Endpoint Detection Superpowers with Sysmon + Splunk

Olaf Hartong
Specialist Leader Blue Team | Deloitte

splunk> .conf19

Who am I?

Olaf Hartong

Blue Team Specialist Leader

Currently having fun @ Deloitte

13+ years in Info Security
Consulted at banks, educational institutions and governmental organizations

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments
- SOC Maturity transformations

Former documentary photographer
Father of 2 boys

@olafhartong
github.com/olafhartong
ohartong@deloitte.nl

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Why am I here?

- The Endpoint is a frequently used entry way into a network
- Endpoint Detection & Remediation (EDR) solutions are great, however often quite costly
- There is an alternative approach to the detection aspect, using an adversarial framework
- It allows you to leverage your existing data platform, in this case Splunk

Agenda

- MITRE ATT&CK
- Sysmon
  - What is it
  - Why use it
  - Configuration, mapped to ATT&CK
- ThreatHunting application
  - The goal
  - My challenges
  - Demonstration

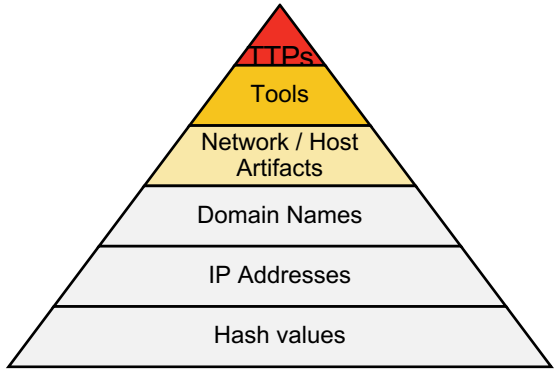
This is not a magic bullet. It will require tuning and real investigative work to be truly effective in your environment

DISCLAIMER

MITRE ATT&CK

" A framework for describing the behavior of cyber adversaries operating within enterprise networks. "

- Comprehensive library of "what to look for"
- Threat model & framework
- Library of attacker activity (TTPs)



ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

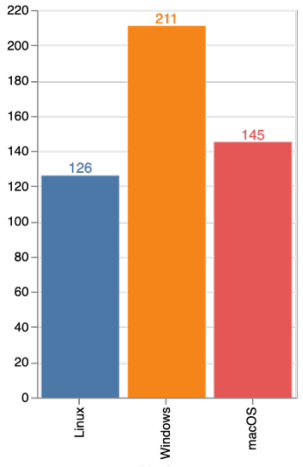
https://attack.mitre.org
https://mitre.github.io/attack-navigator/
@MITREattack

ATT&CK's Structure

245 Techniques!

Covering:

- 211 Windows
- 126 Linux
- 145 MacOS



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	33 items	59 items	28 items	67 items	19 items	22 items	17 items	13 items	22 items	9 items	14 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Launchctl	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	Shared Webroot	Screen Capture	Multi-Stage Channels		Service Stop
	Local Job Scheduling	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	Keychain	Query Registry	SSH Hijacking	Video Capture	Multiband Communication		Stored Data Manipulation
	LSASS Driver	Create Account	Launch Daemon	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Remote System Discovery	Taint Shared Content		Multilayer Encryption		Transmitted Data Manipulation
	Mshta	DLL Search Order Hijacking	New Service	Disabling Security Tools	Network Sniffing	Security Software Discovery	Third-party Software		Port Knocking		
	PowerShell	Dylib Hijacking	Path Interception	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote Access Tools		
	Regsvcs/Regasm	External Remote Services	Plist Modification	DLL Side-Loading	Private Keys	System Network Configuration Discovery	Windows Remote Management		Remote File Copy		
	Regsvr32	File System Permissions Weakness	Port Monitors	Execution Guardrails	Securityd Memory	System Network Connections Discovery			Standard Application Layer Protocol		
	Rundll32	Hidden Files and Directories	Process Injection	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Owner/User Discovery			Standard Cryptographic Protocol		
	Scheduled Task	Hooking	Scheduled Task	Extra Window Memory Injection		System Service Discovery			Standard Non-Application Layer Protocol		
	Scripting	Hypervisor	Service Registry Permissions Weakness	File Deletion		System Time Discovery			Uncommonly Used Port		
	Service Execution	Image File Execution Options Injection	Setuid and Setgid	File Permissions Modification		Virtualization/Sandbox Evasion			Web Service		
	Signed Binary Proxy Execution	Kernel Modules and Extensions	SID-History Injection	File System Logical Offsets							
	Signed Script Proxy Execution	Launch Agent	Startup Items	Gatekeeper Bypass							
	Source	Launch Daemon	Sudo	Group Policy Modification							
	Space after Filename	Launchctl	Sudo Caching	Hidden Files and Directories							
	Third-party Software	LC_LOAD_DYLIB Addition	Valid Accounts	Hidden Users							
	Trap	Local Job Scheduling	Web Shell	Hidden Window							
	Trusted Developer Utilities	Login Item		HISTCONTROL							
	User Execution	Logon Scripts		Image File Execution Options Injection							
	Windows Management Instrumentation	LSASS Driver		Indicator Blocking							
	Windows Remote Management	Modify Existing Service		Indicator Removal from Tools							
	XSL Script Processing	Netsh Helper DLL		Indicator Removal on Host							
		New Service		Indirect Command Execution							
		Office Application Startup		Install Root Certificate							
		Path Interception		InstallUtil							
		Plist Modification		Launchctl							
		Port Knocking		LC_MAIN Hijacking							
		Port Monitors		Masquerading							
		Rc.common		Modify Registry							
		Re-opened Applications		Mshta							
		Redundant Access		Network Share Connection Removal							
		Registry Run Keys / Startup Folder		NTFS File Attributes							
		Scheduled Task		Obfuscated Files or Information							
		Screensaver		Plist Modification							
		Security Support Provider		Port Knocking							
		Service Registry Permissions Weakness		Process Doppelgänging							
		Setuid and Setgid		Process Hollowing							
		Shortcut Modification		Process Injection							
		SIP and Trust Provider Hijacking		Redundant Access							
		Startup Items		Regsvcs/Regasm							
		System Firmware		Regsvr32							
		Systemd Service		Rootkit							
		Time Providers		Rundll32							
		Trap		Scripting							
		Valid Accounts		Signed Binary Proxy Execution							
		Web Shell		Signed Script Proxy Execution							
		Windows Management Instrumentation Event Subscription		SIP and Trust Provider Hijacking							
		Winlogon Helper DLL		Software Packing							
				Space after Filename							
				Template Injection							
				Timestomp							
				Trusted Developer Utilities							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

splunk> .conf19

Technique structure

[TITLE] *Credential Dumping*
[DESCRIPTION] *Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.*

ID: *T1003*
Tactic: *Credential Access*
Platform: *Windows, Linux, macOS*
Permissions Required: *Administrator, SYSTEM, root*
Data Sources: *API monitoring, Process monitoring, PowerShell logs, Process command-line parameters*
CAPEC ID: *CAPEC-567*
Contributors: *Vincent Le Toux, Ed Williams, Trustwave, SpiderLabs*
Version: *1.0*

Examples

Name	Description
APT28	APT28 regularly deploys both publicly available and custom password retrieval tools on victims.[18][19]
Mimikatz	Mimikatz performs credential dumping to obtain account and password information useful in gaining access to additional systems and enterprise network resources. It contains functionality to acquire information about credentials in many ways, including from the LSA, SAM table, credential vault, DCSync/NetSync, and DPAPI.[52][15][53]

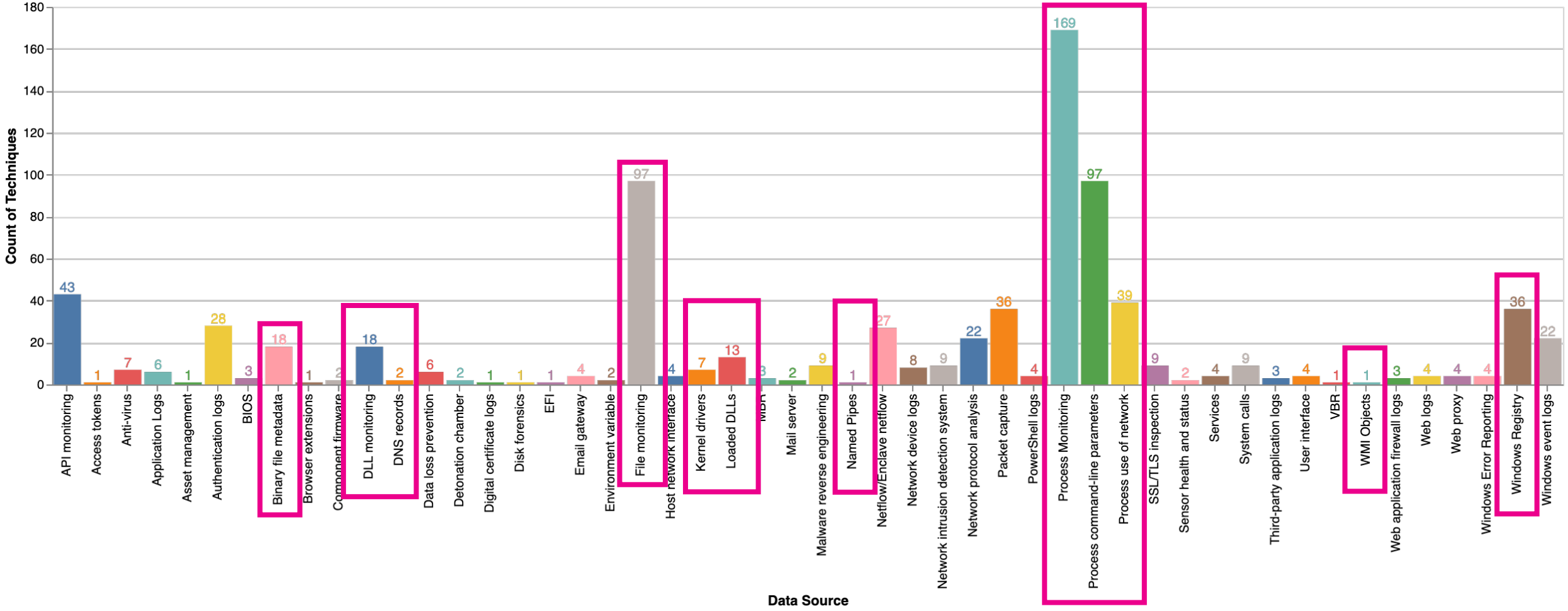
Mitigation

Detection

References

Data dispersion

The MITRE ATT&CK mentions per data source



splunk> .conf19

What is Sysmon?

This is where the subtitle goes

- Sysmon is a free, powerful host-level tracing tool, developed by a small team of Microsoft employees
- Initially developed for internal use at Microsoft
- Released under the Sysinternals license
- Sysmon is using a device driver and a service that is running in the background and loads very early in the boot process

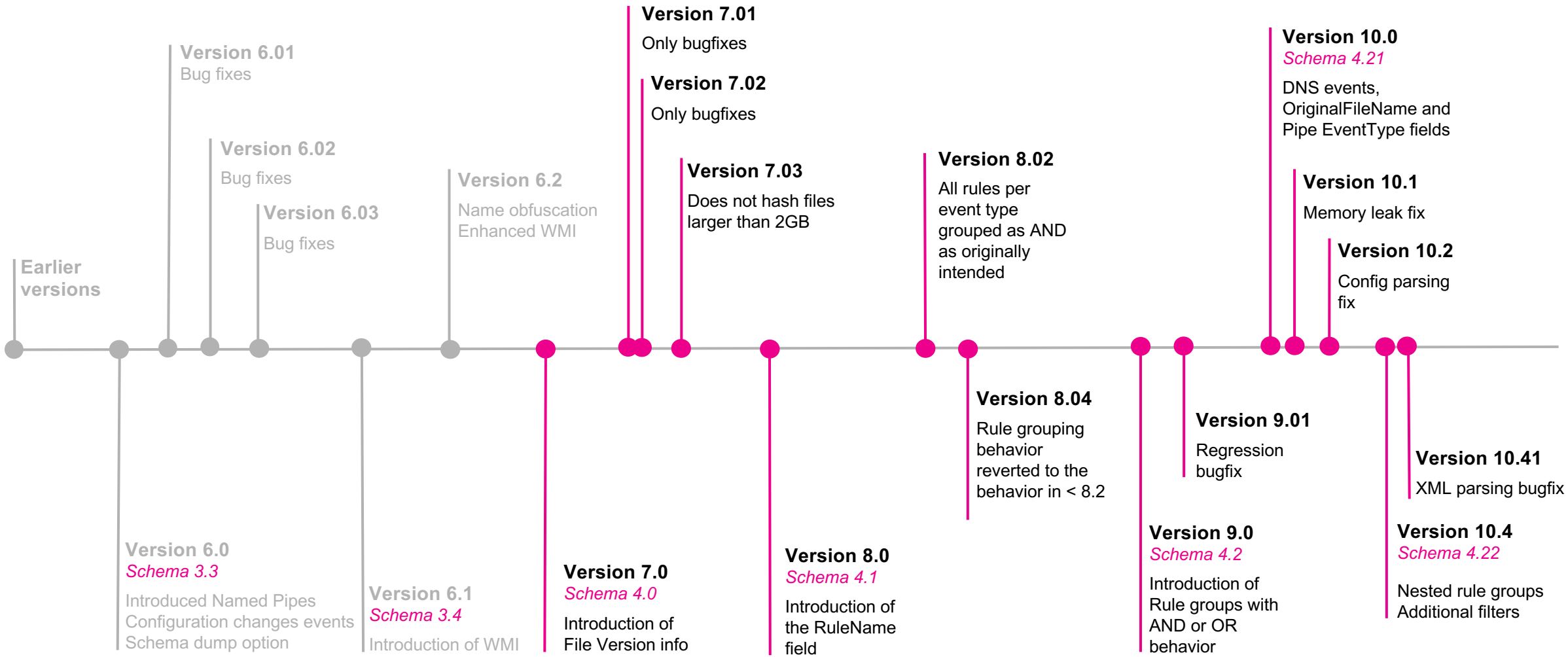
https://live.sysinternals.com
https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

What is Sysmon?

The event types it can write to the event log

- Process creation
- Process termination
- Network connections
- File creation timestamp changes
- Driver/Image loading
- Create remote threads
- Raw disk access
- Process memory access
- Registry access
- Named Pipes
- WMI
- DNS

The evolution of Sysmon



splunk> .conf19

Why use Sysmon ?

MITRE Data source perspective:

A little over **68%** of all techniques can (partially) be detected with process monitoring, **40%** with process command-line parameters

MITRE Threat group perspective:

Almost **65%** of known attacker groups prefer to use the command-line interface, standard application layer protocols and often start their attack with System information discovery

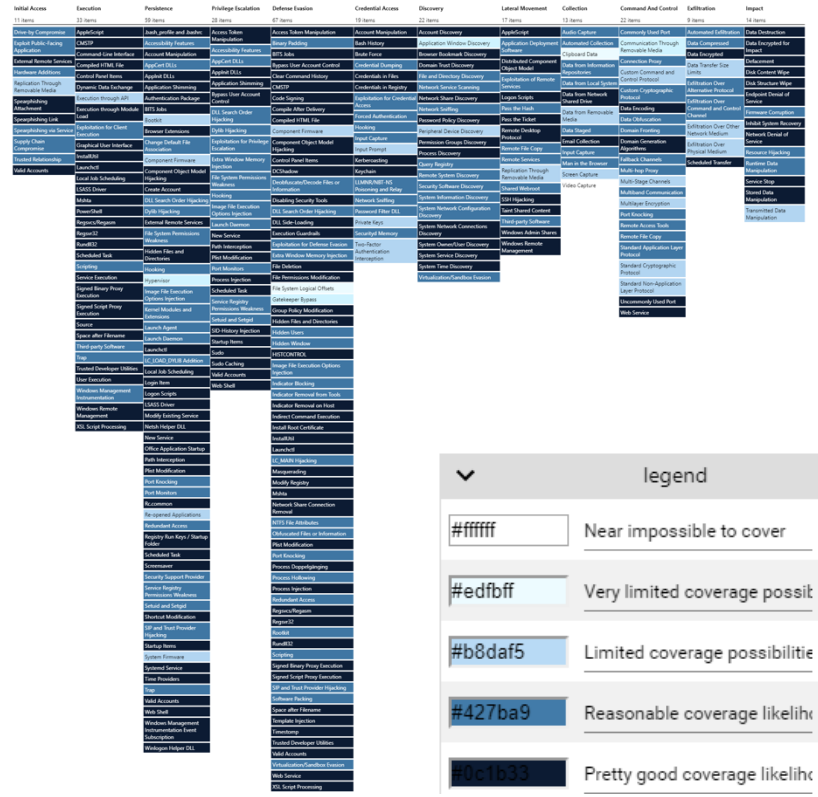
MITRE ATT&CK applicability

The likelihood of achieving full technique coverage per activity

Alerting

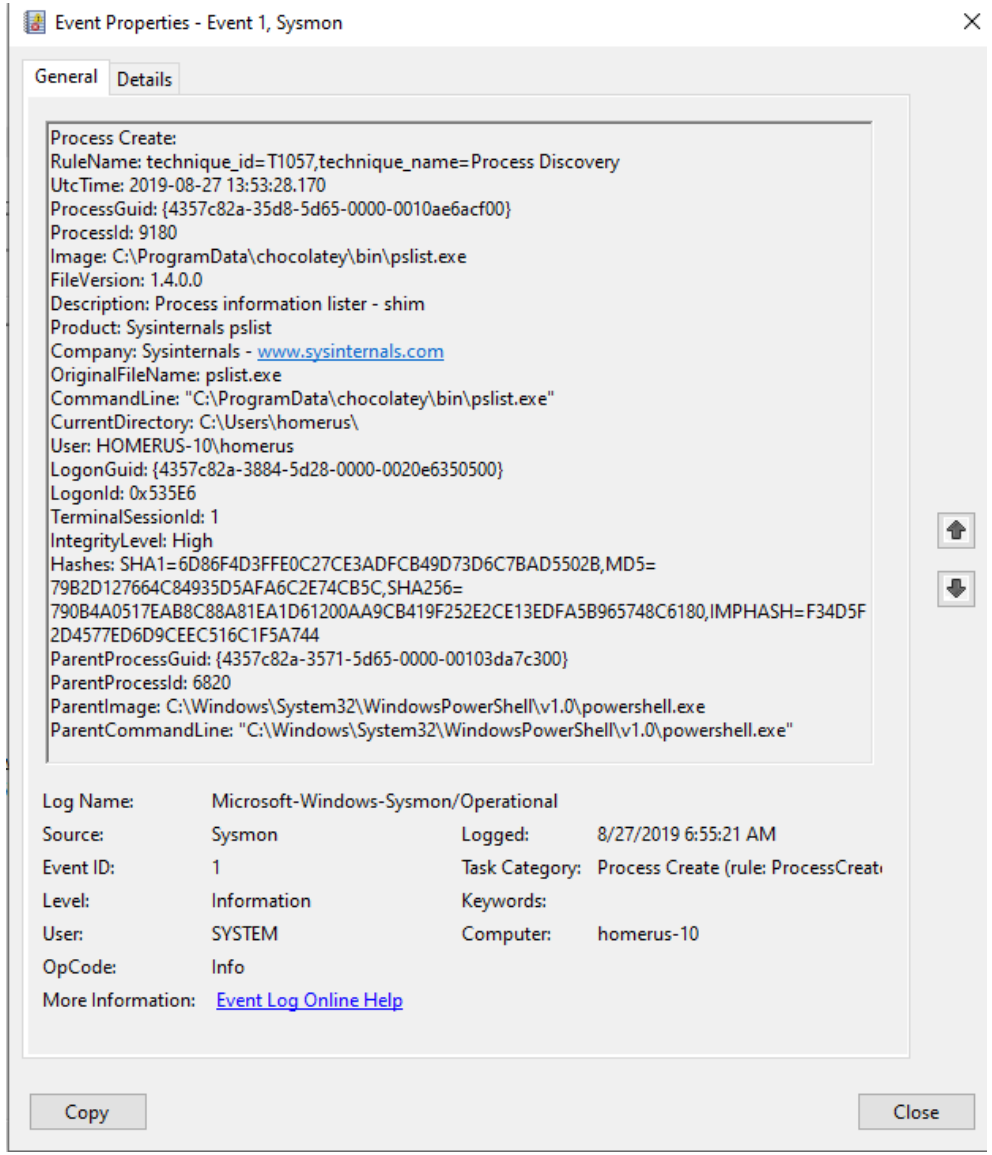
Hunting

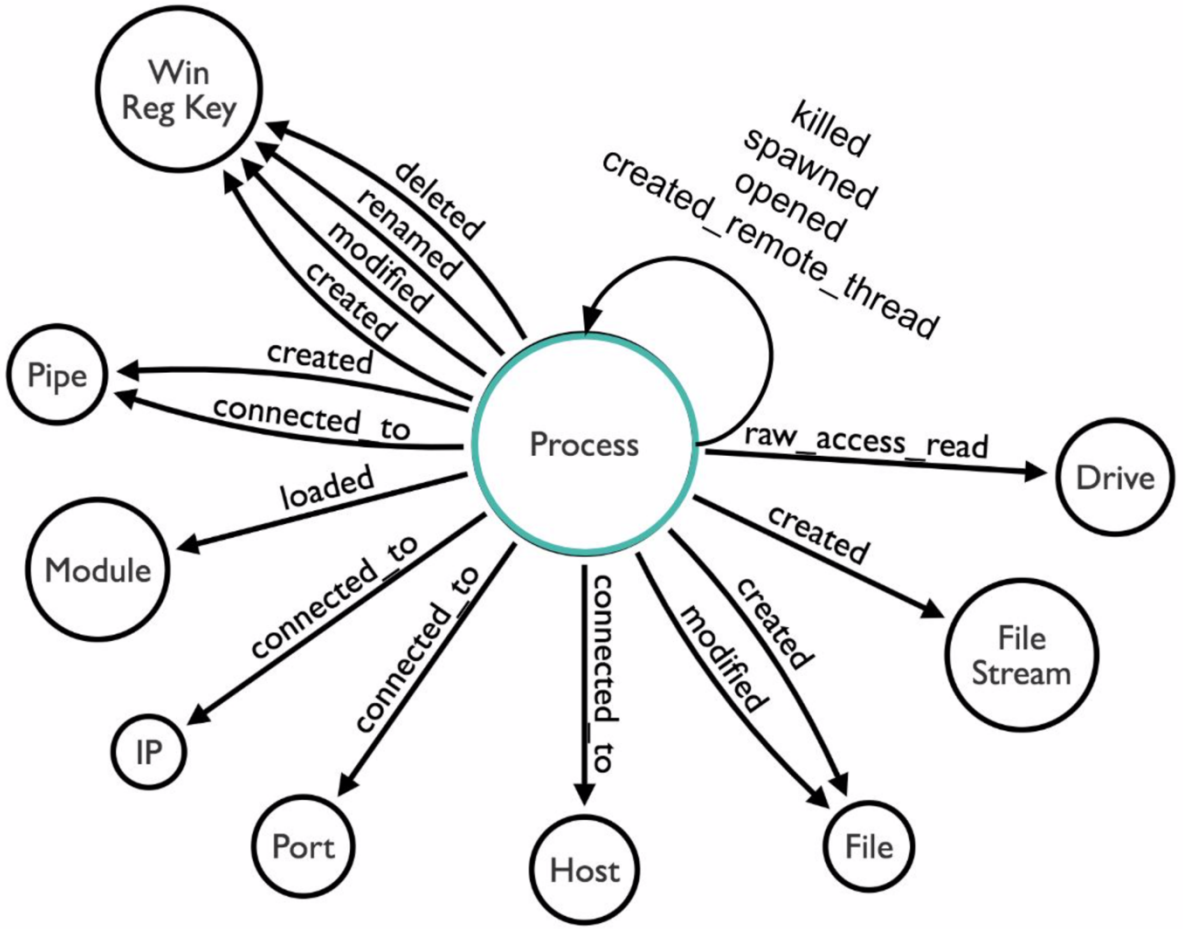
Forensics



splunk> .conf19

Why use Sysmon ?

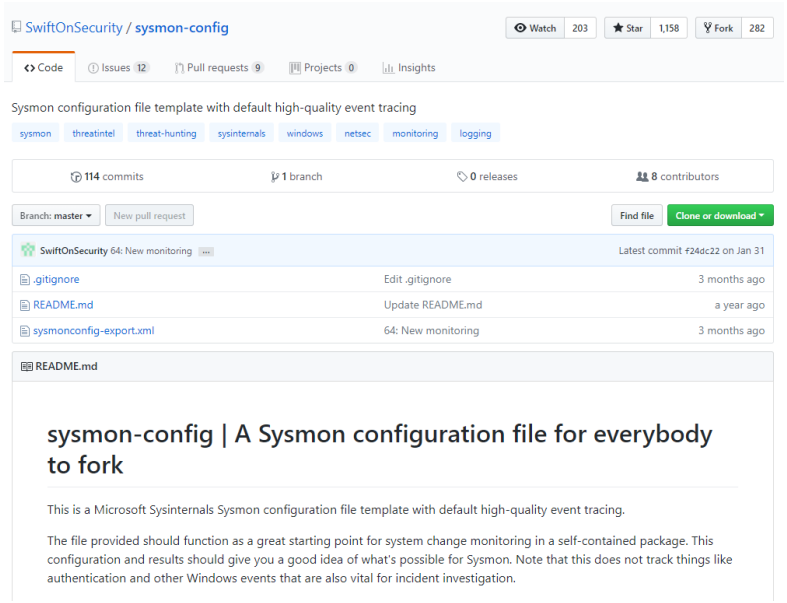




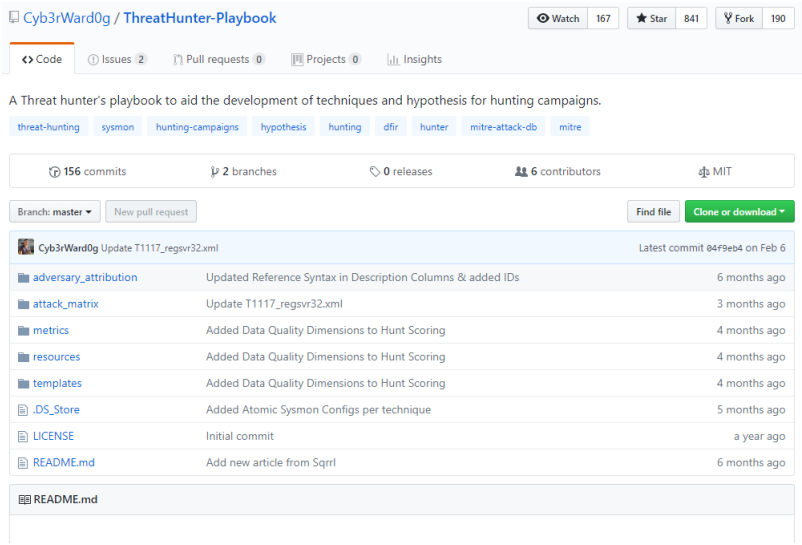
splunk> .conf19

Sysmon

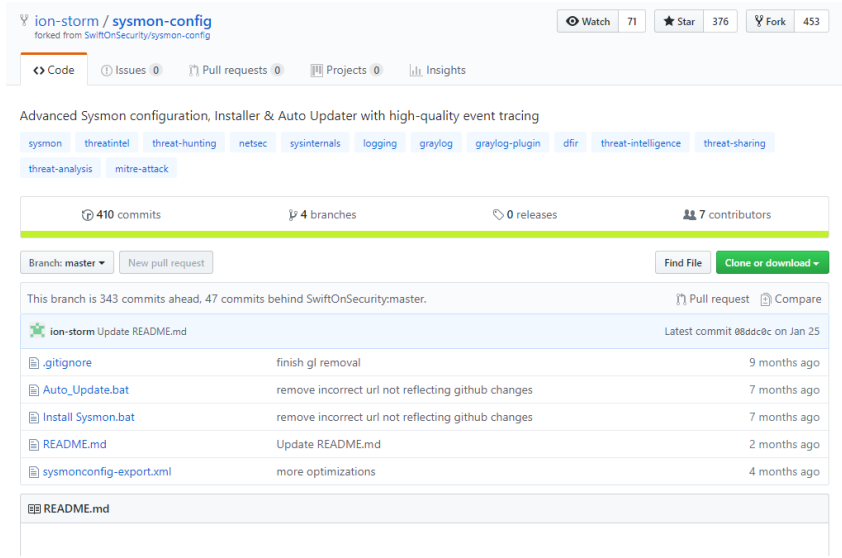
Some configuration examples



https://github.com/SwiftOnSecurity/sysmon-config
@SwiftOnSecurity



https://github.com/Cyb3rWard0g/ThreatHunter-Playbook
@Cyb3rWard0g



https://github.com/ionstorm/sysmon-config
@ionstorm

Great work by many others, a few examples;
@Neo23x0, @c_APT_ure, @hexacorn, @darkoperator, @mattifestation, @Sbousseaden, @mhaag
@markrussinovich, @analyze_v

splunk> .conf19

Introducing Sysmon-modular

- A Sysmon configuration repository, set up in a modular fashion for easier maintenance and generation of tailored configurations
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques

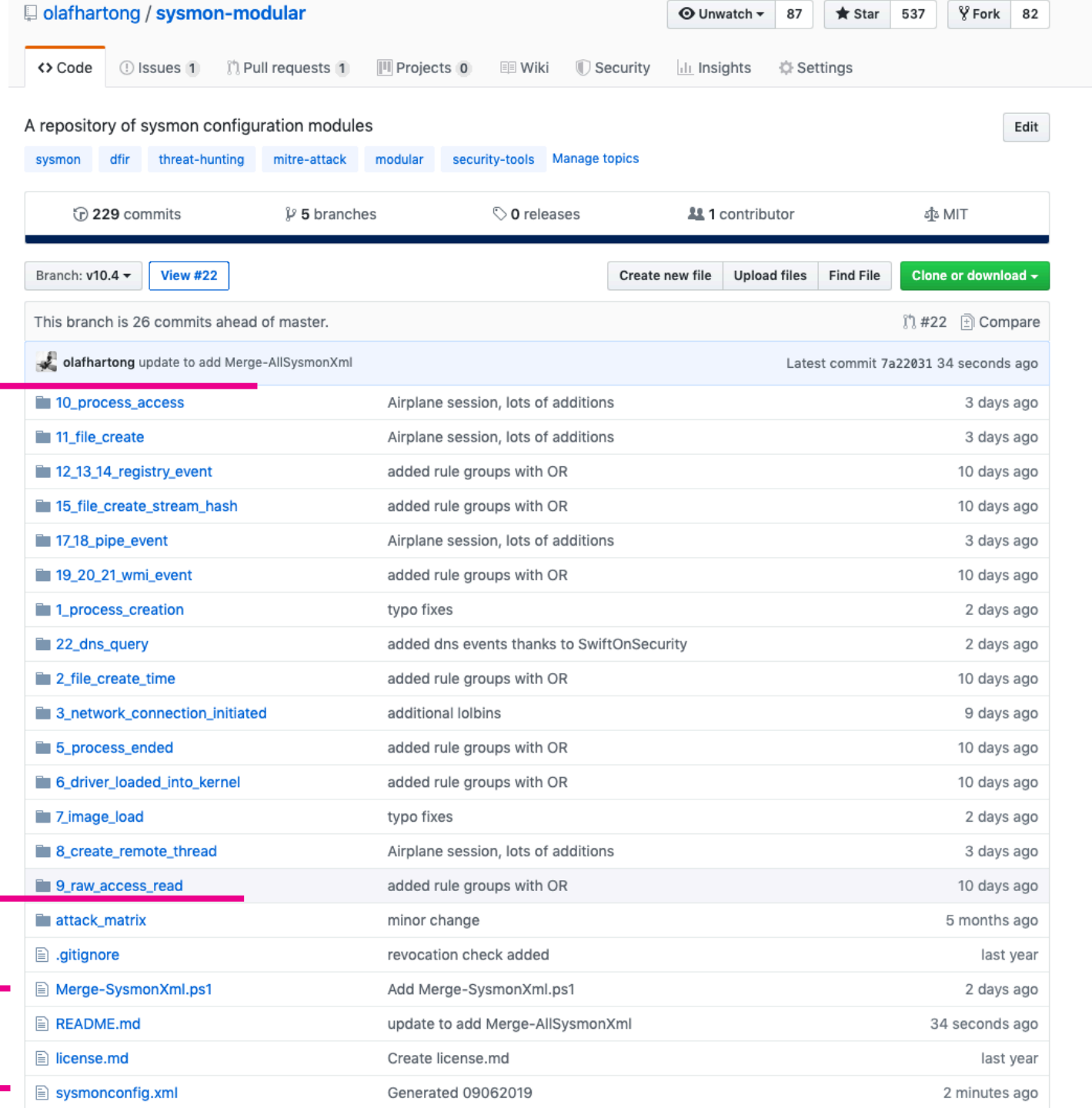
github.com/olafhartong/Sysmon-modular

Configuration Structure

All available event types

Merge script

Complete generated configuration



olafhartong / sysmon-modular

Unwatch 87 | Star 537 | Fork 82

Code | Issues 1 | Pull requests 1 | Projects 0 | Wiki | Security | Insights | Settings

A repository of sysmon configuration modules

Edit

sysmon | dfir | threat-hunting | mitre-attack | modular | security-tools | Manage topics

229 commits | 5 branches | 0 releases | 1 contributor | MIT

Branch: v10.4 | View #22 | Create new file | Upload files | Find File | Clone or download

This branch is 26 commits ahead of master. #22 Compare

olafhartong update to add Merge-AllSysmonXml — Latest commit 7a22031 34 seconds ago

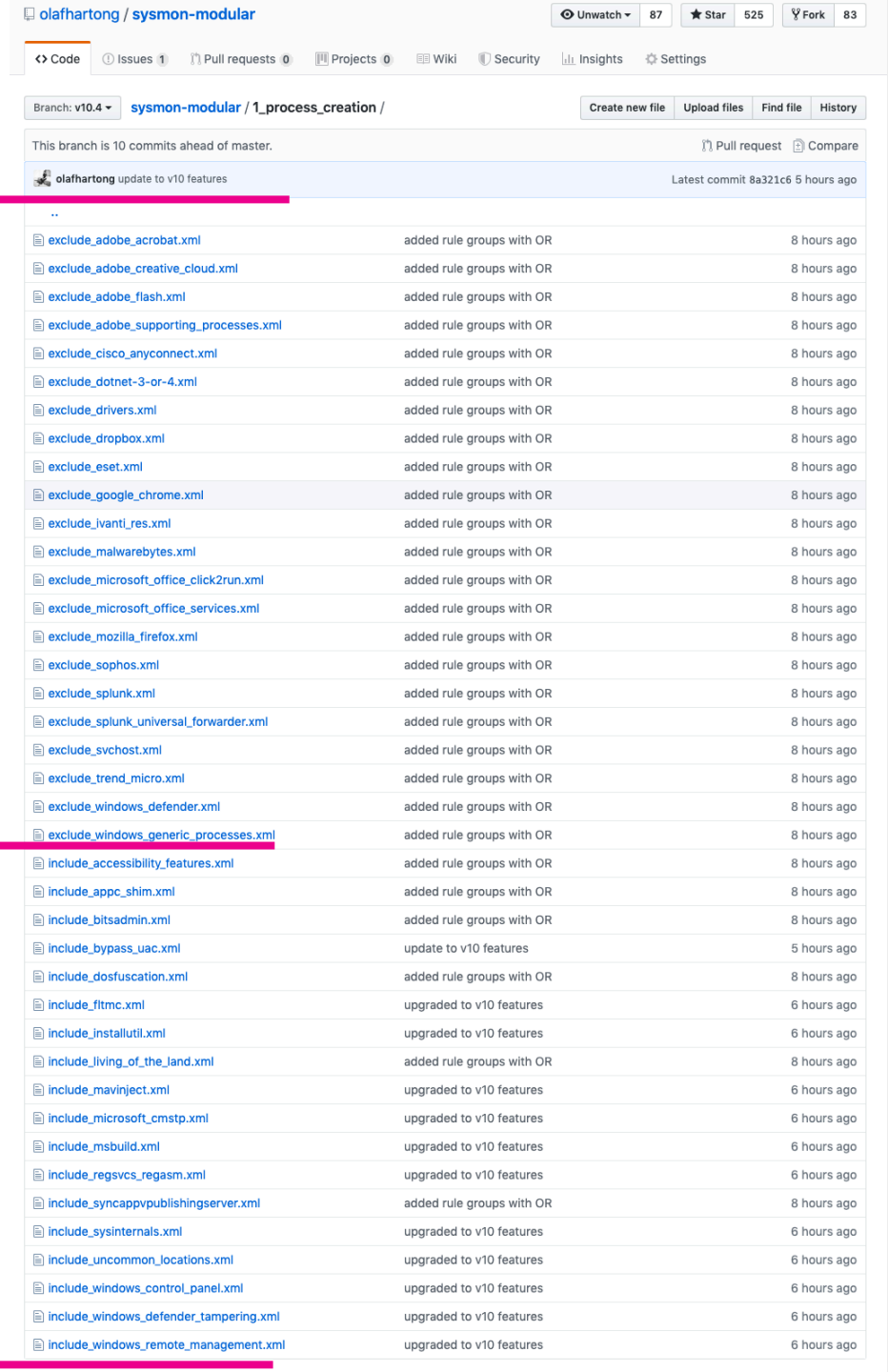
10_process_access	Airplane session, lots of additions	3 days ago
11_file_create	Airplane session, lots of additions	3 days ago
12_13_14_registry_event	added rule groups with OR	10 days ago
15_file_create_stream_hash	added rule groups with OR	10 days ago
17_18_pipe_event	Airplane session, lots of additions	3 days ago
19_20_21_wmi_event	added rule groups with OR	10 days ago
1_process_creation	typo fixes	2 days ago
22_dns_query	added dns events thanks to SwiftOnSecurity	2 days ago
2_file_create_time	added rule groups with OR	10 days ago
3_network_connection_initiated	additional lolbins	9 days ago
5_process_ended	added rule groups with OR	10 days ago
6_driver_loaded_into_kernel	added rule groups with OR	10 days ago
7_image_load	typo fixes	2 days ago
8_create_remote_thread	Airplane session, lots of additions	3 days ago
9_raw_access_read	added rule groups with OR	10 days ago
attack_matrix	minor change	5 months ago
.gitignore	revocation check added	last year
Merge-SysmonXml.ps1	Add Merge-SysmonXml.ps1	2 days ago
README.md	update to add Merge-AllSysmonXml	34 seconds ago
license.md	Create license.md	last year
sysmonconfig.xml	Generated 09062019	2 minutes ago

Configuration Structure

For process creation events

Excluded processes

Included processes



olafhartong / sysmon-modular

Unwatch 87 | Star 525 | Fork 83

Code | Issues 1 | Pull requests 0 | Projects 0 | Wiki | Security | Insights | Settings

Branch: v10.4 | sysmon-modular / 1_process_creation / | Create new file | Upload files | Find file | History

This branch is 10 commits ahead of master. | Pull request | Compare

olafhartong update to v10 features | Latest commit 8a321c6 5 hours ago

exclude_adobe_acrobat.xml	added rule groups with OR	8 hours ago
exclude_adobe_creative_cloud.xml	added rule groups with OR	8 hours ago
exclude_adobe_flash.xml	added rule groups with OR	8 hours ago
exclude_adobe_supporting_processes.xml	added rule groups with OR	8 hours ago
exclude_cisco_anyconnect.xml	added rule groups with OR	8 hours ago
exclude_dotnet-3-or-4.xml	added rule groups with OR	8 hours ago
exclude_drivers.xml	added rule groups with OR	8 hours ago
exclude_dropbox.xml	added rule groups with OR	8 hours ago
exclude_eset.xml	added rule groups with OR	8 hours ago
exclude_google_chrome.xml	added rule groups with OR	8 hours ago
exclude_ivanti_res.xml	added rule groups with OR	8 hours ago
exclude_malwarebytes.xml	added rule groups with OR	8 hours ago
exclude_microsoft_office_click2run.xml	added rule groups with OR	8 hours ago
exclude_microsoft_office_services.xml	added rule groups with OR	8 hours ago
exclude_mozilla_firefox.xml	added rule groups with OR	8 hours ago
exclude_sophos.xml	added rule groups with OR	8 hours ago
exclude_splunk.xml	added rule groups with OR	8 hours ago
exclude_splunk_universal_forwarder.xml	added rule groups with OR	8 hours ago
exclude_svchost.xml	added rule groups with OR	8 hours ago
exclude_trend_micro.xml	added rule groups with OR	8 hours ago
exclude_windows_defender.xml	added rule groups with OR	8 hours ago
exclude_windows_generic_processes.xml	added rule groups with OR	8 hours ago
include_accessibility_features.xml	added rule groups with OR	8 hours ago
include_appc_shim.xml	added rule groups with OR	8 hours ago
include_bitsadmin.xml	added rule groups with OR	8 hours ago
include_bypass_uac.xml	update to v10 features	5 hours ago
include_dosfuscation.xml	added rule groups with OR	8 hours ago
include_fltmc.xml	upgraded to v10 features	6 hours ago
include_installutil.xml	upgraded to v10 features	6 hours ago
include_living_of_the_land.xml	added rule groups with OR	8 hours ago
include_mavinject.xml	upgraded to v10 features	6 hours ago
include_microsoft_cmstp.xml	upgraded to v10 features	6 hours ago
include_msbuild.xml	upgraded to v10 features	6 hours ago
include_regsvcs_regasm.xml	upgraded to v10 features	6 hours ago
include_syncappvpublishingserver.xml	added rule groups with OR	8 hours ago
include_sysinternals.xml	upgraded to v10 features	6 hours ago
include_uncommon_locations.xml	upgraded to v10 features	6 hours ago
include_windows_control_panel.xml	upgraded to v10 features	6 hours ago
include_windows_defender_tampering.xml	upgraded to v10 features	6 hours ago
include_windows_remote_management.xml	upgraded to v10 features	6 hours ago

splunk> .conf19

Configuration Example

Exclude Splunk

Branch: master ▾ **sysmon-modular** / 1_process_creation / **exclude_splunk.xml** Find file | Copy path

olafhartong major overhaul, removing all template overhead c0c5333 on 16 Apr

1 contributor

10 lines (10 sloc) | 563 Bytes Raw | Blame | History

```
1  <Sysmon schemaversion="4.1">
2    <EventFiltering>
3       <ProcessCreate onmatch="exclude">
4                       <Image condition="begin with">C:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
5                       <ParentImage condition="is">C:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
6                       <Image condition="begin with">D:\Program Files\Splunk\bin\</Image> <!--Splunk child processes-->
7                       <ParentImage condition="is">D:\Program Files\Splunk\bin\splunkd.exe</ParentImage> <!--Splunk:Daemon-->
8                       </ProcessCreate>
9   </EventFiltering>
10 </Sysmon>
```

Configuration Example

Include Sysinternals tools mapped to ATT&CK techniques

Branch: v10.4 ▾ **sysmon-modular** / 1_process_creation / **include_sysinternals.xml** Find file | Copy path

olafhartong upgraded to v10 features 9b1db90 6 hours ago

1 contributor

33 lines (32 sloc) | 3.7 KB Raw | Blame | History

```
<OriginalFileName<Sysmon schemaversion="4.22">
   <EventFiltering>
 <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="include">
        <!--Note: Not all Sysinternals listed here, only the ones I know/suspect to be used for malicious activity -->
        <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsList.exe</OriginalFileNam
        <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="is">PsService.exe</Origi
        <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.exe</OriginalFileNam
        <OriginalFileName name="technique_id=T1035,technique_name=Service Execution" condition="is">PsExec.c</OriginalFileName>
        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsGetSID.exe</Ori
        <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PsKill.exe</Original
        <OriginalFileName name="technique_id=T1089,technique_name=Disabling Security Tools" condition="is">PKill.exe</OriginalF
        <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="contains">ProcDump</OriginalFi
        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">PsLoggedOn.exe</O
        <OriginalFileName name="technique_id=T1105,technique_name=Remote File Copy" condition="image">PsFile.exe</OriginalFileN
        <OriginalFileName name="technique_id=T1088,technique_name=Bypass User Account Control" condition="contains">ShellRunas<
        <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PipeList.exe</OriginalFileN
        <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessChk.exe</O
        <OriginalFileName name="technique_id=T1083,technique_name=File and Directory Discovery" condition="is">AccessEnum.exe</
        <OriginalFileName name="technique_id=T1033,technique_name=System Owner/User Discovery" condition="is">LogonSessions.exe
        <OriginalFileName name="technique_id=T1005,technique_name=Data from Local System" condition="is">PsLogList.exe</Origina
        <OriginalFileName name="technique_id=T1057,technique_name=Process Discovery" condition="is">PsInfo.exe</OriginalFileNam
        <OriginalFileName name="technique_id=T1007,technique_name=System Service Discovery" condition="contains">LoadOrd</Origi
        <OriginalFileName name="technique_id=T1098,technique_name=Account Manipulation" condition="is">PsPasswd.exe</OriginalFi
        <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="is">ru.exe</OriginalFileName>
        <OriginalFileName name="technique_id=T1012,technique_name=Query Registry" condition="contains">Regsize</OriginalFileNam
        <OriginalFileName name="technique_id=T1003,technique_name=Credential Dumping" condition="is">ProcDump</OriginalFileName
        <CommandLine name="technique_id=T1003,technique_name=Credential Dumping"  condition="is">-ma lsass.exe</CommandLine>
      </ProcessCreate>
</RuleGroup>
</EventFiltering>
</Sysmon>
```

Latest features:

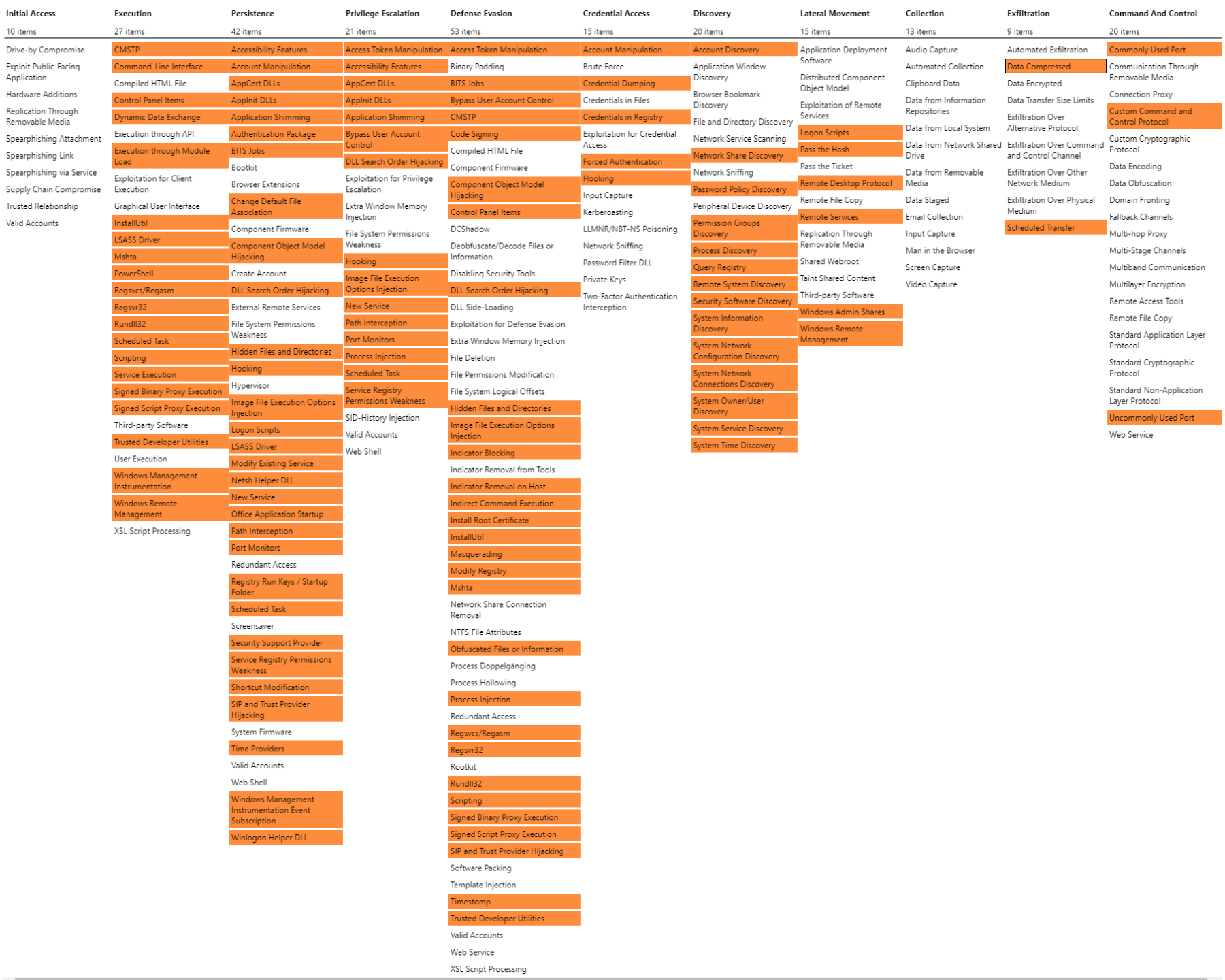
- OriginalFileName field
- DNS Events

- Additional filters;
  contains any, contains all
- Nested rule grouping (yeah!)

```
<Sysmon schemaversion="4.22">
   <EventFiltering>
 <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="include">
        <Rule name="Eventviewer Bypass UAC" groupRelation="and">
          <ParentImage name="technique_id=T1088,technique_name=Bypass User Account Control" condition="image">eventvwr.exe</ParentImage>
          <Image condition="is not">c:\windows\system32\mmc.exe</Image>
        </Rule>
      </ProcessCreate>
</RuleGroup>
</EventFiltering>
</Sysmon>
```

ATT&CK coverage

Approximate, the configuration will also generate events for techniques otherwise tagged



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	27 items	42 items	21 items	53 items	15 items	20 items	15 items	13 items	9 items	20 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Password Policy Discovery	Remote File Copy	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Peripheral Device Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Kerberoasting	Permission Groups Discovery	Replication Through Removable Media	Input Capture		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multiband Communication
	PowerShell	Create Account	New Service	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Admin Shares			Remote Access Tools
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Remote File Copy
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion		System Network Configuration Discovery				Standard Application Layer Protocol
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection		System Network Connections Discovery				Standard Cryptographic Protocol
	Scripting	Hooking	Service Registry Permissions Weakness	File Deletion		System Owner/User Discovery				Standard Non-Application Layer Protocol
	Service Execution	Hypervisor	SID-History Injection	File Permissions Modification		System Service Discovery				Uncommonly Used Port
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File System Logical Offsets		System Time Discovery				Web Service
	Signed Script Proxy Execution	Logon Scripts	Web Shell	Hidden Files and Directories						
	Third-party Software	LSASS Driver		Image File Execution Options Injection						
	Trusted Developer Utilities	Modify Existing Service		Indicator Blocking						
	User Execution	Netsh Helper DLL		Indicator Removal from Tools						
	Windows Management Instrumentation	New Service		Indicator Removal on Host						
	Windows Remote Management	Office Application Startup		Indirect Command Execution						
	XSL Script Processing	Path Interception		Install Root Certificate						
		Port Monitors		InstallUtil						
		Redundant Access		Masquerading						
		Registry Run Keys / Startup Folder		Modify Registry						
		Scheduled Task		Mshta						
		Screensaver		Network Share Connection Removal						
		Security Support Provider		NTFS File Attributes						
		Service Registry Permissions Weakness		Obfuscated Files or Information						
		Shortcut Modification		Process Doppelgänging						
		SIP and Trust Provider Hijacking		Process Hollowing						
		System Firmware		Process Injection						
		Time Providers		Redundant Access						
		Valid Accounts		Regsvcs/Regasm						
		Web Shell		Regsvr32						
		Windows Management Instrumentation Event Subscription		Rootkit						
		Winlogon Helper DLL		Rundll32						
				Scripting						
				Signed Binary Proxy Execution						
				Signed Script Proxy Execution						
				SIP and Trust Provider Hijacking						
				Software Packing						
				Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						
				XSL Script Processing						

Data volume

Average per 7 days, on servers. Workstations will generate less

Average Data Size per Host and Source

Source	Avg Host Count	Avg Source Volume (MB)	Avg Host Source Volume (MB)
WinEventLog:Security	232.14	11682.962	50.327
WinEventLog:Microsoft-Windows-Sysmon/Operational	218.14	5528.664	25.345
WinEventLog:Microsoft-Windows-WMI-Activity/Operational	152.57	122.911	0.806
WinEventLog:Microsoft-Windows-PowerShell/Operational	38.29	21.885	0.572
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	1.00	0.104	0.104
WinEventLog:Application	6.00	0.325	0.054
C:\\Windows\\sysmon.log	222.43	0.021	0.000

Introducing the ThreatHunting app

Goal

- Create an investigative workflow approach for Threat Hunters
- Work with ML (Mandatory Learning) to get to know your environment
- There are no false positives, just informational triggers
- Supply the user with tools to contextualize and investigate these events
- Use MITRE ATT&CK as the foundation for hunts


github.com/olafhartong/ThreatHunting


splunkbase.splunk.com/app/4305

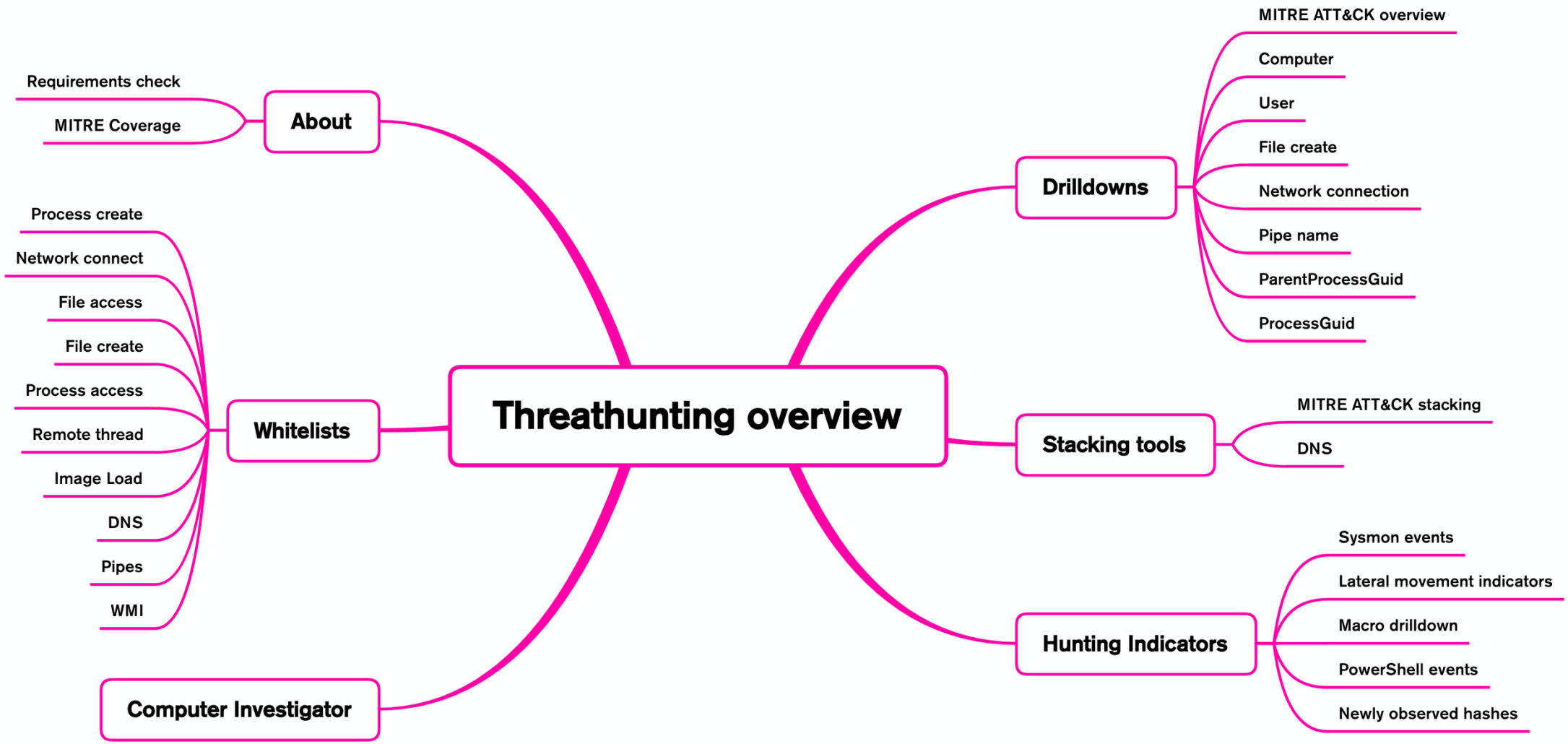
Introducing the ThreatHunting app

Challenges

- No data model I liked, created one based on OSSEM
- Inventing a whitelist capability on 150+ searches
- I’m not a great coder
- Rebuilt the app over 4 times to address hindsight, let’s call this Agile
- Keeping the app performing swiftly
- Still some technical limitations

https://github.com/Cyb3rWard0g/OSSEM

Introducing the ThreatHunting app



ATT&CK coverage

144 Reports!

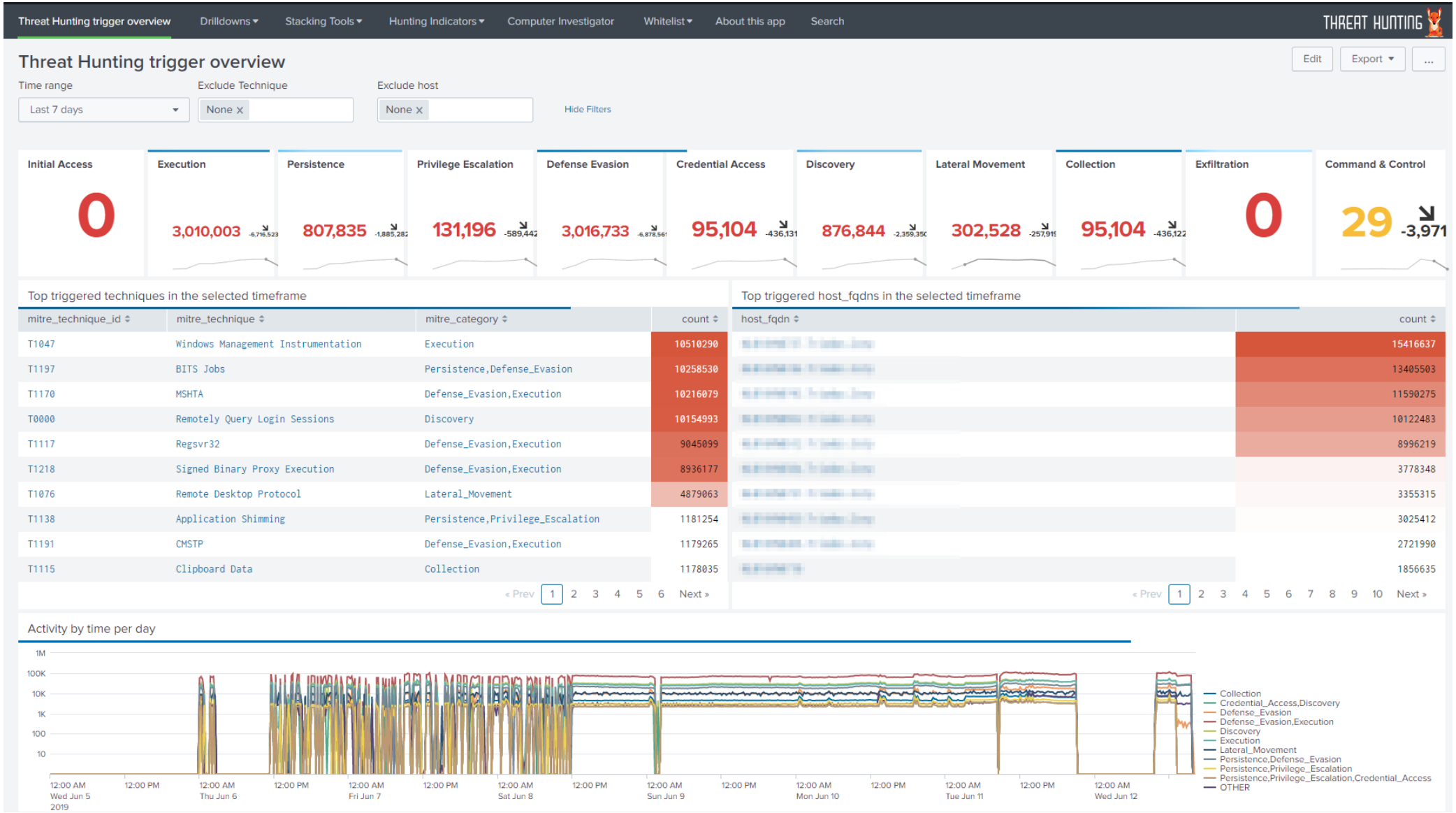
and several live dashboards

Generating triggers for over 130 Techniques*

* triggers are not intended to cover the full technique

DEMO

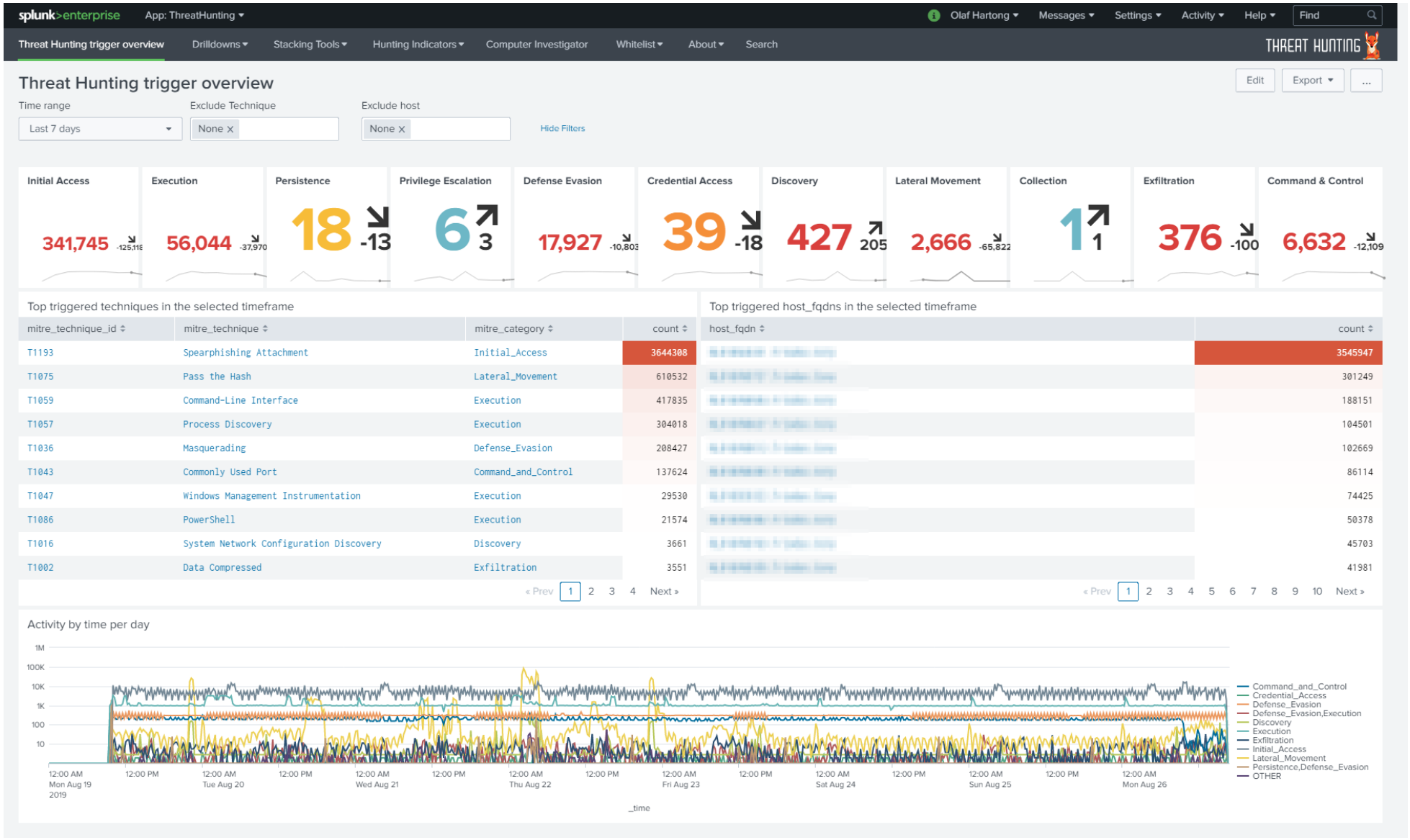
One of my oopsies



splunk> .conf19

Real customer example

Initial deployment, un-whitelisted. After a few days these numbers are managable



splunk> .conf19

Try it yourself

A lab environment complete with security tooling and logging best practices, containing;

- Windows DC
- Windows WEF server
- Windows 10
- Logger machine, containing Splunk, Bro, Suricata, Kolide and much more

github.com/clong/DetectionLab

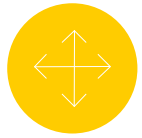
Roadmap

Things on my backlog

Optimizations to the app, add drilldown dashboards
Additional contextual enrichment (workflows)
Check new hashes daily against VT

Windows, PowerShell (transcript) and WMI logging
Threat hunting triggers and dashboards on these logs

Linux coverage
OSQuery configuration and build threat hunting triggers on these logs



Other log sources and triggers for;
Bro/Zeek , Firewalls, Antivirus, EDRs and more

S	M	T	W	T	F	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	39	31		

Pull requests are welcome!

Available now!

Any questions ?

github.com/olafhartong/threathunting

splunkbase.splunk.com/app/4305

github.com/olafhartong/Sysmon-modular

@olafhartong
github.com/olafhartong
ohartong@deloitte.nl

splunk> .conf19

splunk>

Thank You!