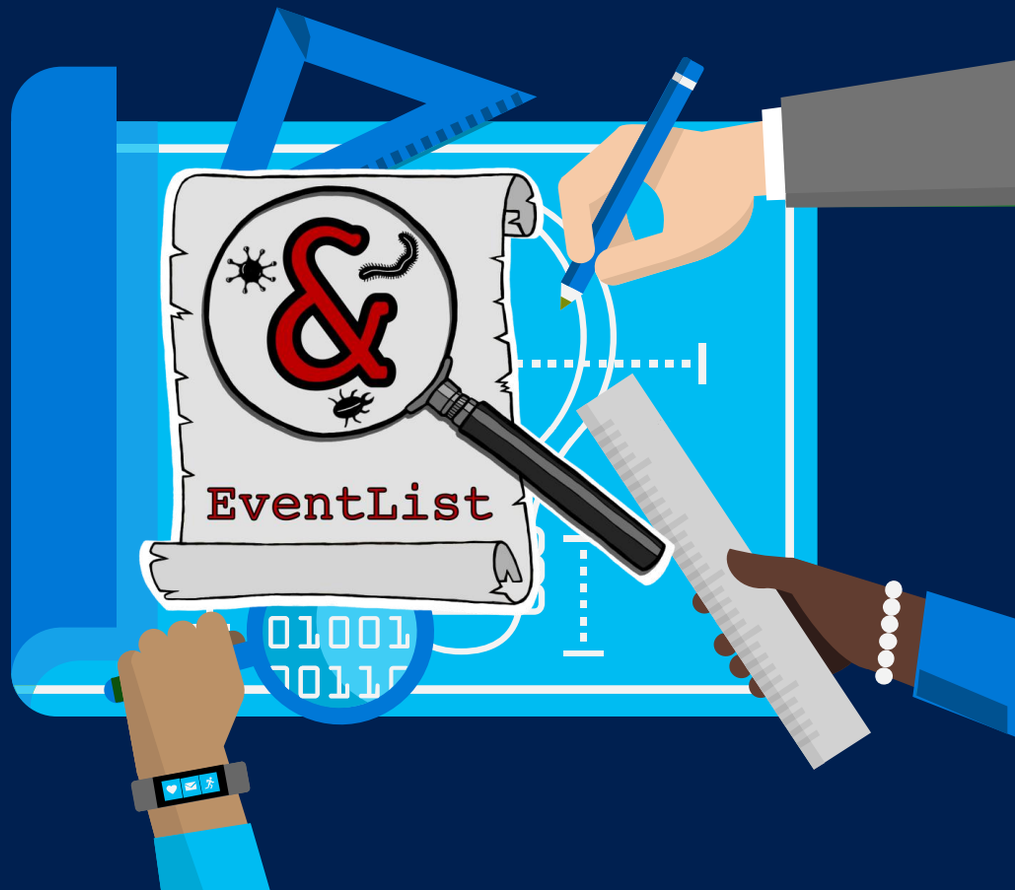
Microsoft

What the log?! So many events, so little time…

Miriam Wiesner

Security Program Manager for Microsoft Defender ATP

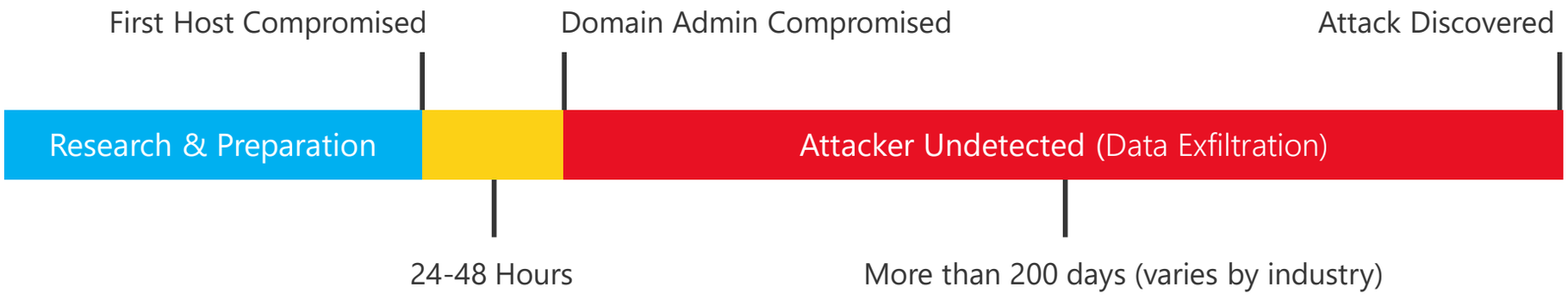
Twitter: @miriamxyra
LinkedIn: miriamwiesner
Blog: https://miriamxyra.com



Disclaimer

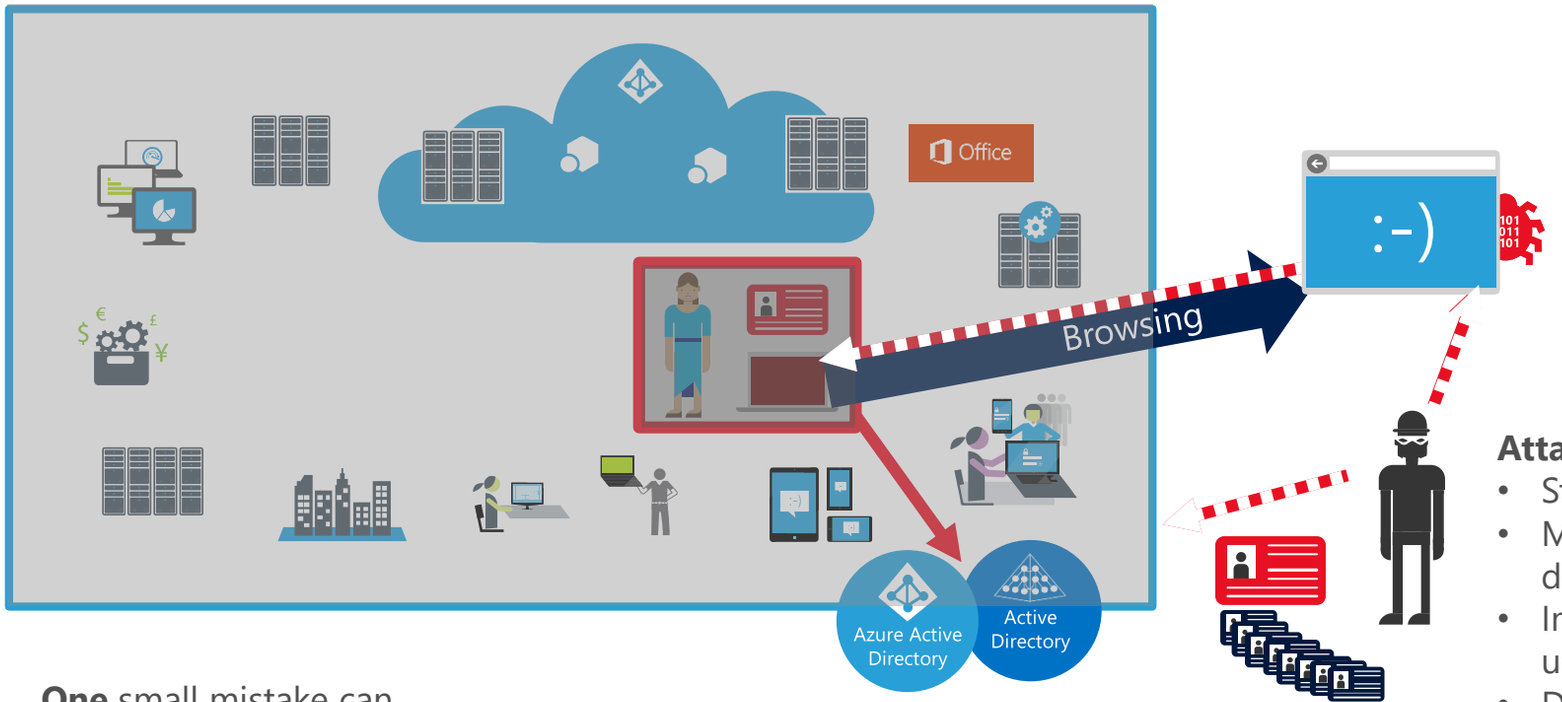
This presentation and the tool demonstrated during the session is my personal work and not supported by Microsoft.

Typical Attack Timeline & Observations



Identity is the new security "perimeter" under attack

Active Directory and Administrators control all the assets



One small mistake can lead to attacker control

Attackers Can

- Steal any data
- Modify documents
- Impersonate users
- Disrupt business operations

Microsoft Security Compliance Toolkit 1.0

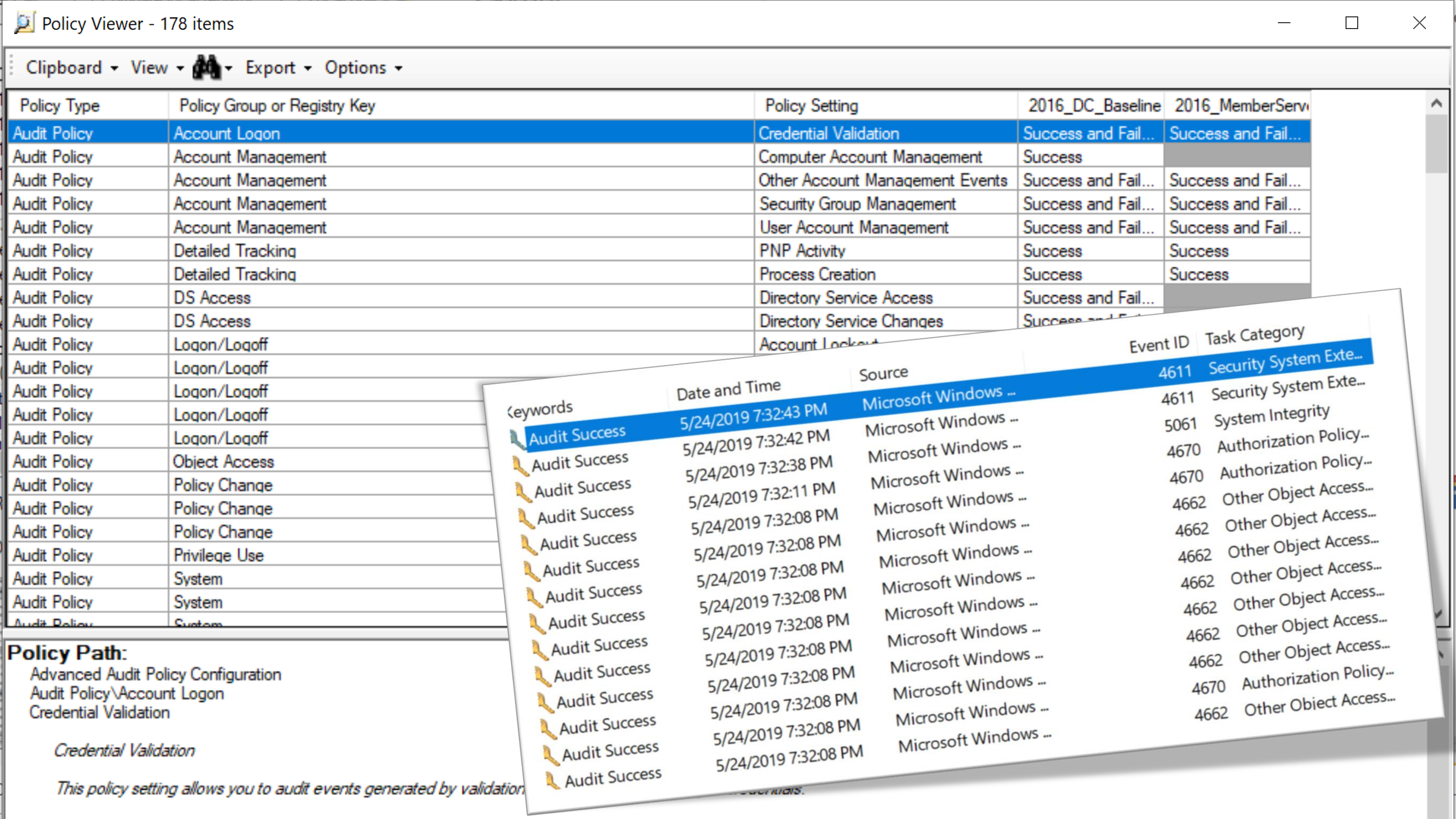
Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English** Download

Choose the download you want

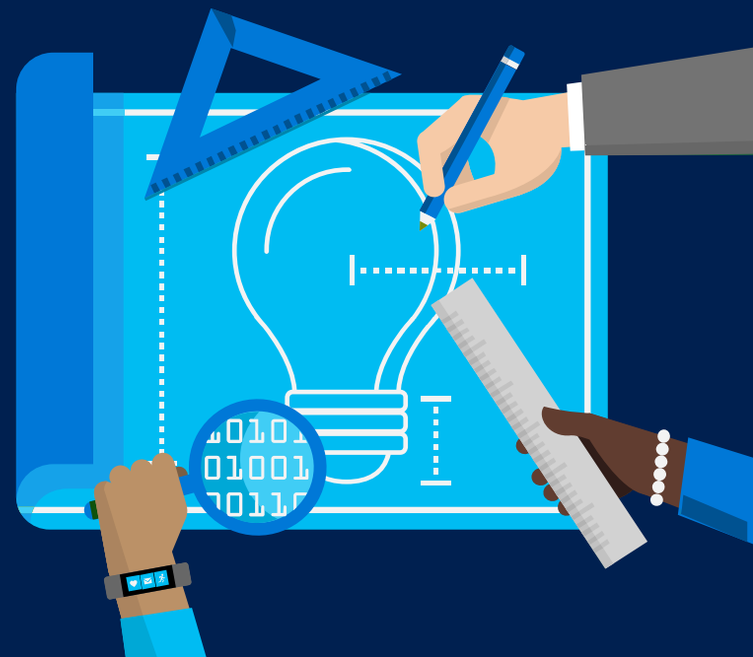
File Name	Size
LGPO.zip	797 KB
Office-2016-baseline.zip	4.5 MB
PolicyAnalyzer.zip	1.6 MB
Windows 10 Version 1507 Security Baseline.zip	904 KB
Windows 10 Version 1511 Security Baseline.zip	902 KB
Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB

Microsoft Security Compliance Toolkit
https://aka.ms/SCT


Policy Viewer - 178 items
Clipboard
View
Export
Options
Policy Type
Policy Group or Registry Key
Policy Setting
2016_DC_Baseline
2016_MemberServ
Audit Policy | Account Logon | Credential Validation | Success and Fail... | Success and Fail...
Audit Policy | Account Management | Computer Account Management | Success
Audit Policy | Account Management | Other Account Management Events | Success and Fail... | Success and Fail...
Audit Policy | Account Management | Security Group Management | Success and Fail... | Success and Fail...
Audit Policy | Account Management | User Account Management | Success and Fail... | Success and Fail...
Audit Policy | Detailed Tracking | PNP Activity | Success | Success
Audit Policy | Detailed Tracking | Process Creation | Success | Success
Audit Policy | DS Access | Directory Service Access | Success and Fail...
Audit Policy | DS Access | Directory Service Changes
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff
Audit Policy | Object Access
Audit Policy | Policy Change
Audit Policy | Policy Change
Audit Policy | Policy Change
Audit Policy | Privilege Use
Audit Policy | System
Audit Policy | System
Policy Path:
Advanced Audit Policy Configuration
Audit Policy\Account Logon
Credential Validation
Credential Validation
This policy setting allows you to audit events generated by validation
Keywords
Date and Time
Source
Event ID
Task Category
Audit Success | 5/24/2019 7:32:43 PM | Microsoft Windows ... | 4611 | Security System Exte...
Audit Success | 5/24/2019 7:32:42 PM | Microsoft Windows ... | 4611 | Security System Exte...
Audit Success | 5/24/2019 7:32:38 PM | Microsoft Windows ... | 5061 | System Integrity
Audit Success | 5/24/2019 7:32:11 PM | Microsoft Windows ... | 4670 | Authorization Policy...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4670 | Authorization Policy...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4670 | Authorization Policy...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ... | 4662 | Other Object Access...
Audit Success | 5/24/2019 7:32:08 PM | Microsoft Windows ...
Audit Success

1994. II
1992 II
2003 II
2002 II
2001 II

EventList 1.0



AutoSave Off | EventList.xlsm - Excel | Miriam Wiesner

File Home Insert Draw Page Layout Formulas Data Review View Developer Help Search | Share | Comments

Paste | Calibri 11 | Protect | General | Conditional Formatting | Format as Table | Cell Styles | Insert | Delete | Format | Ideas

Clipboard Font Alignment Protection Number Styles Cells Editing Ideas

A1

Sensitivity: General

EventList

Welcome to EventList - the Bas

Prerequisites:

Macros must be enabled. All bas

Baselines are part of the **Security**

How to use:

Step 1: Import the baselines.

Import Baselines

Step 2: Choose a baseline from the

Step4: Delete all imported baselines

Delete all imported baseli

ccount Logon	Audit Credential Validation	4774	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4774	Success and Failure
ccount Logon	Audit Credential Validation	4775	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4775	Success and Failure
ccount Logon	Audit Credential Validation	4776	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4776	Success and Failure
ccount Logon	Audit Credential Validation	4777	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4777	Success and Failure
ccount Management	Audit Security Group Management	4727	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4737	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4728	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4729	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4730	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4731	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4731	Success
ccount Management	Audit Security Group Management	4732	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4732	Success
ccount Management	Audit Security Group Management	4731	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4731	Success
ccount Management	Audit Security Group Management	4733	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4733	Success
ccount Management	Audit Security Group Management	4734	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4734	Success
ccount Management	Audit Security Group Management	4735	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4735	Success
ccount Management	Audit Security Group Management	4754	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4755	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4756	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4757	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4758	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management	Success
ccount Management	Audit Security Group Management	4764	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4764	Success
ccount Management	Audit Security Group Management	4799	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4799	Success and Failure
ccount Management	Audit User Account Management	4720	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4720	Success and Failure
ccount Management	Audit User Account Management	4722	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4722	Success and Failure

MITRE ATT&CK

Impact

Execution

Initial Access

Discovery

Persistence

Privilege Escalation

Defense Evasion

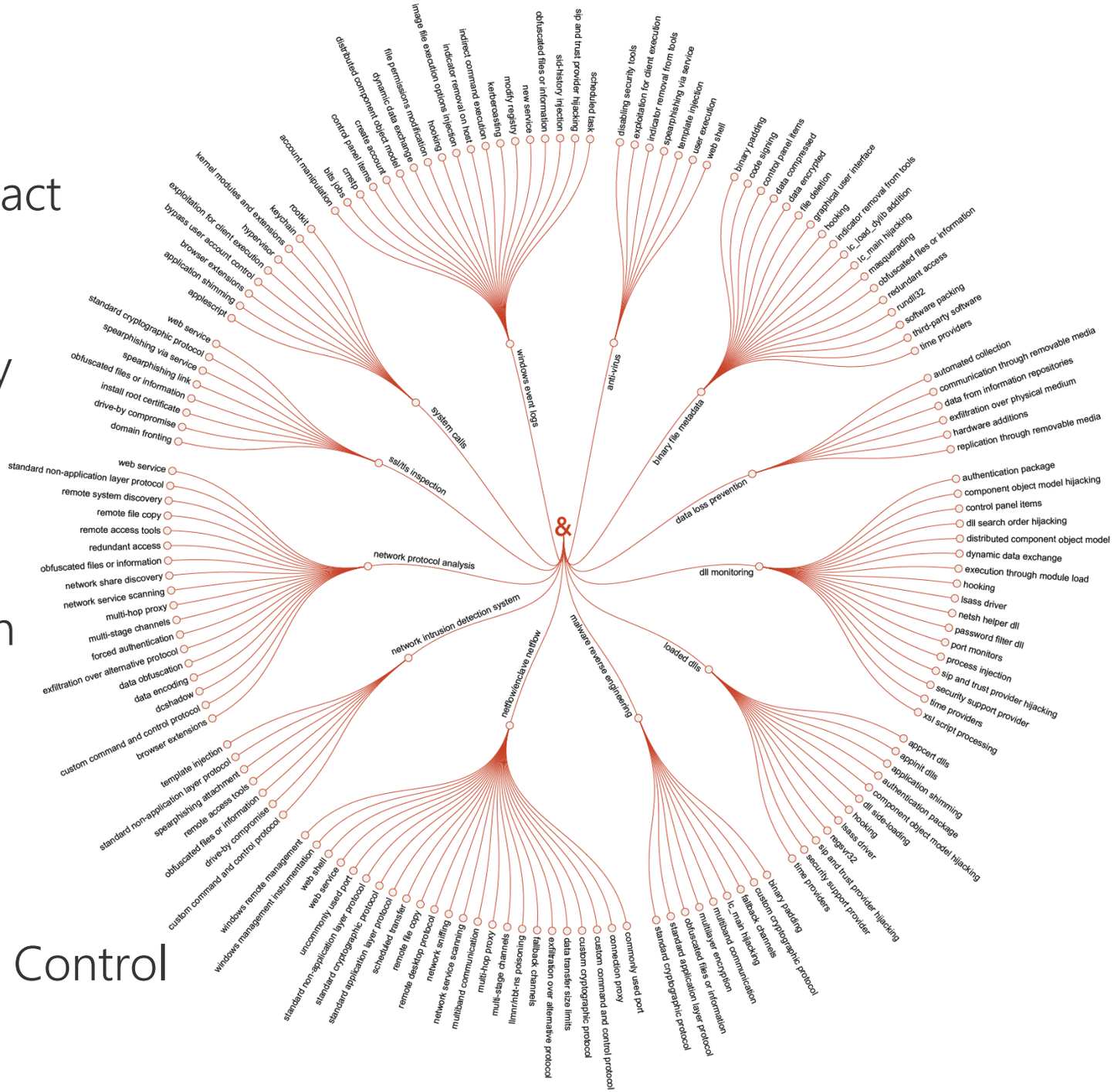
Collection

Exfiltration

Credential Access

Command and Control

Lateral Movement



MATRICES

PRE-ATT&CK

Enterprise

All Platforms

Linux

macOS

Windows

Mobile

Home > Matrices > Enterprise

&CK™ Navigator

Enterprise Matrix

The full ATT&CK Matrix

Last Modified: 2019-04-25 20

Initial Access	Execut									Impact
Drive-by Compromise	AppleSc									Data Destruction
Exploit Public-Facing Application	CMSTP									Data Encrypted for Impact
External Remote Services	Command-L Interface									Defacement
Hardware Additions	Compiled HTML									Disk Content Wipe
Replication Through Removable Media	Control Panel Ite									Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange									dpoint Denial of Service
Spearphishing Link	Execution through API									Firmware orruption
Spearphishing via Service	Execution through Module Load									it System ecovery
Supply Chain Compromise	Exploitation for Client Execution									rk Denial ervice
Trusted Relationship	Graphical User Interface								Fallback Channels	Resource Hijacking
Valid Accounts	InstallUtil		Weakness	Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels	Runtime Data Manipulation
	LSASS Driver	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Process Discovery	SSH Hijacking	Screen Capture	Multi-hop Proxy	Service Stop

Pass the Hash

Pass the hash (PtH) is a method of authenticating as a user without having access to the user's cleartext password. This method bypasses standard authentication steps that require a cleartext password, moving directly into the portion of the authentication that uses the password hash. In this technique, valid password hashes for the account being used are captured using a Credential Access technique. Captured hashes are used with PtH to authenticate as that user. Once authenticated, PtH may be used to perform actions on local or remote systems.

Windows 7 and higher with KB2871997 require valid domain user credentials or RID 500 administrator hashes. [1]

ID: T1075
Tactic: Lateral Movement
Platform: Windows
System Requirements: Requires Microsoft Windows as target system
Data Sources: Authentication logs
Contributors: Travis Smith, Tripwire
Version: 1.0

Examples

Name	Description
APT1	The APT1 group is known to have used pass the hash.[2]
APT28	APT28 has used pass the hash for lateral movement.[3]
APT32	APT32 has used pass the hash for lateral movement.[4]
Cobalt Strike	Cobalt Strike can perform pass the hash.[5]
Empire	Empire can perform pass the hash attacks.[6]
HOPLIGHT	HOPLIGHT has been observed loading several APIs associated with Pass the Hash. [7]

MITRE ATT&CK

Impact

Execution

Initial Access

Discovery

Persistence

Privilege Escalation

Defense Evasion

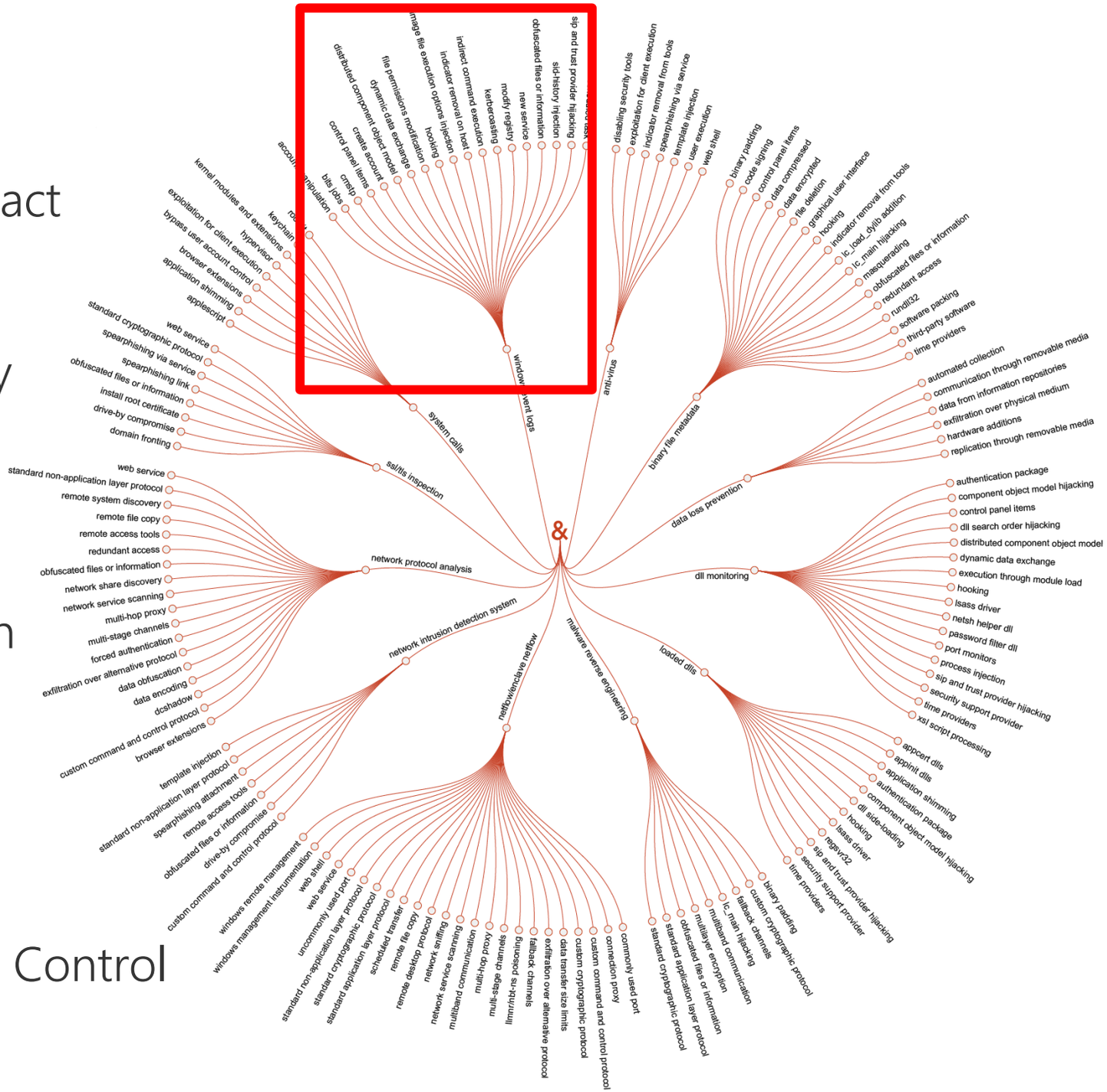
Collection

Exfiltration

Credential Access

Command and Control

Lateral Movement




scheduled task
sip and trust provider hijacking
sid-history injection
obfuscated files or information
new service
modify registry
kerberoasting
indirect command execution
indicator removal on host
image file execution options injection
hooking
file permissions modification
dynamic data exchange
distributed component object model
create account
control panel items
cmstp
bits jobs
account manipulation
windows event logs
system calls
ssl/tls inspe
rootkit
kernel modules and extens
hypervisor
user account control
browser extensions
applescript
service
binary file metadata
web shell
user execution
template injection
spearphishing via service
indicator removal from tools
exploitation for client execution
disabling security tools

Hunting queries?

Which events should be forwarded?

Which events will be generated?

Demo

EventList

SIGMA

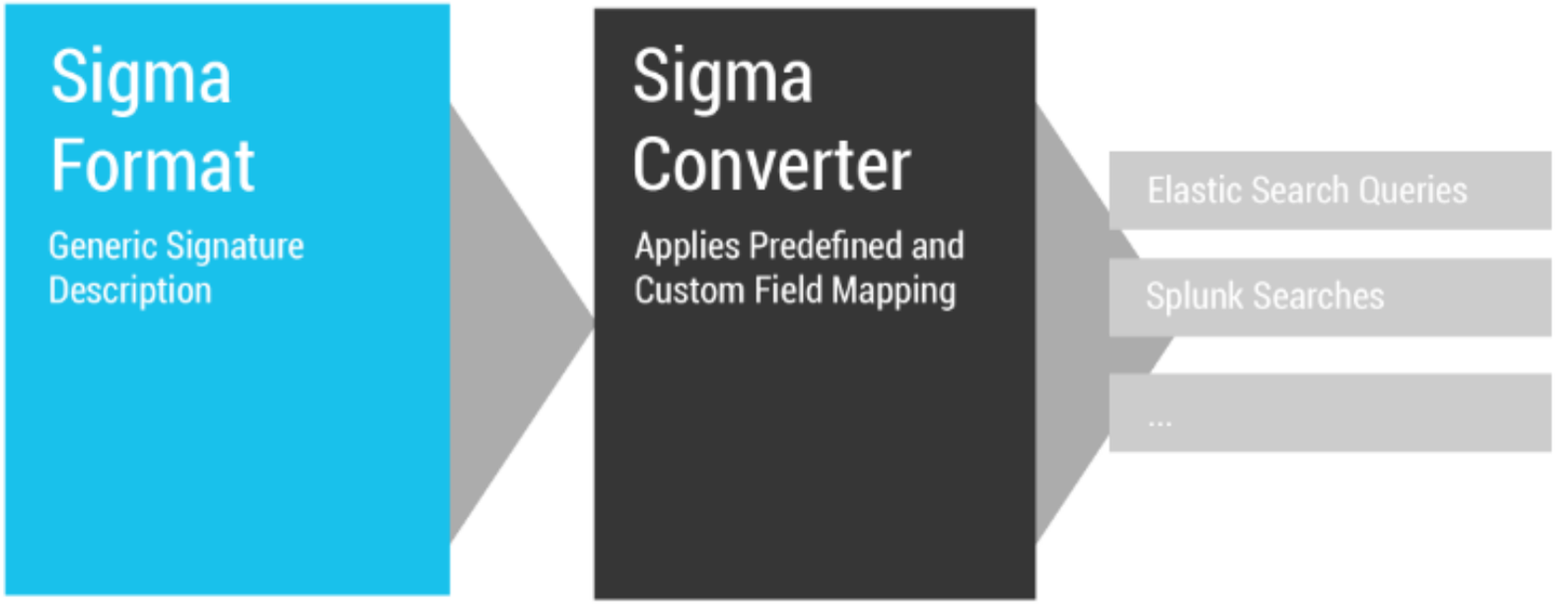
https://github.com/Neo23x0/sigma

Supported Targets

- Splunk (plainqueries and dashboards)
- ElasticSearch Query Strings
- ElasticSearch Query DSL
- Kibana
- Elastic X-Pack Watcher
- Logpoint
- Windows Defender Advanced Threat Protection (WDATP)
- Azure Sentinel / Azure Log Analytics
- ArcSight
- QRadar
- Qualys
- RSA NetWitness
- PowerShell
- Grep with Perl-compatible regular expression support

Current work-in-progress

- Splunk Data Models



Contribute to EventList

- Are you interested in contributing to EventList...
  - ...to improve it?
  - ...to implement new features?
  - ...to implement cross-platform support?
- What are your ideas and suggestions for EventList?

- GitHub: https://github.com/miriamxyra/EventList
  - Create a Pull Request for the „development branch“

- Contact me:
  - @miriamxyra

Thank you!

Follow me on Twitter: @miriamxyra
https://miriamxyra.com

Slides: https://github.com/miriamxyra/Presentations