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 speaker is correct and try
again.
At line:1 char:1
+ Julien Reisdorffer
+ ~~~~
    + CategoryInfo          : SpeakerNotFound: (JR:Speaker)
[], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException
```

2018

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

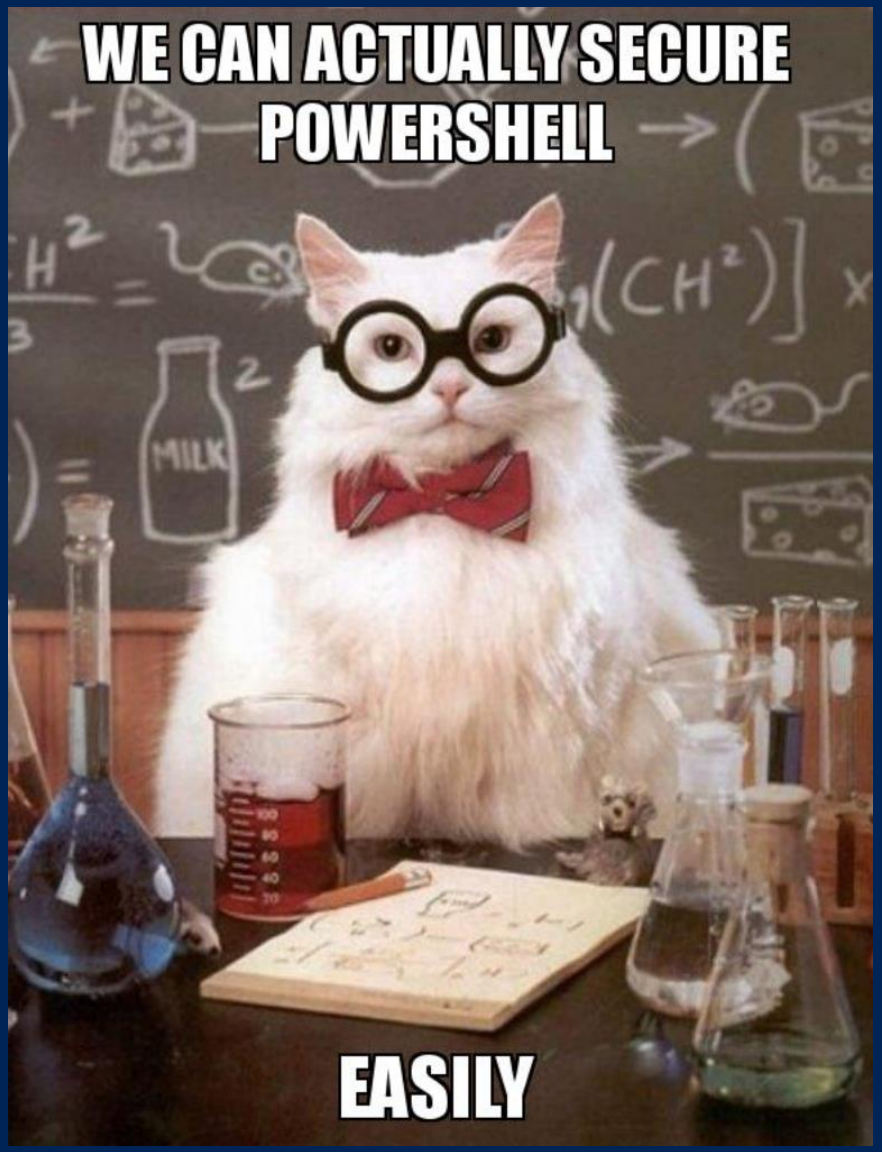
Intro

Background PS Security

Why PowerShell Security matters

Powershell is evil.

No it isn't.



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

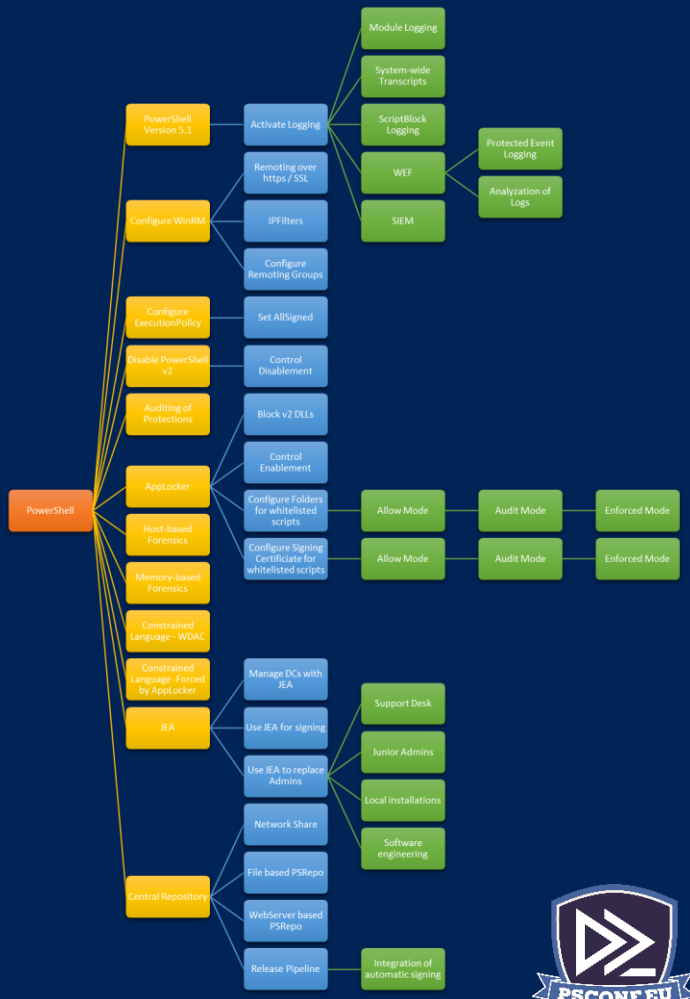
What is the challenge?

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

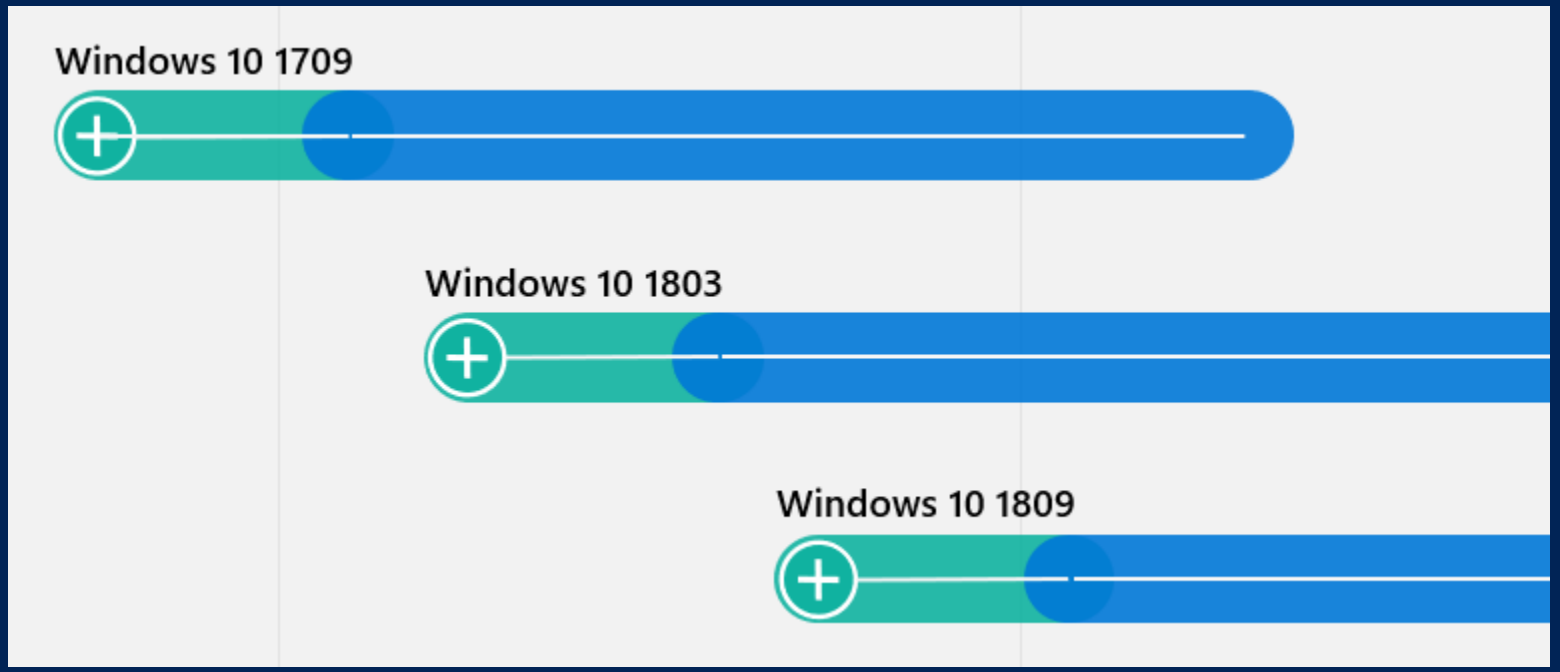
Many Dependencies



High Number of Technical Controls

Many Dependencies

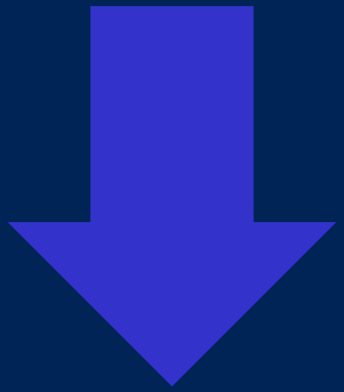
Continuous Improvement



High Number of Technical Controls

Many Dependencies

Continuous Improvement



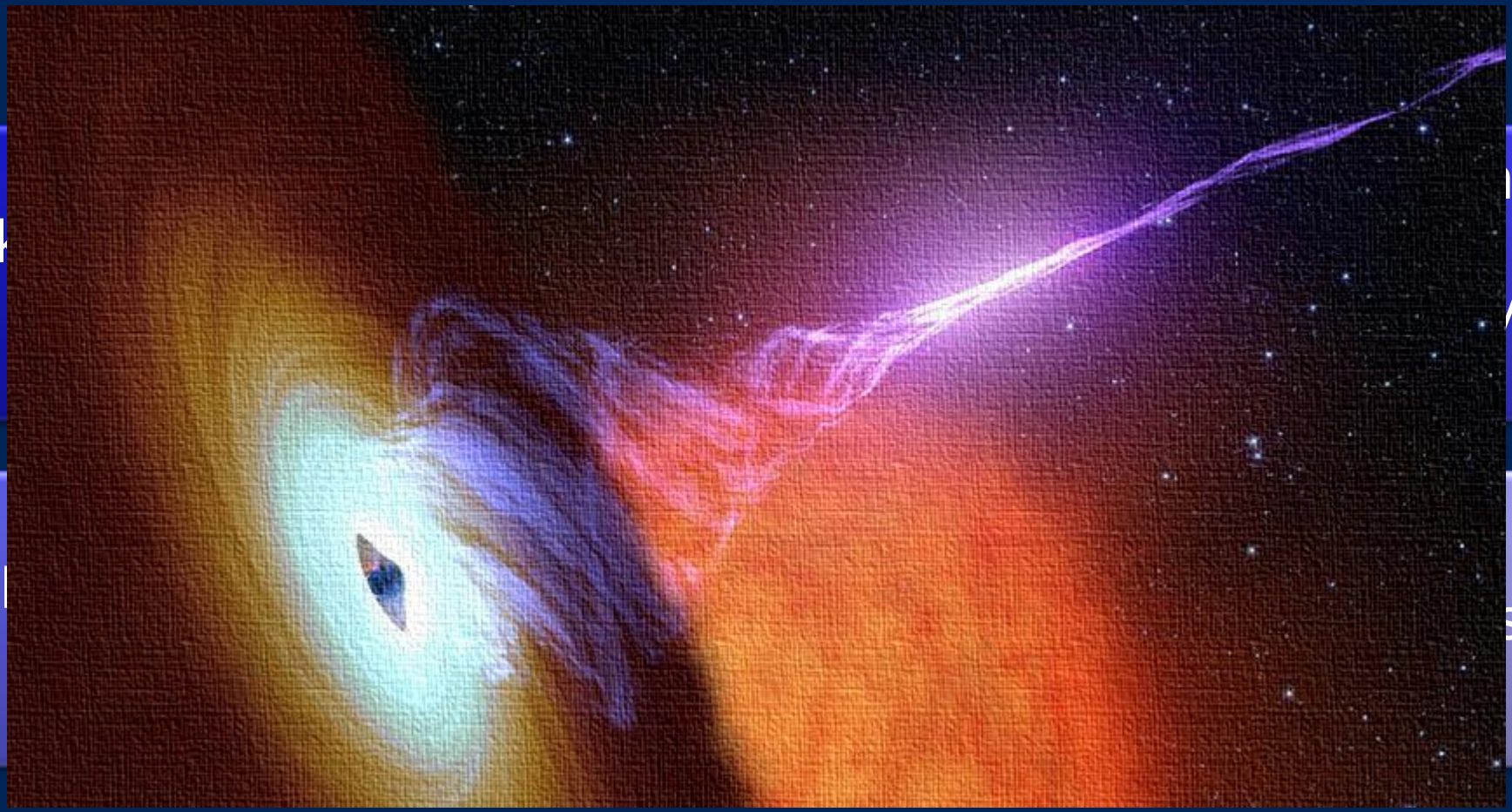
Prioritization


POWERSHELL SECURITY
I DON´T KNOW WHERE TO START

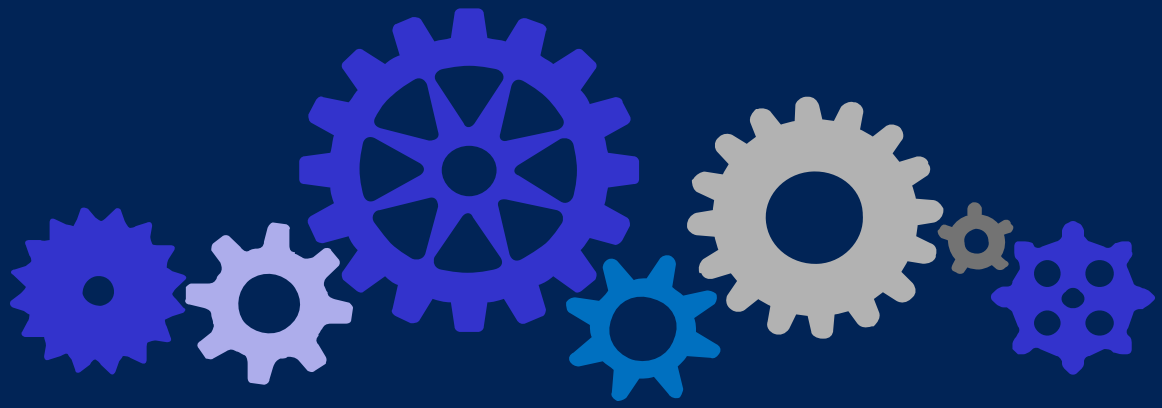
Experiences from the Fields

- 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



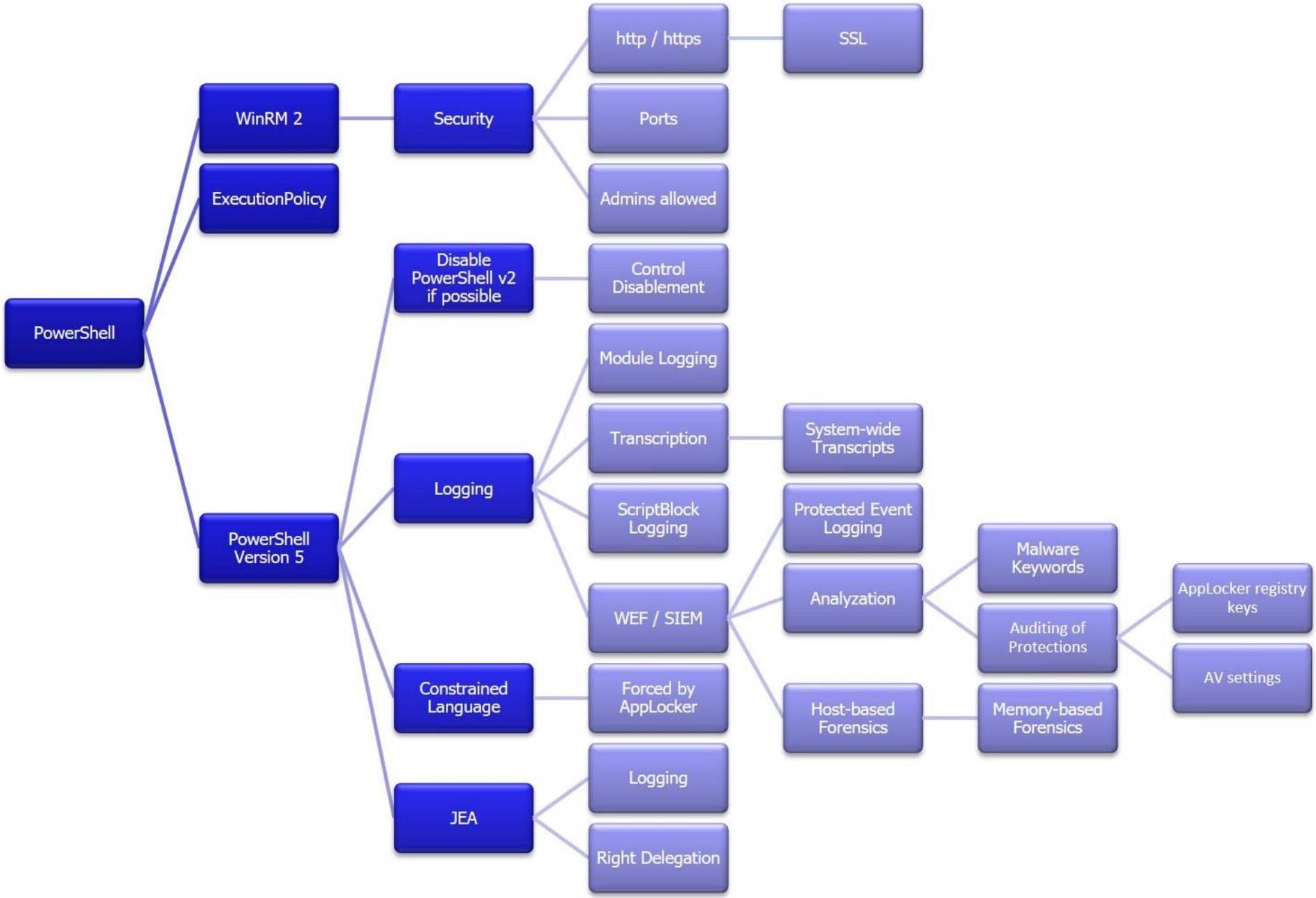
How we tried to solve the problem.

What is actually needed

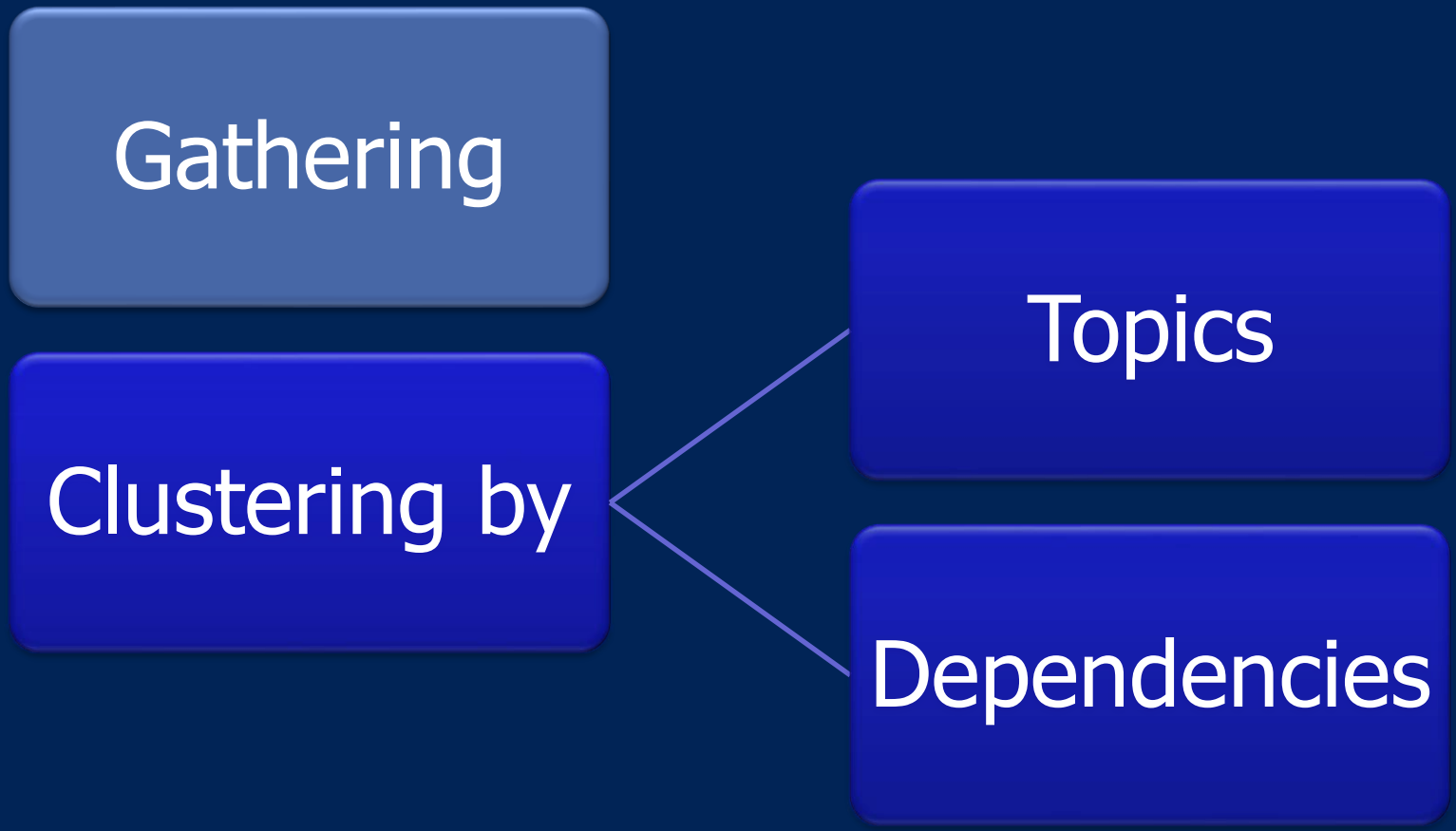
Old ideas back on the table again

PowerShell Security for Enterprise Customers

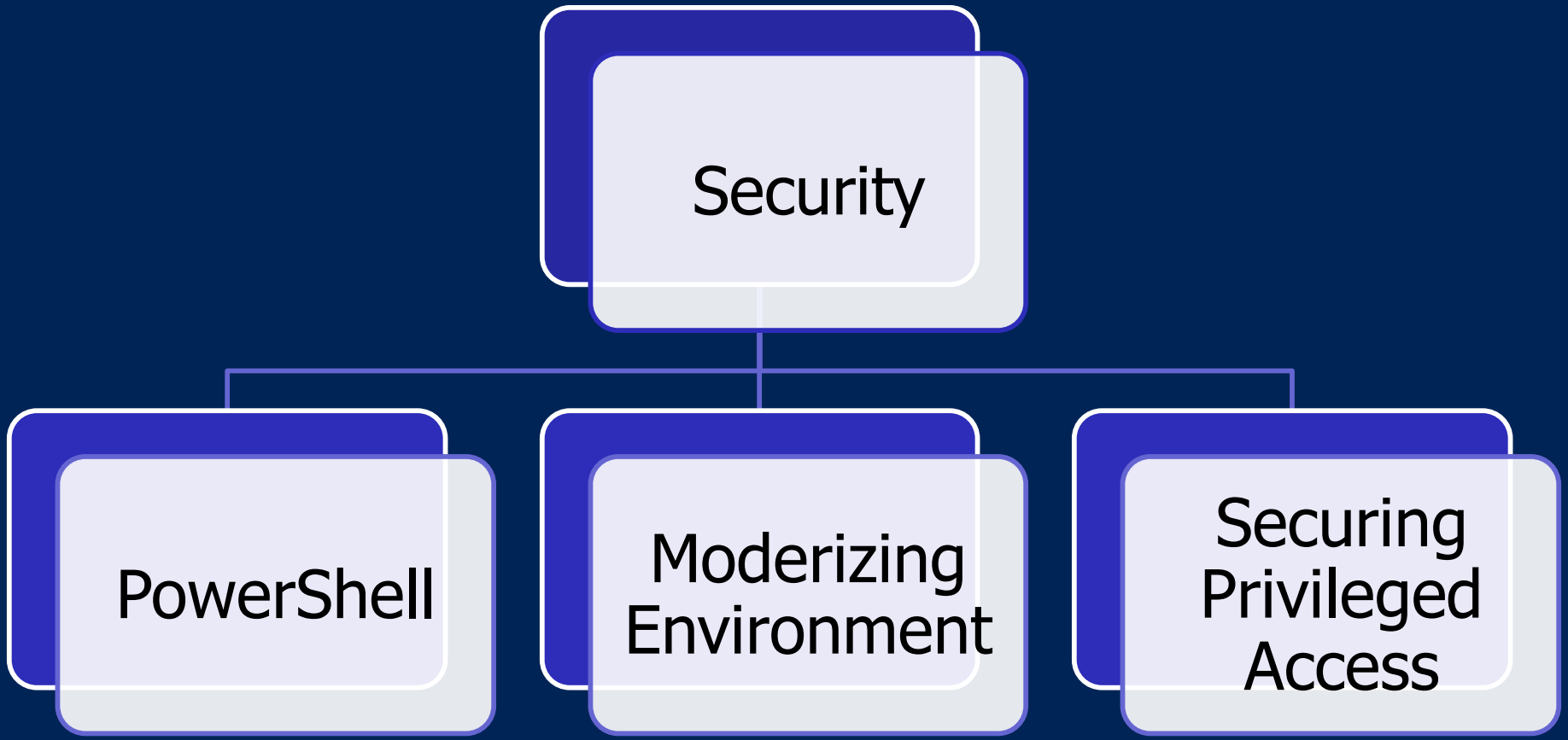
- http://aka.ms/PSSecEnt


PowerShell
WinRM 2
ExecutionPolicy
PowerShell Version 5
Security
http / https
SSL
Ports
Admins allowed
Disable PowerShell v2 if possible
Control Disablement
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
Forced by AppLocker
JEA
Logging
Right Delegation

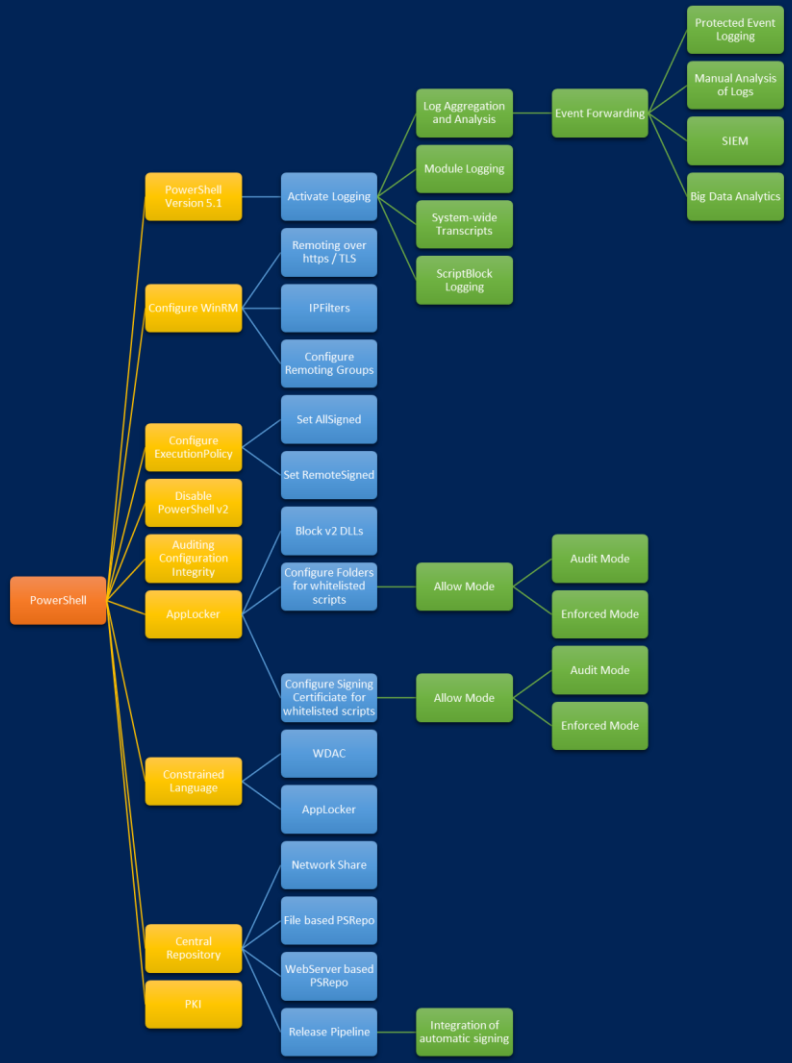
Technical Security Controls



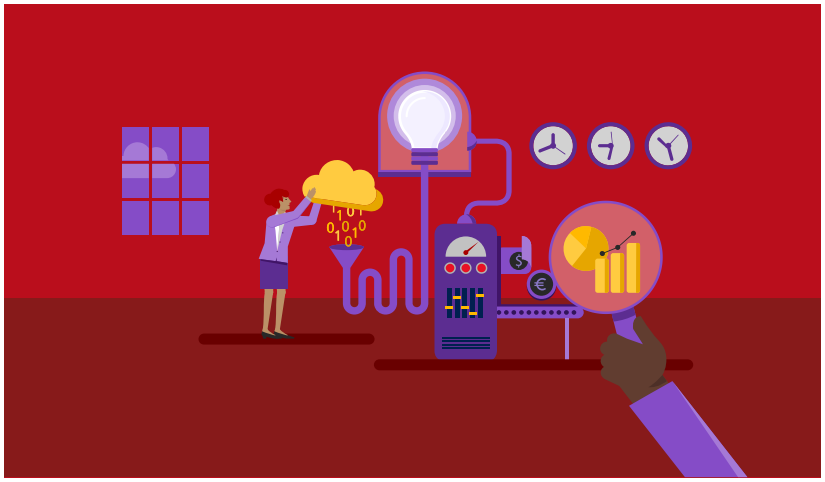
Topics


Security
PowerShell
Moderizing Environment
Securing Privileged Access

Step 1 - Inventory



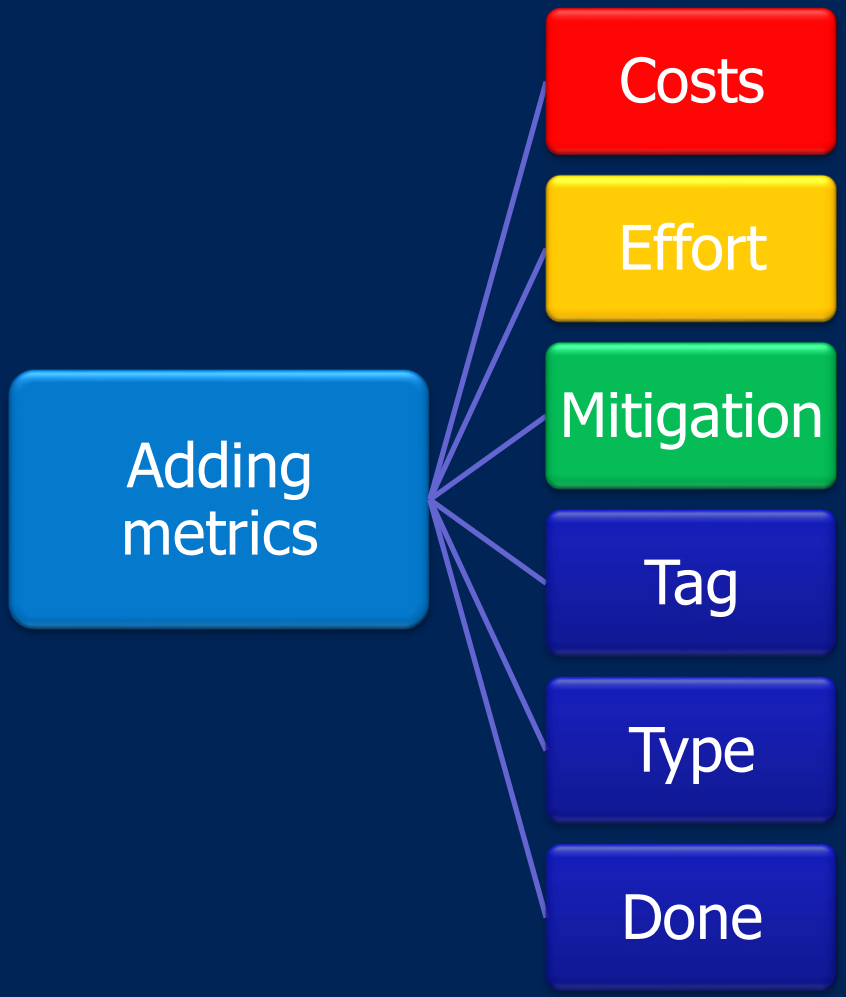
PSCONF.EU



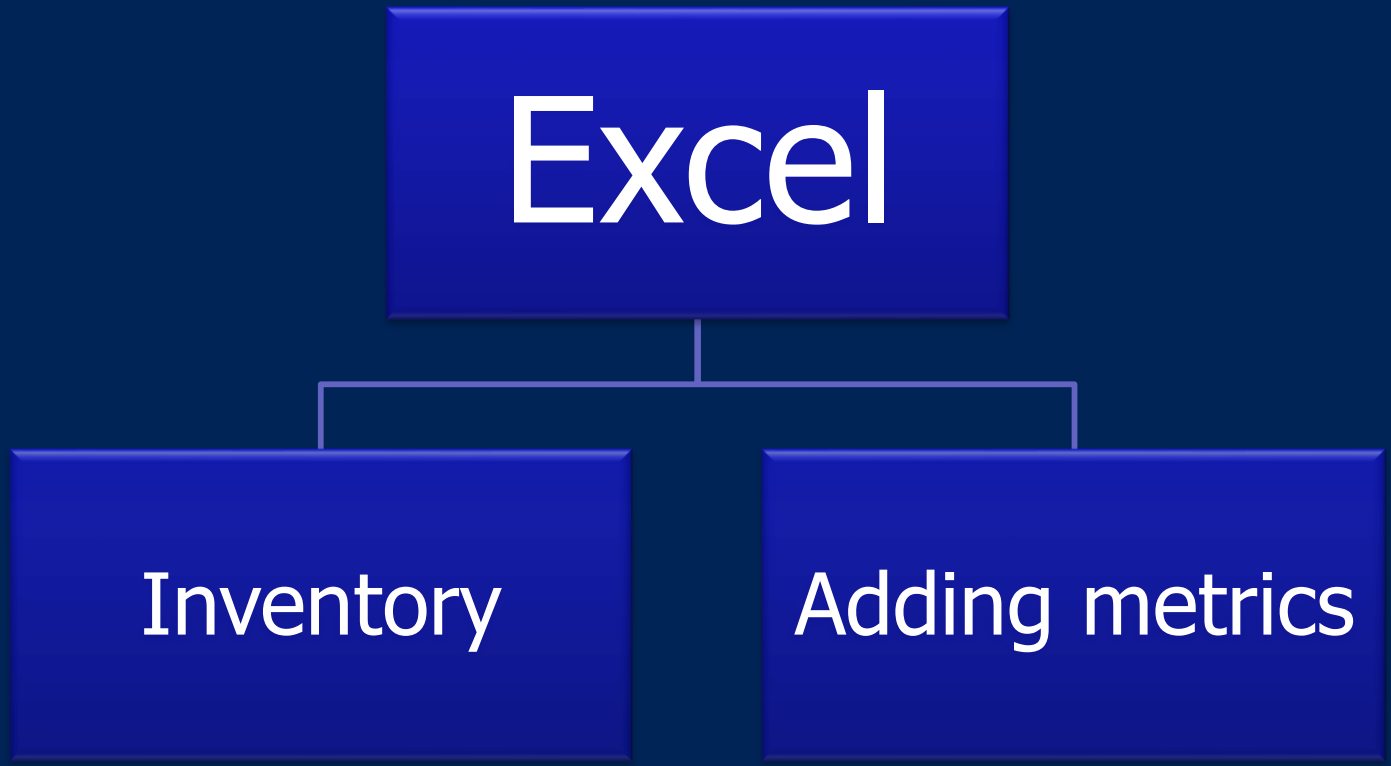
DEMO

Step 1 – Brainstorming
Excel SmartArts

Step 2 – adding metrics

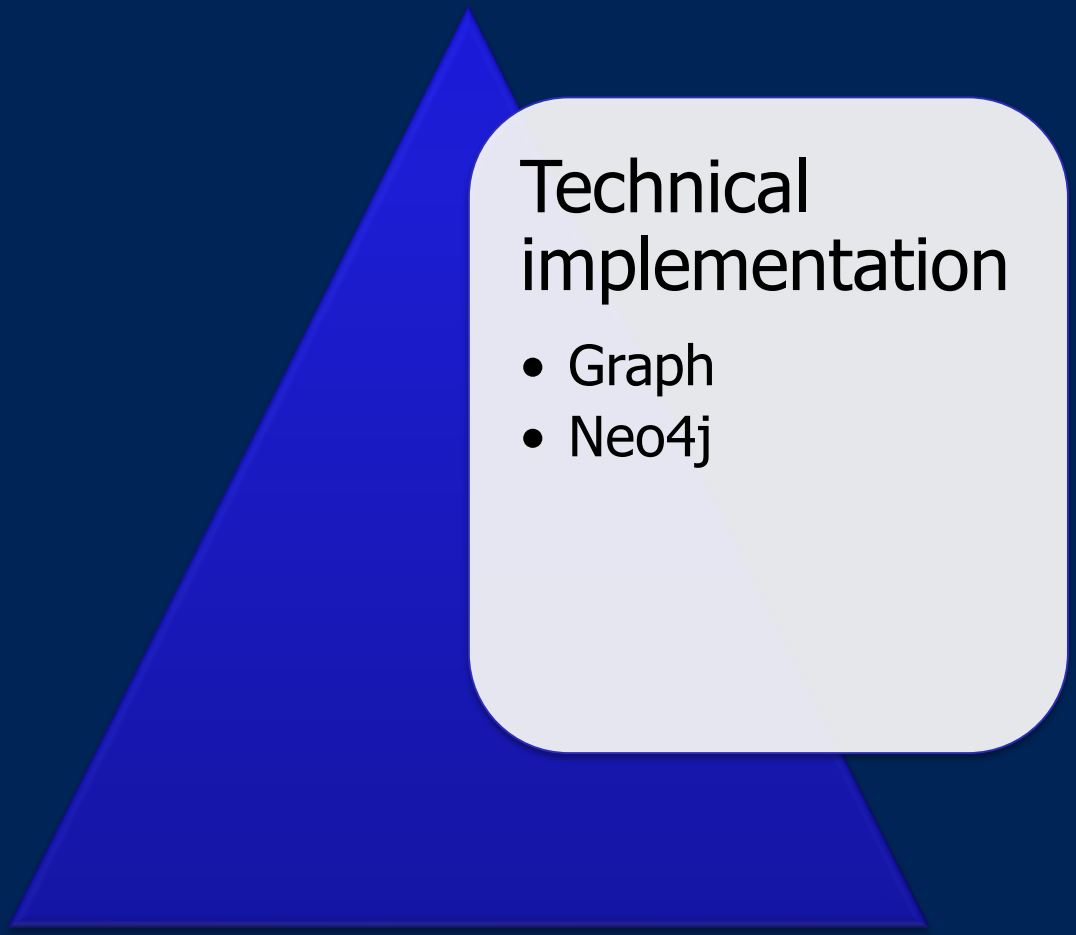


Demo




PRIORITIZE ALL THE
SECURITY CONTROLS!

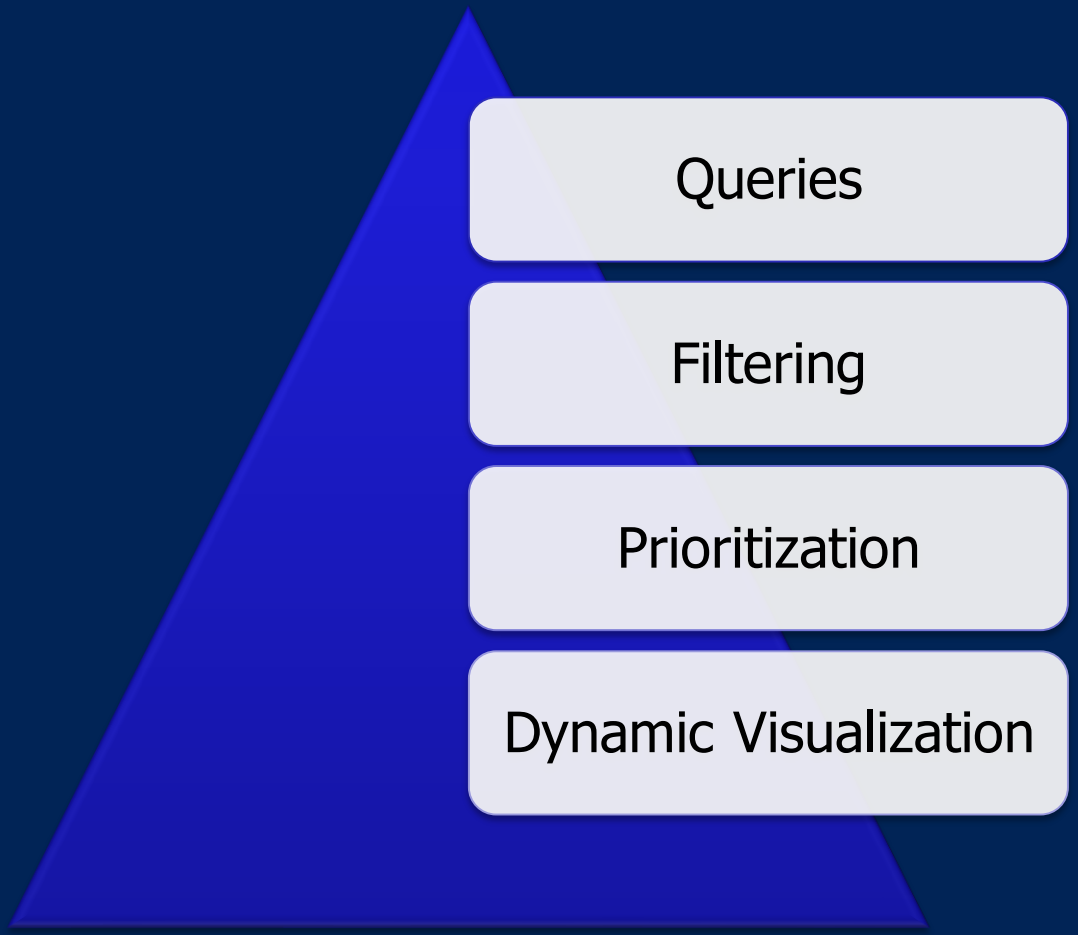
Step 3 - Visualization



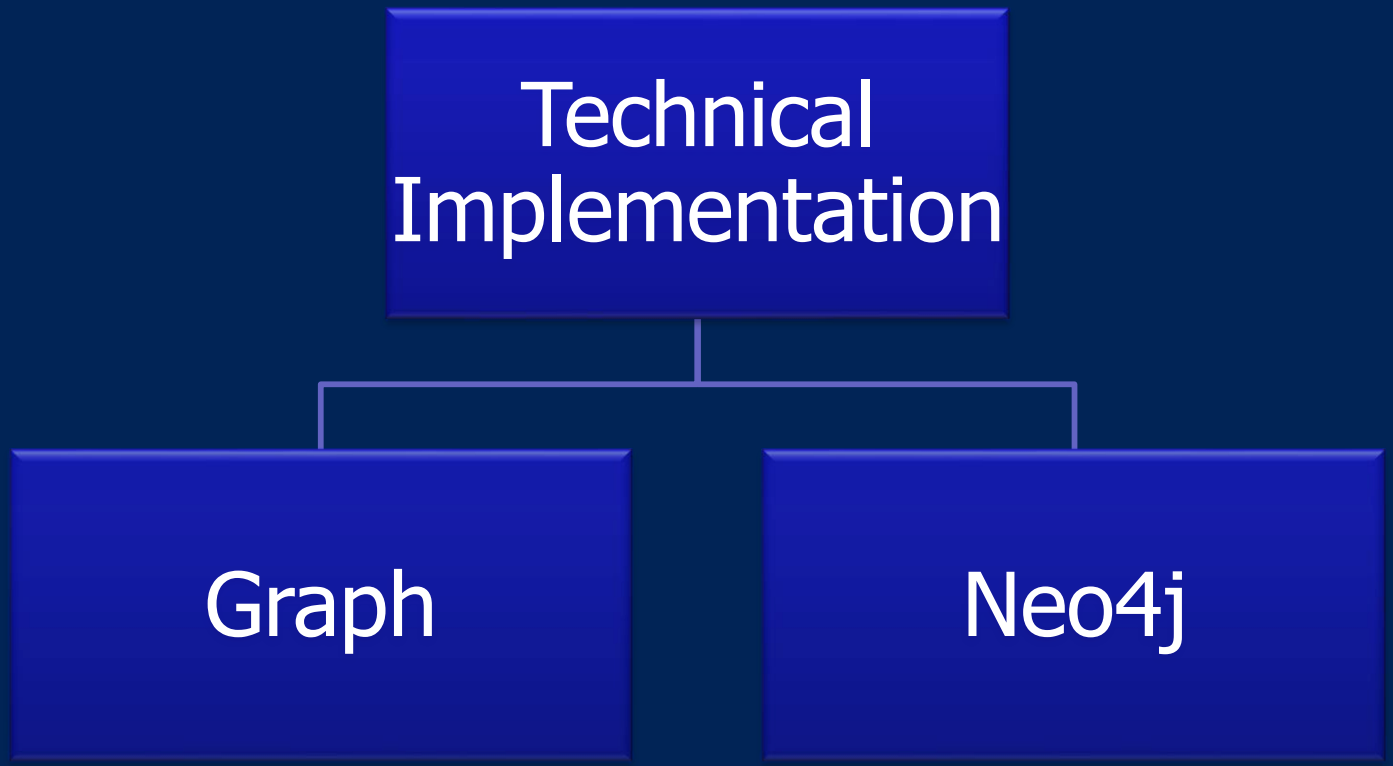
Technical implementation

- Graph
- Neo4j

Step 4 – Working with metrics



Demo



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 – WUhuuuh!

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?