the University of Victoria [redacted].

We appreciate if you can provide your response by December 15th, 2023.

* 1. I agree with

☐ I understand the above conditions of participation in this survey. I have had the opportunity to have any questions answered by the researchers and consent to participate in this research project.

Threat Hunting Personas Final Report Feedback

Feedback

Thank you for reading the final report on threat hunting personas from the CHISEL group at the University of Victoria. Please provide your feedback by answering 5 questions below. Your feedback will be used to validate that we are accurately reporting our findings. Your answers will be anonymous.

* 2. What resonated the most with you in this report?

* 3. Were there any findings that you did not expect to see?

* 4. Do you have any new perspective on the threat hunting process after the interview?

* 5.

In terms of the personas, which (if any) do you identify the most with?

* 6. Overall, how was your interview experience?

Figure E.1: Member checking survey distributed to participant with technical report

Threat Hunter Personas Feedback

Consent Form

Thanks for your interest in providing feedback for the study "Improving Cognitive and Collaborative Support for Security Threat Hunters''. The study is being conducted by a team of researchers at the University of Victoria led by prof Margaret-Anne Storey. [redacted]

Purpose and Objectives

This survey aims to collect feedback from the participants of the study. These insights will confirm the validity of the findings presented as personas shared with participants.

Voluntary Participation

Your participation in this research must be entirely voluntary. If you decide to participate, you may withdraw at any time without consequences or any explanation. If you withdraw from the study, your data will be not used in any research articles and will be destroyed. The responses from the survey will also be destroyed.

Anonymity

Apart from identifying information collected by the research team, your anonymity will be protected. The research team for this study will be the only people that have access to this information. We will not inform your managers whether you choose to participate in the study or not. The research team will maintain a way to identify each piece of the data collected to enable follow-up with participants in subsequent research phases. This identifying information will be protected and only in the possession of the research team.

Confidentiality

Your confidentiality and the confidentiality of the data will be protected by being kept electronically on password-protected computers in the CHISEL office at the University of Victoria. No one other than the researchers of this study will have access to information that identifies you within the research data.

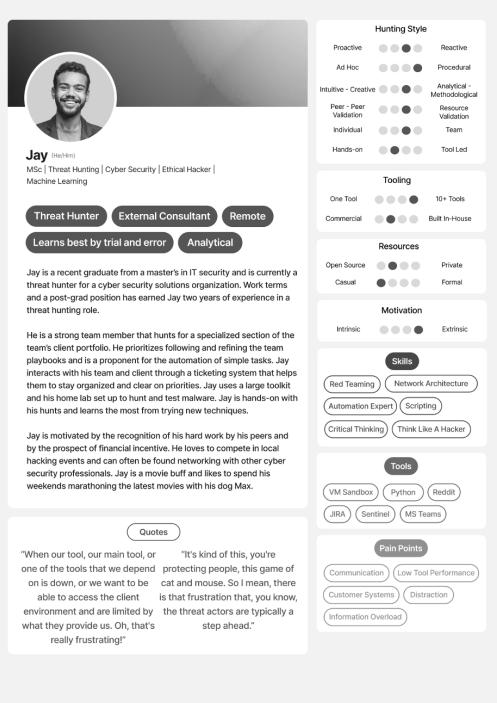
Ethics Protocol Approval

In addition, you may verify the ethical approval of this study or raise any concerns you might have by contacting the Human Research Ethics Office at the University of Victoria [redacted].

* 1. I agree with

☐ I understand the above conditions of participation in this survey. I have had the opportunity to have any questions answered by the researchers and consent to participate in this research project.

* 3.
Jay - Analytical. Automation Expert. Problem Solver.

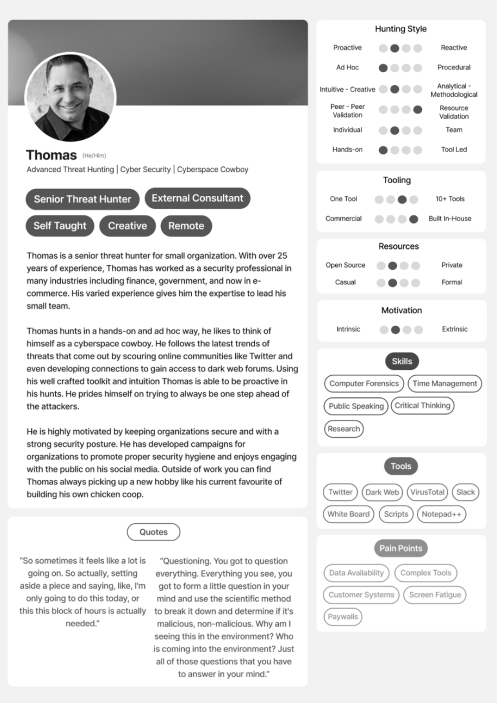


I identify with this persona (Jay).

To a great extent	Somewhat	Very little	Not at all
◯	◯	◯	◯

* 4.

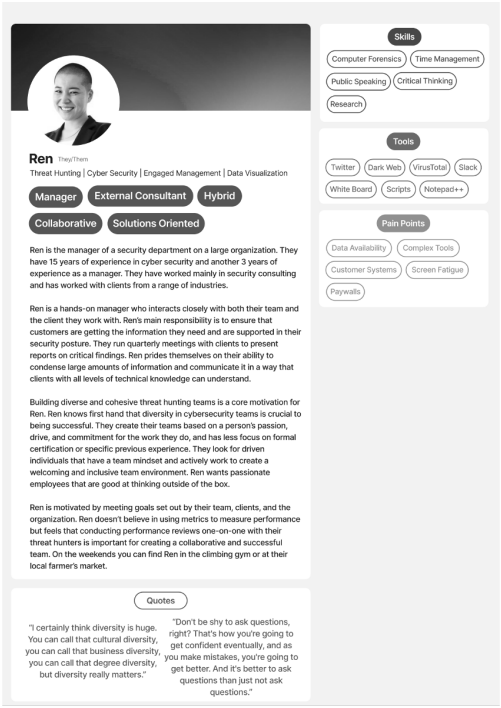
Thomas - Cyberspace Cowboy. Experienced. Self Taught.



I identify with this persona (Thomas).

To a great extent	Somewhat	Very little	Not at all
◯	◯	◯	◯

* 5.
Ren - Manager. Client Relations. Good Communicator.



I identify with this persona (Ren).

To a great extent	Somewhat	Very Little	Not at all
◯	◯	◯	◯

* 6. Of the four personas, **who do you identify with most?**

- ◯ Olivia
- ◯ Jay
- ◯ Thomas
- ◯ Ren

Thank you for taking the time to provide your feedback.

Figure E.2: Member checking survey distributed to participant to confirm which persona resonated most

Appendix F

Codebook

Code	Definition
Experience	Previous experience.
Certifications	Educational experience. ex: professional degree, certification
Work Experience	Work experience. Ex: threat hunting with a different company, experience working in security.
Environment	The work environment.
Physical Environment	The physical environment. Ex: hardware, desk set-up, chair, .
Client Environment	The description of the environment that the client provides access to. (OS, logs)
Social Environment	Social structure and aspects of the threat hunter's environment.
Incentives	Metrics and rewards provided by the environment to motivate threat hunters. Ex: bonuses, recognition.
Organizational Structure	Description of the hierarchy of roles within the organization. Ex: managers, senior threat hunters.
Organizational Culture	Description of values held by the organization or group. Ex: hard work is important.
Workflow	Description of threat hunter workflow of tasks. Processes and order of operations.
Incident Escalation	Description of how the investigation of anomalies are escalated by risk.
Routine	Description of the order in which tasks (technical and administrative) are completed.
Skills	Skills that the threat hunter have or should have.
Non-Technical Skill	Description of a soft skill. Ex: clear communication, working with lots of people.
Technical Skill	Description of a hard skill. Ex: knowing operating systems, blue teaming and red teaming.
Errors	Description of errors that can be made by the threat hunter.
Improvements	Suggestions for improvements to current tools and practices.
Tooling Improvements	Suggestions for improvements to the current tools. Ex: more integration of external tools.
Improvements to practice	Suggestions for improvements to current practices. Ex: more breaks to rest eyes.
Resource Improvements	Suggestions for improvements to resources. Ex: a way to indicate the trustworithiness of a source.
Threat Landscape	Description of the threat landscape (cyberspace). Reasons a threat can exist. Ex: threat actor incentive, systemic vulnerability (lack of talent in threat hunt
Anomaly Description	Description of an anomaly or incident faced by the threat hunter.
Tasks	Tasks completed by the threat hunter.
Administrative Task	Task not part of active threat hunting. Ex: preparing reports, preparing presentations, testing use cases in a lab
Active Threat Hunting Task	Task involved in identifying, anticipating, intercepting or preventing an attack.
Collaborative Task	Task that is a collaboration between two stakeholders. Ex: presenting findings to the client, sharing information with the SOC team.
Collaborators	Description of stakeholders and their relationship to the threat hunter.
Internal Collaborator	Stakeholders within the company. Ex: peers, managers, data science team.
External Collaborator	Stakeholders outside of the company. Ex: the clients.
Collaboration Tool	Tool used to facilitate collaboration tasks. Ex: teams, email, MS notes.
Tooling	Tools used to achieve threat hunting.
Internal Tools	Tools created by the company. Ex: ArcSight Intelligence
External Tools	Tools used by threat hunters that are created by third parties. Ex: VirusTotal, AbuseIP
Non-Technical Tools	Tools that are not directly related to threat hunting. Ex: OneNote, pen, paper, notepad
Positives	Benefits or advantages of current tools and practices. Ex: positive work environment, Arcsight is good for exploring data
Resources	Resources that threat hunters access
Information Resources	Resources access by the threat hunter to stay up to date on information and help their threat hunting. ex: blog, news articles
Communities as a Resource	Resources that are communities in which you interact directly with others in the community. Ex: forums, twitter, facebook groups, dark-web forums
Challenges	Description of challenges faced by the threat hunter.
Collaboration Challenges	Challenges with the collaboration process or collaboration tools. Ex: different learning styles
Interruptions	Interuption of a task or work flow
Personal Challenges	Challenges associated with the person (emotional or physical). Ex: tired eyes, context switching
Tooling Challenges	Challenges associated with the tools both internal and external.
Environmental Challenge	Challenges associated witht the threat hunting environment, physical, social and organizational.
Resource Challenge	Challenges associated with resources (both information and communities).
Characteristics	The characteristics of the threat hunter.
Learning Style	Ways the threat hunter learns. Learning styles. Ex: peer to peer, reading, aural.
Motivation	Reasons for being a threat hunter. Ex: salary, being the last line of defense, setting goals
Mindset	The mindset the threat hunter has or should have. Ex: analytical thinker, dedication.
Sentiment	Feelings or emotions expressed by threat hunters in relation to threat hunting. Ex: frustration, excitement.
Jargon	Words or language specific to threat hunting (domain specific). Ex: visibility of the system.
Journey	The personal journey the threat hunter took to becoming a threat hunter.
Quotable	A direct quote could be pulled from this exerpt of the transcript.

Figure F.1: Codes and their definitions.

Core Cetegories	Sub Categories	Leaf Concepts	Dual Sub-Categories
Core categories are the inner most nodes and are represented by **bold** text. These are generally not used as codes unless a new type of concept is found.	Sub-categories are the next layer of concepts and are represented by standard text. These are generally used as the main codes unless a more specific concept is named in the leaf categories.	Leaf concepts are the final layer of concepts that are the most detailed and represented by *italic* text. These are generally used as codes.	Dual Sub-categories are concepts that fit into two core categories equally and represented by ***bold-italic*** text. These are generally used as codes in the same way that sub-categories are used as codes.
Experience	Education	*Incentives*	***Collaboration Task***
Environment	Work Experience	*Organization Structure*	***Collaboration Tool***
Work Flow	Physical Environment	*Oganization Value*	***Journey***
Skills	Client Environment	*Investigation Barriers*	
Improvements	Social Environment		
Tasks	Incident Escalation		
Collaboration	Routine		
Tooling	Non-Technical Skill		
Positives	Technical Skill		
Resources	Tooling Improvements		
Challenges	Self Care Improvements		
Characteristics	Anomaly Description		
Errors	Threat Landscape		
	Administrative Task		
	Active Threat Hunting Task		
	Internal Collaboration		
	External Collaboration		
	Internal Tools		
	External Tools		
	Non-Technical Tools		
	Communities as Resources		
	Collaboration Challenges		
	Interuptions		
	Personal Challenges		
	Environmental Challenge		
	Tooling Challenges		
	Resource Challenges		
	Learning Style		
	Motivation		
	Mindset		
	Sentiment		
	Jargon		

Figure F.2: Guide for using codebook, rules for coding, category and subcategory labels.

Interviewer	2.1	well okay great yeah could you describe kind of what a typical working day then is when you're hunting		
Interviewee	2.1	yeah so when I start threat hunting I follow		
Interviewee	2.1	a framework that we have. We use tickets right now. But for exaample,	Non-Technical Tools	Information Resources
Interviewee	2.1	with the tension between Ukraine and Russia there are more and more related threats towards our organization.	Threat Landscape	
Interviewee	2.1	Sometimes we received some intel from the intelligence centre team then I check for any threats or risk towards our	Threat Landscape	Internal Collaborator
Interviewee	2.1	organization or not by building a hypothesis	Active Threat Hunting Task	
Interviewee	2.1	Sometimes we have public exposed assets or other times its all internal, then we start following the framework I mentioned	Active Threat Hunting Task	
Interviewee	2.1	I won't give a yes or no answer to this question because based on my experience		
Interviewee	2.1	when I hunt I'm im often facing some many issues in our network and I frequently	Active Threat Hunting Task	
Interviewee	2.1	change my hypothesis but it's one of those techniques that threats hunters have to do to hunt	Active Threat Hunting Task	Non-Technical Skill
Interviewee	2.1	you start with one thing but might switch it up in the middle	Active Threat Hunting Task	
Interviewee	2.1	then I might mean to stop with the first hypothesis but often it's the		
Interviewee	2.1	new threats have will either validate or invalidate the the hypothesis then I'll have to start over a bit	Active Threat Hunting Task	
Interviewee	2.1	But thinking about the tools that I use I use different tools but it depends on the	Active Threat Hunting Task	
Interviewee	2.1	environment right? in some environments I rarely see full access to	Environmental Challenge	
Interviewee	2.1	all logs. But in the sim tools that you have for example you can use just a splunk	Tooling Challenges	
Interviewee	2.1	or sentinel or whatever you as a sim tool that you use then you have access to everything	Tooling Challenges	
Interviewee	2.1	In the majority of the organization I work with they uh just have all the logs available to	Environmental Challenge	
Interviewee	2.1	the sim tools then you need to frequently switch from one tool to another tool because	Tooling Challenges	
Interviewee	2.1	you have some questions that cannot be answered	Tooling Challenges	
Interviewee	2.1	Is that enough detail?		

Figure F.3: Sample of threat hunter interview coding. Anonymized and rephrased quotes for privacy and ethics.

Appendix G

Persona Template

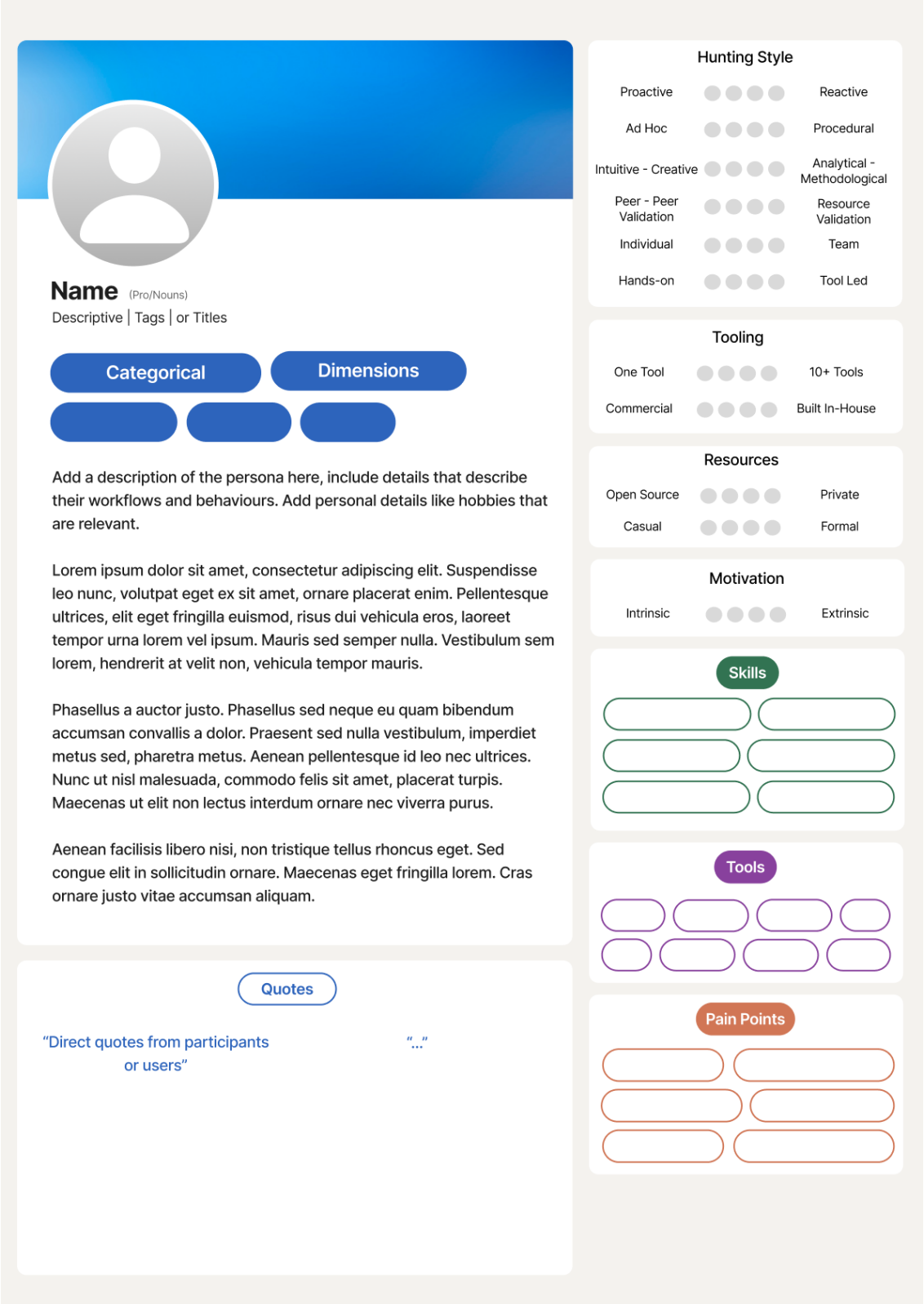


Figure G.1: Template of LinkedIn style persona