



PowerShell Security Live Demo



David das Neves
[@David_das_Neves](https://twitter.com/David_das_Neves)



Julien Reisdorffer
[@JReisdorffer](https://twitter.com/JReisdorffer)



Miriam Wiesner
[@miriamxyra](https://twitter.com/miriamxyra)



Raimund Andree
[@raimundandree](https://twitter.com/raimundandree)



2018

PowerShell Security Live Demo

Miriam Wiesner

Premier Field Engineer, Microsoft

Raimund Andree

Sr. Premier Field Engineer, Microsoft

David das Neves

Premier Field Engineer, Microsoft

Julien Reisdorffer

Sr. Consultant Cybersecurity, Microsoft



Agenda

- Introduction / Background PS Security
- Overview Technical Security Controls
- AutomatedLab
- PSV5.1
- Whitelisting
- Security Compliance Toolkit

Agenda

- Logging, WEF, Sysmon
- JEA
- Windows Admin Center
- Wrap Up / Call to Action
- Q&A

Intro

Background PS Security



Why PowerShell Security matters



Security Response



Candid Wueest
detect, react, protect
25 NOV 2015

Symantec Official Blog

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

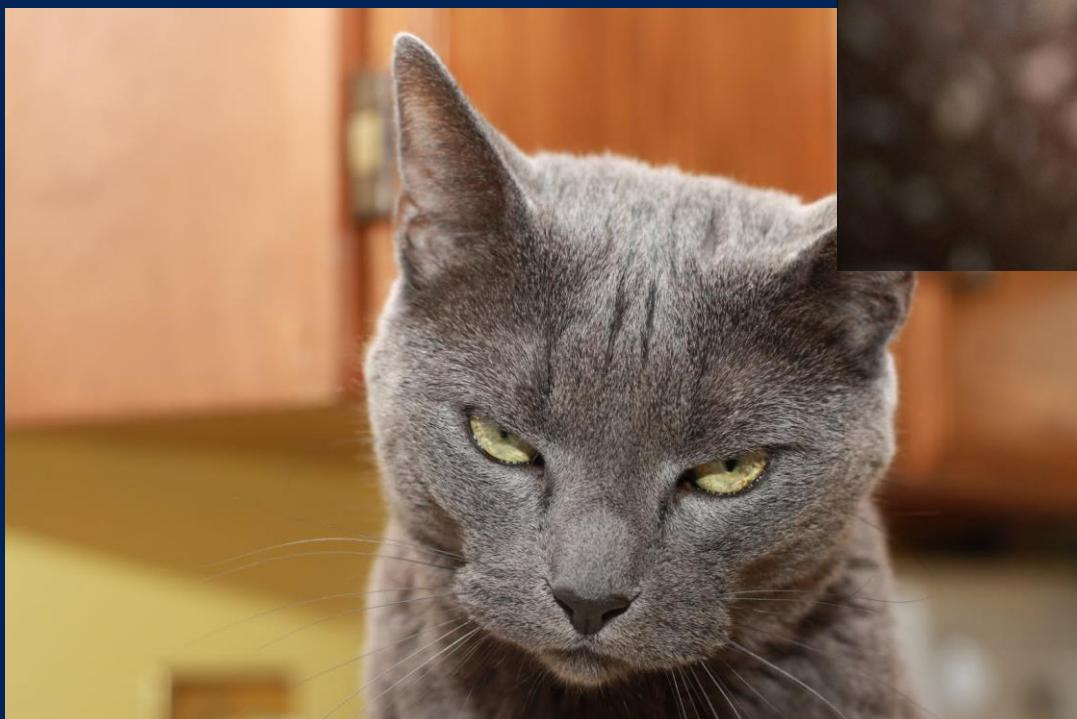
g+ 10 | LinkedIn 305 | Twitter | Reddit | Email | Like 1



The latest quarterly threat report from McAfee noted a fourfold increase in fileless hacking attacks utilising Microsoft PowerShell scripts. PowerShell activity in its *Unified Threat Research* report.

THIS ARTICLE COVERS

Powershell is evil.



Top Myths

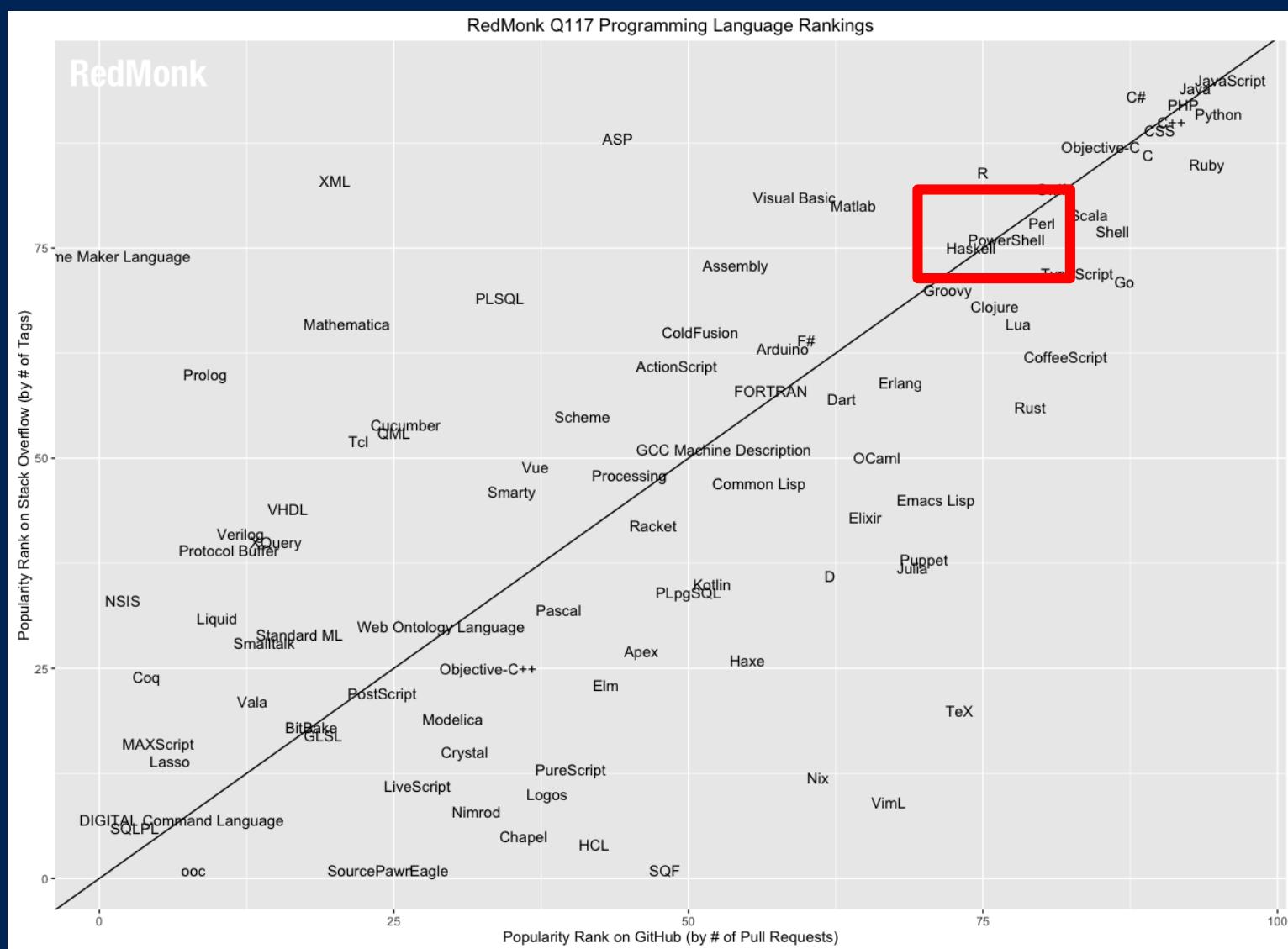
PowerShell is insecure

PowerShell Remoting is
insecure

ExecutionPolicy is a
Security Feature

PowerShell is just
PowerShell.exe

Powershell is powerful



A Comparison of Shell and Scripting Language Security

Engine	<input checked="" type="checkbox"/> Event Logging	<input checked="" type="checkbox"/> Transcription	<input checked="" type="checkbox"/> Dynamic Evaluation Logging	<input checked="" type="checkbox"/> Encrypted Logging	<input checked="" type="checkbox"/> Application Whitelisting	<input checked="" type="checkbox"/> Antimalware Integration	<input checked="" type="checkbox"/> Local Sandboxing	<input checked="" type="checkbox"/> Remote Sandboxing	<input checked="" type="checkbox"/> 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



Overview

Technical Security Controls



Topics

Security

PowerShell

Modernizing
Environment

Securing
Privileged
Access

Overview

	Exploit Guard	Cloud App Security and Office 365 Advanced Security Management		
Health Attestation	Office 365 Advanced Threat Protection	Azure AD Identity Protection	Cloud App Security and Office 365 DLP	
Virtualized Based Security	Microsoft Edge and Application Guard	Advanced Threat Analytics	Azure Information Protection	 Highly recommended
UEFI Secure Boot	Device Guard or/and AppLocker	Credential Guard	Windows Information Protection	 Validate
Trusted Boot	Windows Defender or 3 rd Party Anti Virus Protection	Windows Hello for Business	BitLocker Admin and Monitoring (MBAM)	
Window Update	SmartScreen	Local Administrator Password Solution	BitLocker to GO	Conditional Access
TPM	Security Baseline	MFA	BitLocker	Windows Defender Advanced Threat Protection
				
Device protection	Threat resistance	Identity protection	Information protection	Breach detection investigation & response

Technical Guideline

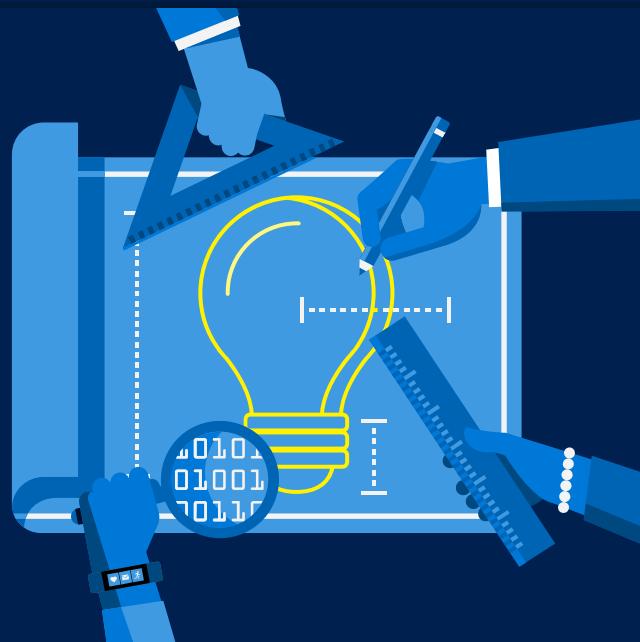
Windows 10 Link List

- <http://aka.ms/w10Links>

PowerShell Security for Enterprise Customers

- <http://aka.ms/PSSecEnt>

Discussion



Conference Day 4 - April 20th, 2018

8:30 – 9:30

PowerShell Security - what to prioritize?

AutomatedLab

Hybrid Lab



Problem

- Creating labs can be complex and time taking using of work
- The more complex it is, the more likely to do mistakes
- Over time a get a unique piece of art

Why Automate?

Time to Deploy

Configuration Drift

Human Error Avoidance

Simplifying Complexity

Fast and Easy Repeatability

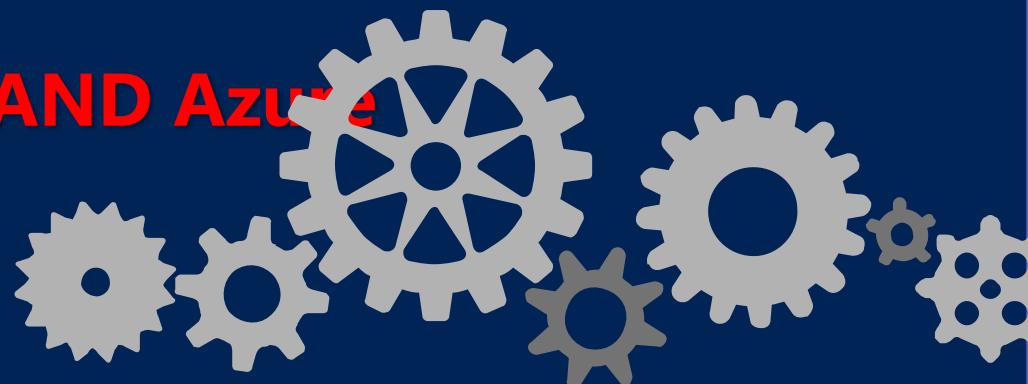
IaC Best Practices

Treat your infrastructure like "cattle",



AutomatedLab Capabilities

- Framework to manage lab resources like
 - networks, disks, VMs, common services, software installation, customization
 - Let's you easily customize your lab after deployment
 - Deploys on Hyper-V **AND Azure**



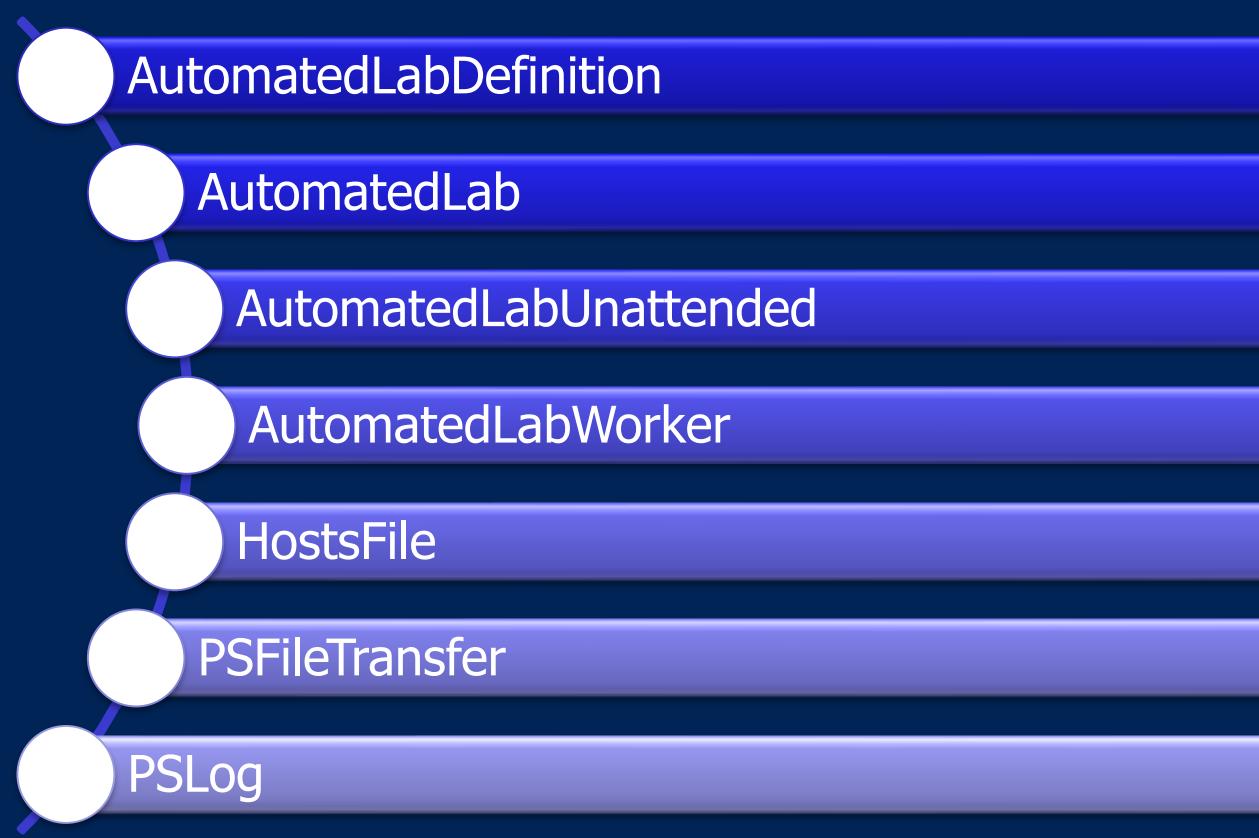
AutomatedLab Requirements

- Basic PowerShell Knowledge (there is no UI and no plans to add one)
- ISO files (from MSDN for example)
- [AutomatedLab](#)

How does it work?

Powershell Modules

AutomatedLab comes with 7 PowerShell modules because we have tried to separate the solution into its main building blocks. This makes the coding and troubleshooting easier.



AutomatedLab Cmdlets

- **New-LabDefinition**
 - Add-LabIsolImageDefinition
 - Add-LabVirtualNetworkDefinition
 - Add-LabMachineDefinition
- **Install-Lab**
 - Install-LabSoftwarePackage
 - Invoke-LabCommand
 - Install-LabWindowsFeature
- **Get-LabVM**
 - Restart-LabVM –Wait / Wait-LabVM
 - Get-LabVMStatus

Internals

- VHDS
 - Differential Disks
 - One per OS
- Powershell Remoting
 - Internal or External Network Adapter
 - CredSSP for double hop
 - NTLM used
 - *Set-LabHostRemoting* must be called on the Host
- Checkpoints
 - Integrated cmdlets *Checkpoint-LabVM* and *Restore-LabVM*
- Post Installation Activities
 - *Scripts*
- *Software Packages*
 - *MSI / Exe -files with quiet-flag*



Examples

#The most easy example

```
New-LabDefinition -Name Lab1' -  
DefaultVirtualizationEngine HyperV
```

```
Add-LabMachineDefinition -Name Client1 -Memory 1GB -  
OperatingSystem 'Windows Server 2012 R2  
SERVERDATACENTER'
```

```
Install-Lab
```

#Just one single Windows 2012 R2 server, nothing thrilling



#The Most Easy Example Extended

```
$PSDefaultParameterValues = @{  
    'Add-LabMachineDefinition:ToolsPath' = "$LabSources\Tools"  
    'Add-LabMachineDefinition:DomainName' = 'contoso.com'  
    'Add-LabMachineDefinition:Memory' = 1GB  
    'Add-LabMachineDefinition:OperatingSystem' = 'Windows Server 2012  
R2 SERVERDATACENTER'  
}  
  
New-LabDefinition -Name 'Lab1' -DefaultVirtualizationEngine HyperV
```

```
Add-LabMachineDefinition -Name DC -Role RootDC
```

```
Add-LabMachineDefinition -Name PKI -Roles
```

```
Add-LabMachineDefinition -Name Server1
```

```
Install-Lab
```

#A little bit more thrilling having now AD, a CA and a member server



#Software and Custom Commands

```
Install-LabSoftwarePackage -ComputerName Server1 -Path  
E:\LabSources\SoftwarePackages\Notepad++.exe -CommandLine /S -  
AsJob
```

```
Invoke-LabCommand -ActivityName AddSite -ComputerName (Get-LabVM  
-Role RootDC) -ScriptBlock {  
    Get-Date  
} -PassThru
```

```
Invoke-LabCommand -ActivityName AddSite -ComputerName (Get-LabVM  
-Role RootDC) -ScriptBlock {  
    $dc = Get-ADDomainController -Discover  
    New-ADReplicationSite -Name 'Datacenter - DR'  
}
```

#Install software and use custom commands as you need it.



Demo

AutomatedLab



AppLocker

Whitelisting



The Threats....

- Malware (ransomware) drops bad stuff and executes it
- User is tricked into running bad stuff
 - Downloaded or emailed...
- User decides to run unauthorized/unlicensed software

Whitelisting Business Value

- Users run only authorized software
- *Powerful* defense against malware/ransomware
- Spectrum of defenses

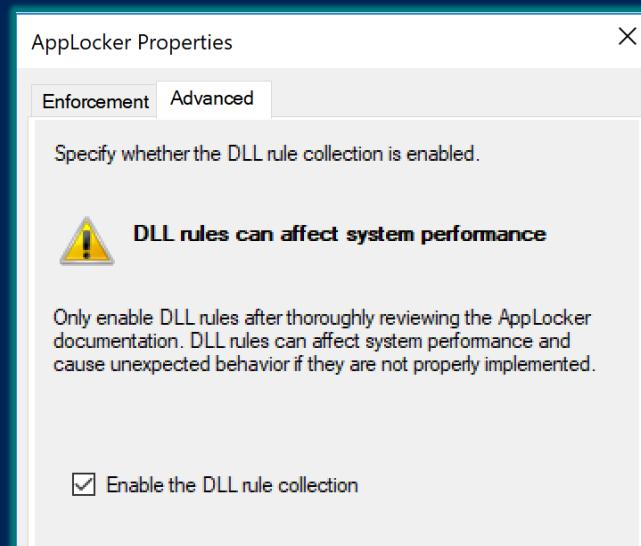
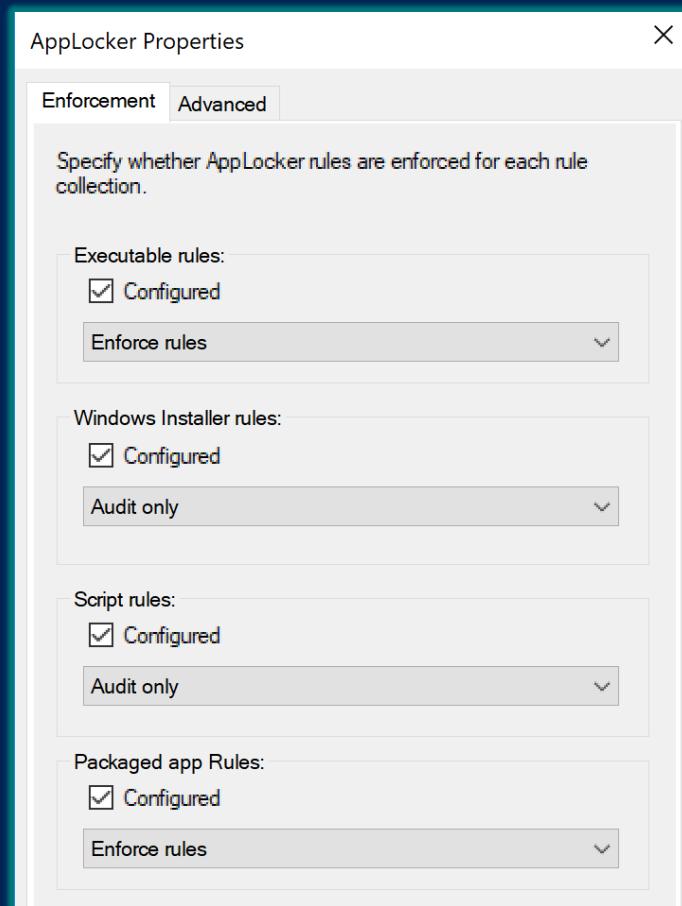
Available implementations

- From Microsoft: AppLocker, Device Guard → Windows Defender Application Control (WDAC)
- Third parties: (expensive)

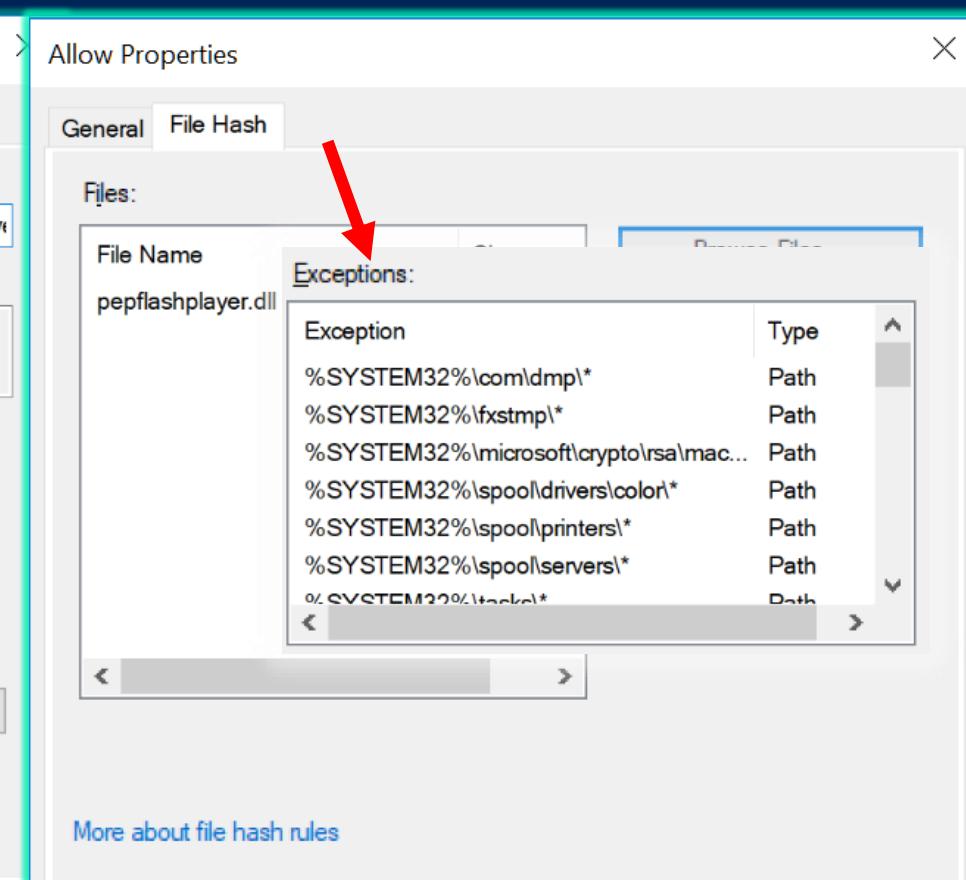
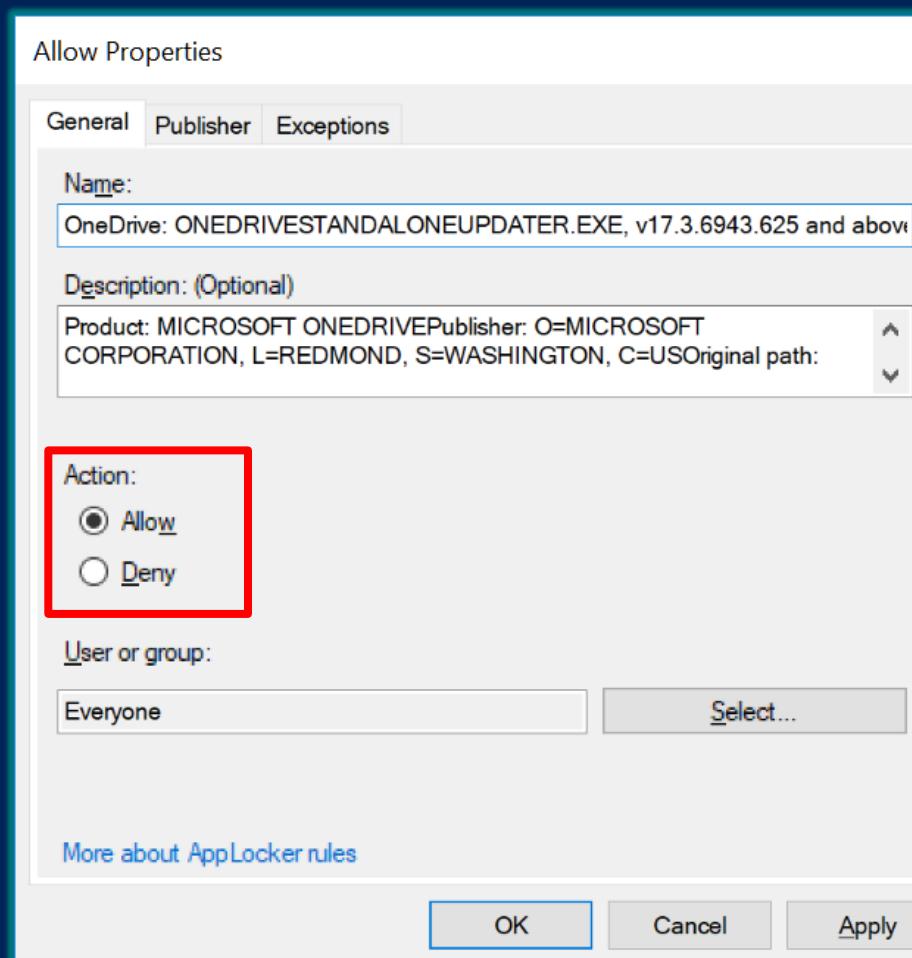
→ Restricts *non-admin* actions

Intro to AppLocker

AppLocker rule collections



AppLocker rules



DEMO

Signing, AppLocker, ExecutionPolicy



Security configuration baselines, and the Security Compliance Toolkit

What are baselines for?

Why not just make the defaults better?

Target: well-managed enterprises

Broadly applicable – should work for most

Streamlined

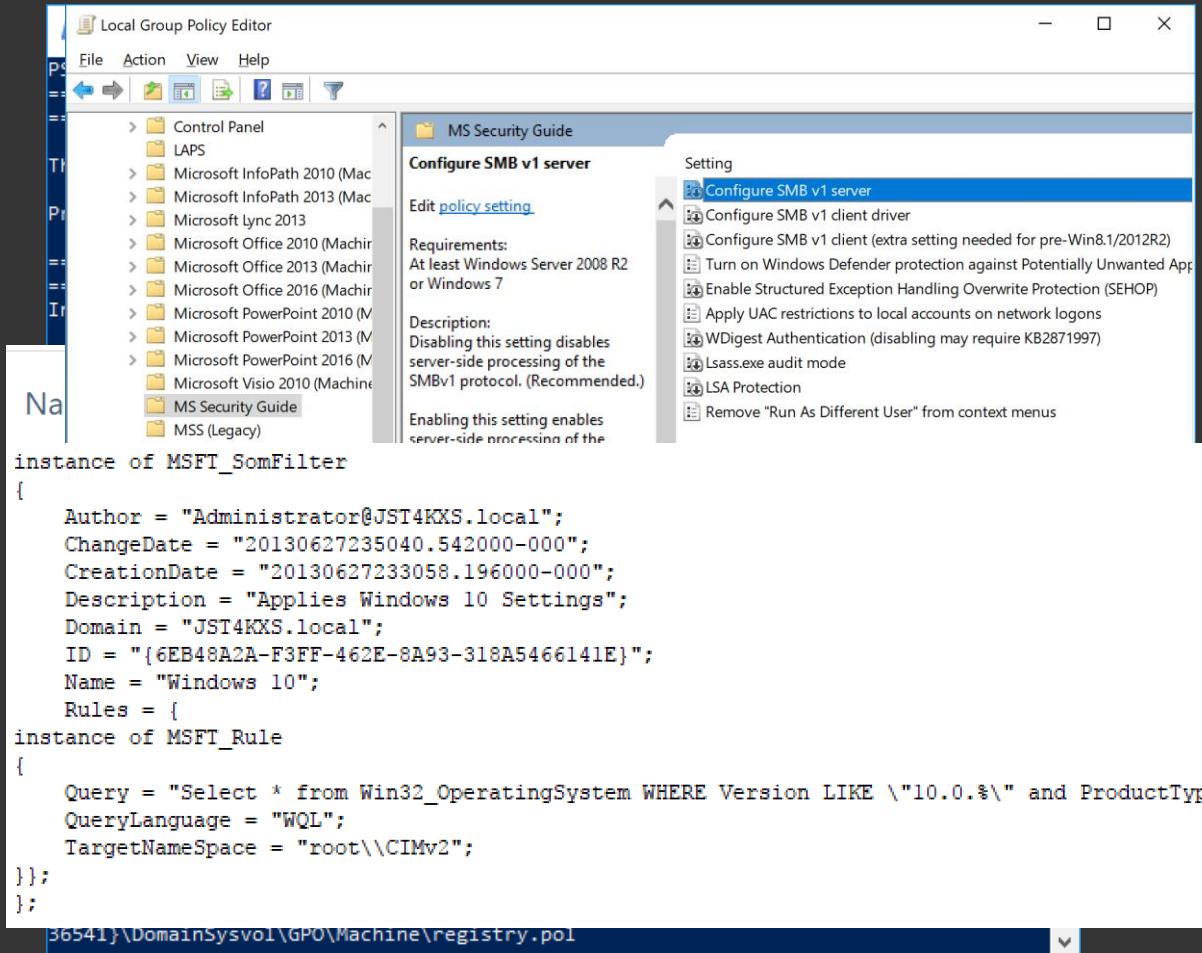
- Don't turn *all* the knobs
- Mitigate contemporary security threats
- Enforce only some defaults

GPO-based

- See also: MDM, DSC

Baseline packages

-  Documentation
-  GP Reports
-  GPOs
-  Local_Script
-  Templates
-  WMI Filters



Security Compliance Toolkit – Policy Analyzer

Policy Viewer - 384 items

Clipboard View Export Options

Policy Type	Policy Group or Registry Key	Policy Setting	Local registry	MSFT-Win10-v1709-
HKLM	System\CurrentControlSet\Policies\Microsoft\FVE	RDVDenyWriteAccess	1	
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	autodisconnect	15	
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	enablesecuritysignature	0	1
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	requiresecuritysignature	0	1
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	RestrictNullSessAccess	1	1
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	SMB1	0	
HKLM	System\CurrentControlSet\Services\LanmanWorkstation\Parameters	EnablePlainTextPassword	0	0
HKLM	System\CurrentControlSet\Services\LanmanWorkstation\Parameters	EnableSecuritySignature	1	1
HKLM	System\CurrentControlSet\Services\LanmanWorkstation\Parameters	Require Security Signature	0	1
HKLM	System\CurrentControlSet\Services\LDAP	LDAPClientIntegrity	1	1
HKLM	SYSTEM\CurrentControlSet\Services\MrxSmb10	Start	2	4
HKLM	SYSTEM\CurrentControlSet\Services\Netbt\Parameters	NoNameReleaseOnDemand	1	
HKLM	System\CurrentControlSet\Services\Netlogon\Parameters	disablepasswordchange	0	0

Policy Path:
Security Settings
Local Policies\Security Options
Microsoft network server: Digitally sign communications (if client agrees)

Local registry:
Option: Disabled
Data: 0
Type: REG_DWORD
GPO: Local registry

MSFT-Win10-v1709-RS3-FINAL:
Option: Enabled
Data: 1
Type: REG_DWORD
GPO: MSFT Windows 10 RS3 - Computer

Security Compliance Toolkit – LGPO.exe

To apply policy settings:

LGPO.exe command [...]

where "command" is one or more of the following (each of which can be concatenated):

To parse a Registry.pol file to LGPO text (stdout):

```
LGPO.exe /parse [...] /m path\registry.pol /u path\registry.pol [/v]
/m path\registry.pol           To build a Registry.pol file from LGPO text:           ls
/u path\registry.pol          LGPO.exe /r path\lgpo.txt /w path\registry.pol [/v]      istrators
/ua path\registry.pol         /r path\lgpo.txt      Read input from LGPO text file lministrators
/un path\registry.pol        /w path\registry.pol   Write new registry.pol file
/u:username                  /quiet, /nologo, /user:username, /user:local user
/q                           specified by "username"
                               quiet output (no headers)
                               * "zone" for IE zone mapping extension
                               * "mitigation" for mitigation options, including font blocking
                               * "audit" for advanced audit policy configuration
                               * "LAPS" for Local Administrator Password Solution
                               * "DGVBS" for Device Guard virtualization-based security
                               * "DGCI" for Device Guard code integrity policy
/boot                        reboot after applying policies
/v                           verbose output
/q                           quiet output (no headers)
```

DEMO

Security Compliance Toolkit



Windows Event Forwarding (WEF)

Simple Threat Detection Stack



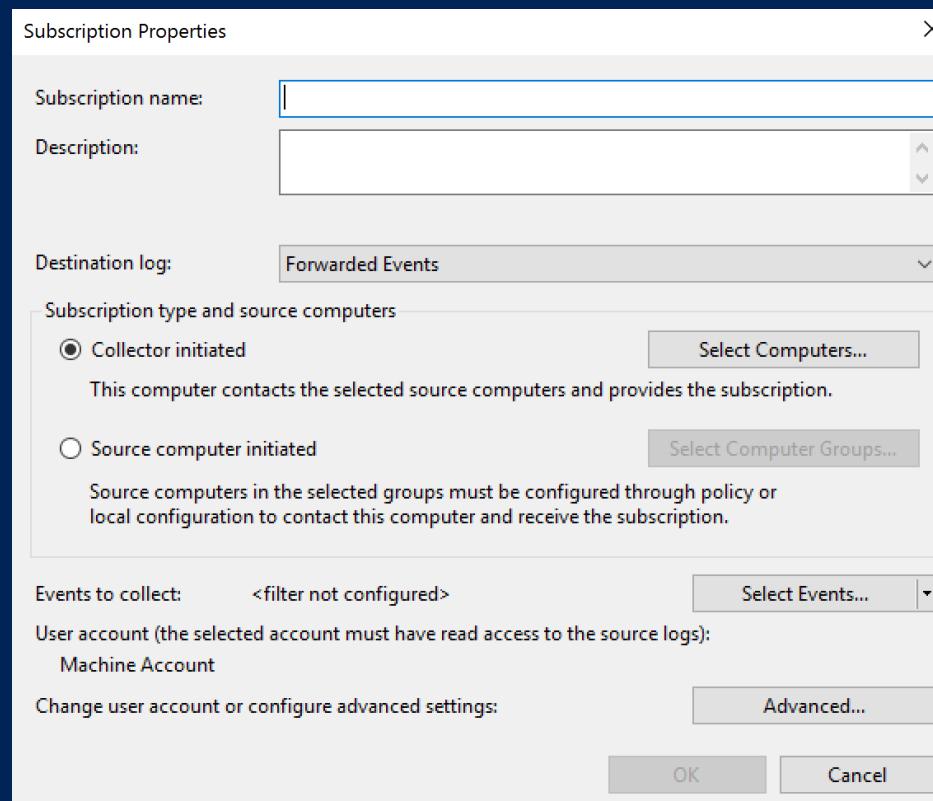
WEF Overview

- Log Forwarding integrated into Windows
- Transport mechanism encrypted and authenticated through Kerberos (Opt-In HTTPS)
- Works at scale!

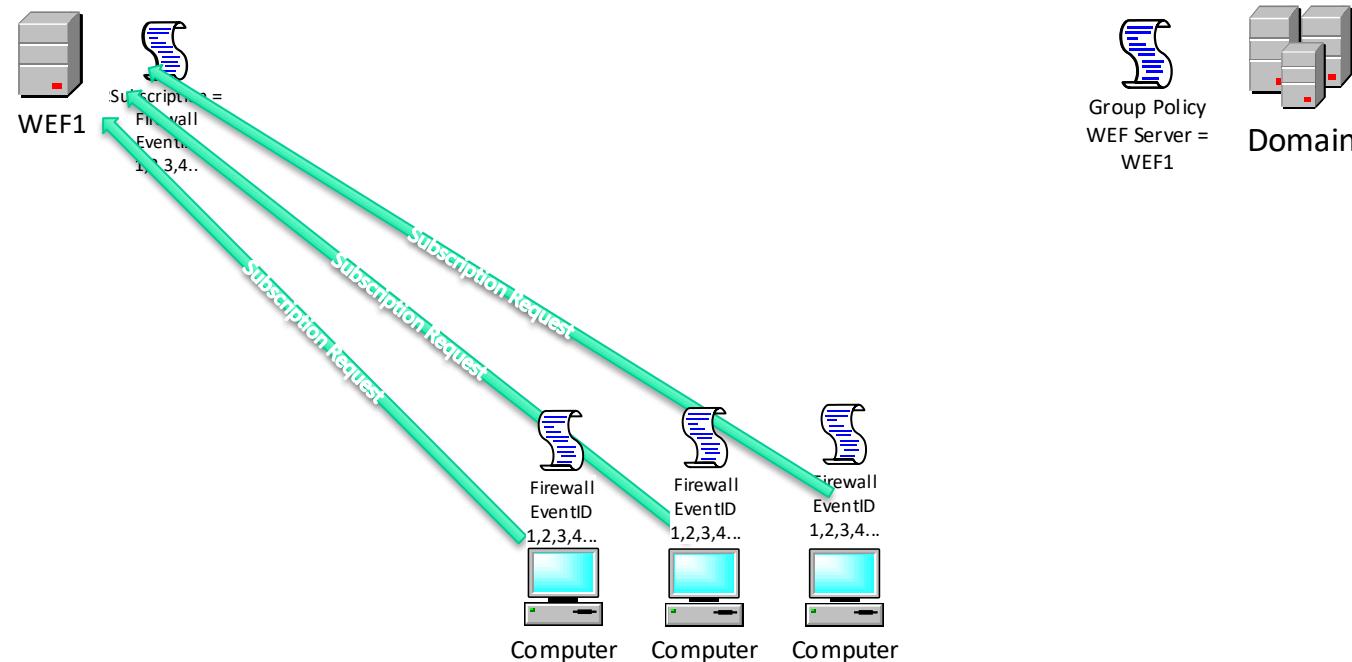
WEF Transport Internals

- Uses **Subscriptions** to determine which events to forward
 - Source-initiated (Push)
 - Collector-initiated (Pull)

WEF Transport Internals



WEF Transport Internals



WEF Transport Internals

Event delivery optimization options	Description
Normal	This option ensures reliable delivery of events and does not attempt to conserve bandwidth
Minimize bandwidth	This option ensures that the use of network bandwidth for event delivery is strictly controlled
Minimize latency	This option ensures that events are delivered with minimal delay

Events collected – Powershell Events

- Purpose: Detecting Malicious Code executed through Powershell
 - 4103 – Module Logging
 - 4104 – Script Block Logging!!!

Events collected – Core Subscription

- Purpose: Indicators of Attack/Persistence Creation
 - Security Event Log 1102 - Security Event Log was cleared
 - System Event Log 7045 - New Service creation event
 - Security Event Log 4720 - New local user created
 - Scheduled Task Operational Log 106/200 - Scheduled Task was registered or executed

Events collected – Account Lockouts

- Purpose: Indicators for Accounts under Attack
 - Security Event Log 4740 - A user account was locked out

Events collected – Interesting Accounts

- Purpose: Monitor potential compromised or Honey Toke Accounts
 - 4624 - Successful LogonSystem Event Log 7045 - New Service creation event
 - 4625 - Unsuccessful Logon
 - 4648 - Logon was Attempted with Explicit Credentials

Events collected – Malware

- Purpose: Monitor Windows Defender Detections and Operational Status
 - 1006 / 1116 – Malware found
 - 1007 / 1117 – Action Taken
 - 1008 – Action failed
 - 2000 / 2002 – Definitions updated
 - 2001 / 2003 – Definitions Update failed

DEMO

Configuring WEF



Sysmon

Simple Threat Detection Stack



Sysmon Overview

- Background system monitoring utility
- Record system events to the Windows event log
- Can be used for system anomaly detection
- Forensics can trace intruder activity across the network

Operational Number of events: 965 () New events available				
Level	Date and Time	Source	Event ID	Task Category
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:47 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:41 PM	Sysmon	3 (1)	
Information	7/27/2014 7:21:41 PM	Sysmon	1 (1)	
Information	7/27/2014 7:21:41 PM	Sysmon	3 (1)	
Information	7/27/2014 7:21:26 PM	Sysmon	3 (1)	
Information	7/27/2014 7:20:45 PM	Sysmon	3 (1)	
Information	7/27/2014 7:10:55 AM	Sysmon	2 (1)	

Event 1, Sysmon

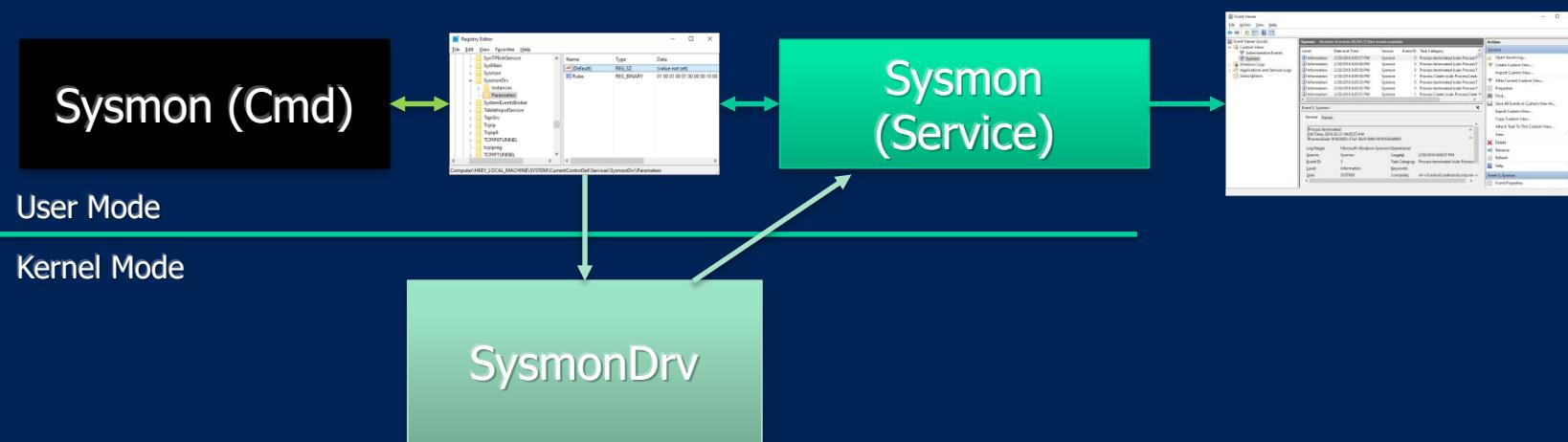
Friendly View XML View

+ System

- EventData

UtcTime	7/28/2014 2:21 AM
ProcessGuid	{00502001-B3BB-53D5-0000-001020881A63}
ProcessId	15060
Image	C:\WINDOWS\system32\eventvwr.exe
CommandLine	"C:\WINDOWS\system32\eventvwr.exe"
User	NTDEV\markru
LogonId	0xae2d0
TerminalSessionId	1
IntegrityLevel	Medium
HashType	SHA1
Hash	1CBCCBAB8A152EC2F64E910797CED089880F6670
ParentProcessGuid	{00502001-53F7-53C0-0000-00107DCD0E00}
ParentProcessId	5508
ParentImage	C:\WINDOWS\Explorer.EXE
ParentCommandLine	C:\WINDOWS\Explorer.EXE

Sysmon Architecture



Basic Configuration Options

- Installing with no options logs all the following with SHA1 hashes where applicable:

Process create, Process terminate, Driver loaded, File creation time changed, Sysmon service state changed, Sysmon configuration changed

- Additional basic options:

Option	Description
-h [SHA1] [MD5] [SHA256] [IMPHASH] [*]	Hash algorithm(s)
-n [process,...]	Logs network events
-l [process,...]	Logs image load events
--	Restores default configuration (-c only)

Hashes and VirusTotal

- You can extract a hash and paste it into VT search for a report:

The screenshot displays two windows side-by-side. On the left is a Sysmon event viewer showing an event titled 'Event 1, Sysmon' with a timestamp of 9/13/2014 12:21:50 PM. The 'General' tab is selected, showing details about a process creation event. Key information includes:

- Process Create:
- UtcTime: 9/13/2014 7:21 PM
- ProcessGuid: {00000000-9920-5414-0000-0010ba4b8a02}
- ProcessId: 3928
- Image: C:\Users\test\AppData\Local\Temp\drvinst-2.exe
- CommandLine: "C:\Users\test\AppData\Local\Temp\drvinst-2.exe" /ci
- User: Vera-PC\test
- LogonGuid: {00000000-d33f-5412-0000-0020a7d11701}
- LogonId: 0x117D1A7
- TerminalSessionId: 1
- IntegrityLevel: Medium
- HashType: SHA1
- Hash: 7297DFCED5D4686860F5936015EAC1085EFBD42
- ParentProcessGuid: {00000000-98e0-5414-0000-0010e31c8a02}
- ParentProcessId: 1044
- ParentImage: C:\Users\test\AppData\Local\SwvUpdater\Updater.exe
- ParentCommandLine: C:\Users\test\AppData\Local\SwvUpdater\Upda

On the right is a browser window displaying the VirusTotal analysis page for the SHA256 hash a96b6460cf356fceac19e7ef65da417d7475b70067804ff7d4665b64ee0965fd. The analysis results show:

- SHA256: a96b6460cf356fceac19e7ef65da417d7475b70067804ff7d4665b64ee0965fd
- File name: inethnfd-setup.exe
- Detection ratio: 22 / 55
- Analysis date: 2014-09-15 04:39:59 UTC (1 year, 5 months ago)

The VirusTotal interface includes tabs for Analysis, File detail, Additional information, Comments (0), Votes, and Behavioural information. Below the analysis table, there is a legend indicating 0 red faces and 0 green faces.

Antivirus	Result	Update
AVG	Generic_r.TL	20140915
Agnitum	PUA.Amonetize!	20140914
AhnLab.V3	PUP/Mim32.Amonetize	20140914

Best Practices and Tips

- Install it on all your systems
 - Proven at scale
 - Data will be there when you need it for DFIR
- Configure all event types for maximum visibility
 - Filter out noise, especially uninteresting image loads
 - Test overhead on mission-critical systems
 - Make sure event log is large enough to capture desired time window
- Forward events off box
 - To prevent deletion by attackers
 - For analyzing aggregate network behavior
 - For tracing activity between systems

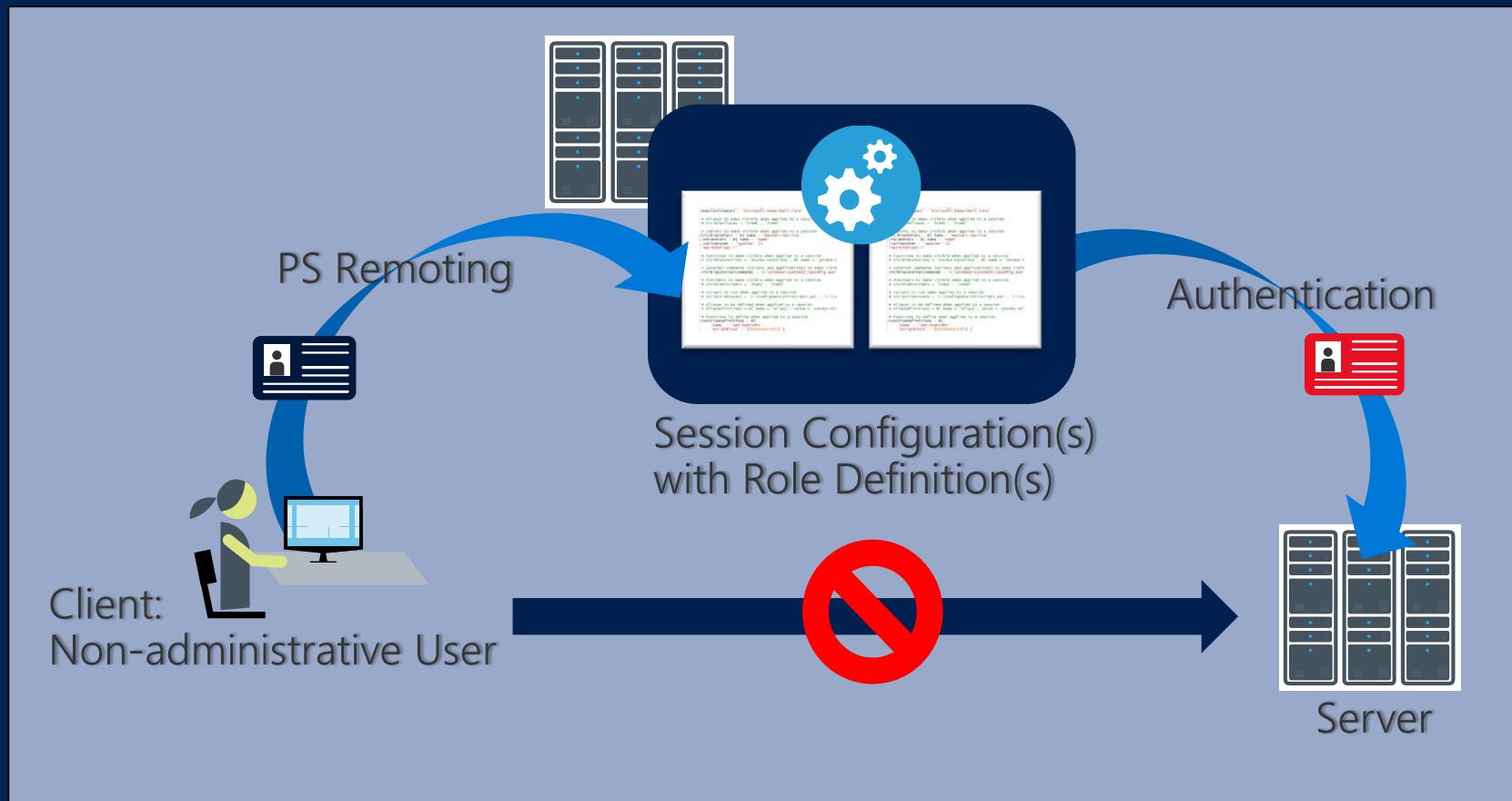


Just Enough Administration

Use Cases

- High privileged operations outsourced
 - Junior Administrators
 - Supporter
 - Server Operators
- Service Accounts
- Client Help Desk
- Multi-Tenant Administration
- Auditing
- Lower trust system operations
- Securing “in-Tier” Credentials
- ...and many more...

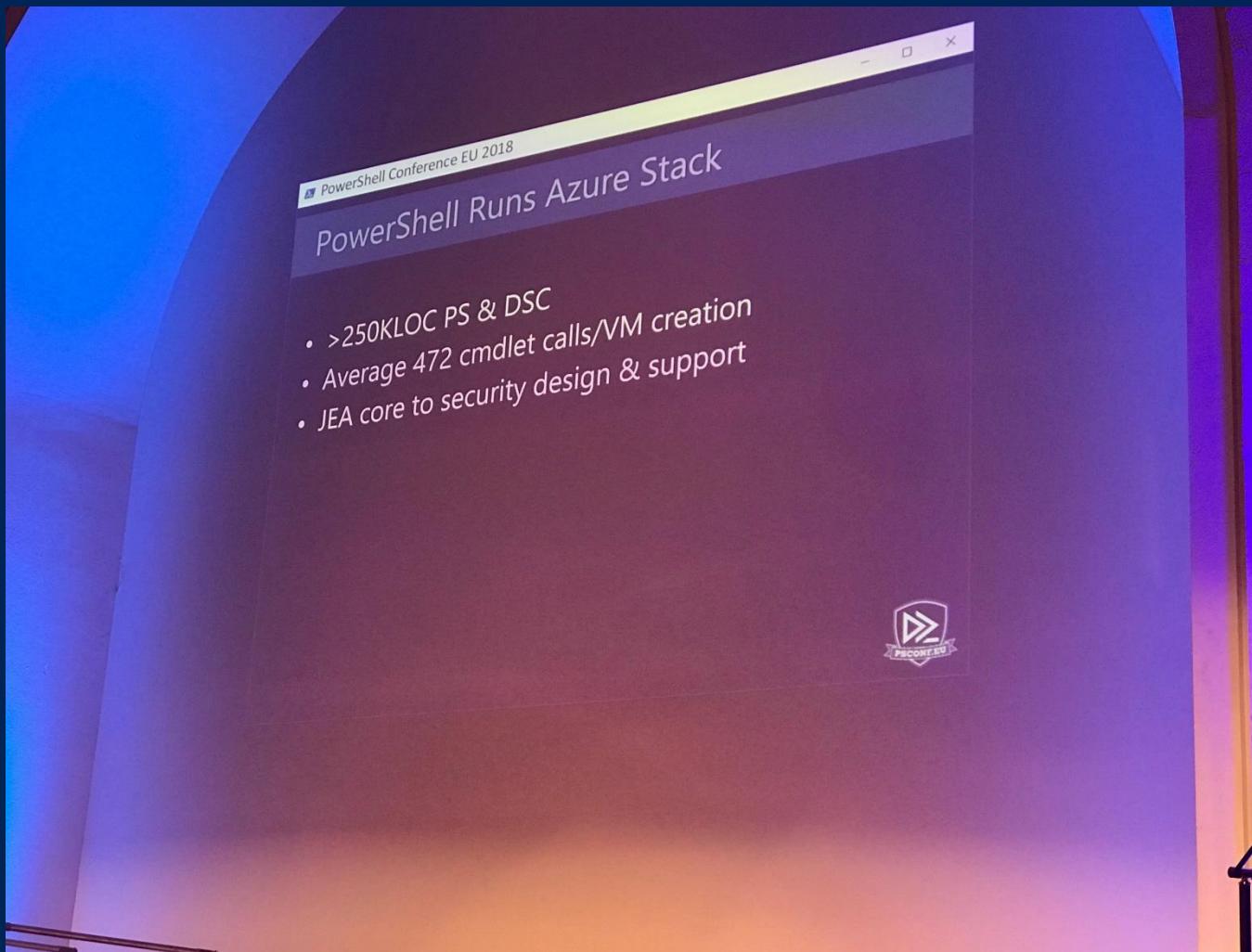
JEA functionality



Prerequisites

PowerShell 6 Core:
Everywhere

PowerShell Runs Azure Stack



DEMO

Most common concerns about JEA

- Oh, it's difficult to implement
 - Yes it is, but we are working on it
 - Feel free to submit your role template configs
- ...is there a GUI?
 - Windows Admin Center (formerly Project Honolulu)

The screenshot shows the Windows Admin Center interface with the title 'Windows Admin Center'. The main section is titled 'All Connections' and displays a list of three items. The columns are 'Name', 'Type', 'Last Connected', 'Managing As', and 'Tags'. The items are:

Name	Type	Last Connected	Managing As	Tags
dc01.xyra.corp	Server	4/13/2018 1:57:23 PM	xyra\administrator	
srv01.xyra.corp	Server	Never	xyra\administrator	
win10.xyra.corp	Windows PC	Never	xyra\administrator	

Windows Admin Center

DEMO

Windows Admin Center – JEA support



Miriam Wiesner
@MiriamXyra

Hey [@servermgmt](#) - is there an easy way to track the commands used by Windows Admin Center to build more granular [#JEA](#) role capability files?

04/13/18, 9:38 PM

1 LIKE



...

Windows Admin Center – JEA support



Ryan Puffer
@rpsqrd

Replying to @MiriamXyra and @servermgmt

Hey Miriam! Windows Admin Center doesn't directly call underlying cmdlets, instead we call custom functions which can run several commands in succession if necessary. You can see those functions by running "Get-Command -Module Microsoft.Sme*" on a machine configured for RBAC. 1/2

04/16/18, 11:01 PM

2 RETWEETS 1 LIKE



Ryan Puffer
@rpsqrd

Replying to @rpsqrd and 2 others

We'd love it if you could file a request on User Voice for custom role support (and get others to upvote it if it's important to them, too!) 2/2

windowsserver.uservoice.com...

04/16/18, 11:04 PM

1 RETWEET 1 LIKE



Please vote on UserVoice!

1
vote

Voted!

Implement a possibility to configure individual JEA roles in Windows Admin Center

We need custom role support for adding custom defined JEA roles in Windows Admin Center!

 Miriam Wiesner shared this idea · Apr 19, 2018 · [Delete...](#)

0 comments

Add a comment...

[Post comment](#)

 Tweet

<https://aka.ms/Individual-JEA-Roles>





KEEP
CALM
AND
USE
JEA

Call To Action!

-  Apply the latest patches and updates.
-  Adopt best practices for securing & using PowerShell.
-  Implement the principle of least privilege.
-  Deploy behavior monitoring mechanisms.
-  Secure possible points of entry.
-  Disable unnecessary components.
-  Proactively monitor your systems and networks.

And now – How?

Step by step planning

Complete features prioritized

Set up a long-term Roadmap

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

Questions?