PowerShell Security at Enterprise Customers

David das Neves
Premier Field Engineer, Microsoft

David das Neves
PFE, Microsoft

Introduction

PowerShell Security?

Why PowerShell Security matters

Security Response

Candid Wueest

detect, react, protect

25 NOV 2015

View Profile

Symantec Official Blog

+6
6 Votes

PowerShell threats surge: 95.4 percent of analyzed scripts were malicious

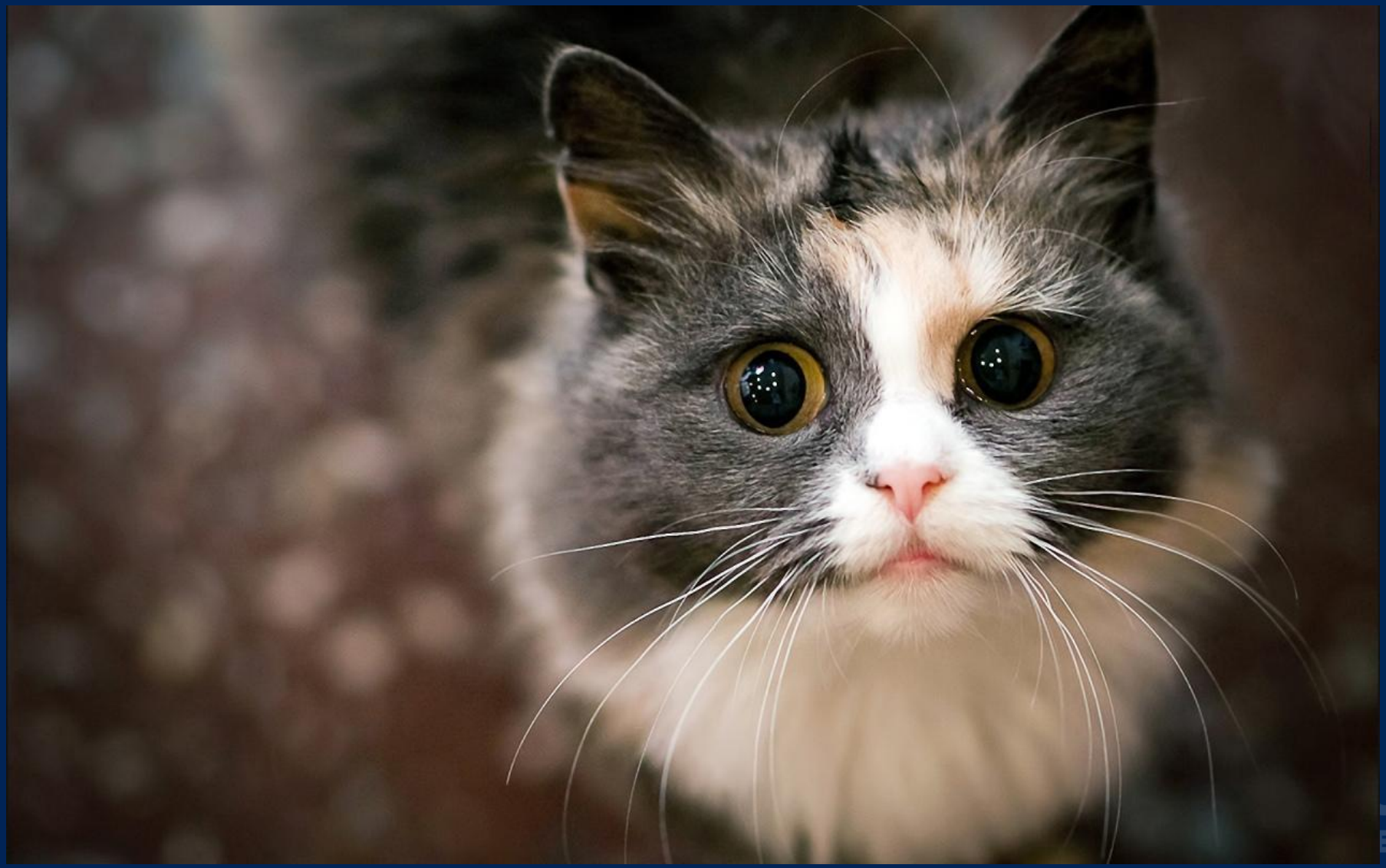
Symantec analyzed 111 threat families that use PowerShell, finding that they leverage the framework to download payloads and traverse through networks.

By: Candid Wueest SYMANTEC EMPLOYEE ACCREDITED

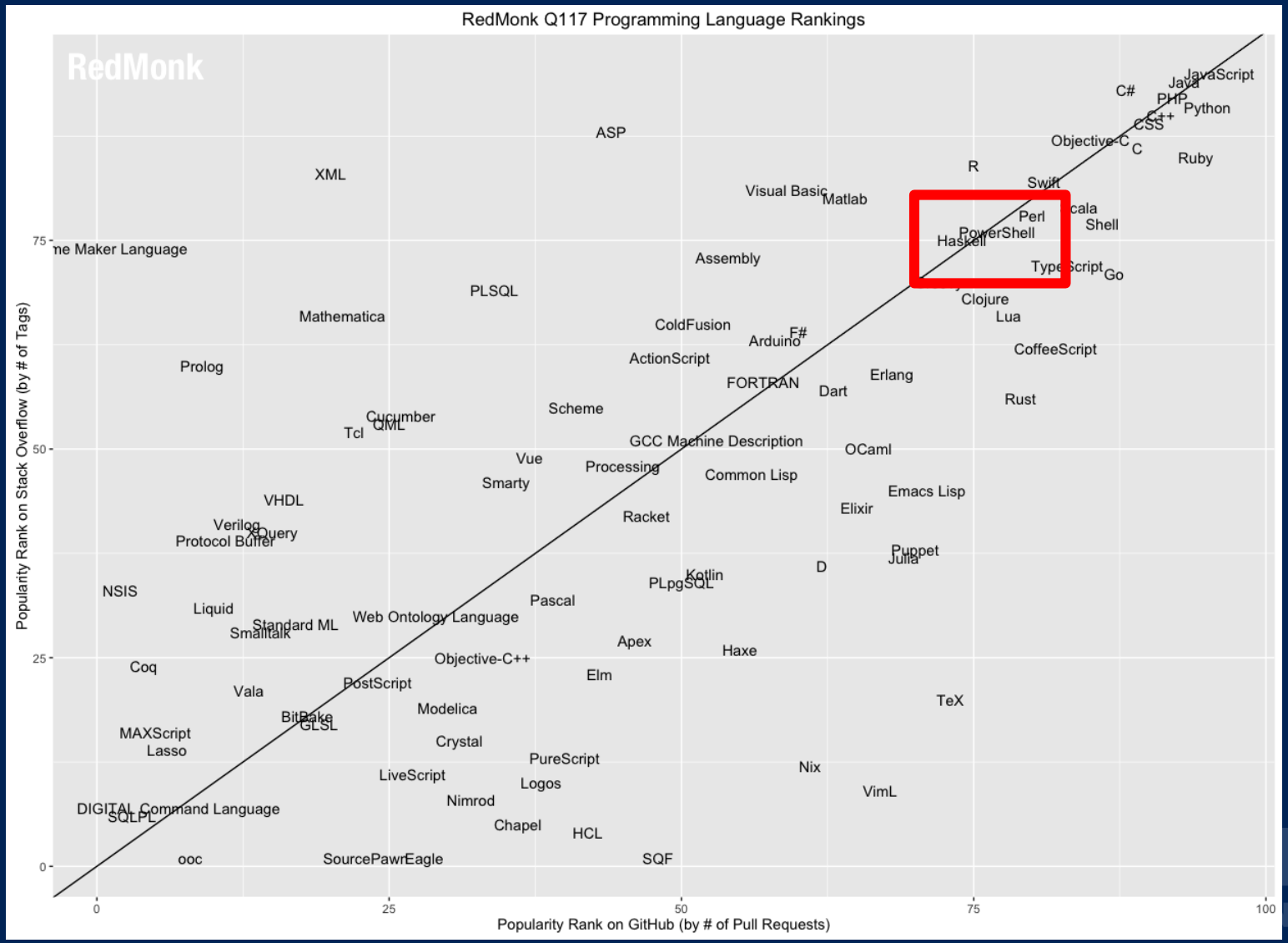
Created 08 Dec 2016 | 0 Comments | : 简体中文, 日本語

10 | 305 | Like 1

PowerShell is evil.



PowerShell is powerful



A Comparison of Shell and Scripting Language Security by Lee

- Event Logging
- Transcription
- Dynamic Evaluation Logging
- Application Whitelisting
- Antimalware Integration
- Local Sandboxing
- Remote Sandboxing
- Untrusted Input Tracking

A Comparison of Shell and Scripting Language Security

Engine	Event Logging	Transcription	Dynamic Evaluation Logging	Encrypted Logging	Application Whitelisting	Antimalware Integration	Local Sandboxing	Remote Sandboxing	Untrusted Input Tracking
Bash	No**	No*	No	No	Yes	No	No*	Yes	No
CMD / BAT	No	No	No	No	Yes	No	No	No	No
Jscript	No	No	No	No	Yes	Yes	No	No	No
LUA	No	No	No	No	No	No	No*	Yes	Yes
Perl	No	No	No	No	No	No	No*	Yes	Yes
PHP	No	No	No	No	No	No	No*	Yes	Yes
PowerShell	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No**
Python	No	No	No	No	No	No	No	No	No**
Ruby	No	No	No	No	No	No	No**	No**	Yes
sh	No**	No*	No	No	No	No	No*	Yes	No
T-SQL	Yes	Yes	Yes	No	No	No	No**	No**	No
VBScript	No	No	No	No	Yes	Yes	No	No	No
zsh	No**	No*	No	No	No	No	No*	Yes	No

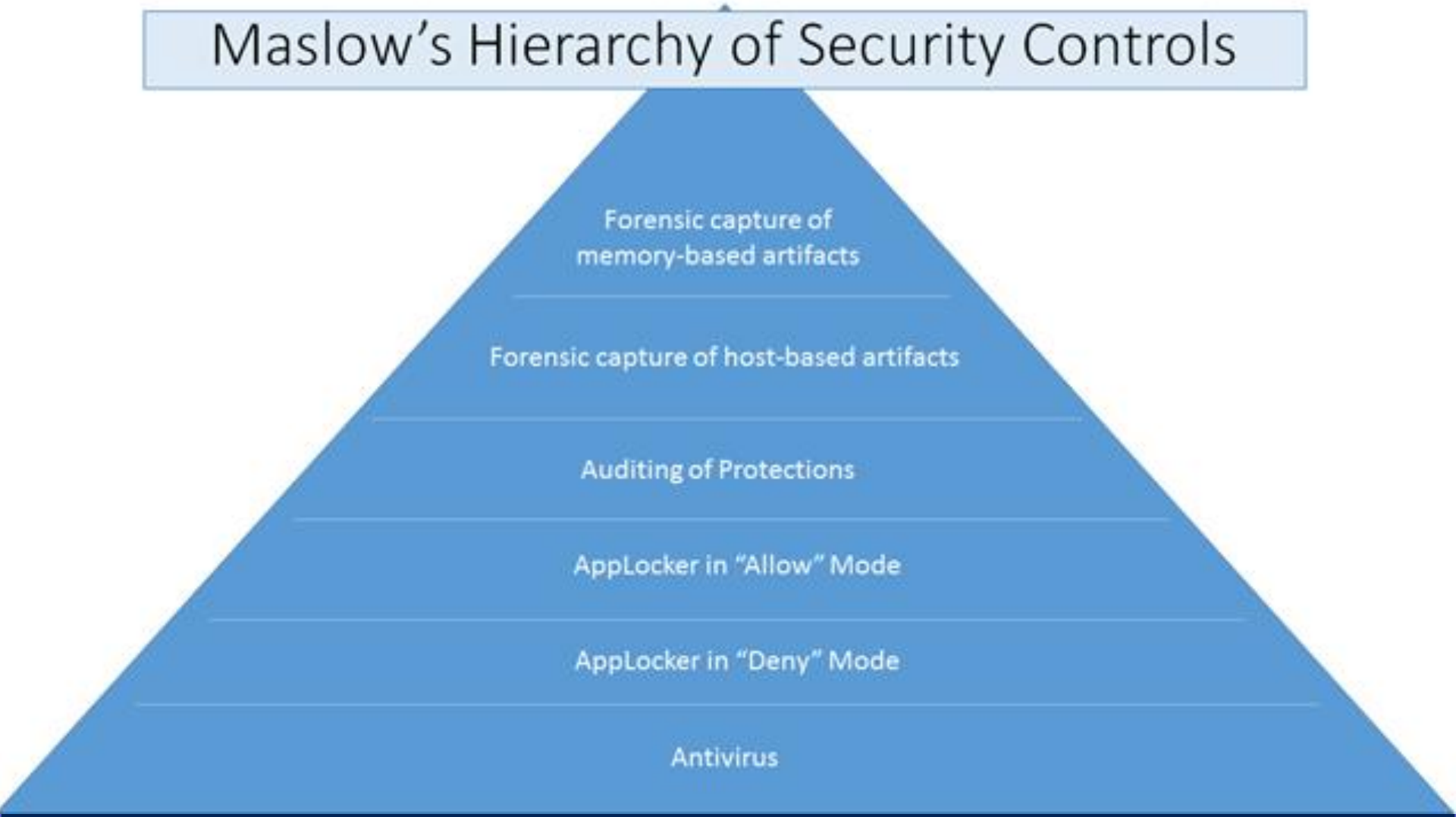
* Feature exists, but cannot enforce by policy

** Experiments exist

https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/

Lee Holmes, Azure Management Security, April 10, 2017

Maslow's Hierarchy of Security Controls



http://www.leeholmes.com/blog/2014/12/08/maslows-hierarchy-of-security-controls/

Maslow´s Hierarchy of Security Controls

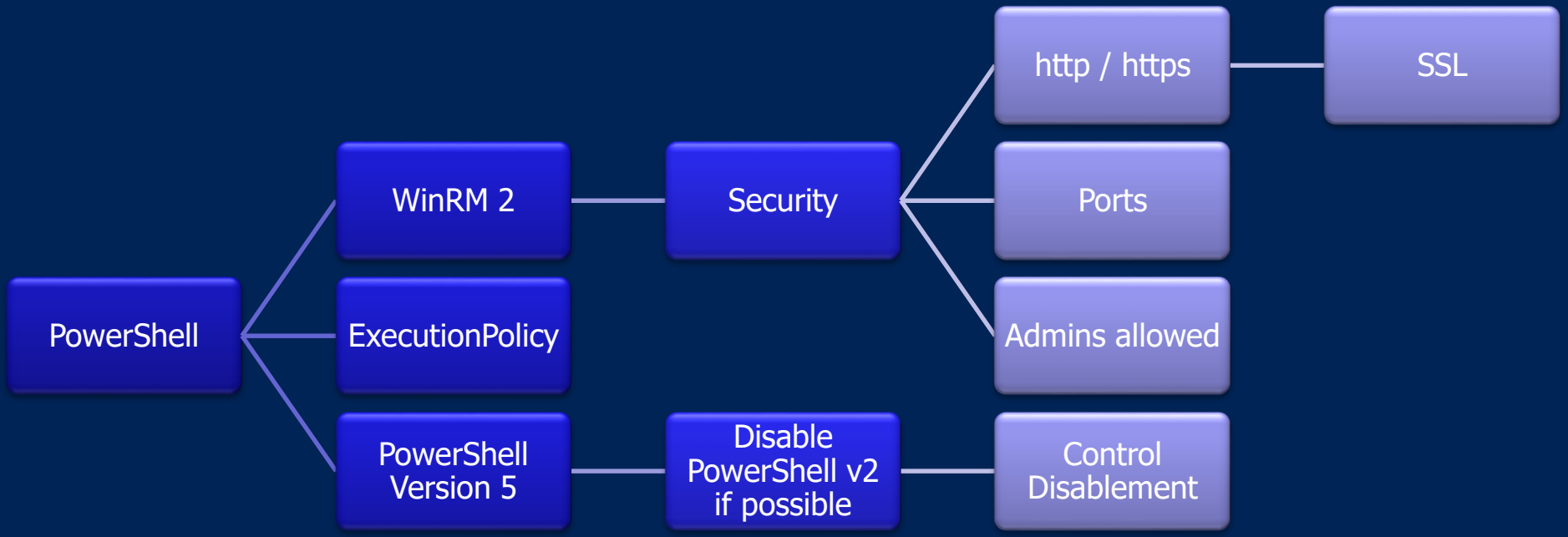
Control	Benefit	Impact Without Control	Limitations
Antivirus / Antimalware	Can limit the execution of malware known to the AV industry.	Attacker can write and run any code, custom C++ applications, internet tools, etc.	Can be disabled by administrators. AV signatures can be evaded if the attacker is capable of recompiling or modifying an application.
Applocker in Deny Mode	Can limit the execution of malware known to your organization.	Attacker can write and run any code, custom C++ applications, etc., as long as they aren't well known attack tools or exploits.	Can be disabled by administrators. Only blocks known evil / undesirable malware, can be bypassed with only minor application changes.
Applocker in Allow Mode	Can prevent the execution of unknown / unapproved applications.	Attacker can write arbitrary custom applicatons, as long as they are not detected by AV orApplocker Deny rules.	Can be disabled by administrators. Attacker can still leverage in-box tools like VBScript, Office macros, HTA applications, local web pages, PowerShell, etc.

Maslow´s Hierarchy of Security Controls

Auditing of protections (AppLocker registry keys, AV settings, etc.)	By implementing and watching for registry / filesystem audit events generated when an attacker disables protections like AppLocker, attackersbecome more visible.	Attacker can disable most built-in controls, and then compromise a system without being impacted by that control.	Auditing is a reactive technology, not a preventative technology. An attack might still be successful, but proper audit monitoring can help you detect it.
Forensic capture / examination of host-based artifacts	Can help detect attacks based on in-box applications that modify the system in some way (such as putting a .VBS / .HTA file on disk).	Attacks that leverage in-box tools may not be detected.	Requires significant expertise and custom tooling to capture and forward all “interesting” forensic artifacts. Can be avoided by in-box components (such as Internet Explorer, VBScript “stagers”, PowerShell, and debuggers) that have the ability to invoke in-memory commands.
Memory forensics / application-specific logging	Can detect forensic artifacts that do not touch disk.	Memory-only attacks may go undetected.	Not all components that have the ability to invoke in-memory commands expose application-specific logging. Memory-only forensics require significant expertise and custom tooling.

Security Approach

Approaching – Remoting & Version



PowerShell Version

WMF 5.1 can be installed on Windows 7, Windows 8.1, Windows Server 2008 R2, 2012, and 2012 R2, and provides a number of improvements.

It is **not required** to install WMF 4.0 prior to installing WMF 5.1 on Windows 7 and Windows Server 2008 R2. That was an issue for the WMF 5.1 Preview release, and has been resolved.

→ Migrate to PowerShell Version 5

→ **And with your existent Win 7/8.1 devices!**

PowerShell Version 5 is a must

Some of the fundamental security features:

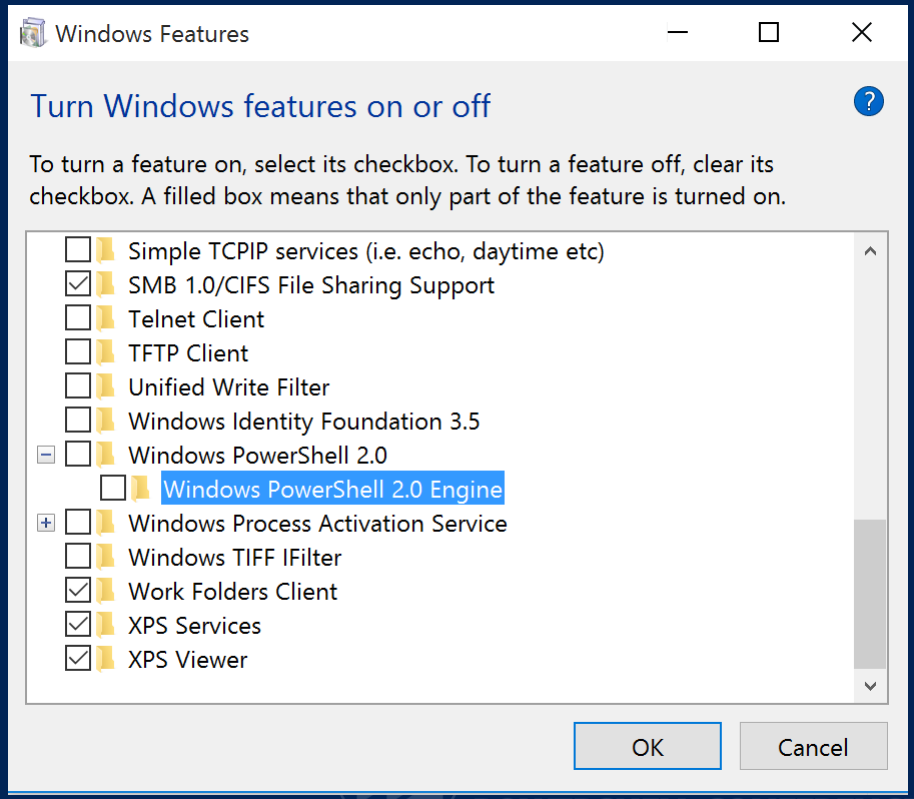
- Script block logging
- System-wide transcripts
- Constrained PowerShell
- Antimalware Integration aka AMSI (Windows 10)

PowerShell Version 2 – Attack Vector

Time ...	Process Name	PID	Operation	Path	Result	Detail
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\Microsoft.NET\Framework64	SUCCESS	IndexNumber: 0x10000000007ff
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\Microsoft.NET\Framework64	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\Microsoft.NET\Framework64	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\Microsoft.NET\Framework64\v2.0.50727	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\Microsoft.NET\Framework64\v2.0.50727	SUCCESS	IndexNumber: 0x1000000000800
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\Microsoft.NET\Framework64\v2.0.50727	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG	SUCCESS	IndexNumber: 0x1000000000816
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	IndexNumber: 0x900000000fd75
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\Microsoft.NET\Framework64\v4.0.30319	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\System32	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\System32	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\System32	SUCCESS	IndexNumber: 0x100000000090d
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\System32	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\System32	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\System32\en-US	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\System32\en-US	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\System32\en-US	SUCCESS	IndexNumber: 0x1000000000bd8
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\System32\en-US	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\System32\en-US	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\System32\WindowsPowerShell	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\System32\WindowsPowerShell	ACCESS DENIED	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\System32\WindowsPowerShell	SUCCESS	IndexNumber: 0x1000000000d17
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\System32\WindowsPowerShell	SUCCESS	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\System32\WindowsPowerShell	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\System32\WindowsPowerShell\v1.0	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\System32\WindowsPowerShell\v1.0	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\System32\WindowsPowerShell\v1.0	SUCCESS	IndexNumber: 0x1000000000d18
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\System32\WindowsPowerShell\v1.0	END OF FILE	Control: FSCTL_FILE_PREFETCH
8:54:4...	PSAttack.exe	3400	CloseFile	C:\Windows\System32\WindowsPowerShell\v1.0	SUCCESS	
8:54:4...	PSAttack.exe	3400	CreateFile	C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6	SUCCESS	Desired Access: Read Data/List Directory, Synchr
8:54:4...	PSAttack.exe	3400	SetBasicInform...	C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTi
8:54:4...	PSAttack.exe	3400	QueryFileIntern...	C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6	SUCCESS	IndexNumber: 0x1000000002255
8:54:4...	PSAttack.exe	3400	FileSystemControl	C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6	SUCCESS	Control: FSCTL_FILE_PREFETCH

PowerShell Version 2

- Windows 10 / Server 2016 provides the ability to remove PowerShell v2.0 (no, this doesn't remove PowerShell)
- Recommended after testing



PowerShell Remoting

- always encrypted
- single port
  - 5985 (http)
  - 5986 (https)
    - With certificate
- In a domain only members of the Domain administrators group have the ability to remote.
- Advanced logging possibilities

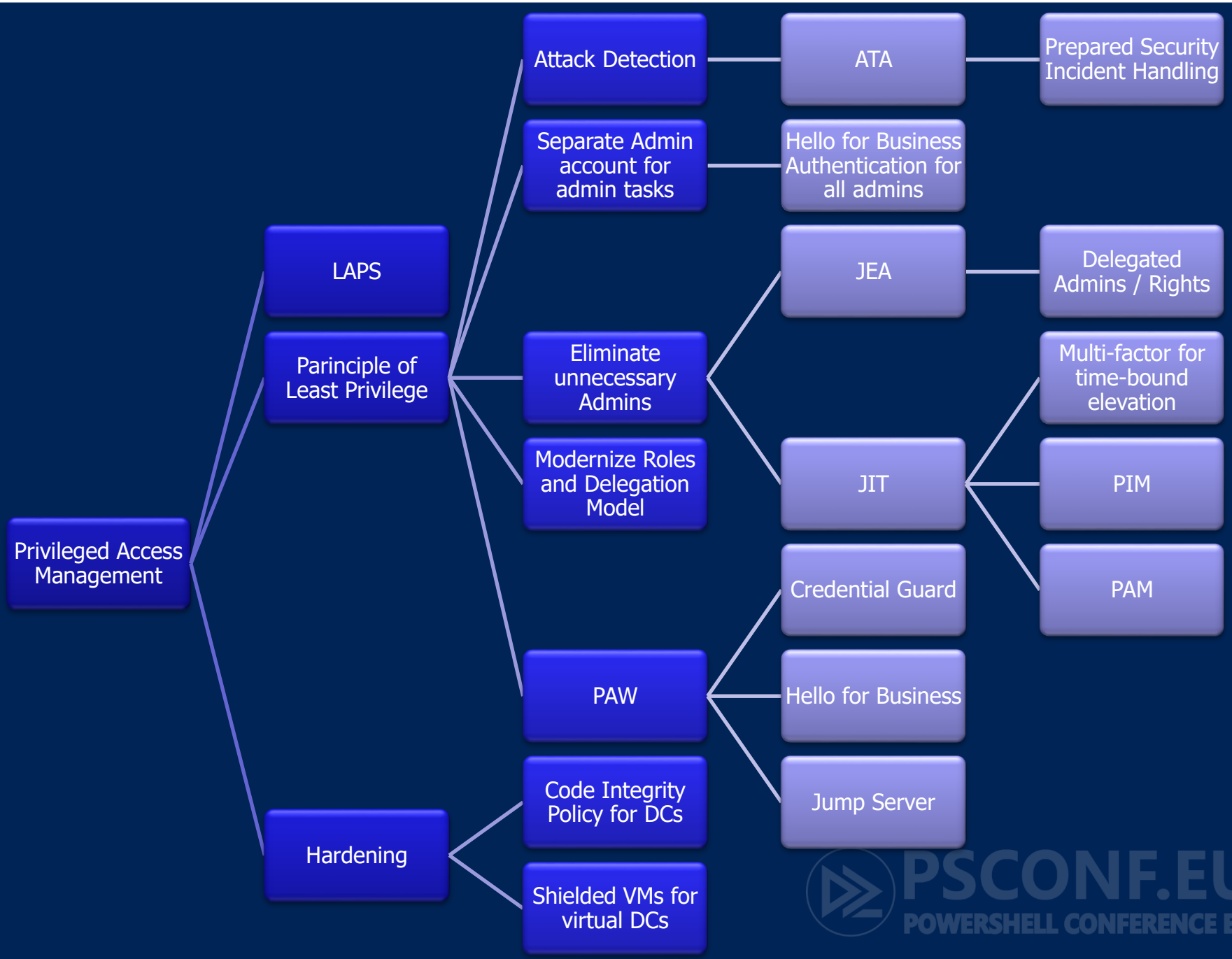
ExecutionPolicy

ExecutionPolicy ... ature.

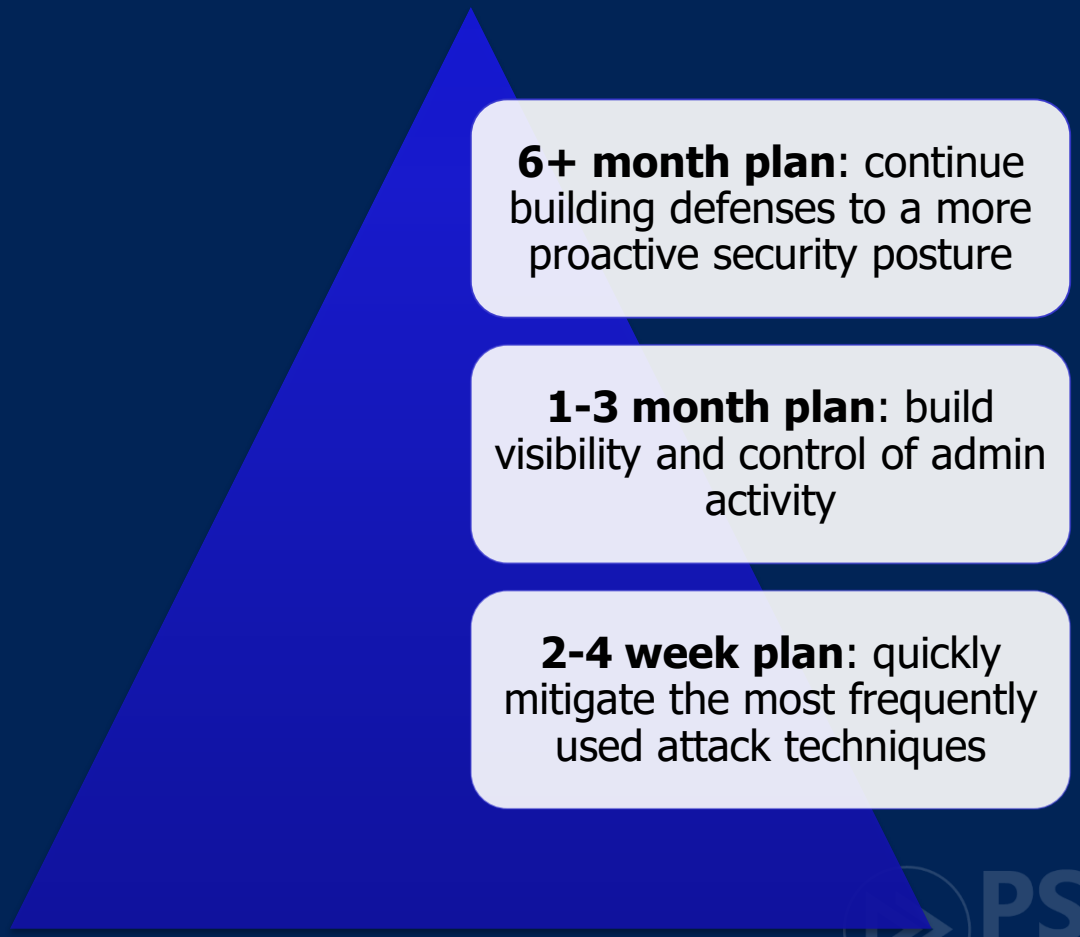
Oh wait..

ExecutionPolicy is not a Security Feature!

ExecutionPolicy is like a baby door. The ExecutionPolicy keeps babies save but every grown-up surpasses it easily.

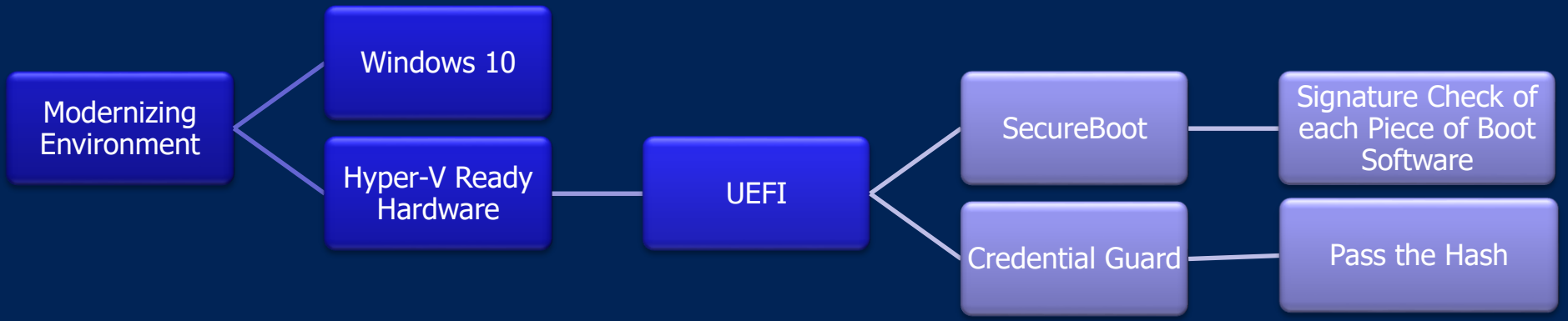


Securing Privileged Access Roadmap Objectives



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access

Approaching – Modernizing Environment



Pass the Hash

Today's Security Challenge

Pass the Hash Attacks

Access to one device can lead to access to many

1.

Single IT Pro's machine is compromised

IT Pro manages kiosks/shared devices on network

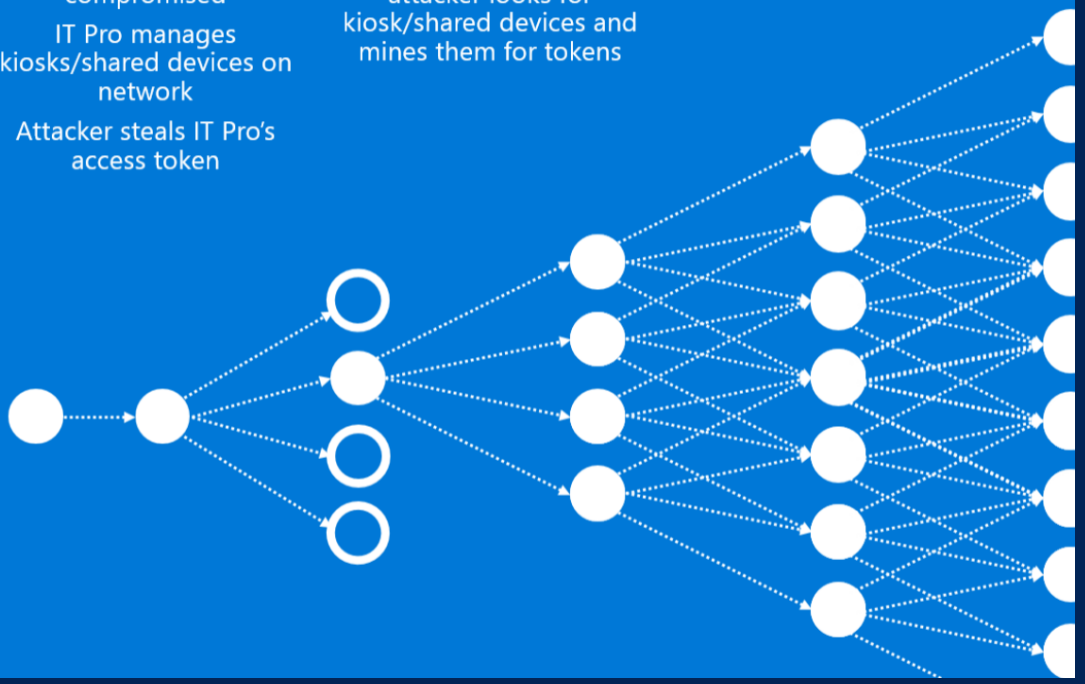
Attacker steals IT Pro's access token

2.

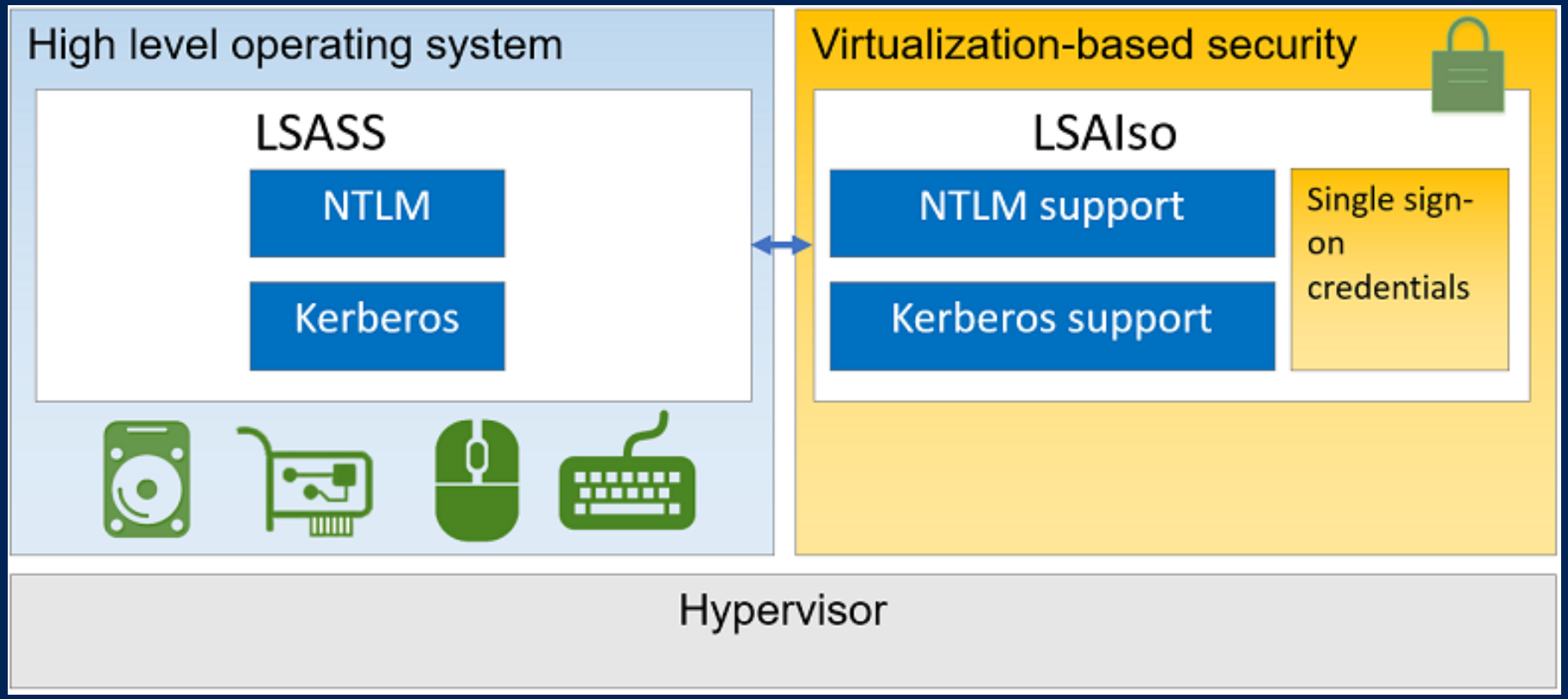
Using IT Pro's access token attacker looks for kiosk/shared devices and mines them for tokens

3.

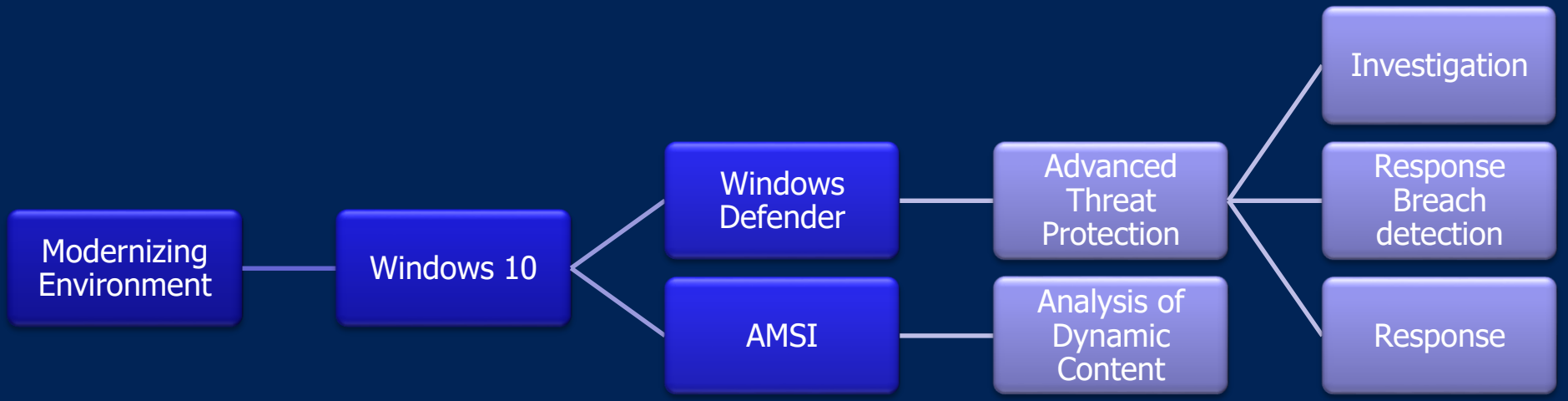
Repeat



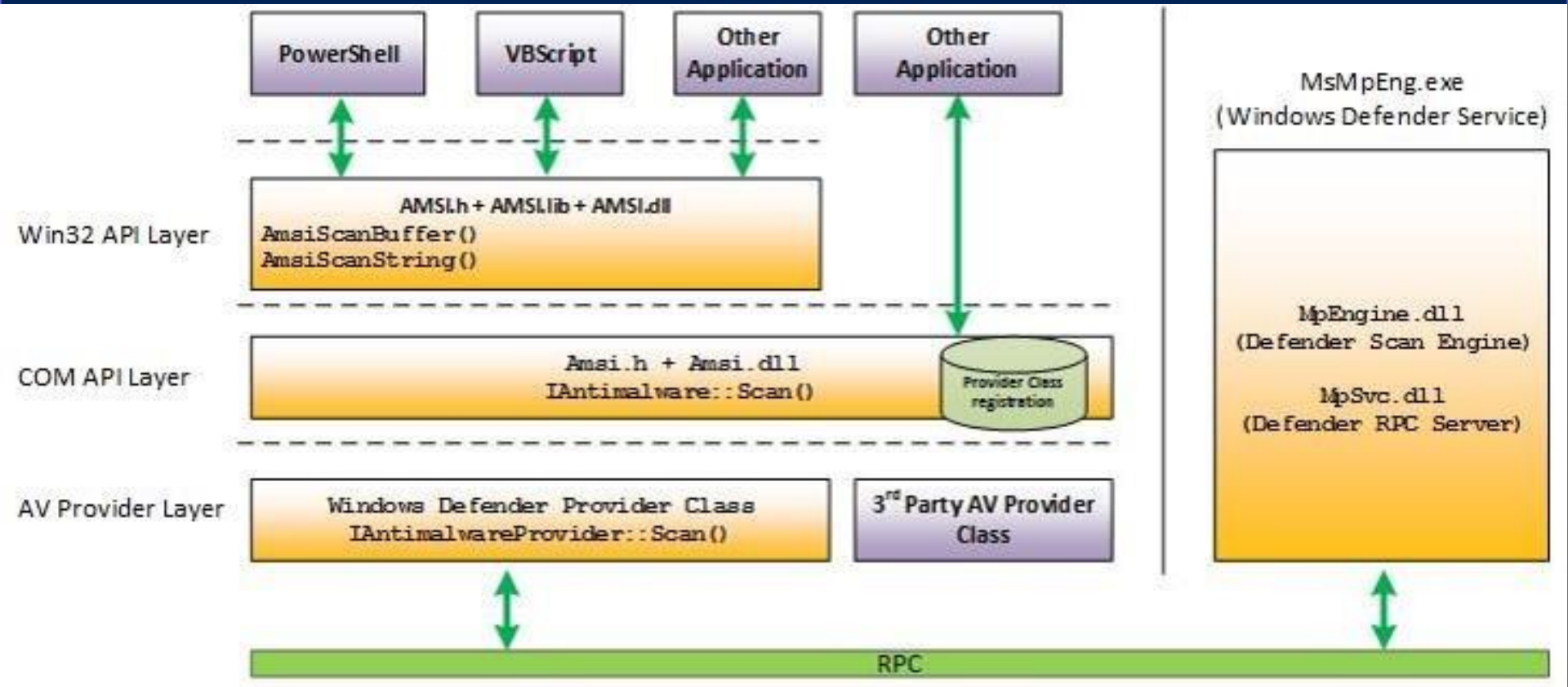
Credential Guard



Approaching – new Windows 10 Features



Anti-Malware Scan Interface



The most important quote

"THERE ARE TWO KINDS OF BIG COMPANIES:
THOSE WHO'VE BEEN COMPROMISED,
AND THOSE ***WHO DON'T KNOW*** THEY'VE BEEN
COMPROMISED."

JAMES COMEY, DIRECTOR FBI

Windows 10 Defense Stack

Windows Defender Advanced Threat Protection

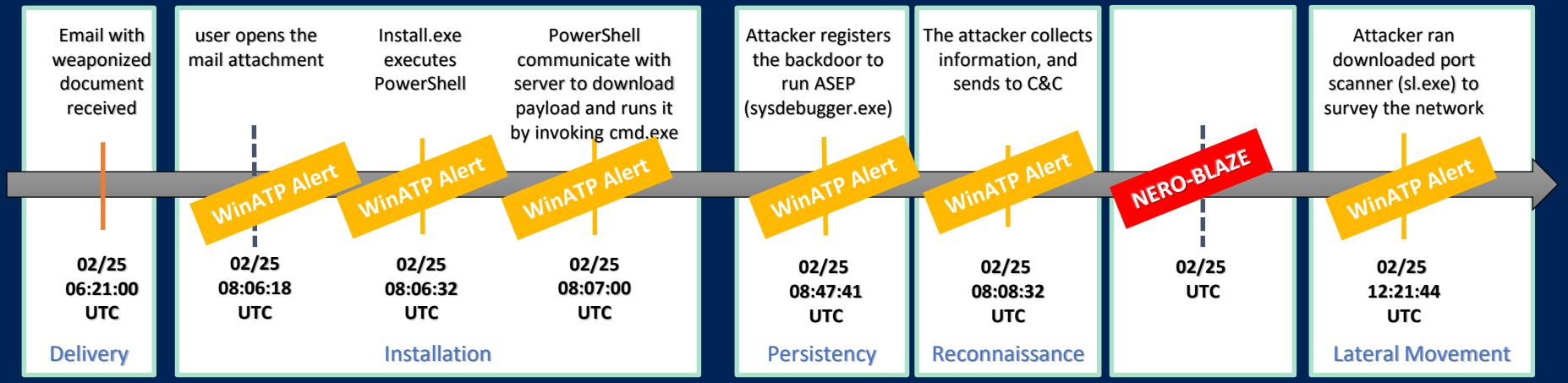
Post-Breach

Detection investigation

and response

PowerShell Conference EU 2017

Catching the Attack



- Outlook drops PE under %Users% folder (install.exe)
- Outlook ran the dropped PE

A suspicious PowerShell script executed by install.exe

Suspicious PowerShell communicates with external IP and executed cmd.exe with redirected handles

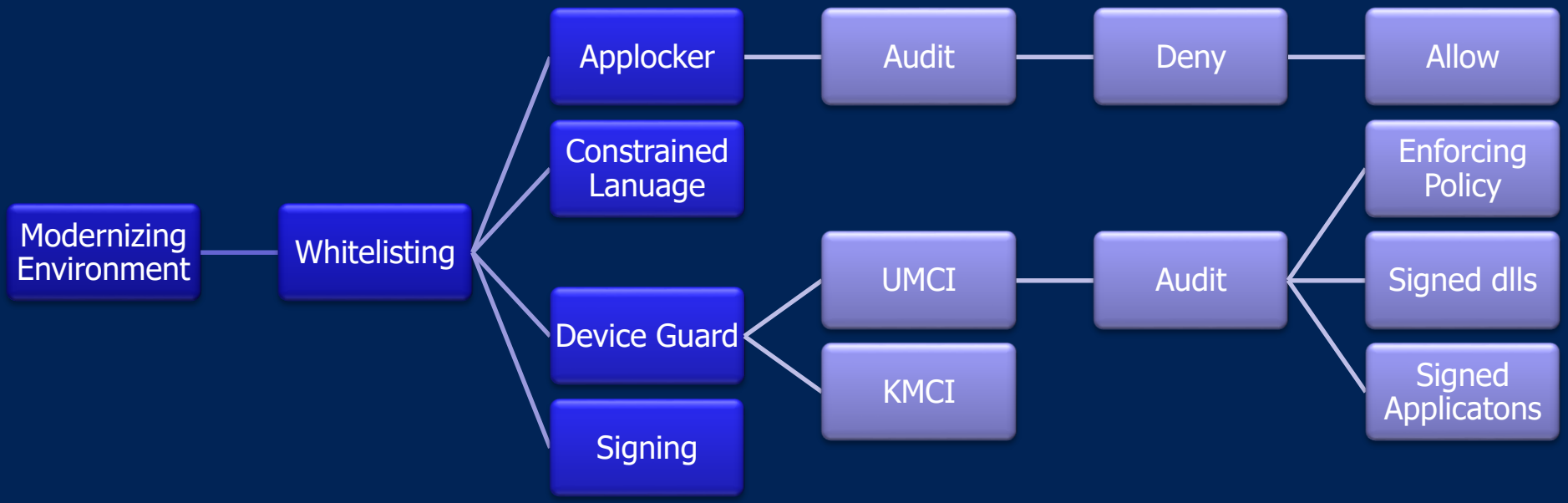
- PowerShell runs cmd.exe
- cmd.exe runs reg.exe

PowerShell communicated with external IP

C2 IP attributed to NEROBLAZE attacker, based on Threat Intelligence

Ports canning over TCP & UDP pattern

Approaching – Whitelisting

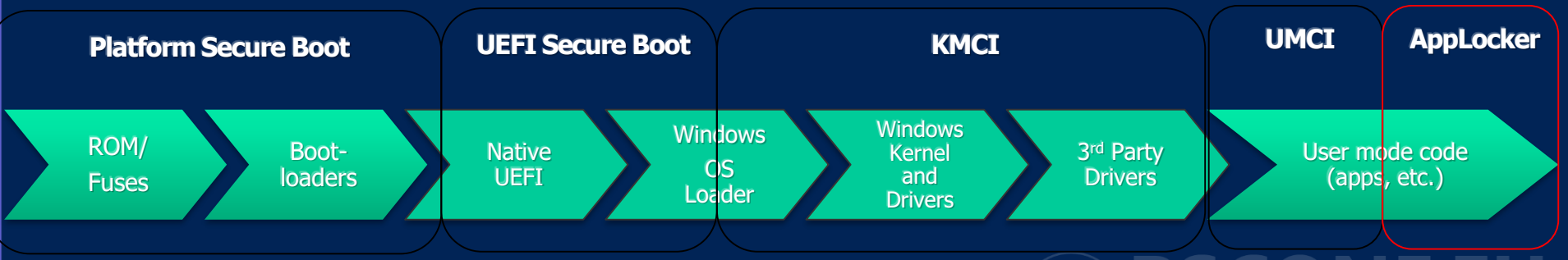


Securing Scripts

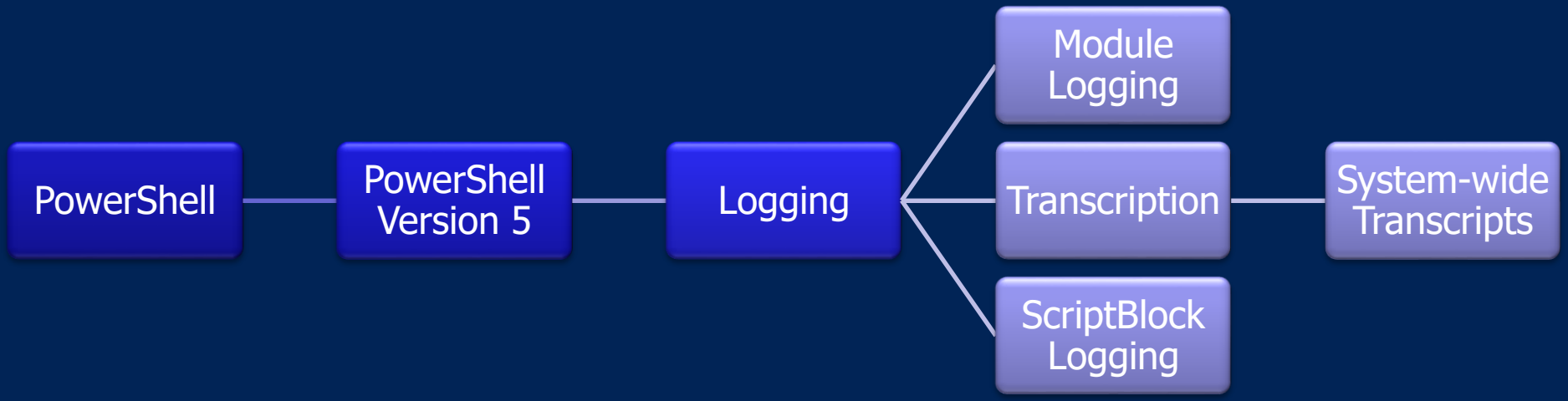
- Scripts can do dangerous things
- Windows Script Host will require signed scripts
  - WSH is the scripting host for VBScript (.vbs), Jscript (.js), Windows script file (.wsf) and Windows script component (.wsc) scripts
- MSIs must be signed
- PowerShell will be in “ConstrainedLanguage” mode
  - Signed PowerShell scripts can be in full language mode
- .bat & .cmd scripts are not restricted

Device Guard

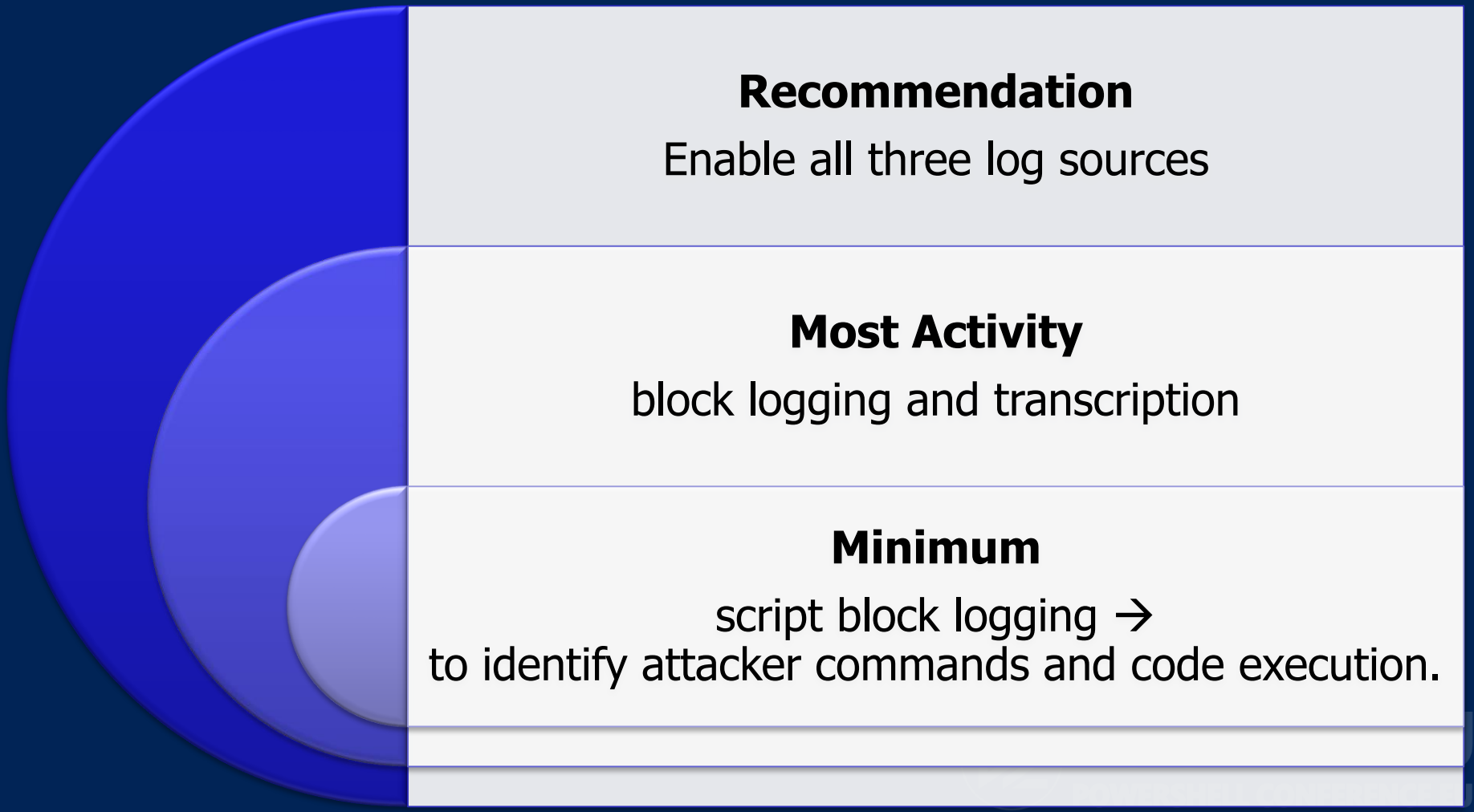
- Secure Boot
  - Includes Secure Firmware Updates and Platform Secure Boot
- Kernel Mode Code Integrity (KMCI)
- User Mode Code Integrity (UMCI)
- App Locker



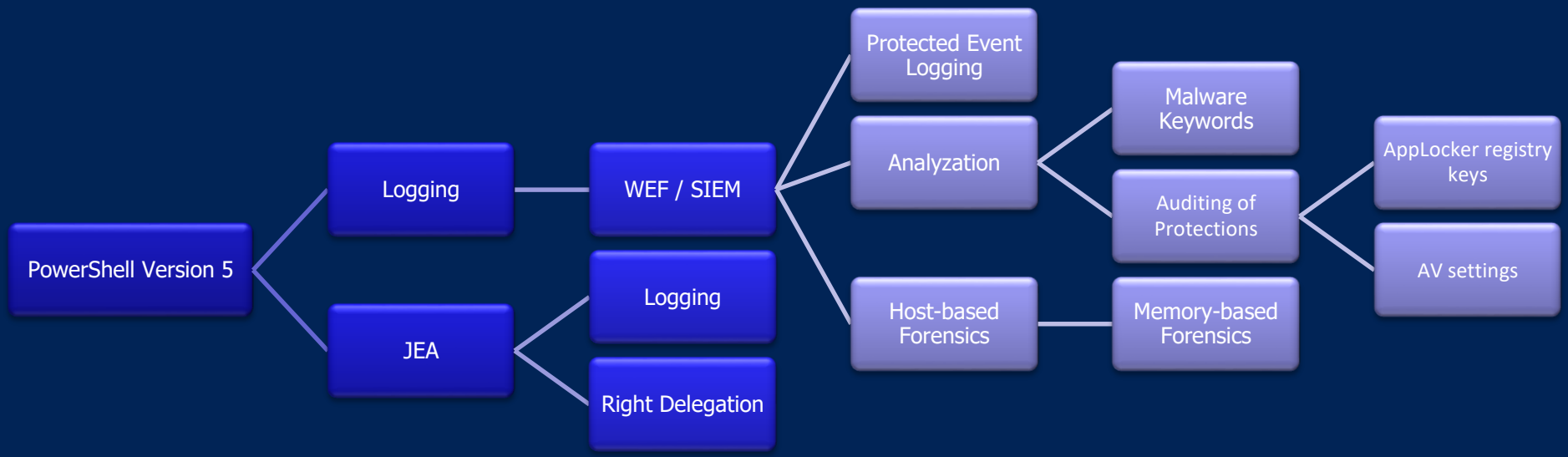
Approaching – Basic Logging



Logging Best Practice



Approaching – extended Logging and JEA



WEF

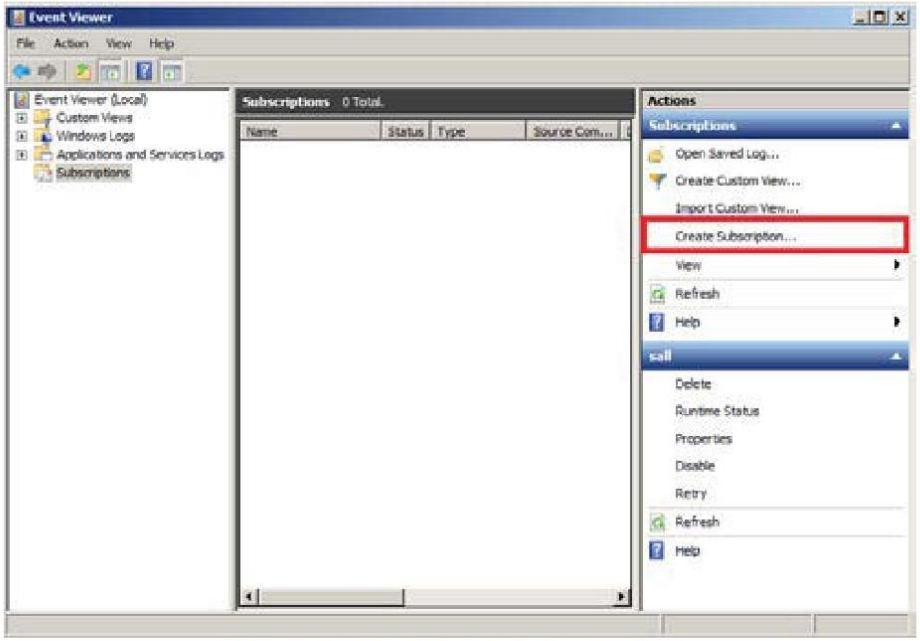


Figure 1: Creating a Subscription

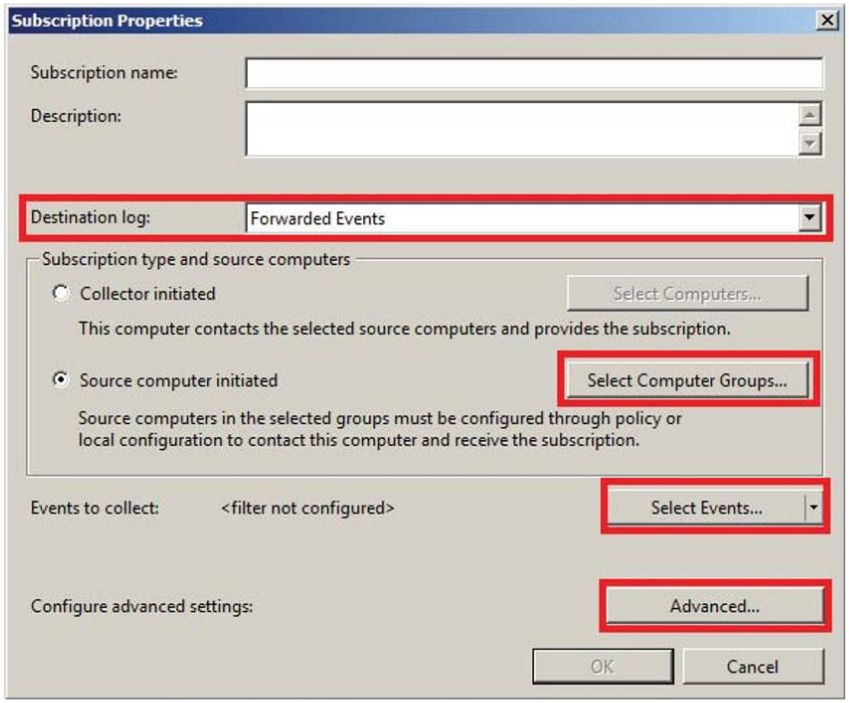


Figure 2: Configuring Subscription Properties

WEF - Malware Keywords

Offensive PowerShell Detection Indicators

- AdjustTokenPrivileges
- IMAGE_NT_OPTIONAL_HDR64_MAGIC
- Management.Automation.RuntimeException
- Microsoft.Win32.UnsafeNativeMethods
- ReadProcessMemory.Invoke
- Runtime.InteropServices
- SE_PRIVILEGE_ENABLED
- System.Security.Cryptography
- System.Reflection.AssemblyName
- System.*Runtime.InteropServices*
- LSA_UNICODE_STRING
- MiniDumpWriteDump
- PAGE_EXECUTE_READ
- Net.Sockets.SocketFlags
- Reflection.Assembly
- SECURITY_DELEGATION
- CreateDelegate
- TOKEN_ADJUST_PRIVILEGES
- TOKEN_ALL_ACCESS
- TOKEN_ASSIGN_PRIMARY
- TOKEN_DUPLICATE
- TOKEN_ELEVATION
- TOKEN_IMPERSONATE
- TOKEN_INFORMATION_CLASS
- TOKEN_PRIVILEGES
- TOKEN_QUERY
- Metasploit
- Advapi32.dll
- kernel32.dll
- AmsiUtils
- KerberosRequestorSecurityToken
- Security.Cryptography.CryptoStream

Sean Metcalf
TrimarcSecurity.com

JEA Technical

Endpoint

Role Capabilities

PSRemoting

Server

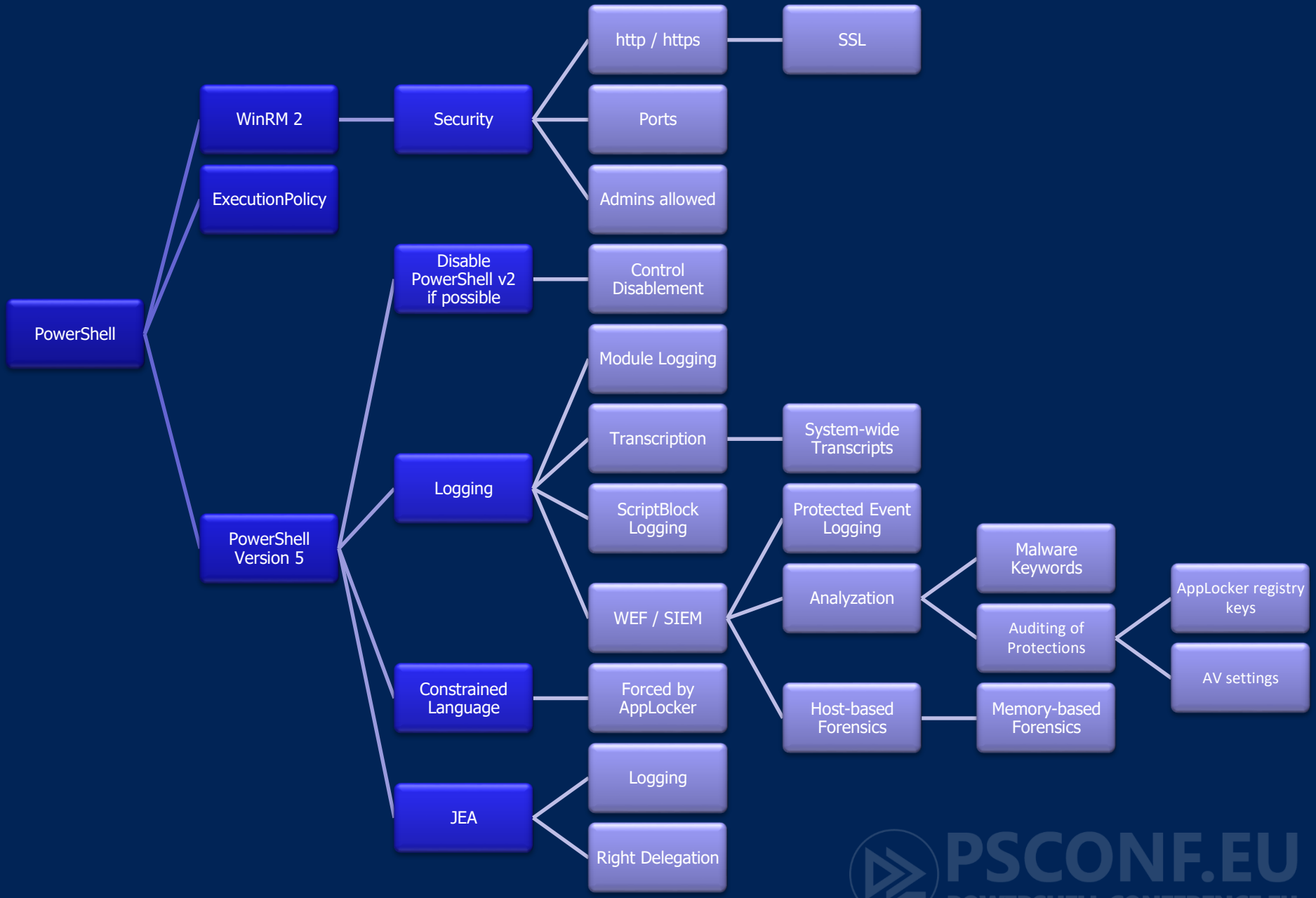
Authentication
Authorization

Additional capabilities

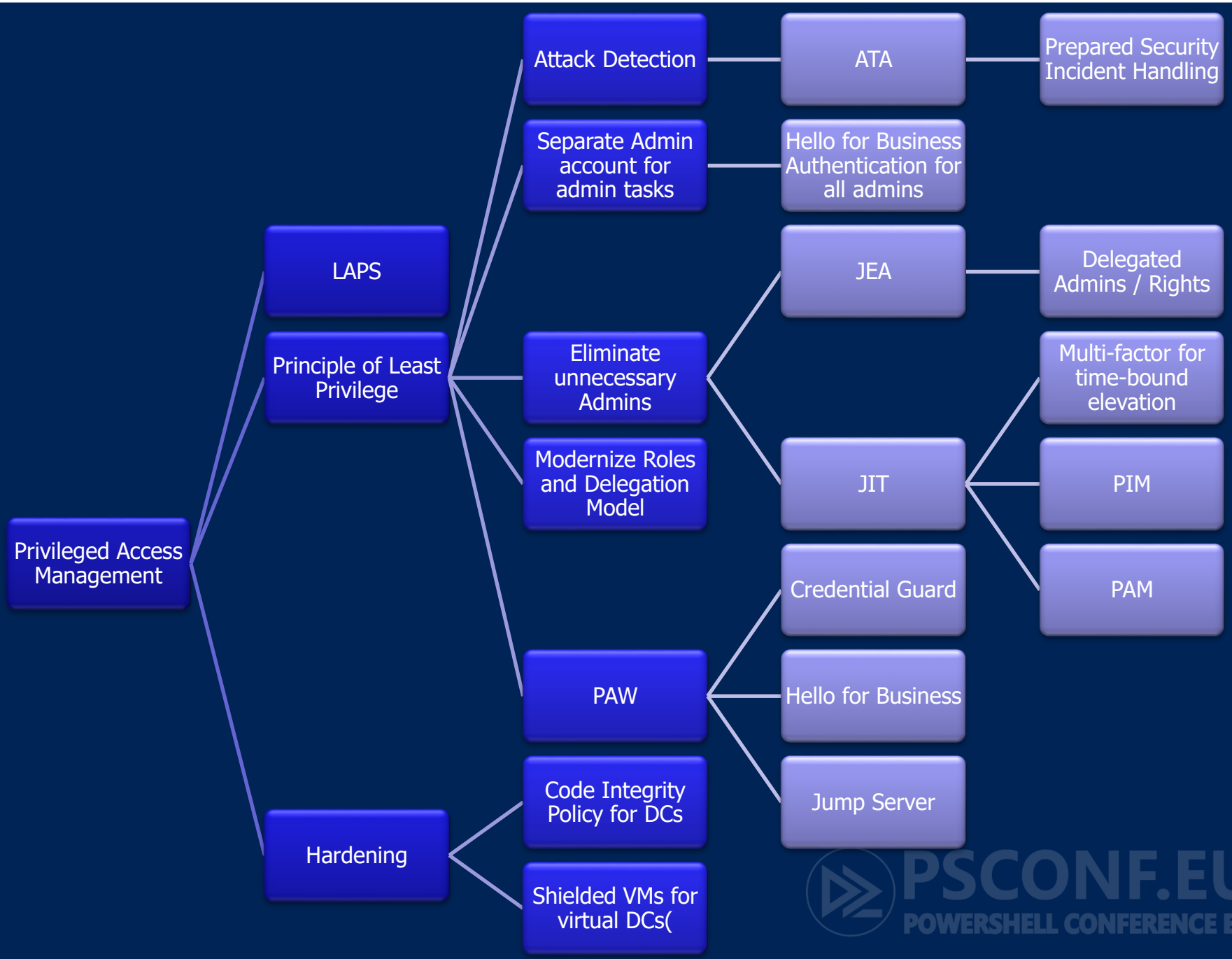
Client
User without Admin rights

Full Picture

PowerShell Conference EU 2017



PowerShell Conference EU 2017



Increasing the Security Level

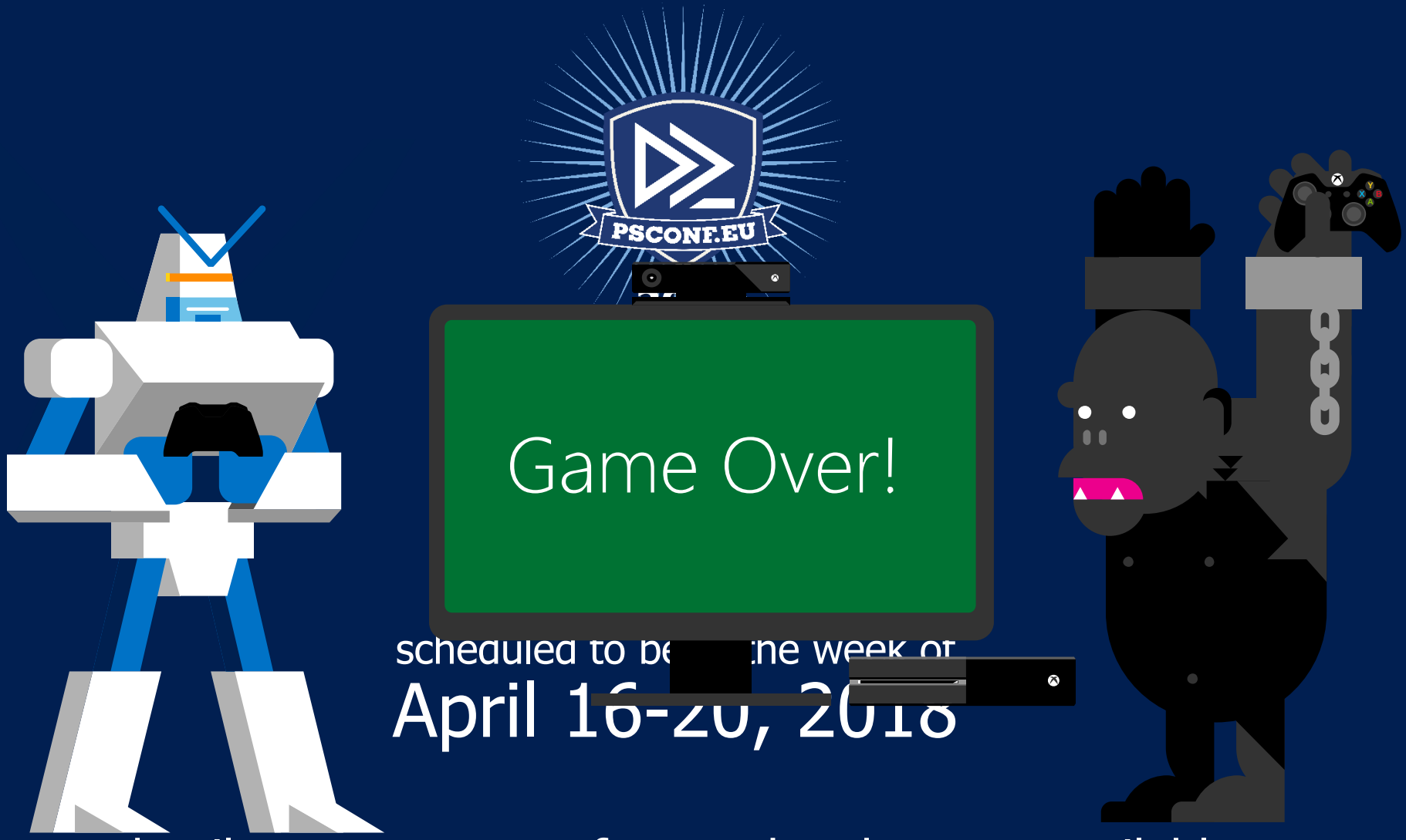
Questions?

Next Steps...

- Now: 15 min break

- Grab a coffee
- Stay here to enjoy next presentation
- Change track and switch to another room

- Ask me questions or meet me in a breakout session room afterwards



scheduled to be the week of

April 16-20, 2018

details on www.psconf.eu as they become available