PowerShell Security
Live Demo

David das Neves
@David_das_Neves

Julien Reisdorffer
@JReisdorffer

Miriam Wiesner
@miriamxyra

Raimund Andree
@raimundandree

PSCONF.EU

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

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

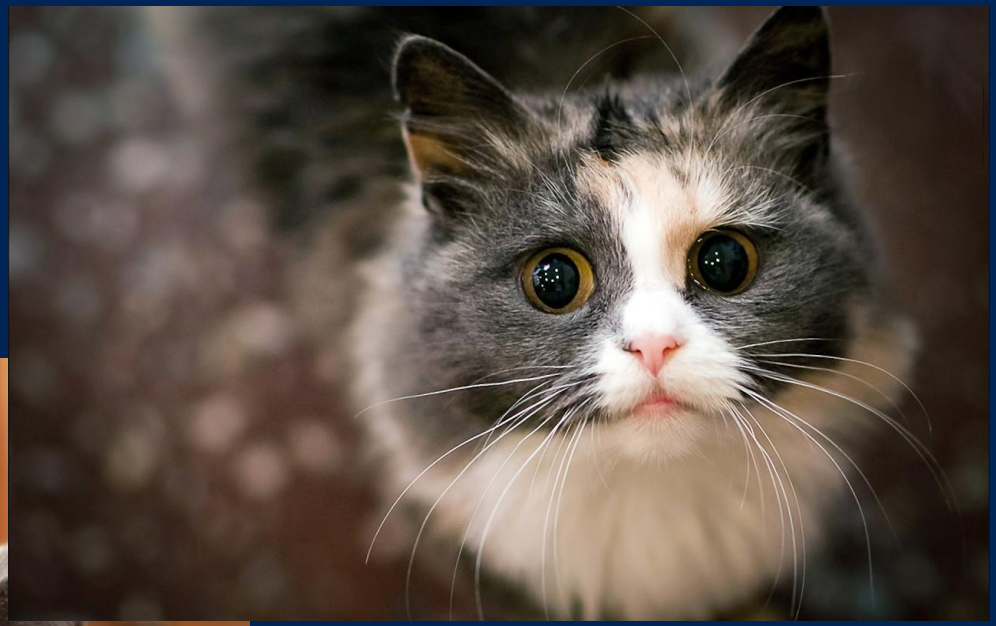
10 | 305 | Like 1

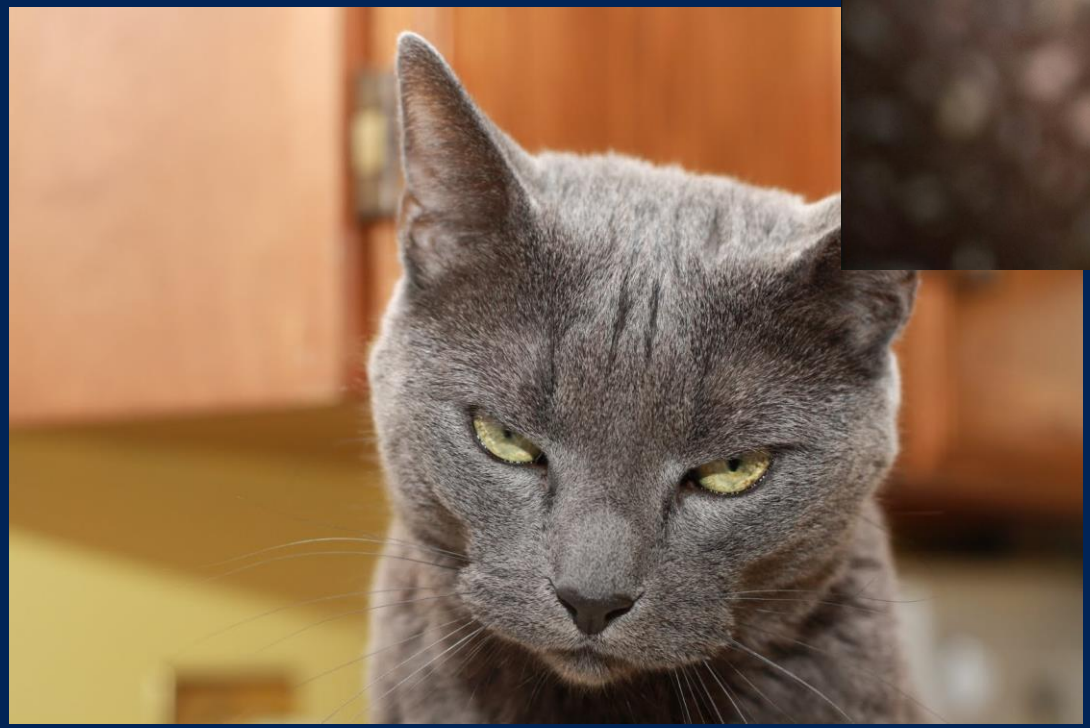
THIS ARTICLE COVERS

The latest quarterly threat report from McAfee noted a fourfold increase in fileless hacking attacks utilising Microsoft PowerShell scripts.

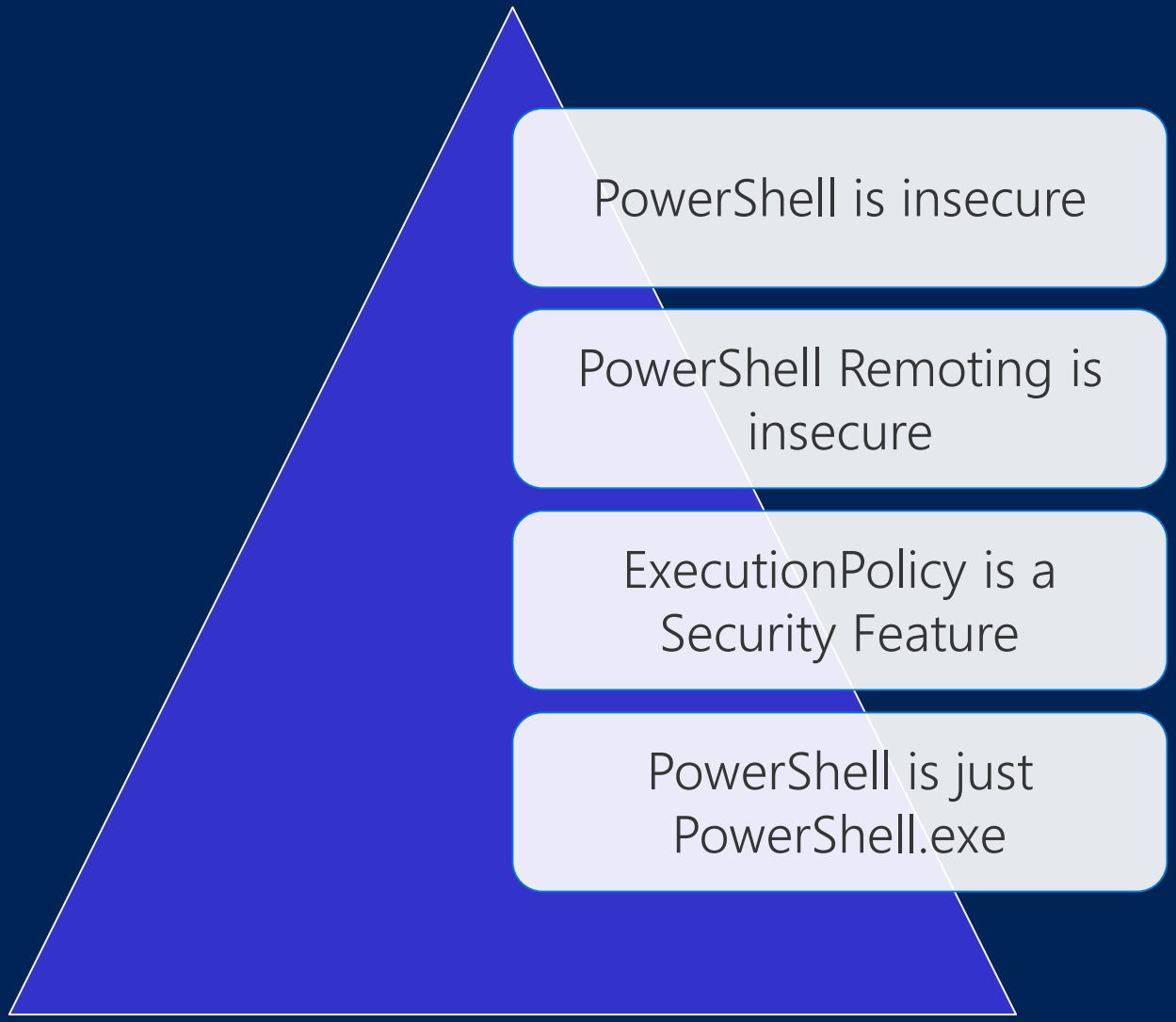
PowerShell activity in its *Unified Threat Research* report.

Powershell is evil.

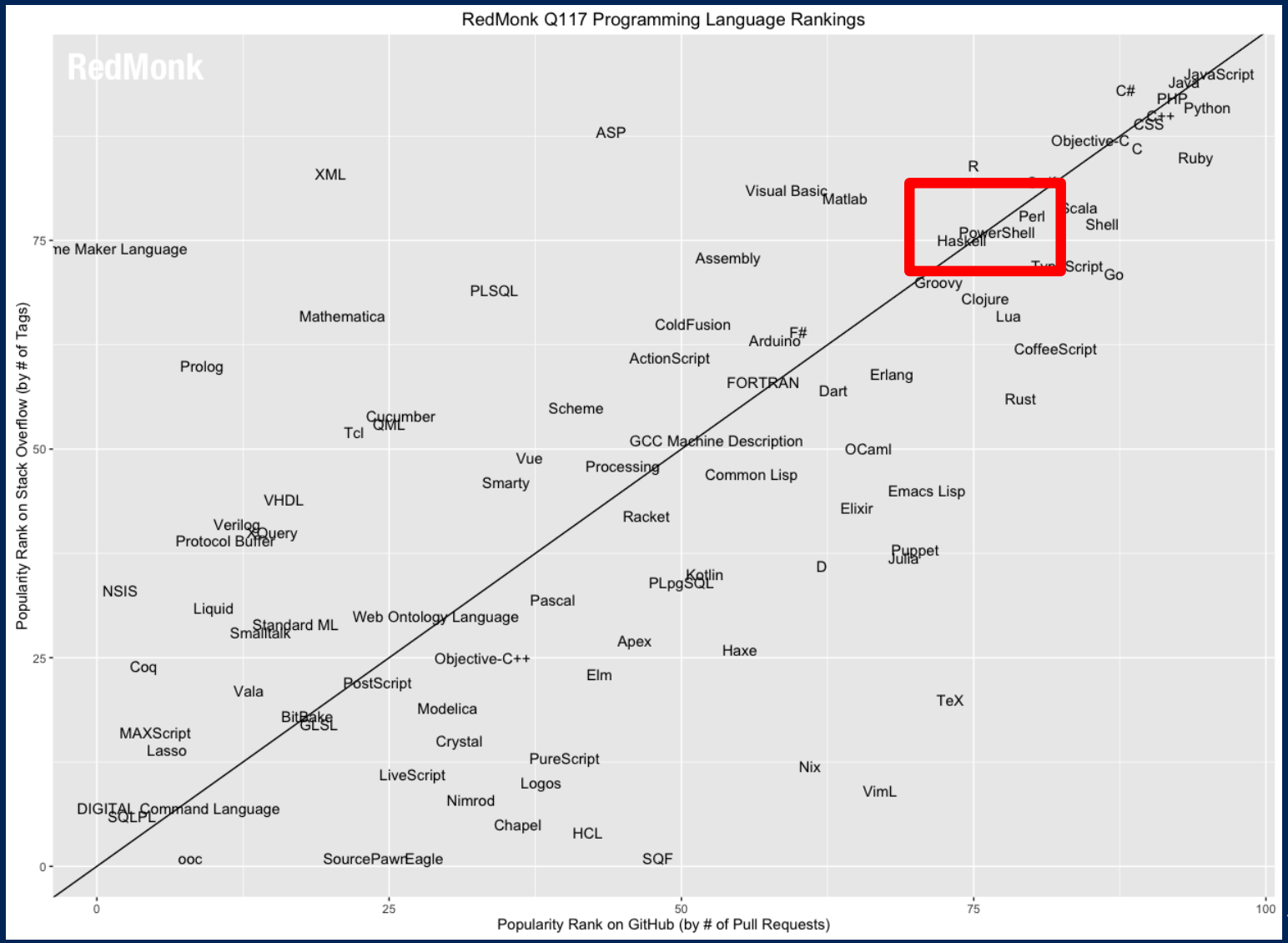




Top Myths



Powershell is powerful



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

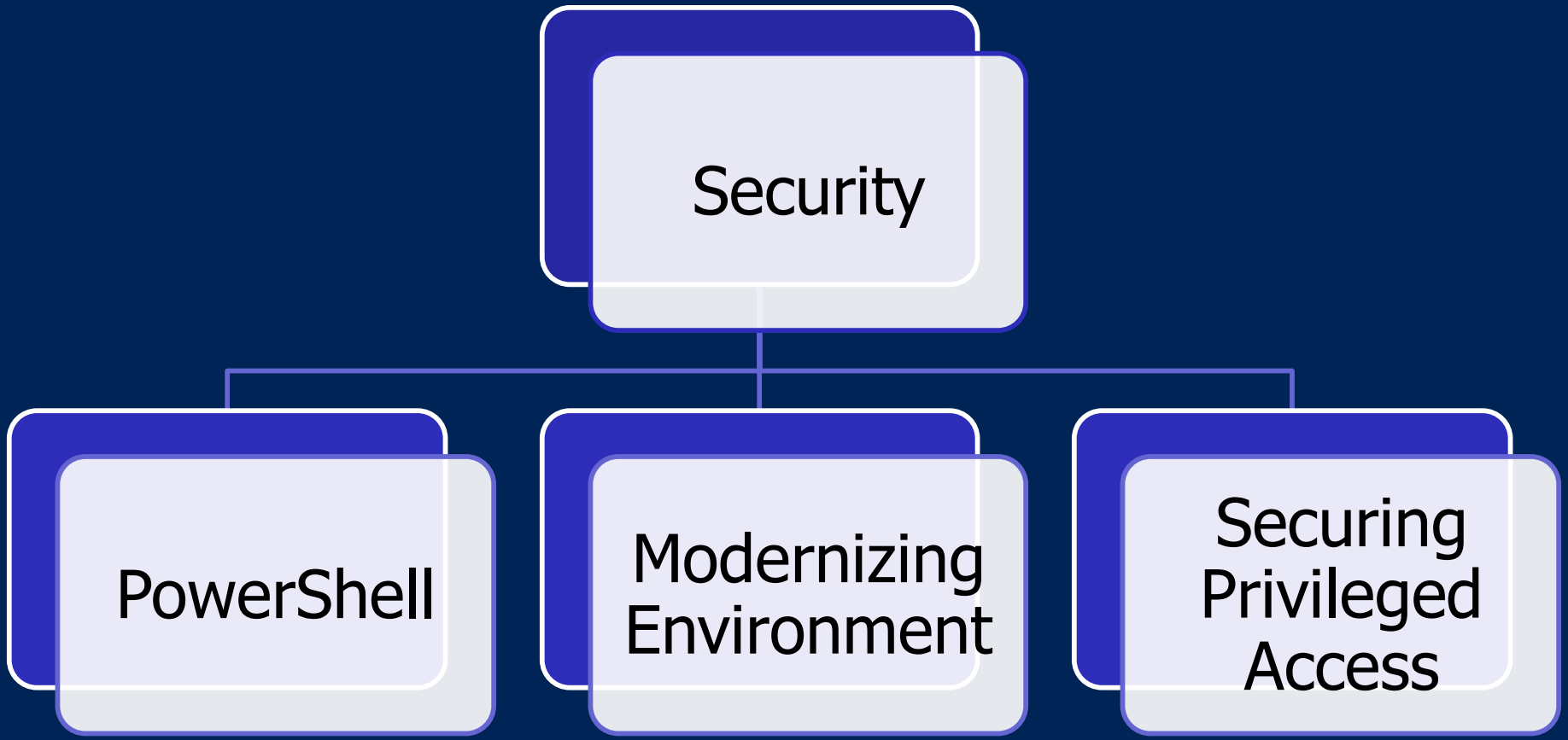
https://blogs.msdn.microsoft.com/powershell/2017/04/10/a-comparison-of-shell-and-scripting-language-security/

Lee Holmes, Azure Management Security, April 10, 2017

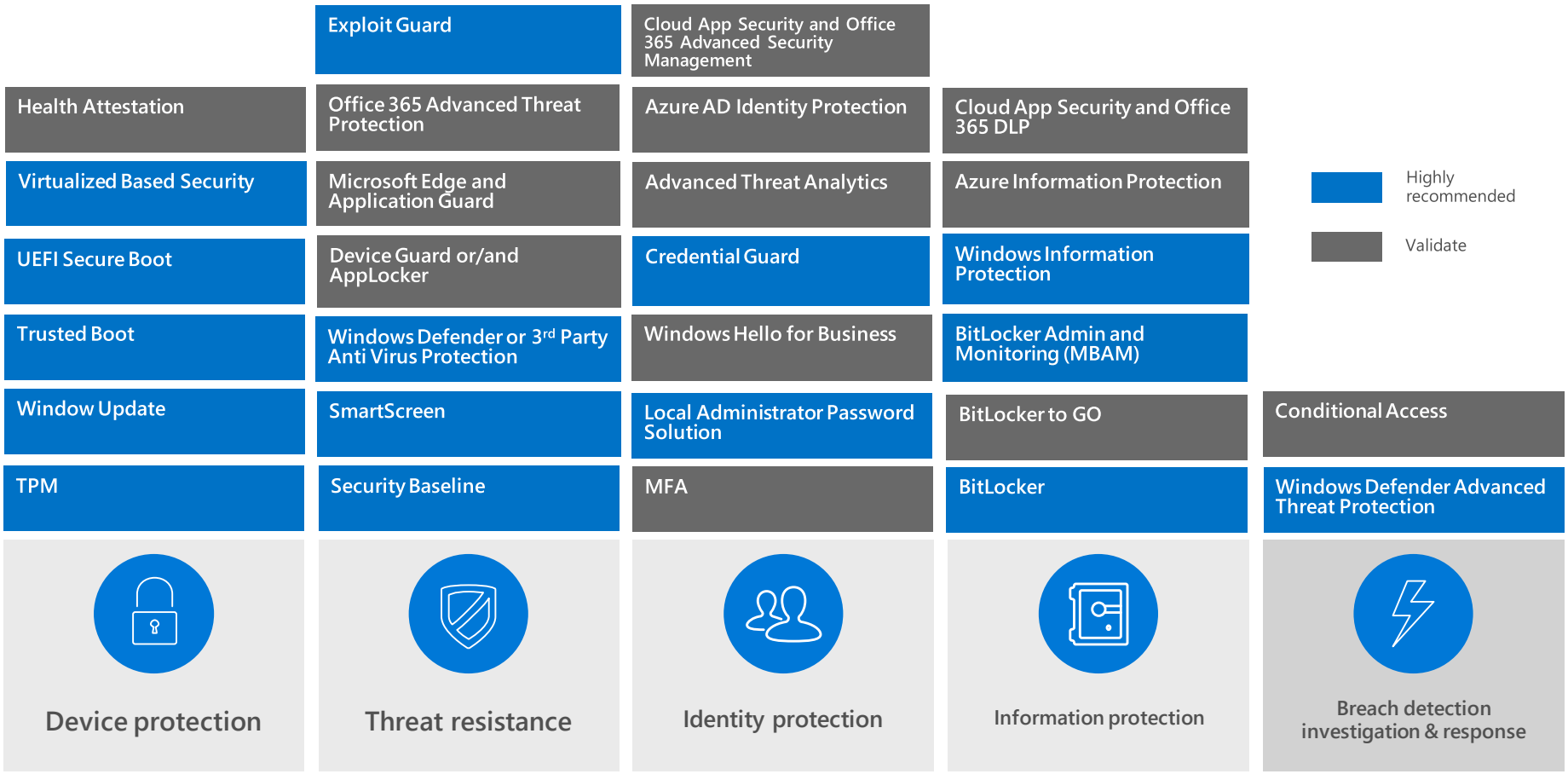
Overview

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
UEFI Secure Boot
Device Guard or/and AppLocker
Credential Guard
Windows Information Protection
Trusted Boot
Windows Defender or 3rd 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
Highly recommended
Validate
Device protection
Threat resistance
Identity protection
Information protection
Breach detection investigation & response

Technical Guideline

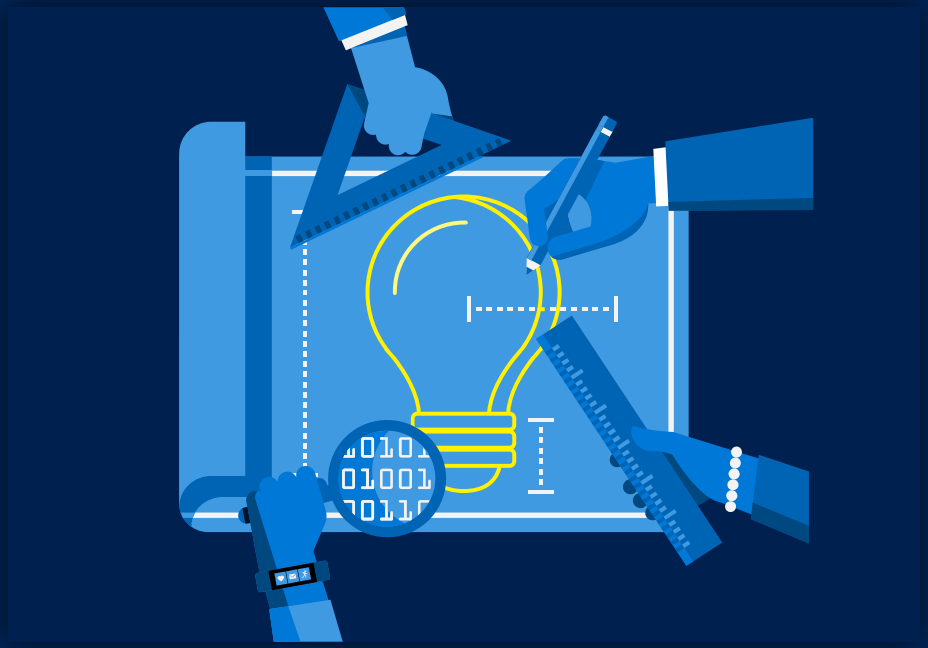
Windows 10 Link List

- 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 Repeatablity

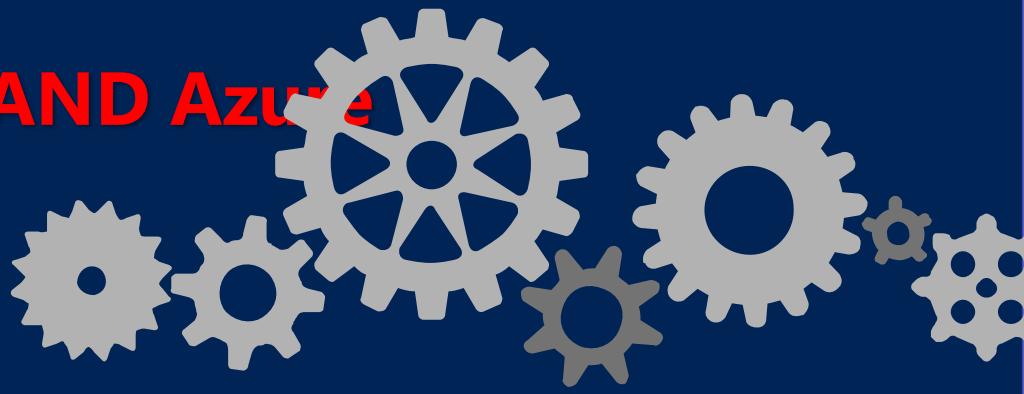
IaC Best Practices

Treat your infrastructure like "cattle",

.....Not "pets"

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**



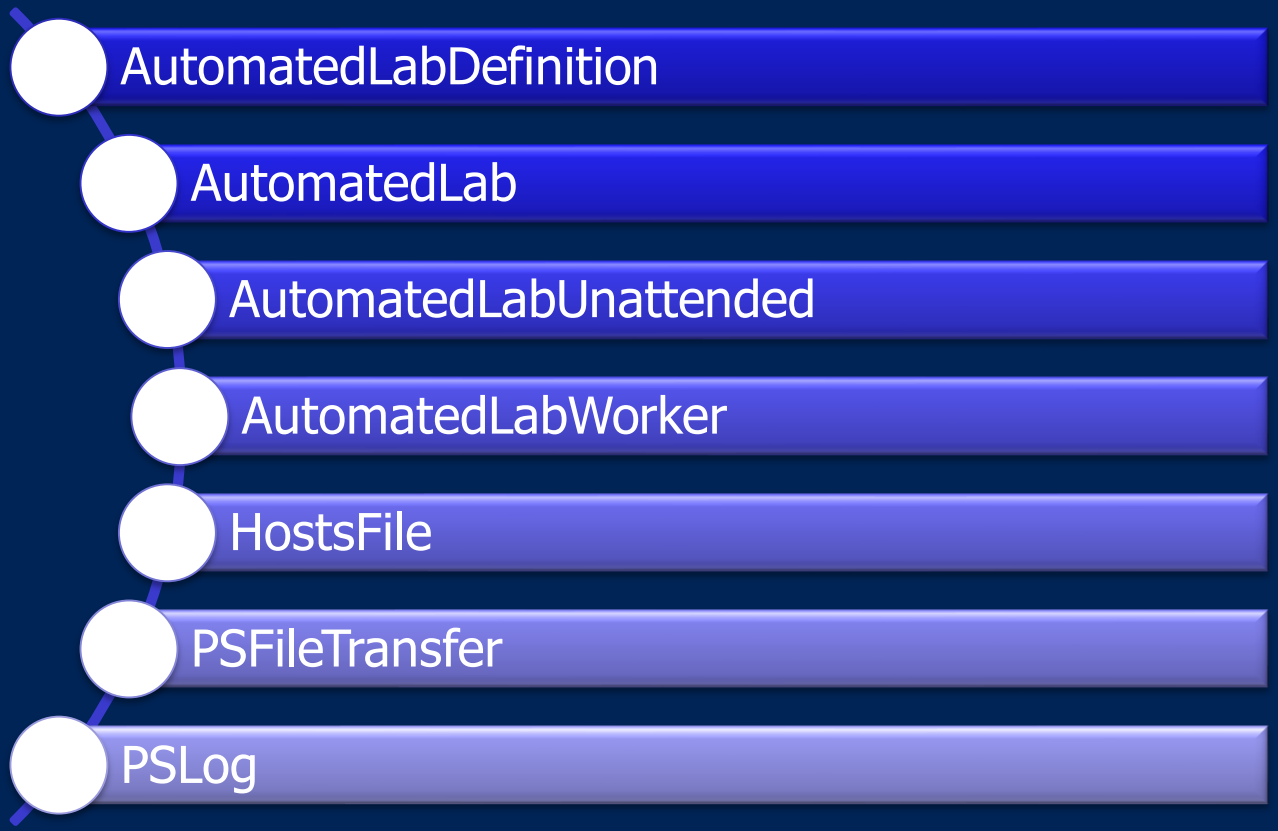
AutomatedLab Requirements

- 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-LabIsoImageDefinition
  - 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

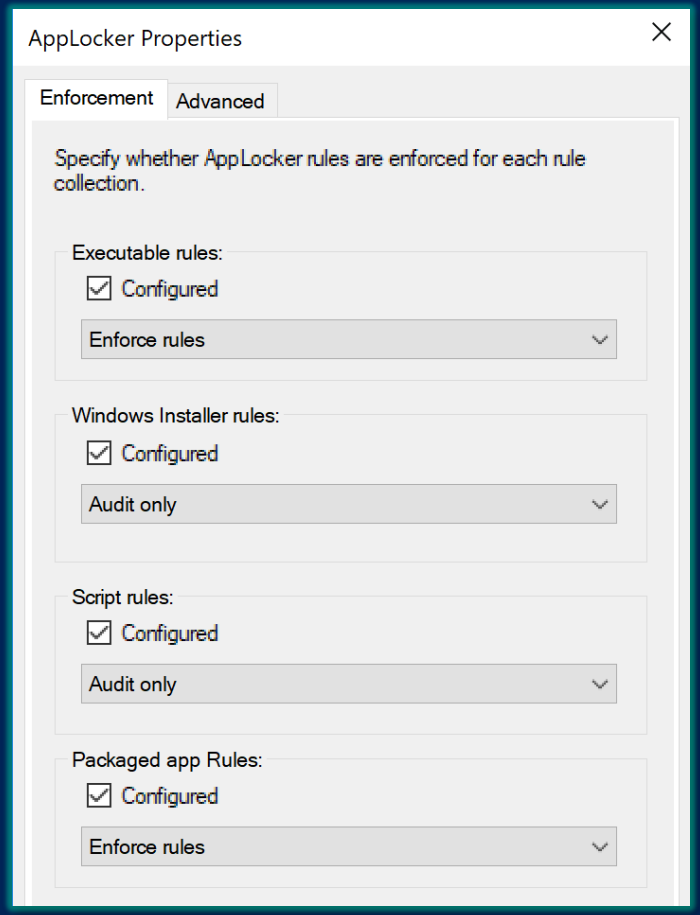
Available implementations

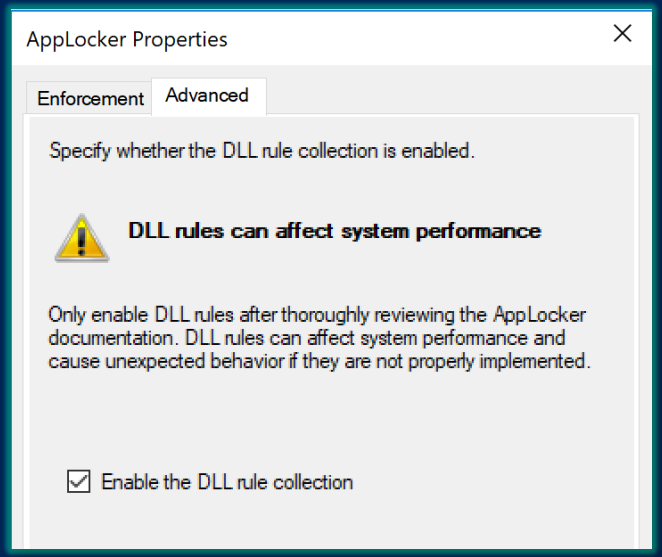
- From Microsoft: AppLocker, ~~Device Guard~~ → Windows Defender Application Control (WDAC)
- Third parties: (expensive)

→ Restricts *non-admin* actions

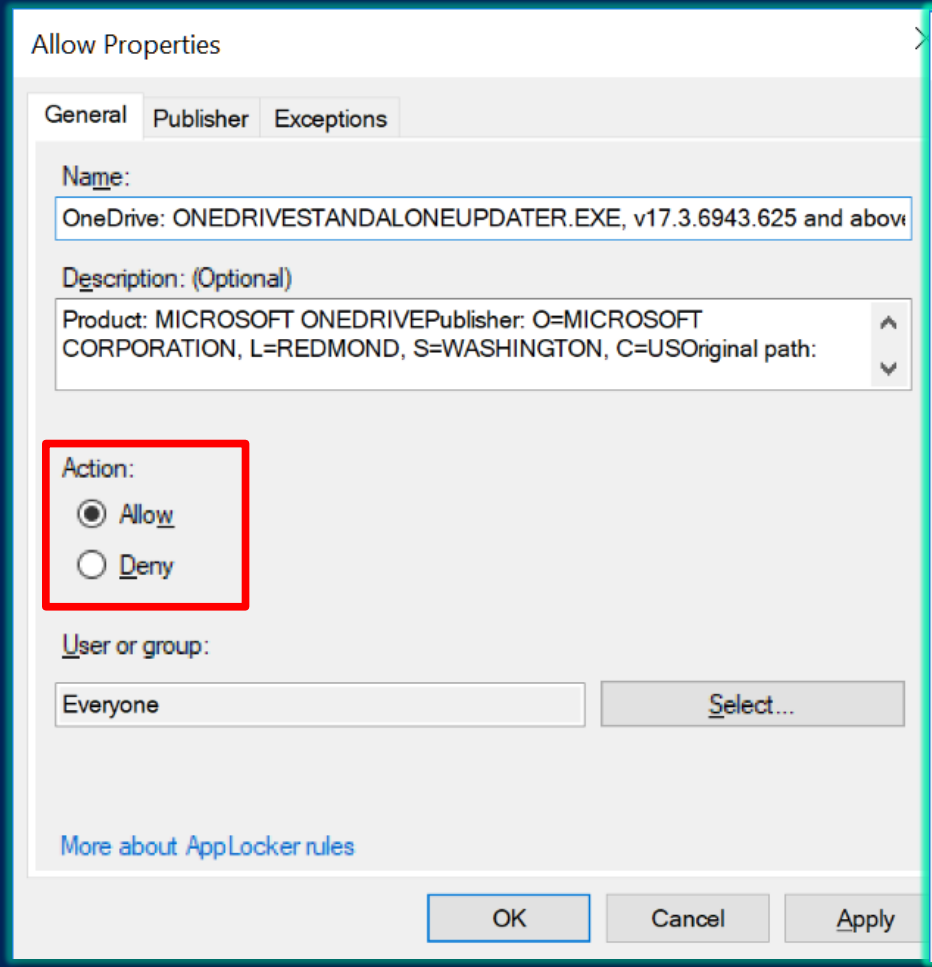
Intro to AppLocker

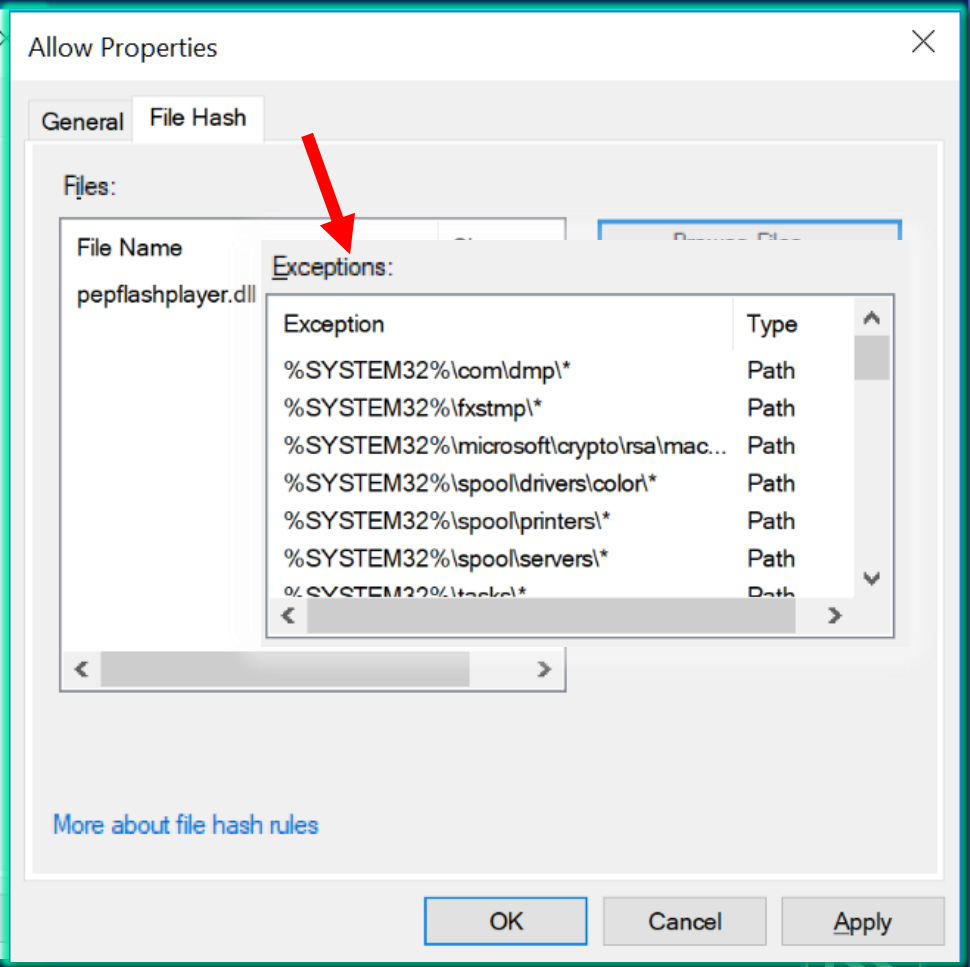
AppLocker rule collections





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

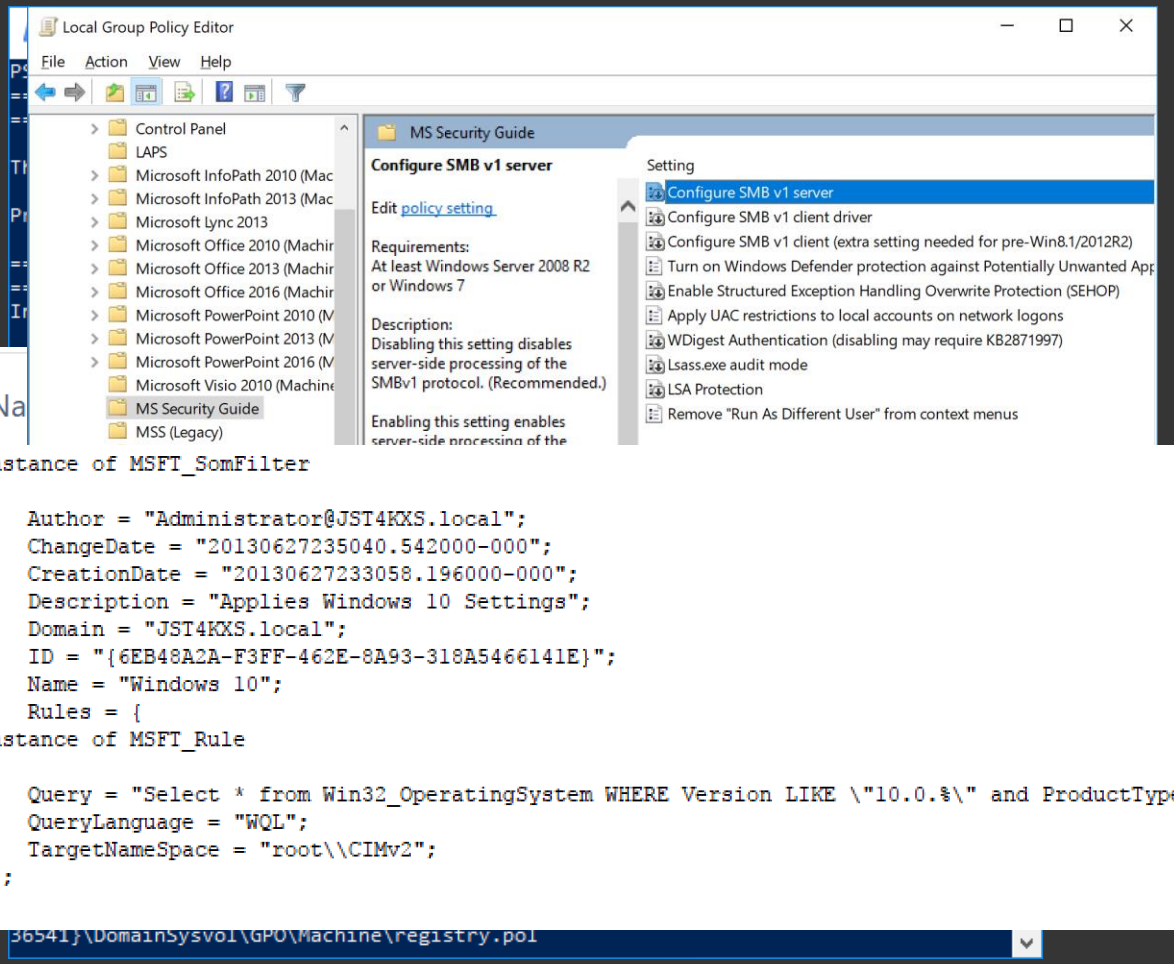
- Don't turn *all* the knobs
- Mitigate contemporary security threats
- Enforce only some defaults

GPO-based

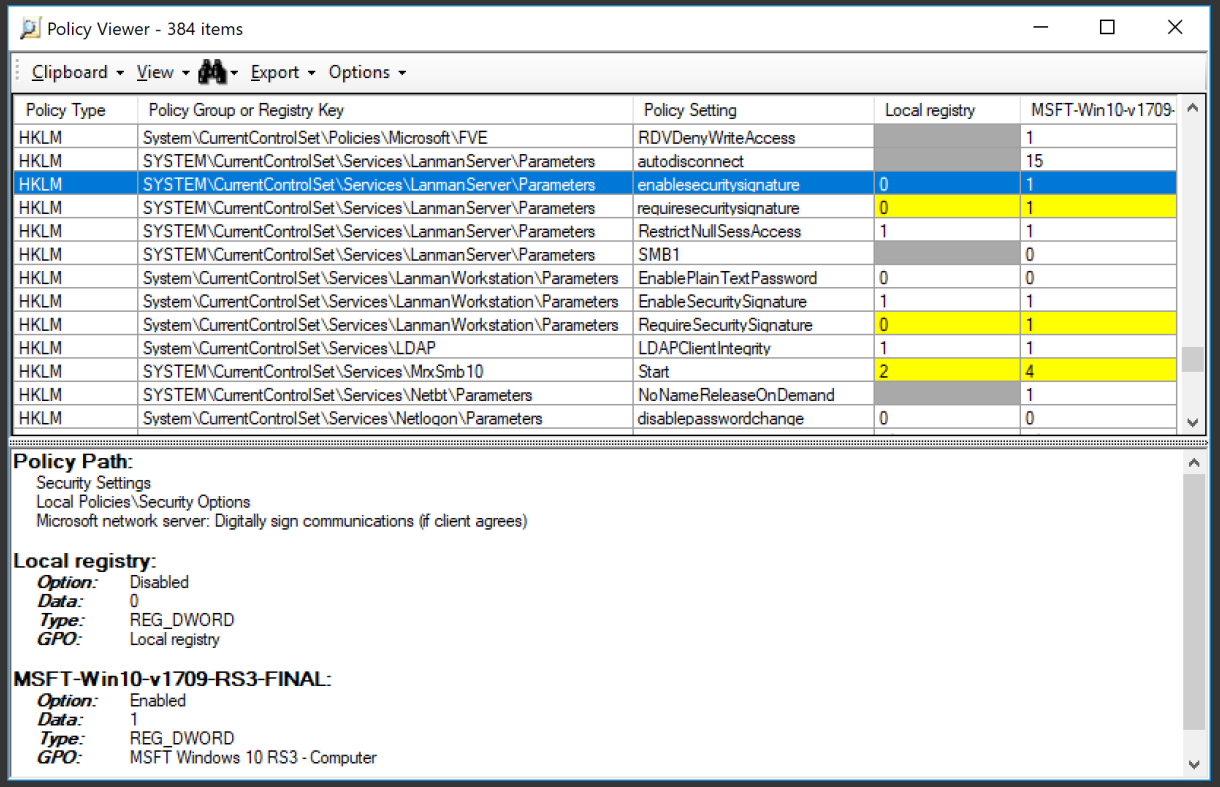
- See also: MDM, DSC

Baseline packages

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



Security Compliance Toolkit – Policy Analyzer



Security Compliance Toolkit – LGPO.exe

```
To apply policy settings:

    LGPO.exe command [...]
```

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

    LGPO.exe /
```

```
To build a Registry.pol file from LGPO text:

    LGPO.exe /r path\lgpo.txt /w path\registry.pol [/v]

    /r path\lgpo.txt       Read input from LGPO text file
    /w path\registry.pol   Write new registry.pol file
```

```
    /m path\re
    /u path\re
    /ua path\r
    /un path\r
    /u:usernar
                             specified by "username"
    /q                       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 Forwading (WEF) and Sysmon

Simple Threat Detection Stack

Windows Event Forwading (WEF)

Simple Threat Detection Stack

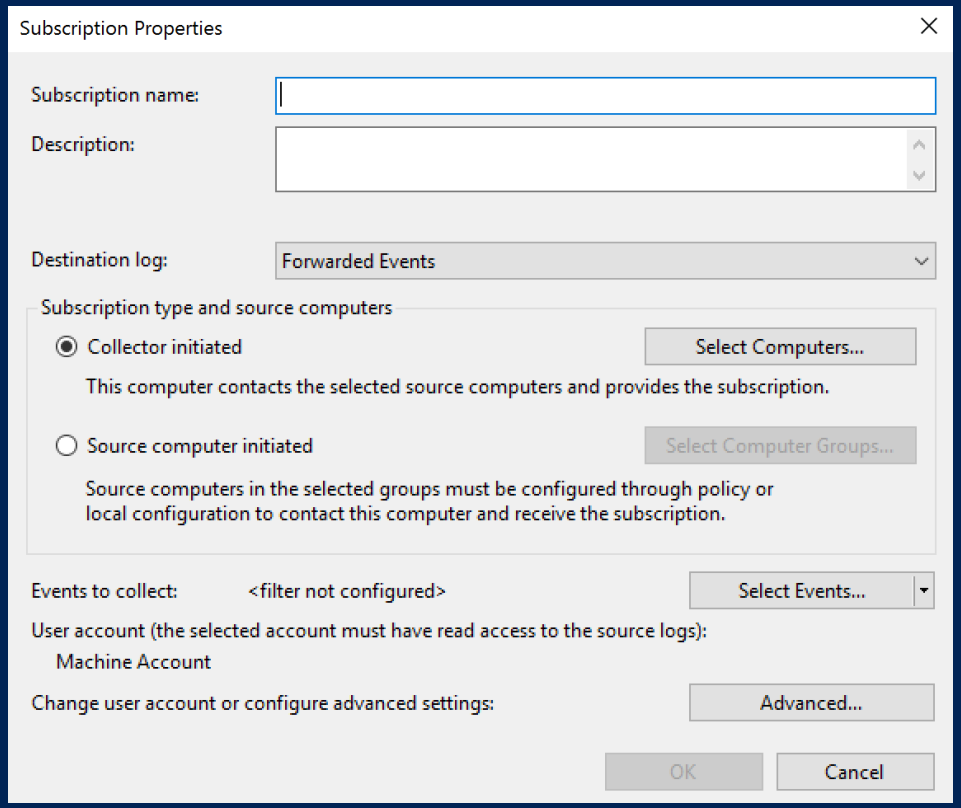
WEF Overview

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

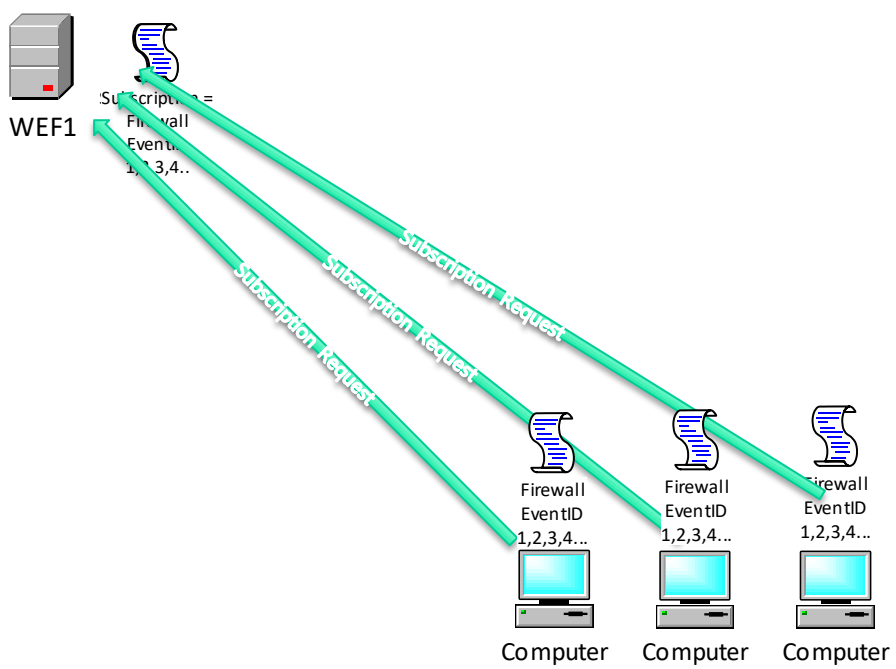
WEF Transport Internals

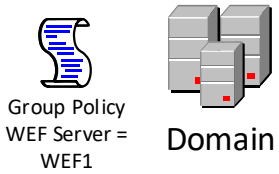
- Uses **Subscriptions** to determine which events to forward
- Source-initiated (Push)
- Collector-initiated (Pull)

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

DEMO

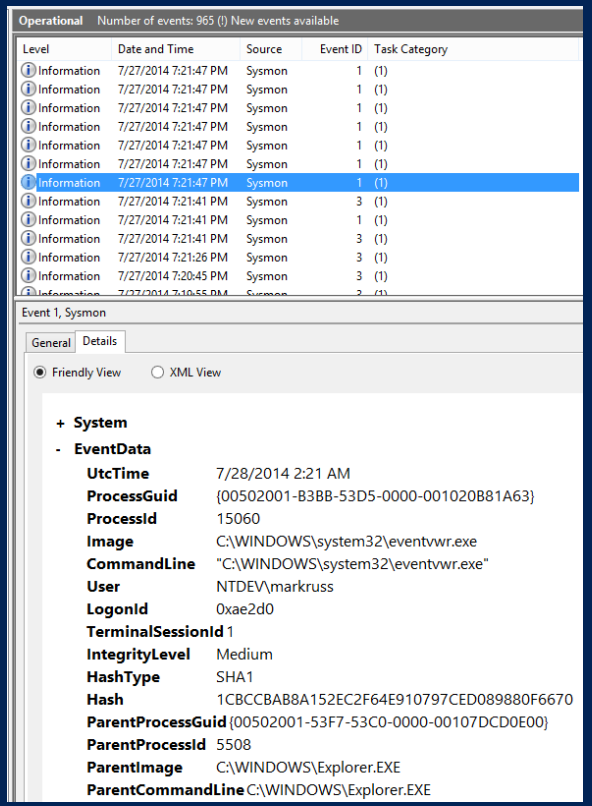
Configuring WEF

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



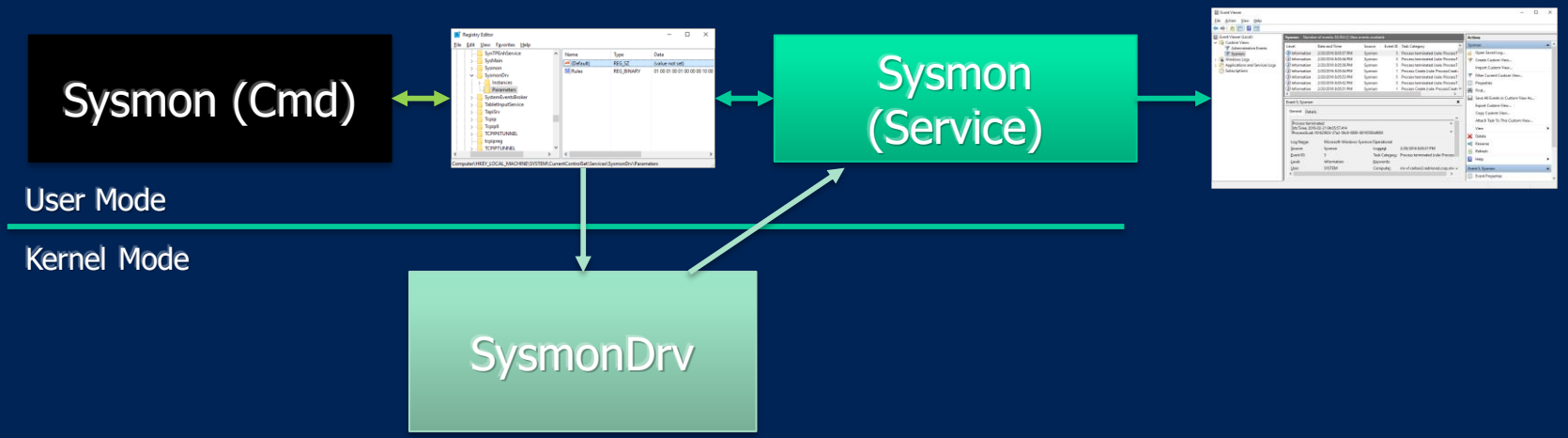
- Windows service and device driver (~2 MB total)
  - Single binary includes 32-bit and 64-bit versions of both
  - Service doubles as command-line frontend
- Installation:
  sysmon -i -accepteula [options]
  - Extracts binaries into %systemroot%
  - Registers event log manifest
  - Enables default configuration

```
Usage:
Install:    sysmon -i [<configfile>]
              [-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]
Configure:  sysmon -c [<configfile>]
              [--|[-h <[sha1|md5|sha256|imphash|*],...>] [-n [<process,...>]]
              [-l [<process,...>]]]
Uninstall:  sysmon -u
```

```
C:\Users\miwiesne\Downloads\SysinternalsSuite>Sysmon.exe -i -accepteula

System Monitor v6.02 - System activity monitor
Copyright (C) 2014-2017 Mark Russinovich and Thomas Garnier
Sysinternals - www.sysinternals.com

Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.
```



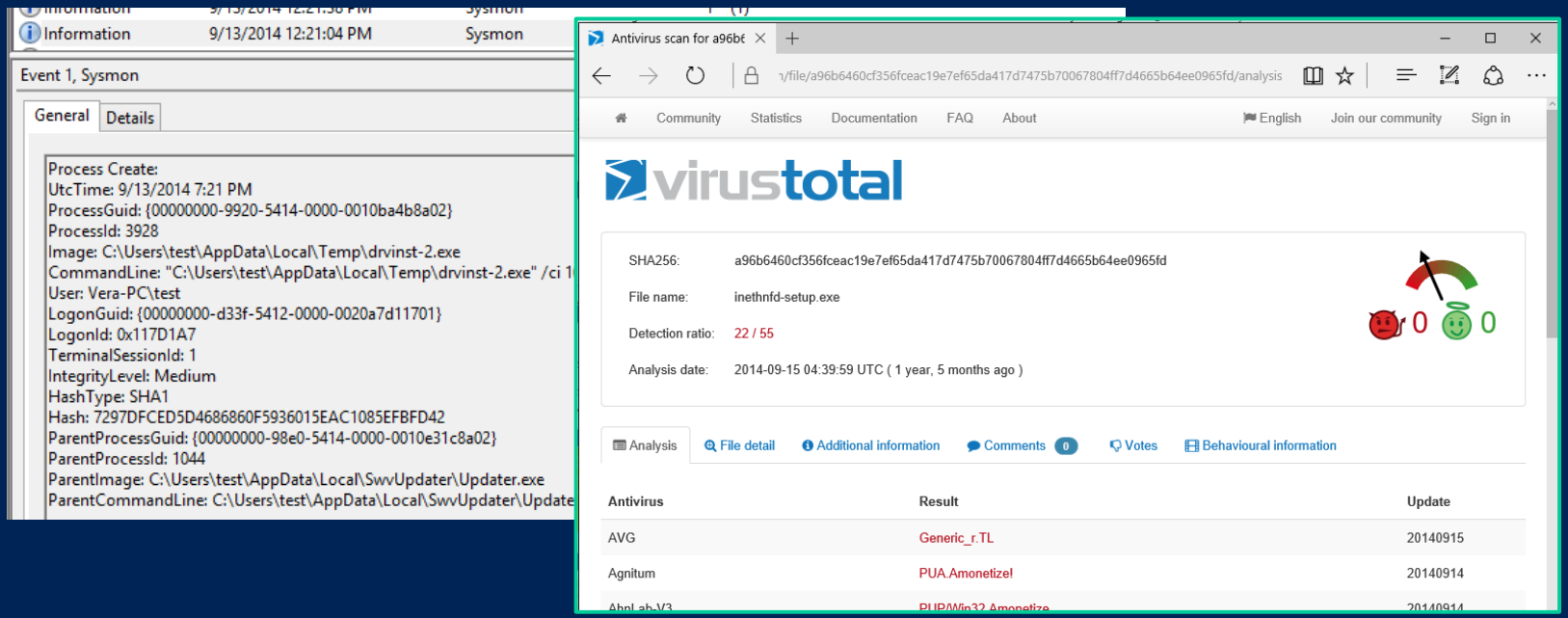
- Installing with no options logs all the following with SHA1 hashes where applicable:

  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)

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



- Basic options are limited:
  - Cannot disable events via basic options (e.g. CreateRemoteThread, RawAccessRead)
  - Advanced filtering not possible (e.g. process name filters)
- Sysmon configuration file supports all configuration options:

  install: **sysmon -i –accepteula c:\SysmonConfig.xml**

  update: **sysmon -c c:\SysmonConfig.xml**

- **@SwiftOnSecurity** (Securitay) has published a Sysmon configuration
  - Has been using Sysmon for over a year
  - Deployed across thousands of systems
  - Commented configuration explains rationale

https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml

- Additional analysis from Lennart Koopman

https://medium.com/@lennartkoopmann/explaining-and-adapting-tays-sysmon-configuration-27d9719a89a8#.rwt51mfrg

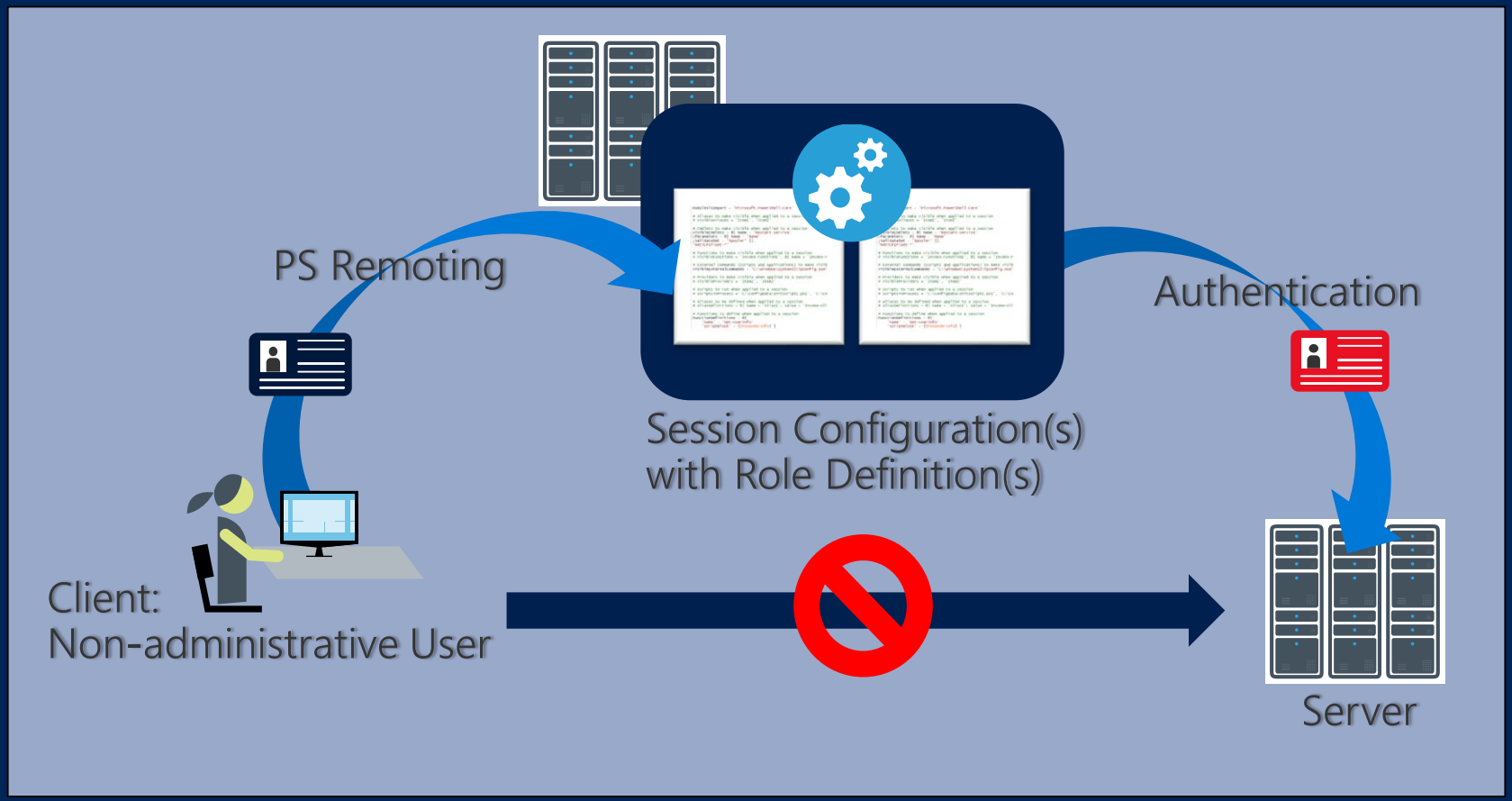
- Install it on all your systems
  - Proven at scale
  - Data will be there when you need it for DFIR
- Configure all event types for maximum visibility
  - Filter out noise, especially uninteresting image loads
  - Test overhead on mission-critical systems
  - Make sure event log is large enough to 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…

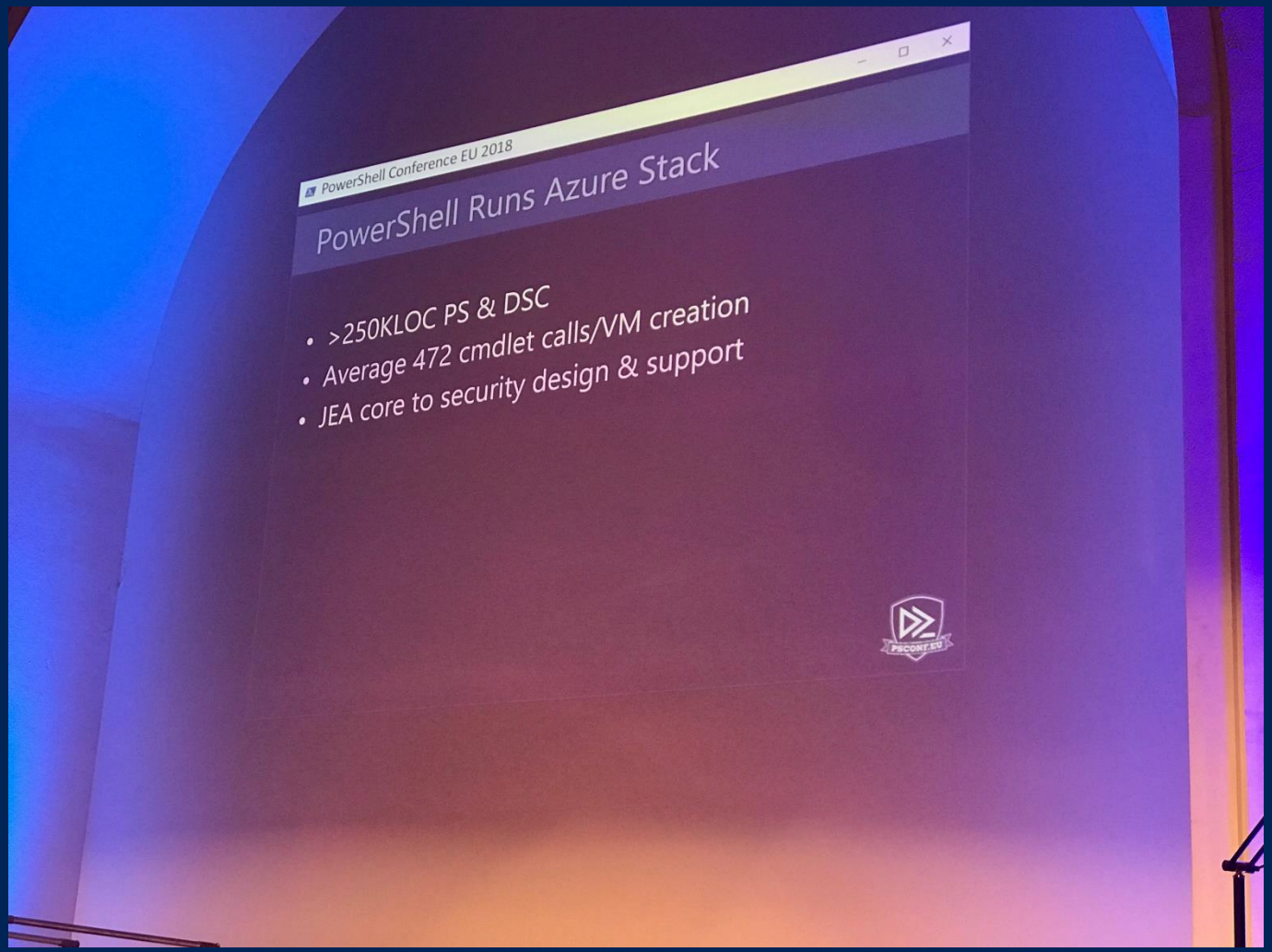
JEA functionality



Prerequisites

PowerShell 6 Core:
Everywhere

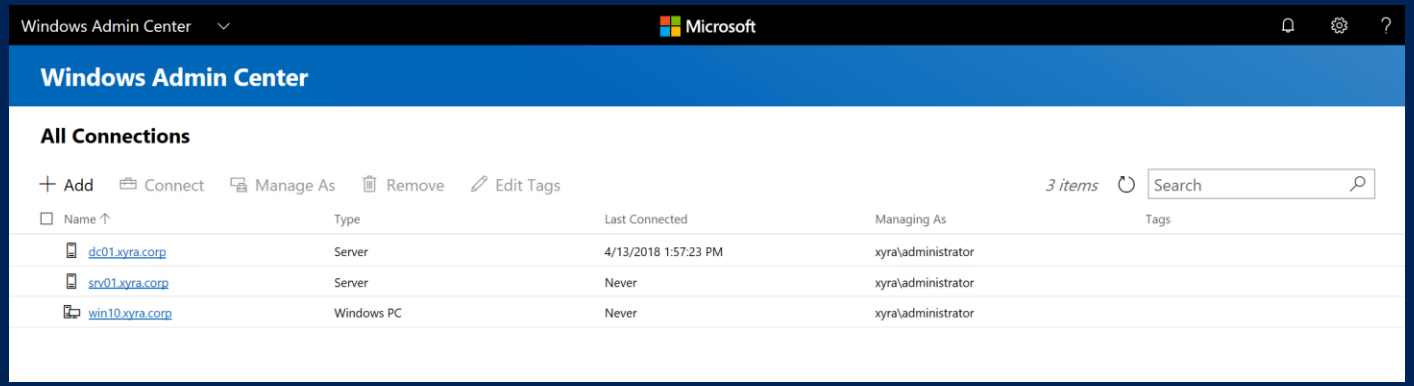
PowerShell Runs Azure Stack



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)



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

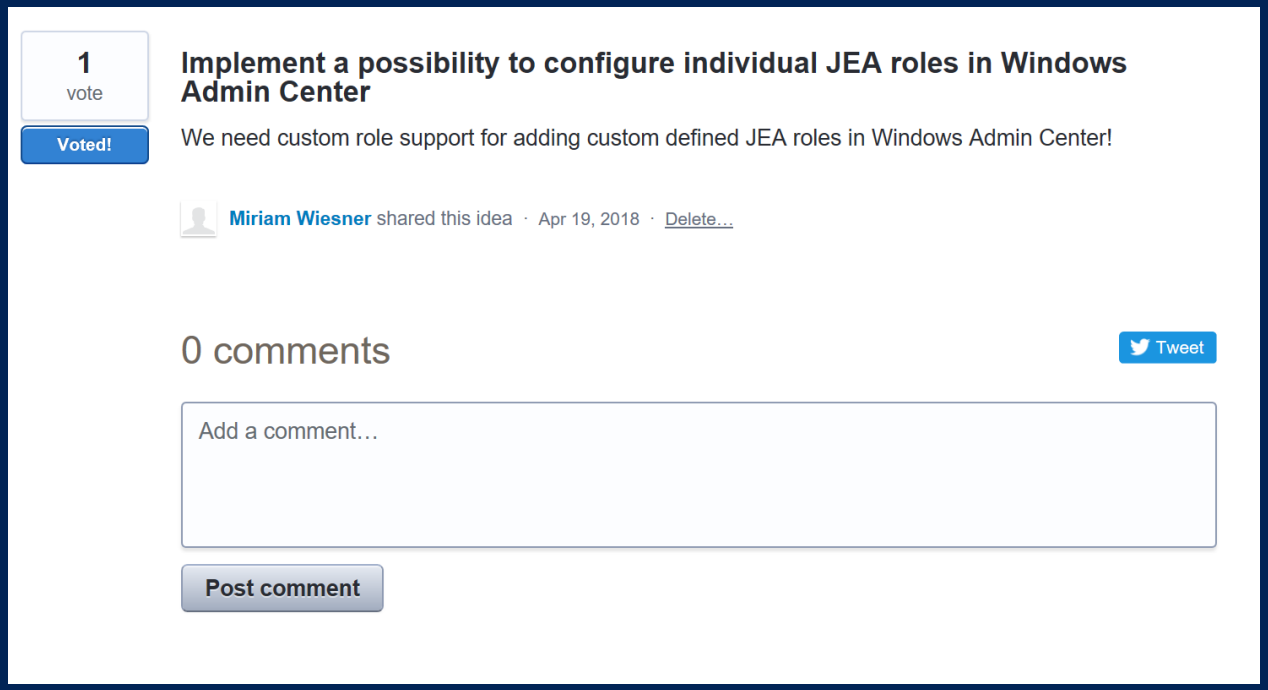
Replying to @rpsqrd and 2 others
We'd love it if you could file a request on User Voice for custom role support (and get others to upvote it if it's important to them, too!) 2/2

windowsserver.uservoice.com...

04/16/18, 11:04 PM

1 RETWEET **1** LIKE

Please vote on UserVoice!



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?