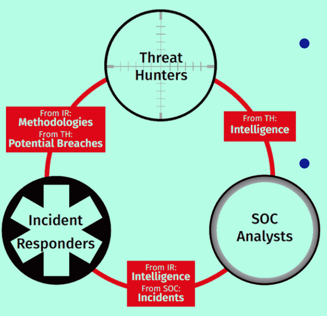
THREAT HUNTING & INTRUSION EXPLANATION

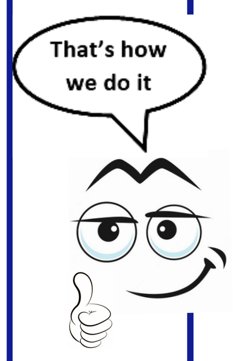
Motivation

Large event logs, false positives/negative alerts, no threat explanation... Threat hunting can be painful. However, existing research around threat hunting is limited. Challenges around threat hunting are not well documented. Consequently, frameworks that organisations can deploy and consider to mitigate and make threat hunting efficient are lacking.

Introduction



- Threat hunting puts one layer of security
- However, advanced attacks have become complex that requires more technical expertise to detect and analyse.
- The intrusion ranges over days and months, the log size becomes huge and hence becomes complicated to indicate threats.
- Therefore it is essential to address the latest challenges and lessons learned about threat hunting to solve at least some of them.



Proposed Solution

- To find the solutions, first we need to understand the challenges. We aim perform a user study to find the threat hunting challenges
- Designing a method/framework that organisations deploy and consider where the issue might lie.
- Sense making of anomalies from open source knowledge framework
- Evaluation of it will again take back to the users.

User Study

A qualitative study with SOC analysts to understand

- Threat hunting challenges that analysts faces in day-to-day jobs.
- We want to understand the challenges in terms of People, Process and Technology

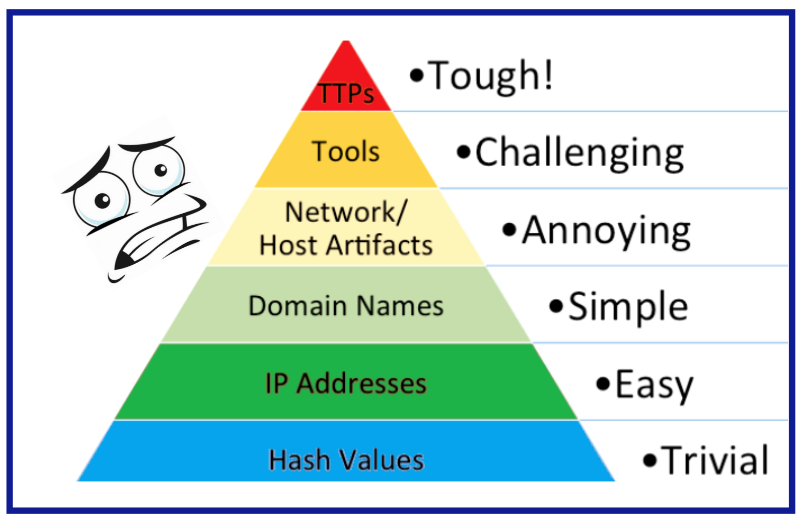
The Problem

Finding threats from large event logs

Threats/ IoCs explanation

Pain of false positives alerts

The Pyramid of pain



TTPs •Tough!

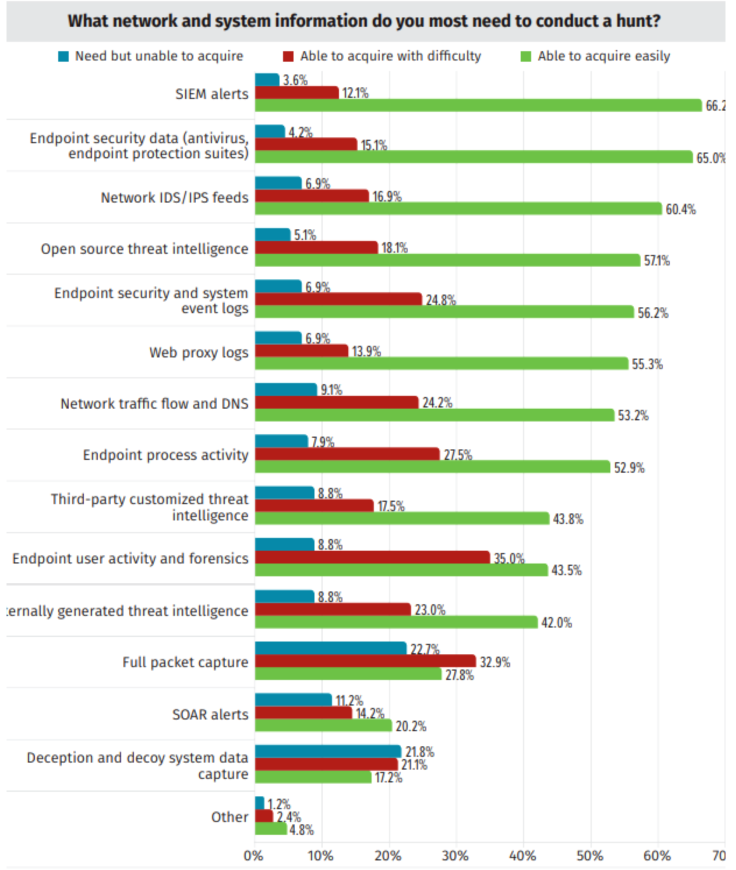
Tools •Challenging

Network/ Host Artifacts •Annoying

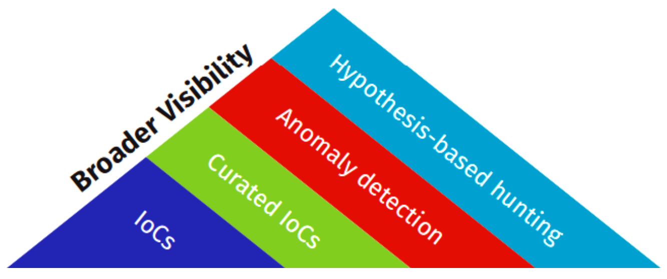
Domain Names •Simple

IP Addresses •Easy

Hash Values •Trivial



Some of the Statistics from SANS on threat hunting requirements and limitations shows, this user study will be great research contribution in the domain



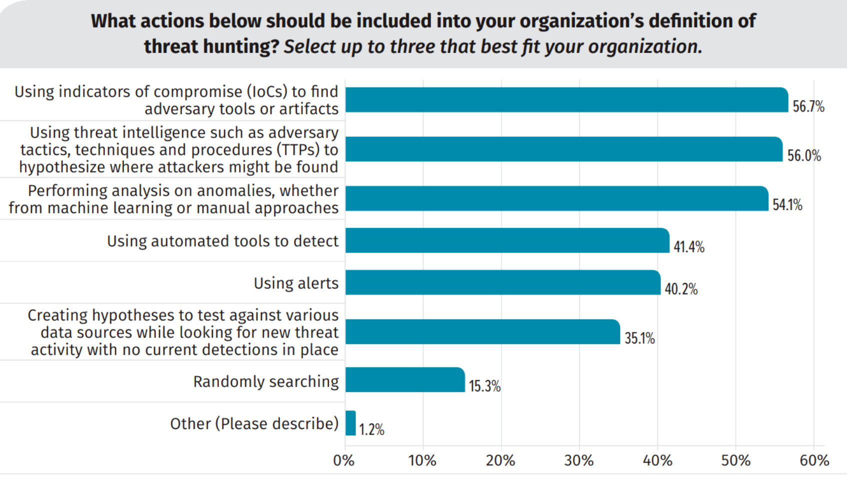
Broader Visibility

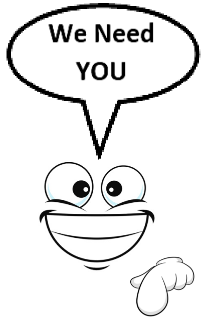
IoCs

Curated IoCs

Anomaly detection

Hypothesis-based hunting





Participants Recruitment

- We aim to recruit the SOC users to take part in this user study
- The SOC users have experience and and knowledge on handling day-to-day cyber incidents and threat hunting.
- If you are working in SOC, we invite you to take part in the user study.

Expected Outcome

- Provide an understanding of threat hunting challenges and mitigation strategies
- Provide a sense making of IOCS/threats from ATT&CK and hunting for the anomalies based on tactics, techniques, and procedures (TTPs). MITRE TTPs

IOCs + MITRE ATT&CK.

All images are acquired from: SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters
https://www.sans.org/media/analyst-program/2019-threat-hunting-survey-differing-experienced-hunters-39220.pdf

Priyanka Badva
priyanka.badva@bristol.ac.uk

University of BRISTOL