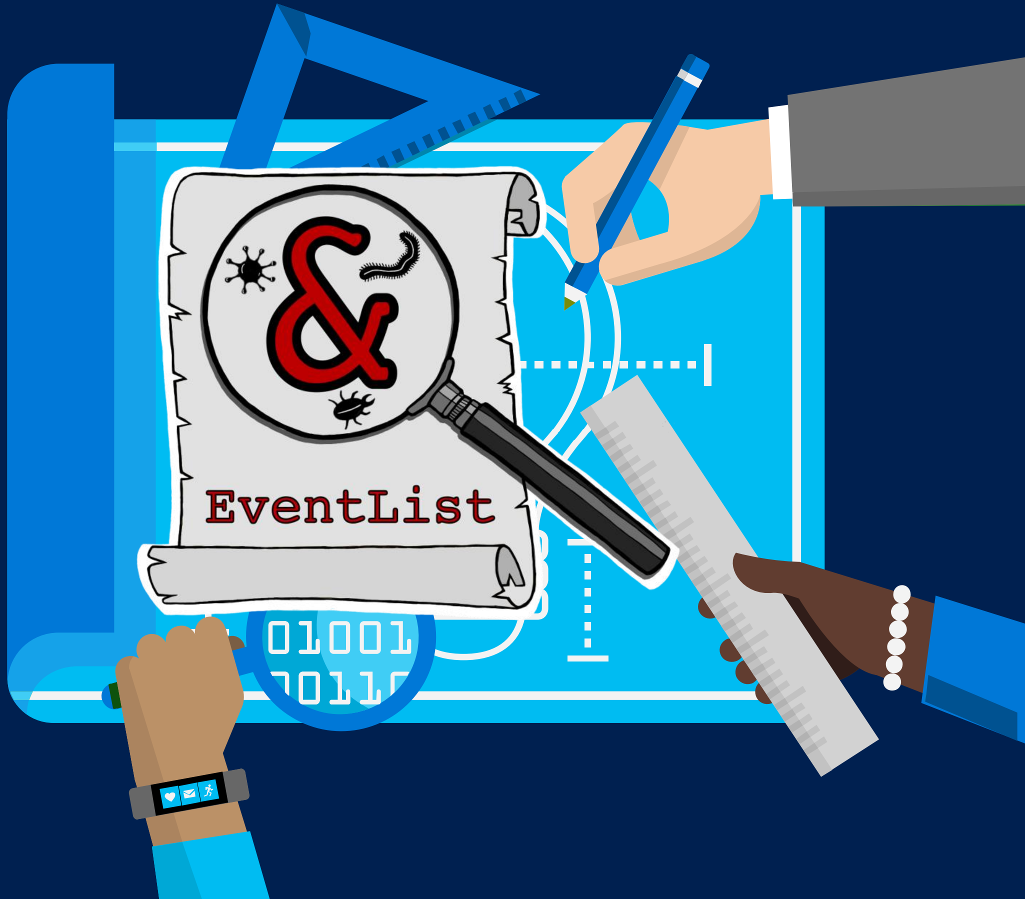
Microsoft

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.

No Ninjacats or Unicorns were harmed in the process of creating this tool.

MITRE ATT&CK

Impact

Execution

Initial Access

Discovery

Persistence

Privilege Escalation

Defense Evasion

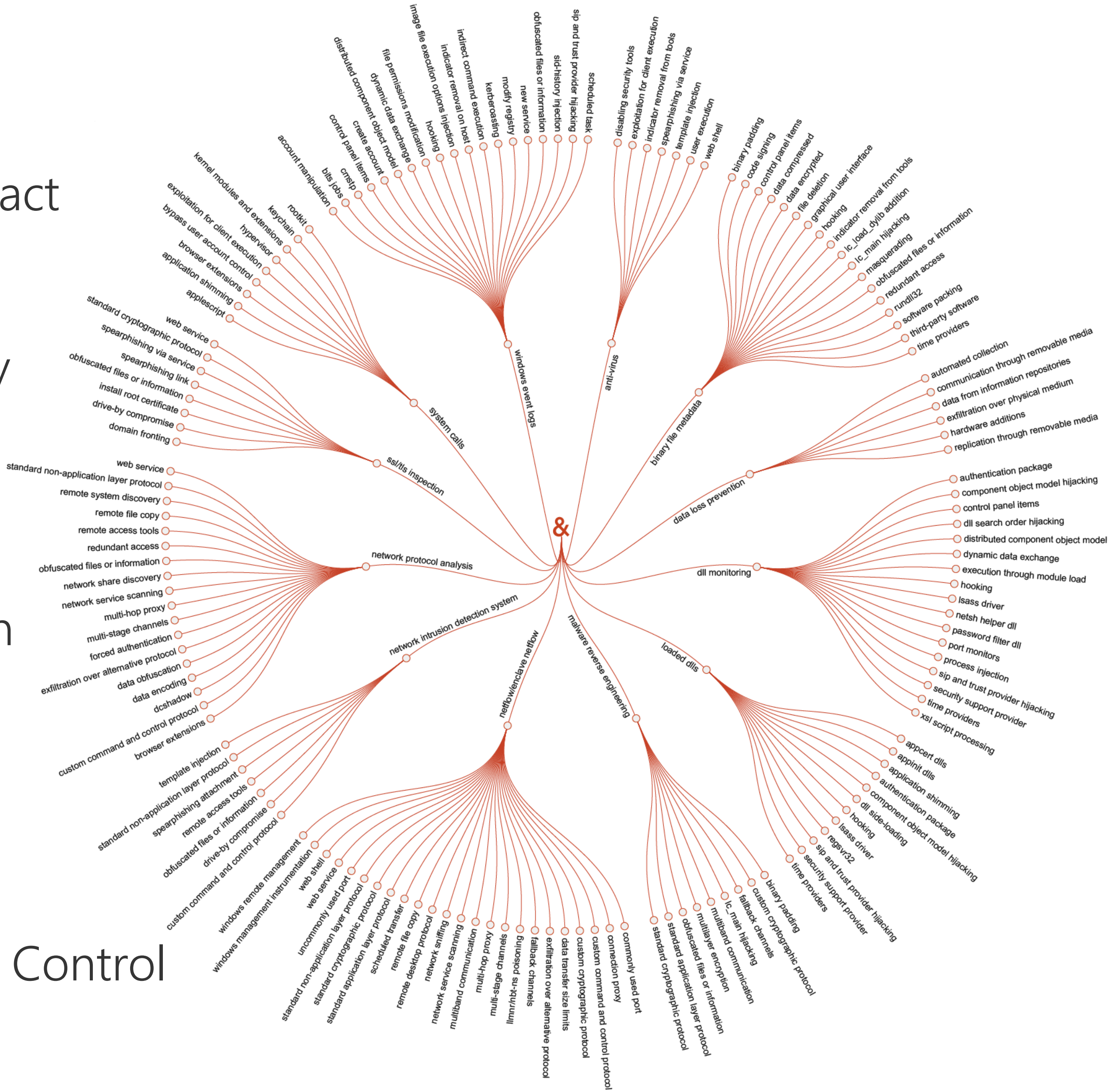
Collection

Exfiltration

Credential Access

Command and Control

Lateral Movement



MITRE ATT&CK

Impact

Execution

Initial Access

Discovery

Persistence

Privilege Escalation

Defense Evasion

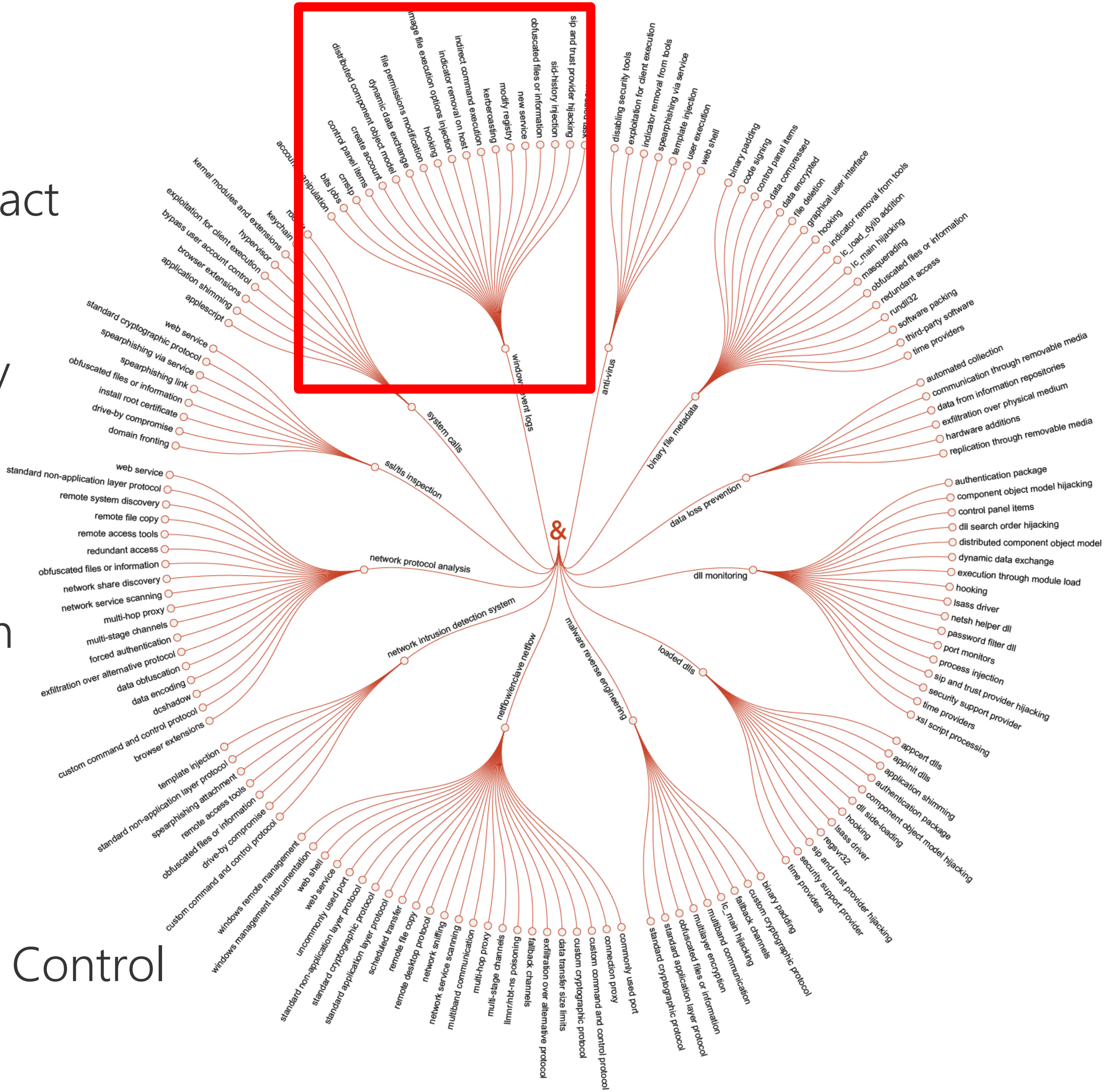
Collection

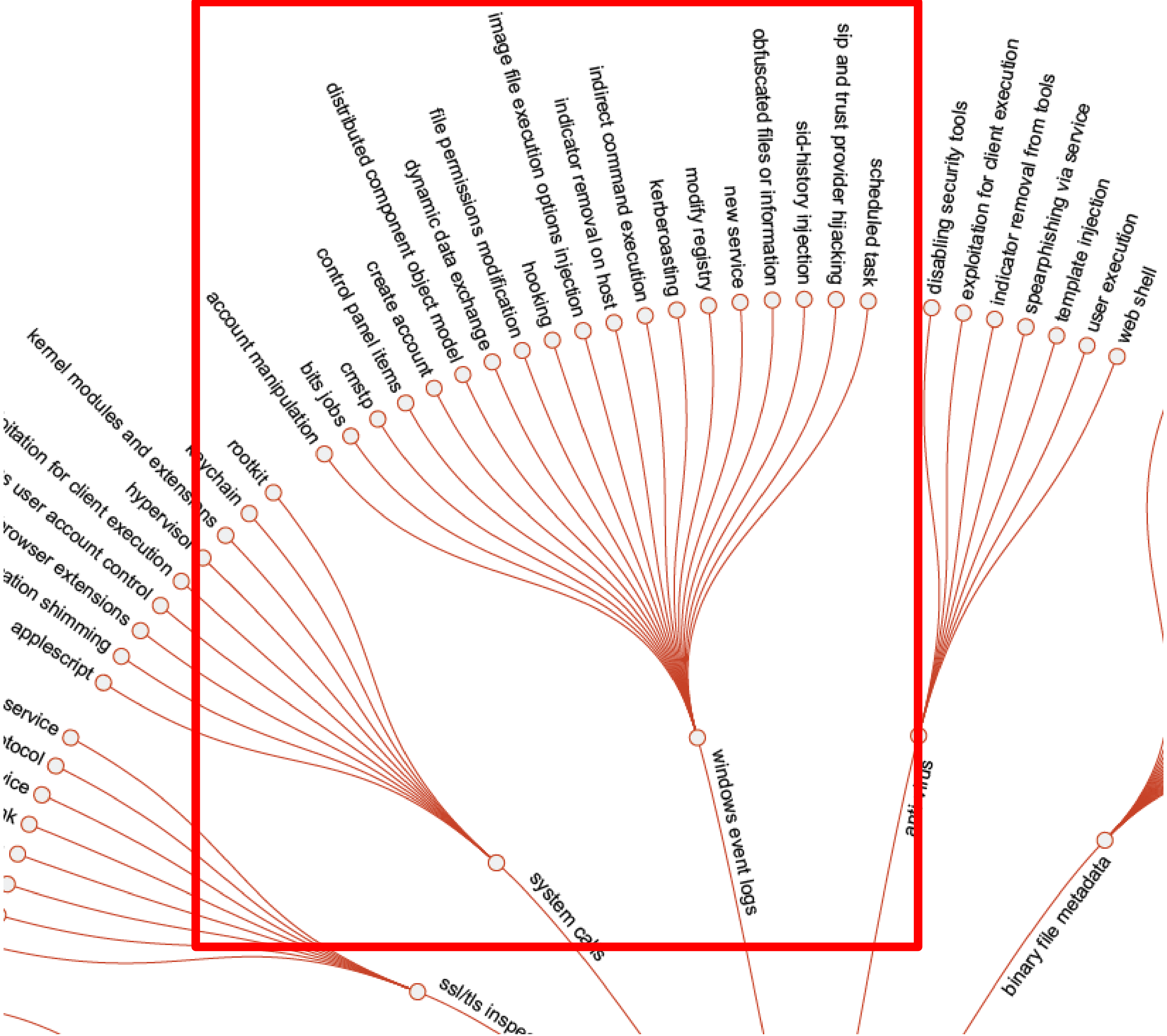
Exfiltration

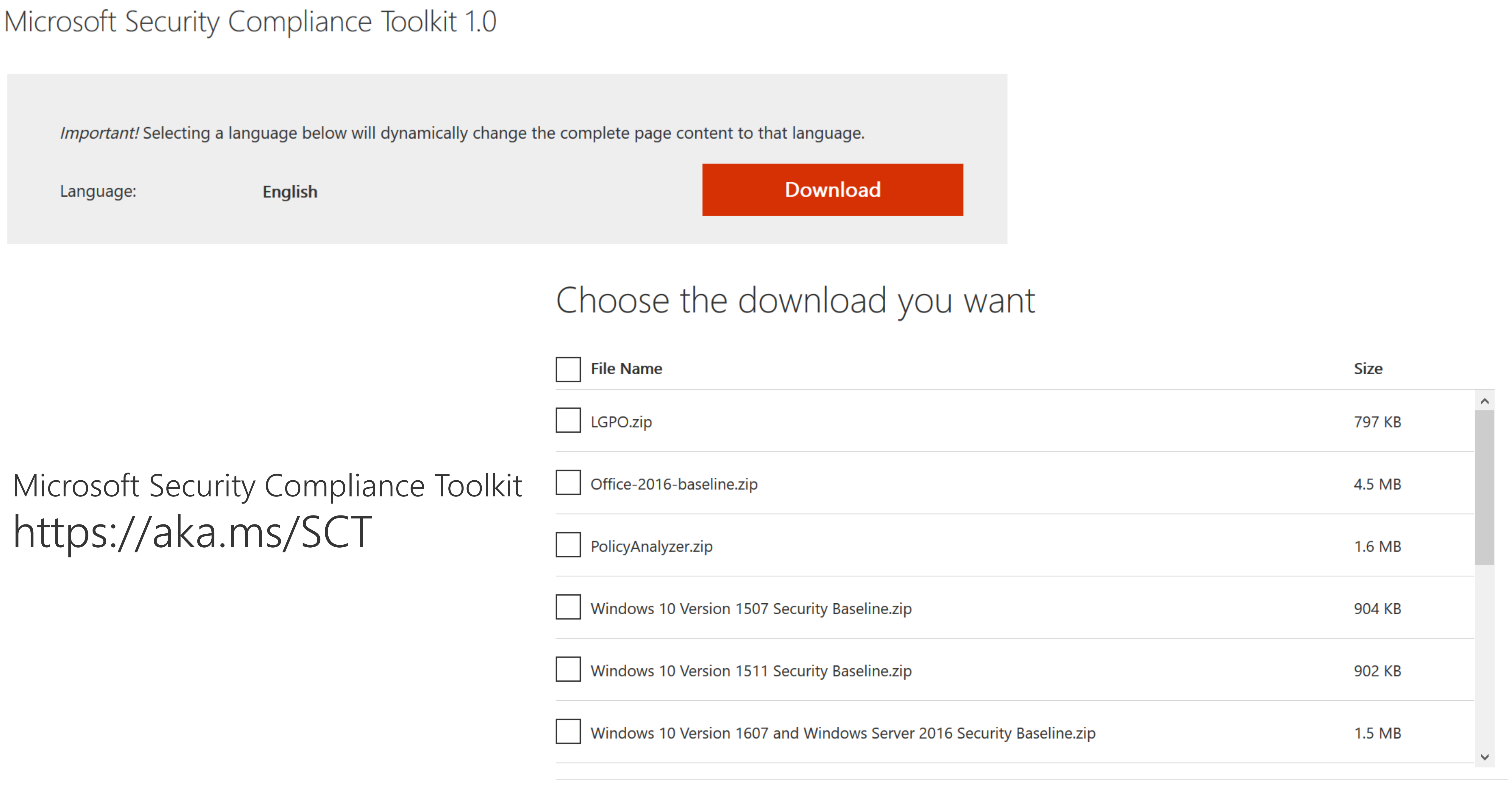
Credential Access

Command and Control

Lateral Movement




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



Microsoft Security Compliance Toolkit 1.0

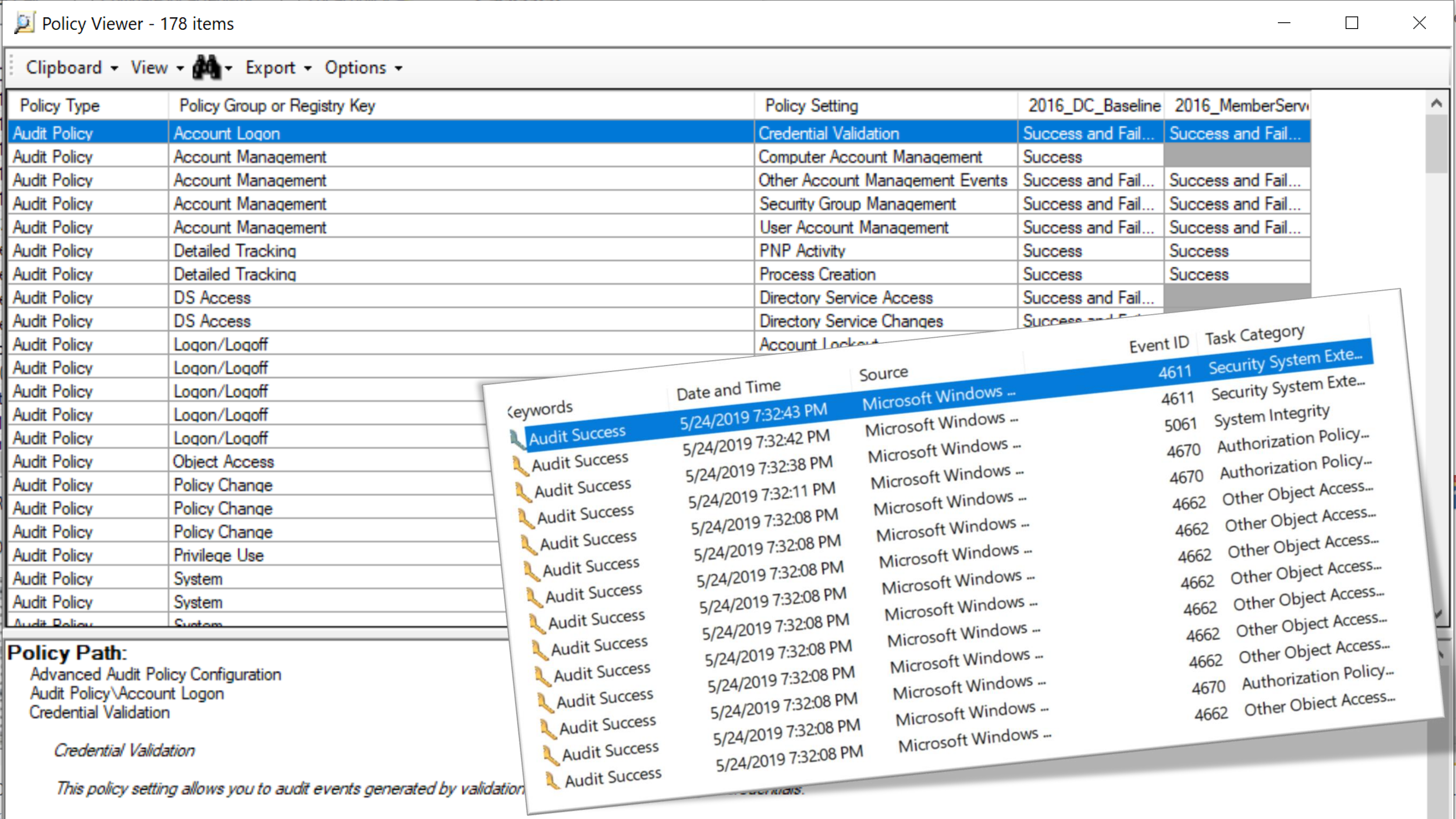
Important! Selecting a language below will dynamically change the complete page content to that language.

Language: **English**

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 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	Success and Fail...	
Audit Policy	Logon/Logoff	Account Lockout		
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			
Audit Policy	System			

Policy Path:
Advanced Audit Policy Configuration
Audit Policy\Account Logon
Credential Validation

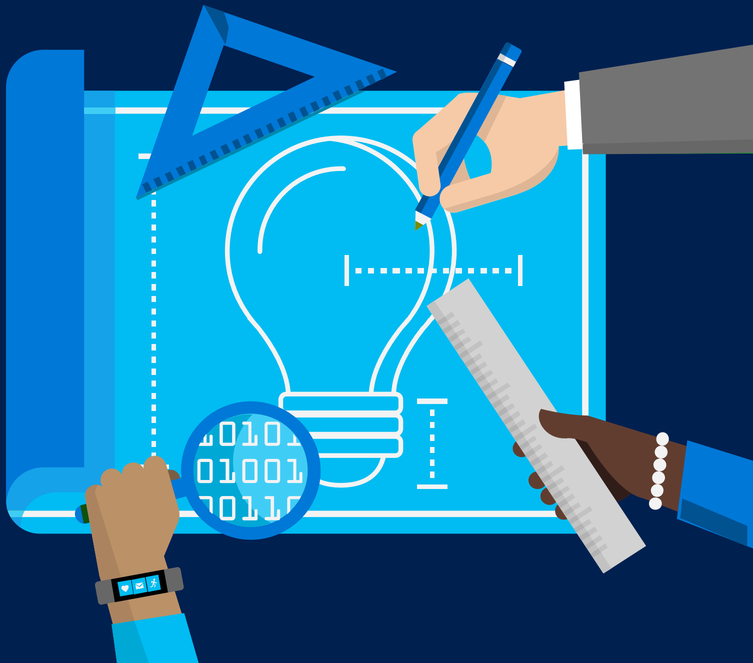
Credential Validation

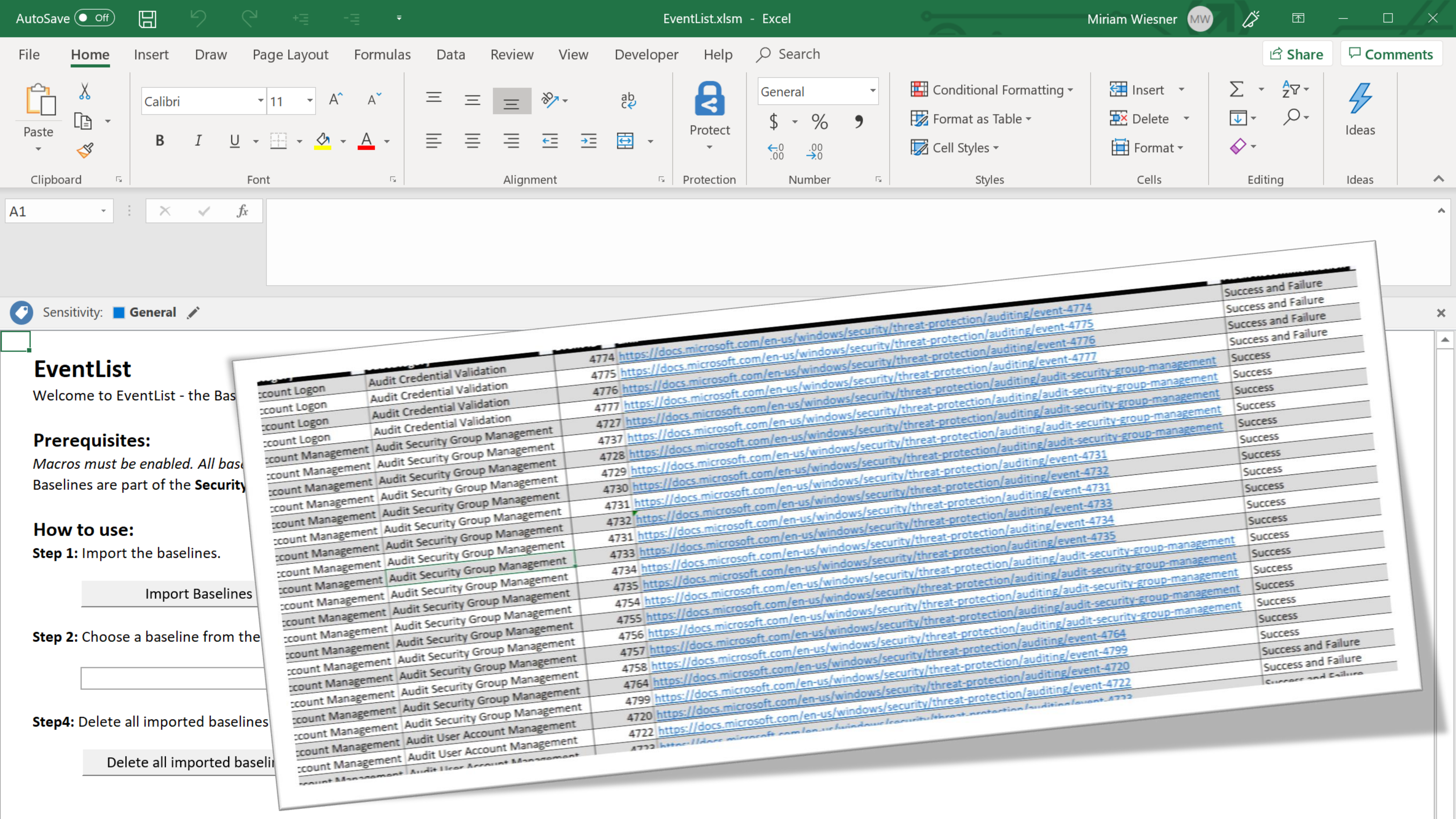
This policy setting allows you to audit events generated by validation ... *credentials.*

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...

1994. 11
2003 (11)
2002 (11)
2001 (11)
1992 (11)

EventList 1.0





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
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
ccount Management	Audit User Account Management	4723	https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4723	

Hunting queries?

Which events should be forwarded?

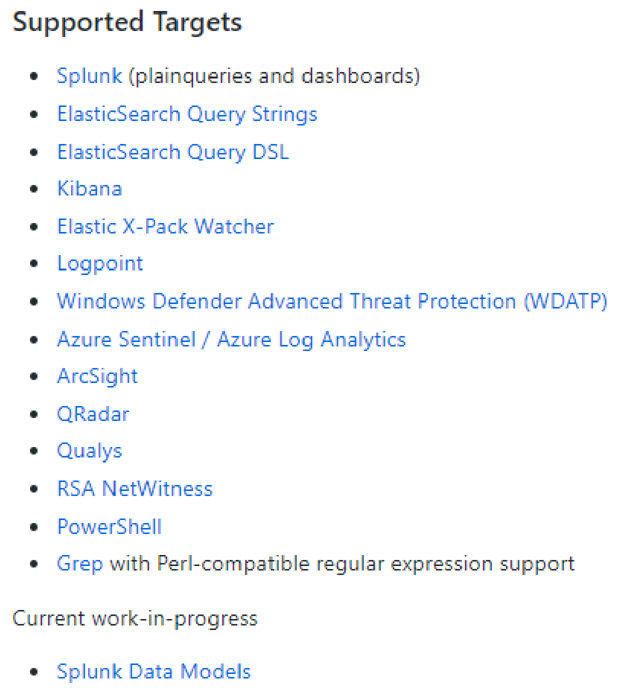
Which events will be generated?

Demo

EventList

SIGMA

https://github.com/Neo23x0/sigma

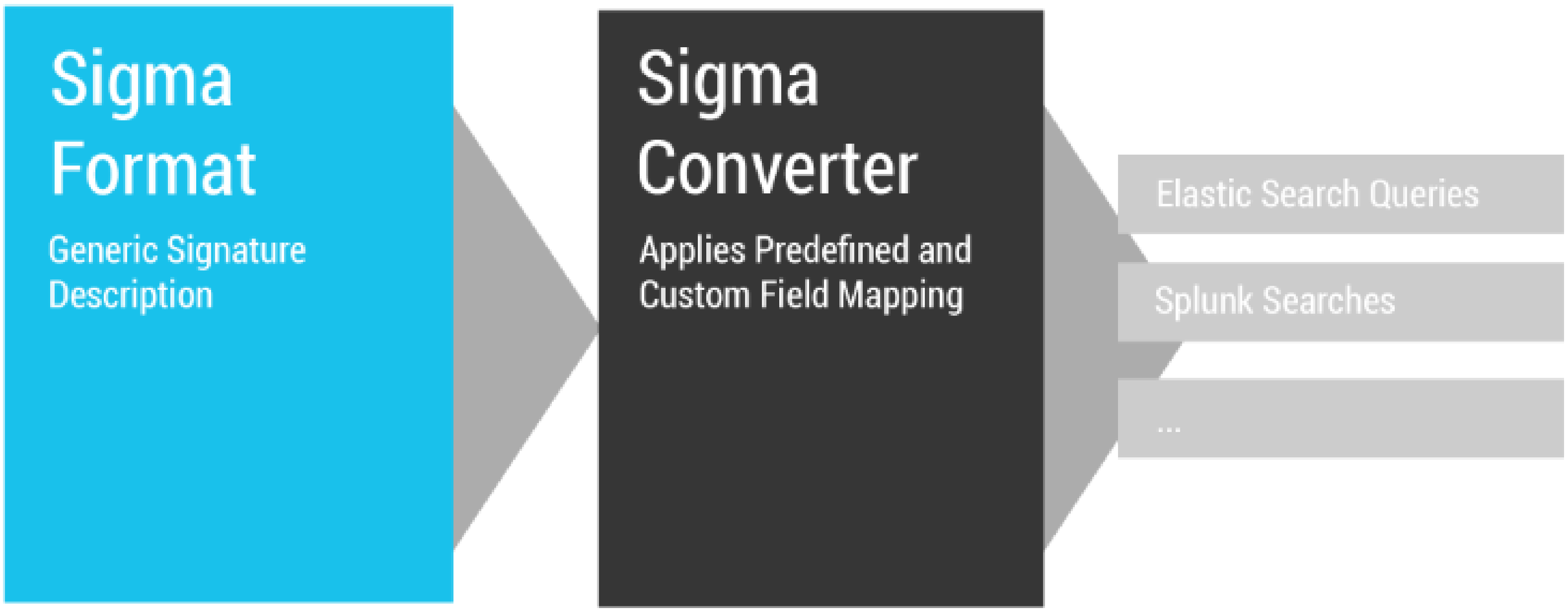


Supported Targets

- 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


Sigma Format
Generic Signature Description
Sigma Converter
Applies Predefined and Custom Field Mapping
Elastic Search Queries
Splunk Searches
...

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