SYSMON + ATT&CK
to feed your SIEM

This presentation is provided "as is" without any express of implied warranty.

This presentation is for educational purposes only.

Before doing anything you should consult your corporate InfoSec authority.

Whoami

- Raphael Francoeur
- Threat Detection Engineer

@ Canada Life
- SANS: GCIA,GCWN,GCDA
- 3 little ninjas

AGENDA

01

What is it ?

02

Why you should use it ?

03

How we use it ?

04

Q & A

“The path that leads to what we truly desire is long and difficult, but only by following that path do we achieve our goal.”

- Master Splinter

01

What is it ?

Maybe you know,
maybe you don’t,
but lets make sure.

IF SOC’s were SANDWICHES

WITHOUT Sysmon

WITH Sysmon

SYSMON

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

ION-STORM / SYSMON-CONFIG

https://github.com/ion-storm/sysmon-config

FORK of SwiftOnSecurity/sysmon-config

This is the install plan

```
PS C:\temp> sysmon -i "sysmonconfig.xml"
```

```
start-process wevtutil.exe -ArgumentList "sl Microsoft-Windows-Sysmon/Operational /ms:2147483648" -wait
```

The update plan

```
& c:\windows\sysmon.exe -c .\sysmonconfig_noFileBlocks_allDNS.xml
```

The backout plan

```
& c:\windows\sysmon.exe -u force
```

The config

```
<Sysmon schemaversion="4.90">
    <HashAlgorithms>md5,sha1,sha256,imphash</HashAlgorithms>
    <CheckRevocation/>
    <EventFiltering>
    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="RG=ProcessCreate Include Group" groupRelation="or">
        <ProcessCreate onmatch="include">
            <!--MITRE ATT&CK TACTIC: Reconnaissance-->
            <!--MITRE ATT&CK TECHNIQUE: Active Scanning-->
            <Rule name="Attack=T1595.002,Technique=Vulnerability Scanning,Tactic=Reconnaissance,DS=Process: Process Creation,Level=3,Alert=Nessus Scan Detected,Risk=100" groupRe
                <ParentCommandLine condition="contains any">TEMP\nessus_;nessus_task_list</ParentCommandLine>
                <CommandLine condition="contains any">TEMP\nessus_;nessus_task_list</CommandLine>
            </Rule>
            <Rule name="Attack=T1595.002,Technique=Vulnerability Scanning,Tactic=Reconnaissance,DS=Process: Process Creation,Level=4,Alert=Port Scan Tool Detected,Risk=100" grou
                <CommandLine condition="contains any">rcpping;tcpping;tcping;routerscan;grabff;Port-Scan;netscan;\nmap;ipscan;nacmdline.exe</CommandLine>
                <OriginalFileName condition="is any">advanced_port_scanner.exe;rcpping.exe;nc.exe;nc64.exe;netcat.exe;ncat.exe;nmap.exe;zenmap.exe;advanced_ip_scanner.exe</Origi
                <Product condition="contains any">Network Scanner;Advanced IP Scanner</Product>
            </Rule>
            <Rule name="Attack=T1087,Technique=Account Discovery,Tactic=Discovery,DS=Process: Process Creation,Level=4,Alert=ADFind.exe Discovery,Risk=100" groupRelation="or">
                <OriginalFileName condition="contains">adfind</OriginalFileName
                <Product condition="contains">adfind</Product>
                <CommandLine condition="contains any">-gcb -sc;/gcb /sc;-f (objectcategory=;/f (objectcategory=;trustdmp</CommandLine>
            </Rule>
            <!--MITRE ATT&CK TECHNIQUE: Gather Victim Host Information-->
            <!--MITRE ATT&CK TECHNIQUE: Gather Victim Identity Information-->
            <!--MITRE ATT&CK TECHNIQUE: Gather Victim Network Information-->
            <!--MITRE ATT&CK TECHNIQUE: Gather Victim Org Information-->
            <!--MITRE ATT&CK TECHNIQUE: Phishing for Information-->
            <!--MITRE ATT&CK TECHNIQUE: Search Closed Sources-->
            <!--MITRE ATT&CK TECHNIQUE: Search Open Technical Databases-->
            <!--MITRE ATT&CK TECHNIQUE: Search Open Websites/Domains-->
            <!--MITRE ATT&CK TECHNIQUE: Search Victim-Owned Websites-->

            <!--MITRE ATT&CK TACTIC: Resource Development-->
```

Alert=netsh ipv6 modification

="Attack=T1629.003

Risk=40"

Technique=Impair Defenses: Disable or Modify Tools

Tactic=Defense Evasion

Level=2

DS=Process: Process Creation

The Schema (EID 1)

```
\Sysmon64.exe" -s | out-file c:\temp\sysmon_schema.xml
```

```
<manifest schemaversion="4.83" binaryversion="17">
  <configuration>
  <events>
    <event name="SYSMONEVENT_ERROR" value="255" level="Error" template="Error report" version="3">
    <event name="SYSMONEVENT_CREATE_PROCESS" value="1" level="Informational" template="Process Create" rulename=
    "ProcessCreate" ruledefault="include" version="5">
      <data name="RuleName" inType="win:UnicodeString" outType="xs:string" />
      <data name="UtcTime" inType="win:UnicodeString" outType="xs:string" />
      <data name="ProcessGuid" inType="win:GUID" />
      <data name="ProcessId" inType="win:UInt32" outType="win:PID" />
      <data name="Image" inType="win:UnicodeString" outType="xs:string" />
      <data name="FileVersion" inType="win:UnicodeString" outType="xs:string" />
      <data name="Description" inType="win:UnicodeString" outType="xs:string" />
      <data name="Product" inType="win:UnicodeString" outType="xs:string" />
      <data name="Company" inType="win:UnicodeString" outType="xs:string" />
      <data name="OriginalFileName" inType="win:UnicodeString" outType="xs:string" />
      <data name="CommandLine" inType="win:UnicodeString" outType="xs:string" />
      <data name="CurrentDirectory" inType="win:UnicodeString" outType="xs:string" />
      <data name="User" inType="win:UnicodeString" outType="xs:string" />
      <data name="LogonGuid" inType="win:GUID" />
      <data name="LogonId" inType="win:HexInt64" />
      <data name="TerminalSessionId" inType="win:UInt32" />
      <data name="IntegrityLevel" inType="win:UnicodeString" outType="xs:string" />
      <data name="Hashes" inType="win:UnicodeString" outType="xs:string" />
      <data name="ParentProcessGuid" inType="win:GUID" />
      <data name="ParentProcessId" inType="win:UInt32" outType="win:PID" />
      <data name="ParentImage" inType="win:UnicodeString" outType="xs:string" />
      <data name="ParentCommandLine" inType="win:UnicodeString" outType="xs:string" />
      <data name="ParentUser" inType="win:UnicodeString" outType="xs:string" />
    </event>
    <event name="SYSMONEVENT_FILE_TIME" value="2" level="Informational" template="File creation time changed" rul
```

The Raw Event (EID 1)

```
- <EventData>
    <Data Name="RuleName">Attack=T1016,Technique=System Network Configuration Discovery,Tactic=Discovery,DS=Process: Process
      Creation,Level=0,Desc=ipconfig discovery,Risk=20</Data>
    <Data Name="UtcTime">2023-10-26 03:50:06.544</Data>
    <Data Name="ProcessGuid">{35db2687-e1ee-6539-a7c3-030000006d00}</Data>
    <Data Name="ProcessId">25568</Data>
    <Data Name="Image">C:\Windows\System32\ipconfig.exe</Data>
    <Data Name="FileVersion">10.0.19041.1 (WinBuild.160101.0800)</Data>
    <Data Name="Description">IP Configuration Utility</Data>
    <Data Name="Product">Microsoft® Windows® Operating System</Data>
    <Data Name="Company">Microsoft Corporation</Data>
    <Data Name="OriginalFileName">ipconfig.exe</Data>
    <Data Name="CommandLine">C:\WINDOWS\Sysnative\ipconfig.exe /flushdns</Data>
    <Data Name="CurrentDirectory">C:\WINDOWS\system32\</Data>
    <Data Name="User">NT AUTHORITY\SYSTEM</Data>
    <Data Name="LogonGuid">{35db2687-1c25-651b-e703-000000000000}</Data>
    <Data Name="LogonId">0x3e7</Data>
    <Data Name="TerminalSessionId">0</Data>
    <Data Name="IntegrityLevel">System</Data>
    <Data
      Name="Hashes">SHA1=D9BBB4E4900FF03B0486FAC32768170249DAD82D,MD5=62F170FB07FDBB79CEB7147101406EB8,SHA256=53E000F
    <Data Name="ParentProcessGuid">{35db2687-2500-651b-f301-000000006d00}</Data>
    <Data Name="ParentProcessId">10592</Data>
    <Data Name="ParentImage">C:\Program Files (x86)\Zscaler\ZSATunnel\ZSATunnel.exe</Data>
    <Data Name="ParentCommandLine">"C:\Program Files (x86)\Zscaler\ZSATunnel\ZSATunnel.exe"</Data>
    <Data Name="ParentUser">NT AUTHORITY\SYSTEM</Data>
  </EventData>
</Event>
```

02

Why you should use it ?

~~Don~~t be scared, it’s fun.

Some Why’s

Unveil the Underbelly : Sysmon is your secret weapon to unveil the mysterious inner workings of your Windows systems. * It's like X-ray vision for your computers! *
Process Ninja Skills : Sysmon logs every move processes make, from spawning to executing cryptic commands. *It's like having a play-by-play of a hacker's tactics. *
Registry Scribe : Every change in the Windows registry gets recorded. *It's like having a scribe documenting the whispers of your system's heart.*
Craft Your Rules : Customize Sysmon rules to hunt down specific behaviors or threats. *It's like having a magic wand to summon your desired security spells.*
Regulatory Sorcery : Sysmon is your magic potion to comply with security standards and regulations. Stay on the right side of the compliance wizards.
Threat Hunter's Companion : With Sysmon, you're not just a security analyst; you're a digital Sherlock Holmes, hunting for hidden cyber criminals / idiots .

OOB Mitre Coverage

Reconnaissance
10 techniques

- Active Scanning (1/3)
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- Search Closed Sources (0/2)
- Search Open Technical Databases (0/5)
- Search Open Websites/Domains (0/3)
- Search Victim-Owned Websites

Resource Development
8 techniques

- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (1/7)
- Develop Capabilities (1/4)
- Establish Accounts (0/3)
- Obtain Capabilities (0/6)
- Stage Capabilities (0/6)

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution
14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (5/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (1/3)
- Native API
- Scheduled Task/Job (2/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (1/2)
- User Execution (1/3)
- Windows Management Instrumentation

Persistence
19 techniques

- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (1/4)
- Event Triggered Execution (4/16)
- External Remote Services
- Hijack Execution Flow (1/12)
- Implant Internal Image
- Modify Authentication Process (0/8)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (2/5)
- Server Software Component (1/5)
- Traffic Signaling (0/2)
- Valid Accounts (0/4)

Privilege Escalation
13 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (0/5)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (1/4)
- Domain Policy Modification (1/2)
- Escape to Host
- Event Triggered Execution (4/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1/12)
- Process Injection (1/12)
- Scheduled Task/Job (2/5)
- Valid Accounts (0/4)

Defense Evasion
42 techniques

- Abuse Elevation Control Mechanism (1/4)
- Access Token Manipulation (1/5)
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (1/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (1/10)
- Hijack Execution Flow (1/12)
- Impair Defenses (5/10)
- Indicator Removal (1/9)
- Indirect Command Execution
- Masquerading (2/8)
- Modify Authentication Process (0/8)
- Modify Cloud Compute Infrastructure (0/4)
- Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- Obfuscated Files or Information (1/11)
- Plist File Modification
- Pre-OS Boot (0/5)
- Process Injection (1/12)

Credential Access
17 techniques

- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forge Web Credentials (0/2)
- Input Capture (1/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (2/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)
- Steal Web Session Cookie
- Unsecured Credentials (0/8)

Discovery
31 techniques

- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)
- System Information Discovery
- System Location Discovery (0/1)
- System Network Configuration Discovery

Lateral Movement
9 techniques

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (1/2)
- Remote Services (5/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection
17 techniques

- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (1/4)
- Screen Capture
- Video Capture

Command and Control
16 techniques

- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (1/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

Exfiltration
9 techniques

- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (1/3)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
13 techniques

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

03

How we use it ?

If you trigger, You get Sysmon'ed
$visibility++

The config levels

DEFCON 4 : Just Mitre

DEFCON 3 : More DNS

<DnsQuery onmatch="exclude" />

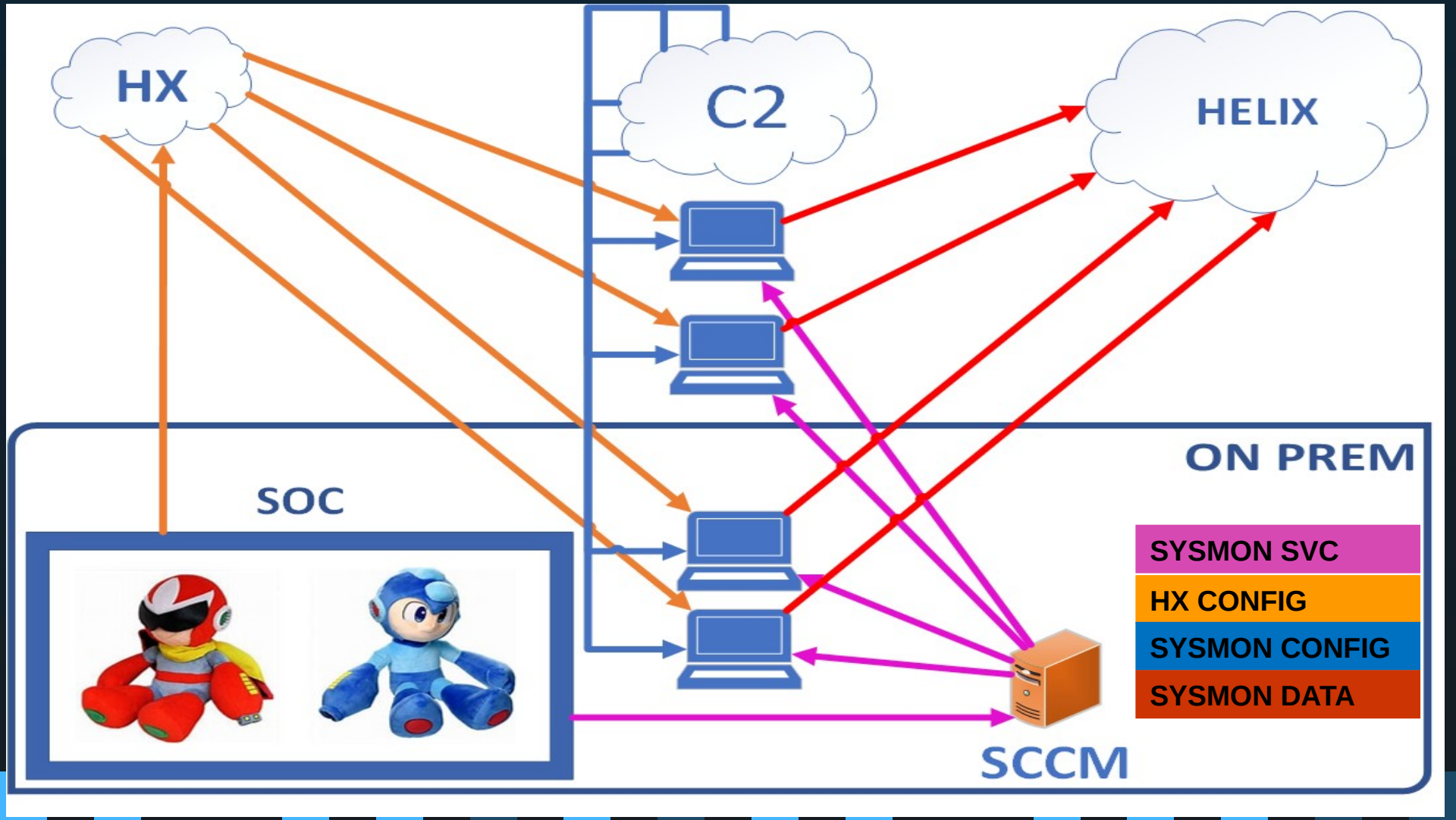
DEFCON 2 : More DNS + Process

DEFCON 1 : More DNS + Process + Clipboard Changes

(gloves are off)

The tech

Endpoint Management Solution	C2	EDR	SIEM
SCCM: Coordinates the installs report service status and config hashes Troubleshoot stragglers	Protected middle box to host Sysmon's config off-prem since **WFH** is a thing	HX equipped with EventStreamer 2.0 and ships Win logs to SIEM	Trellix HELIX


HX
C2
HELIX
ON PREM
SOC
SYSMON SVC
HX CONFIG
SYSMON CONFIG
SYSMON DATA
SCCM

Eventid	Category	Total ↓
3	network connection detected (rule: networkconnect)	2438935
11	file created (rule: filecreate)	2252616
13	registry value set (rule: registryevent)	1380796
22	dns query (rule: dnsquery)	587363
1	process create (rule: processcreate)	571903
7	image loaded (rule: imageload)	387801
10	process accessed (rule: processaccess)	97821
2	file creation time changed (rule: filecreatetime)	59571
8	createremotethread detected (rule: createremotethread)	52632
6	driver loaded (rule: driverload)	23862
15	file stream created (rule: filecreatestreamhash)	4208
255		347
25	process tampering (rule: processtampering)	277
4	sysmon service state changed	151
16	sysmon config state changed	36
17	pipe created (rule: pipeevent)	3

False Positives
ASR is a beach full of jellyfish

04

Questions and stuff

Other cool stuff

GitHub - SwiftOnSecurity/sysmon-config
Sysmon configuration file template with default high-quality event tracing

GitHub - huntandhackett/sysmon-indepth:
Understanding the operation and limitations of Sysmon's events
FileBlock Events bypass – But... you should trip something else

GitHub - olafhartong/sysmon-modular:
A repository of sysmon configuration modules

THANKS

For letting me out of the basement.