



PowerShell Security

What to prioritize?



David das Neves
Microsoft



Julien Reisdorffer
Microsoft

Julien Reisdorffer : The term 'JReisdorffer' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that ~~the~~^{the} speaker is correct and try again.



2018

At line:1 char:1

+ Julien Reisdorffer

+ ~~~~

+ CategoryInfo : SpeakerNotFound: (JR:Speaker)

[], CommandNotFoundException

+ FullyQualifiedErrorId : CommandNotFoundException

PowerShell Security What to prioritize?



David das Neves

Premier Field Engineer, Microsoft

Julien Reisdorffer

Sr. Consultant Cybersecurity, Microsoft



David das Neves



Agenda

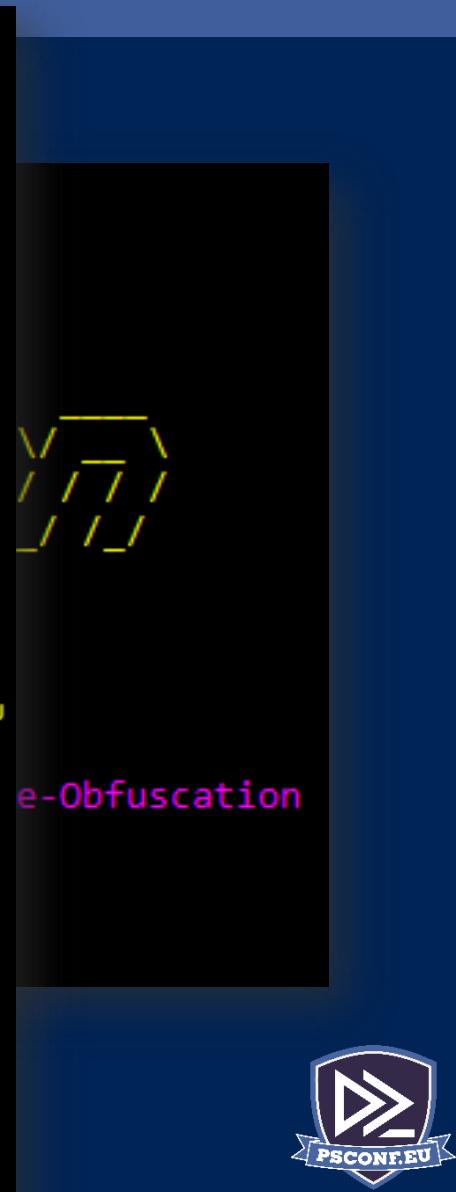
- Introduction / Background PS Security
- Motivation & Implementation
- Demo
- Wrap Up / Call to Action
- Q&A

Intro

Background PS Security



Why PowerShell Security matters



```
C:\Temp\PSAT
=====
Empire:
=====
[Web]: h
=====
PS>Attack
Decrypti
Decrypti
Decrypti
Decrypti
Decrypti
Decrypti
Decrypti
Decrypti
91 Decrypti
Decrypti
1 Decrypti
1 Decrypti
(Emprise)
Decrypti
Choose one of the below options:
[*] MEMORY      Memory-only remote download cradles
[*] DISK         Disk-based remote download cradles
```

Tool :: Invoke-CradleCrafter
Author :: Daniel Bohannon (DBO)
Twitter :: @danielhbohannon
Blog :: http://danielbohannon.com
Github :: https://github.com/danielbohannon/Invoke-CradleCrafter
Version :: 1.0
License :: Apache License, Version 2.0
Notes :: If (!\$Caffeinated) {Exit}

To HELP MENU :: Available options shown below:

Au	Tutorial of how to use this tool	TUTORIAL
Tw	Show this Help Menu	HELP,GET-HELP,?, -?, /?, MENU
Bl	Show options for cradle to obfuscate	SHOW OPTIONS, SHOW, OPTIONS
Cl	Clear screen	CLEAR, CLEAR-HOST, CLS
Gi	Execute ObfuscatedCradle locally	EXEC, EXECUTE, TEST, RUN
Ve	Copy ObfuscatedCradle to clipboard	COPY, CLIP, CLIPBOARD
Wr	Write ObfuscatedCradle Out to disk	OUT
Li	Reset ALL obfuscation for ObfuscatedCradle	RESET
No	Undo LAST obfuscation for ObfuscatedCradle	UNDO
Bo	Go Back to previous obfuscation menu	BACK, CD ..
Qu	Quit Invoke-CradleCrafter	QUIT, EXIT
P	Return to Home Menu	HOME, MAIN

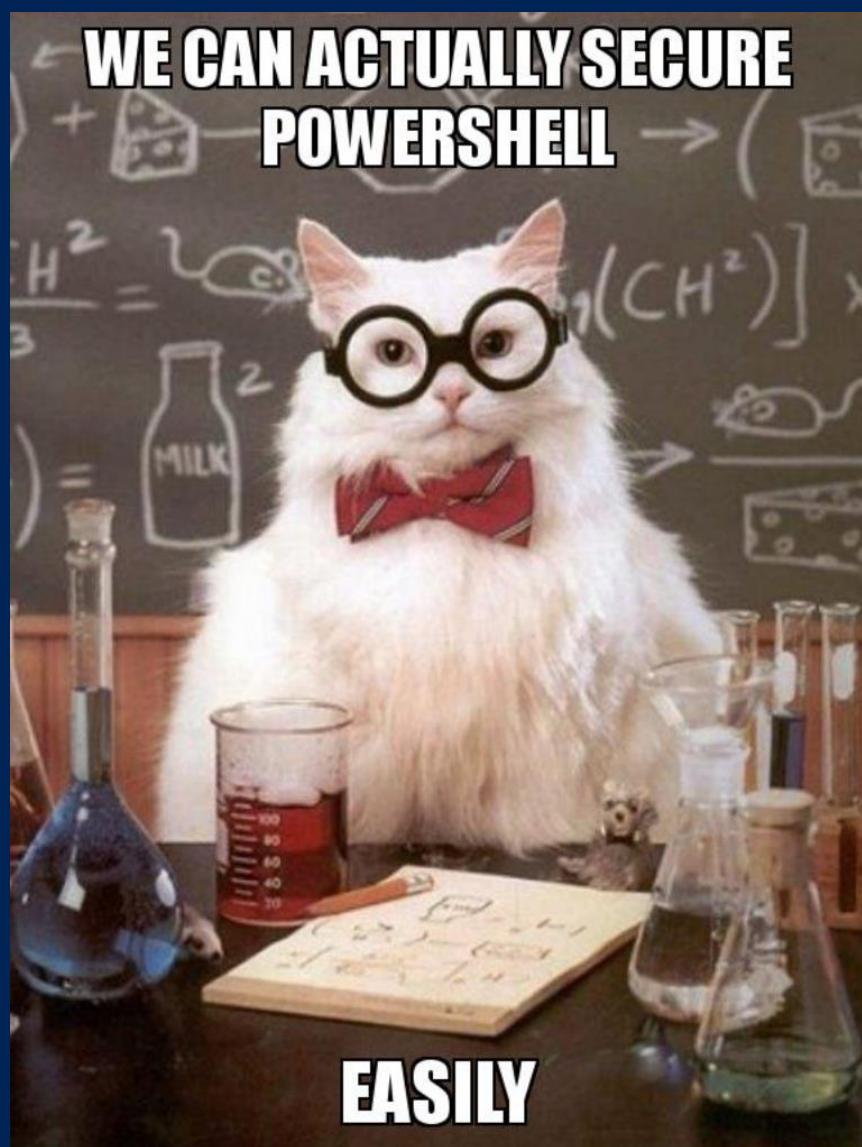
e-Obfuscation

Powershell is evil.

HACKERS USE POWERSHELL

IT'S EVIL!

No it isn't.



EASILY

Some Notes from the Field

"Who the hell should know this all?"

"It's too complicated to set everything up.
Therefore we postponed it for now."

"But Whitelisting is hard! It means that you need to know where all of your scripts are!"

"We actually don't know who uses PowerShell in our company."

"We have set up logging and analysis.
But now we are getting a freakin' high number of incidents!"

"Is it possible to uninstall PowerShell?"

Motivation

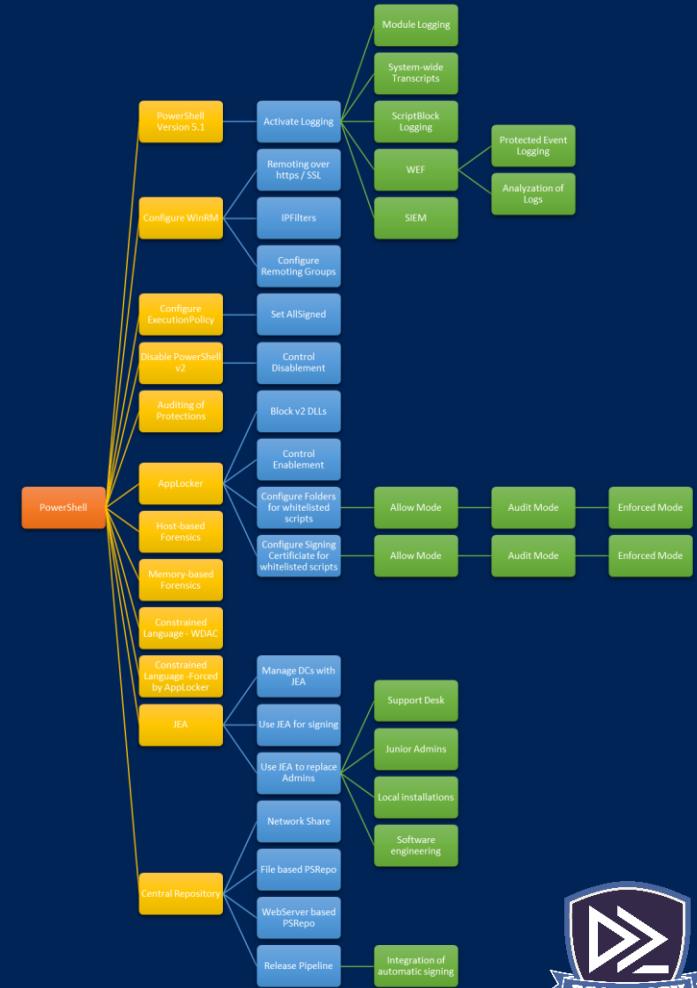
What is the challenge?

High Number of Technical Controls

PowerShell Version 5
Configure WinRM
Remoting over https / SSL
SSL
Ports
Admins allowed
ExecutionPolicy
PowerShell Version 5
Disable PowerShell v2
Control Disablement
Activate Logging
Module Logging
Transcription
System-wide Transcripts
ScriptBlock Logging
WEF / SIEM
Protected Event Logging
Analyzation
Malware Keywords
Auditing of Protections
AppLocker registry keys
AV settings
Host-based Forensics
Memory-based Forensics
Constrained Language - WDAC
Constrained Language -Forced by AppLocker
JEA

High Number of Technical Controls

Many Dependencies



High Number
of Technical
Controls

Many
Dependencies

Continuous
Improvement

Windows 10 1709



Windows 10 1803



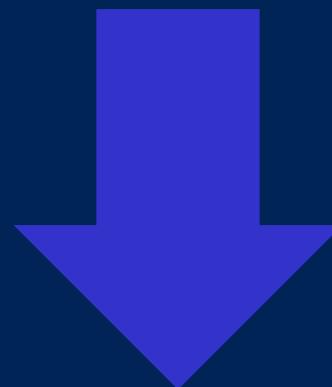
Windows 10 1809



High Number
of Technical
Controls

Many
Dependencies

Continuous
Improvement



Prioritization

POWERSHELL SECURITY

I DON'T KNOW WHERE TO START



Experiences from the Fields

Lacking knowledge about PowerShell Security

Customers are lacking overviews and roadmaps

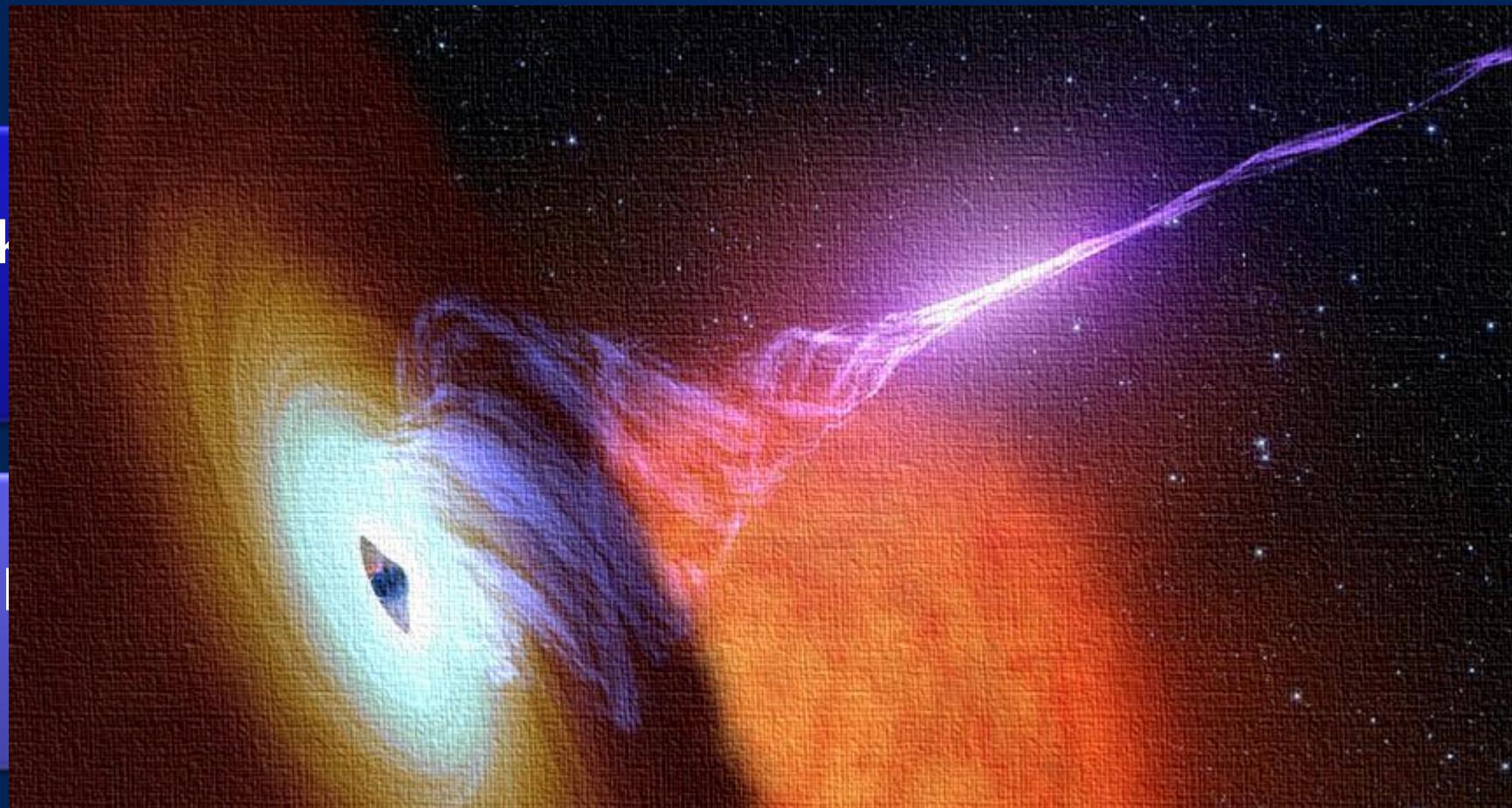
Lacking focus on important technical security controls

No awareness of risk

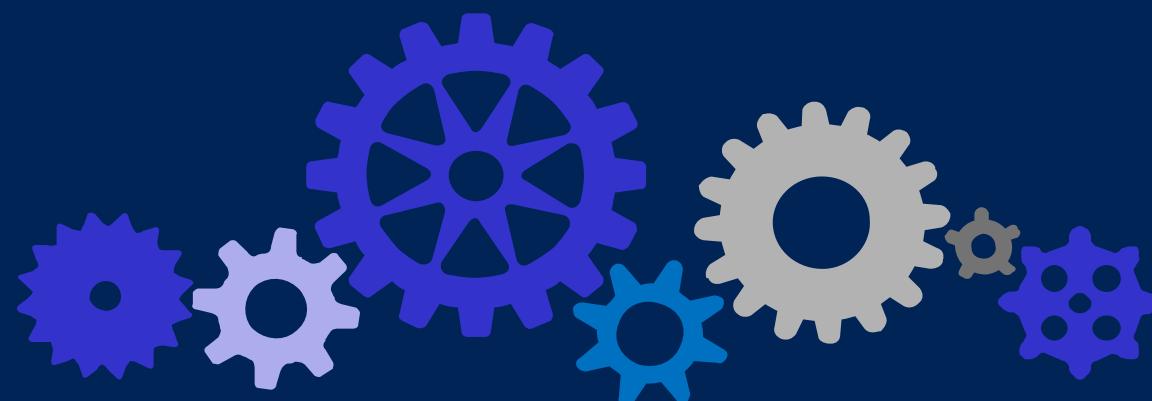
Lack of tools

Lack of resources

Experiences from the Fields



Implementation



How we tried to solve the problem.

What is actually needed

Technical Security Controls

- Overview
- Dependencies
- Costs (resources, time and money)

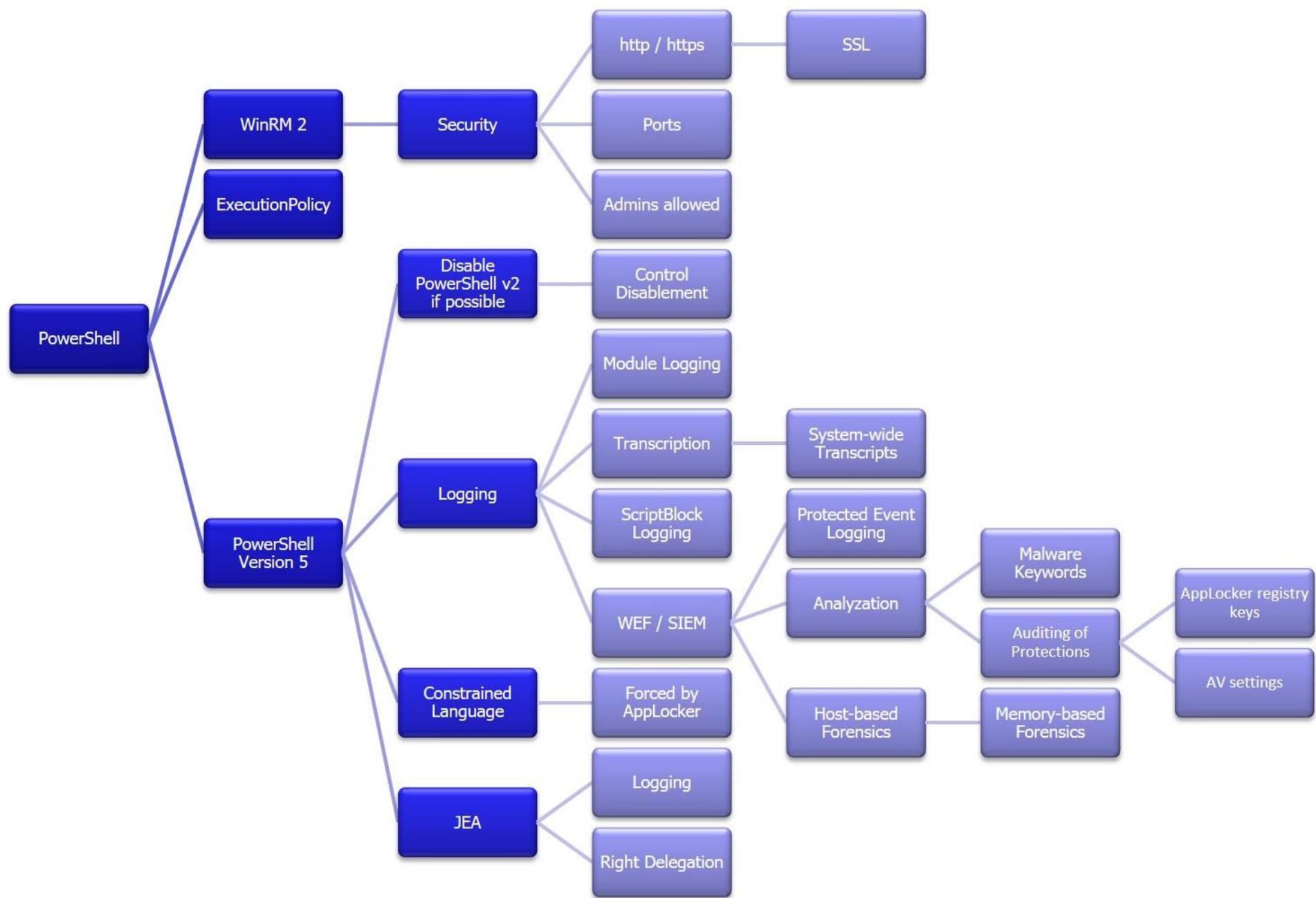
Threat landscape

Risk mitigation vectors

Old ideas back on the table again

PowerShell Security for Enterprise Customers

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



Technical Security Controls

Gathering

Clustering by

Topics

Dependencies

Topics

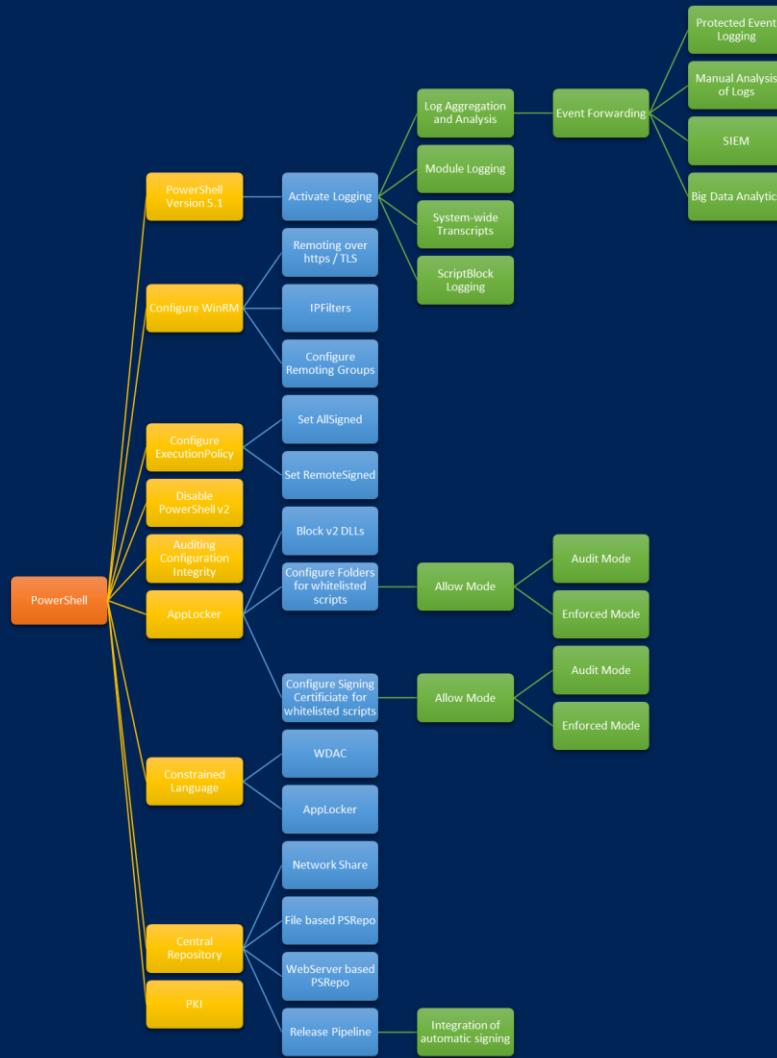
Security

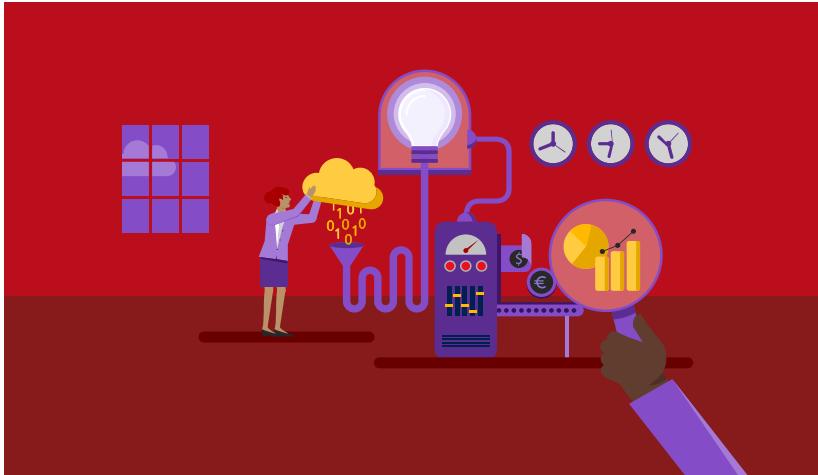
PowerShell

Moderizing
Environment

Securing
Privileged
Access

Step 1 - Inventory





DEMO

Step 1 – Brainstorming Excel SmartArts

Step 2 – adding metrics



Demo

Excel

Inventory

Adding metrics



Step 3 - Visualization

Technical implementation

- Graph
- Neo4j

Step 4 – Working with metrics

Queries

Filtering

Prioritization

Dynamic Visualization

Demo

Technical
Implementation

Graph

Neo4j

What's next?

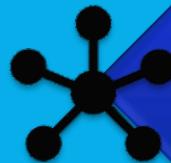


Next Steps



Adding Complexity

- Differentiate types more granularly
- Add additional information and dependencies



Adding more models like MITRE ATT&CK



Calculate values with algorithms



More crazy stuff with automated attacks and data – WUhuuuuh!

Call to Action!



Call To Action! PowerShell Security

- 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.

Final Line

**STARTING TO PRIORITIZE
TECHNICAL SECURITY CONTROLS**



BLUE TEAM FTW!

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?