Understanding Threat Hunting Personas

Technical Report

November 2023

The CHISEL Group University of Victoria

Table of Contents

Introduction

Who are threat hunters? What does a threat hunting workflow look like? What are the challenges they face? We respond to these, and other questions based on the findings obtained through a mix of qualitative research methods. We briefly introduce the interview process and participant demographics where 20 interviews were conducted with threat hunters from several sectors of industry and different parts of the globe. We discover a rich context of threat hunting practices and tools. We introduce several diverse personas that emerged from our research. We discuss the tools, technologies, resources of information and communities these personas rely on, and how they work together to detect and mitigate threats.

*Disclaimer: The aim of this report is to summarize the findings from the interviews conducted. Report details **only** what participants mention in the interviews. This is **not** a comprehensive list of all tasks, tools, resources, skills, and behaviours. **Duplicates** or **contradictory entries** may appear due to participants reporting them in this way. Technical tools refer to tools that are used in **active threat hunting** processes. Technical tools refer to tools used for tasks **other** than active threat hunting (administrative or communication).*

Research team

University of Victoria, BC, Canada – The CHISEL Group

Margaret-Anne Storey
Professor and Canada Research Chair

Alessandra Milani
PhD Student in Computer Science

Samantha Hill
Master Student in Computer Science

Arty Star
PhD Student in Computer Science

Callum Curtis
Undergraduate student in Software Engineering

+ Former project team members: Enrique Larios Vargas and Marcus Dunn.

For more information about this research project, message chiselgroup@gmail.com

Project sponsors

opentext™

NSERC CRSNG

MITACS

Highlights From the Results

Threat Hunting Process: The threat hunting **workflow** typically consists of retrieving data, shaping data, searching the data for threats, and developing automated detections for identified threats. Common **tasks** for threat hunters include creating presentations and reports, writing scripts to automate simple tasks, researching tools and threats, and submitting recommendations of next steps to clients and management. Two common **mistakes** that threat hunters are at risk of making include overestimating the severity of an anomaly and falsely identifying activity as suspicious or malicious. The greatest **challenges** facing threat hunters include communication with diverse sets of collaborators, high diversity and low visibility of customer systems, and information overload from tools. Tooling is frequently identified by threat hunters as representing a significant opportunity for **mitigating these challenges**.

Tools: Threat hunters rely on a diverse set of **technical** and **non-technical** tools. Selection of technical tools varied significantly between participants. Non-technical tools mainly supported notetaking, presentations and reporting, organization, and communication. For the **list of tools** uncovered by this study, consider the Tools section of the Findings. The most commonly cited **advantages** of existing tools were mitigation of repetitive tasks, followed by stability and support. **Disadvantages** of existing tooling included lack of cohesion between tools, poor performance, and ineffective visualizations.

Resources of Information and Communities: There are a variety of information and community resources used by threat hunters to stay informed; the **list of resources** can be found in the Resources of Information and Communities section of the Findings. The most commonly cited **limitations** associated with these resources included unreliability of information, paywalls, and risks related to maintaining a presence on the dark web. Participants suggested that integrating these resources into their tools or providing a way to verify the trustworthiness of an information source would help **mitigate** these limitations.

Collaboration in Threat Hunting: Threat hunters interact with a broad set of collaborators from the **internal** organization as well as from **external** organizations. Internal collaborators include the security operations center, data science team, and threat intelligence team. External collaborators include the client, cybersecurity insurance companies, and supply chain vendors. For the **list of collaborators** uncovered by this study, consider the Collaboration in Threat Hunting section of the Findings. Threat hunters typically **communicate** synchronously within their teams through shift hand-over meetings and weekly meetings, and asynchronously through messaging platforms such as Slack or Teams. The frequency and rigour of communications depends on the maturity of

the organization, with threat hunting teams in immature organizations often favoring an ad hoc approach. The most cited **challenge** facing collaboration in threat hunting is the geographic dispersion of teams. Threat hunters recommend automating report generation, reducing the number of meetings, and establishing a formal handoff protocol to **improve** collaboration.

Learning Aspects:

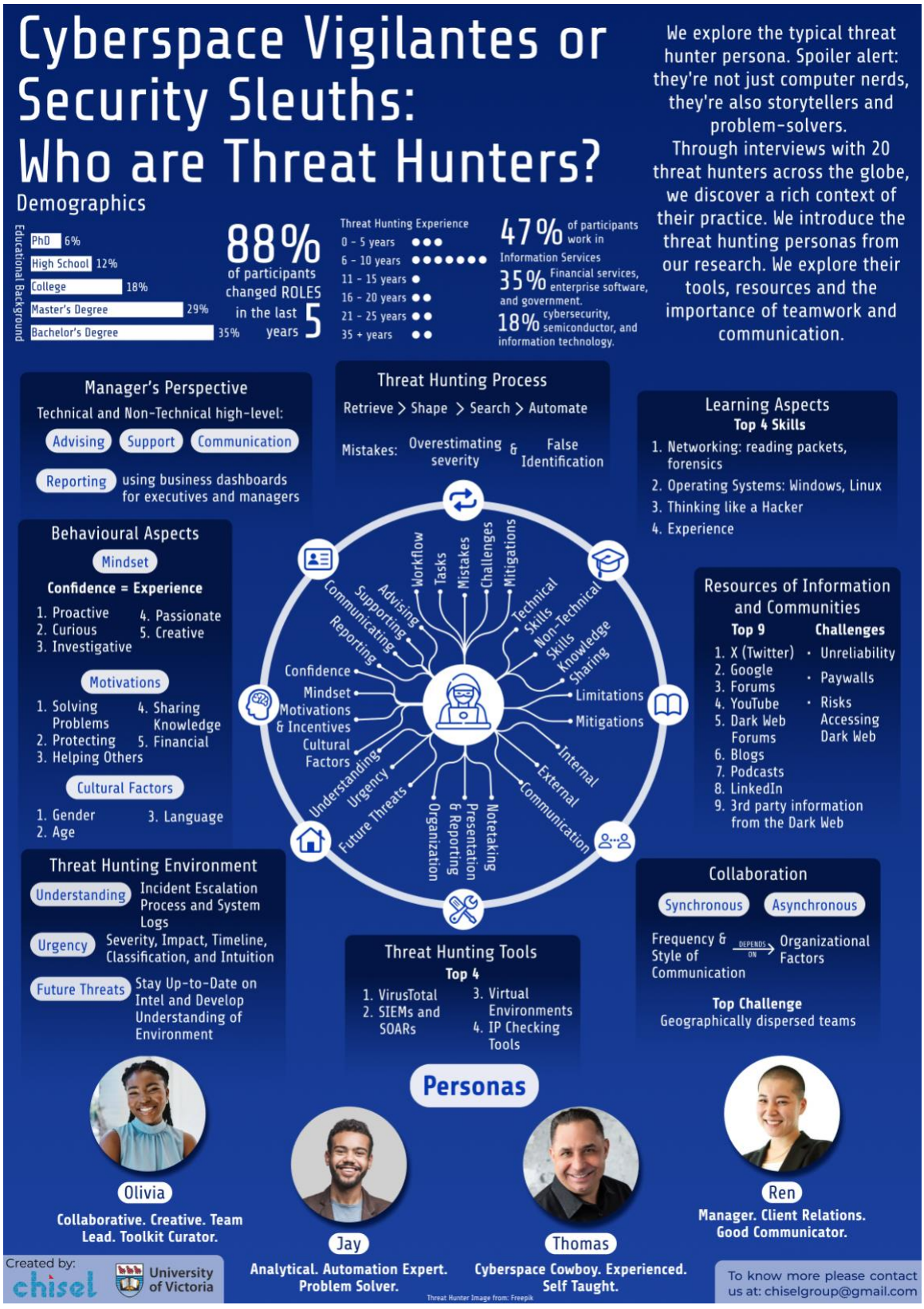
Core technical skills for a threat hunter include knowledge of operating systems, networking, programming, and cybersecurity basics. Core non-technical skills include communication, problem-solving, and analytical ability. Consider the Learning Aspects section for the **technical** and **non-technical** threat hunting skills revealed by this study. Threat hunters **leverage** mentorship, reading articles, watching videos, and completing certifications to learn and stay informed of the latest cybersecurity news. Threat hunters employ meetings, reports, presentations, and conferences to **disseminate** their knowledge and expertise.

Threat Hunting Environment (Situational Awareness): Threat hunters often rely on a formal incident escalation process and system logs to **understand** an incident. To determine the **urgency** of a security incident, the severity, impact, timeline, and classification of the incident is considered, as well as the threat hunter's intuition. In anticipation of **future threats** and their implications, threat hunters stay up to date on current threats and develop their understanding of the environment that they are hunting within to improve their ability to identify abnormal behavior.

Behavioural Aspects: The amount of threat hunting experience was the most commonly cited factor in building a threat hunter's **confidence.** However, multiple participants shared their belief that it is impossible to ever become completely confident in yourself as a threat hunter. The **mindset** of a threat hunter is proactive, curious, investigative, passionate, and creative. **Motivations** for being a threat hunter include solving hard problems, protecting assets or organizations, helping people, sharing knowledge, and receiving monetary compensation. Recognition, from within the organization and from without, as well as financial reward are two common rewards or **incentives** that positively influence threat hunters. The most commonly cited **cultural factors** influencing the work of threat hunters are gender, age, and language.

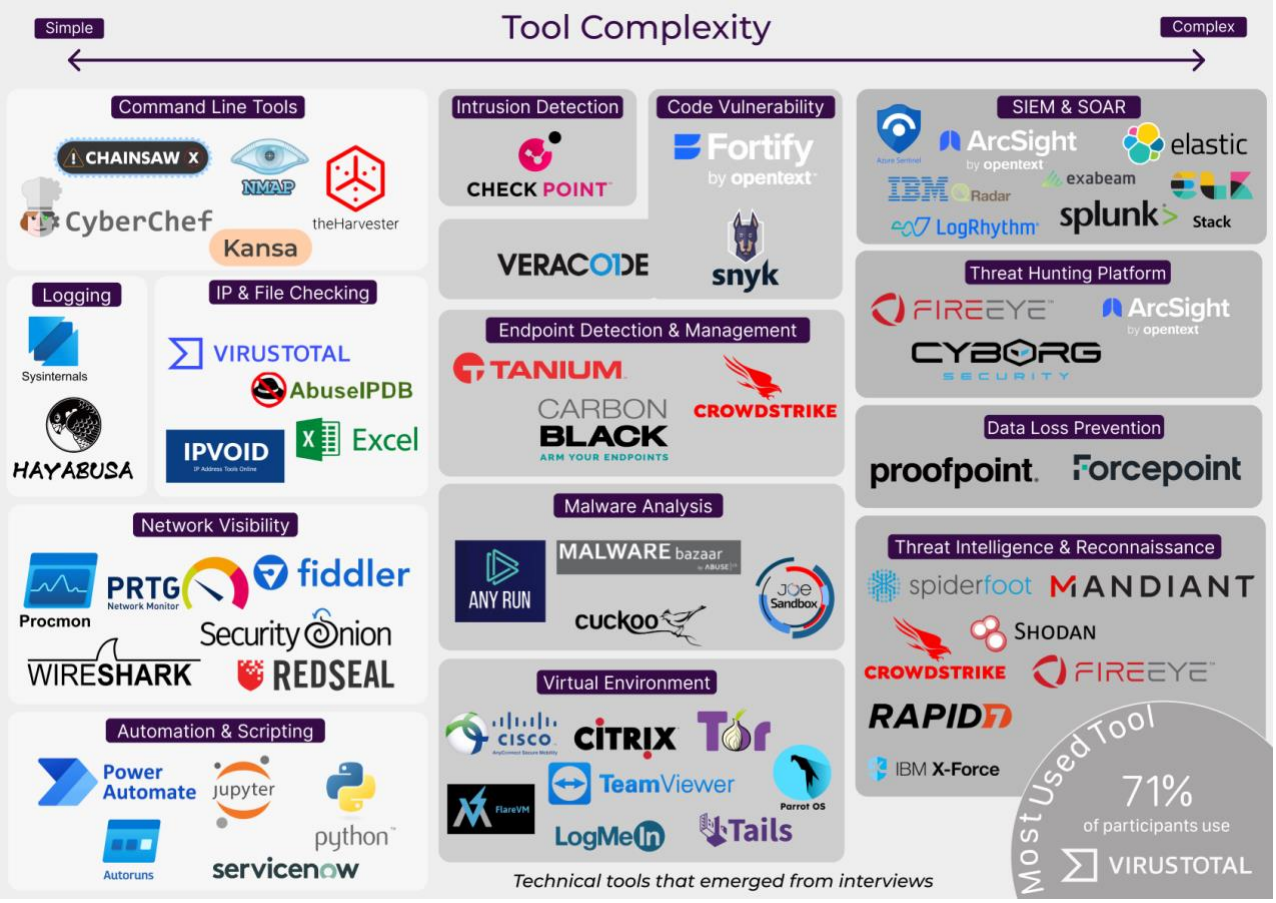
Manager's Perspective: **Tasks** specific to managers of threat hunting teams include high-level security advising, support for active incidents, improving communication processes within and outside of the team, and reporting to executives. Due to their closer relationship with executives and upper management, managers often employ business dashboards for **reporting** purposes.

Highlights Infographic



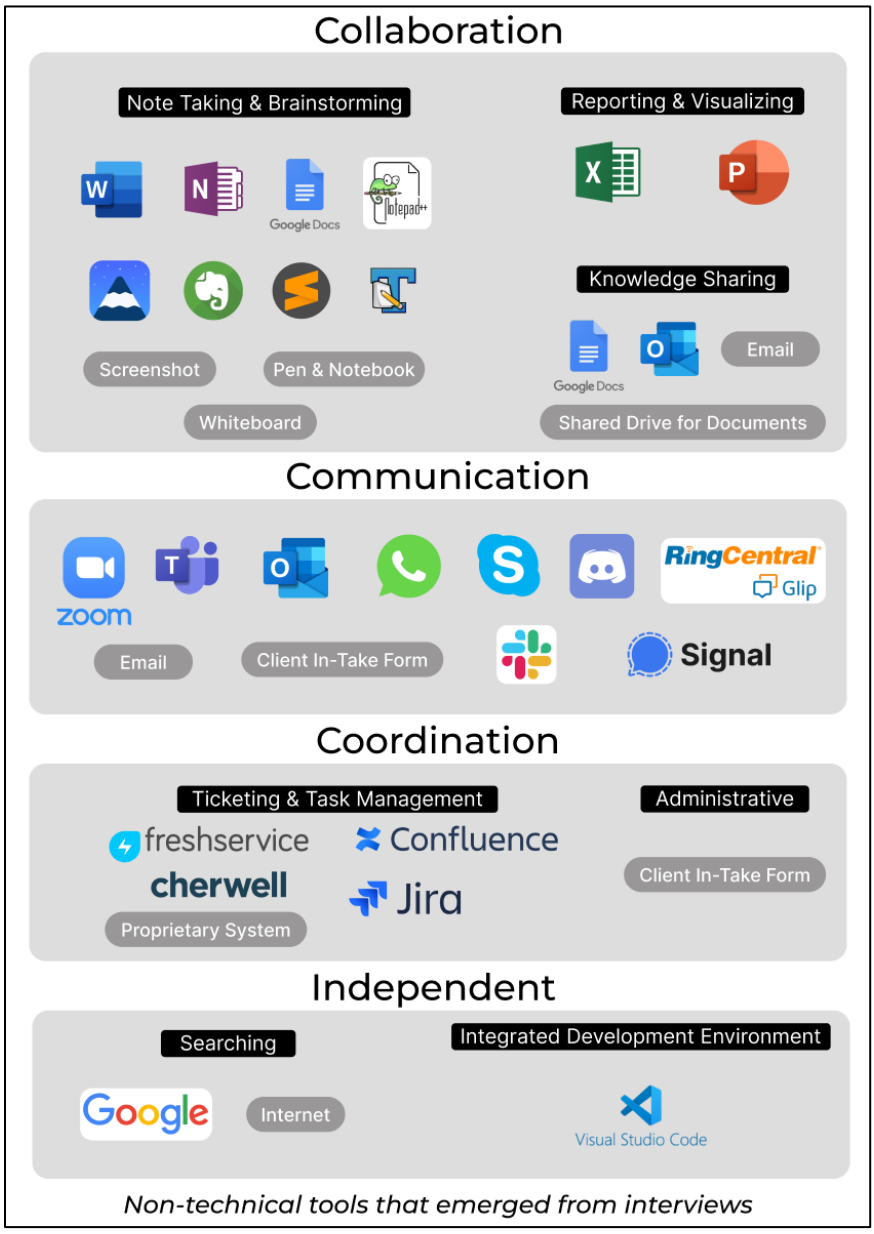
Tool Infographics

Technical Tools (*used to support active threat hunting tasks*)



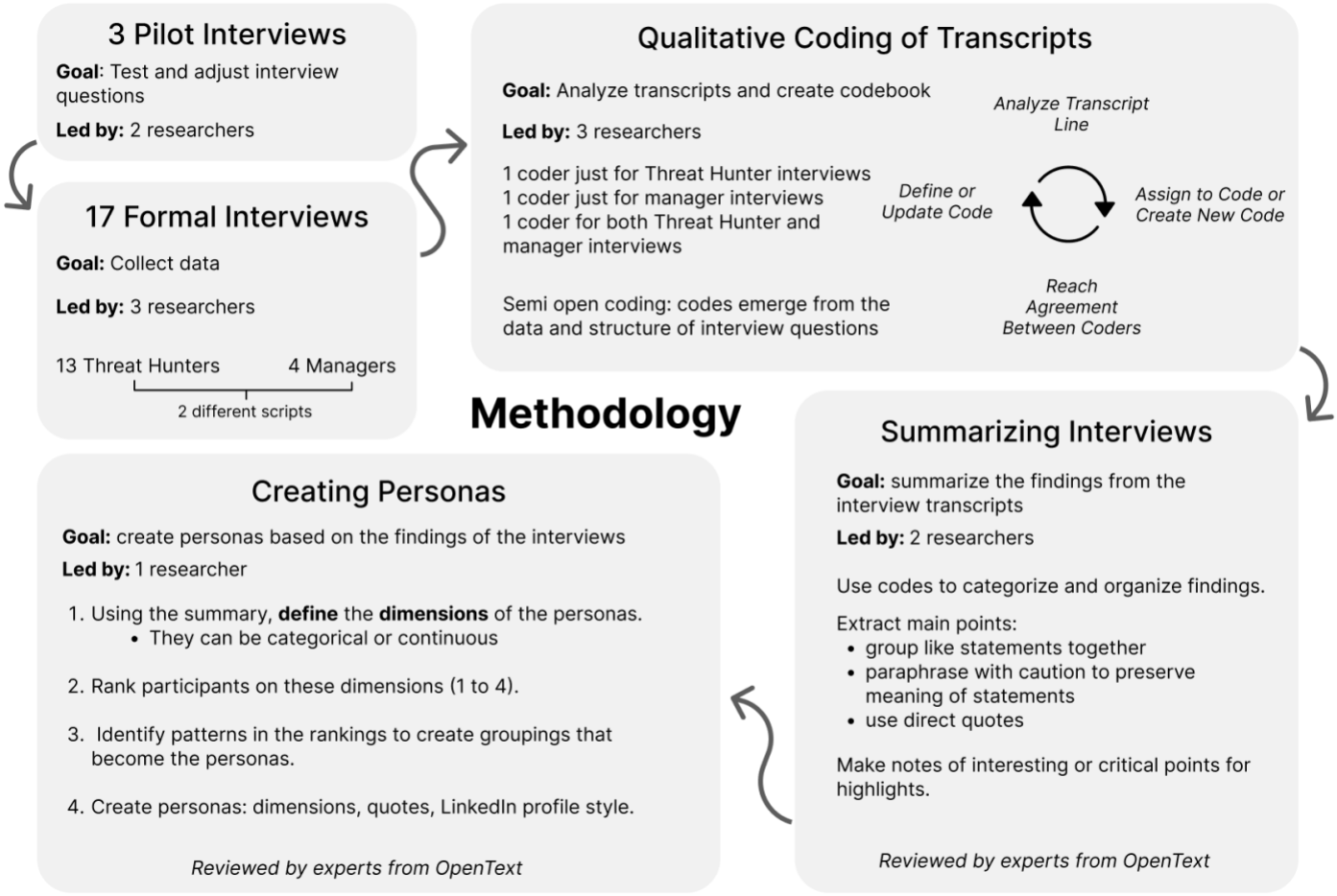
Technical tools that emerged from interviews

Non-Technical Tools (*used to support tasks that are not active threat hunting tasks*)



Non-technical tools that emerged from interviews

Interview Process and Data Analysis



Note: We conducted a total of 20 interviews. The first three were considered pilot and did not follow the same qualitative coding as the following 17 interviews. However, the pilot interviews were fundamental to support with an initial background and to revise the data collection and data analysis strategies.

Participants Demographics

Country (Location)	Total
Not Informed	6
Canada	4
Philippines	2
United Kingdom	2
United States	1
Ireland	1
The Netherlands	1

Educational Background	Total
Bachelor's Degree	6
Master's Degree	5
College	3
High School	2
Ph.D. or Higher	1

Work Modality	Total
Remote	11
Hybrid	5
Not informed	1

Organization Headquarters	Total
Canada	8
United States	5
Brazil	1
United Kingdom	1
Belgium	1
Finland	1

Organization Size	Total
Medium (5k-50K)	10
Small/Medium (1k – 5k)	3
Small (< 1K)	3
Extra Large (> 500k)	1

Work industry	Total
Information Services	8
Financial Services, Banking, and Insurance	2
Enterprise Software	2
Government	2
Cybersecurity	1
Semiconductor	1
Information Technology	1

Team Size	Total
5 years or less	8
6 - 10 years	4
11 - 20 years	2
21 - 30	3

Threat Hunting Expertise	Total
1 (Basic)	0
2	1
3 (Intermediate)	3
4	10
5 (Expert)	3

Work Experience	Total
5 years or less	3
6 – 10 years	7
11 - 20 years	3
21 - 30 years	2
31 - 40	2

Time in the position

About how long have you been in your current position?

Answer range from **1** Year to **19** years.

13 out of **17** participants have been in their current position less than **5** years.

List of the positions

- Threat Hunter
- Senior Threat Hunter
- Lead Threat Hunter

- Threat Researcher
- Senior Threat Researcher
- Lead Threat Research Analyst

- Threat Intelligence Engineer
- Sr Threat Response Analyst

All participants were doing threat hunting, but not always with officially a “threat hunter” position. Other titles include:

- Senior Cybersecurity Consultant
- Security Engineer Tech Lead
- CEO/Principal Consultant
- CISO
- Security
- Platform Engineer

Note: We have not collected demographic information related to age, gender, or ethnicity. This summary does not consider the demographic data from other threat hunters interviewed (e.g., during the pilot).

Personas

In this section, we present three threat hunter personas and one manager persona. These personas were created to represent the threat hunter groups **observed during our interviews**. The personas are aimed to fit a broad spectrum of threat hunters and are **not** intended to be comprehensive. The personas are **not** intended to be traditional organizational personas, they do not necessarily represent the range of threat hunter personas within a singular organization. These personas are intended to represent the main findings from our interviews and a snapshot of what threat hunters look like today in cybersecurity.

First, **Olivia** represents the creative team lead threat hunter who hunts proactively and prides herself in her leadership skills. Second, **Jay** represents the newer threat hunter, fresh from an academic track with excellent analytic skills and a reactive hunting style. Third, **Thomas** represents the most experience threat hunter that works in a small team with an intuitive hunting style. Finally, **Ren** represents a manager who is not directly involved in daily threat hunting but manages the collaboration between a threat hunting team, the clients, and the organization they are involved with.

Note: Dimension definitions can be found in the figure after the personas. Full page versions of the personas can be found in the appendix.

Olivia
Collaborative. Creative.
Team Lead. Toolkit Curator.

Jay
Analytical. Automation Expert.
Problem Solver.

Thomas
Cyberspace Cowboy.
Experienced. Self-Taught.

Ren
Manager. Client Relations.
Good Communicator.

Olivia (She/Her)

Threat Hunting | Cyber Security | Collaborative Solutions | Making Connections

Team Lead **External Consultant** **Hybrid**

Learns best through mentorship **Collaborative**

Olivia is a cyber security professional with over 7 years of experience. She earned her SANS certification during her training under her mentor. She has since become a senior member of a threat hunting team that provides valuable feedback and guidance to her peers. She recently earned a promotion to team lead.

She leads an awesome team of threat hunters through the complex and quickly changing hunts presented by her diverse portfolio of clients. Navigating the threat landscape using a small well crafted tool kit, Olivia's priority is ensuring the safety of customer assets. She frequently communicates with clients to ensure that her team is providing up-to-date information on current threats and how they can help their client stay secure.

Olivia is motivated by the feeling of helping others and by having a strong and connected team. She prides herself in the way that she can empathize with clients and teammates. In her spare time you can find Olivia captaining her local volleyball team and enjoying the theatre scene.

Quotes

"It always has to be peer reviewed. So I have to ask a colleague, hey, this is what I found, can you do a quick sanity check? Does this sound all right?"

" I just know what the tools can provide me. Sometimes weirdly enough, the tool also determines your workflow, right? So I know how to use the tool and then based on that, I create my workflow."

Hunting Style

Proactive	Reactive
Ad Hoc	Procedural
Intuitive - Creative	Analytical - Methodological
Peer - Peer Validation	Resource Validation
Individual	Team
Hands-on	Tool Led

Tooling

One Tool	10+ Tools
Commercial	Built In-House

Resources

Open Source	Private
Casual	Formal

Motivation

Intrinsic	Extrinsic

Skills

Communication | SANS Courses | Storytelling | Network Architecture | Problem Solving | Report Generation

Tools

White Board | IPAbuse | SIEM Tool | MS OneNote | VirusTotal | MS Teams

Pain Points

Report Generation | Customer Systems | Organizational Support | Context Switching | Diverse Personalities

Jay (He/Him)

MSc | Threat Hunting | Cyber Security | Ethical Hacker | Machine Learning

Threat Hunter **External Consultant** **Remote**

Learns best by trial and error **Analytical**

Jay is a recent graduate from a master's in IT security and is currently a threat hunter for a cyber security solutions organization. Work terms and a post-grad position has earned Jay two years of experience in a threat hunting role.

He is a strong team member that hunts for a specialized section of the team's client portfolio. He prioritizes following and refining the team playbooks and is a proponent for the automation of simple tasks. Jay interacts with his team and client through a ticketing system that helps them to stay organized and clear on priorities. Jay uses a large toolkit and his home lab set up to hunt and test malware. Jay is hands-on with his hunts and learns the most from trying new techniques.

Jay is motivated by the recognition of his hard work by his peers and by the prospect of financial incentive. He loves to compete in local hacking events and can often be found networking with other cyber security professionals. Jay is a movie buff and likes to spend his weekends marathoning the latest movies with his dog Max.

Quotes

"When our tool, our main tool, or one of the tools that we depend on is down, or we want to be able to access the client environment and are limited by what they provide us. Oh, that's really frustrating!"

"It's kind of this, you're protecting people, this game of cat and mouse. So I mean, there is that frustration that, you know, the threat actors are typically a step ahead."

Hunting Style

Proactive	Reactive
Ad Hoc	Procedural
Intuitive - Creative	Analytical - Methodological
Peer - Peer Validation	Resource Validation
Individual	Team
Hands-on	Tool Led

Tooling

One Tool	10+ Tools
Commercial	Built In-House

Resources

Open Source	Private
Casual	Formal

Motivation

Intrinsic	Extrinsic

Skills

Red Teaming | Network Architecture | Automation Expert | Scripting | Critical Thinking | Think Like A Hacker

Tools

VM Sandbox | Python | Reddit | JIRA | Sentinel | MS Teams

Pain Points

Communication | Low Tool Performance | Customer Systems | Distraction | Information Overload

Thomas (He/Him)

Advanced Threat Hunting | Cyber Security | Cyberspace Cowboy

Senior Threat Hunter | External Consultant | Self Taught | Creative | Remote

Thomas is a senior threat hunter for small organization. With over 25 years of experience, Thomas has worked as a security professional in many industries including finance, government, and now in e-commerce. His varied experience gives him the expertise to lead his small team.

Thomas hunts in a hands-on and ad hoc way, he likes to think of himself as a cyberspace cowboy. He follows the latest trends of threats that come out by scouring online communities like Twitter and even developing connections to gain access to dark web forums. Using his well crafted toolkit and intuition Thomas is able to be proactive in his hunts. He prides himself on trying to always be one step ahead of the attackers.

He is highly motivated by keeping organizations secure and with a strong security posture. He has developed campaigns for organizations to promote proper security hygiene and enjoys engaging with the public on his social media. Outside of work you can find Thomas always picking up a new hobby like his current favourite of building his own chicken coop.

Quotes

"So sometimes it feels like a lot is going on. So actually, setting aside a piece and saying, like, I'm only going to do this today, or this this block of hours is actually needed."

"Questioning. You got to question everything. Everything you see, you got to form a little question in your mind and use the scientific method to break it down and determine if it's malicious, non-malicious. Why am I seeing this in the environment? Who is coming into the environment? Just all of those questions that you have to answer in your mind."

Hunting Style

Proactive	Reactive
Ad Hoc	Procedural
Intuitive - Creative	Analytical - Methodological
Peer - Peer Validation	Resource Validation
Individual	Team
Hands-on	Tool Led

Tooling

One Tool	10+ Tools
Commercial	Built In-House

Resources

Open Source	Private
Casual	Formal

Motivation

Intrinsic	Extrinsic

Skills

Computer Forensics | Time Management | Public Speaking | Critical Thinking | Research

Tools

Twitter | Dark Web | VirusTotal | Slack | White Board | Scripts | Notepad++

Pain Points

Data Availability | Complex Tools | Customer Systems | Screen Fatigue | Paywalls

Ren

They/Them

Threat Hunting | Cyber Security | Engaged Management | Data Visualization

Manager **External Consultant** **Hybrid**

Collaborative **Solutions Oriented**

Ren is the manager of a security department on a large organization. They have 15 years of experience in cyber security and another 3 years of experience as a manager. They have worked mainly in security consulting and has worked with clients from a range of industries.

Ren is a hands-on manager who interacts closely with both their team and the client they work with. Ren's main responsibility is to ensure that customers are getting the information they need and are supported in their security posture. They run quarterly meetings with clients to present reports on critical findings. Ren prides themselves on their ability to condense large amounts of information and communicate it in a way that clients with all levels of technical knowledge can understand.

Building diverse and cohesive threat hunting teams is a core motivation for Ren. Ren knows first hand that diversity in cybersecurity teams is crucial to being successful. They create their teams based on a person's passion, drive, and commitment for the work they do, and has less focus on formal certification or specific previous experience. They look for driven individuals that have a team mindset and actively work to create a welcoming and inclusive team environment. Ren wants passionate employees that are good at thinking outside of the box.

Ren is motivated by meeting goals set out by their team, clients, and the organization. Ren doesn't believe in using metrics to measure performance but feels that conducting performance reviews one-on-one with their threat hunters is important for creating a collaborative and successful team. On the weekends you can find Ren in the climbing gym or at their local farmer's market.

Quotes

"I certainly think diversity is huge. You can call that cultural diversity, you can call that business diversity, you can call that degree diversity, but diversity really matters."

"Don't be shy to ask questions, right? That's how you're going to get confident eventually, and as you make mistakes, you're going to get better. And it's better to ask questions than just not ask questions."

Skills

Computer Forensics | Time Management | Public Speaking | Critical Thinking | Research

Tools

Twitter | Dark Web | VirusTotal | Slack | White Board | Scripts | Notepad++

Pain Points

Data Availability | Complex Tools | Customer Systems | Screen Fatigue | Paywalls

Categorical Dimensions

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

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.

Experience
1 - (1 - 4 years of experience)
2- (5-9 years of experience)
3 - (10 - 19 years of experience)
4 - (20 + years of experience).

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.

Learning Strategies
Self Taught: TH learns primarily through teaching themselves from resources.
Trial and Error: TH learns primarily by trying and failing in secure environment.
Formal Certification: TH learns primarily through courses and formal training.
Mentorship and Collaboration: TH learns primarily through working with peers or a mentor and getting feedback.

Location
Remote: TH works entirely from a non-office setting / from home.
Hybrid: TH works both remotely and in an office setting.
Office: TH works entirely from an office setting.

Continuous Dimensions

Hunting Style
Proactive: threats are identified before an attack occurs that leverages the threat.
Reactive: response to attacks is done as they appear.

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).

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

Collaboration Mode
Individual: hunting is done individually.
Team: hunting is done as a team.

Validation of Findings
Peer-Peer: TH validate their findings by checking with their peers.
Resources: TH validates their findings by checking resources.

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.

Tool Quantity
One tool: hunts are done with only one tool.
10+: hunts are being done using 10 or more tools.

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)

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.

Formality of Resources
Casual: resources used by threat hunter are like blogs, feeds, or social media and are not peer reviewed.
Formal: resources used by threat hunter is formal articles or literature often peer reviewed.

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.

Findings

Threat Hunting Process

What does it mean to be a threat hunter?

- Proactively detect and analyze security anomalies.
- Be adaptable in unprecedented situations.
- Be up to date on security intelligence.
- Being aware of the current landscape.
- Automated threat analysis.
- A creative process.
- Industry standard definition describes a manual process.
- Forming a hypothesis and testing it.
- Finding the areas in which organizations need to improve their security.
- Thinking like a threat actor.
- Being curious.
- Good situational awareness.
- Have good instincts.
- Advanced forensics.
- Proactive.
- Protecting the general public.
- The last line of defense.

What does a threat hunting workflow look like?

- Handoff, active hunting in ArcSight, incident escalation, peer and manager review, weekly reports.
- Handoff/Review, active hunting with a variety of tools, peer-review, pass-off to appropriate IR team, preparing presentations, and communicating with clients.
- Handoff at a set time to the next shift of threat hunters.
- 9-5 style workdays with no handoff.
- Using logs to identify the attacker's progress in the system.
- Tools, to some degree, determine the workflow.
- Find a threat, record it, search for it in all other parts of the environment.
- Hypothesis, research, hunt, validate hypothesis.
- Scheduled hunts each day.
- Research client organization to understand the threats and customize hunts for those threats.
- Threat called in from another party.
- Hunts are focused on until completion; no task switching until hunt is complete.
- 15 minutes to triage, an hour to give first update.

- Ticket comes in with a threat, type of attack determines, playbook to be used determined, initiate the playbook.
- Identify the threat and its type and what the remediation steps are, identify the people needed to escalate the threat, isolate the necessary machines.
- Get threat assigned, research threat, identify the location of the threat in the environment, create rules in the tools to catch the threat in the future.
- Gather information from the client on the threat, then search the system to find the threat.
- Log-in to TH system, assess the quality of the data, determine if an anomaly is a threat, create rules in the system to block the threats.
- Issues are escalated from tier one up to tier three.
- First responder on issue becomes lead and pulls in other threat hunters and collaborators as needed, escalating to management if not resolved quickly.
- When an incident occurs, use the business continuity plan to collect every collaborator you need to respond and reach out to relevant vendors in your supply chain.
- Threat hunting team creates report on incident and hands it to an incident commander to lead the response.
- Get the data, sculpt the data, search the data, find the bad, develop a detection to automatically find the bad later.
- Gain permission from management to pursue a hypothesis.
- Normally no more than two threat hunters work on the same mission.
- Find suspicious event, determine if false positive, ask colleagues for advice, escalate to manager, tackle the incident.

What are the common tasks of threat hunters?

- Reviewing use cases.
- Checking ticketing systems and completing tasks.
- Triaging alerts generated through automated processes.
- Creating presentations and reports.
- Organizing and running meetings with peers.
- Find vulnerabilities, mitigate them, and apply to production.
- Create courses for non-threat hunters to learn about security.
- Most urgent threat first.
- Keep an append-only journal for the hunt that cannot be modified.
- Gathering intelligence and indicators of compromise (IOCs).
- Handling all communication with a specific client.
- Analysis.
    - Timeline analysis.

    - Artifact analysis.
    - Analyze the logs.
    - Analyze raw data.
- Writing scripts that automate simple tasks.
    - Fixing scripts/code.
    - Developing tools for exfiltration.
    - Pulling data.
- Formulating a hypothesis
- Researching threats and tools.
- Create, execute, and maintain queries.
- Create rules to detect malicious files.
- Find zero-day threats.
- Checking rare processes in a system.
- Check for failed log-ins.
- Making recommendations for next steps to clients and management.
- Documenting important parts of hunts for colleagues and clients.
- Create play books.
- Do table-top exercises.
- Managing 4-5 clients at a time.
- Understanding the client's environment.
- Check for any notes or pending task from previous threat hunters.
- Marking files as malicious.
- Understanding the client's environment.
- Check for any notes or pending tasks from previous threat hunters on the hunt.
- Marking files as malicious.
- Understand the attack vectors that the attacker used.
- Analyze business goals.
- Keep detailed asset inventory.
- Create network maps.
- Root cause analysis.
- Writing custom detections in an EDR tool.
- Searching through communications within an organization for expressions of concern about a vulnerability.
- Determining the severity of incidents reported by lower-tier personnel.

What are the most common mistakes threat hunters make?

- Overestimation of the severity of an anomaly and inappropriately raising the incident to the customer.

- Knowing the boundaries of the role and not taking on too much.
- Cutting corners in the hunting process.
    - Lack of attention to detail.
    - Move past things too quickly.
- Human error that could be solved by automation.
- Over rely on tooling.
- Not learning your tool well.
- Misidentifying suspicious activity – type 1 errors.
- Not collecting enough evidence to be able to report on or analyze an alert.
- Poor communication of the stage of a threat.
- To feel safe.
- To stop looking.
- Making assumptions.
    - Assuming a task is easier than it is.
    - To assume the threat is exactly what is seems.
- Being reactive and not proactive.
- Miss something.
- Trusting the wrong information and following the wrong path.
- Jumping to conclusion of what something means.
- Not looking at enough information.
- Falling into a routine.
- Not continuously searching for new and better tools.
- Relying on a single tool and not considering its limitations.
- Creating a hypothesis too early due to bias.
- Over multitasking especially because of mundane tasks.
- Jumping to a conclusion and using your tool to confirm your bias.
- Not investigating an anomaly all the way to the root cause.

What are the challenges threat hunters face?

- Customer systems.
    - Poor visibility into customer systems.
    - Client environments being diverse.
    - The software the client uses dictates the procedure.
- Having to convince your team that a given threat can exist and it is serious enough to worry about.
- Physical tiredness.
    - Tired eyes.
    - Screen fatigue.

- Context switching.
    - Between clients
    - Between hunting and administrative tasks.
- Tooling issues.
    - Internal tooling issues.
    - Tools not having up to date or complete information.
    - Cost of tools/tech.
- Challenges brought on by the organization.
    - Working for a large organization. Challenges not being addressed quick enough.
    - Working for a company that does not adequately support them.
    - Conflict over resource allocation between teams.
    - Security is not prioritized by other teams in the organization.
    - Organizational culture is to not share info about the threats in other teams.
- Distraction.
- Information Overload.
- Interruptions.
- False positives.
- Communication challenges.
    - Communicating information at an appropriate level of complexity and in the appropriate context for collaborators outside of the threat hunting team.
    - Information is sometimes hard to put into words or writing.
    - Identifying the right person to reach out to.
- Data availability.
- Data retention.
- People.
    - Having different learning styles from peers.
    - Users of a system cause unintentional security issues.
    - Getting responses from the client or stakeholders in a timely fashion.
- Making the right queries.
- Unknown threats (zero-day threats).
- High volume of threats and not very much time.
- Knowing what information to trust.
- Client not taking recommendations into practice. Threat hunters then dealing with the same threats over and over.
- Senior threat hunters having to help put out fires rather than being proactive.
- Caught between management and lower-tier cybersecurity analysts.
- Blocked because of lack of access or due to pending items belonging to others.

- Conflict between usability and security which make users reluctant to adopt stricter security measures.
- Too many meetings.

What do threat hunters recommend to mitigate those challenges?

- Tooling.
    - Integration of external tools and resources into the main tool.
    - Versioning or tracking action history.
    - Automation of simple tasks.
    - Getting the right tools.
    - Knowing the tools well.
    - Improving tool performance.
    - Tools run on autopilot until a risk surfaces.
- Time management.
- Steps the organization can take.
    - More knowledgeable management
    - Organization values work-life balance.
- Not doing some more menial administrative tasks.
- Clear communication.
- Getting comfortable in your environment (both digital and physical).
- Stay up to date on intel.
- Communicate the repercussions of not implementing good security.
- Escalate access challenges up the management chain.
- Think like an attacker.
- Developing good relationships with other teams in the organization.
- Practice the workflow to streamline it.
- Develop a better understanding of where to hunt in databases.
- Audit logs to ensure the data collected is what is needed.
- Whitelisting legitimate files.
- Collect more data.
- Make more data available.
- Understand the threat being dealt with.
- Understand personal work styles.
- Reduce bias by using AI as a more impartial judge that considers the data alone.
- Try to avoid escalating an incident to tier-three to avoid taking up time of collaborators.
- Document findings carefully.
    - Document findings that were not addressed or could not be addressed.
- Cross-training and rotating tasks to prevent boredom and broaden understanding.

Tools

What are the tools that threat hunters use for threat hunting?

Technical (used to support active threat hunting tasks)

- IP Abuse
- AbuseIP DB
- VirusTotal
- ArcSight
- Tor
- FireSoto
- Citrix
- Sentinel
- Tanium
- Firewalls
- Excel
- Microsoft Flow
- X-Force
- Internally developed scripts
- Rapid7
- CrowdStrike
- EDR - Endpoint Detection and Response
- Elk Stack
- Chainsaw
- Jupyter notebooks
- Sysmon
- Kibana
- Shodan
- SaaS tools for code review
  - Veracode
  - Snyk
  - Fortify
  - Unique Saas Tool
- Nasus from Azure
- Virtual Machine
  - Linux box
  - Flare VM
- Parrot OS
- Virtual Machine for dark web
  - Tails
- Nmap
- Kanza
- Wireshark
- Spiderfoot
- Harvester
- Splunk
- Python
- Mandiant
  - Mandiant Mirror
- Lab set-up at home
- ADR – advanced detection and response
- IDS – intrusion detection system
- Security onion
- Elastic certs
- ExaBeam
- CyberChef
- IPVoid
- TeamViewer
- LogMeIn
- AnyConnect
- VNC
- Cyborg Security Hunter
- Hayabusa – Log ingester
- LogRythm
- QRadar
- Proprietary tool – details not specified.
  - CrowdStrike proprietary tools
  - SIEM Tool
  - Databases
- FireEye
- Kubrows
- Atlas
- Carbon Black
- AnyRun
- Malware Baazar
- Command line
- Checkpoint
- PRTG – Paessler Router Traffic Grapher
- Proof Point – data loss prevention tool
- Enforce Point – data loss prevention tool
- Autoruns
- Procmon

- Fiddler
- PA Studio – check metadata of an executable
- Sandboxes
  - Joe sandbox
  - Cuckoo
- UEBA
- RedSeal
- Service

Non-technical (used to support tasks that are not threat hunting tasks)

- Pen/marker
- Notepad/Notebook
- Google doc
- WhatsApp
- RingCentral
- GLIP
- Discord
- Email
- VS Code
- Signal
- Skype
- Cherwell
- Confluence
- Slack
- Zoom
- Antivirus
- Password manager
- Ticketing system
  - JIRA
  - FreshService
- Shared drive for documents
- Whiteboard
- Screenshot
- Internet
- Tools that already exist in client environment
- Intake form for client called-in threats / incidents.
- Microsoft Office Suite
  - MS teams
  - OneNote
  - Excel
  - PowerPoint
  - Word
  - Outlook
- Notetaking app
  - Sublime Text
  - Up notes
  - Notepad++
  - TextPad
  - Evernote

Note: Duplicate entries of tools in technical and non-technical categories means that participants reported the use of these tool to support both active threat hunting tasks and tasks outside of active threat hunting.

What are the advantages of those tools?

- Beneficial to have threat hunting specific system, since the corporate SIEM may not ingest all relevant data.
- Beneficial to have tools in the cloud so they can be accessed by the entire team.
- Showing the right information when needed.
- ArcSight is good for exploring.
- Tools reduce the number of repetitive tasks – automation.
- Features to help take down copycat or phishing domains.
- Tools reduce the number of repetitive tasks.
- Tools being used are stable and have few flaws.
- Think out loud – brainstorming ideas on a whiteboard.
- Mainstream tools have communities that offer support.
- Ability to share your work with peers.
- Being able to easily search.

- Take in data from various sources.
- Visualize data with charts, graphs, and maps.
- Continuity over lots of platforms.
- Open-source tools provide free information.
- Combining tools will give you a more complete picture of a threat.
- Bigger screens mean less scrolling and more productivity.
- Proprietary tool simplifies the process of threat hunting.
- Use of AI to detect anomalies in the event data.
- The tools cover everything a threat hunter needs to be effective.
- Enable the threat hunter to execute a remote script to collect data that may otherwise be invisible.
- Ability to write custom detections.
- Ability to tune alerting to mitigate alert fatigue.
- API access to automate a lot of processes with the tool.
- Splunk shows you all the needed information from the beginning.

What are the disadvantages of those tools?

- Have to open new tabs to access web-based tools that are not part of ArcSight.
- QRadar and Digital Shadows have graphs that are not significantly useful or exciting.
- Every tool claim to be mission-critical so it's hard to tell which to use.
- Rate limiting on external tools.
- Machine Learning / AI is new so not matured and can be a limitation to threat hunting due to the higher number of false positives.
- Graphs not making sense.
- Performance of tools could be better.
- Usability of tools could be better.
- Lacking up to date information on new threats.
- Takes configuration, steep learning curve.
- Tools not being secure enough.
- Information overload.
- Tool influences the workflow.
- Tools made by the threat hunter may not be stable or maintained.
- Open-source tools may change a lot and may not be stable.
- False positives.
- Not able to change the criticality of a finding in the tools.
- Tools not aggregated into one platform.
- Not being able to easily interface with or integrate with existing tools.
- Tools are built for specific platforms.

- There's no standardized way of threat hunting.
- Relying on automated processes leads to reduced hunting speed.
- Fidelity of tools.
- Too many settings on tools that THs don't have time to set.
- Reporting is very technical and doesn't always have a visual component.
- Tools don't provide enough information.
- Visualizations.
- Rules must be maintained and refined constantly.
- Physical notes are vulnerable to insider threats.
- Performance of tools depend heavily on quality of data.
- Tools are improving but rely on accurate asset inventory which is typically lacking.
- Visualizations look good on reports but don't effectively help you find the bad.
- Tools that run remotely on endpoints must be performant to avoid disturbing users in the organization.

What does the physical environment of a threat hunter look like?

- Work environment style (remote/hybrid/in-person).
- Computers.
    - Laptop.
    - Dedicated machine(s) for air-gapped environments.
- KVM to swap between computers.
- Monitors (ultrawide, single monitor, dual monitor, etc.).
- Supporting tech (iPad, raspberry Pi, etc.).
- Office equipment.
    - Standing desk.
    - Comfortable chair.
    - Wireless keyboard/mouse.
- Network simulation equipment.
- VPN.
- NIST cybersecurity framework poster.
- Music.
- Always chat window open on one monitor.
- Good speakers to listen to music.

Resources of Information and Communities

What resources of information and communities do threat hunters use?

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

What are the limitations of those resources of information?

- Dark web - not from the company computer, forums are by invitation only.
- Expensive to maintain a presence on the dark web and collect information.
- Risky to maintain a presence on the dark web and collect information.
- A lot of work to maintain a safe environment to access the dark web from.
- Some are not up to date in the face of software updates (software update appeared as an anomaly but the process did not appear in any resources).
- Limit to the number of searches they can perform a minute.
- Not worth staying up to date with the latest exploits for their organization.
- Behind a paywall.

- Information is confidential.
- The hunting might be in a very specific domain and resource support might not exist for this domain.
- Information is not concise, and the knowledge needed needs to be distilled from a larger resource.
- Information may not be reliable.
- Resources are limited by how well a threat hunter can ask a question.
- Information overload.
- Free resources may not share all the information.
- It is difficult to achieve full coverage of a threat.
- May have limited licenses available for an organization.

What do threat hunters recommend to improve those resources?

- Better integration of resources into the main hunting tool.
- Having a way to verify that a resource can be trusted.
- Accepting that there may be some unanswered questions.
- Have a way to share more details about findings.
- Normalization/standardization of information.
- Standardization of queries.
- Better accessibility.
- Organization to provide paid access to resources.
- Use of AI to ingest and query organizational data.

Collaboration in Threat Hunting

Who are the collaborators that threat hunters usually interact with?

- Separate teams for different incident severity levels.
- Collaborate closely with red team, purple team, threat hunters, threat intel, data loss prevention, and insider threat.
- Dependent on the incident could be collaborating with anyone in the internal or client organization.
- **Internal**.
    - Teammates.
    - Managers.
    - Developers.
    - System architects.
    - Teams.
        - SOC.
        - Consultancy.
        - Data science.
        - Threat intelligence.
        - IT.
        - DevOps.
        - Red.
        - Blue.

    - System administrators.
    - Security researchers.
    - Other threat hunting teams in other areas globally.
    - Threat operations.
    - Incident response.
    - Network operations center.
    - Customer support.
    - Sales.
    - Legal.
    - Pen testing.
    - Endpoint management.
    - Product development.
- **External**.
    - Customer/client.
    - Customer SOC.
    - Customer data center team.
    - Product owner of tools.
    - The public.
    - Security researchers.
    - Mentor.
    - Vendors and supply chain.
    - Cybersecurity insurance company.

What does the collaboration process look like?

- Communication.
    - **Internal**.
        - Slack.
        - Teams.
        - WhatsApp.
        - SharePoint.
        - Email.
        - Signal.
        - In person.
        - Telegram.
        - Discord.
        - Telephone.
        - Zoom.
        - Zapier.
        - Trello.
        - Ticketing system.
    - **External**.
        - Email.
        - Teams.
        - Zoom.
        - X (Twitter).
        - LinkedIn.
        - Cisco Jabber.
        - Annual magazine reports for clients.
        - Client portal system.
- Hand over.
- Urgent internal communication occurs during WhatsApp - there is an expectation of being available at all times.
- Daily Meetings.
- Weekly Meetings.
- Bi-weekly meetings.
- Monthly meetings with management.
- Off hour communication about non-sensitive data on messaging platforms.
- Peer review/validation of found threats.
- Sharing information resources.
    - Internal web pages.
    - Images of drawn diagrams.

- Preparing presentations/reports.
  - PowerPoint.
  - Specifically for managers.
  - Start with non-technical summary and gradually become more technical.
  - Always end report with recommendations and desired outcomes.
  - Simple tables, pie charts, and bar charts used as visualizations.
  - Consult everyone involved in incident response when creating report.
  - Screenshots but not charts, maybe just a flow diagram.
- Agile/Scrum.
- Each hunt is kept as a case with one location for all information on the hunt.
- Simple clear communication that anyone with any level of technical knowledge will understand.
- Ad hoc.
- Depends on maturity of the organization.
- Follow playbook and communication plan.
- Beneficial to have an informal communication channel without formal management.
- Communicating how the threat hunter found the issue and how it can be fixed.
- During incident response, bring all relevant people from affected teams onto a single call.
- After incident response, ask collaborators what the next least secure thing could be.

What are the collaboration challenges threat hunters face?

- Client environment visibility.
- Different systems for different clients.
- Different learning styles between threat hunters on a team.
- Conflict between teams on resource allocation.
- Communication is limited in the remote / work from home environment.
- Levels of knowledge are different between collaborators so knowing how much or how little to explain is tricky.
- Geographically dispersed teams.
- Report generation is not automated.
- Teams that do not communicate their work with the rest of the company.
- Avoiding externally-accessible communication tools.
- Must document everything to allow other threat hunters to take over for a client.
- Pointing out flaws in applications developed by collaborators.
- Finding another threat hunter on the same schedule as you that you can reliably interact with.
- Communicating how a bias affected your handling of an event.
- Have to repeatedly ask questions to confirm you are receiving the correct information.

What do threat hunters recommend to improve collaboration?

- Better access / visibility into client systems.
- Centralized place for communication.
- Meetups/in-person gatherings of peers.
- Work in the same location/office.
- Standardized handoff protocol.
- Having resources available to answer frequently asked questions.
- Less meetings.
- Automate report generation.
- More collaboration.
- Maintaining good security hygiene to avoid scrambling when an incident is found in an unconsidered part of the environment.

Learning Aspects

What are the core skills that threat hunters should have?

- **Technical**.
  - Understanding operating systems.
  - Red teaming.
  - Blue teaming.
  - Networking.
  - Knowledge of Regex.
  - Knowing how an attacker thinks.
  - Experience doing hunts.
  - Knowing what is typical behavior for the systems you work with.
  - Have an area of expertise.
  - Certifications (SANS, OSCP, CISSP).
  - Scripting languages (Bash, Python, PowerShell).
  - Programming.
  - Knowledge of the command line.
  - Knowing the types of attacks/threats.
  - System administration knowledge.
  - Public versus private IP addresses.
  - Common ports.
  - Knowledge of event IDs that commonly appear in logs.
  - Security basics.
  - Computer forensics.
  - Malware analysis skills.
  - Knowledge of the threat landscape.
  - Background in development.
  - Technical support experience.
  - Pattern recognition.
  - SOC incident response experience.
  - Knowledge of AI and ML to develop detections.
- **Non-technical**.
  - Situational awareness.
  - Documenting steps.

- Good communication skills.
- Ability to convey concepts in simple terms.
- Ability to convert resource information into actions.
- Storytelling.
- Interpersonal skills.
- Critical thinking.
- Analytical skills.
- Knowing when to stop.
- Not being afraid to ask for help / find an expert who knows more.
- Public speaking.
- Writing skills.
- Organized.
- Problem solving.
- Flexibility.
- Ability to learn fast.
- Knowing the right information to gather.
- Creating a welcoming environment for the team.
- Research skills.
- Patience.
- Observant.
- Ability to reverse engineer.
- Troubleshooting.
- Tolerant of audits and compliance.
- Independent.

What are the practices/strategies threat hunters follow for learning?

- Being mentored - peers, senior threat hunters, managers, community.
- Mostly on the job training.
  - Capture the flag.
  - Hack the box.
- Staying up to date on latest cybersecurity news.
- Learning from teammates.
- Self-taught.
- Learn by doing (simulations, practice, trial and error).
- News.
- Listening to podcasts.
- Watching videos.
- Continued education (master's degree).
- Formal certifications (SANS, CASP+, OSCP).
- Note taking when being taught or mentored.
- Learn by visualizing things.
- ChatGPT.
- Following security people on social media.
- Webinar.
- Conferences.
- Googling new or unfamiliar topics.
- Reading.
  - X (Twitter).
  - Blogs.
  - Mastodon.
  - Medium.
  - DarkNet Diaries.
  - LinkedIn.
  - Newsletters (SANS, Dragon).
  - Blogs.
  - Reports.
  - Books.
  - Magazines.

How do threat hunters disseminate their knowledge/expertise?

- Through peers.
- Managers.
- Knowledge sharing presentations.
- Team meetings.
- OneNote for hand-off.
- Hand-off meetings.
- Reports for clients.
- Email.
- Resources are shared over messaging software.
- Internal documentation.
- Share information over Confluence.
- Whiteboard sessions.
- Blogs.
- Conferences.

What challenges do threat hunters face when disseminating knowledge/expertise?

- Differing learning approaches.
- Different levels of knowledge between collaborators.
- Lack of local community.
- Keeping up with new information - threat landscape and knowledge is changing very rapidly.
- Knowledge is spread between teammates and there is limited time to share knowledge.
- Need to synthesize findings into a simple and readable format.

Threat Hunting Environment (Situational Awareness)

How are threat hunters aware of what they need to know to grasp and incident?

- Incident escalation process.
- Personnel.
- Communication channels.
- Easy access to the data for analysis.
- Logs from the attack.
- Registries from the attacks.
- The affected assets.
- The timeline of the incident.
- The phase in which the threat is in.
- How the client wants the threat to be handled.
- The number of clients affected.
- The number of machines impacted.
- How the threat was discovered.
- Having really good knowledge of the tools and resources they use.

How do threat hunters understand the urgency of a security incident?

- Current attacks are given highest priority.
- All incidents are treated as high priority until proved otherwise.
- Classification of severity or urgency.
- The machine learning rating provides some context for the classification.

- If the attacker has already infiltrated the system, the attack is given the highest priority.
- Threat hunters find a potential high priority anomaly and seniors may reduce to lower priority.
- Timeline of the incident.
- Assets are in prioritized buckets.
- Gut feeling, that comes from experience, about how critical the threat is.
- The role of a threat hunter is to understand the urgency of threat activity.
- Type of user causing the threat.
- Type of incident.
- Type of data that has possibly been accessed by threat actors.
- Severity and impact.
- Tool provides classification.
- What entities/systems are compromised by the threat.
- Higher priority if client has already found the threat.
- Frameworks help decide priority.
- Thinking in terms of risk to crown jewels.
- Consider the incident response plan.
- UEBA and RedSeal help narrow events down to highest priority.
- What-if tool analysis indicates priorities.
- Imagine where you would attack if you were the attacker and how severe that could be.
- Urgency is determined by a separate SOC team.

How do threat hunters understand a security incident?

- Checking in with their peers and managers to validate their findings.
- Using tools to check details on anomalies.
- Using the data provided by the tools to build situational awareness.
- Machine learning tags as a first approximation of the severity of an incident.
- Try to determine who is accessing the resources (perhaps they are doing it correctly).
- Finding the origin of the vulnerability.
- Build a timeline of the attack from the anomaly data.
- Collect as much knowledge as possible.
- Vulnerability scan.
- What-if modeling tool.

How do threat hunters anticipate future threats and their implications?

- Sharing information about threats with peers.
- Staying up to date on current threats.
- Making connections between threat incidents.

- Monitored indicators of attack.
- Finding low severity “hygiene” issues and reporting in a weekly meeting.
- Knowing the environment that hunts are being done in. Being able to recognize when something is abnormal.
- Writing process of a hunt.
- Understanding the architecture of systems.
- Removing parts of a network that are not being used.
- Review historical threats to find patterns.
- Mapping out the attack chain in an environment.
- Looking ahead at the tech trends and business trends.
- Sometimes you can’t know what’s coming.
- Understanding the threat landscape for the industry and scale of a particular client.
- Attackers using AI to support malicious activity.
- The frequency and complexity of attacks is only going to increase.

Behavioural Aspects

What makes threat hunters feel confident about threat hunting?

- Experience.
- Finding a few threats that are actually threats (not a false positive) makes a threat hunter more confident.
- Hearing others’ experiences.
- Collaboration with and validation from people more experienced.
- Never being 100% confident.
- Forensic thinking skills.
- Positive feedback.
- Having a process/routine/protocol to follow for hunting.
- Doing research.
- Staying up to date on current knowledge.
- Having a good team.
- Being confident in yourself.
- Not being afraid to ask for help or to ask questions.
- Sharing your knowledge with others.
- Having asked a lot of questions in the past.
- People start recognizing your achievements.
- Some people are confident right away.
- Must fully understand the content and be able to communicate it clearly.

- Must know the correct person to talk to about something.
- Certifications.

What is the mindset of a threat hunter?

- Constantly learning.
- Wise.
- Adaptability.
- Resilient.
- Questioning.
- Skeptical.
- Paranoid.
- Proactive.
- Not task-oriented.
- Sense of responsibility.
- Curious.
- Inquisitive.
- Investigative.
- Forensic.
- Passionate.
- Creativity.
- Methodical.
- Scientific.
- Thorough.
- Competitive.
- Counterattack.
- Problem solver.
- Thinks for themselves.
- Open-minded.
- Doesn't rely solely on certifications, constant learning is just as important.
- Research oriented.
- Willing to do the nitty gritty.
- Not egotistical.
- Patient.
- Persistent / determined.
- Does their best / tries their best.
- Instinctive.
- Driven.
- Logical.
- Unemotional.
- Prepared for many possibilities.
- Rulebreaker inclination.
- Innate belief in themselves.
- Suspicious.
- Contrarian.

What are the motivations for being a threat hunter?

- Experience.
- Solving hard problems.
- Protecting assets or an organization.
- Helping the people/customer.
- Combination of passion and hobby.
- Being a part of a community.
- Collaboration / being a part of a team.
- Sharing knowledge.
- Responsibility.
- Money/salary.
- Self-improvement.
- Self-fulfillment, achieving personal goals.
- Good morale / professional relationship development.
- Being able to extract useful information from a large amount of data.
- Finding useful information for people.

- Fun.
- Being technical.
- Continuous learning.
- Finding a big threat.
- Enjoying what you do.
- Catch bad guys.
- Being one step ahead of the threat actors.
- Becoming an indispensable trouble shooter for the company.
- Having a singular, focussed mission to protect the company.

What are the rewards and incentives that positively influence threat hunters?

- Bonus / financial recognition.
- Recognition from internal organization.
- Recognition from outside of the internal organization.
- Metrics.
- Rewards program.
- Intrinsic recognition.

What are the cultural factors that might influence the work of threat hunters?

- Location.
- Diversity.
- Ethnicity and race.
- Gender.
- Recruiting diversity is difficult.
- Age.
- Language.
- The cyber security mindset of the country they're located in.
- Ethics are different in different places.
- The reputation of different locations can affect how a threat hunter perceives the suspicion of an event.
- Culture the threat hunter belongs to.

Manager's Perspective

What are the manager-specific workflows?

- Check the incident board and tackle the fires – if nothing is on fire, go into proactive mode.

What are the manager-specific tasks?

- Top-down security advising.
- Assigned to shadow an active incident and handle communication with the client and executives.
- Prioritizing creation of systematic processes based on organization maturity.
- Reducing toil for threat hunters through automation and creation of systematic processes.
- Reporting to executives.
- Hiring threat hunters with the right skills and mindset.

- Helping with incident responses in spare time.
- Supporting collaboration in the team.

Who are the collaborators that only the manager interacts with?

- Executives.

How do managers present information to stakeholders?

- Business dashboards.

Glossary

Table of terms used in this document; not intended to be a comprehensive reference for terms in cybersecurity.

Term	Definition
ADR	Advanced Detection and Response
CASP+	CompTIA Advanced Security Practitioner
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
EDR	Endpoint Detection and Response
IDS	Intrusion Detection System
IT	Information Technology
MISP	Malware Information Sharing Platform
OSCP	Offensive Security Certified Professional
OSINT	Open-Source Intelligence
OTX	Open Threat Exchange
OWASP	Open Worldwide Application Security Project
SANS	SysAdmin, Audit, Network, and Security Institute
SIRT	Security Incident Response Team
SOC	Security Operations Center
UEBA	User and Entity Behavior Analytics
WMI	Windows Management Instrumentation

Appendix

Full size versions of all the figures presented in the report can be found below. Grayscale versions are included in the text for simplicity; colour versions are available in the appendices. The appendices appear as follows:

- Persona: Olivia
- Persona: Jay
- Persona: Thomas
- Persona: Ren

Olivia (She/Her)

Threat Hunting | Cyber Security | Collaborative Solutions | Making Connections

Team Lead **External Consultant** **Hybrid**

Learns best through mentorship **Collaborative**

Olivia is a cyber security professional with over 7 years of experience. She earned her SANS certification during her training under her mentor. She has since become a senior member of a threat hunting team that provides valuable feedback and guidance to her peers. She recently earned a promotion to team lead.

She leads an awesome team of threat hunters through the complex and quickly changing hunts presented by her diverse portfolio of clients. Navigating the threat landscape using a small well crafted tool kit, Olivia's priority is ensuring the safety of customer assets. She frequently communicates with clients to ensure that her team is providing up-to-date information on current threats and how they can help their client stay secure.

Olivia is motivated by the feeling of helping others and by having a strong and connected team. She prides herself in the way that she can empathize with clients and teammates. In her spare time you can find Olivia captaining her local volleyball team and enjoying the theatre scene.

Quotes

"It always has to be peer reviewed. So I have to ask a colleague, hey, this is what I found, can you do a quick sanity check? Does this sound all right?"

" I just know what the tools can provide me. Sometimes weirdly enough, the tool also determines your workflow, right? So I know how to use the tool and then based on that, I create my workflow."

Hunting Style

Proactive	Reactive
Ad Hoc	Procedural
Intuitive - Creative	Analytical - Methodological
Peer - Peer Validation	Resource Validation
Individual	Team
Hands-on	Tool Led

Tooling

One Tool	10+ Tools
Commercial	Built In-House

Resources

Open Source	Private
Casual	Formal

Motivation

Intrinsic	Extrinsic

Skills

- Communication
- SANS Courses
- Storytelling
- Network Architecture
- Problem Solving
- Report Generation

Tools

- White Board
- IPAbuse
- SIEM Tool
- MS OneNote
- VirusTotal
- MS Teams

Pain Points

- Report Generation
- Customer Systems
- Organizational Support
- Context Switching
- Diverse Personalities

Jay (He/Him)

MSc | Threat Hunting | Cyber Security | Ethical Hacker | Machine Learning

Threat Hunter **External Consultant** **Remote**

Learns best by trial and error **Analytical**

Jay is a recent graduate from a master's in IT security and is currently a threat hunter for a cyber security solutions organization. Work terms and a post-grad position has earned Jay two years of experience in a threat hunting role.

He is a strong team member that hunts for a specialized section of the team's client portfolio. He prioritizes following and refining the team playbooks and is a proponent for the automation of simple tasks. Jay interacts with his team and client through a ticketing system that helps them to stay organized and clear on priorities. Jay uses a large toolkit and his home lab set up to hunt and test malware. Jay is hands-on with his hunts and learns the most from trying new techniques.

Jay is motivated by the recognition of his hard work by his peers and by the prospect of financial incentive. He loves to compete in local hacking events and can often be found networking with other cyber security professionals. Jay is a movie buff and likes to spend his weekends marathoning the latest movies with his dog Max.

Quotes

"When our tool, our main tool, or one of the tools that we depend on is down, or we want to be able to access the client environment and are limited by what they provide us. Oh, that's really frustrating!"

"It's kind of this, you're protecting people, this game of cat and mouse. So I mean, there is that frustration that, you know, the threat actors are typically a step ahead."

Hunting Style

Proactive	○ ○ ● ○	Reactive
Ad Hoc	○ ○ ○ ●	Procedural
Intuitive - Creative	○ ○ ● ○	Analytical - Methodological
Peer - Peer Validation	○ ○ ● ○	Resource Validation
Individual	○ ○ ● ○	Team
Hands-on	○ ● ○ ○	Tool Led

Tooling

One Tool	○ ○ ○ ●	10+ Tools
Commercial	○ ● ○ ○	Built In-House

Resources

Open Source	○ ● ○ ○	Private
Casual	● ○ ○ ○	Formal

Motivation

Intrinsic	○ ○ ○ ●	Extrinsic

Skills

- Red Teaming
- Network Architecture
- Automation Expert
- Scripting
- Critical Thinking
- Think Like A Hacker

Tools

- VM Sandbox
- Python
- Reddit
- JIRA
- Sentinel
- MS Teams

Pain Points

- Communication
- Low Tool Performance
- Customer Systems
- Distraction
- Information Overload

Thomas (He/Him)

Advanced Threat Hunting | Cyber Security | Cyberspace Cowboy

Senior Threat Hunter **External Consultant**

Self Taught **Creative** **Remote**

Thomas is a senior threat hunter for small organization. With over 25 years of experience, Thomas has worked as a security professional in many industries including finance, government, and now in e-commerce. His varied experience gives him the expertise to lead his small team.

Thomas hunts in a hands-on and ad hoc way, he likes to think of himself as a cyberspace cowboy. He follows the latest trends of threats that come out by scouring online communities like Twitter and even developing connections to gain access to dark web forums. Using his well crafted toolkit and intuition Thomas is able to be proactive in his hunts. He prides himself on trying to always be one step ahead of the attackers.

He is highly motivated by keeping organizations secure and with a strong security posture. He has developed campaigns for organizations to promote proper security hygiene and enjoys engaging with the public on his social media. Outside of work you can find Thomas always picking up a new hobby like his current favourite of building his own chicken coop.

Quotes

"So sometimes it feels like a lot is going on. So actually, setting aside a piece and saying, like, I'm only going to do this today, or this this block of hours is actually needed."

"Questioning. You got to question everything. Everything you see, you got to form a little question in your mind and use the scientific method to break it down and determine if it's malicious, non-malicious. Why am I seeing this in the environment? Who is coming into the environment? Just all of those questions that you have to answer in your mind."

Hunting Style

Proactive	Reactive
Ad Hoc	Procedural
Intuitive - Creative	Analytical - Methodological
Peer - Peer Validation	Resource Validation
Individual	Team
Hands-on	Tool Led

Tooling

One Tool	10+ Tools
Commercial	Built In-House

Resources

Open Source	Private
Casual	Formal

Motivation

Intrinsic	Extrinsic

Skills

Computer Forensics, Time Management, Public Speaking, Critical Thinking, Research

Tools

Twitter, Dark Web, VirusTotal, Slack, White Board, Scripts, Notepad++

Pain Points

Data Availability, Complex Tools, Customer Systems, Screen Fatigue, Paywalls

Ren

They/Them

Threat Hunting | Cyber Security | Engaged Management | Data Visualization

Manager **External Consultant** **Hybrid**

Collaborative **Solutions Oriented**

Ren is the manager of a security department on a large organization. They have 15 years of experience in cyber security and another 3 years of experience as a manager. They have worked mainly in security consulting and has worked with clients from a range of industries.

Ren is a hands-on manager who interacts closely with both their team and the client they work with. Ren's main responsibility is to ensure that customers are getting the information they need and are supported in their security posture. They run quarterly meetings with clients to present reports on critical findings. Ren prides themselves on their ability to condense large amounts of information and communicate it in a way that clients with all levels of technical knowledge can understand.

Building diverse and cohesive threat hunting teams is a core motivation for Ren. Ren knows first hand that diversity in cybersecurity teams is crucial to being successful. They create their teams based on a person's passion, drive, and commitment for the work they do, and has less focus on formal certification or specific previous experience. They look for driven individuals that have a team mindset and actively work to create a welcoming and inclusive team environment. Ren wants passionate employees that are good at thinking outside of the box.

Ren is motivated by meeting goals set out by their team, clients, and the organization. Ren doesn't believe in using metrics to measure performance but feels that conducting performance reviews one-on-one with their threat hunters is important for creating a collaborative and successful team. On the weekends you can find Ren in the climbing gym or at their local farmer's market.

Quotes

"I certainly think diversity is huge. You can call that cultural diversity, you can call that business diversity, you can call that degree diversity, but diversity really matters."

"Don't be shy to ask questions, right? That's how you're going to get confident eventually, and as you make mistakes, you're going to get better. And it's better to ask questions than just not ask questions."

Skills

Computer Forensics | Time Management | Public Speaking | Critical Thinking | Research

Tools

Twitter | Dark Web | VirusTotal | Slack | White Board | Scripts | Notepad++

Pain Points

Data Availability | Complex Tools | Customer Systems | Screen Fatigue | Paywalls