The role of Detection Engineering and Threat Hunting in modern SOC

Lech Lachowicz
ISSA Polska

whoami

Professional

- Currently Global Threat Defense Engineering Director in Pepsico
- Active member of ISSA International
- Ex Symantec
- Ex ISSA Polska Board Member
- CISSP since 2010

Hobby

- A coffee lover – I probably know more ways to craft a good coffee than there are T1059 subtechniques and variants.
- Homegrown researcher and builder – I make home appliances and love to use them.
- Snowboarder in winter and biker whole year

The Cyber Fusion Center concept

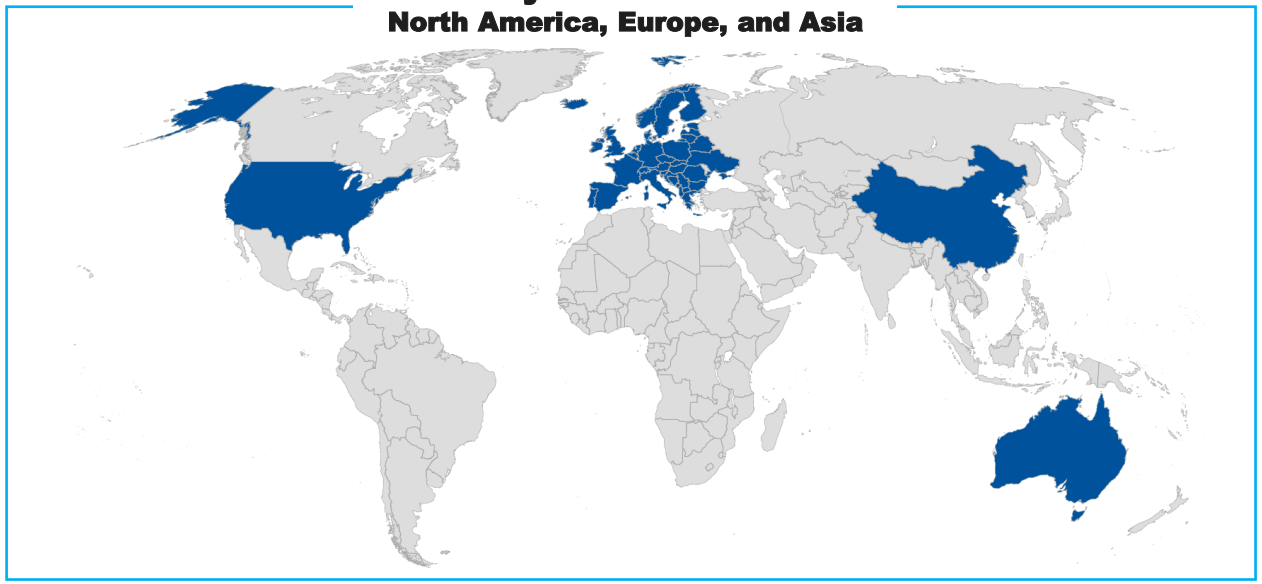
Fusion concept

Unlocking Cybersecurity Capabilities

Cyber Fusion Center (CFC)

is a comprehensive approach to security, consolidating security functions into a single, integrated entity with new capabilities through embedded teams in a collaborative workspace

Global Cyber Fusion Centers
North America, Europe, and Asia



CFC functions

Infrastructure Security

Application Security

Adversary Emulation

Enterprise Incident Mgmt

Cyber Resilience

Cyber Threat Intelligence

Detection Assurance

Threat Defense

Incident Response

Malware Analysis

How does it fit into Threat Informed Lifecycle

Threat Intelligence tracks relevant threats via *threat modeling*

Threat Defense uses this information to *fuel hunts*

Threat Defense hunts discover evil and lead to *automated detections which are* validated by **Adversary Emulation**

Detection Assurance measures & reports on *detection efficacy*

Detections lead to *playbooks* created by **Incident Response**

The detections create *incidents*, which **Incident Response** resolves and is used to inform the threat model

The WHY - Detection can’t be OutSOARced

More Visibility → More Alerts → Alerts Fatigue → SOAR

Historically SOAR platform was brought in to reduce the alert fatigue but there are challenges:

1. Complexity and Maintenance
2. Limited Scalability
3. Over-reliance on Automation
4. Lack of Contextual Understanding
5. False Positives and Negatives

“The main challenge is not about lowering the security alerts volume but crafting good, solid detection.”

What's a good detection?

High fidelity

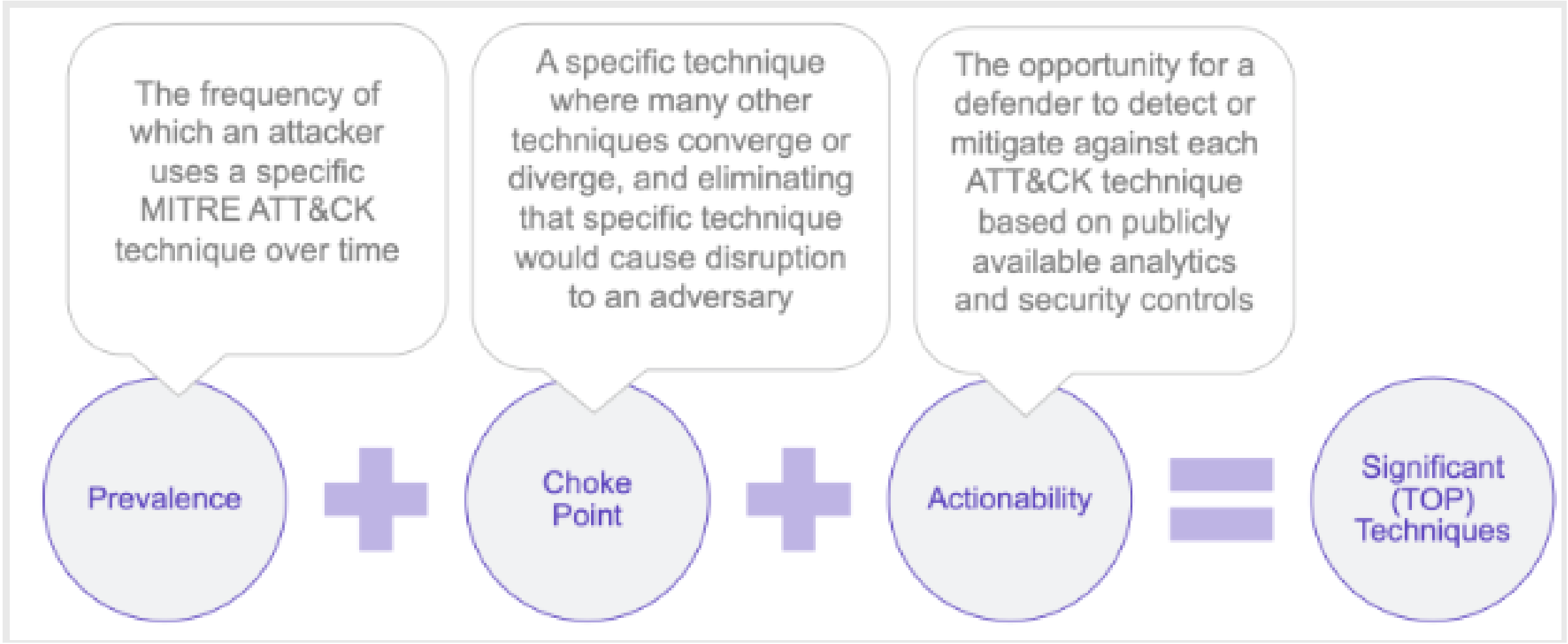
Low False Positive

High relevancy to Org

Reviewed

Measurable

Prioritization methodology

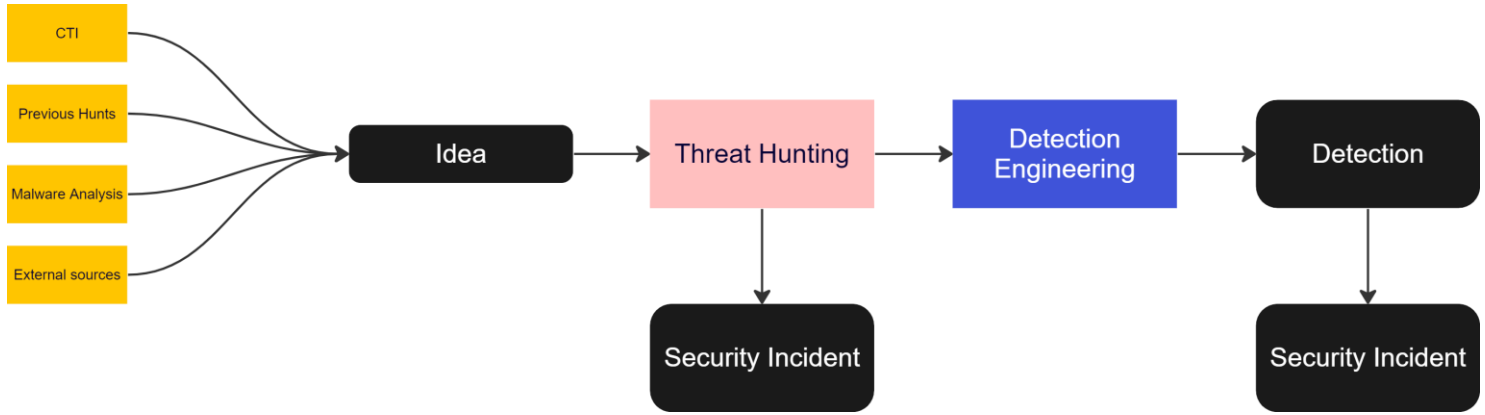


https://top-attack-techniques.mitre-engenuity.org/methodology

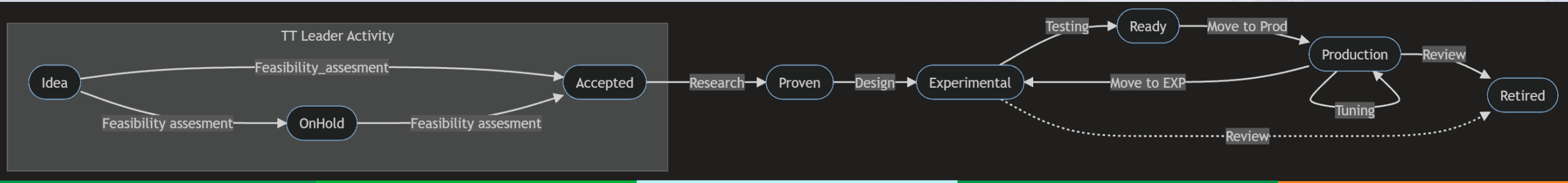
Detection Engineering vs Threat Hunting

Old School vs. New School vs. Your School

https://twitter.com/ateixei/status/1488280157098061829



Detection Engineering



Idea

Detection idea as provided by Threat Defense or any external team, can be an effect of ThreatHunt or can be automatically sourced from external repositories like Sigma and other

Accepted

A raw idea that we want to start working on through hunting and design/research.

Experimental

A detection deployed to detection platforms. All related data exists in NGDC. Further testing is required to move the detection to next stage.

Retired

A detection that's no longer required.

Production

A production detection.
Each event/alert will be signaled to IR.
At this stage a detection should have well defined FP rates and high fidelity.
IR teams should have corresponding triage and remediation playbooks.

OnHold

A detection or just an idea that didn't pass the feasibility assessment because of lack of visibility/coverage, being duplicated, low fidelity or simply high FPs.

Proven

An idea that has completed research and is ready for design.

Ready

Testing is completed and detection is ready for production.

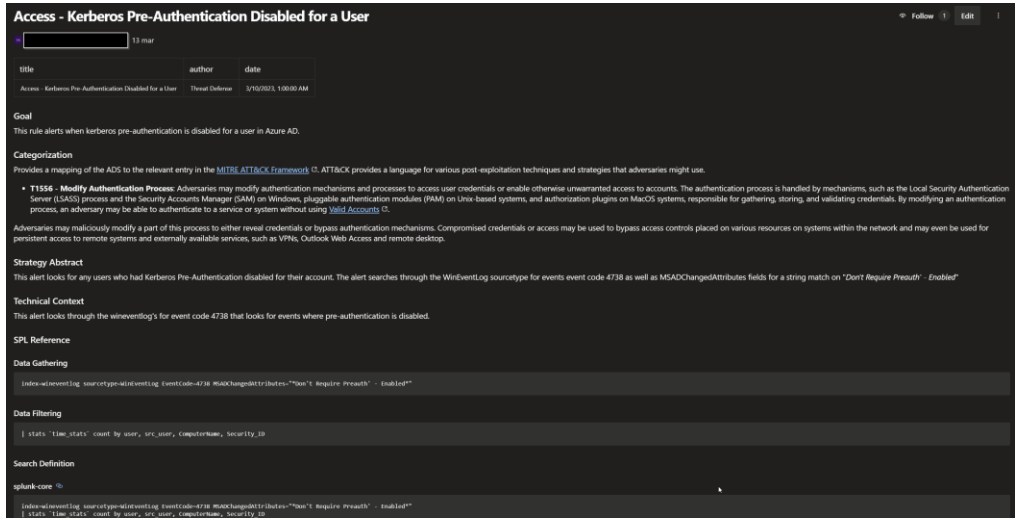
Rejected

A detection will not be worked on.

Documentation – it's not about where, but about how

- Jira
- Azure DevOps
- ServiceNow
- Open source tools
- Excel(SIC!!)

Human readable



Consumable by machine:

Summary and questions

TLP:Yellow

Thank you!

Lech Lachowicz
ISSA Polska