Threat Hunting

Services to enhance Proactive threat detection

In the ever evolving landscape of Cyber security, understanding the distinct roles of **Threat Intelligence and Threat Hunting** is crucial for enhancing an organization's security posture. While these terms are often used together, they serve unique purposes and complement each other.

I am diving into **Threat Hunting concepts in this Post**

	Threat Intel	Threat Hunting
What	**Actionable insights/contextual data** containing IOCs, TTPs etc providing guidance to proactively identify and respond to known, emerging threats	Proactive manual approach **assuming breach in the Network** (Threats evaded existing security controls) involves exploring IOCs, IOA's and TTPs to uncover hidden threats and looking for unknown threats within an environment
How	**Collection, Analysis and dissemination** of current/emerging threats from various intelligence sources to other security devices such as SIEM, SOAR, EDR etc to take necessary actions	Uses **combination of Tool, Behavioral analysis, hypothesis** driven approach
Why	**Prioritize alerts, improve Defence mechanisms** and respond to effectively	**Uncover inactive or long dwelling threats** and strengthen/fine tune security controls
Sources/Tools/Models utilized	**OSINT, Paid Services from vendors, Dark Web, In House** and Data shared within industry specific groups	**SIEM, EDR, NTA, UEBA, Threat Intel** etc
Types	Strategic, Tactical, Technical and Operational	IOC based, TTP based, Event based and Entity based

Note- For Threat Intel, Please refer my last week post **(10-N0V-2024)**

Threat Hunting flow

Threat Hunting plays a critical role, focused on **identifying and mitigating threats that may evaded traditional security defenses.**

Hypothesis Generation

- **Creation of educated assumption based on specific Indicators/threats** for testing.
- Assumption can be based on Threat Intelligence/TTPs/Log events/Entity as explained in next slide.

Data Collection & Preparation

- **Gathering of logs/data sources** from sources (Network/Endpoint/Threat Intel), relevant to hypothesis.
- Normalizing and Enrichment of data, making it high quality for analysis.

Data Analysis

- **Leveraging right set of tools** to query and analyze patterns based upon hypothesis and available data sources
  - SIEM- Aggregate and analyze logs
  - UEBA- Detects user behavior deviations
  - EDR & NTA- Insights on endpoint activities and network traffic

Hunt Execution & Investigation

- **Search for IoC's, Tactics, Signs** of malicious activity based on hypothesis to identify threats that crossed undetected
- Perform validation and investigation on the potential threats identified

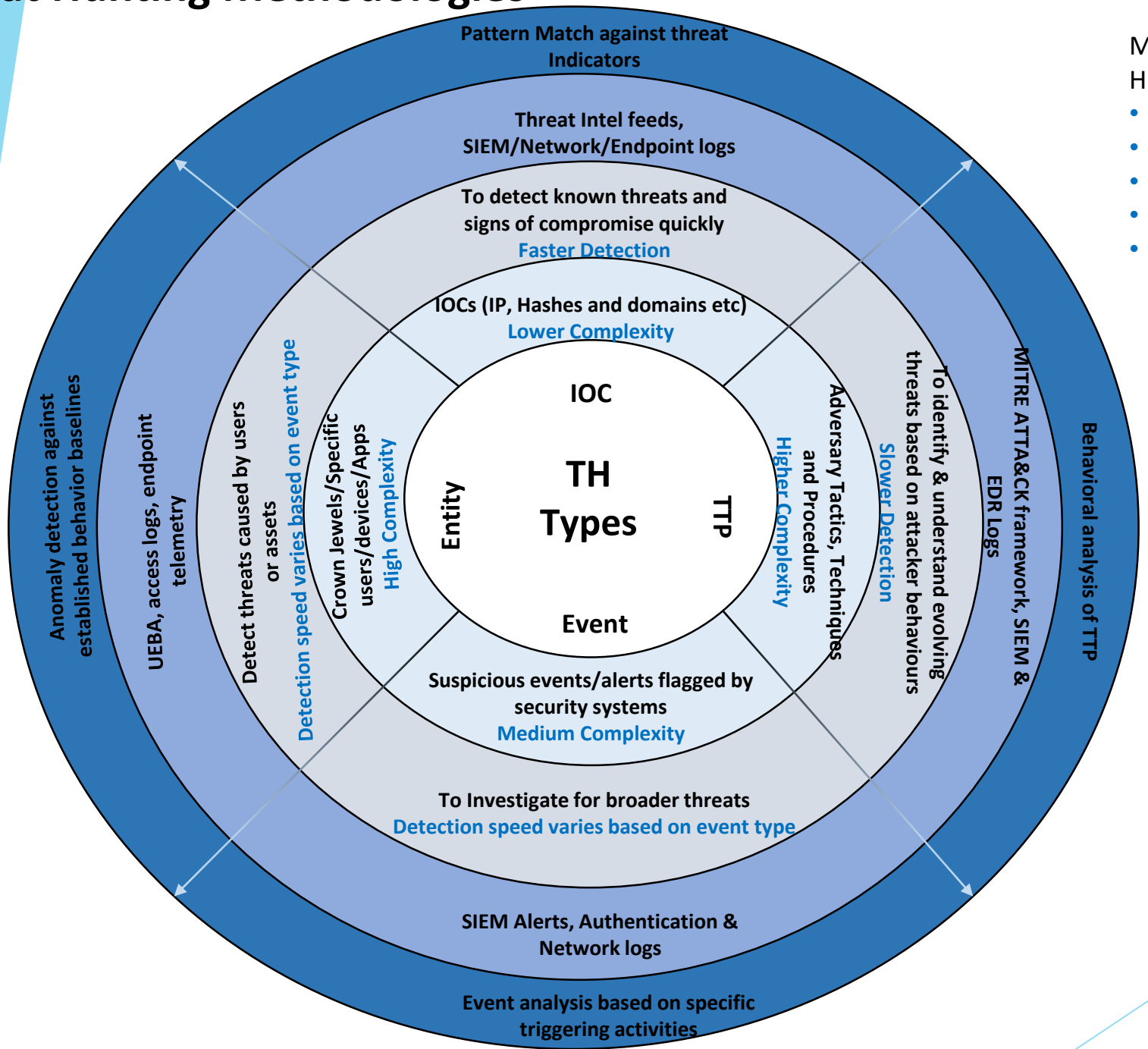
Finding & Reporting

- **Document indicators/threats/assets impacted**, evidence collected and detailed analysis performed with mitigation

Response and Improvement

- If a true positive threat is found, response is triggered making threat hunters work with IR team and device owners
- **Evaluate the effectiveness** of hunt and update threat hunting playbooks and procedures

Threat Hunting Methodologies



Methodologies play a important role in Hunting and several factors like

- **Maturity of SOC**
- **Industry**
- **Threat landscape**
- **Organizational objective**
- **Available tooling and skill** level helps to decide the suitable threat hunting methodology for organization