paloalto NETWORKS

How Not to Ruin Your Day: Avoiding Common Threat Hunting Mistakes

Menachem Perlman

Sr. Manager, Managed Threat Hunting

July 2020

Agenda

- Common Mistakes Some Threat Hunters Make
- Basic Techniques To Find Stealthy Adversaries
- Performing Threat Hunting At Scale Using Automation And Enrichment

BASIC MISTAKES SOME THREAT HUNTERS MAKE

Basic Mistakes

Trying to look at everything collected

Rely solely on IOCs

Ignoring context

Focus on comfort zone

Ignoring known and signed files

Not reading about new attack methods

Not So Basic Mistakes

Hunting only for APTs

Trying to look for what you just read, 1:1 as the article

Not having an internal feedback process

Looking for files

Continue investigating

Basic Mistakes, Example

Trying to look at everything collected

Rely solely on IOCs

Ignoring context

Focus on comfort zone

Ignoring known and signed files

Not reading about new attack methods

Back To The Basics

Threat Actors Likes LOLBins - use common tools and commands

Living **O**ff **T**he **L**and **B**inary

Nbtstat, Psexec, Net View, CMD, Schtasks

Why?

Nothing to LOL about!

Why?

Easy

Already exists in the network

No need to deliver

Not blocked by default

Hard to discover

Cyber Hunters Approach

Collect everything

Analyze everything

Automate everything

The customer know about it

One hunting method fit all

Don’t Make These Mistakes

Collect everything	Is that necessary?	No, you don’t need to collect everything. Collect the important things but from ALL data sources, instead of everything from a single data source
Analyze everything	Is that possible?	Almost, but as a hunter, focus on the low fidelity alerts or devices without any alert and when needed leverage high fidelity alerts
Automate everything	Should you?	Try to, always think about scale and automation when possible , always remember a person in loop is mandatory

Don’t Make These Mistakes, Cont.

The customer know about it

Is that true?

No, don’t assume the security or IT team saw some activity, provide as much details as possible

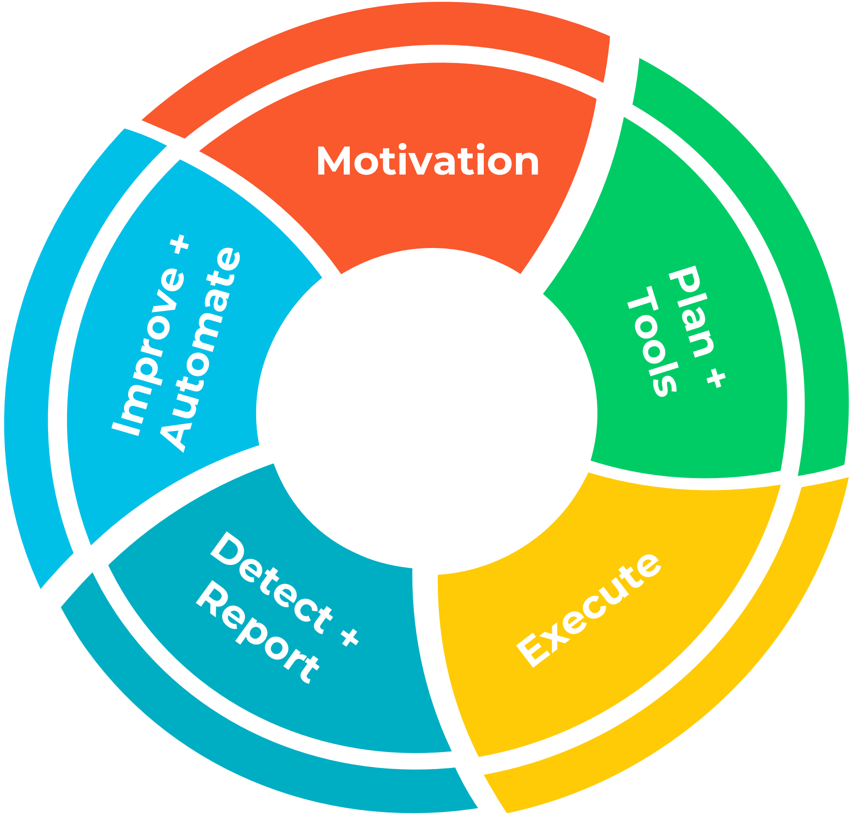
One Hunting Method fit all

Is that true?

No, using multiple methods is necessary, depends on the data source, situation and the case

TECHNIQUES TO FIND STEALTHY ADVERSARIES

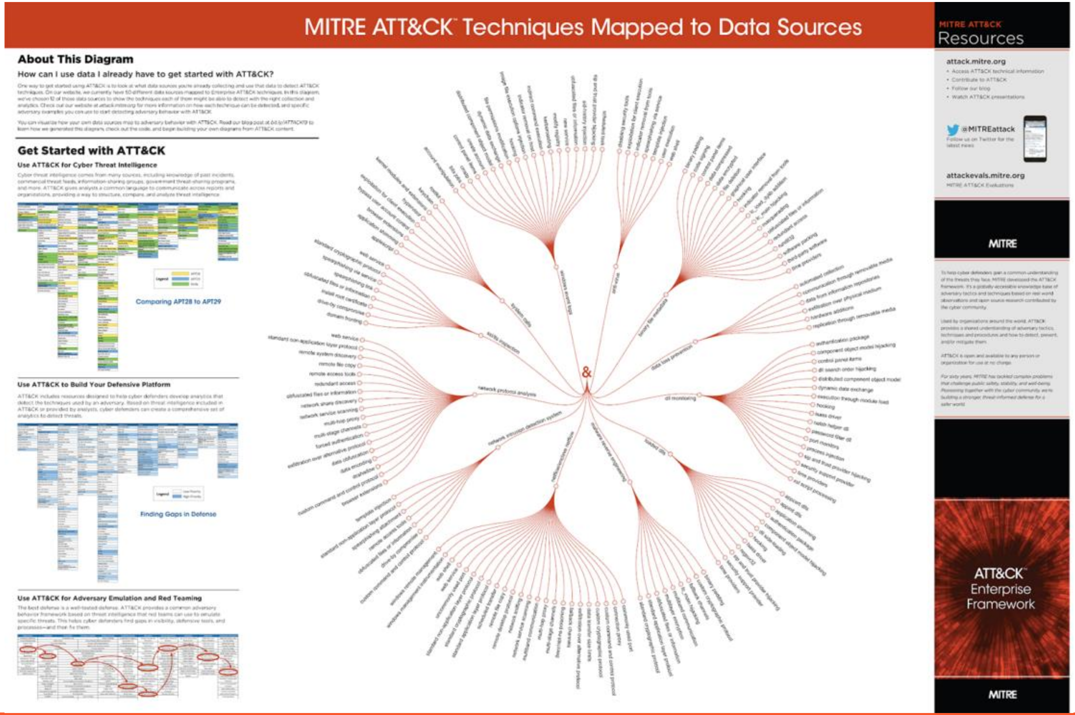
Hunting Model



MITRE

Great source for ideas and common behaviors to look for

But, there are more



MITRE ATT&CK™ Techniques Mapped to Data Sources

About This Diagram

How can I use data I already have to get started with ATT&CK?

Get Started with ATT&CK

Use ATT&CK for Cyber Threat Intelligence

Comparing APT28 to APT29

Use ATT&CK to Build Your Defensive Platform

Finding Gaps in Defense

Use ATT&CK for Adversary Emulation and Red Teaming

MITRE ATT&CK Resources

attack.mitre.org

- Access ATT&CK technical information
- Contribute to ATT&CK
- Follow our blog
- Watch ATT&CK presentations

@MITREattack

Follow us on Twitter for the latest news

attackevals.mitre.org

MITRE ATT&CK Evaluations

MITRE

ATT&CK™ Enterprise Framework

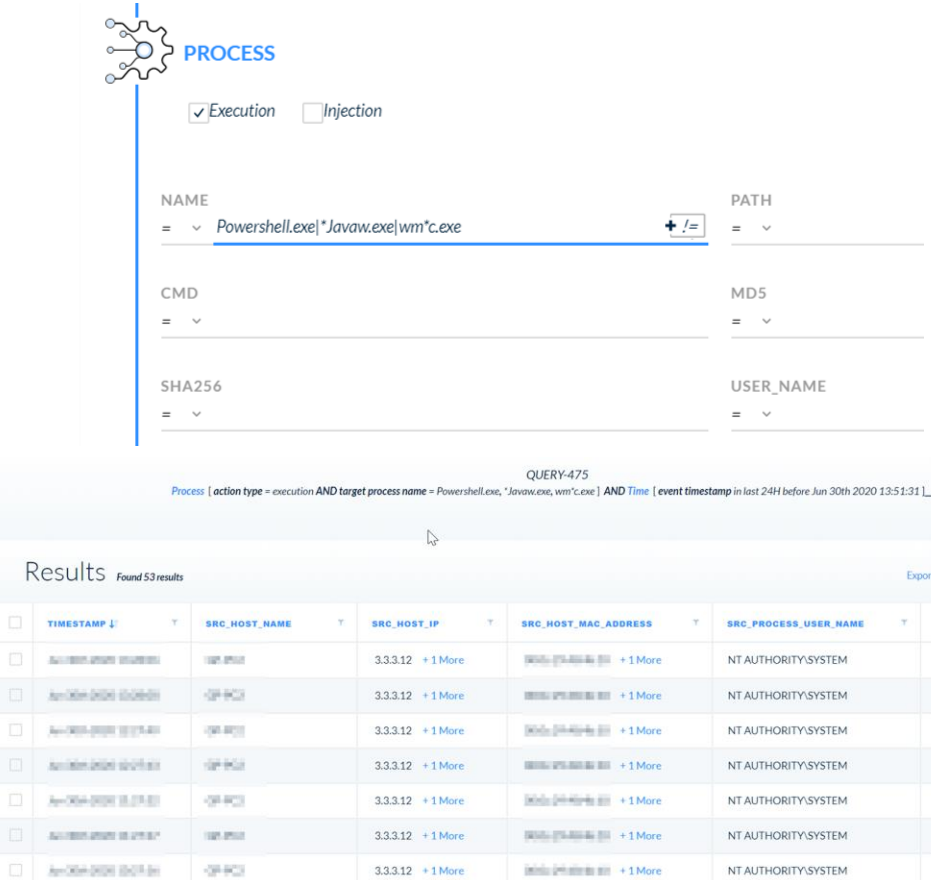
MITRE

Source MITRE

Script Engine

Look for all script execution for the following:

- Powershell.exe
- csscript.exe/wsscript.exe
- Mshta.exe
- Javaw.exe
- wmic.exe



PROCESS

☑ Execution □ Injection

NAME = Powershell.exe|*Javaw.exe|wm*c.exe

PATH =

CMD =

MD5 =

SHA256 =

USER_NAME =

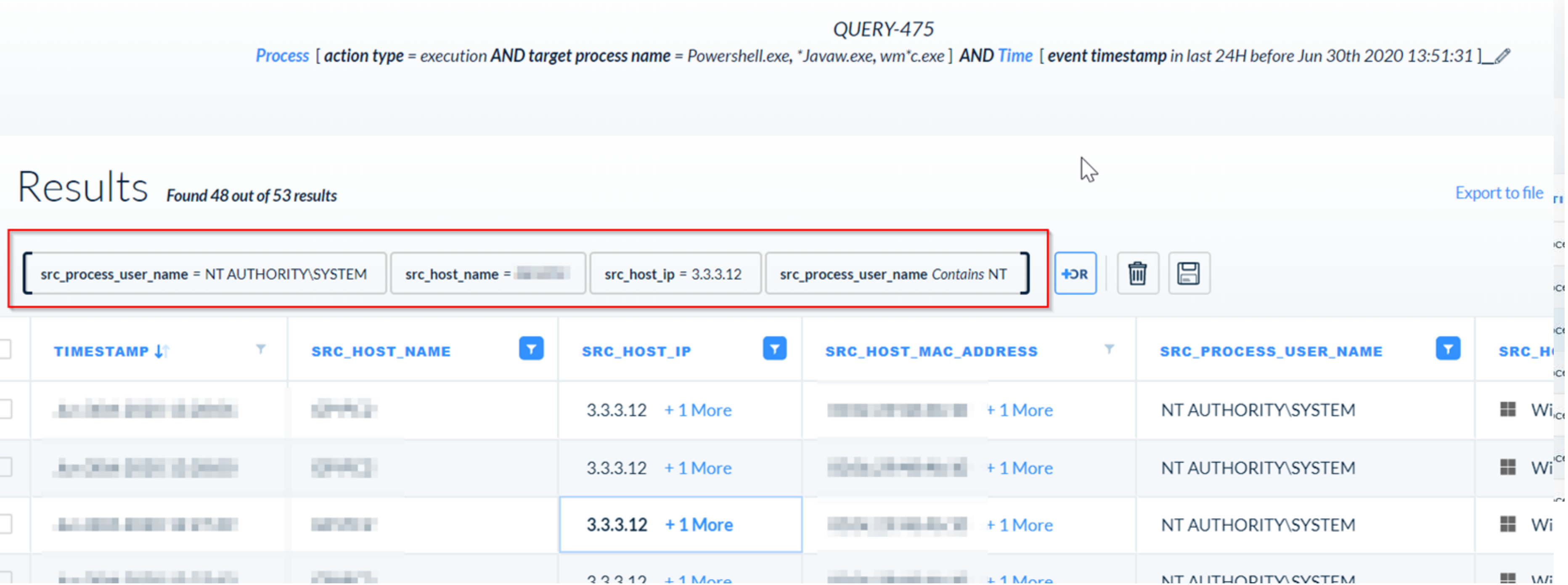
QUERY-475

Process [action type = execution AND target process name = Powershell.exe, *Javaw.exe, wm*c.exe] AND Time [event timestamp in last 24H before Jun 30th 2020 13:51:31]

Results Found 53 results

□	TIMESTAMP	SRC_HOST_NAME	SRC_HOST_IP	SRC_HOST_MAC_ADDRESS	SRC_PROCESS_USER_NAME
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM
□	[redacted]	[redacted]	3.3.3.12 +1 More	[redacted] +1 More	NT AUTHORITY\SYSTEM

Script Engine - Filter Results



QUERY-475

Process [**action type** = execution **AND target process name** = Powershell.exe, *Javaw.exe, wm*c.exe] **AND** Time [**event timestamp** in last 24H before Jun 30th 2020 13:51:31]

Results *Found 48 out of 53 results*

Export to file

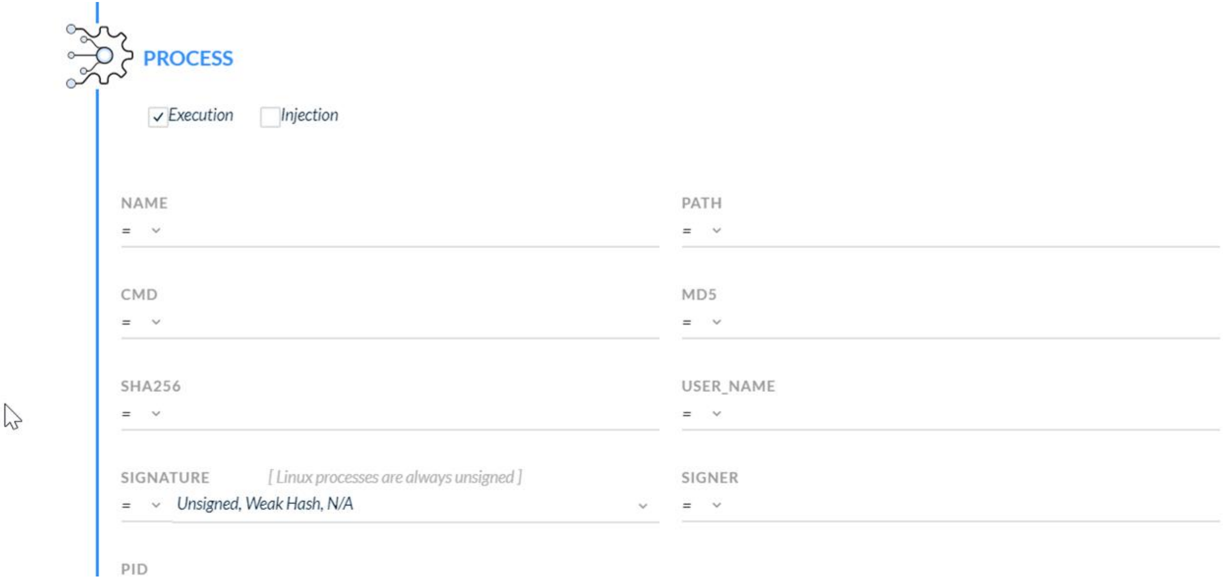
[src_process_user_name = NT AUTHORITY\SYSTEM | src_host_name = [redacted] | src_host_ip = 3.3.3.12 | src_process_user_name *Contains* NT]

	TIMESTAMP	SRC_HOST_NAME	SRC_HOST_IP	SRC_HOST_MAC_ADDRESS	SRC_PROCESS_USER_NAME	SRC_H
□	[redacted]	[redacted]	3.3.3.12 + 1 More	[redacted] + 1 More	NT AUTHORITY\SYSTEM	Wi
□	[redacted]	[redacted]	3.3.3.12 + 1 More	[redacted] + 1 More	NT AUTHORITY\SYSTEM	Wi
□	[redacted]	[redacted]	3.3.3.12 + 1 More	[redacted] + 1 More	NT AUTHORITY\SYSTEM	Wi
□	[redacted]	[redacted]	3.3.3.12 + 1 More	[redacted] + 1 More	NT AUTHORITY\SYSTEM	Wi

Unsigned Process

The goals is to find unsigned process running in the organization, often being leveraged as part of a targeted attack

There are probably a lot, so focus on a shorter time frame



PROCESS

☑ Execution ☐ Injection

NAME =

PATH =

CMD =

MD5 =

SHA256 =

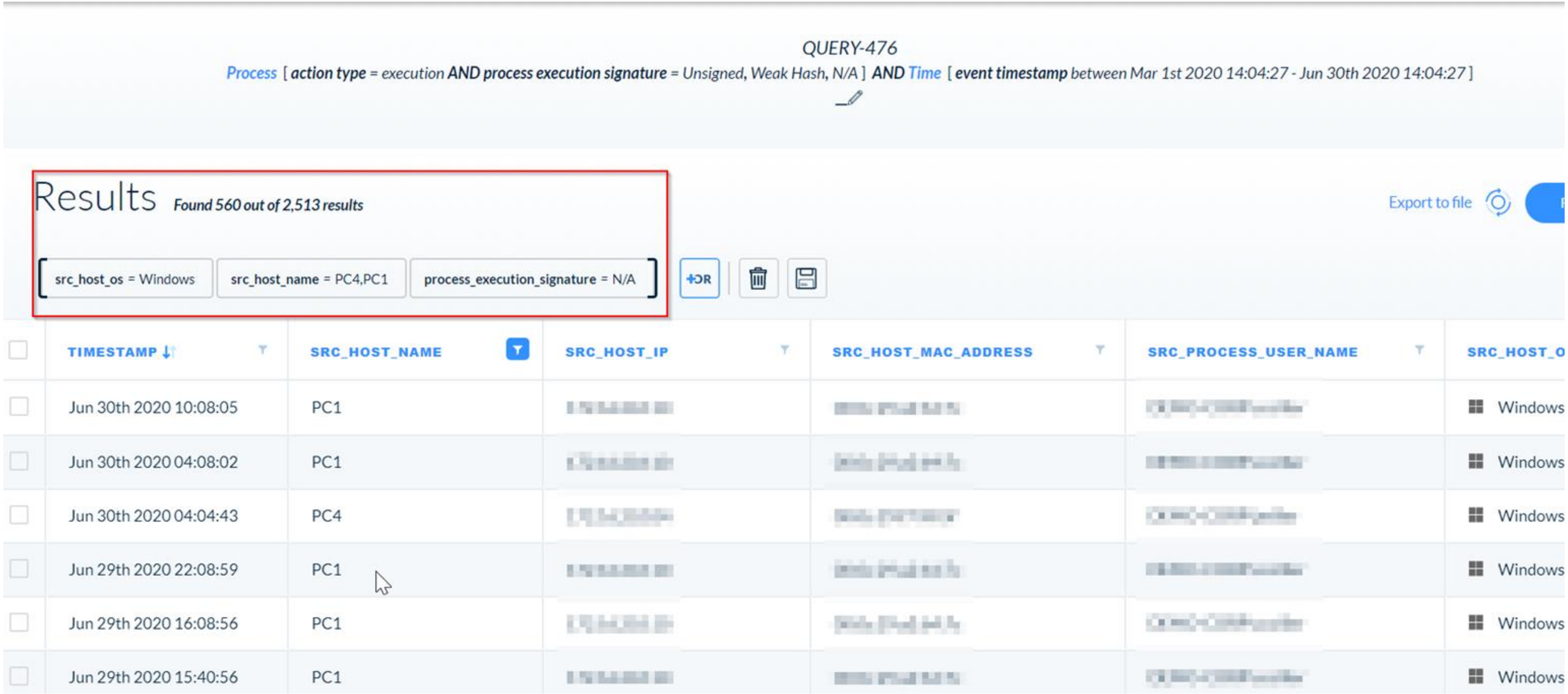
USER_NAME =

SIGNATURE [Linux processes are always unsigned]
= Unsigned, Weak Hash, N/A

SIGNER =

PID

Unsigned Processes - Filter Results



QUERY-476

Process [***action type*** = *execution* ***AND process execution signature*** = *Unsigned, Weak Hash, N/A*] ***AND*** *Time* [***event timestamp*** *between Mar 1st 2020 14:04:27 - Jun 30th 2020 14:04:27*]

Results *Found 560 out of 2,513 results*

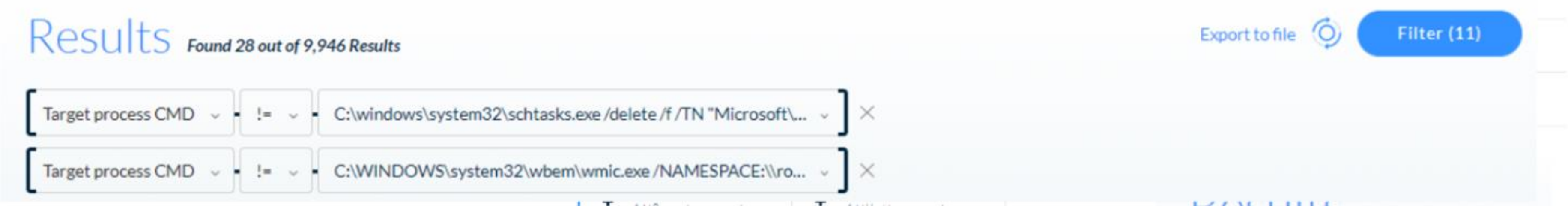
[src_host_os = Windows | src_host_name = PC4,PC1 | process_execution_signature = N/A]

□	TIMESTAMP ↓	SRC_HOST_NAME	SRC_HOST_IP	SRC_HOST_MAC_ADDRESS	SRC_PROCESS_USER_NAME	SRC_HOST_O
□	Jun 30th 2020 10:08:05	PC1	[redacted]	[redacted]	[redacted]	Windows
□	Jun 30th 2020 04:08:02	PC1	[redacted]	[redacted]	[redacted]	Windows
□	Jun 30th 2020 04:04:43	PC4	[redacted]	[redacted]	[redacted]	Windows
□	Jun 29th 2020 22:08:59	PC1	[redacted]	[redacted]	[redacted]	Windows
□	Jun 29th 2020 16:08:56	PC1	[redacted]	[redacted]	[redacted]	Windows
□	Jun 29th 2020 15:40:56	PC1	[redacted]	[redacted]	[redacted]	Windows

Known Windows Processes

Look for execution of known and legitimate Windows processes that can be leveraged by an attacker, for example:

- ‘ftp.exe’, ‘bitsadmin.exe’ and ‘x/copy.exe’ used to send data
- ’whoami.exe’ to see who’s on the active session
- ‘net.exe’, ‘netsh.exe’, ‘schtasks.exe’, ‘reg.exe’, ‘auditpol.exe’ and ‘wmic.exe’ which can be used to change the configuration of the machine



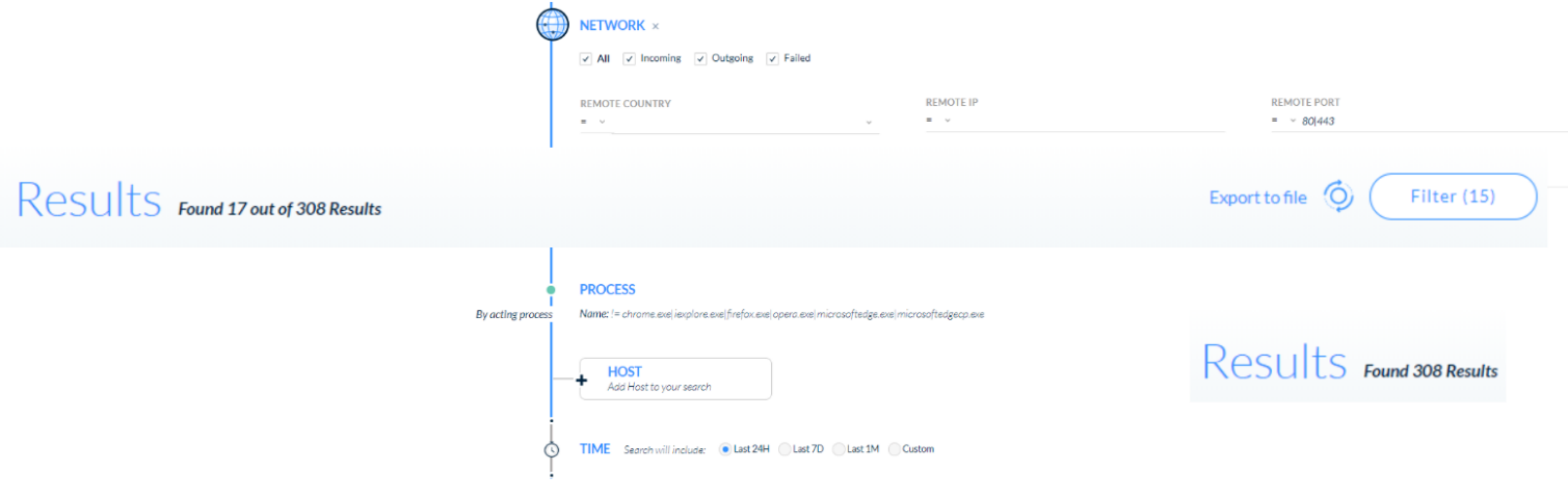
Results Found 28 out of 9,946 Results

Target process CMD	!=	C:\windows\system32\schtasks.exe /delete /f /TN "Microsoft\...
Target process CMD	!=	C:\WINDOWS\system32\wbem\wmic.exe /NAMESPACE:\\ro...

Connections Over 80/443 Not By Browser

The goals is to find items that are communicating over HTTP

There are probably a lot, so focus on a shorter time frame



NETWORK ×

☑ All ☑ Incoming ☑ Outgoing ☑ Failed

REMOTE COUNTRY =

REMOTE IP =

REMOTE PORT = 80|443

Results Found 17 out of 308 Results

PROCESS

By acting process

Name: != chrome.exe|iexplore.exe|firefox.exe|opera.exe|microsoftedge.exe|microsoftedgecp.exe

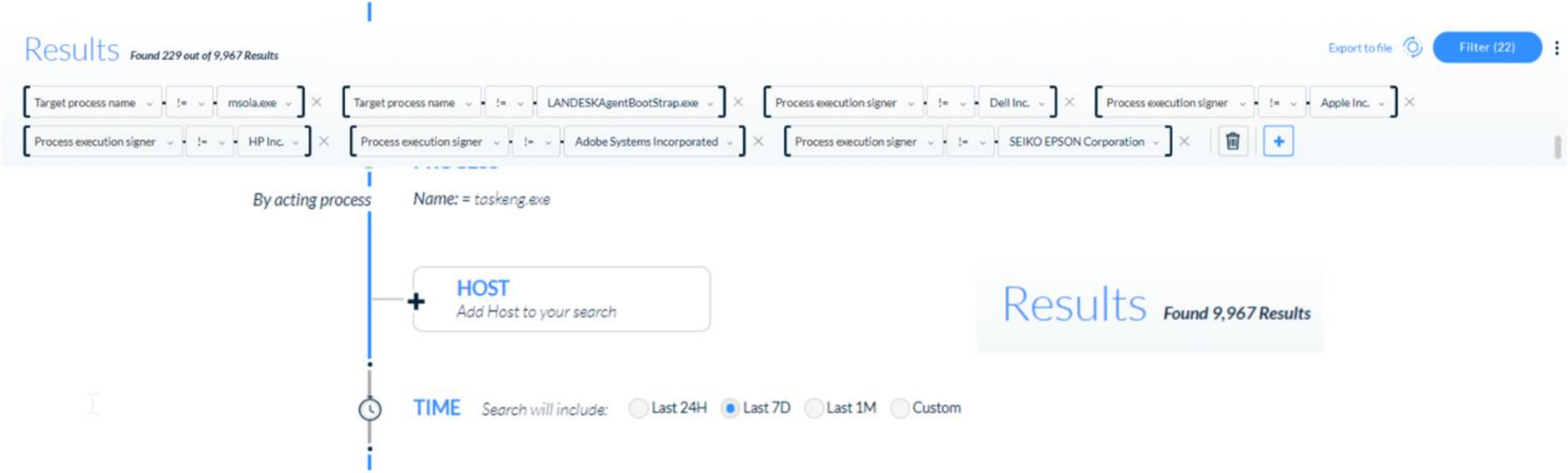
HOST
Add Host to your search

TIME Search will include: ● Last 24H ○ Last 7D ○ Last 1M ○ Custom

Results Found 308 Results

Scheduled Tasks

The goal is to check what starts from ‘taskeng.exe’ – the process who runs scheduled tasks



Results Found 229 out of 9,967 Results

[Target process name != msoia.exe]
[Target process name != LANDESKAgentBootStrap.exe]
[Process execution signer != Dell Inc.]
[Process execution signer != Apple Inc.]
[Process execution signer != HP Inc.]
[Process execution signer != Adobe Systems Incorporated]
[Process execution signer != SEIKO EPSON Corporation]

By acting process Name: = taskeng.exe

Results Found 9,967 Results

TIME Search will include: ○ Last 24H ● Last 7D ○ Last 1M ○ Custom

NGFW Hunting

- Non-browser user-agent on HTTP/S URL logs
- Looking for unknown-tcp and udp
- Large volume of data leaving the organization
- Impossible Traveler
- High ports using unknown applications to external hosts

THREAT HUNTING AT SCALE USING AUTOMATION AND ENRICHMENT

paloalto NETWORKS

THREAT HUNTING

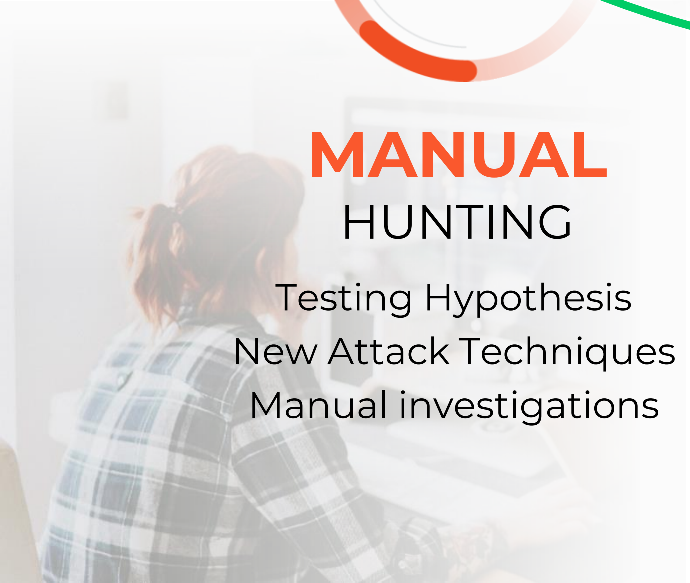
is a combination of

SCIENCE & ART

OUR MISSION

Uncover advanced adversaries using non-traditional methods and tools at scale and always be one step ahead of an intruder

HUNTING **AT SCALE**



MANUAL
HUNTING

Testing Hypothesis
New Attack Techniques
Manual investigations

SEMI-AUTOMATED
HUNTING

Automation and Playbooks
Signals and Detectors
Threat Intelligence
Extended Data Sources
AI and Machine Learning

HYPOTHESIS

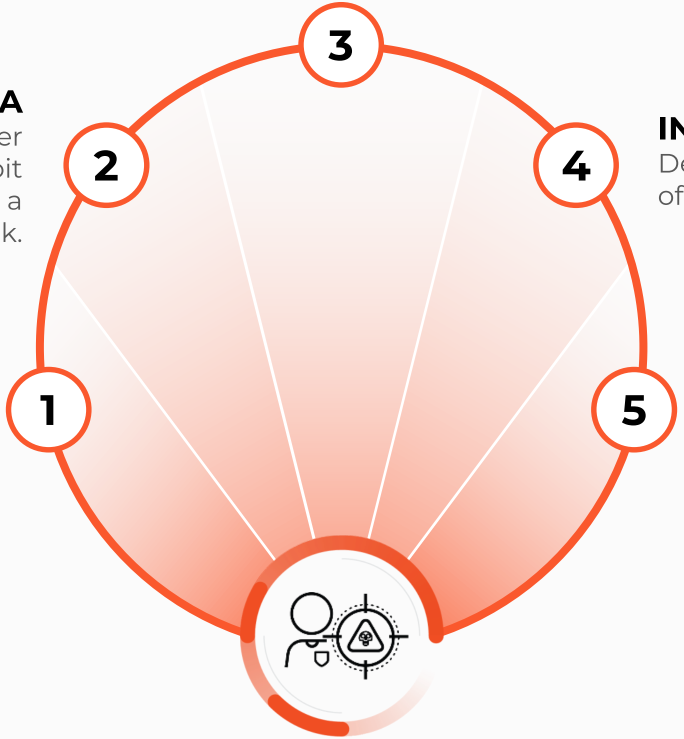
The hunter will validate the hypothesis, check results, and refine the hypothesis until the hunter has discovered threats or is confident that no threat exists.

IDEA

Based on findings from other cases or a newly published exploit or attack, the hunter will design a query to look for the attack.

INVESTIGATION

Deeper investigation of the findings and evidence.



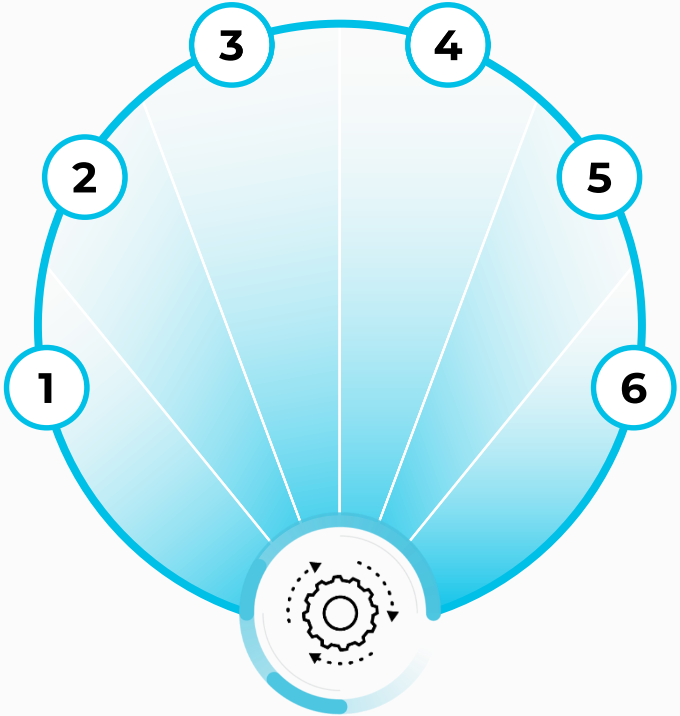
DATA SOURCES

Network, endpoint, cloud and third-party data sources provided by customers.

REPORT

The hunter sends a report with findings to the customer.

MANUAL HUNTING



DATA SOURCES

Network, endpoint, cloud and
third-party data sources
provided by customers.

SIGNALS

Smart signals analyzing all
collected data in order to every
discover threat. Signals are
based on one or all customers.

ENRICHMENT & PRIORITIZATION

Enriching incidents found by the signals
and prioritization.

INITIAL INVESTIGATION

The first step for the hunter is to validate
the signal before investigating it in the
Cortex XDR management console.

DEEP INVESTIGATION

Hunter performs a manual
investigation to confirm the threat and
understand the full scope of the attack.

REPORT

The hunter sends
a report with findings
to the customer.

SEMI-AUTOMATED
HUNTING

Summary

- Operate smart - multiple techniques, collect what is necessary
- Share techniques - collaborate with others, quantify the results
- A person in the loop is always required but an automation mindset is mandatory

Thank you

Paloaltonetworks.com
Menachem Perlman