
black hat
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS
EventList
EventList
What the log?! So many events, so little time...
Miriam Wiesner
#BHUSA @BLACK HAT EVENTS

Miriam Wiesner

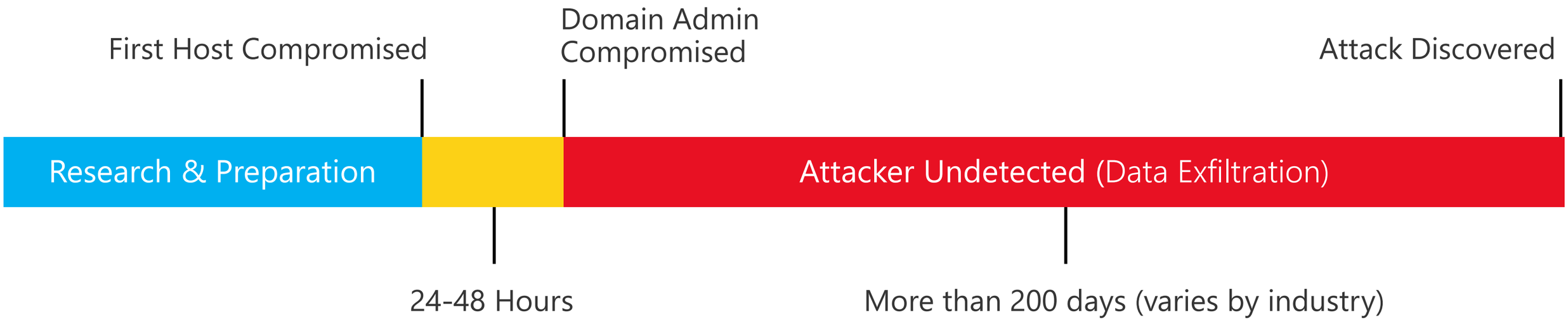
Security Program Manager for Microsoft Defender ATP

@miriamxyra

https://miriamxyra.com

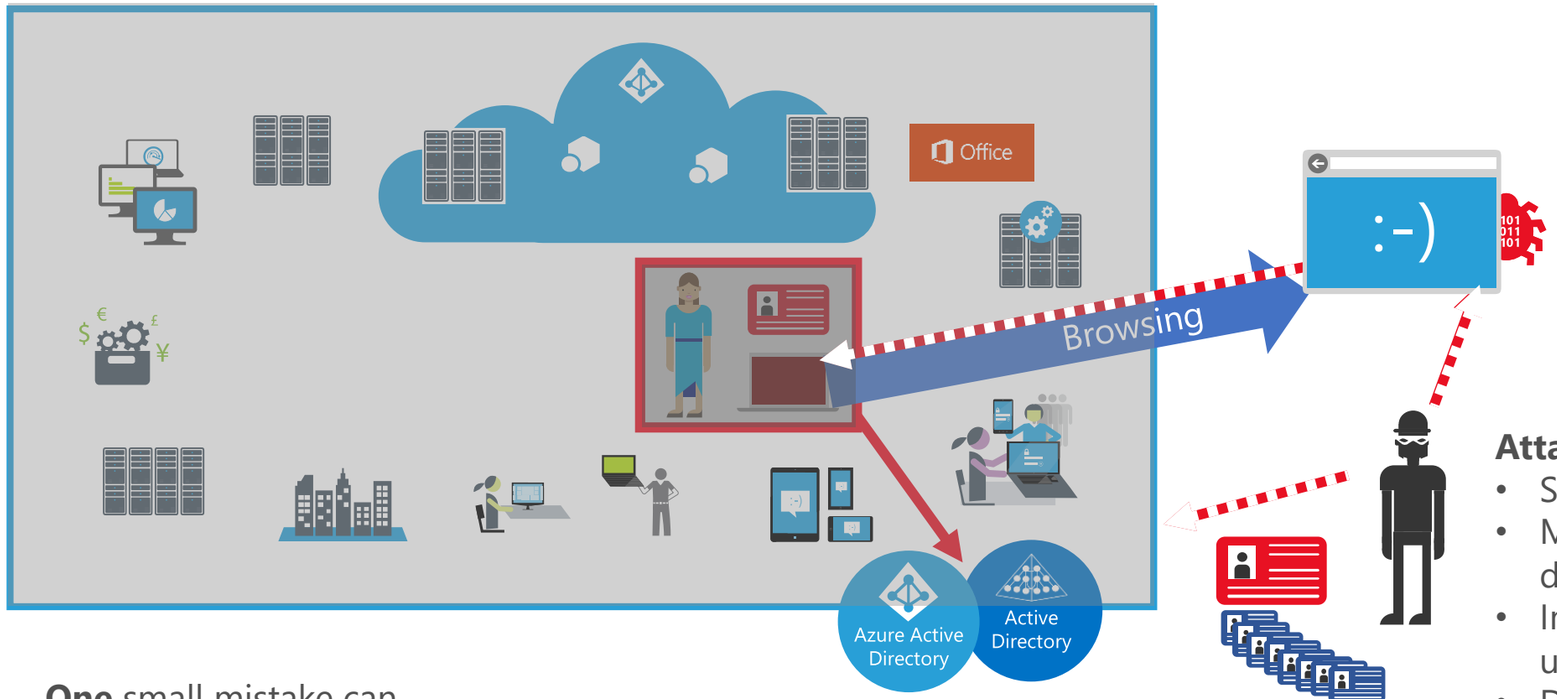
Disclaimer

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


First Host Compromised
Domain Admin Compromised
Attack Discovered
Research & Preparation
Attacker Undetected (Data Exfiltration)
24-48 Hours
More than 200 days (varies by industry)

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

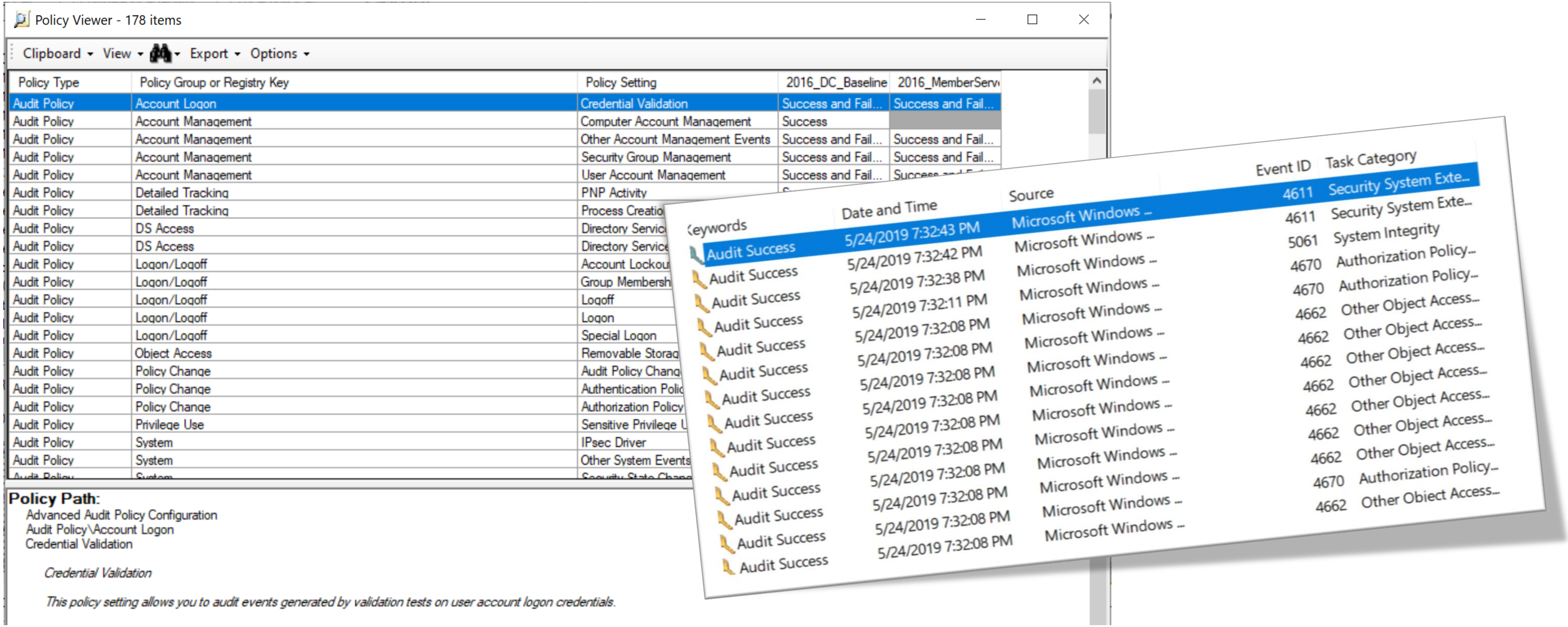
Download

Choose the download you want

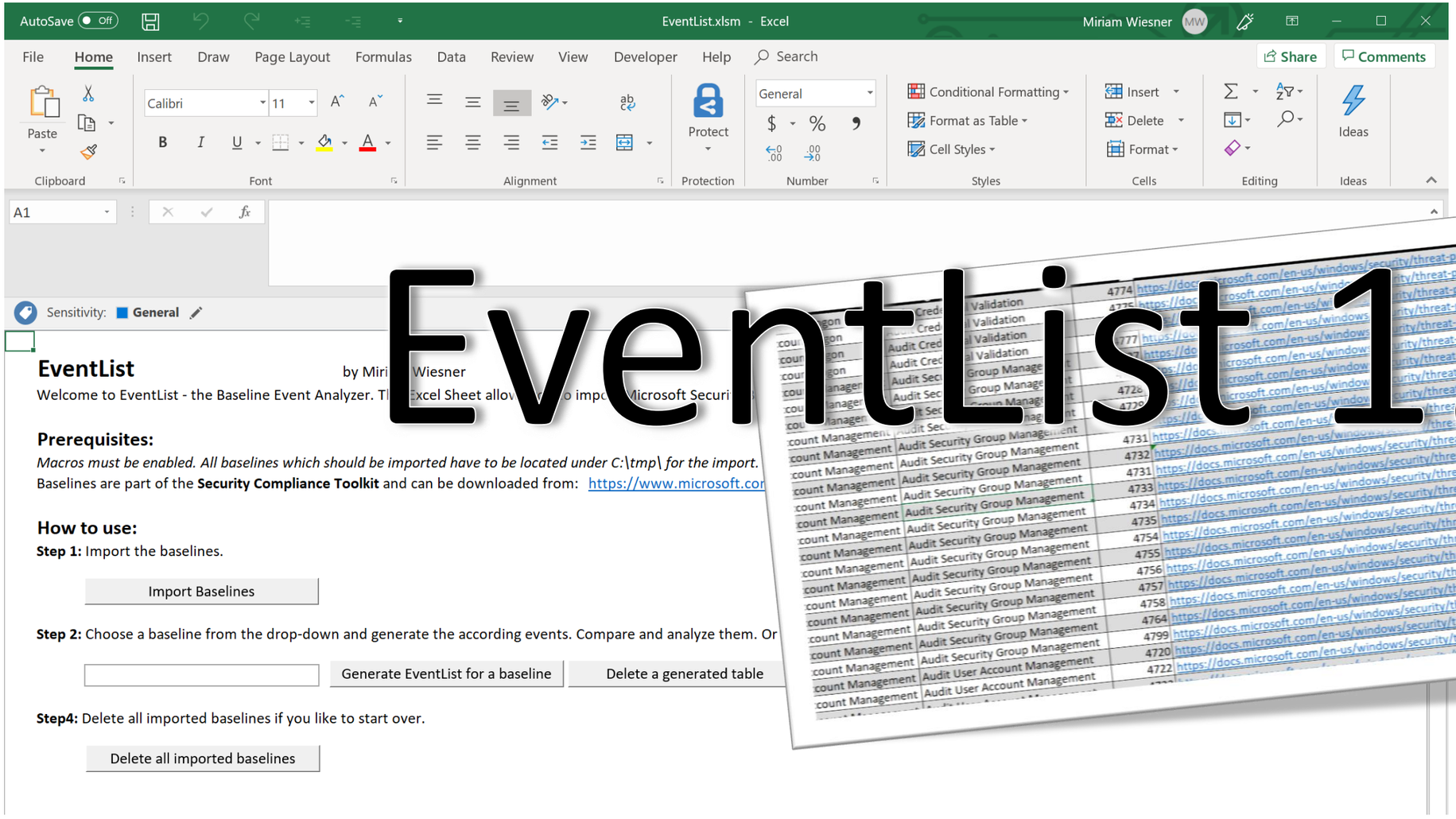
File Name	Size
LGPO.zip	797 KB
Office-2016-baseline.zip	4.5 MB
PolicyAnalyzer.zip	1.6 MB
Windows 10 Version 1507 Security Baseline.zip	904 KB
Windows 10 Version 1511 Security Baseline.zip	902 KB
Windows 10 Version 1607 and Windows Server 2016 Security Baseline.zip	1.5 MB

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...
Audit Policy | Detailed Tracking | PNP Activity
Audit Policy | Detailed Tracking
Audit Policy | DS Access
Audit Policy | DS Access
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff
Audit Policy | Logon/Logoff | Logoff
Audit Policy | Logon/Logoff | Logon
Audit Policy | Logon/Logoff | Special Logon
Audit Policy | Object Access
Audit Policy | Policy Change
Audit Policy | Policy Change
Audit Policy | Policy Change
Audit Policy | Privilege Use
Audit Policy | System | IPsec Driver
Audit Policy | System | Other System Events
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 tests on user account logon 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...
Audit Success


1994. II
1992 II
2003 II
2002 II
2001 II



EventList1.0

MITRE ATT&CK

Impact

Execution

Initial Access

Credential Access

Persistence

Privilege Escalation

Defense Evasion

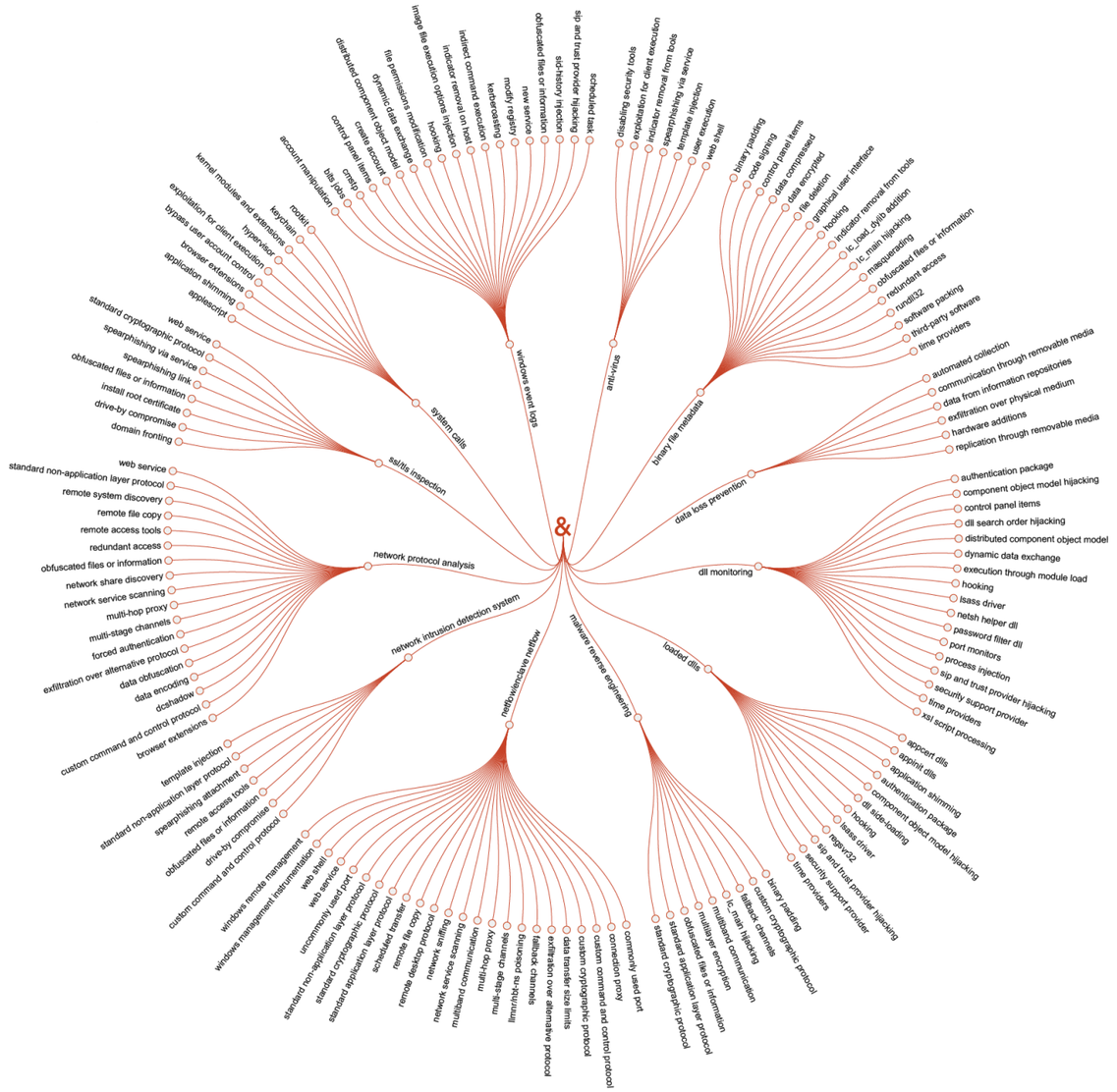
Lateral Movement

Discovery

Exfiltration

Command and Control

Collection



MATRICES

PRE-ATT&CK

Enterprise

All Platforms

Linux

macOS

Windows

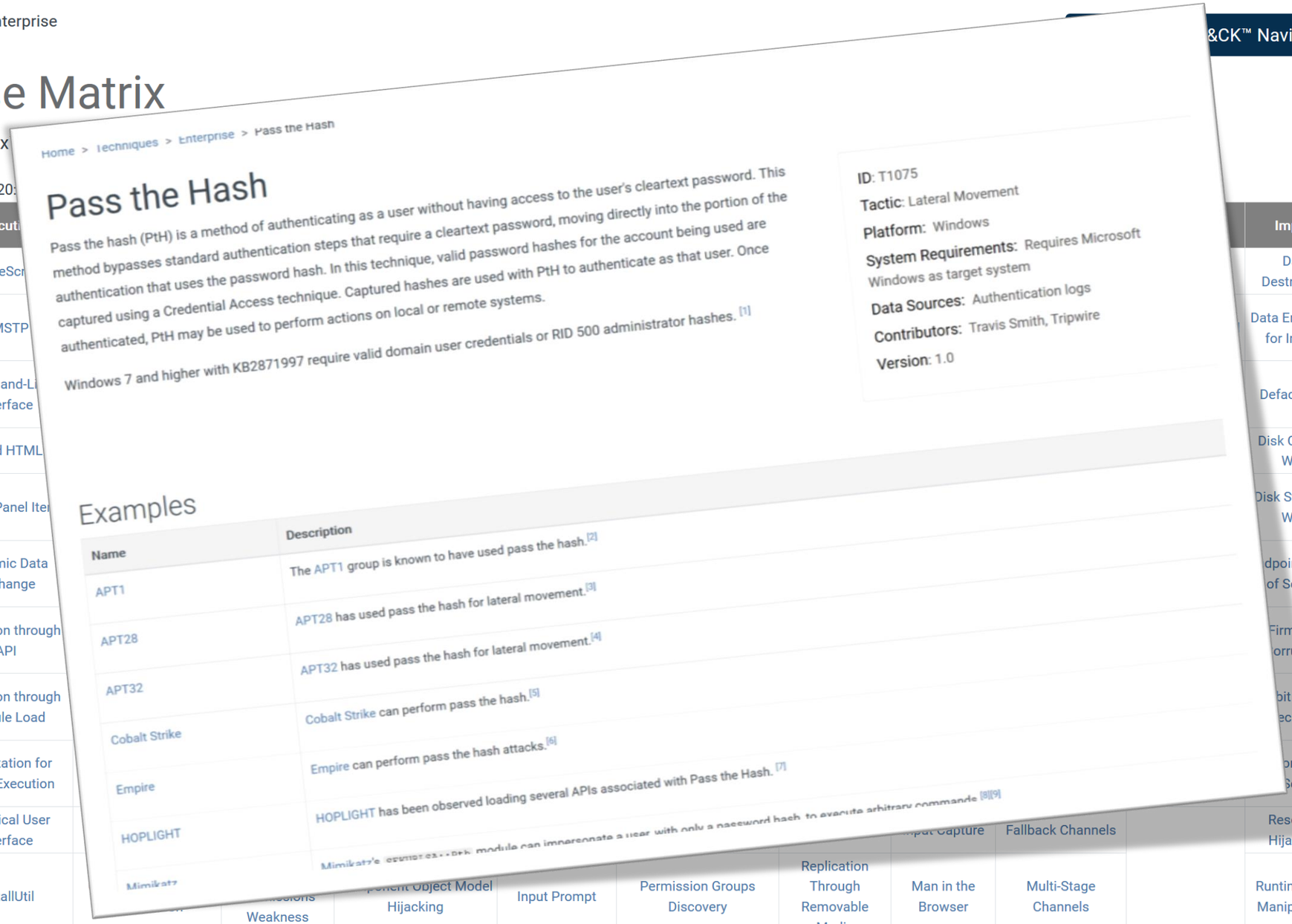
Mobile

Enterprise Matrix

The full ATT&CK Matrix

Last Modified: 2019-04-25 20:

Initial Access	Execution									Impact
Drive-by Compromise	AppleScr									Data Destruction
Exploit Public-Facing Application	CMSTP									Data Encrypted for Impact
External Remote Services	Command-Li 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									bit System ecovery
Supply Chain Compromise	Exploitation for Client Execution									ork Denial Service
Trusted Relationship	Graphical User Interface									Resource Hijacking
Valid Accounts	InstallUtil		Weakness	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



Home > Techniques > Enterprise > Pass the Hash

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]
Mimikatz	Mimikatz's [illegible] module can impersonate a user, with only a password hash, to execute arbitrary commands.[8][9]

MITRE ATT&CK

Impact

Execution

Initial Access

Credential Access

Persistence

Privilege Escalation

Defense Evasion

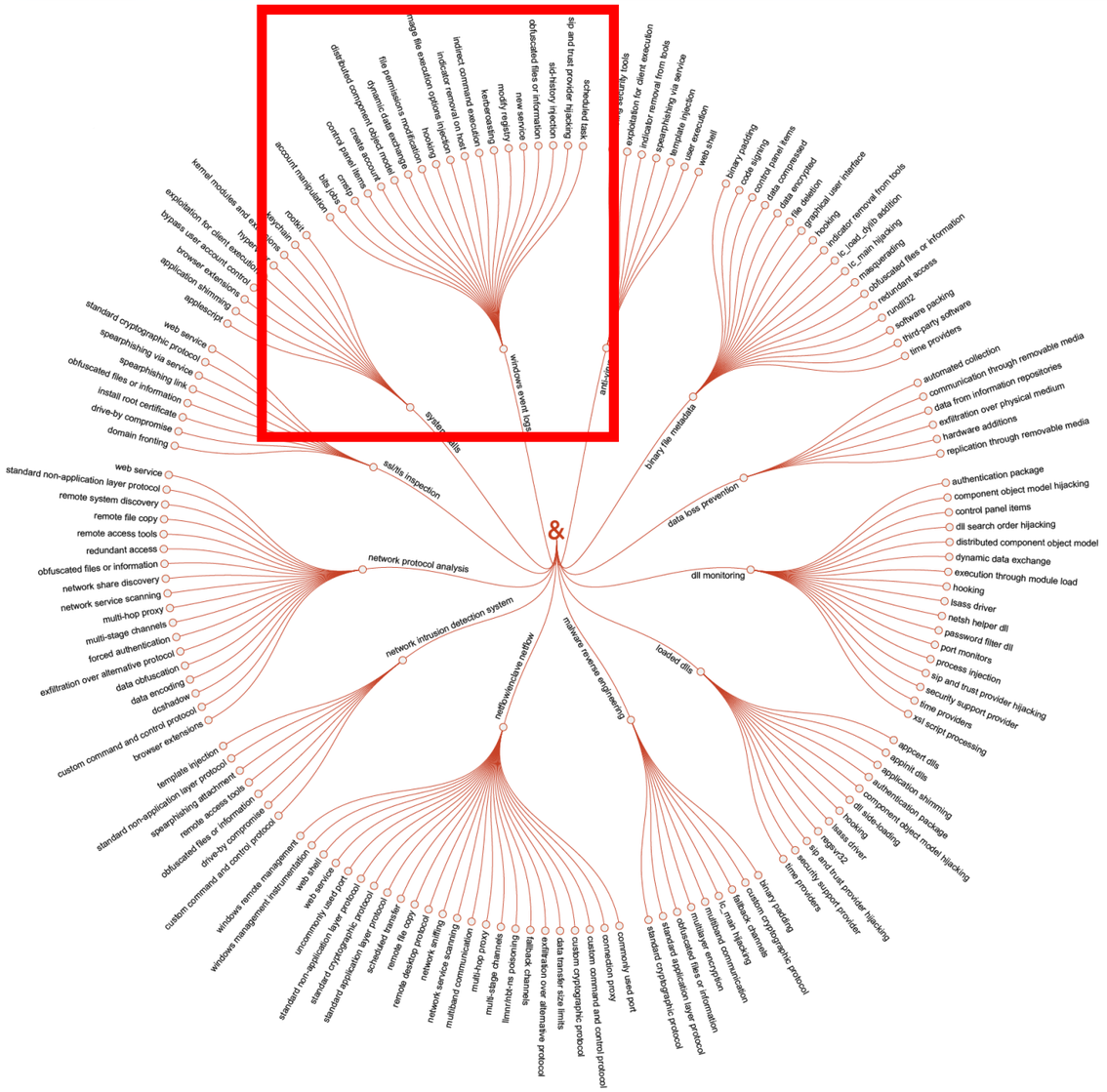
Lateral Movement

Discovery

Exfiltration

Command and Control

Collection




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
rootkit
kernel modules and extensions
hypervisor
applescript
service
disabling security tools
exploitation for client execution
indicator removal from tools
spearphishing via service
template injection
user execution
web shell
binary file metadata

Hunting queries?

Which events should be forwarded?

Which events will be generated?


black hat
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS
DEMO
#BHUSA @BLACK HAT EVENTS

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
  - miriam.wiesner@microsoft.com

black hat USA 2019

Thank you!

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