



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



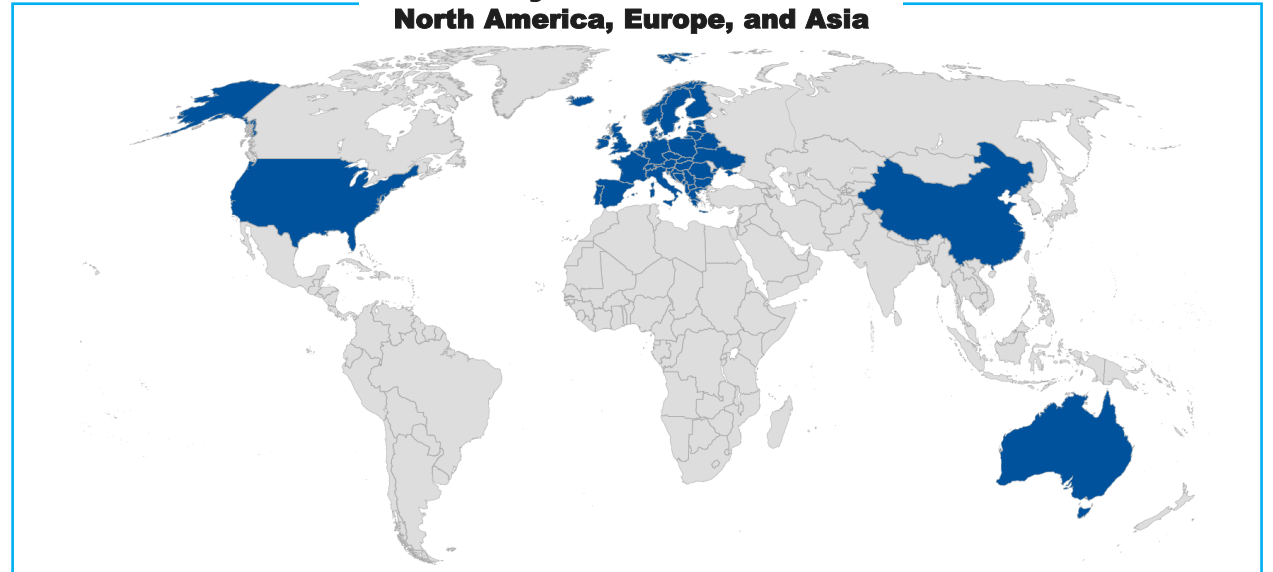
Fusion concept

**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



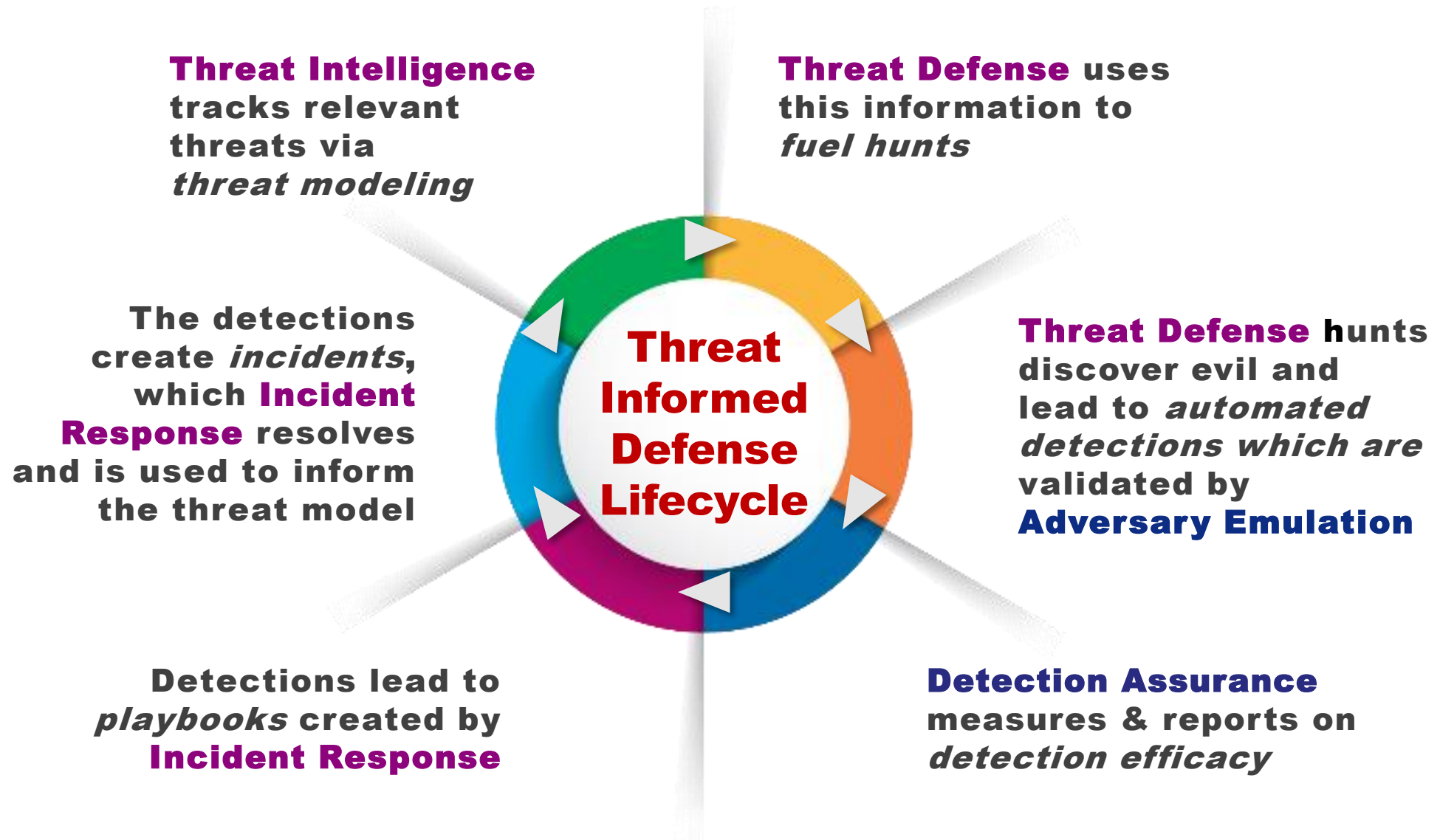
Incident Response



Malware Analysis



How does it fit into Threat Informed Lifecycle



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

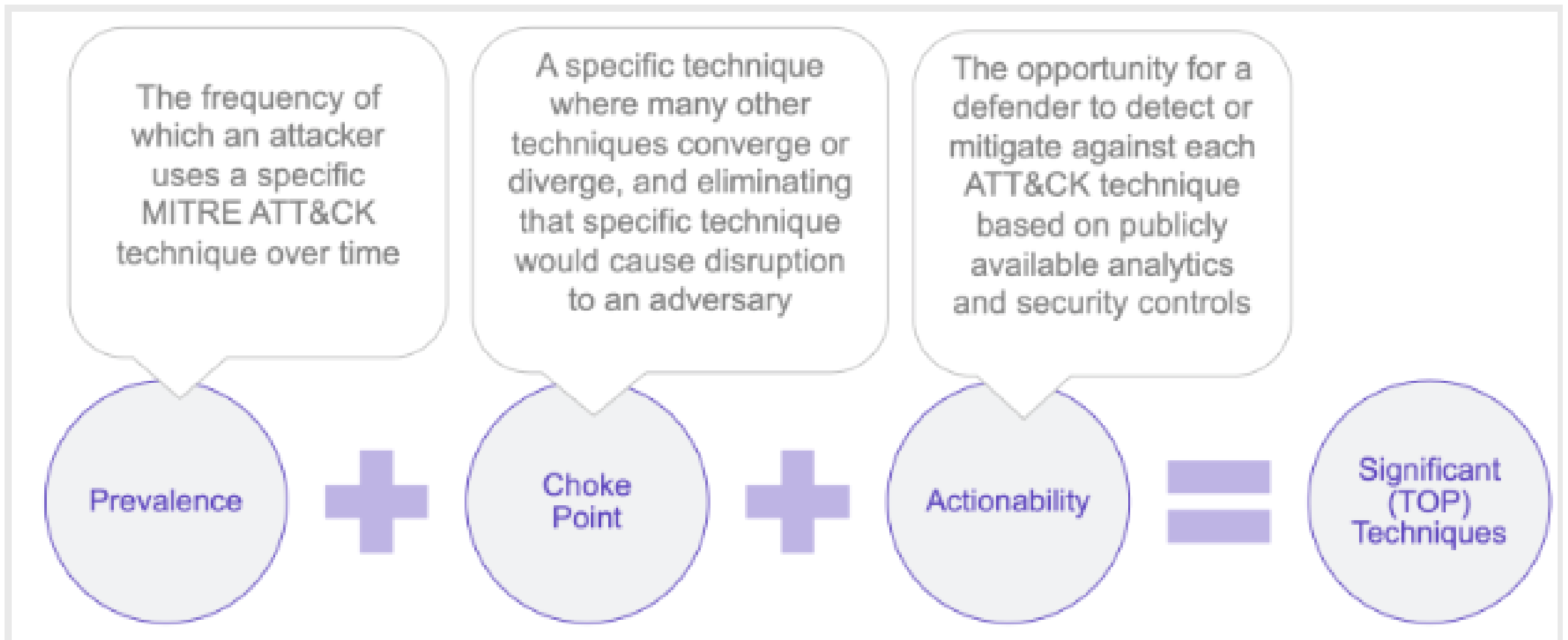
Low False
Positive

High relevancy
to Org

Reviewed

Measurable

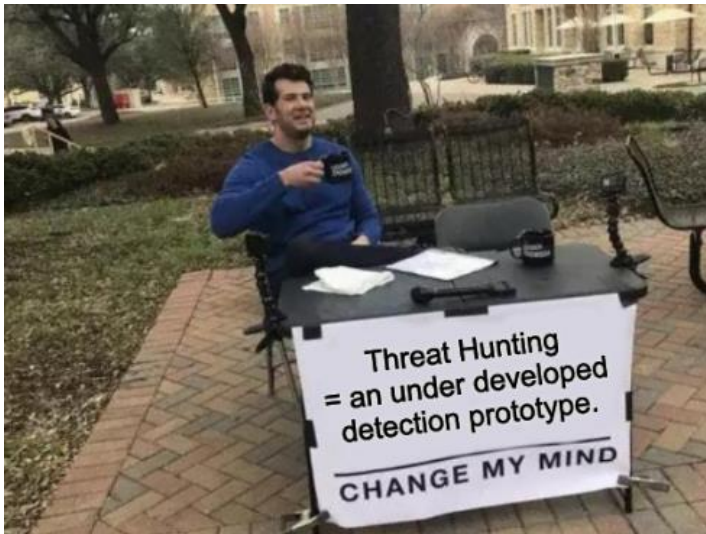
Prioritization methodology



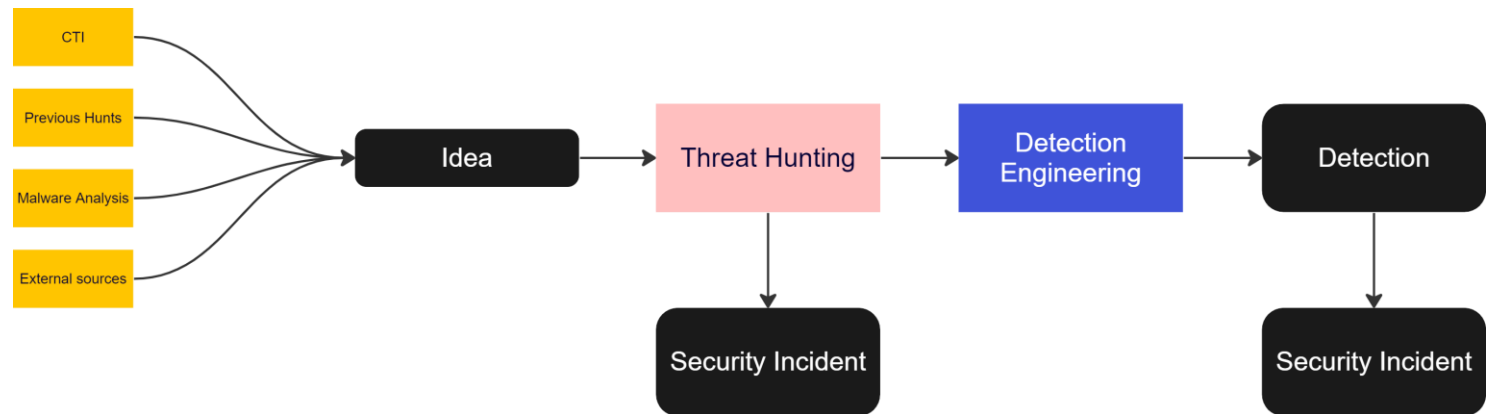
<https://top-attack-techniques.mitre-engenuity.org/methodology>

Detection Engineering vs Threat Hunting

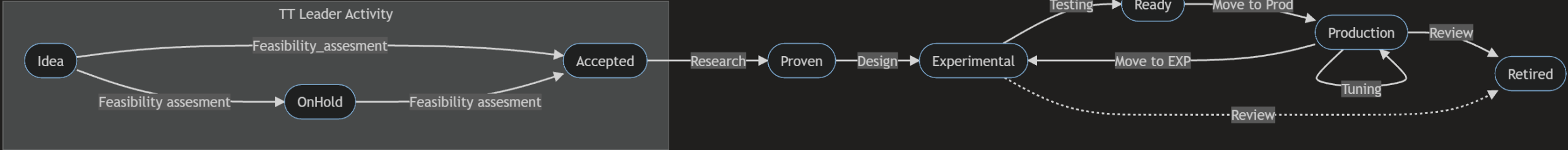
Old School vs. New School vs. Your School



<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

The screenshot shows a Jira ticket interface. At the top, the title is "Access - Kerberos Pre-Authentication Disabled for a User". Below the title, there's a table with columns "title", "author", and "date". The "title" column contains "Access - Kerberos Pre-Authentication Disabled for a User", the "author" column contains "Threat Defense", and the "date" column contains "3/10/2023, 1:00:00 AM". Below the table, there's a "Goal" section with the text "This rule alerts when kerberos pre-authentication is disabled for a user in Azure AD." followed by a "Categorization" section. The "Categorization" section contains a paragraph about the rule's purpose and a "Strategy Abstract" section. The "Strategy Abstract" section contains a paragraph about the rule's purpose. Below the "Strategy Abstract" section, there's a "Technical Context" section. The "Technical Context" section contains a paragraph about the rule's purpose. Below the "Technical Context" section, there's a "SPL Reference" section. The "SPL Reference" section contains a paragraph about the rule's purpose. Below the "SPL Reference" section, there's a "Data Gathering" section. The "Data Gathering" section contains a paragraph about the rule's purpose. Below the "Data Gathering" section, there's a "Data Filtering" section. The "Data Filtering" section contains a paragraph about the rule's purpose. Below the "Data Filtering" section, there's a "Search Definition" section. The "Search Definition" section contains a paragraph about the rule's purpose.

Consumable by machine:

```
Code Blame 110 lines (97 loc) · 5.44 KB
1 name: Kerberos Pre-Authentication Disabled for a User
2 workflow: 0
3 uid: 755916eb-895f-45d4-8057-200a6f07f1b3
4 date: 2023-01-17T22:39:42.402219
5 updated: 2023-01-18T18:55:02.627748
6 see the following fields will be automatically updated by Github's workflow app
7 schema version: 0.2
8 alert_source: [redacted]
9 template: /templates/splunk-generic-template.yml & import default value of 'detection_name' key
10 detection_type: Suspicious Account Activity & see need it, but the structure will not be validated
11 description: |
12   Kerberos is an authentication protocol used to verify the identity of a user or host. Kerberos pre-authentication is a security feature meant to protect against password guessing attacks. An attacker may attempt to disable kerberos pre-authentication in order to later escalate privileges or move laterally.
13
14 security_domain: access & choose one of: access, audit, cloud, email, endpoint, host, hybrid, identity, network, threat, undefined
15 category: Unauthorized access & choose one of: web, external, media, email, infrastructure, cloud, unauthorized access, other
16 subcategory: Abuse of access & available options depend on 'category', see https://[redacted] detectionfieldsReferenceGuide for details
17 platform: windows & choose one of: windows, linux, macos, ios, android, azure, azure ad, office 365, undefined
18 urgency: 3 & [0..4] calculated see: https://[redacted] definitions-<scope>-priority
19 impact: 3 & [0..4] calculated see: https://[redacted] definitions-<scope>-priority
20
21 mitre_attack:
22   technique:
23     - MIT-1536 & technique ID formatted: Txxx.yyy (where 'x' is a digit 0-9)
24     name: Modify Authentication Process & human readable name of the technique
25
26 ## following keys are mandatory (excluding 'response' and 'additional_resources'), and used for documentation purposes.
27 ## all can use multi-line Markdown formatting like the description above
28 goal: This rule alerts when kerberos pre-authentication is disabled for a user in Azure AD.
29 strategy_abstract: |
30   This alert looks for any users who had Kerberos Pre-Authentication disabled for their account. The alert searches through the wineventlog sourcetype for events event code 4738 as well as MSADChangAttributes fields for a string match on "Don't Require Preauth" - enabled"
31
32 technical_context: |
33   This alert looks through the wineventlog's for event code 4738 that looks for events where pre-authentication is disabled.
34
35 ## SPL Reference
36 ## Data Gathering
37 ---
38 Index-wineventlog sourcetype-wineventlog eventcode=4738 MSADChangAttributes="Don't Require Preauth" - enabled"
```

Summary and questions

A stylized globe is positioned on the right side of the slide, showing the continents of North and South America. The globe is rendered in a light blue color with a dotted texture. Overlaid on the globe and the entire background is a complex network of white lines and glowing blue nodes, resembling a global communication or data network. The background is a solid dark blue.



Thank you!



Lech Lachowicz
ISSA Polska