Indonesia Honeynet Project

Demystifying Threat Hunting

Digit Oktavianto
digit dot Oktavianto at gmail dot com

Meetup Cyber Defense Community – BliBli Office
20 Oktober 2017

Who Am I

Who Am I

- Information Security Consultant at XYZ Company
- Independent Security Researcher Focusing on :
    - Cyber Defense Operation
    - Threat Hunting
    - Digital Forensic and Incident Response
    - Malware Analysis
    - All About Blue Team

Demystifying Threat Hunting

5W and 1H About Threat Hunting

3 Common Myth About Threat Hunting

1. **Hunting can be fully automated**

Hunting is not a reactive activity. If the main human input in a hunt is remediating the result of something that a tool automatically found, you are being reactive and not proactive. You are resolving an identified potential incident, which is a critically important practice in a SOC, but not hunting. Hunting requires the input of a human analyst and is about proactive, hypothesis-based investigations.

2. Hunting can only be carried out with vast quantities of data and a stack of advanced tools

Though it may seem like a new term, security analysts across a variety of sectors have been hunting for years. Basic hunting techniques can still be very useful and effective in helping you find the bad guys. An analyst who wants to begin threat hunting should not hesitate to dive into some of the basic techniques with just simple data sets and tools. Take advantage of low hanging fruit!

3 Common Myth About Threat Hunting

3. Hunting is only for elite analysts; only the security 1% with years of experience can do it

As you'll learn, there are many different hunting techniques that have differing levels of complexity. However, not all these techniques take years to master. Many of the same analysis techniques used for incident response and alert investigation and triage can also be leveraged for hunting. The key to getting started is simply knowing what questions to ask, and digging into the datasets related to them. You learn to hunt by doing it, so if you're an analyst who has never hunted before, don't be afraid to dive in.

W1 : What is Threat Hunting?

Many organizations are quickly discovering that **cyber threat hunting** is the next step in the evolution of the modern Security Operations Center (SOC), but they remain unsure of how to start hunting or how far along they are in developing their hunt capabilities

We define **threat hunting as the process of proactively and iteratively searching through networks to detect and isolate advanced threats that evade existing security solutions.** There are many different techniques hunters might use to find the bad guys, and no single one of them is always “right”. The best one often depends on the type of activity you are trying to find.

Cyber threat hunting is the practice of searching iteratively through data to detect advanced threats that evade traditional security solutions

W1 : What is Threat Hunting?

- Hunting consists of **manual or machine-assisted techniques**, as opposed to **relying only on automated systems like SIEMs**. Alerting is important, but cannot be the only focus of a detection program. In fact, one of the **chief goals of hunting should be to improve automated detection by prototyping new ways to detect malicious activity** and then turning those prototypes into effective new automations

W2 : Why Threat Hunting?

- Threats are human. It is the adversaries, not just their tools, such as malware, that interest threat hunters. These adversaries are persistent and flexible and often evade network defenses.
- The threats are often identified as advanced persistent threats (APTs), not just because of the capabilities that the adversaries wield, but also because of their ability to initiate and maintain long-term operations against targets. Focused and funded adversaries will not be countered by security boxes on the network alone. And threat hunters are not simply waiting to respond to alerts or indicators of compromise (IOCs). They are actively searching for threats to prevent or minimize damage

W3 : When Do you Hunt?

- The most significant part of this challenge is to organically integrate threat hunting into existing workflows so that it complements current security efforts. Threat hunting is often appropriately performed by organizations of various levels of security maturity. However, to fully take advantage of threat hunting, organizations must invest in the security infrastructure that is needed to use threat hunting tools and practices properly.
- The more mature of threat hunting capability in the organization, the more often they perform threat hunting on daily basis

W4 : Where Threat Hunting Fits In?

- Organizations performing security operations are already hunting today (usually informally) regardless of where they are in their security maturity.
- However, as appropriate investments are made along the scale—such as monitoring infrastructure to enable active defense actions such as threat hunting—the hunt team produces significantly more output. In that way, threat hunting is an activity that continually provides increasing value to organizations as they grow in their maturity.

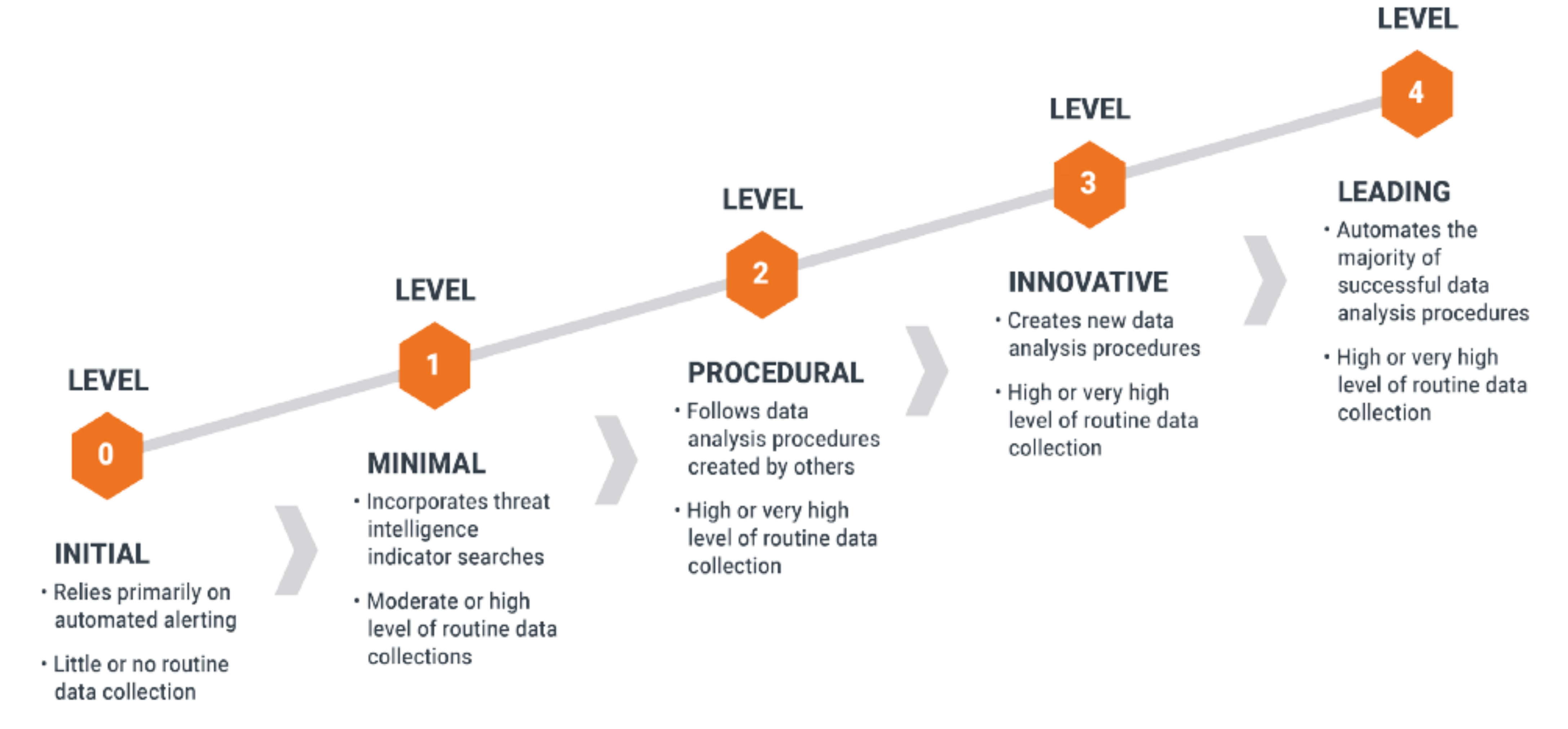
W5 : Who Are The Right People to Hunt?

- Even if they operate in dual-hatted roles such as incident responder/threat hunter or security operations center analyst/threat hunter, threat hunters must be dedicated to actively pursuing adversaries.
- These defenders add the most value when they are fixated on true threats and not restricted to responding to alerts or network maintenance issues such as patching vulnerabilities. In a team structure, threat hunters work alongside other network and security teams in the organization, not in competition with them. Many hunting teams are positioned inside of a security operations center or as part of a computer security incident response team.

1H : How to Hunt?

- Start with a good hypothesis about threats that might be in the organization, the best places in the organization to go hunting and how threats might take advantage of users or business processes to bypass security appliances.
- As an example, hunters can consider crown jewels analysis: They identify the assets and information that are most vital to the organization's mission so that they can prioritize their efforts, use passive defenses and hardening techniques to reduce their risk, and generate hypotheses about what an adversary could do to compromise the assets. In the crown jewels example, hunters combine an understanding of their environment with a hypothesis of what the adversary might do.

Threat Hunting Maturity Model



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

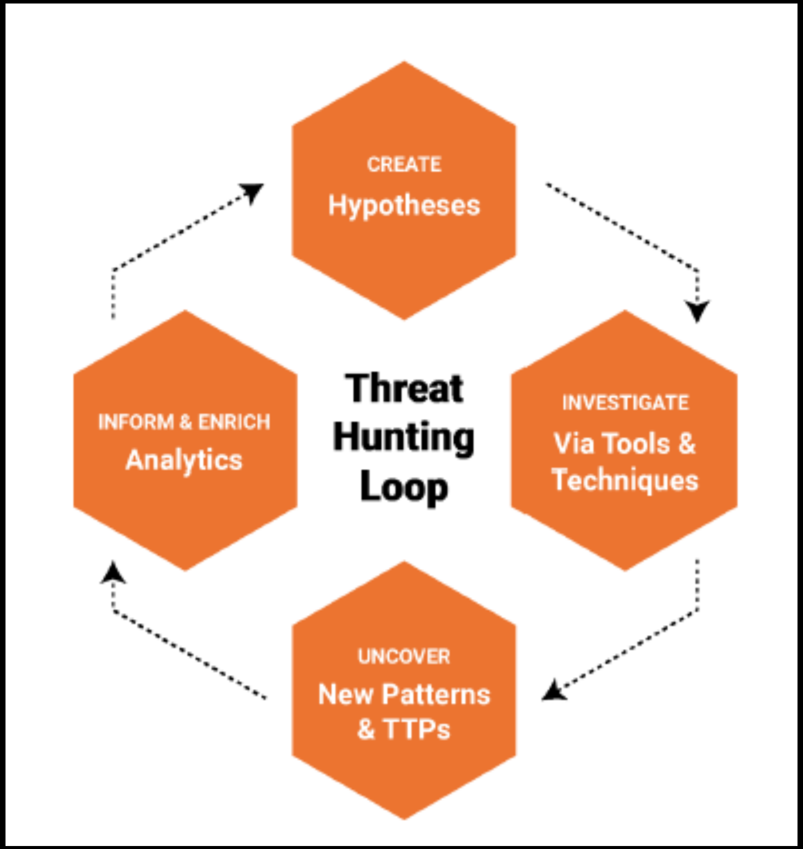
- Creates new data analysis procedures
- High or very high level of routine data collection

LEVEL 4

LEADING

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Threat Hunting Life Cycle



CREATE Hypotheses

INVESTIGATE Via Tools & Techniques

UNCOVER New Patterns & TTPs

INFORM & ENRICH Analytics

Threat Hunting Loop

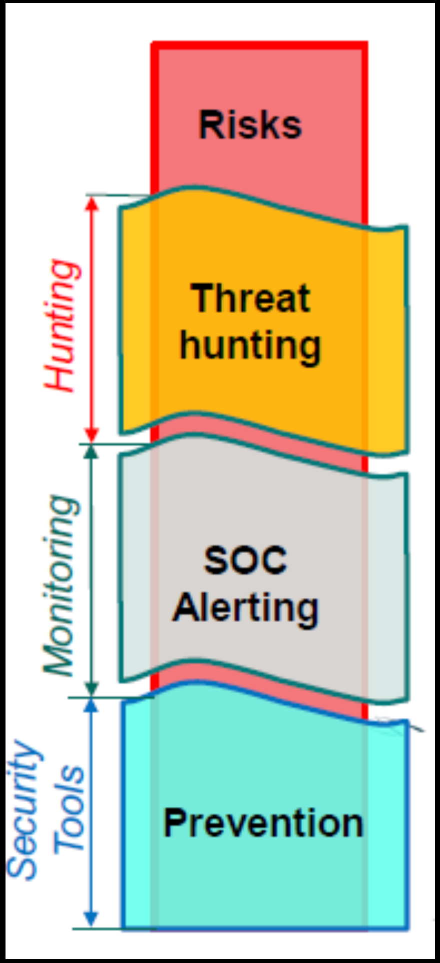
What is it for?

BUSINESS:

- Minimize residual risks
- Minimize time between attack and detection

TECH:

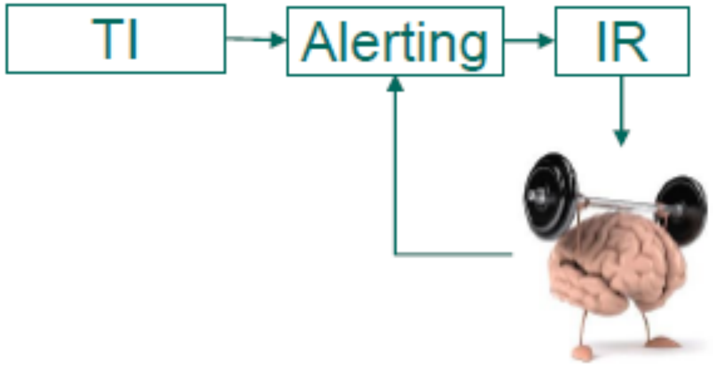
- Unknown [targeted] attacks detection
- Non-malware attacks detection
- TTP based detection
- “Time machine” for evidence analysis



Threat Hunting Vs Alert Based Investigation

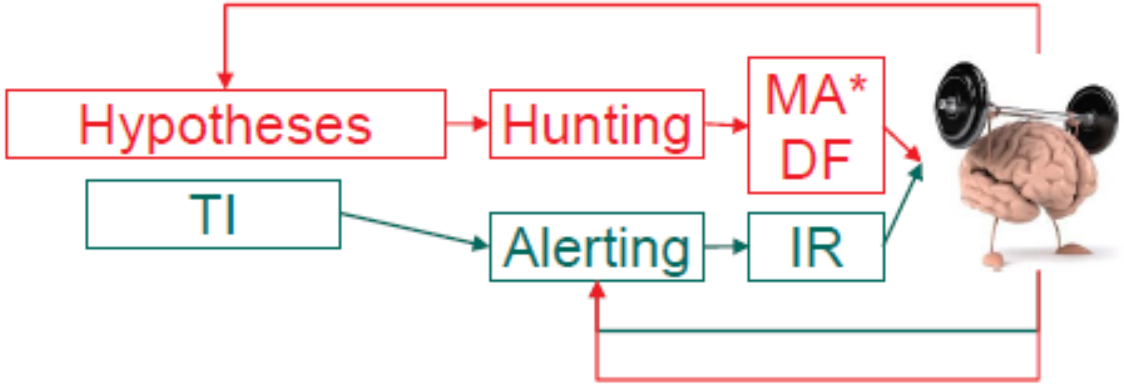
SOC/Alerting

- Reactive
- Detect/forget



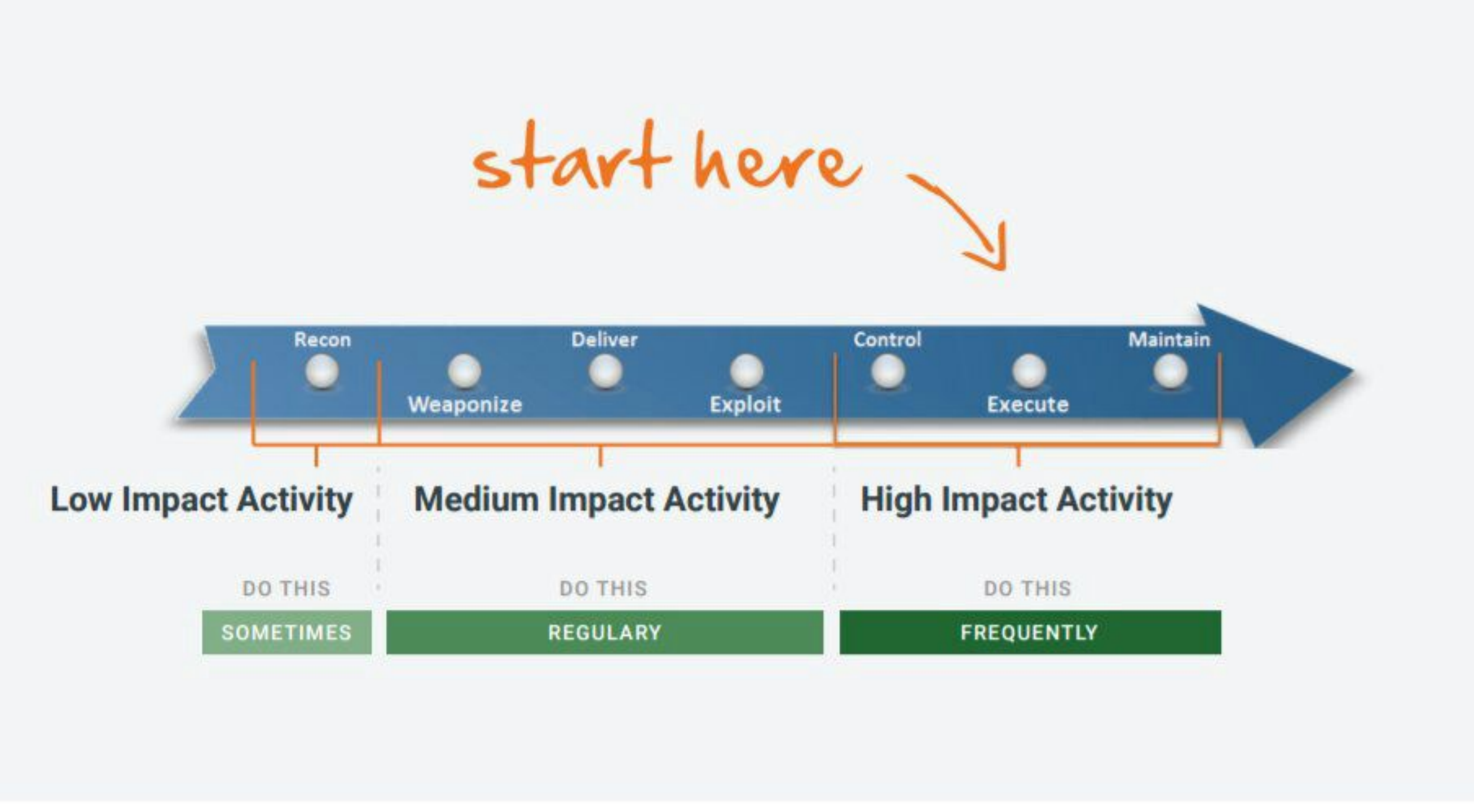
Hunting/Mining

- Proactive
- Repeated searches



* MA – malware analysis, DF – digital forensics, IR – incident response

Threat Hunting Activity



start here

Recon

Weaponize

Deliver

Exploit

Control

Execute

Maintain

Low Impact Activity

Medium Impact Activity

High Impact Activity

DO THIS

SOMETIMES

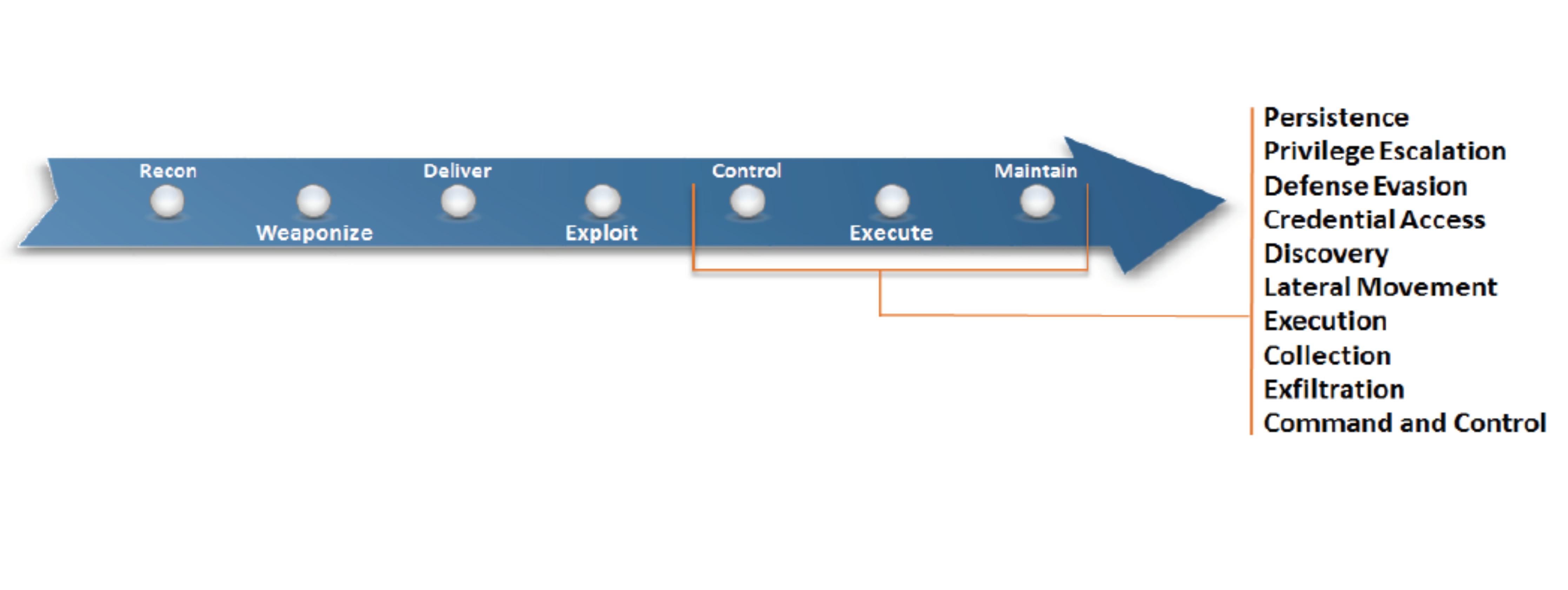
DO THIS

REGULARY

DO THIS

FREQUENTLY

Cyber Kill Chain VS MITRE ATT&CK Framework



MITRE ATT&CK Framework

- For example, the later stages (Control, Maintain, and Execute) of MITRE's seven-stage ATT&CK lifecycle include categories like lateral movement and data exfiltration, under which many kinds of activities can exist. **Here's an example list of potential attacker activities and techniques you might identify**:
- Malware Beaconing
- DLL Injection
- Pass the Hash (PtH)
- Mimikatz
- DNS Tunneling

How do I Hunt On the Cheap

- Look at your network and your hosts
- General Hunt methodology
  - Collect data
  - Analyze collection – outliers and indications of bad
  - Follow up on leads
  - Remediate
  - Repeat
- Specific places to look and what to look for in the data
  - Network
  - Host

Threat Hunting
Sample Use Case

Sample Threat Hunting Use Case

- Hunting for Internal Recon
- Hunting for Command and Control (C&C)
- Hunting for Persistence Malware Activity
- Hunting for Lateral Movement

Hunting for Internal Recon Process

Hypothesis: An attacker conducting internal reconnaissance would attempt to carry out host enumeration and automate these commands with a script Look for these commands to be spawned by a script:

- whoami
- net user
- useraccount (WMIC)
- Get-NetIPConfiguration (PowerShell)
- hostname
- ipconfig
- nicconfig (WMIC)

Hunting for Internal Recon Process

Investigation (Tools and Data)

Determine what datasets you are using:

- Process execution metadata
- Process filenames
- Process file hashes

Hunting for Command and Control

Hypothesis: *Attackers may be operating on a C2 channel that uses* custom encryption (uncommon protocol) *on a* common network port

Look for:

- Anomalies in monitored network port channels, i.e. connections that do not have protocol artifacts related to the common port you are looking at. For example, look for connections that have no identifiable HTTP metadata over port 80/TCP

Hunting for Command and Control

Investigation (Tools and Data)

Determine what datasets you are using:

For identifying use of common protocols, you will want to focus primarily on application protocol metadata, including:

- Endpoint Logs (Gathered from OSSEC)
- Proxy logs, IIS logs
- DNS resolution logs
- Bro HTTP, SSL, DNS, SMTP logs

Hunting for Persistence Malware Activity

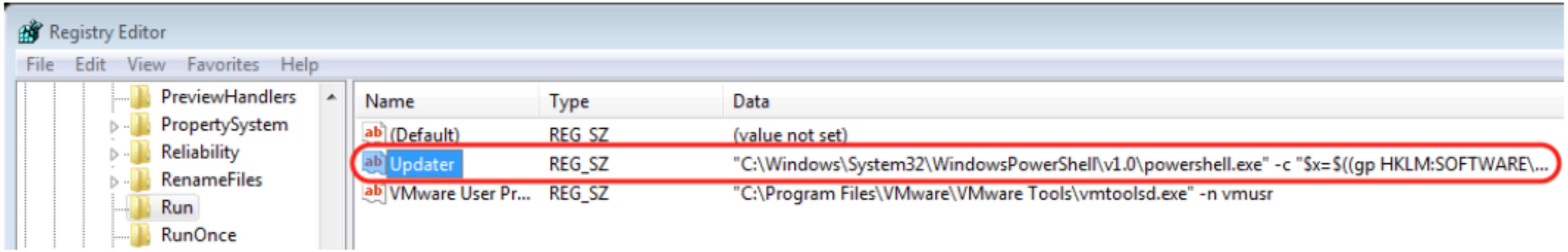
Hypothesis: *Attackers may create a scheduler task, or add registry value for the intend to persistence activity in target host*

Look for:

- Anomaly Scheduler Task
- Registry for Persistence Malware Hiding

Hunting for Persistence Malware Activity

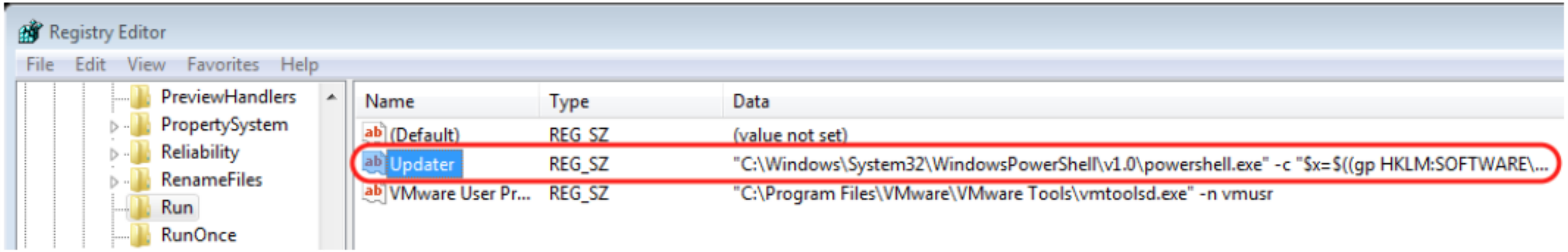
- Inject HKLM\Software\Microsoft\Windows\CurrentVersion\Windows\Run



Name	Type	Data
(Default)	REG_SZ	(value not set)
Updater	REG_SZ	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$x=$((gp HKLM:SOFTWARE\...
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

Hunting for Persistence Malware Activity

- Inject HKLM\Software\Microsoft\Windows\CurrentVersion\Windows\Run



Name	Type	Data
(Default)	REG_SZ	(value not set)
Updater	REG_SZ	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -c "$x=$((gp HKLM:SOFTWARE\...
VMware User Pr...	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr

Remote execution via PsExec (& clones, e.g. PaExec)

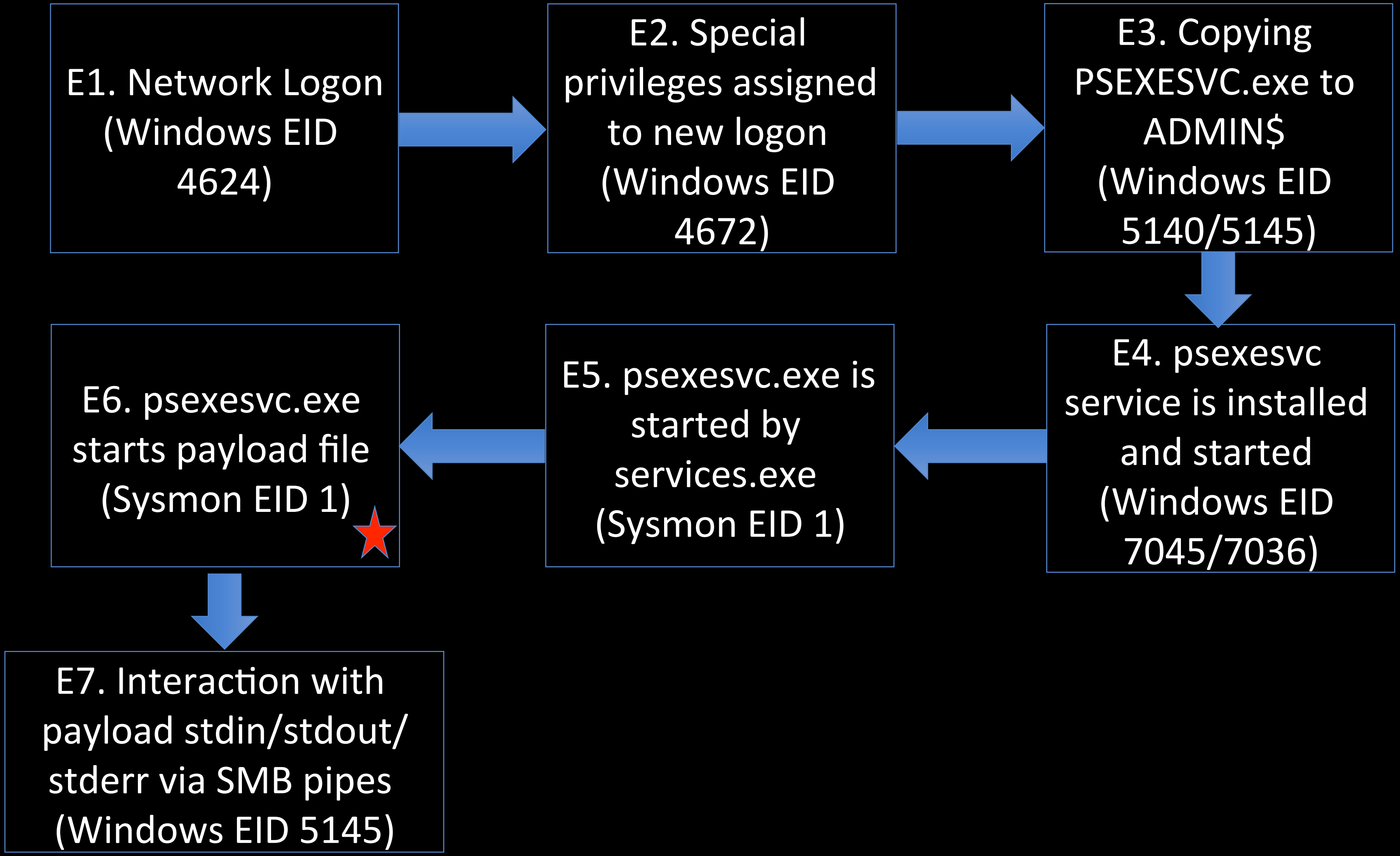
How

- PsExex:
  - *psexec.exe \\pc0002 -c mimikatz.exe privilege::debug sekurlsa::logonpasswords exit*
- PaExec:
  - *paexec.exe \\pc0002 -c mimikatz.exe privilege::debug sekurlsa::logonpasswords exit*

Requirements & limitations

- ADMIN$ administrative share is enabled on remote host
- TCP/445 port is accessible on remote host

Remote execution via PsExec (& clones) – events sequence on destination side



E1. Network Logon (Windows EID 4624)

E2. Special privileges assigned to new logon (Windows EID 4672)

E3. Copying PSEXESVC.exe to ADMIN$ (Windows EID 5140/5145)

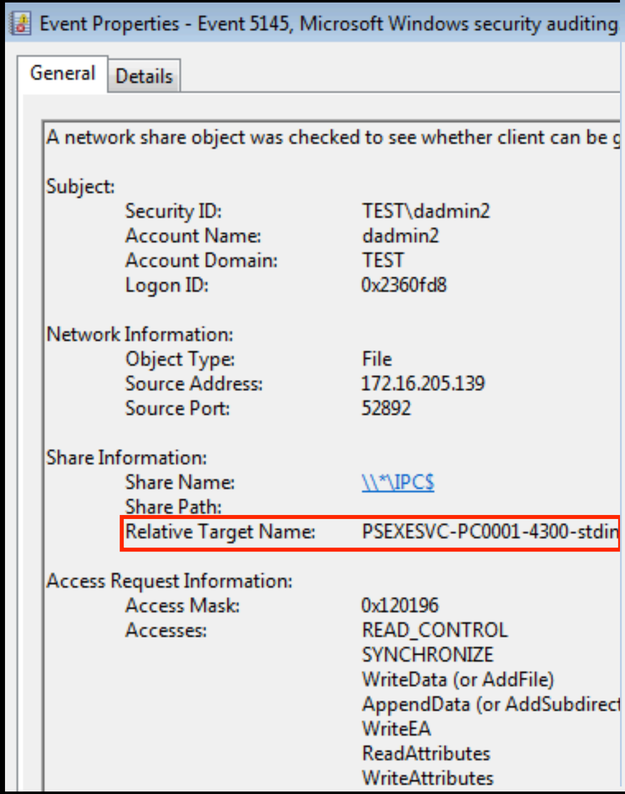
E4. psexesvc service is installed and started (Windows EID 7045/7036)

E5. psexesvc.exe is started by services.exe (Sysmon EID 1)

E6. psexesvc.exe starts payload file (Sysmon EID 1)

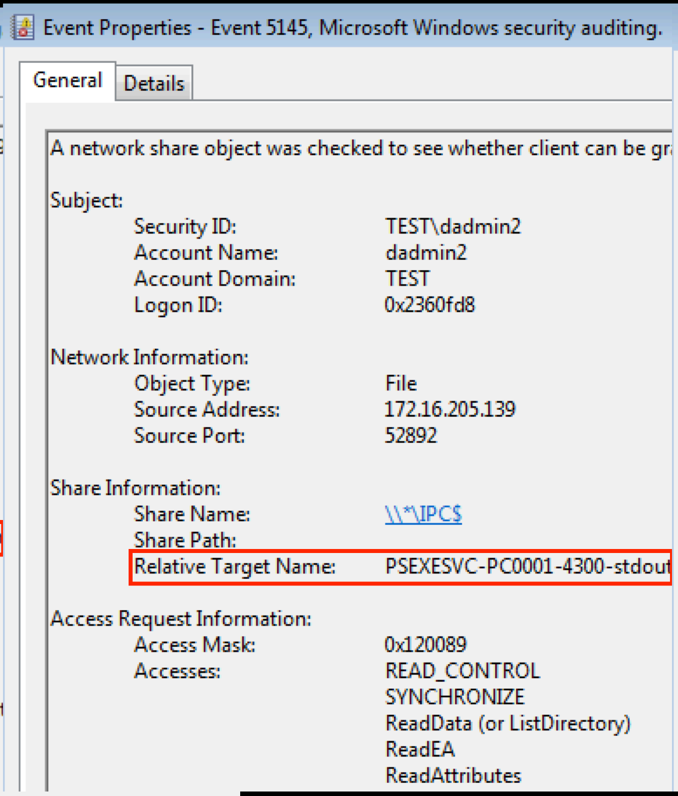
E7. Interaction with payload stdin/stdout/stderr via SMB pipes (Windows EID 5145)

Remote execution via PsExec (& clones) – the most interesting events



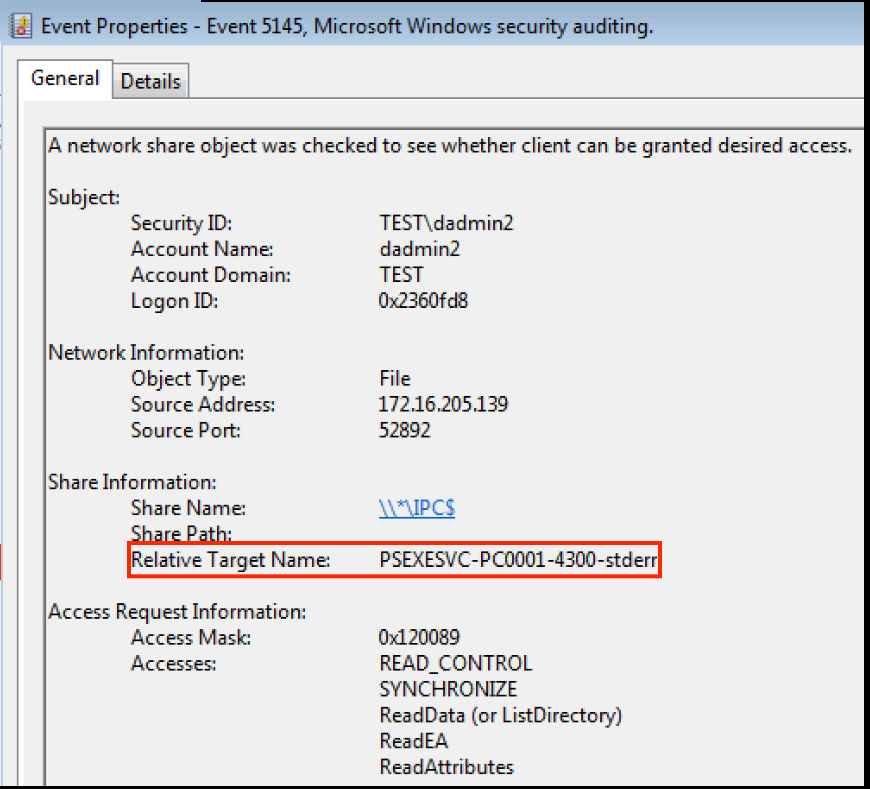
Event Properties - Event 5145, Microsoft Windows security auditing

```
A network share object was checked to see whether client can be g

Subject:
        Security ID:            TEST\dadmin2
        Account Name:           dadmin2
        Account Domain:         TEST
        Logon ID:               0x2360fd8

Network Information:
        Object Type:            File
        Source Address:         172.16.205.139
        Source Port:            52892

Share Information:
        Share Name:             \\*\IPC$
        Share Path:
        Relative Target Name:   PSEXESVC-PC0001-4300-stdin

Access Request Information:
        Access Mask:            0x120196
        Accesses:               READ_CONTROL
                                SYNCHRONIZE
                                WriteData (or AddFile)
                                AppendData (or AddSubdirect
                                WriteEA
                                ReadAttributes
                                WriteAttributes
```



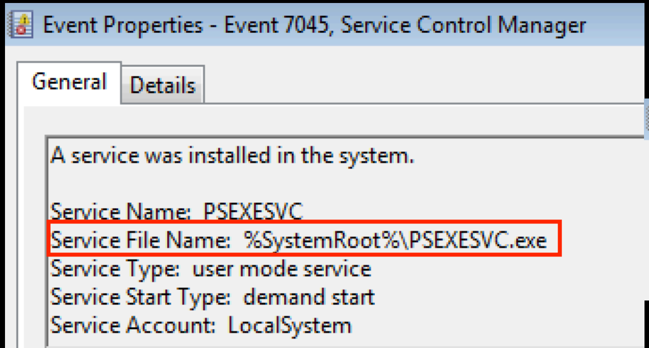
Event Properties - Event 5145, Microsoft Windows security auditing.

```
A network share object was checked to see whether client can be gr

Subject:
        Security ID:            TEST\dadmin2
        Account Name:           dadmin2
        Account Domain:         TEST
        Logon ID:               0x2360fd8

Network Information:
        Object Type:            File
        Source Address:         172.16.205.139
        Source Port:            52892

Share Information:
        Share Name:             \\*\IPC$
        Share Path:
        Relative Target Name:   PSEXESVC-PC0001-4300-stdout

Access Request Information:
        Access Mask:            0x120089
        Accesses:               READ_CONTROL
                                SYNCHRONIZE
                                ReadData (or ListDirectory)
                                ReadEA
                                ReadAttributes
```



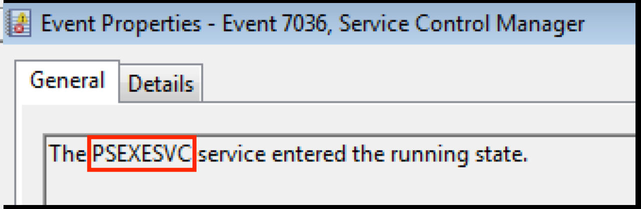
Event Properties - Event 5145, Microsoft Windows security auditing.

```
A network share object was checked to see whether client can be granted desired access.

Subject:
        Security ID:            TEST\dadmin2
        Account Name:           dadmin2
        Account Domain:         TEST
        Logon ID:               0x2360fd8

Network Information:
        Object Type:            File
        Source Address:         172.16.205.139
        Source Port:            52892

Share Information:
        Share Name:             \\*\IPC$
        Share Path:
        Relative Target Name:   PSEXESVC-PC0001-4300-stderr

Access Request Information:
        Access Mask:            0x120089
        Accesses:               READ_CONTROL
                                SYNCHRONIZE
                                ReadData (or ListDirectory)
                                ReadEA
                                ReadAttributes
```



Event Properties - Event 7045, Service Control Manager

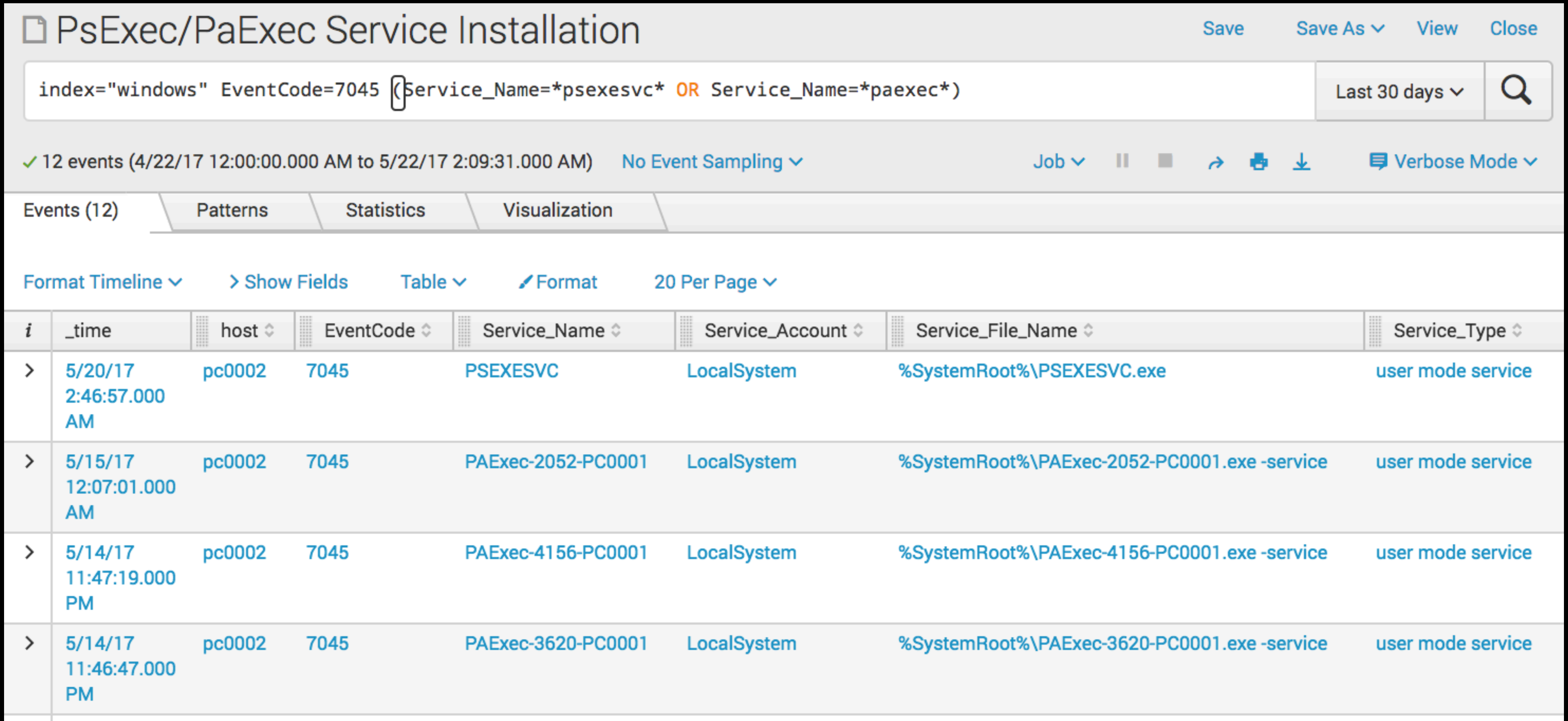
```
A service was installed in the system.

Service Name:  PSEXESVC
Service File Name:  %SystemRoot%\PSEXESVC.exe
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```



Event Properties - Event 7036, Service Control Manager

```
The PSEXESVC service entered the running state.
```

Hunting: search for PsExec (& clones) artifacts – services



PsExec/PaExec Service Installation

```
index="windows" EventCode=7045 (Service_Name=*psexesvc* OR Service_Name=*paexec*)
```

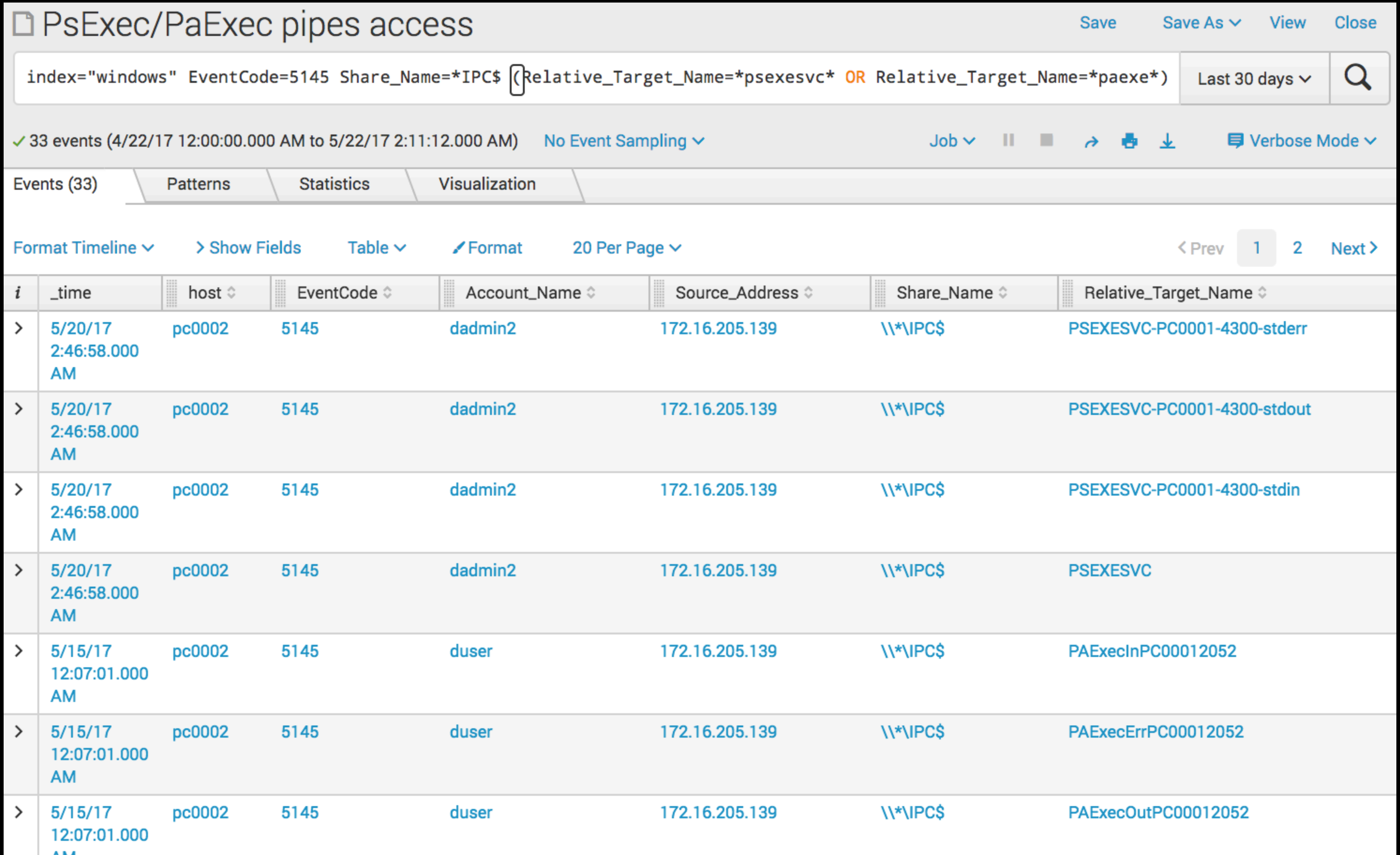
Last 30 days

✓ 12 events (4/22/17 12:00:00.000 AM to 5/22/17 2:09:31.000 AM) No Event Sampling

Verbose Mode

i	_time	host	EventCode	Service_Name	Service_Account	Service_File_Name	Service_Type
>	5/20/17 2:46:57.000 AM	pc0002	7045	PSEXESVC	LocalSystem	%SystemRoot%\PSEXESVC.exe	user mode service
>	5/15/17 12:07:01.000 AM	pc0002	7045	PAExec-2052-PC0001	LocalSystem	%SystemRoot%\PAExec-2052-PC0001.exe -service	user mode service
>	5/14/17 11:47:19.000 PM	pc0002	7045	PAExec-4156-PC0001	LocalSystem	%SystemRoot%\PAExec-4156-PC0001.exe -service	user mode service
>	5/14/17 11:46:47.000 PM	pc0002	7045	PAExec-3620-PC0001	LocalSystem	%SystemRoot%\PAExec-3620-PC0001.exe -service	user mode service

Hunting: search for PsExec (& clones) artifacts – access to pipes



PsExec/PaExec pipes access

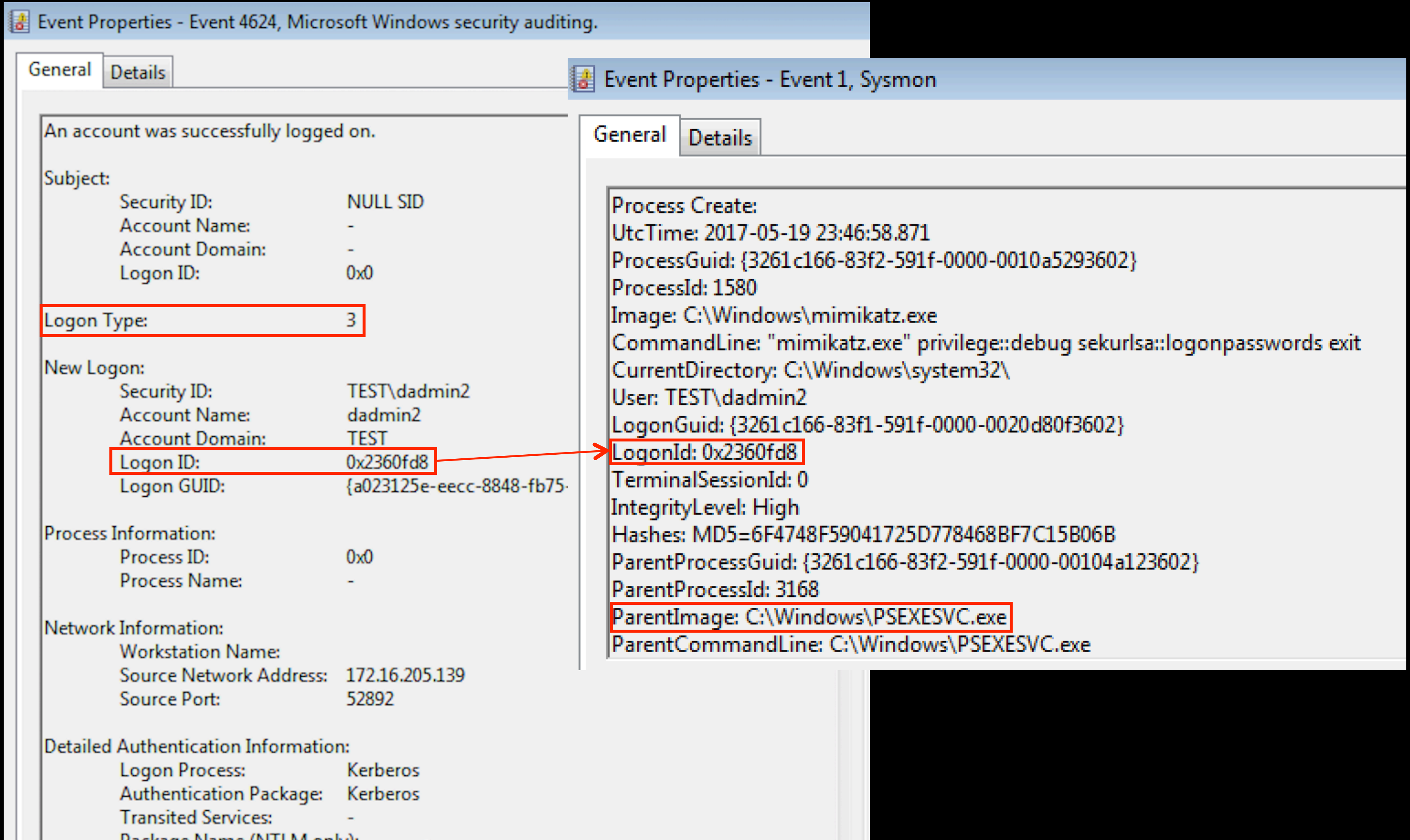
```
index="windows" EventCode=5145 Share_Name=*IPC$ (Relative_Target_Name=*psexesvc* OR Relative_Target_Name=*paexe*)
```

Last 30 days

✓ 33 events (4/22/17 12:00:00.000 AM to 5/22/17 2:11:12.000 AM)

i	_time	host	EventCode	Account_Name	Source_Address	Share_Name	Relative_Target_Name
>	5/20/17 2:46:58.000 AM	pc0002	5145	dadmin2	172.16.205.139	*\IPC$	PSEXESVC-PC0001-4300-stderr
>	5/20/17 2:46:58.000 AM	pc0002	5145	dadmin2	172.16.205.139	*\IPC$	PSEXESVC-PC0001-4300-stdout
>	5/20/17 2:46:58.000 AM	pc0002	5145	dadmin2	172.16.205.139	*\IPC$	PSEXESVC-PC0001-4300-stdin
>	5/20/17 2:46:58.000 AM	pc0002	5145	dadmin2	172.16.205.139	*\IPC$	PSEXESVC
>	5/15/17 12:07:01.000 AM	pc0002	5145	duser	172.16.205.139	*\IPC$	PAExecInPC00012052
>	5/15/17 12:07:01.000 AM	pc0002	5145	duser	172.16.205.139	*\IPC$	PAExecErrPC00012052
>	5/15/17 12:07:01.000	pc0002	5145	duser	172.16.205.139	*\IPC$	PAExecOutPC00012052

Remote execution via PsExec (& clones) – the most interesting events

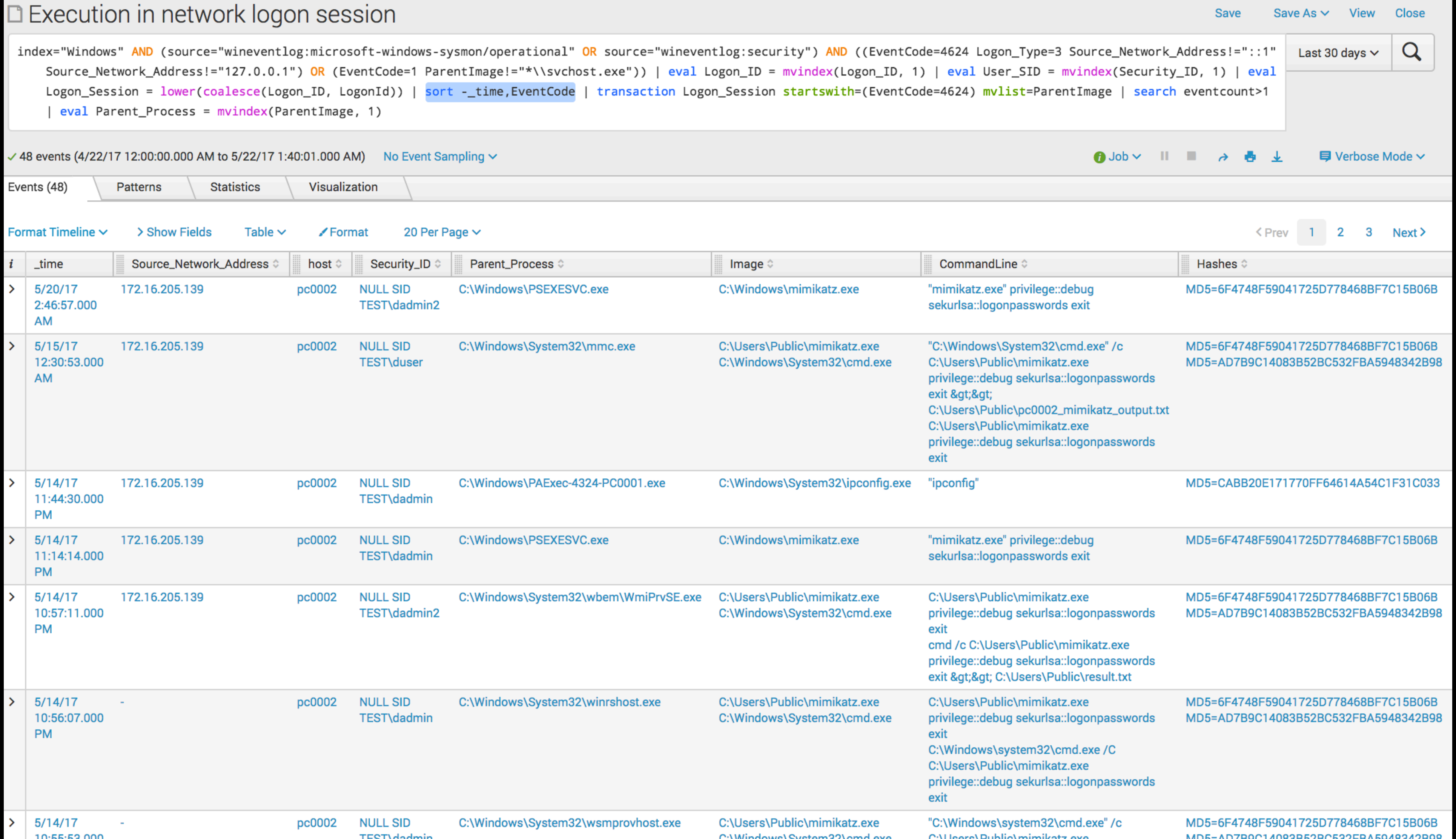


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details

```
An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            TEST\dadmin2
        Account Name:           dadmin2
        Account Domain:         TEST
        Logon ID:               0x2360fd8
        Logon GUID:             {a023125e-eecc-8848-fb75-

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:
        Source Network Address: 172.16.205.139
        Source Port:            52892

Detailed Authentication Information:
        Logon Process:          Kerberos
        Authentication Package: Kerberos
        Transited Services:     -
        Package Name (NTLM only):
```

```
Process Create:
UtcTime: 2017-05-19 23:46:58.871
ProcessGuid: {3261c166-83f2-591f-0000-0010a5293602}
ProcessId: 1580
Image: C:\Windows\mimikatz.exe
CommandLine: "mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit
CurrentDirectory: C:\Windows\system32\
User: TEST\dadmin2
LogonGuid: {3261c166-83f1-591f-0000-0020d80f3602}
LogonId: 0x2360fd8
TerminalSessionId: 0
IntegrityLevel: High
Hashes: MD5=6F4748F59041725D778468BF7C15B06B
ParentProcessGuid: {3261c166-83f2-591f-0000-00104a123602}
ParentProcessId: 3168
ParentImage: C:\Windows\PSEXESVC.exe
ParentCommandLine: C:\Windows\PSEXESVC.exe
```

Hunting: search for executions in network logon sessions (WinRM, WMI, PsExec, Powershell Remoting, MMC20 COM)



Execution in network logon session

```
index="Windows" AND (source="wineventlog:microsoft-windows-sysmon/operational" OR source="wineventlog:security") AND ((EventCode=4624 Logon_Type=3 Source_Network_Address!="::1"
    Source_Network_Address!="127.0.0.1") OR (EventCode=1 ParentImage!="*\\svchost.exe")) | eval Logon_ID = mvindex(Logon_ID, 1) | eval User_SID = mvindex(Security_ID, 1) | eval
    Logon_Session = lower(coalesce(Logon_ID, LogonId)) | sort -_time,EventCode | transaction Logon_Session startswith=(EventCode=4624) mvlist=ParentImage | search eventcount>1
    | eval Parent_Process = mvindex(ParentImage, 1)
```

✓ 48 events (4/22/17 12:00:00.000 AM to 5/22/17 1:40:01.000 AM)

i	_time	Source_Network_Address	host	Security_ID	Parent_Process	Image	CommandLine	Hashes
>	5/20/17 2:46:57.000 AM	172.16.205.139	pc0002	NULL SID TEST\dadmin2	C:\Windows\PSEXESVC.exe	C:\Windows\mimikatz.exe	"mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit	MD5=6F4748F59041725D778468BF7C15B06B
>	5/15/17 12:30:53.000 AM	172.16.205.139	pc0002	NULL SID TEST\duser	C:\Windows\System32\mmc.exe	C:\Users\Public\mimikatz.exe C:\Windows\System32\cmd.exe	"C:\Windows\System32\cmd.exe" /c C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit &gt;&gt; C:\Users\Public\pc0002_mimikatz_output.txt C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit	MD5=6F4748F59041725D778468BF7C15B06B MD5=AD7B9C14083B52BC532FBA5948342B98
>	5/14/17 11:44:30.000 PM	172.16.205.139	pc0002	NULL SID TEST\dadmin	C:\Windows\PAExec-4324-PC0001.exe	C:\Windows\System32\ipconfig.exe	"ipconfig"	MD5=CABB20E171770FF64614A54C1F31C033
>	5/14/17 11:14:14.000 PM	172.16.205.139	pc0002	NULL SID TEST\dadmin	C:\Windows\PSEXESVC.exe	C:\Windows\mimikatz.exe	"mimikatz.exe" privilege::debug sekurlsa::logonpasswords exit	MD5=6F4748F59041725D778468BF7C15B06B
>	5/14/17 10:57:11.000 PM	172.16.205.139	pc0002	NULL SID TEST\dadmin2	C:\Windows\System32\wbem\WmiPrvSE.exe	C:\Users\Public\mimikatz.exe C:\Windows\System32\cmd.exe	C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit cmd /c C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit &gt;&gt; C:\Users\Public\result.txt	MD5=6F4748F59041725D778468BF7C15B06B MD5=AD7B9C14083B52BC532FBA5948342B98
>	5/14/17 10:56:07.000 PM	-	pc0002	NULL SID TEST\dadmin	C:\Windows\System32\winrshost.exe	C:\Users\Public\mimikatz.exe C:\Windows\System32\cmd.exe	C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit C:\Windows\system32\cmd.exe /C C:\Users\Public\mimikatz.exe privilege::debug sekurlsa::logonpasswords exit	MD5=6F4748F59041725D778468BF7C15B06B MD5=AD7B9C14083B52BC532FBA5948342B98
>	5/14/17 10:55:53.000	-	pc0002	NULL SID TEST\dadmin	C:\Windows\System32\wsmprovhost.exe	C:\Users\Public\mimikatz.exe C:\Windows\System32\cmd.exe	"C:\Windows\system32\cmd.exe" /c C:\Users\Public\mimikatz.exe	MD5=6F4748F59041725D778468BF7C15B06B MD5=AD7B9C14083B52BC532FBA5948342B98

Final Thoughts

- Threat Hunting - the only effective way to counter customized threats
- Threat Hunting - ‘must have’ process of security operations
- Threat Hunting - can’t be fully automated
- Threat Hunting - never-ending self-improving closed cycle via IR/DF/MA
- Threat Hunting needs data & human-machine analysis
- Threat Hunting can be done by yourself!

References

- https://www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785
- https://blog.rootshell.be/2014/02/10/tracking-processesmalwares-using-ossec/
- http://santi-bassett.blogspot.co.id/2014/09/osseccon-2014-malware-detection-with.html
- https://www.slideshare.net/votadlos/hunting-lateral-movement-in-windows-infrastructure
- https://sqrrl.com/media/Your-Practical-Guide-to-Threat-Hunting.pdf
- https://zachgrace.com/public/presentations/DerbyCon_2016_ZG_BG.pdf
- http://sqrrl.com/media/Framework-for-Threat-Hunting-Whitepaper.pdf

Thank You

Indonesia
Honeynet
Project

Deception Technology | Malware | Data Mining | Cyber Crime | Tools

@IDHoneynet

Indonesia Honeynet Project

groups.google.com/group/id-honeynet