University of BRISTOL
Bristol Cyber Security Group

REPHRAIN
Protecting citizens online

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

Priyanka Badva

Kopo Marvin Ramokapane

Elenora Pantano

Awais Rashid

USENIX Security 2024

Introduction

- Threat Hunting is a process aimed at identifying potential cyber threats and malicious activities within an organization’s network or systems.

- Threat hunting can be broadly categorized into two main approaches:
  - Proactive hunting
  - Reactive hunting

Motivation

- There is growing need to understand security workers
  - Bug Bounty hunters (e.g., Akgul et al., 2023)
  - CISOs (e.g., Hielscher et al., 2023)
  - Security analysts (Alahmadi et al., 2022)
  - Pen testers (Votipka et al., 2018)

- Limited understanding of threat hunters, their practices and challenges
  - ***RQ1:*** *Who performs threat-hunting activities, and what methods and processes do they use?*
  - ***RQ2:*** *What challenges do threat hunters face, and what strategies do they employ as best practices to overcome them?*

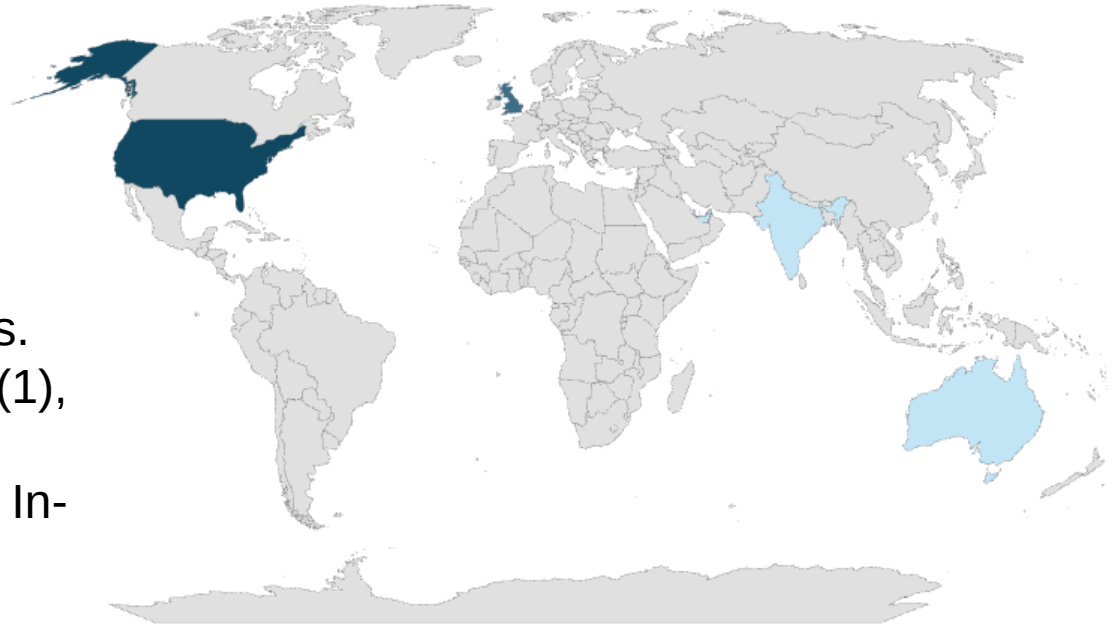
Methodology

Participants Recruitment

- To identify and recruit professionals whose daily work was to hunt for threats
- Minimum of 2.5 years of experience in the field.
- Snowball
- Recruitment channels - personal and professional connections, social media, slack channels

Sample

- Twenty-two (22) participants from various countries.
- US (9), UK (7), Qatar (1), Australia (1), Singapore (1), Germany (1), India (1) and UAE (1)
- Managed Security Service Providers (MSSP) (11), In-house + MSSP (6), In-house (5)



Findings

Who performs threat hunting ?

- Analysts with diverse qualifications
- Dedicated threat hunting teams or have other organizational responsibilities.
- Teams are formed randomly

*"I have a team of 8 people, most of them actually **started on our forensic team**, and I've kind of poached people from the forensic team ... **Pentest team to form the threat hunt team**. I had to cross-train the forensics guys and the pen-testers."*

*"Our company had **one dedicated threat hunter**, [name]. **He's also a science instructor**. He kind of worked on threat hunting but he didn't work in the SOC doing the day-to-day job, [he did] informal type of threat hunting stuff. Me and a few others started doing threat hunting on our own and we proposed a threat hunting program."*

Takeaway

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

Findings

How do they perform threat hunting?

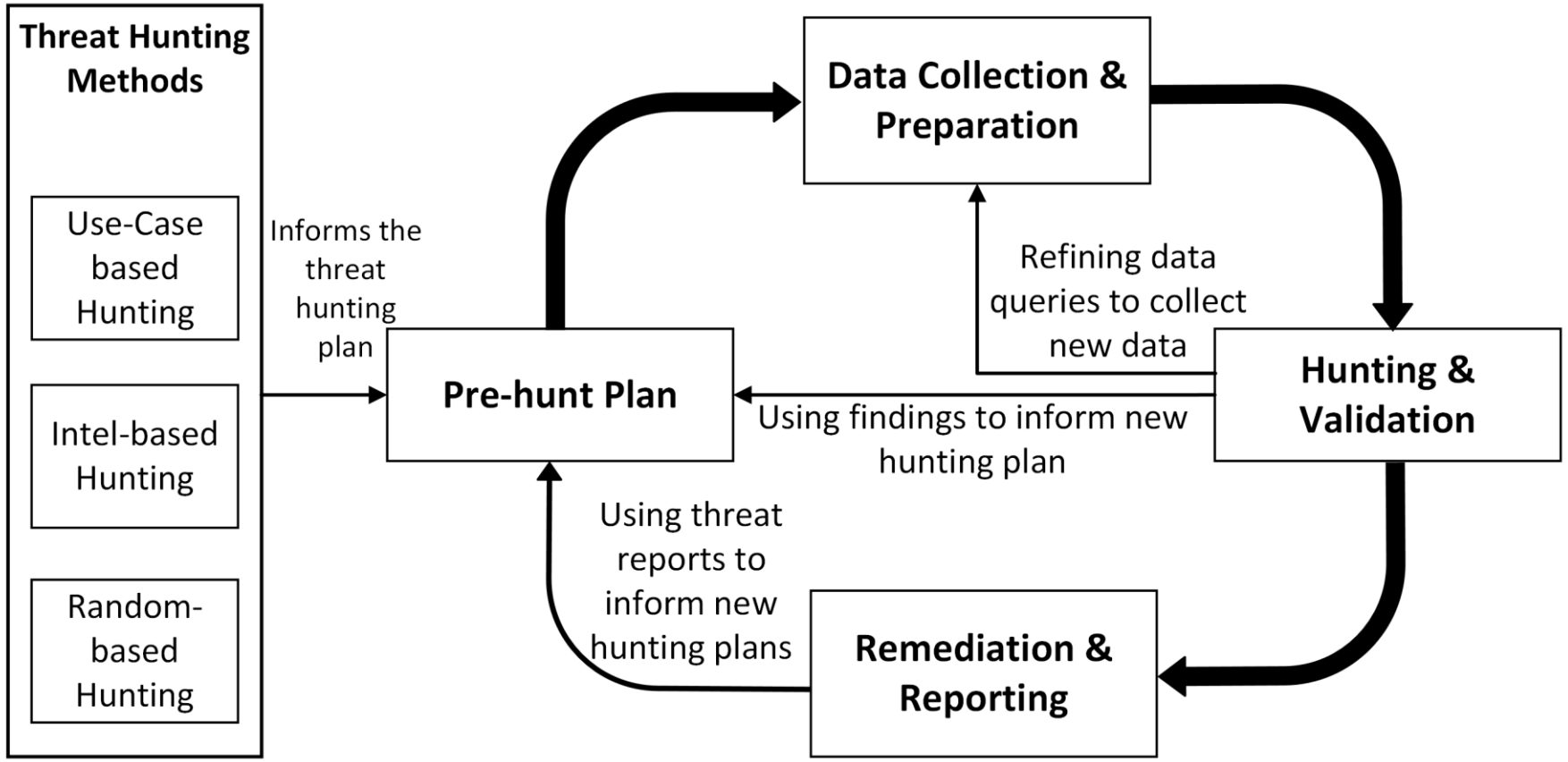
- **Use-case hunting -** using predefined scenarios or patterns of suspicious activities to identify and investigate known threats and attack patterns. These use cases are based on the threat hunters' knowledge of threat actors, the systems they own, and the typical attack patterns.

- **Intel-based hunting** - leveraging technical threat intelligence, such as known indicators of compromise/attacks (IoC/IoA), to guide the hunting process. This method relies on up-to date threat intelligence to proactively detect potential threats.

- **Random hunting -** conducting hunts without prior knowledge of specific indicators of compromise or a predefined plan. This approach involves being alert to potential threats during regular responsibilities or while conducting other specific hunts.

Findings

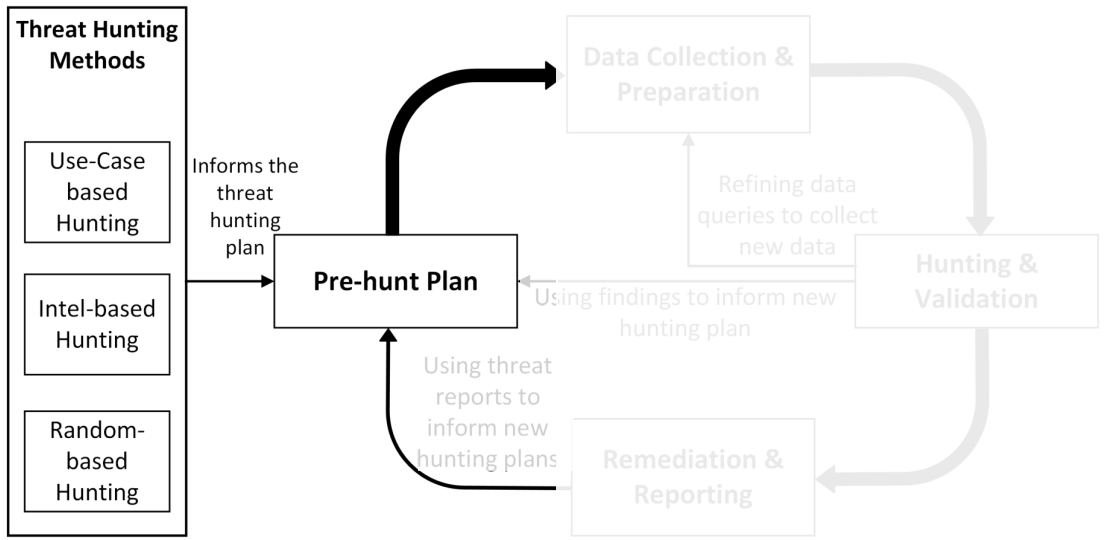
How do they perform threat hunting?



Findings

How do they perform threat hunting?

Pre-planning



- Dedicated planning phase. Threat hunters gather to formulate a plan that outlines the specific areas they intend to investigate.

"We try to plan all that stuff out at the beginning. It's planning, getting together in the beginning with everyone involved. And, then just let the system run, and then if something comes up later, you deal with it as a team."

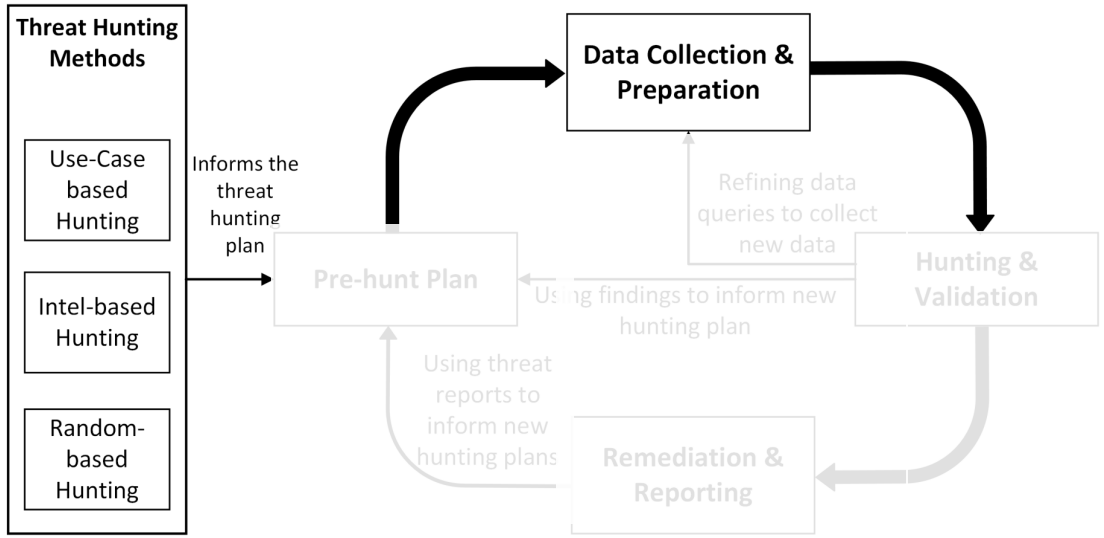
Takeaway

Most threat hunting activities start with a **dedicated plan**, where hunters **define the scope of the investigation, assess threat intelligence, generate hypotheses or use cases, identify relevant data sources**, and allocate resources based on their chosen approach.

Findings

How do they perform threat hunting?

Data Collection and Preparations



- Data collection from various sources: firewalls, antivirus, Endpoint Detection and Response tools (EDR).
- Hunting approach determines what data is collected

"Before you even get to data collection, you talk about the frame of where they are approaching it from. [...] People will see something on Twitter and say, 'That's a great idea; let me go and hunt for it,' but they don't really bring a rigorous approach to it."

- Enough data improves the quality of the hunt.

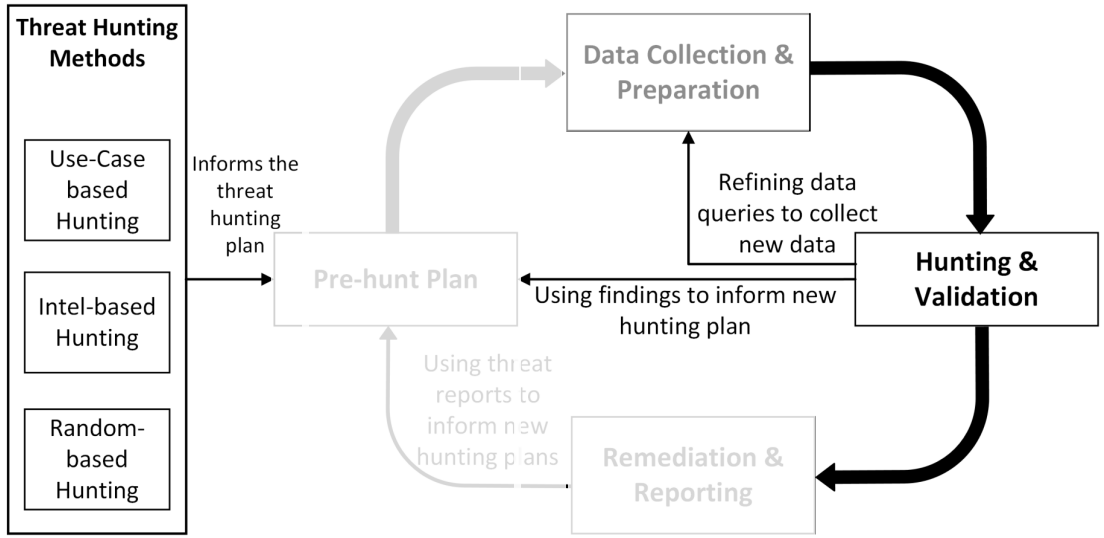
Takeaway

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

Findings

How do they perform threat hunting?

Hunting and Validating



- Hunting and validating threats is completed through an interactive and connected process.

- Example: **Random hunts** tend to occur unplanned and are often initiated by hunches or when the hunter observes something that looks malicious.

"I could be looking at something and think that looks weird. To me, that is an identification. An analyst looking at data and saying, 'That does not quite look right' is absolutely identification."

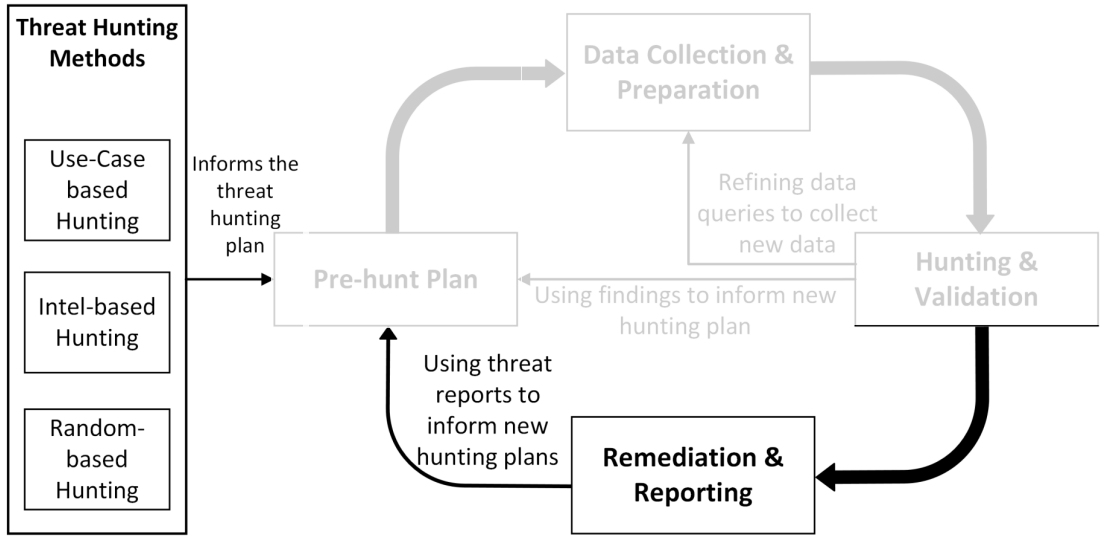
Takeaway

Threat identification and validation **are interconnected processes**. Threat hunters employ various tools and manually search and validate indicators of compromise. Validation is a team process.

Findings

How do they perform threat hunting?

Remediation and Reporting



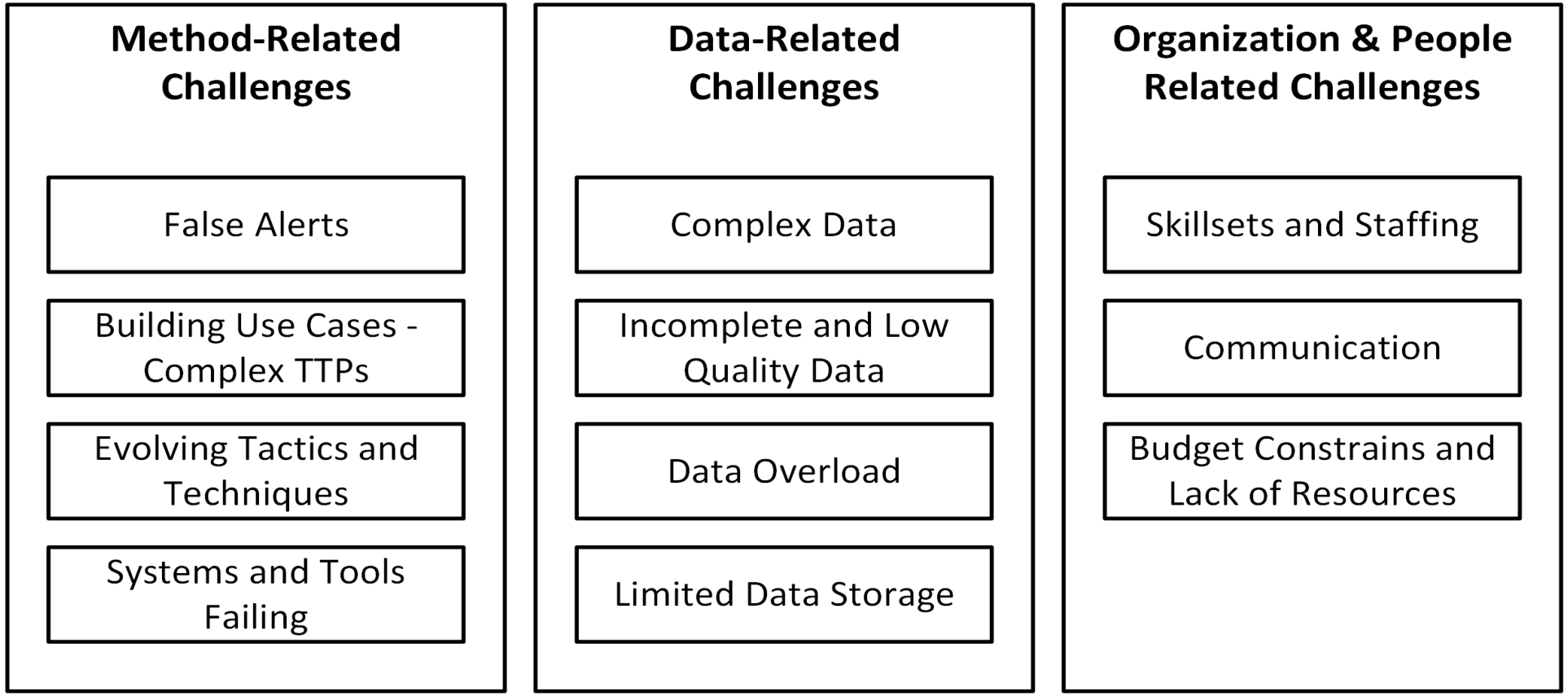
- Interconnected and often addressed together.
- Severity of the threats and time is critical in remediation and reporting. For severe issues, immediate action is taken
- Lessons are critical part of reporting.

"As I said, in the lessons learned part, we will be giving them more detailed information about how to enhance their detection analytics to fix where they failed to alert."

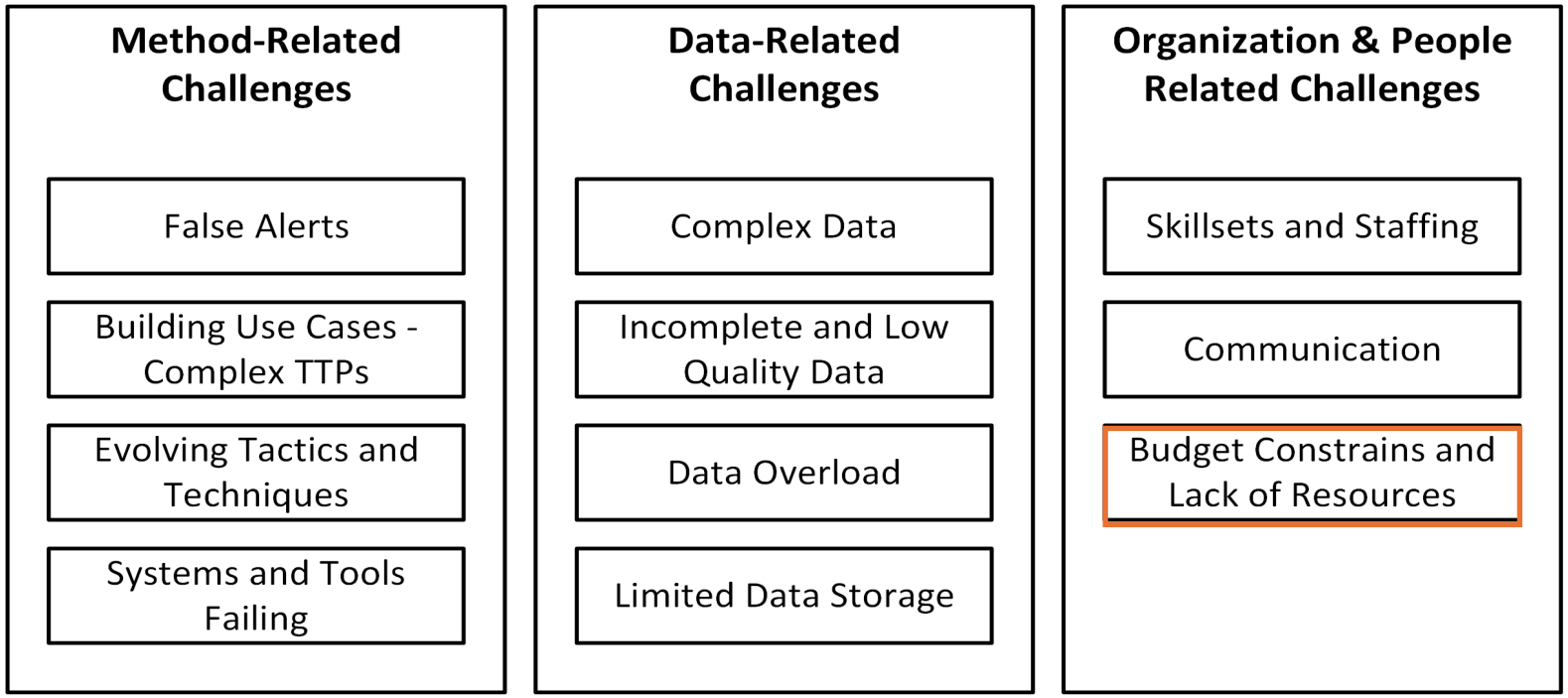
Takeaway

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

Threat hunting Challenges



Threat hunting Challenges



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

Strategies for effective hunting

Strategy 1: Re-analysing, Re-tuning, and Collaborating

Strategy 2: Automating Repetitive Tasks

Strategy 3: Refining data collection strategies

Strategy 4: Being flexible and Open minded

Strategy 5: Keeping up with current threats

Strategy 6: Asking for better budget allocation

Strategies for effective hunting

Strategy 1: Re-analysing, Re-tuning, and Collaborating

Strategy 2: Automating Repetitive Tasks

Strategy 3: Refining data collection strategies

Strategy 4: Being flexible and Open minded

Strategy 5: Keeping up with current threats

Strategy 6: Asking for better budget allocation

"One way of making threat hunting easier is **not following a rigid and repetitive process as threats constantly evolve**, one needs to be creative and find new ways of hunting for threats. **Being strict in approach or not adapting the process could lead to missing new or emerging threats**"

University of BRISTOL

Bristol Cyber Security Group

REPHRAIN
Protecting citizens online

Thank You

Threat Modelling, Threat Hunting, SOC related job

priyanka.badva@bristol.ac.uk
https://x.com/PriyankaBadva
https://www.linkedin.com/in/priyanka-badva/