



Once Upon a Login

How Logon Sessions Help Defenders See the Bigger Picture

About Me (@jsecurity101)

Consultant @SpecterOps/Defensive Security Researcher

- Detection, Threat Hunting, Compromise Assessments
- Windows Internals, All Things Data, Reverse Engineering
- Open-Source Author/Contributor
 - Atomic Test Harnesses
 - MSRPC-To-ATT&CK
 - Windows APIs To Sysmon-Events

Formerly Sr. Threat Researcher @RedCanary

Host of the Detection: Challenging Paradigms Podcast



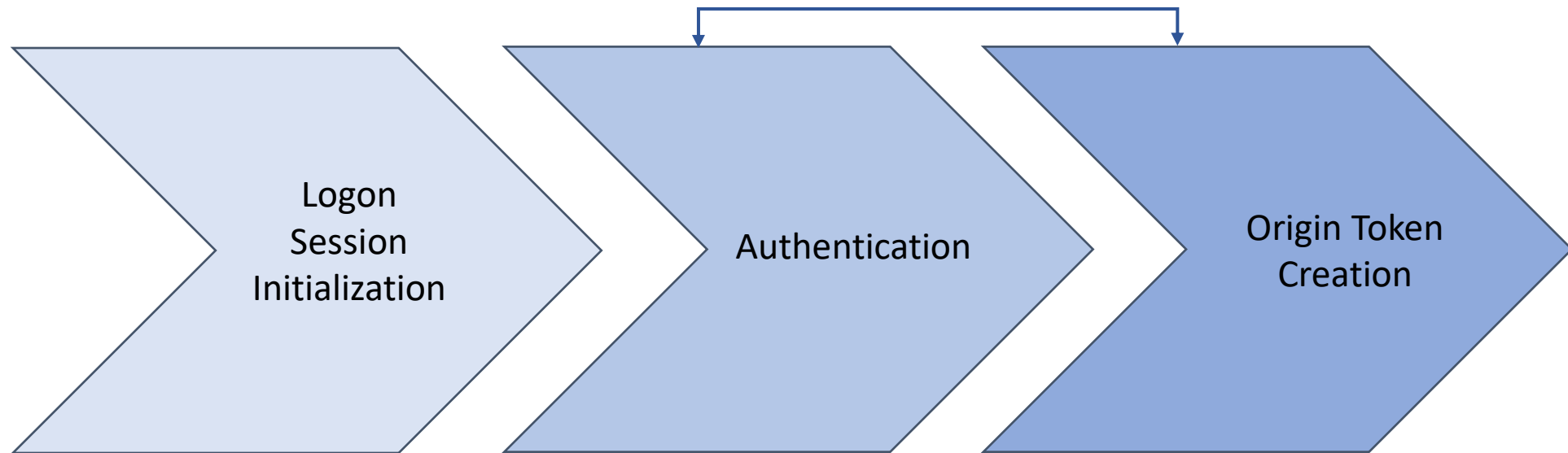
Overview

- The “Why”?
- What are logon sessions?
- Defensive Capabilities
- Available Telemetry
- Test-Cases
- PowerShell Script Drop

The “Why”

- Majority of detection and investigation strategies are heavily process centric
- This leads to A LOT of analysis for the analyst
- Potential “lost” activity
- TIME CONSUMING

Logon Sessions



Logon Sessions

- Session that is created upon a user's successful logon
- Terminates when the user is logged off
- Referenced via a LogonId value
 - LowPart of LUID structure
- If the user that logs in has High IL privileges (administrative privileges) 2 logon sessions are generated. Known as a split token/linked token.
 - 1 for Medium IL session
 - 1 for High IL session

Split Token Example

The image shows a Windows Event Viewer window on the left and two Windows PowerShell windows on the right. The Event Viewer window displays Event 4624, 'An account was successfully logged on.' The 'Details' tab is selected, showing logon information for a user named 'Admin' from the 'WINDOWS-DEV' domain. The 'Logon ID' is 0xC81BE and the 'Linked Logon ID' is 0xC8192. The 'Logon GUID' is {00000000-0000-0000-0000-000000000000}. The PowerShell windows show the execution of the `Get-NtToken` command for the process ID of the user. The first PowerShell window shows the token for the user, with the LUID 00000000-000C81BE. The second PowerShell window shows the token for the administrator, with the LUID 00000000-000C8192. Red lines connect the 'Logon ID' and 'Linked Logon ID' from the Event Viewer to the LUIDs in the PowerShell windows, illustrating the split token concept.

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: SYSTEM
- Account Name: WINDOWS-DEV\$
- Account Domain: WORKGROUP
- Logon ID: 0x3E7

Logon Information:

- Logon Type: 10
- Restricted Admin Mode: No
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: WINDOWS-DEV\Admin
- Account Name: Admin
- Account Domain: WINDOWS-DEV
- Logon ID: 0xC81BE
- Linked Logon ID: 0xC8192
- Network Account Name: -
- Network Account Domain: -
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Windows PowerShell

```
PS C:\Users\Admin> $Token = Get-NtToken -ProcessId $PID
PS C:\Users\Admin> $Token.IntegrityLevel
Medium
PS C:\Users\Admin> $Token.AuthenticationId

LUID
----
00000000-000C81BE

PS C:\Users\Admin>
```

Administrator: Windows PowerShell

```
PS C:\Users\Admin> $AdminToken = Get-NtToken -ProcessId $PID
PS C:\Users\Admin> $AdminToken.IntegrityLevel
High
PS C:\Users\Admin> $AdminToken.AuthenticationId

LUID
----
00000000-000C8192
```

Access Tokens

- Securable objects that serve to identify the security context of processes/threads
- Contain information—
 - User SID
 - Group Memberships
 - Privileges
 - Logon ID/Logon Session
- Represented in the kernel via TOKEN structure
- Generated after authentication
 - 1 token per logon session

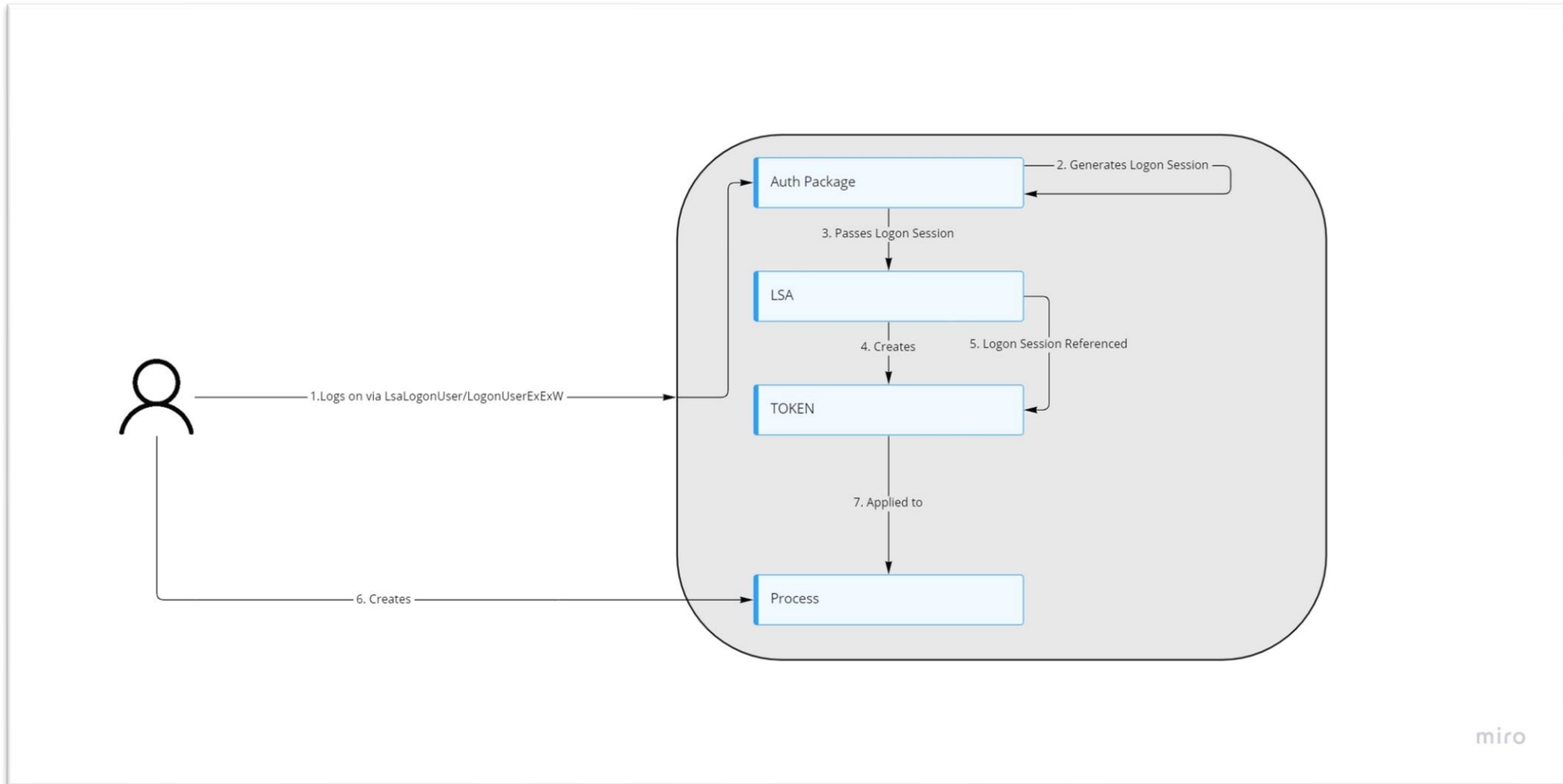
Logon Sessions in Token Structure

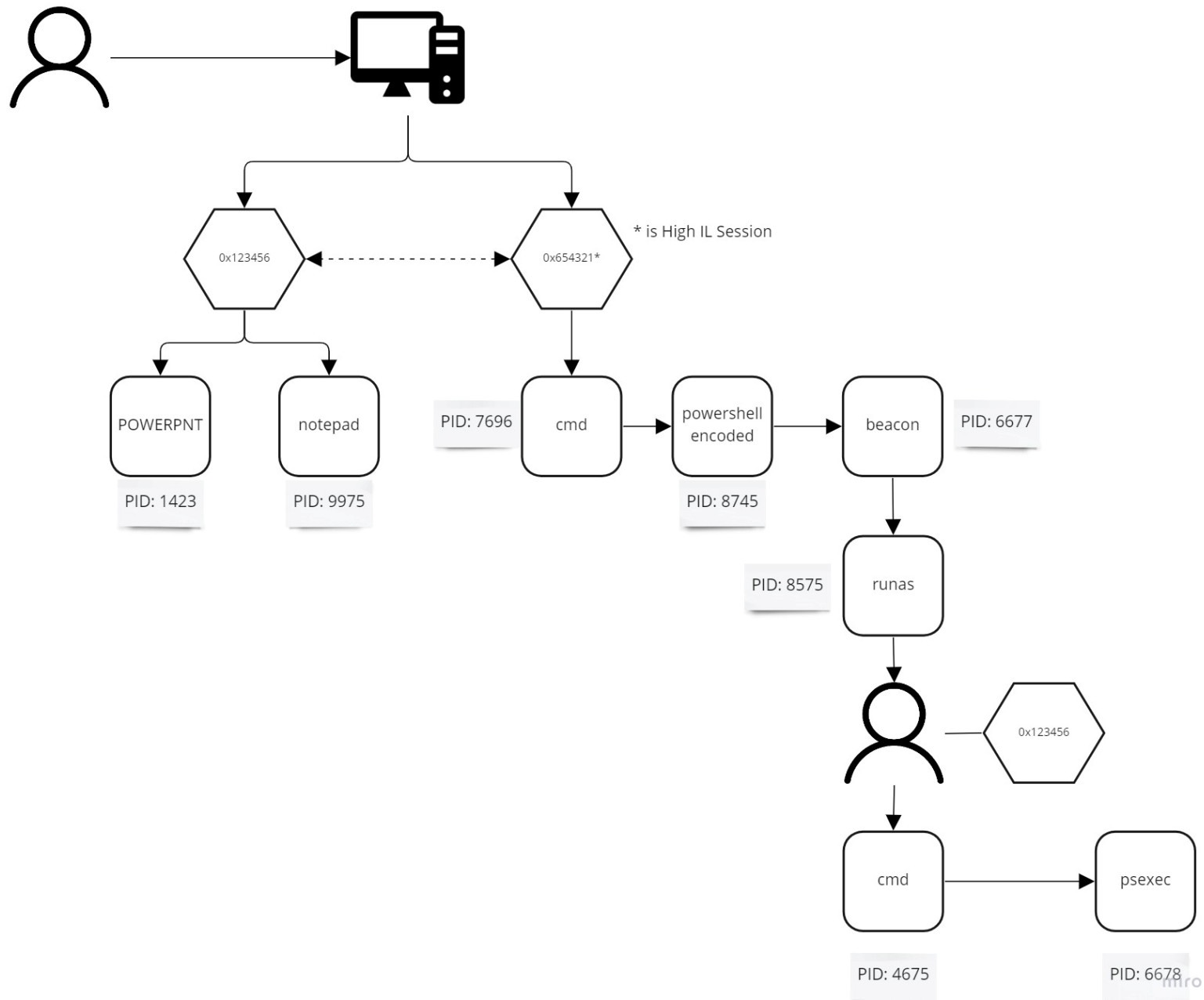
```
0: kd> dt nt! _TOKEN
+0x000 TokenSource      : _TOKEN_SOURCE
+0x010 TokenId          : _LUID
+0x018 AuthenticationId : _LUID
+0x020 ParentTokenId    : _LUID
+0x028 ExpirationTime   : _LARGE_INTEGER
+0x030 TokenLock        : Ptr64 _ERESOURCE
+0x038 ModifiedId       : _LUID
+0x040 Privileges       : _SEP_TOKEN_PRIVILEGES
+0x058 AuditPolicy      : _SEP_AUDIT_POLICY
+0x078 SessionId        : UInt4B
+0x07c UserAndGroupCount : UInt4B
+0x080 RestrictedSidCount : UInt4B
+0x084 VariableLength   : UInt4B
+0x088 DynamicChanged   : UInt4B
+0x08c DynamicAvailable : UInt4B
+0x090 DefaultOwnerIndex : UInt4B
+0x098 UserAndGroups    : Ptr64 _SID_AND_ATTRIBUTES
+0x0a0 RestrictedSids    : Ptr64 _SID_AND_ATTRIBUTES
+0x0a8 PrimaryGroup     : Ptr64 Void
+0x0b0 DynamicPart      : Ptr64 UInt4B
+0x0b8 DefaultDacl      : Ptr64 _ACL
+0x0c0 TokenType        : _TOKEN_TYPE
+0x0c4 ImpersonationLevel : _SECURITY_IMPERSONATION_LEVEL
+0x0c8 TokenFlags       : UInt4B
+0x0cc TokenInUse       : UChar
+0x0d0 IntegrityLevelIndex : UInt4B
+0x0d4 MandatoryPolicy   : UInt4B
+0x0d8 LogonSession      : Ptr64 _SEP_LOGON_SESSION_REFERENCES
+0x0e0 OriginatingLogonSession : _LUID
+0x0e8 SidHash           : _SID_AND_ATTRIBUTES_HASH
+0x0f8 RestrictedSidHash : _SID_AND_ATTRIBUTES_HASH
+0x308 pSecurityAttributes : Ptr64 _AUTHZBASEP_SECURITY_ATTRIBUTES_INFORMATION
+0x310 Package           : Ptr64 Void
+0x318 Capabilities      : Ptr64 _SID_AND_ATTRIBUTES
+0x320 CapabilityCount    : UInt4B
+0x328 CapabilitiesHash  : _SID_AND_ATTRIBUTES_HASH
+0x438 LowboxNumberEntry : Ptr64 _SEP_LOWBOX_NUMBER_ENTRY
+0x440 LowboxHandlesEntry : Ptr64 _SEP_CACHED_HANDLES_ENTRY
+0x448 pClaimAttributes   : Ptr64 _AUTHZBASEP_CLAIM_ATTRIBUTES_COLLECTION
+0x450 TrustLevelSid      : Ptr64 Void
+0x458 TrustLinkedToken   : Ptr64 _TOKEN
+0x460 IntegrityLevelSidValue : Ptr64 Void
+0x468 TokenSidValues     : Ptr64 _SEP_SID_VALUES_BLOCK
+0x470 IndexEntry         : Ptr64 _SEP_LUID_TO_INDEX_MAP_ENTRY
+0x478 DiagnosticInfo    : Ptr64 _SEP_TOKEN_DIAG_TRACK_ENTRY
+0x480 BnoIsolationHandlesEntry : Ptr64 _SEP_CACHED_HANDLES_ENTRY
+0x488 SessionObject     : Ptr64 Void
+0x490 VariablePart      : UInt8B
```

Diagram illustrating the structure of a Token, specifically highlighting the Logon Session fields:

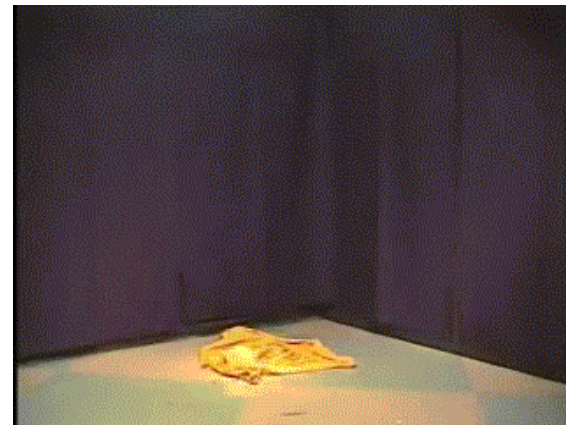
- AuthenticationId** (0x018) is a **_LUID**.
- LogonSession** (0x0d8) is a **Ptr64 _SEP_LOGON_SESSION_REFERENCES**.
- OriginatingLogonSession** (0x0e0) is a **_LUID**.

Logon Session Generation Process





Defensive Capabilities



- Detections
 - Performing JOINS on actions performed in the same logon session
- Investigation
 - More scoped approach
 - Alert goes off (LogonID is exposed)
 - LogonID query to pull all actions performed with that logon session
 - Investigate

Note: There are some gaps within some vendors on which logs expose LogonId fields*

Available Telemetry Today

- Window Security Events
 - High Volume
- Sysmon
 - Only ProcessCreation events
- Microsoft Defender for Endpoint
 - 48(+) different ActionTypes contain LogonId data
- Other EDR vendors

Microsoft Defender for Endpoint

<input type="checkbox"/>	DeviceLogonEvents	LogonSuccess
<input type="checkbox"/>	DeviceProcessEvents	ProcessCreated
<input type="checkbox"/>	DeviceEvents	ProcessPrimaryTokenModified
<input type="checkbox"/>	DeviceEvents	NtAllocateVirtualMemoryRemoteApiCall
<input type="checkbox"/>	DeviceEvents	DpapiAccessed
<input type="checkbox"/>	DeviceEvents	NamedPipeEvent
<input type="checkbox"/>	DeviceEvents	NtProtectVirtualMemoryApiCall
<input type="checkbox"/>	DeviceEvents	ScheduledTaskUpdated
<input type="checkbox"/>	DeviceEvents	LdapSearch
<input type="checkbox"/>	DeviceEvents	ReadProcessMemoryApiCall
<input type="checkbox"/>	DeviceEvents	GetClipboardData
<input type="checkbox"/>	DeviceEvents	BrowserLaunchedToOpenUrl
<input type="checkbox"/>	DeviceEvents	DriverLoad
<input type="checkbox"/>	DeviceEvents	OpenProcessApiCall
<input type="checkbox"/>	DeviceEvents	PnpDeviceConnected
<input type="checkbox"/>	DeviceEvents	ServiceInstalled
<input type="checkbox"/>	DeviceEvents	CreateRemoteThreadApiCall
<input type="checkbox"/>	DeviceEvents	ScheduledTaskDeleted
<input type="checkbox"/>	DeviceEvents	ScheduledTaskCreated
<input type="checkbox"/>	DeviceEvents	QueueUserApcRemoteApiCall

<input type="checkbox"/>	DeviceEvents	NtAllocateVirtualMemoryApiCall
<input type="checkbox"/>	DeviceEvents	AntivirusScanCompleted
<input type="checkbox"/>	DeviceEvents	AppControlCodeIntegritySigningInformation
<input type="checkbox"/>	DeviceEvents	UserAccountModified
<input type="checkbox"/>	DeviceEvents	PowerShellCommand
<input type="checkbox"/>	DeviceEvents	ShellLinkCreateFileEvent
<input type="checkbox"/>	DeviceEvents	FirewallInboundConnectionBlocked
<input type="checkbox"/>	DeviceEvents	FirewallOutboundConnectionBlocked
<input type="checkbox"/>	DeviceEvents	ExploitGuardWin32SystemCallBlocked
<input type="checkbox"/>	DeviceEvents	PnpDeviceAllowed
<input type="checkbox"/>	DeviceEvents	WriteToLsassProcessMemory
<input type="checkbox"/>	DeviceEvents	SetThreadContextRemoteApiCall
<input type="checkbox"/>	DeviceEvents	DnsQueryResponse
<input type="checkbox"/>	DeviceEvents	ScreenshotTaken
<input type="checkbox"/>	DeviceEvents	ExploitGuardChildProcessBlocked
<input type="checkbox"/>	DeviceEvents	ExploitGuardChildProcessAudited

<input type="checkbox"/>	DeviceEvents	SensitiveFileRead
<input type="checkbox"/>	DeviceEvents	AppControlCodeIntegrityDriverRevoked
<input type="checkbox"/>	DeviceEvents	AppControlCodeIntegrityPolicyBlocked
<input type="checkbox"/>	DeviceEvents	SmartScreenAppWarning
<input type="checkbox"/>	DeviceEvents	AntivirusScanCancelled
<input type="checkbox"/>	DeviceEvents	ExploitGuardAcgEnforced
<input type="checkbox"/>	DeviceEvents	RemoteDesktopConnection
<input type="checkbox"/>	DeviceEvents	ControlFlowGuardViolation

MDE NewCredential Limitation

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: MARVEL\panther
- Account Name: panther
- Account Domain: MARVEL
- Logon ID: 0xDAE8F4

Logon Information:

- Logon Type: 9
- Restricted Admin Mode: -
- Virtual Account: No
- Elevated Token: No

Impersonation Level: Impersonation

New Logon:

- Security ID: MARVEL\panther
- Account Name: panther
- Account Domain: MARVEL
- Logon ID: 0xFCDA48
- Linked Logon ID: 0x0
- Network Account Name: thor
- Network Account Domain: marvel
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x14cc
- Process Name: C:\Windows\System32\svchost.exe

Network Information:

- Workstation Name: -
- Source Network Address: ::1
- Source Port: 0

Detailed Authentication Information:

- Logon Process: seclogon
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

```
not compatible with  
runas /netonly /us  
or marvel\thor:
```

```
marvel\thor)
```

```
Version 10.0.171  
Corporation. All
```

```
2> _
```

ActionType	:	InitiatingProcessAccountDomain	:
LogonSuccess	:	nt authority	:
LogonType	:	InitiatingProcessAccountName	:
NewCredentials	:	system	:
AccountDomain	:	InitiatingProcessAccountSid	:
marvel	:	S-1-5-18	:
AccountName	:	InitiatingProcessTokenElevation	:
panther	:	None	:
AccountSid	:	InitiatingProcessSHA1	:
S-1-5-21-2689819607-2865155720-1323879450-1107	:	10750075415d5d806e52f10ef5846aa9caa428c0	:
Protocol	:	InitiatingProcessMD5	:
Negotiate	:	38b2442ac21c90615ab39a52ada3576f	:
LogonId	:	InitiatingProcessFileName	:
16570955	:	svchost.exe	:
RemotelP	:	InitiatingProcessId	:
(00) :1	:	5324	:
	:	InitiatingProcessCommandLine	:
	:	svchost.exe -k netsvcs -p -s seclogon	:

Practical Examples (Credential Dumping)

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 search in (DeviceProcessEvents, DeviceEvents)
2   LogonId in ("3843709") or InitiatingProcessLogonId in ("3843709")
3   | extend PipeName= extractjson("$.PipeName", AdditionalFields)
4   | extend ServiceName= extractjson("$.ServiceName", AdditionalFields)
5   | extend ServiceType= extractjson("$.ServiceType", AdditionalFields)
6   | extend DesiredAccess = extractjson("$.DesiredAccess", AdditionalFields)
7   | summarize by Timestamp, DeviceName, ActionType, InitiatingProcessLogonId, LogonId, FileName, ProcessCommandLine, ServiceName, ServiceType, DesiredAccess, PipeName
```

Getting Started Results

Export

8 items

Search

0:0.47

<input type="checkbox"/>	Timestamp	DeviceName	ActionType	InitiatingProcessLogonId	LogonId	FileName	ProcessCommandLine	ServiceName	ServiceType	DesiredAccess
<input type="checkbox"/>	Sep 26, 2022 1:09:29 AM	asgard-wrkstn.mar...	CreateRemoteThreadApi...		3843709	dllhost.exe	dllhost.exe			
<input type="checkbox"/>	Sep 26, 2022 1:09:30 AM	asgard-wrkstn.mar...	ProcessPrimaryTokenMo...	3843709						
<input type="checkbox"/>	Sep 26, 2022 1:10:16 AM	asgard-wrkstn.mar...	CreateRemoteThreadApi...		3843709	dllhost.exe	dllhost.exe			
<input type="checkbox"/>	Sep 26, 2022 1:10:16 AM	asgard-wrkstn.mar...	ProcessPrimaryTokenMo...	3843709						
<input type="checkbox"/>	Sep 26, 2022 1:10:33 AM	asgard-wrkstn.mar...	CreateRemoteThreadApi...		3843709	dllhost.exe	dllhost.exe			
<input type="checkbox"/>	Sep 26, 2022 1:10:33 AM	asgard-wrkstn.mar...	ProcessPrimaryTokenMo...	3843709						
<input type="checkbox"/>	Sep 26, 2022 1:10:34 AM	asgard-wrkstn.mar...	OpenProcessApiCall	3843709	999	lsass.exe	lsass.exe			4112
<input type="checkbox"/>	Sep 26, 2022 1:21:27 AM	asgard-wrkstn.mar...	ServiceInstalled	3843709		cmd.exe		BeaconService	16	

Practical Examples (Privilege Escalation)

A process was injected with potentially malicious code

ALERT STORY

1:49:02 PM

1:49:03 PM

1:49:03 PM

1:49:14 PM

[12192] cmd.exe /C whoami /all

[13688] whoami.exe whoami /all

Process id 13688

Command line whoami /all

Image file path C:\Windows\SysWOW64\whoami.exe

Image file SHA1 08ca5731b3b23557d5052c2b05d305de06a17d3a

Image file creation time Apr 11, 2018 6:35:00 PM

Execution details Token elevation: Full, Integrity level: High

Mitre techniques T1033: System Owner/User Discovery, T1087: Account Discovery, T1069: Permission Groups Discovery, T1087.001: Local Account, T1087.002: Domain Account

Signer Microsoft Windows

Issuer Microsoft Windows Production PCA 2011

VirusTotal detection ratio 0/0

User MARVEL\panther

Sid S-1-5-21-2689819607-2865155720-1323879450-1107

Log on id 14343824

PE metadata whoami.exe

Suspicious System Owner/User Discovery Low Detected New

cmd.exe process performed System Owner/User Discovery by invoking whoami.exe

Suspicious System Owner/User Discovery Low Detected New

[10192] dllhost.exe

A process was injected with potentially malicious code Medium Detected New

CreateRemoteThread Medium Detected New

Practical Examples (Privilege Escalation)

A process was injected with potentially malicious code

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

Don't want to see it

```
1 search in (DeviceProcessEvents, DeviceEvents, DeviceLogonEvents)
2   LogonId in ("14343824") or InitiatingProcessLogonId in ("14343824")
3   | extend PipeName= extractjson("$.PipeName", AdditionalFields)
4   | extend ServiceName= extractjson("$.ServiceName", AdditionalFields)
5   | extend ServiceType= extractjson("$.ServiceType", AdditionalFields)
6   | extend TaskName = extractjson("$.TaskName", AdditionalFields)
7   | extend DesiredAccess = extractjson("$.DesiredAccess", AdditionalFields)
8   | summarize by Timestamp, DeviceName, ActionType, AccountName, LogonType, Protocol, TaskName, InitiatingProcessLogonId, LogonId, FileName, ProcessCommandLine, DesiredAccess, PipeName
```

Getting Started **Results**

Export

6 items

Search

0:0.31

Low

Chart Type

Custom

<input type="checkbox"/>	Timestamp	DeviceName	ActionType	AccountName	LogonType	Protocol	TaskName	InitiatingProcessLogonId	LogonId	FileName	ProcessCommandLine	DesiredAccess
<input type="checkbox"/>	Sep 26, 2022 12:56:50 PM	asgard-wrkstn.mar...	LogonSuccess	panther	RemoteInteractive	Negotiate			14343824			
<input type="checkbox"/>	Sep 26, 2022 1:53:53 PM	asgard-wrkstn.mar...	ScheduledTaskCreated				\SANS-EXAMPLE	14343824				
<input type="checkbox"/>	Sep 26, 2022 1:47:35 PM	asgard-wrkstn.mar...	ProcessPrimaryTokenMo...					14343824				
<input type="checkbox"/>	Sep 26, 2022 1:49:14 PM	asgard-wrkstn.mar...	CreateRemoteThreadApi...	panther					14343824	dllhost.exe	dllhost.exe	
<input type="checkbox"/>	Sep 26, 2022 1:49:34 PM	asgard-wrkstn.mar...	CreateRemoteThreadApi...	panther					14343824	dllhost.exe	dllhost.exe	
<input type="checkbox"/>	Sep 26, 2022 1:50:17 PM	asgard-wrkstn.mar...	CreateRemoteThreadApi...	panther					14343824	dllhost.exe	dllhost.exe	

Practical Examples (Lateral Movement)

Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)

9/25/2022 10:37:34 PM [692] services.exe

10:37:37 PM [948] svchost.exe -k DcomLaunch -p

9/26/2022 1:59:08 PM [5332] wsmprovhost.exe -Embedding

1:59:09 PM wsmprovhost.exe executed a script

1:59:10 PM wsmprovhost.exe executed a script

1:59:11 PM wsmprovhost.exe executed a script

1:59:12 PM wsmprovhost.exe executed a script

1:59:12 PM wsmprovhost.exe executed a script

1:59:12 PM wsmprovhost.exe executed a script

1:59:12 PM [5280] powershell.exe -Version 5.1 -s -NoLogo -NoProfile

WinRM

High Detected New

Process id 5280

Command line "powershell.exe" -Version 5.1 -s -NoLogo -NoProfile

Image file path C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Image file SHA1 e6bcade7272afdf52d963d0626a1dd4d26b39a7e

Image file creation time Sep 15, 2018 2:14:15 AM

Execution details Token elevation: Default, Integrity level: High

Signer Microsoft Windows

Issuer Microsoft Windows Production PCA 2011

VirusTotal detection ratio 0/0

User MARVEL\thor

Sid S-1-5-21-2689819607-2865155720-1323879450-1104

Log on id 26162239

PE metadata powershell.exe

Practical Examples (Lateral Movement)

Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)

Advanced Hunting

Help resources Schema reference

New query | New query | New query | New query | NewCredentials Logon | New query | LogonSession Timeline | Service Creation | OpenProcess (LSASS) | New query | Create new

> Run query Save Share link Last 7 days

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC. Don't worry

```
1 search in (DeviceProcessEvents, DeviceEvents, DeviceLogonEvents)
2   LogonId in ("26162239") or InitiatingProcessLogonId in ("26162239")
3   | extend PipeName= extractjson("$.PipeName", AdditionalFields)
4   | extend ServiceName= extractjson("$.ServiceName", AdditionalFields)
5   | extend ServiceType= extractjson("$.ServiceType", AdditionalFields)
6   | extend DesiredAccess = extractjson("$.DesiredAccess", AdditionalFields)
7   | summarize by Timestamp, DeviceName, ActionType, AccountName, LogonType, InitiatingProcessLogonId, LogonId, FileName, ProcessCommandLine, ServiceName, DesiredAccess, PipeName
```

Getting Started Results

Export 21 items Search 0:0.109 Low Chart Type

Timestamp	DeviceName	ActionType	AccountName	LogonType	InitiatingProcessLogonId	LogonId	FileName	ProcessCommandLine	ServiceName
<input type="checkbox"/> Sep 26, 2022 1:59:08 PM	earth-dc.marvel.io...	LogonSuccess	thor	Network		26162239			
<input type="checkbox"/> Sep 26, 2022 1:59:08 PM	earth-dc.marvel.io...	ProcessCreated	thor		999	26162239	wsmprovhost.exe	wsmprovhost.exe -Embedding	
<input type="checkbox"/> Sep 26, 2022 1:59:12 PM	earth-dc.marvel.io...	ProcessCreated	thor		26162239	26162239	powershell.exe	"powershell.exe" -Version 5.1 -s -NoLogo -NoProfile	
<input type="checkbox"/> Sep 26, 2022 1:59:13 PM	earth-dc.marvel.io...	ProcessCreated	thor		26162239	26162239	conhost.exe	conhost.exe 0xffffffff -ForceV1	

Practical Examples (Lateral Movement)

Ongoing hands-on-keyboard attacker activity detected (Cobalt Strike)

[Run query](#) [Save](#) [Share link](#) Last 24 hours

Query

Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceNetworkEvents
2 | where LocalPort == "49813" and LocalIP == "192.168.1.221" and ActionType == "ConnectionSuccess"
3 | project-rename ProcessId = InitiatingProcessId
4 | join ( DeviceProcessEvents ) on ProcessId
5 | project DeviceName1, InitiatingProcessAccountName1, FileName, ProcessCommandLine, ProcessId1
```

Getting Started

Results

[Export](#)

2 items 0:0.16 Low [Chart Type](#)

<input type="checkbox"/>	DeviceName1	InitiatingProcessAccountNa...	FileName	ProcessCommandLine	ProcessId1
<input type="checkbox"/>	asgard-wrkstn.marvel.io...	thor	powershell.exe	powershell -nop -exec bypass -EncodedCommand SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuA...	3448
<input type="checkbox"/>	asgard-wrkstn.marvel.io...	thor	powershell.exe	powershell -nop -exec bypass -EncodedCommand SQBFAGfAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBjAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuA...	3448

Practical Examples (Lateral Movement)

Suspicious process executed PowerShell command

The screenshot displays the Windows Task Manager interface, showing a process tree. The following table summarizes the processes shown:

Process ID	Process Name	Command Line	Status
[5324]	svchost.exe	-k netsvcs -p -s seclogon	Running
[13760]	dllhost.exe		Running
[3800]	dllhost.exe		Suspicious process launched using dllhost.exe
[11584]	cmd.exe	/C dir \\EARTH-DC\CS	Suspicious process launched using dllhost.exe
[3448]	powershell.exe	powershell -nop -exec bypass -EncodedCommand SQBFaFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABoAGUAdAAuAFcAZQBjAGMAb...	Running

The powershell.exe process details are expanded, showing the following information:

- Process id: 3448
- Command line: powershell -nop -exec bypass -EncodedCommand SQBFaFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABoAGUAdAAuAFcAZQBjAGMAb...
- Command line (decoded): IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:7174/')
- Image file path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
- Image file SHA1: 1b3b40fbc889fd4c645cc12c85d0805ac36ba254
- Image file creation time: Apr 11, 2018 6:35:26 PM
- Execution details: Token elevation: Limited, Integrity level: Medium
- Signer: Microsoft Windows
- Issuer: Microsoft Windows Production PCA 2011
- VirusTotal detection ratio: 0/0
- User: MARVEL\thor
- Sid: S-1-5-21-2689819607-2865155720-1323879450-1104
- Log on id: 20344488
- PE metadata: powershell.exe

Practical Examples (Lateral Movement)

Detection

Detection rule



i Query results are presented in your local time zone as per settings. Kusto filters, however, work in UTC.

```
1 DeviceLogonEvents
2 | where LogonType == "Network"
3 | join ( DeviceProcessEvents) on LogonId
4 | summarize count() by DeviceName, AccountName, LogonId
```

Getting Started

Results

↓ Export

<input type="checkbox"/>	DeviceName	AccountName	LogonId	count_
<input type="checkbox"/>	 asgard-wrkstn.mar...	testuser		1321
<input type="checkbox"/>	 earth-dc.marvel.lo...	thor	26162239	3

Investigation Script

```
PS C:\> Get-LogonSessionProcesses -Id
```

```
Title           : Displaying Pro
ProcessName      : dllhost.exe
SessionId        : 6
ProcessId        : 13760
ProcessTokenUserName : MARVEL\thor
ProcessTokenSid   : S-1-5-21-26898
ProcessLogonSid   : 1366ea8
ProcessBuddyLogonSid : 1366e65
ProcessTokenType : TokenPrimary
ProcessTokenId    : 20345817
TokenIntegrityLevel : MEDIUM_MANDATO
NetworkEvents     : @{SourceAddress
                  Connection att
```

```
ProcessId        : 9528
ProcessTokenUserName : Win11-Dev\TestUser
ProcessTokenSid   : S-1-5-21-2163304194-2372255453-3992060245-1001
ProcessLogonSid   : 1d57643
ProcessBuddyLogonSid : 1d576a2
ProcessTokenType : TokenPrimary
ProcessTokenId    : 245855549
TokenIntegrityLevel : HIGH_MANDATORY_LEVEL
NetworkEvents     : {}
```

```
Title           : Displaying Process/Primary Information
ProcessName      : conhost.exe
SessionId        : 2
ProcessId        : 12304
ProcessTokenUserName : Win11-Dev\TestUser
ProcessTokenSid   : S-1-5-21-2163304194-2372255453-3992060245-1001
ProcessLogonSid   : 1d57643
ProcessBuddyLogonSid : 1d576a2
ProcessTokenType : TokenPrimary
ProcessTokenId    : 245855761
TokenIntegrityLevel : HIGH_MANDATORY_LEVEL
NetworkEvents     : {}
```

```
PS C:\> Get-LogonSessionProcesses -Id
```

```
Title           : Displaying Pro
ProcessName      : beacon.exe
SessionId        : 6
ProcessId        : 6508
ProcessTokenUserName : MARVEL\panther
ProcessTokenSid   : S-1-5-21-26898
ProcessLogonSid   : dade90
ProcessBuddyLogonSid : dae8f4
ProcessTokenType : TokenPrimary
ProcessTokenId    : 19906273
TokenIntegrityLevel : HIGH_MANDATORY
NetworkEvents     : @{SourceAddress
                  Connection att
```

```
Title           : Displaying Process/Primary Information
ProcessName      : Notepad.exe
SessionId        : 2
ProcessId        : 17248
ProcessTokenUserName : Win11-Dev\TestUser
ProcessTokenSid   : S-1-5-21-2163304194-2372255453-3992060245-1001
ProcessLogonSid   : 1d57643
ProcessBuddyLogonSid : 1d576a2
ProcessTokenType : TokenPrimary
ProcessTokenId    : 245991140
TokenIntegrityLevel : HIGH_MANDATORY_LEVEL
NetworkEvents     : {}
```

```
Title           : Displaying Process/Primary Information
ProcessName      : callback.exe
SessionId        : 2
ProcessId        : 10396
ProcessTokenUserName : Win11-Dev\TestUser
ProcessTokenSid   : S-1-5-21-2163304194-2372255453-3992060245-1001
ProcessLogonSid   : 1d57643
ProcessBuddyLogonSid : 1d576a2
ProcessTokenType : TokenPrimary
ProcessTokenId    : 246886753
TokenIntegrityLevel : HIGH_MANDATORY_LEVEL
NetworkEvents     : @{SourceAddress=192.168.1.205; DestinationAddress=192.168.1.132; PID=10396; Message=TCPv4:
                  Connection attempted between 192.168.1.205:52045 and 192.168.1.132:80.}
```


Conclusion

- Goal is to provide an initial targeted approach
- Logon Session Centric Analysis is not meant to replace previous analysis methodologies
- Other processes will still need to be used due to limitations in today's telemetry
- Really powerful with multiple data sources – Security Events + EDR!!

Resources

- Windows Internals Book Part 1, Chapter 7
- Microsoft Authentication/Logon Documentations
- LogonProcesses.ps1 -
<https://gist.github.com/jsecurity101/12e75415b35a5d220d13674e9ed43373>



Q/A