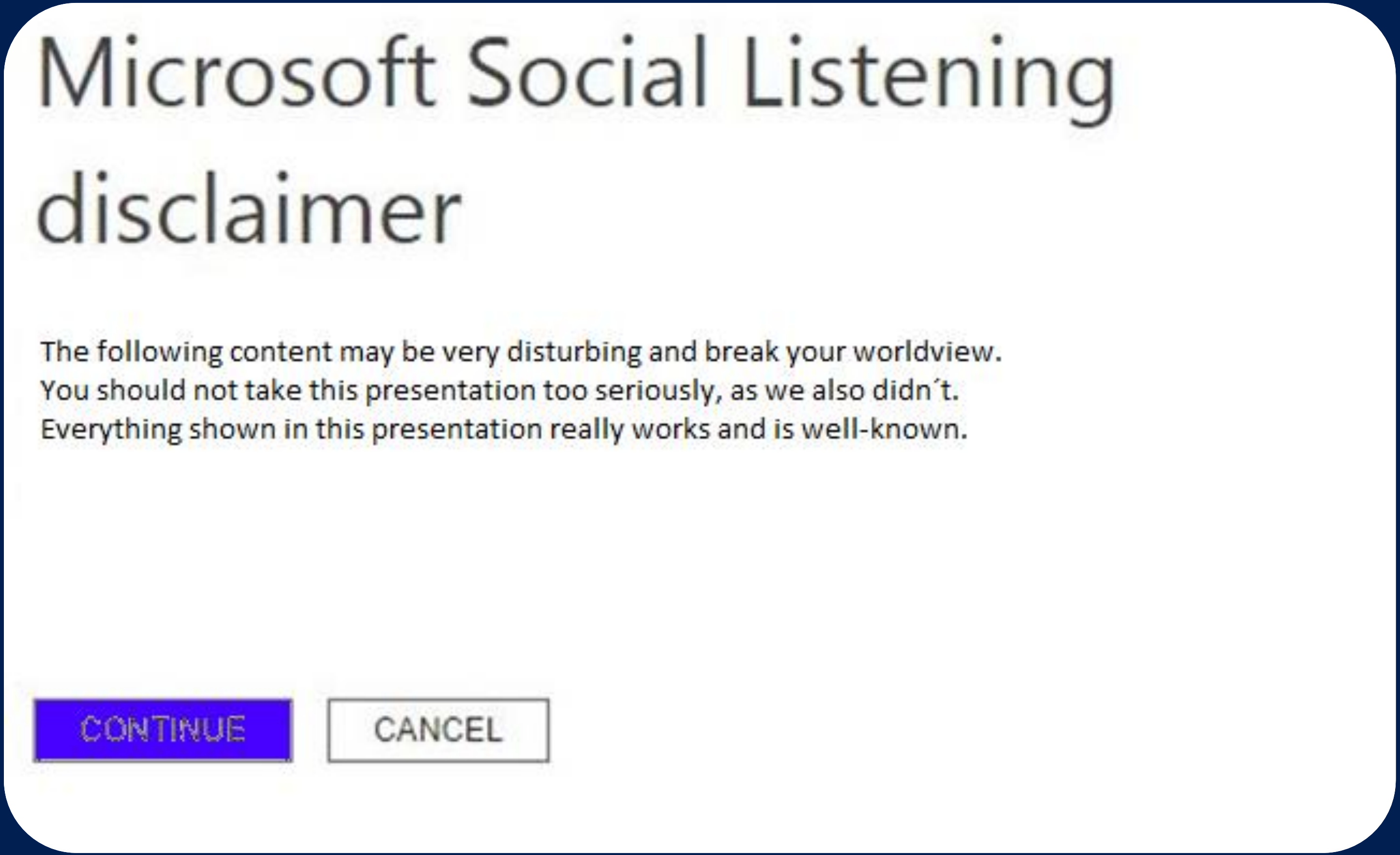
PowerShell Security Red vs. Blue

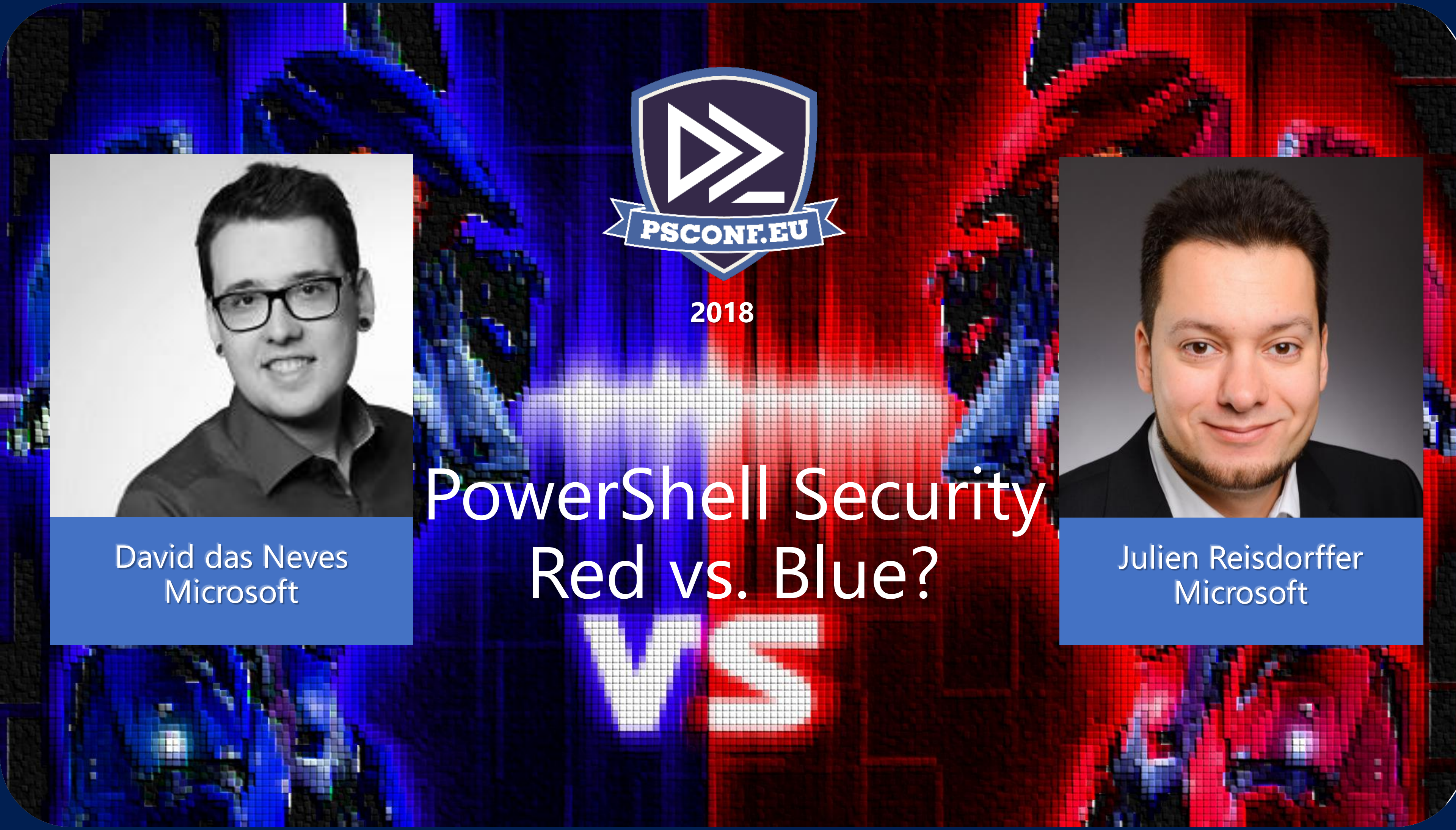
Julien Reisdorffer
Microsoft

David das Neves
Microsoft



Microsoft Social Listening disclaimer

The following content may be very disturbing and break your worldview.
You should not take this presentation too seriously, as we also didn´t.
Everything shown in this presentation really works and is well-known.



PSCONF.EU

2018

David das Neves
Microsoft

PowerShell Security
Red vs. Blue?

Julien Reisdorffer
Microsoft

David das Neves
Premier Field Engineer, Microsoft
Julien Reisdorffer
Sr. Consultant Cybersecurity, Microsoft

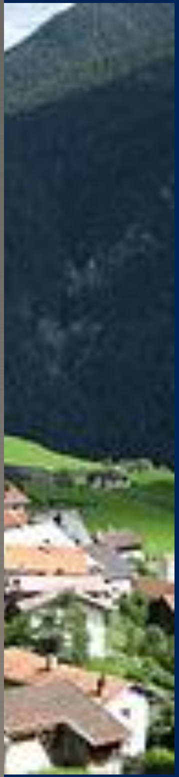
PowerShell Conference EU 2018

David das Neves

PSCONF.EU

PowerShell Conference EU 2018

Julien Reisdorffer



PSCONF.EU

Agenda

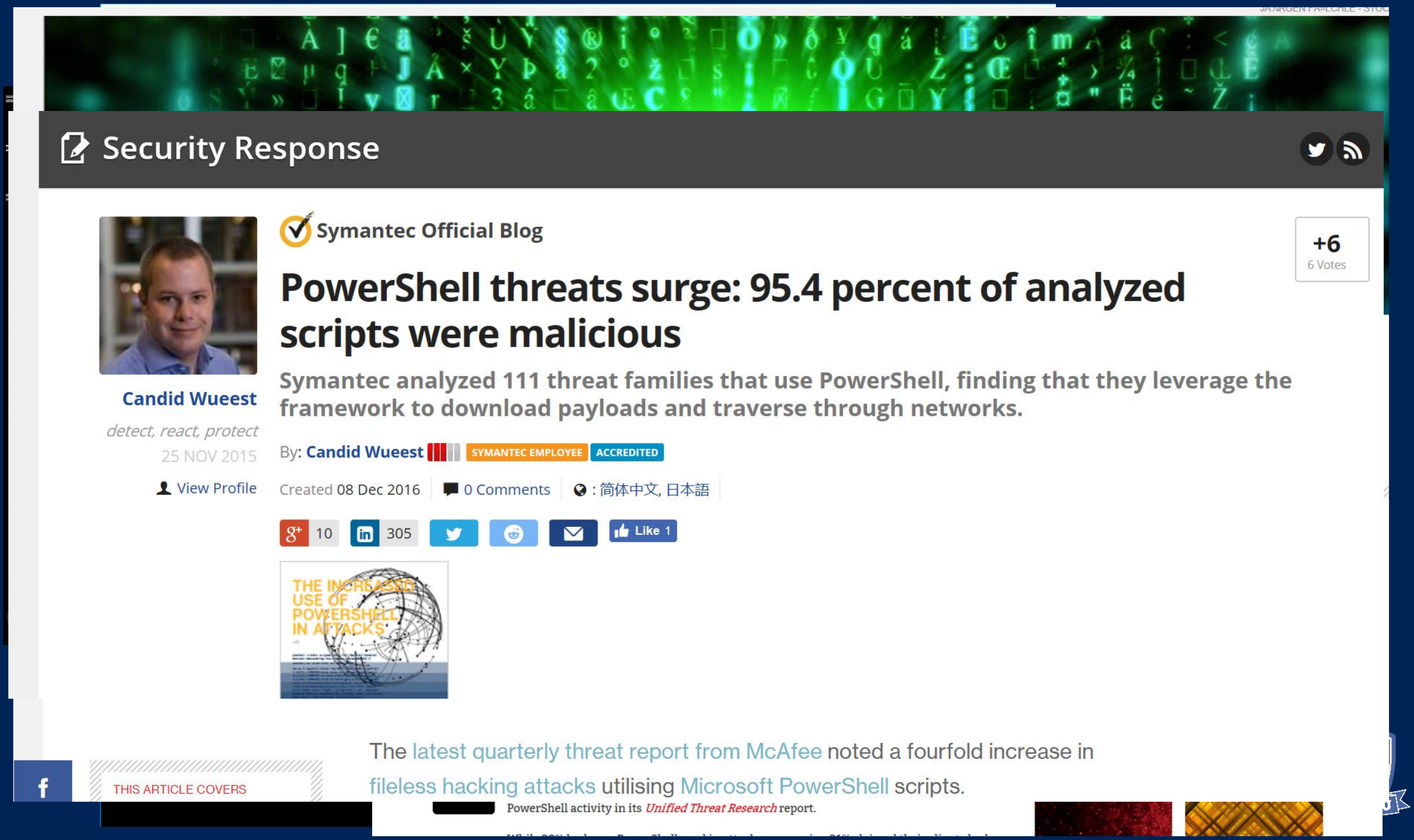
- Current Threat Landscape
- Setting the Scene…
- Demos
  - Attacks → Julien
  - Mitigations → David
- Summary

Intro

Background PS Security

PowerShell Conference EU 2018

Why PowerShell Security matters



Security Response

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.

+6
6 Votes

Candid Wueest
detect, react, protect
25 NOV 2015
View Profile

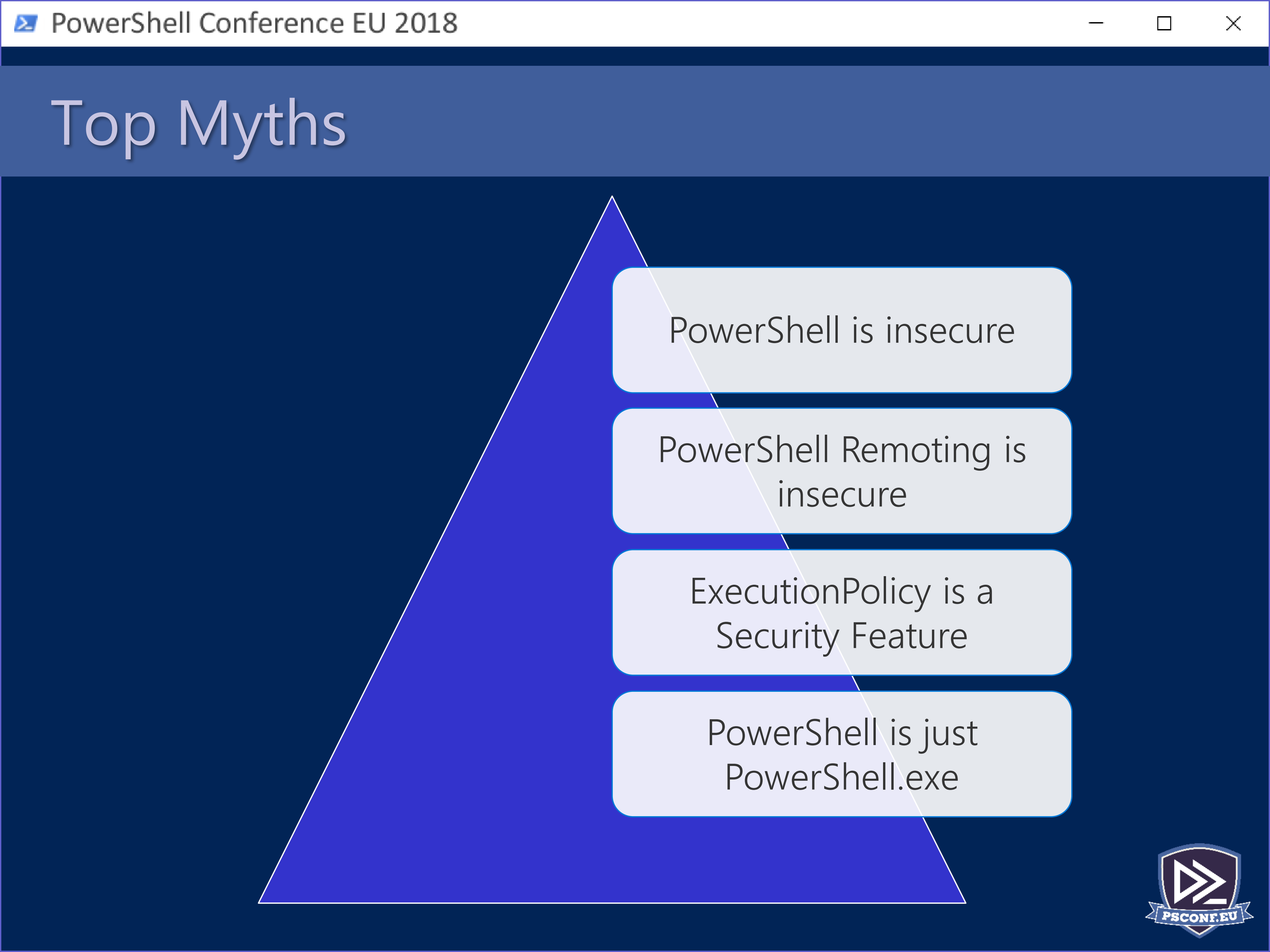
By: Candid Wueest SYMANTEC EMPLOYEE ACCREDITED

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

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

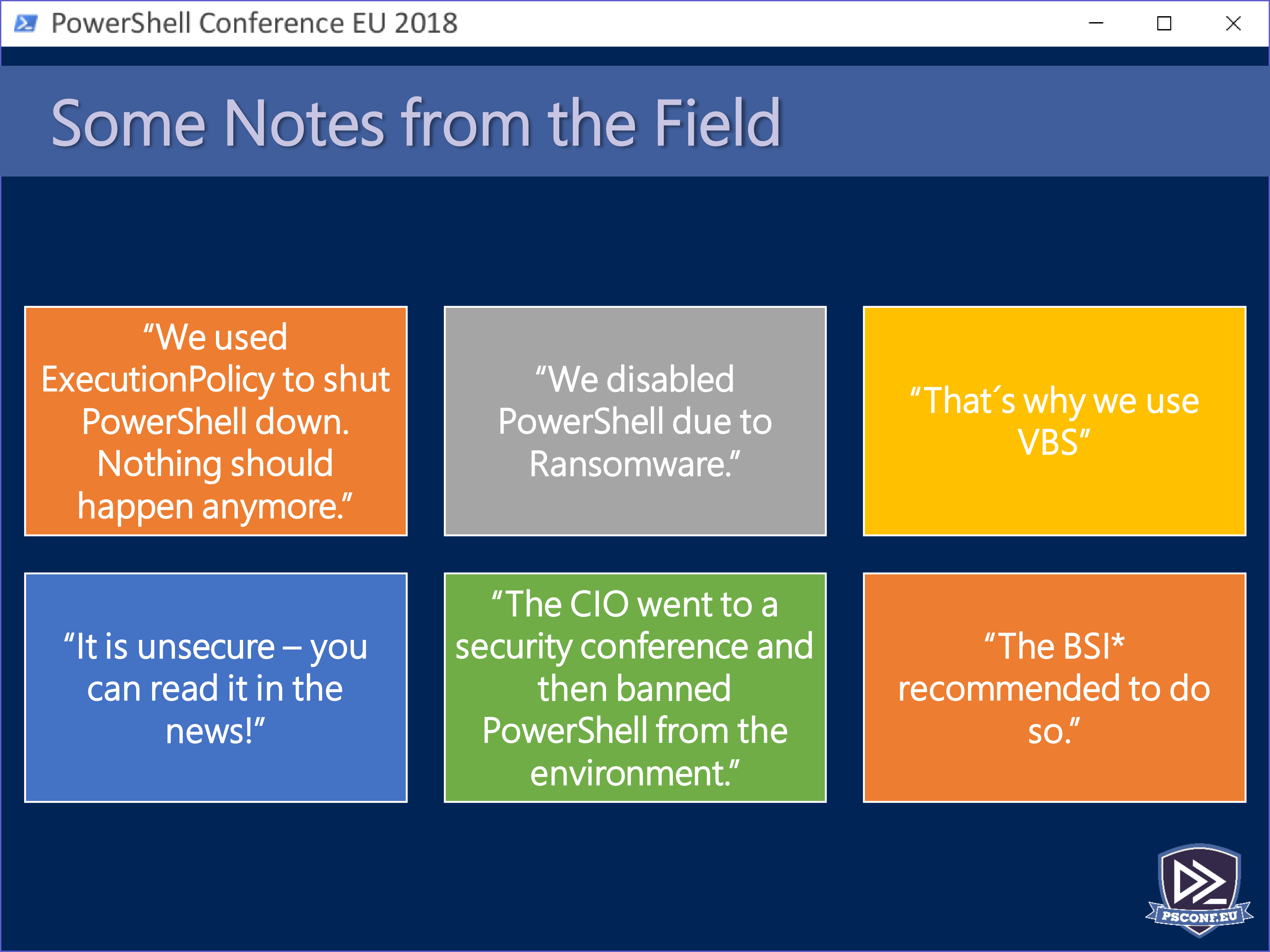
PowerShell activity in its *Unified Threat Research* report.

Powershell is evil.



Top Myths

- PowerShell is insecure
- PowerShell Remoting is insecure
- ExecutionPolicy is a Security Feature
- PowerShell is just PowerShell.exe



Some Notes from the Field

"We used ExecutionPolicy to shut PowerShell down. Nothing should happen anymore."

"We disabled PowerShell due to Ransomware."

"That´s why we use VBS"

"It is unsecure – you can read it in the news!"

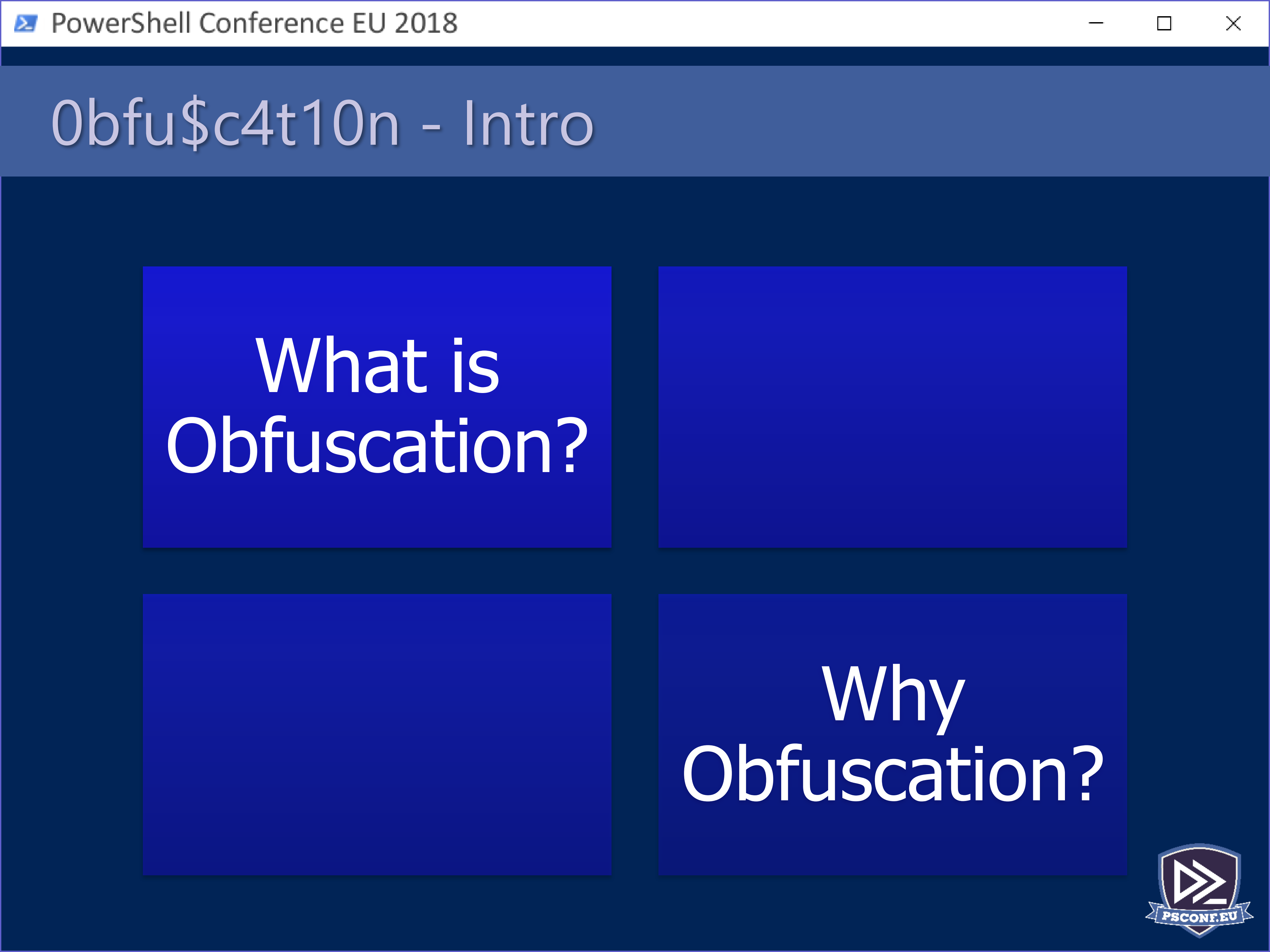
"The CIO went to a security conference and then banned PowerShell from the environment."

"The BSI* recommended to do so."

Summary

0bfu$c4t10n

Sayonara AV

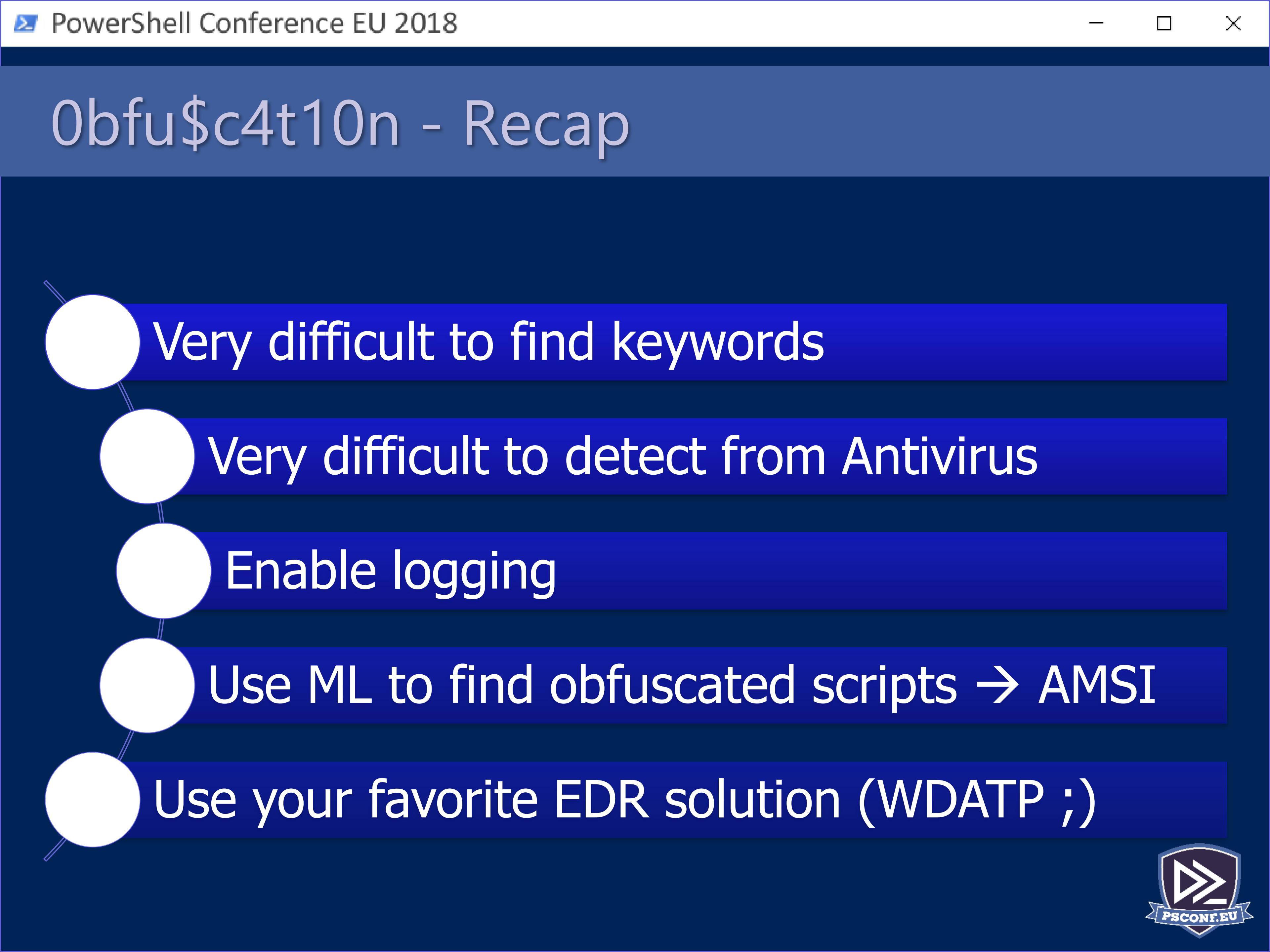


PowerShell Conference EU 2018

0bfu$c4t10n - Intro

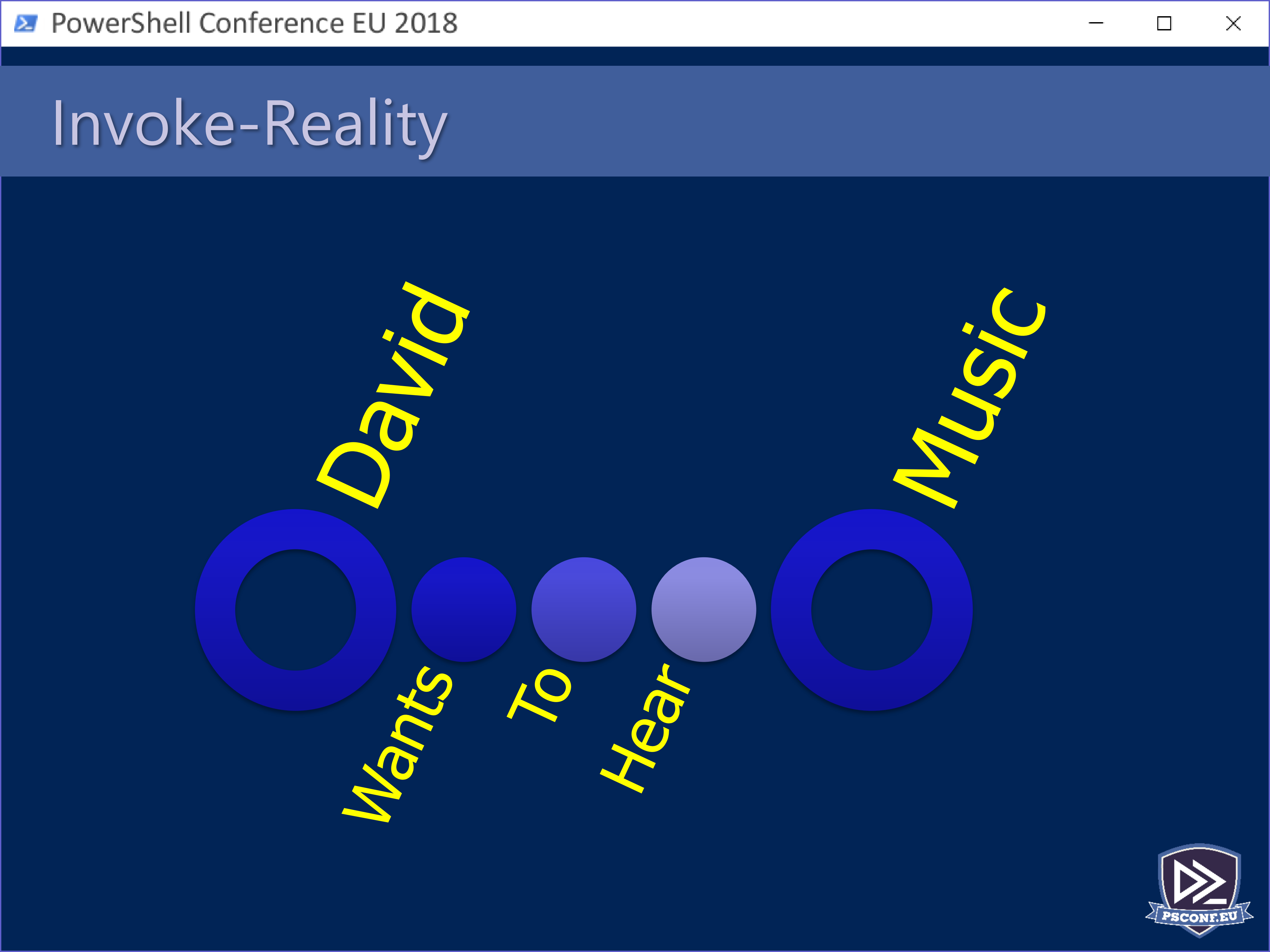
What is Obfuscation?

Why Obfuscation?



0bfu$c4t10n - Recap

- Very difficult to find keywords
- Very difficult to detect from Antivirus
- Enable logging
- Use ML to find obfuscated scripts → AMSI
- Use your favorite EDR solution (WDATP ;)



PowerShell Conference EU 2018

Invoke-Reality

David

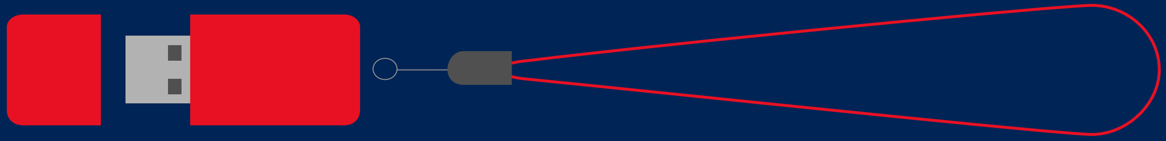
Wants

To

Hear

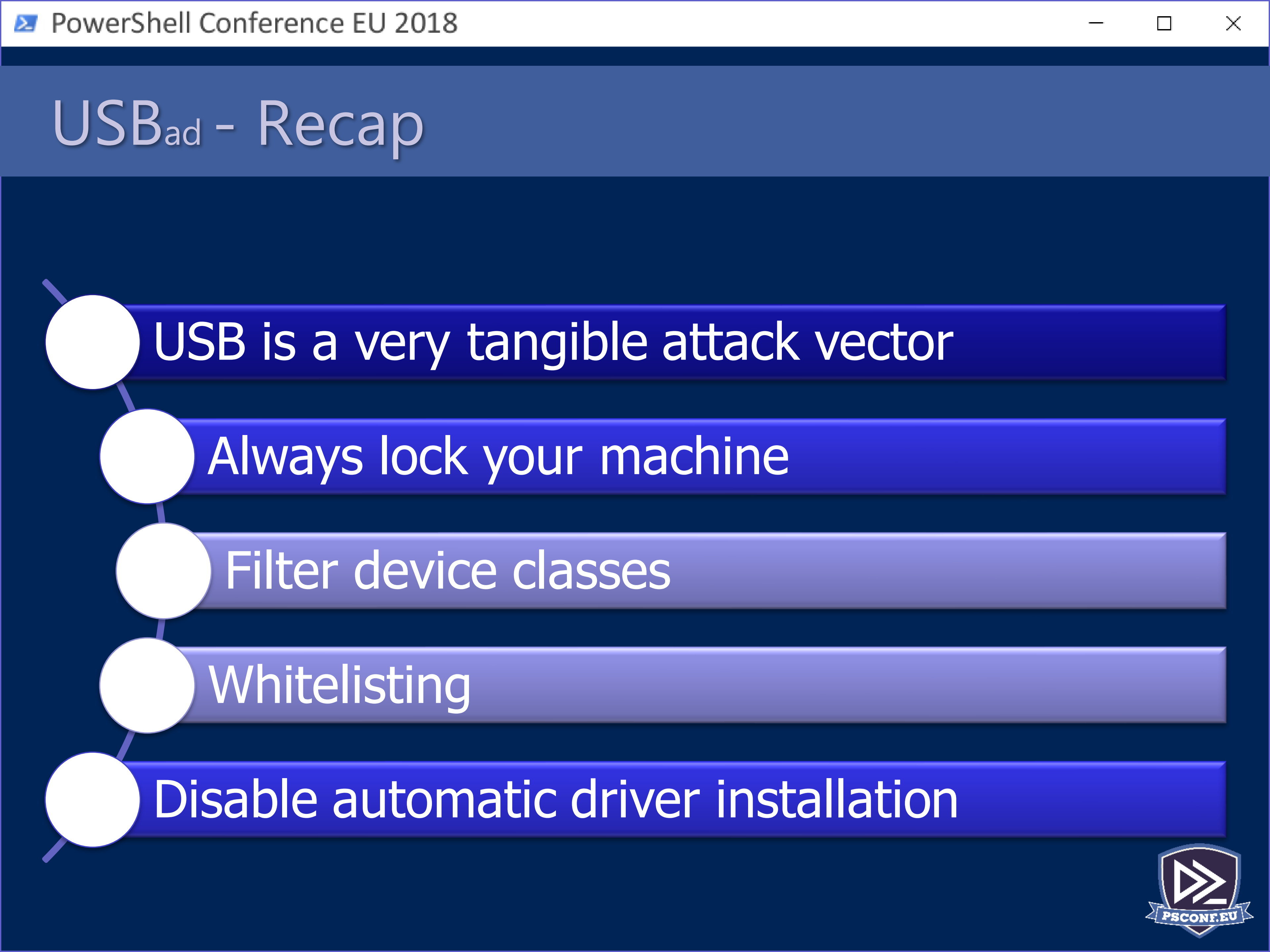
Music

USBad



Get-Physical

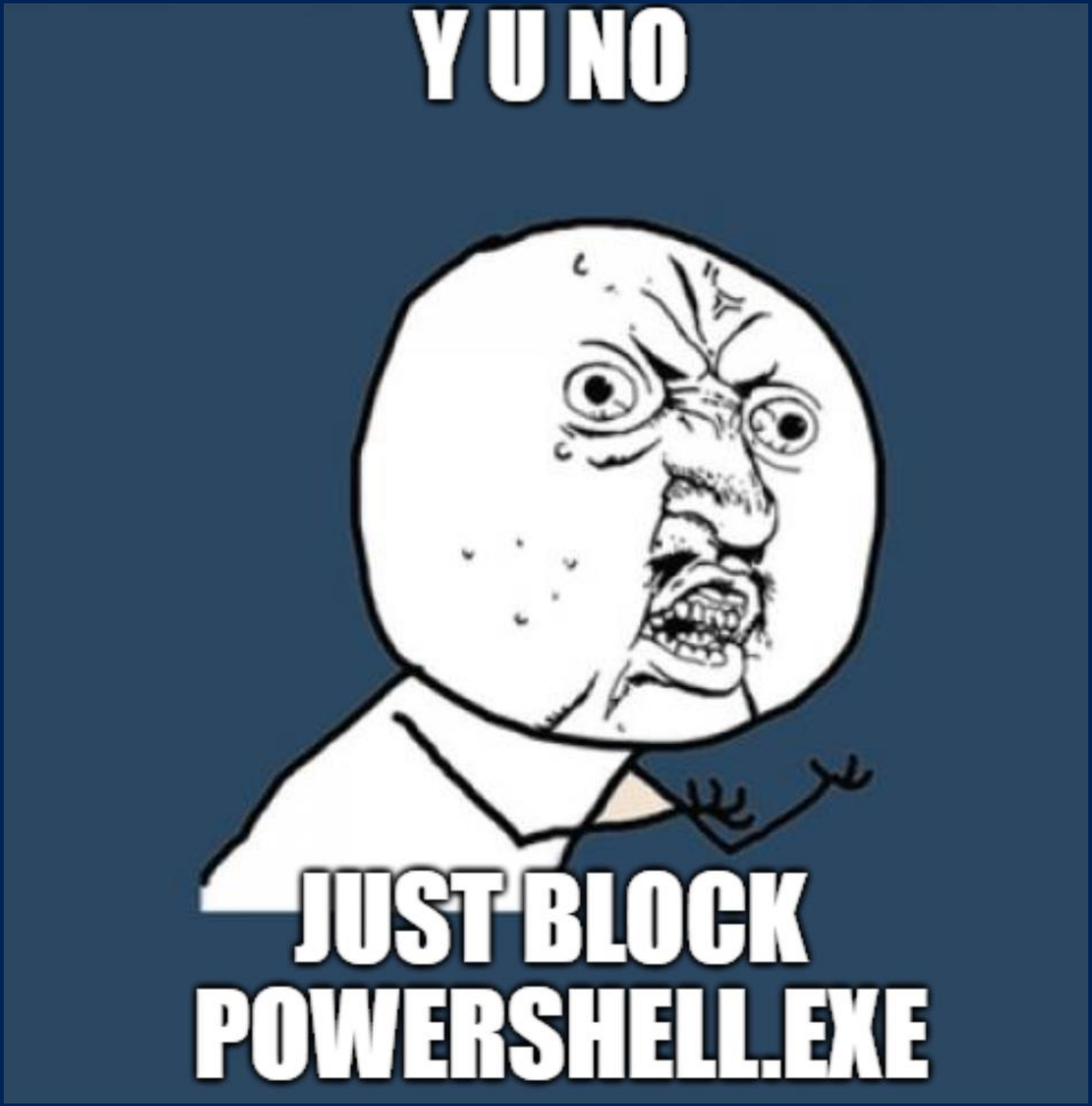
PSCONF.EU



PowerShell Conference EU 2018

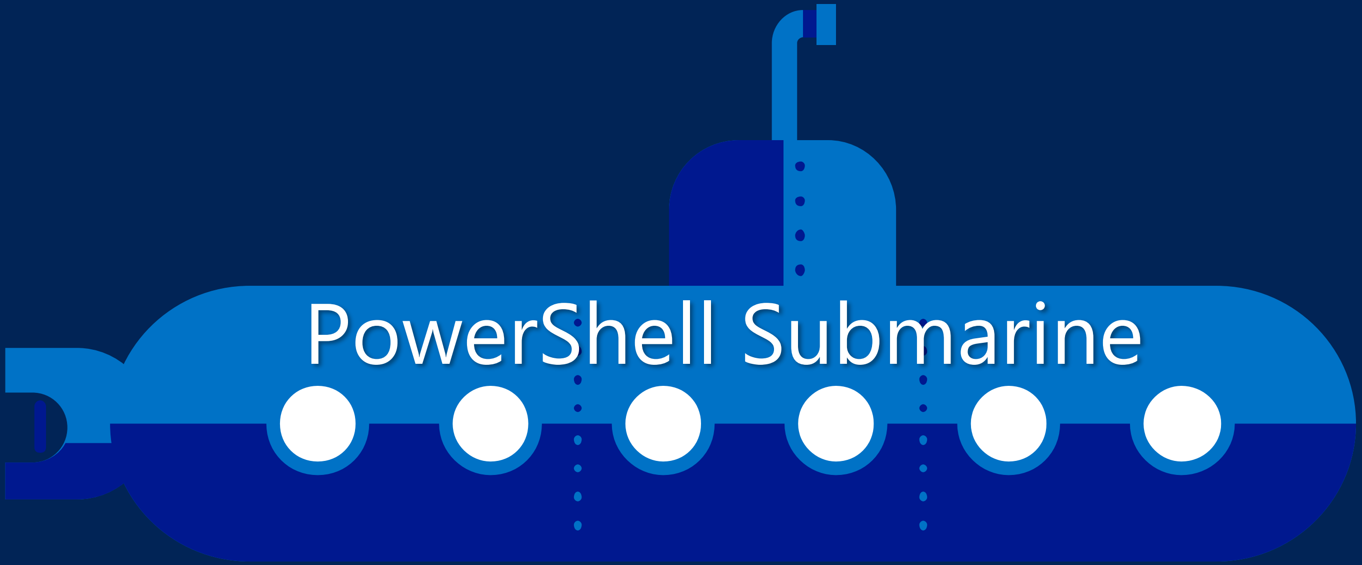
USBad - Recap

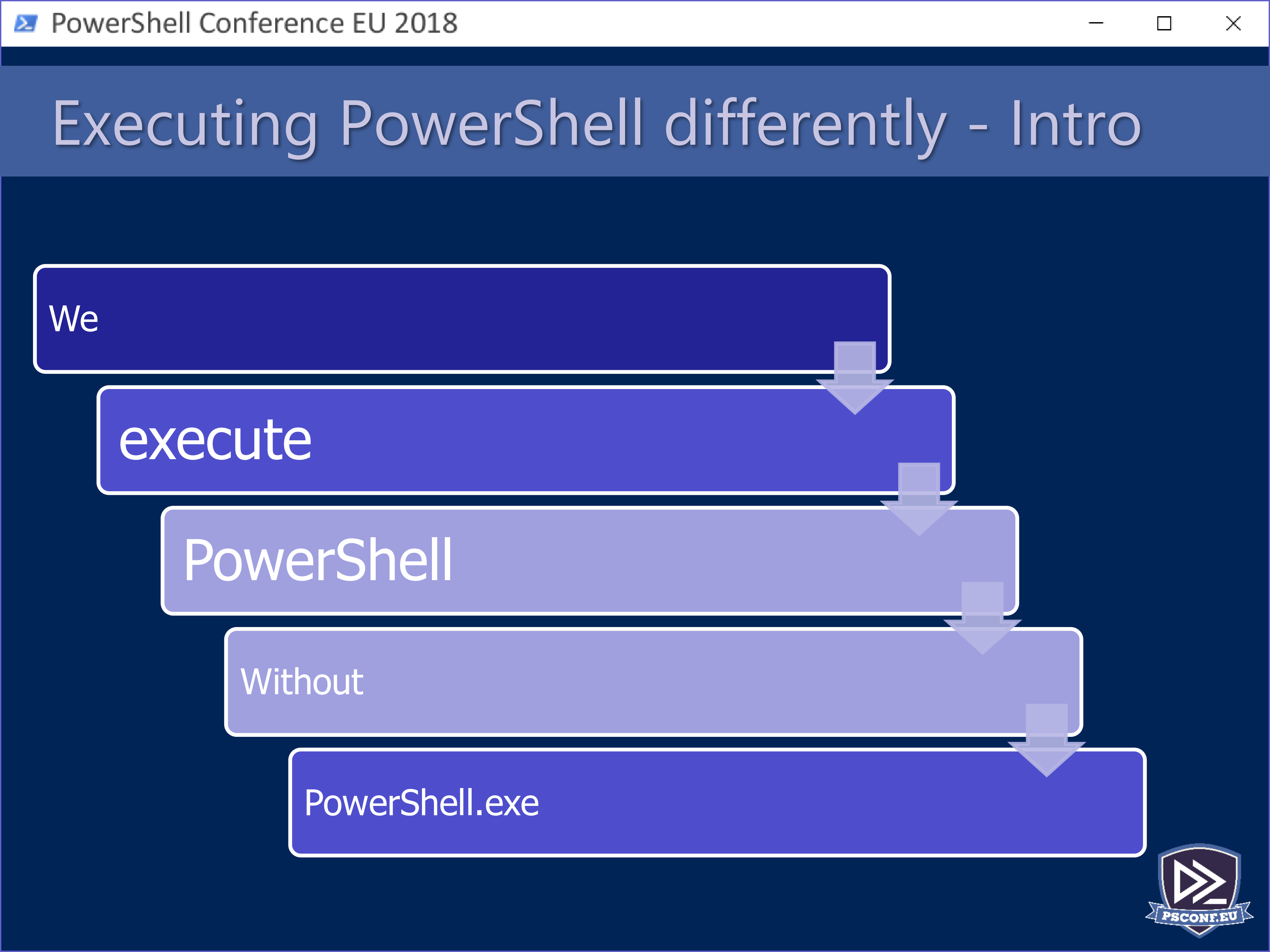
- USB is a very tangible attack vector
- Always lock your machine
- Filter device classes
- Whitelisting
- Disable automatic driver installation


Y U NO
JUST BLOCK
POWERSHELL.EXE

Executing PowerShell

differently





PowerShell Conference EU 2018

Executing PowerShell differently - Intro

We

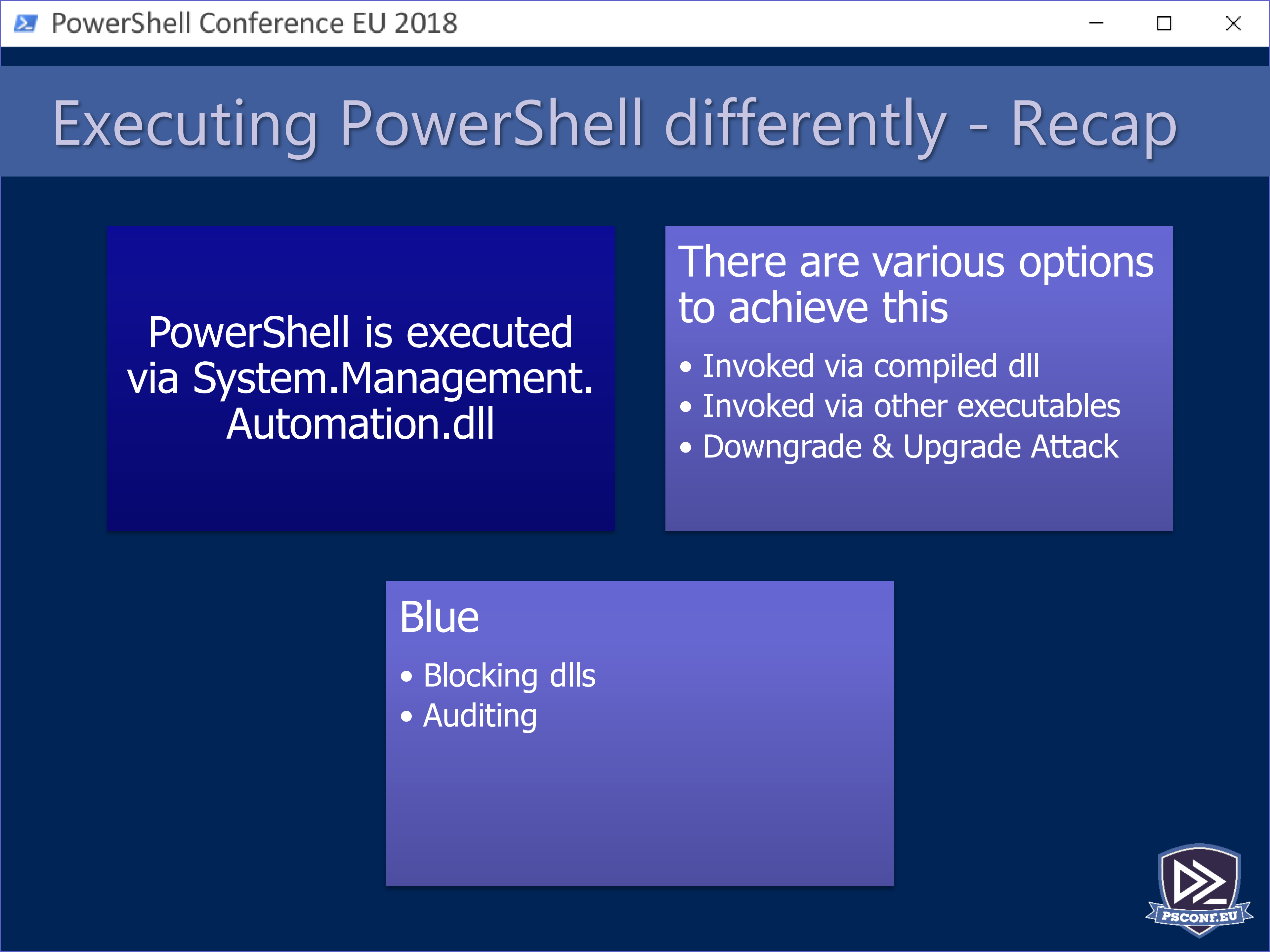
execute

PowerShell

Without

PowerShell.exe

And now?



Executing PowerShell differently - Recap

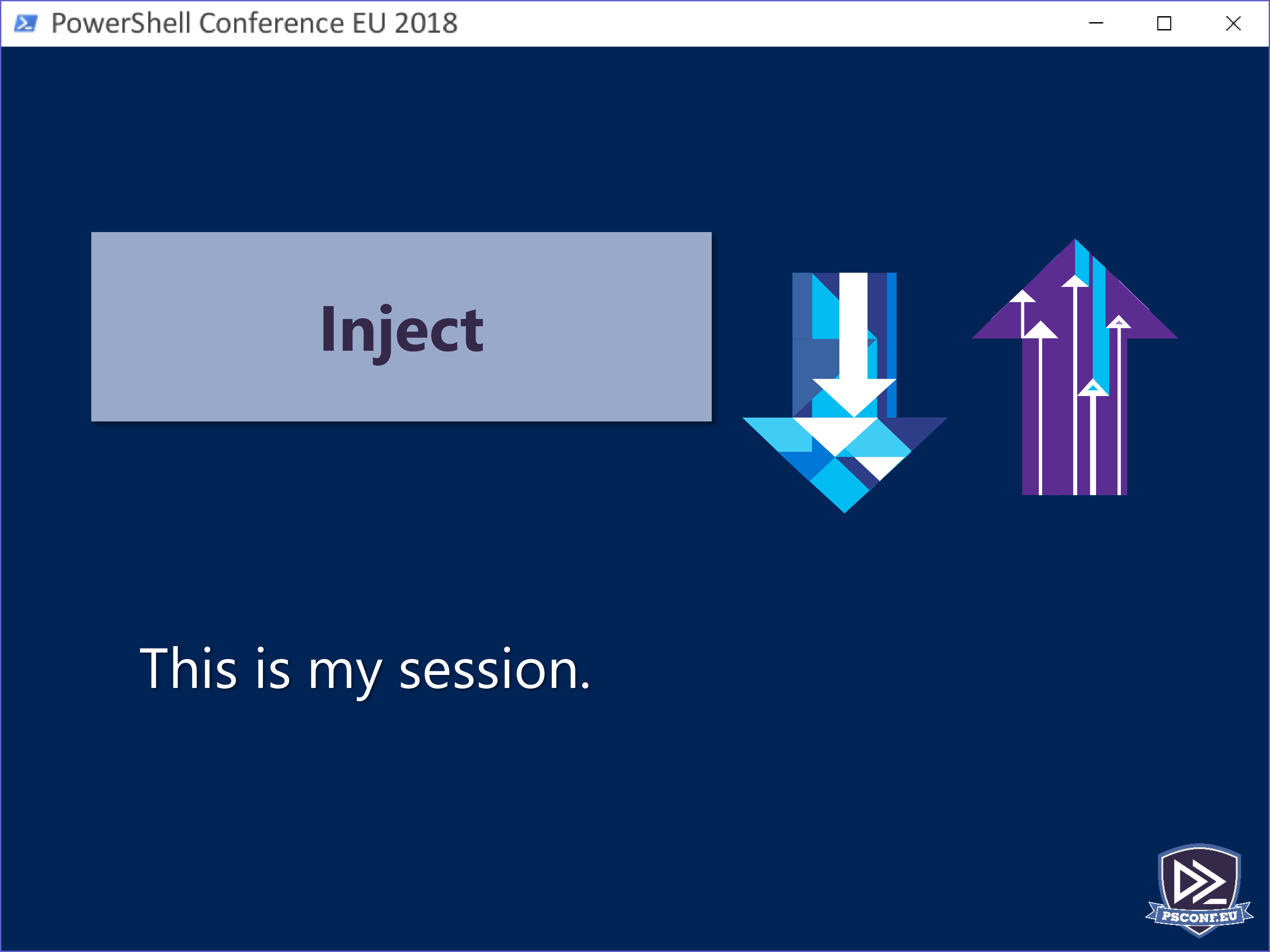
PowerShell is executed via System.Management.Automation.dll

There are various options to achieve this

- Invoked via compiled dll
- Invoked via other executables
- Downgrade & Upgrade Attack

Blue

- Blocking dlls
- Auditing



PowerShell Conference EU 2018

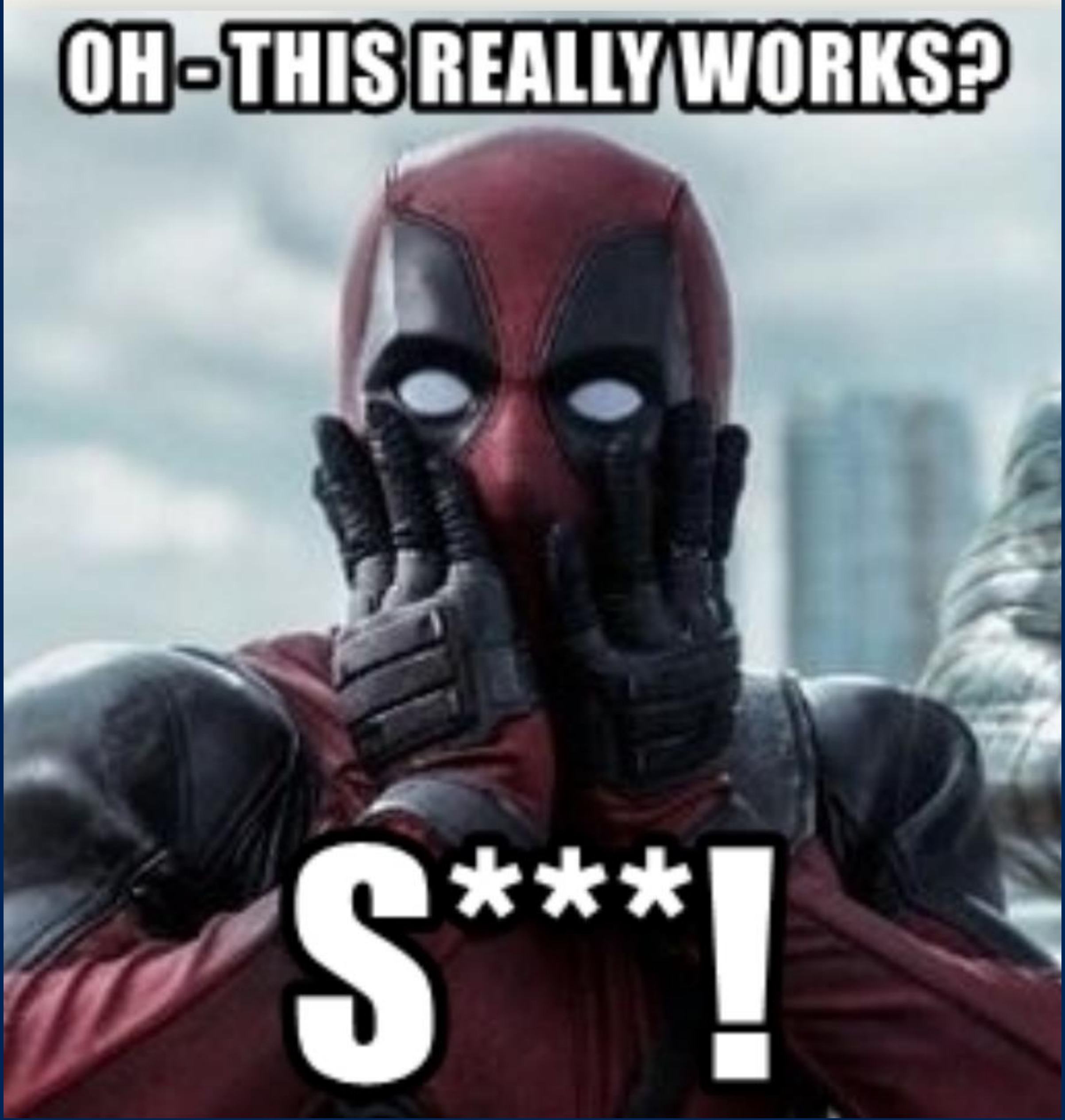
Inject

This is my session.

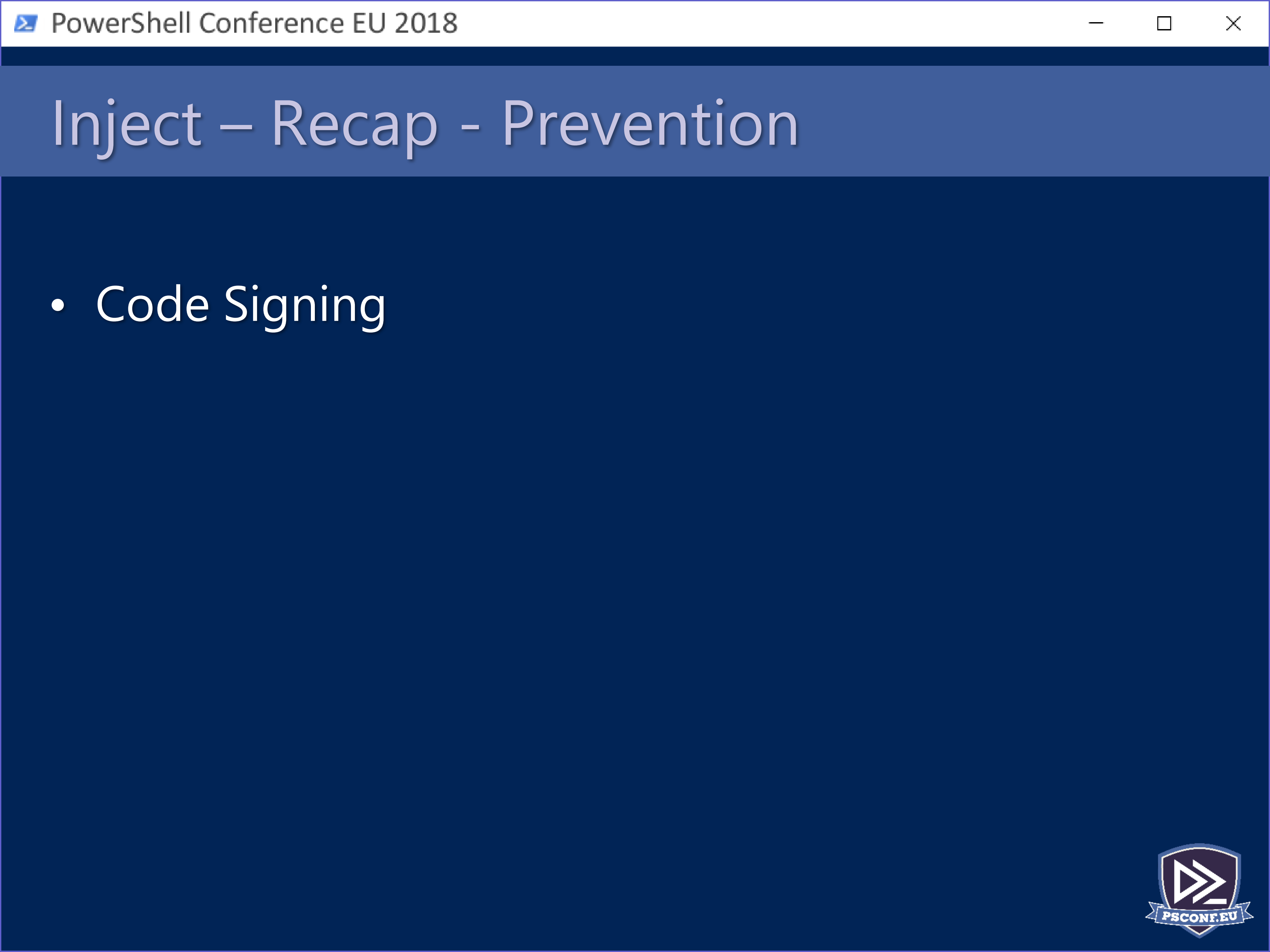
Inject - Intro

- Inject into another process and look at the precious content.

PowerShell Conference EU 2018



PSCONF.EU



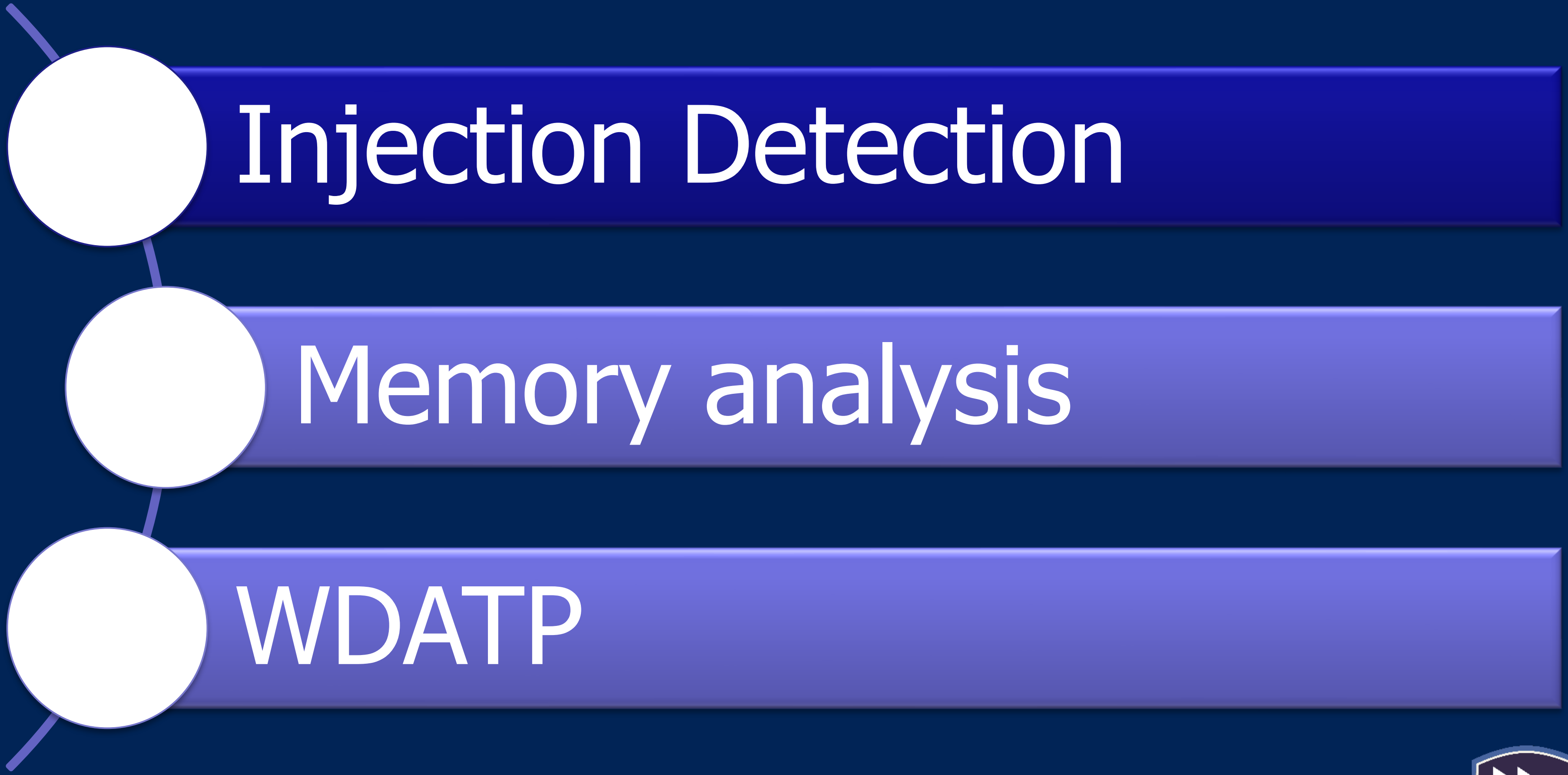
PowerShell Conference EU 2018

Inject – Recap - Prevention

- Code Signing

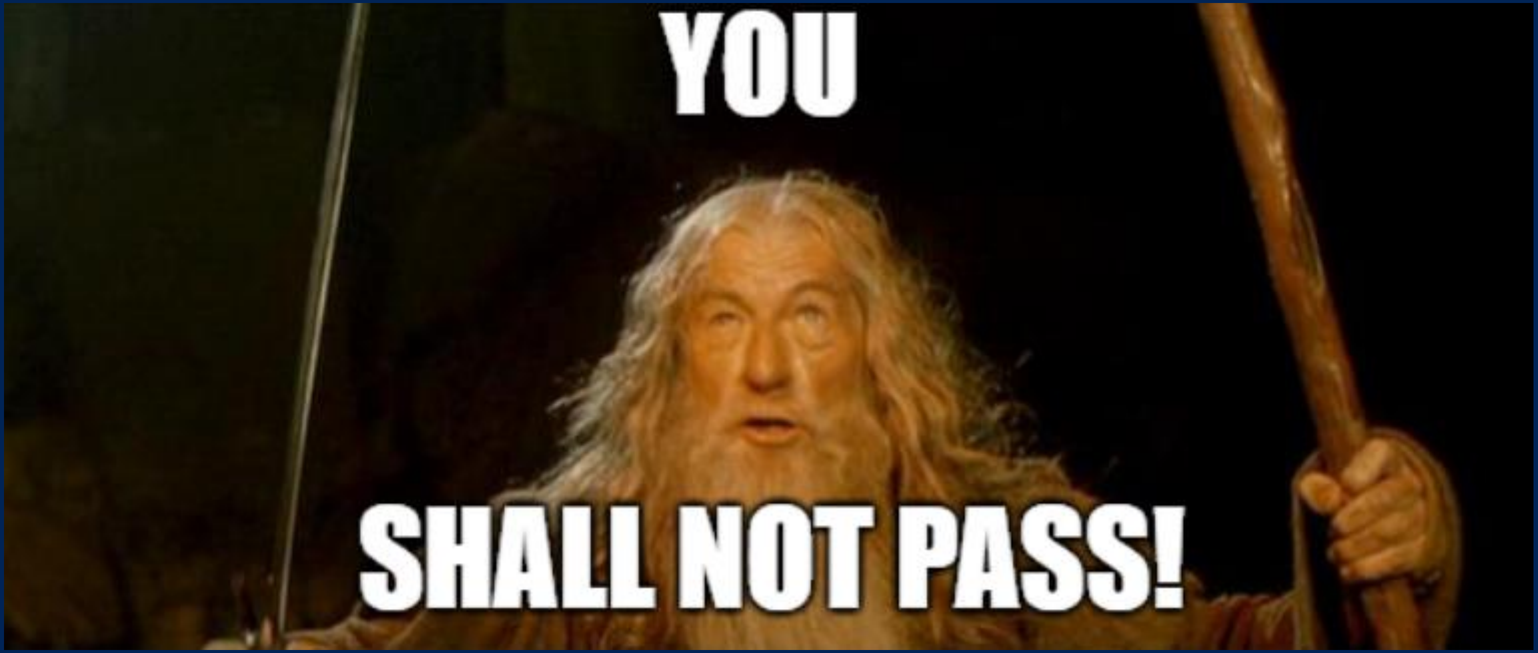
#Whitelisting

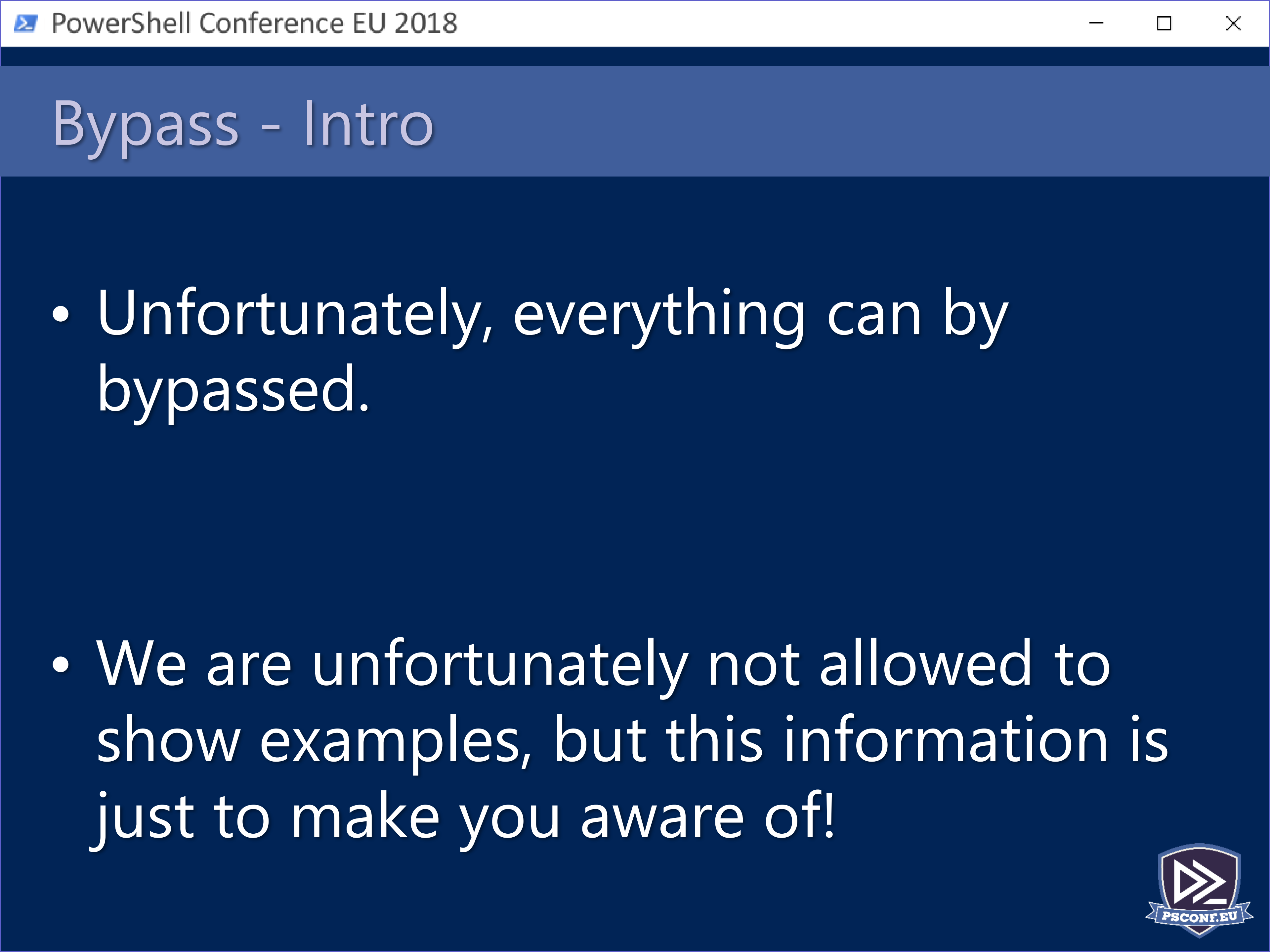
Inject – Recap - Detection



- Injection Detection
- Memory analysis
- WDATP

Bypass

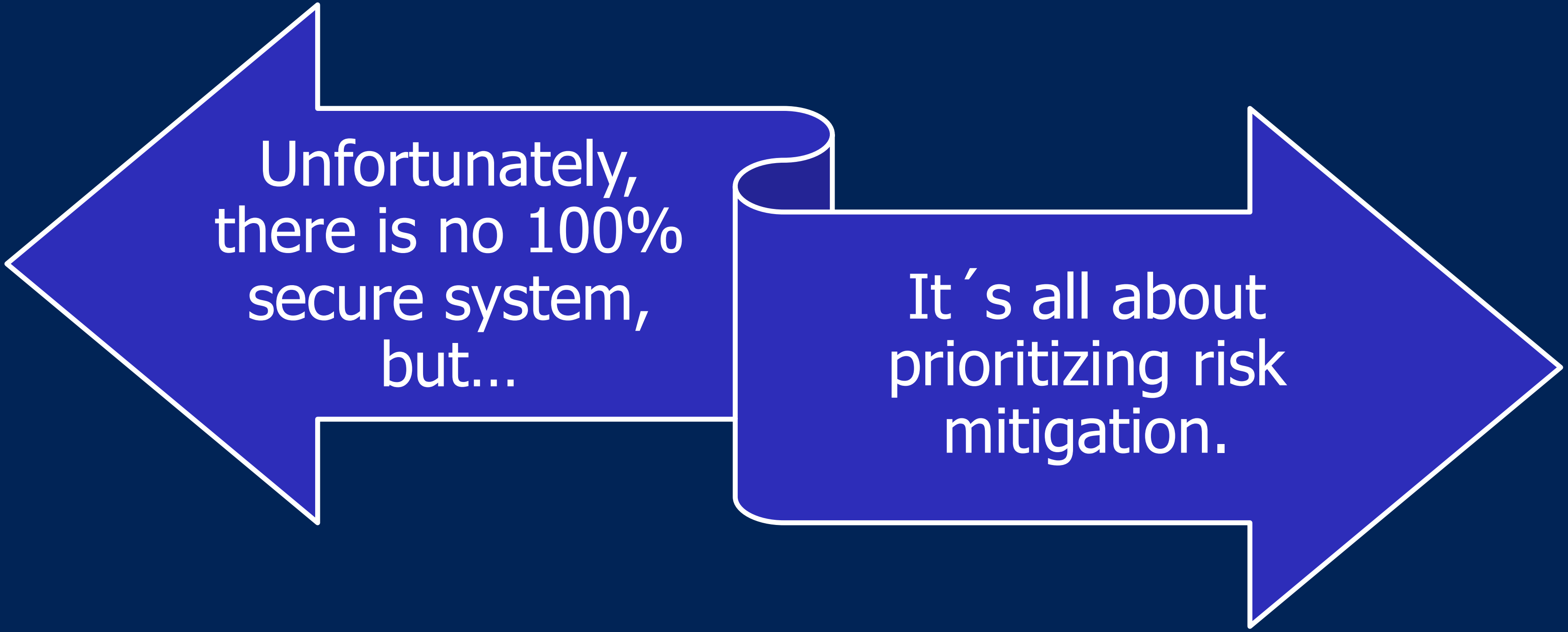




Bypass - Intro

- Unfortunately, everything can by bypassed.
- We are unfortunately not allowed to show examples, but this information is just to make you aware of!

Bypass - Recap



Unfortunately, there is no 100% secure system, but…

It´s all about prioritizing risk mitigation.

Conference Day 4 - April 20th, 2018
8:30 – 9:30
PowerShell Security - what to prioritize?

PowerShell Conference EU 2018

PSCONF.EU

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?