PowerShell Security - All you need to know

David das Neves
Premier Field Engineer

CHEF
CHEF.IO

Microsoft

KEMP
APPLICATION DELIVERY

SAPIEN
Technologies, Inc.

David das Neves
Premier Field Engineer

Twitter: @david_das_neves

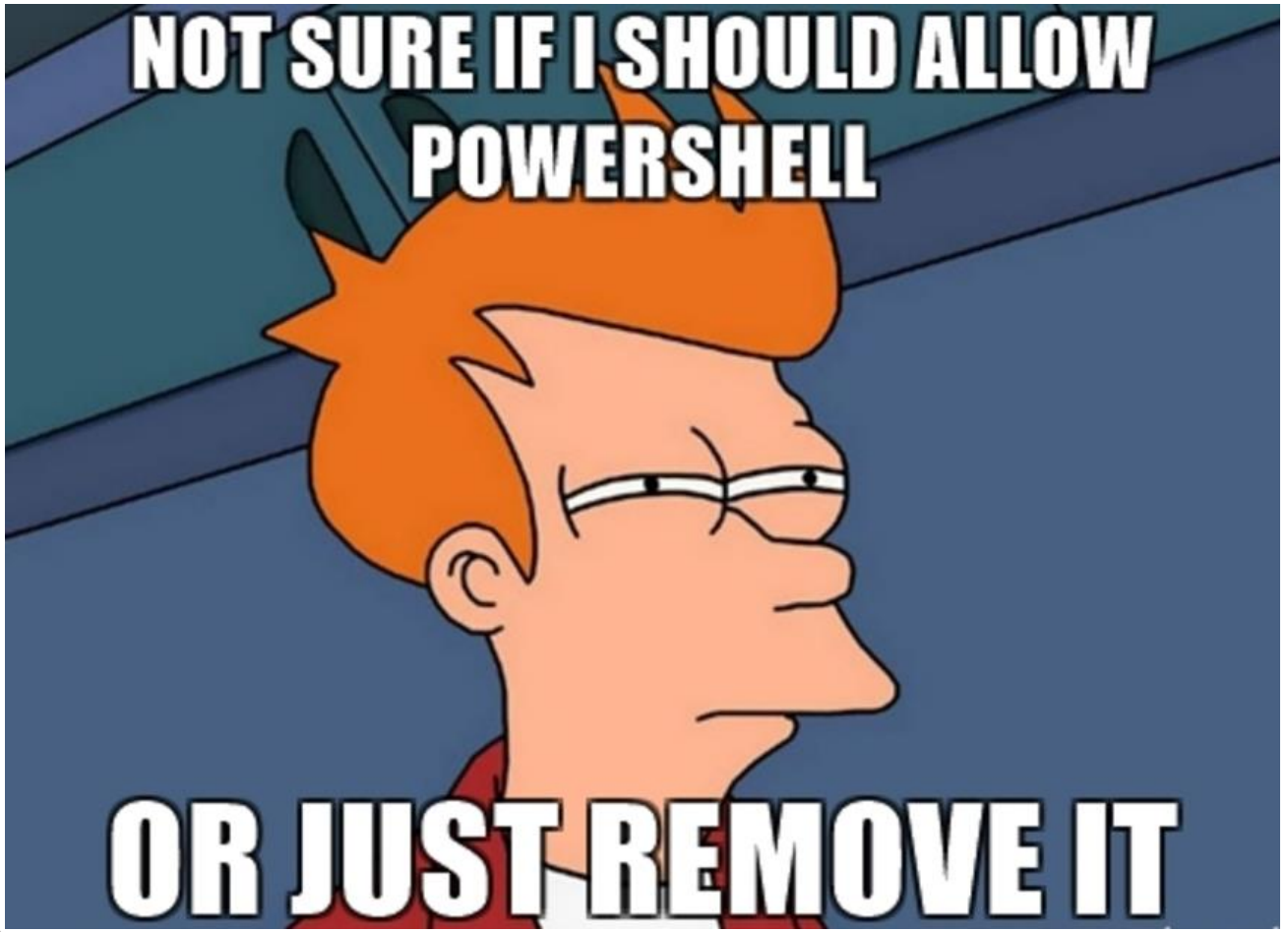
LinkedIn: DaviddasNeves

Blog: http://aka.ms/ddnblog

E-Mail: David.dasNeves@Microsoft.com

Introduction

Why PowerShell Security matters


NOT SURE IF I SHOULD ALLOW POWERSHELL
OR JUST REMOVE IT

Some Notes from the Field

"We don´t know PowerShell Security – therefore we shut it down completely."

"InfoSec will not let us turn on PowerShell remoting."

"Our last audit said that PowerShell needs to be locked down on all servers."

"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."

*German Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik

Top 10 reasons why attackers use PowerShell

1. Installed by default
2. Can be executed fileless
3. Generates few traces by default
4. Has remote access capabilities by default
5. Easy to obfuscate

Top 10 reasons why attackers use PowerShell

6. Defenders often overlook it when hardening

7. Can bypass application-whitelisting

8. Many sandboxes do not handle script-based malware well.

9. Has growing community with ready available scripts.

10. Many system administrators use and trust the framework

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/

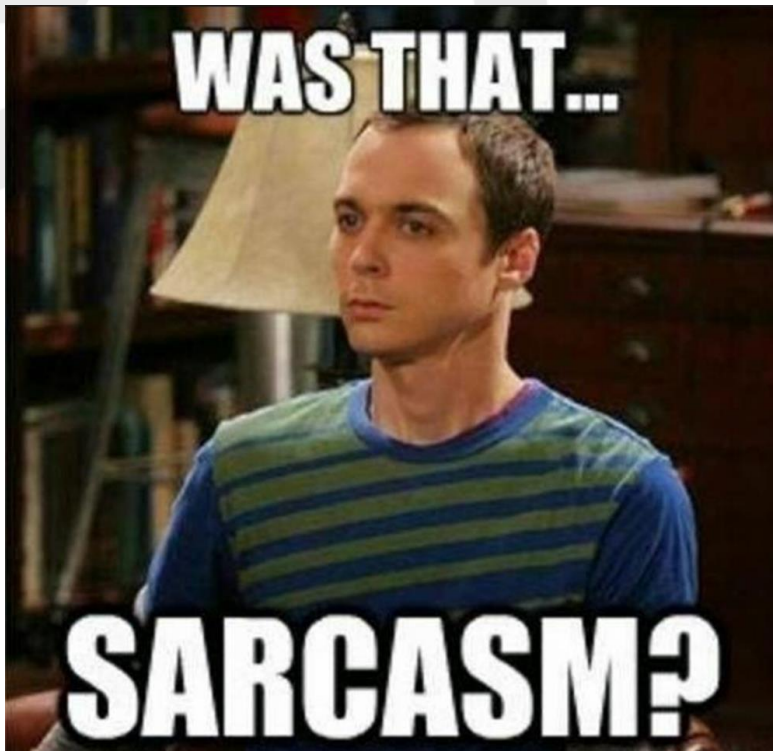
Lee Holmes, Azure Management Security, April 10, 2017

PowerShell Security

What matters.

ExecutionPolicy is a S… F…

Oh wait..



What is most important?

PowerShell is more than PowerShell.exe

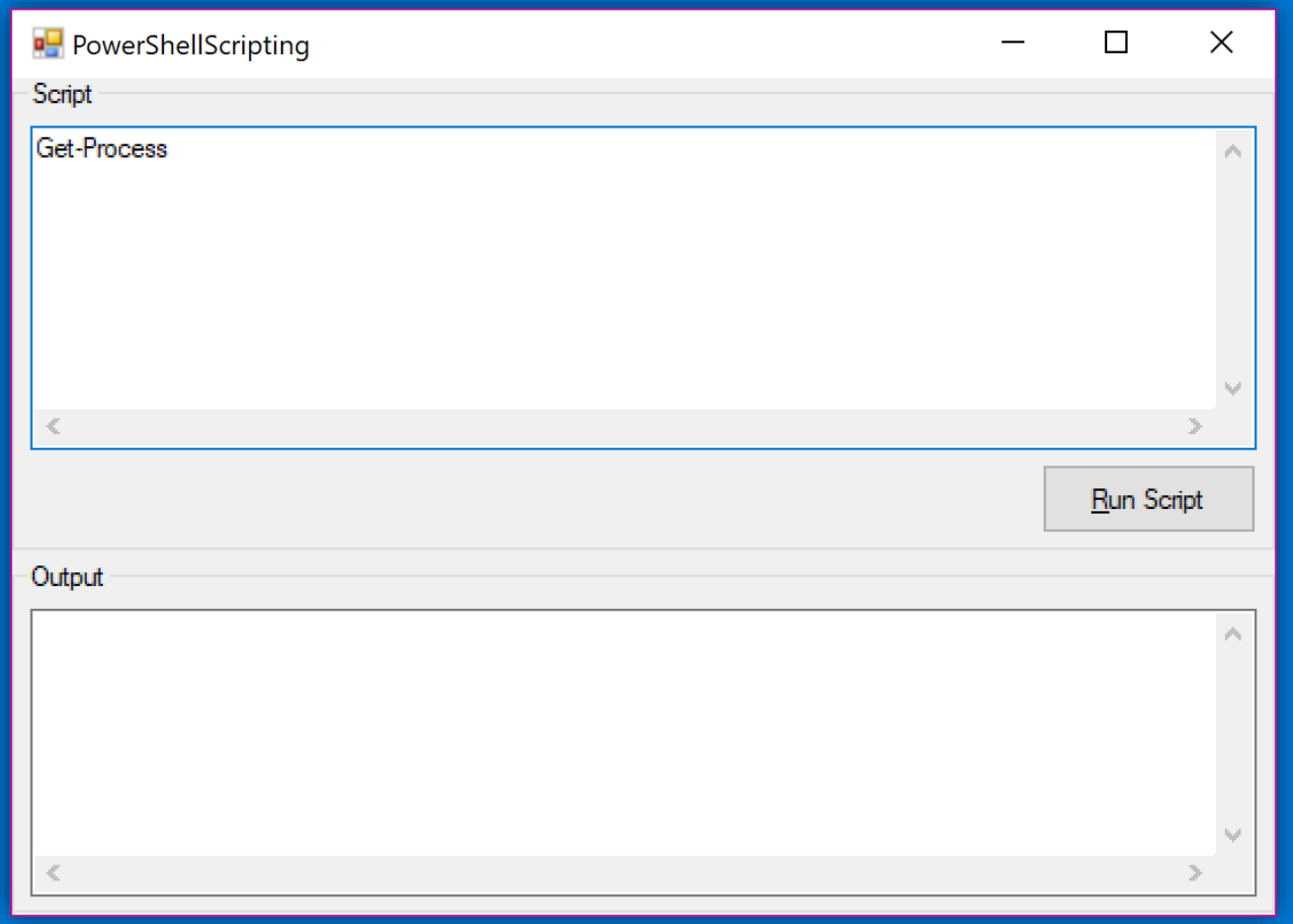
System.Management.Automation Namespace

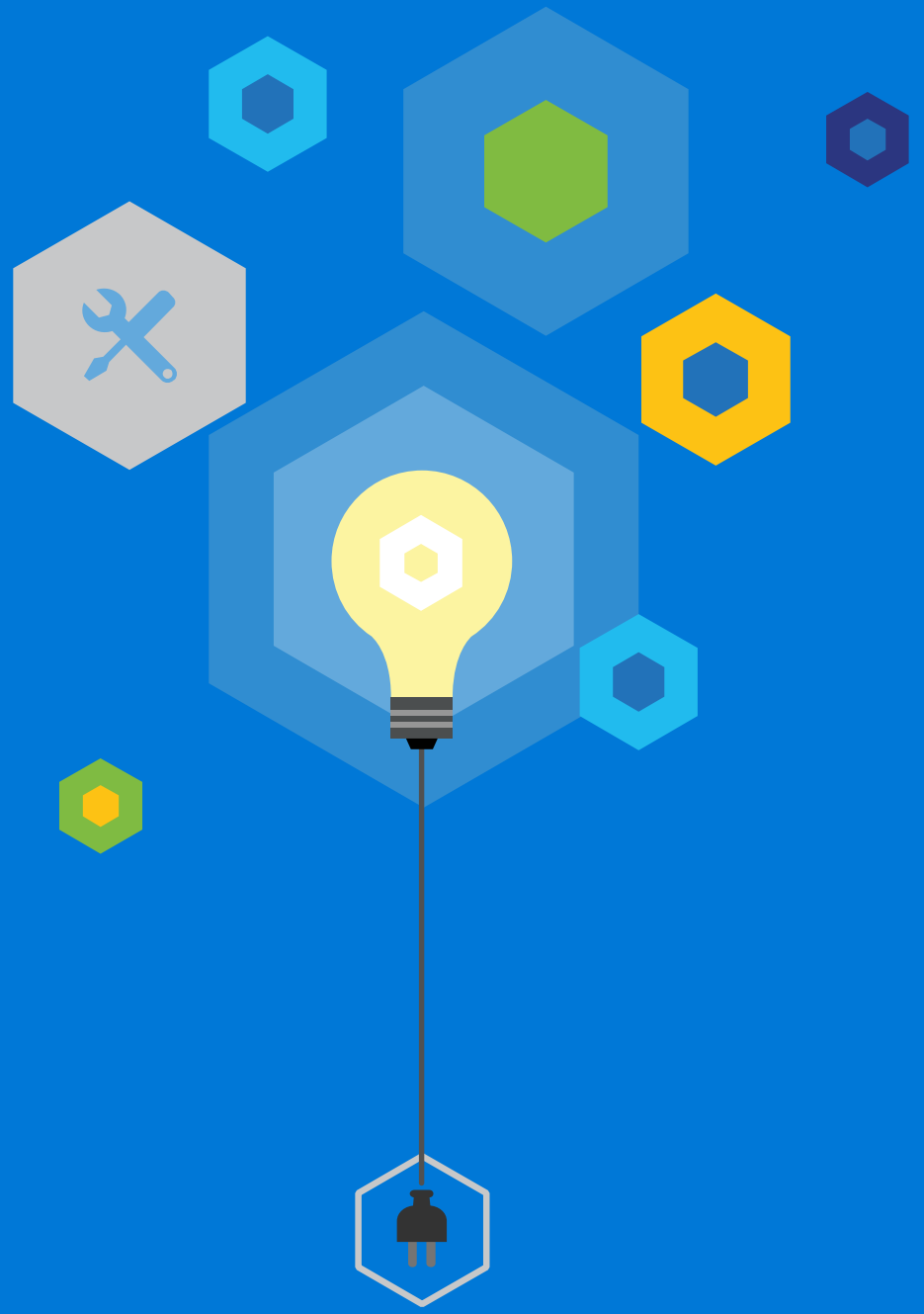
Updated: April 27, 2016

Applies To: Windows PowerShell

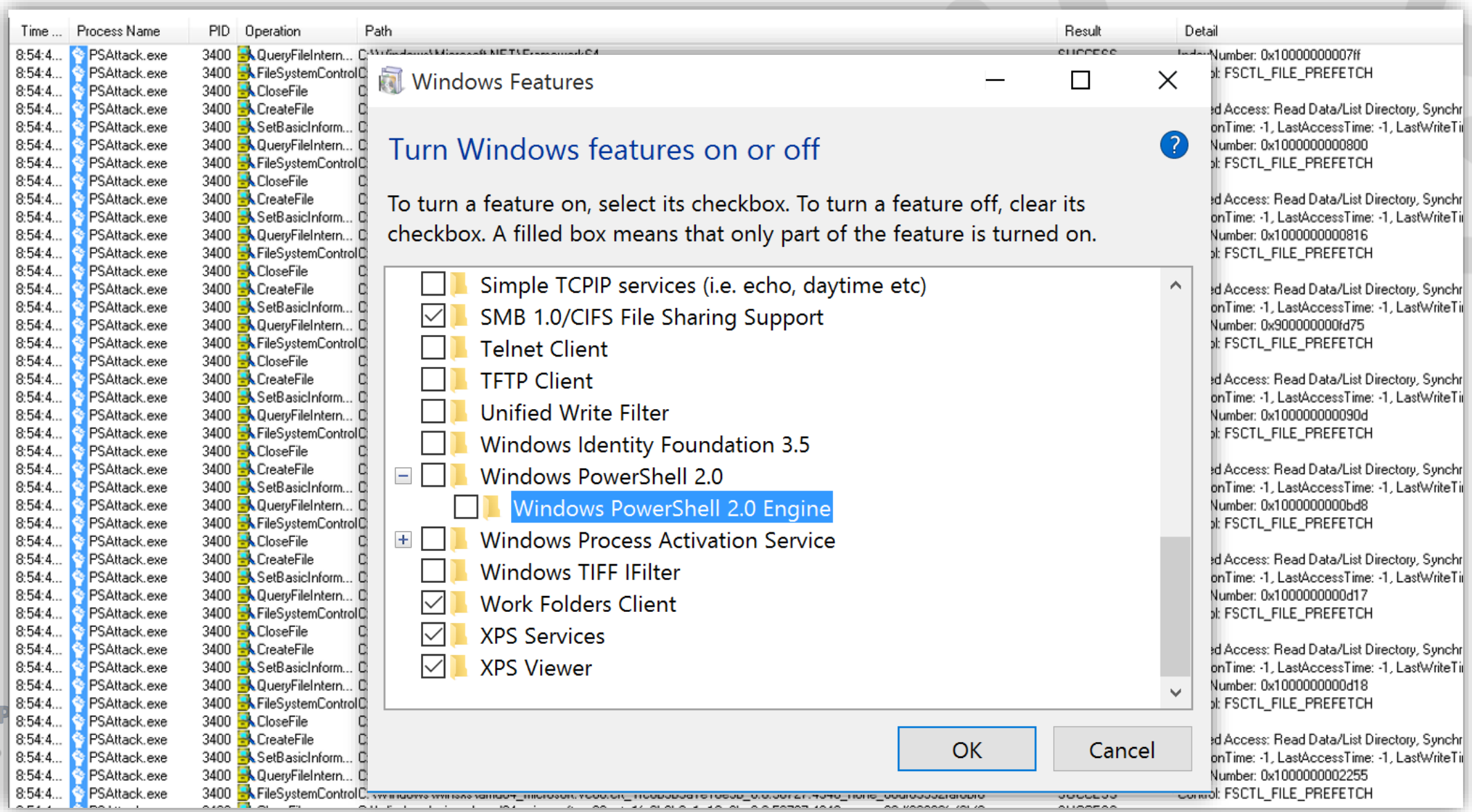
The System.Management.Automation namespace is the root namespace for Windows PowerShell. It contains classes, enumerations, and interfaces. For example, cmdlet developers will use the Cmdlet and PSCmdlet base classes to implement custom cmdlet classes, and host application developers will use the PowerShell class to create runspaces and invoke commands.

Demo – C#Power


PowerShellScripting
Script
Get-Process
Run Script
Output



PowerShell is more than PowerShell.exe



Remoting

Some companies shut down PowerShell, but …

will leave any one or more of these remote management ports open:

- Remote Desktop Protocol (RDP)
- Remote WMI access over RPC, clear text by default, random ports
- Remote event log management
- Remote service management
- SMB file share access
- PSEXEC

PowerShell Remoting

always encrypted

single port

- 5985 (http)
- 5986 (https)
  - With certificate

In a domain only members of the Administrators group have the ability to remote.

Advanced logging possibilities

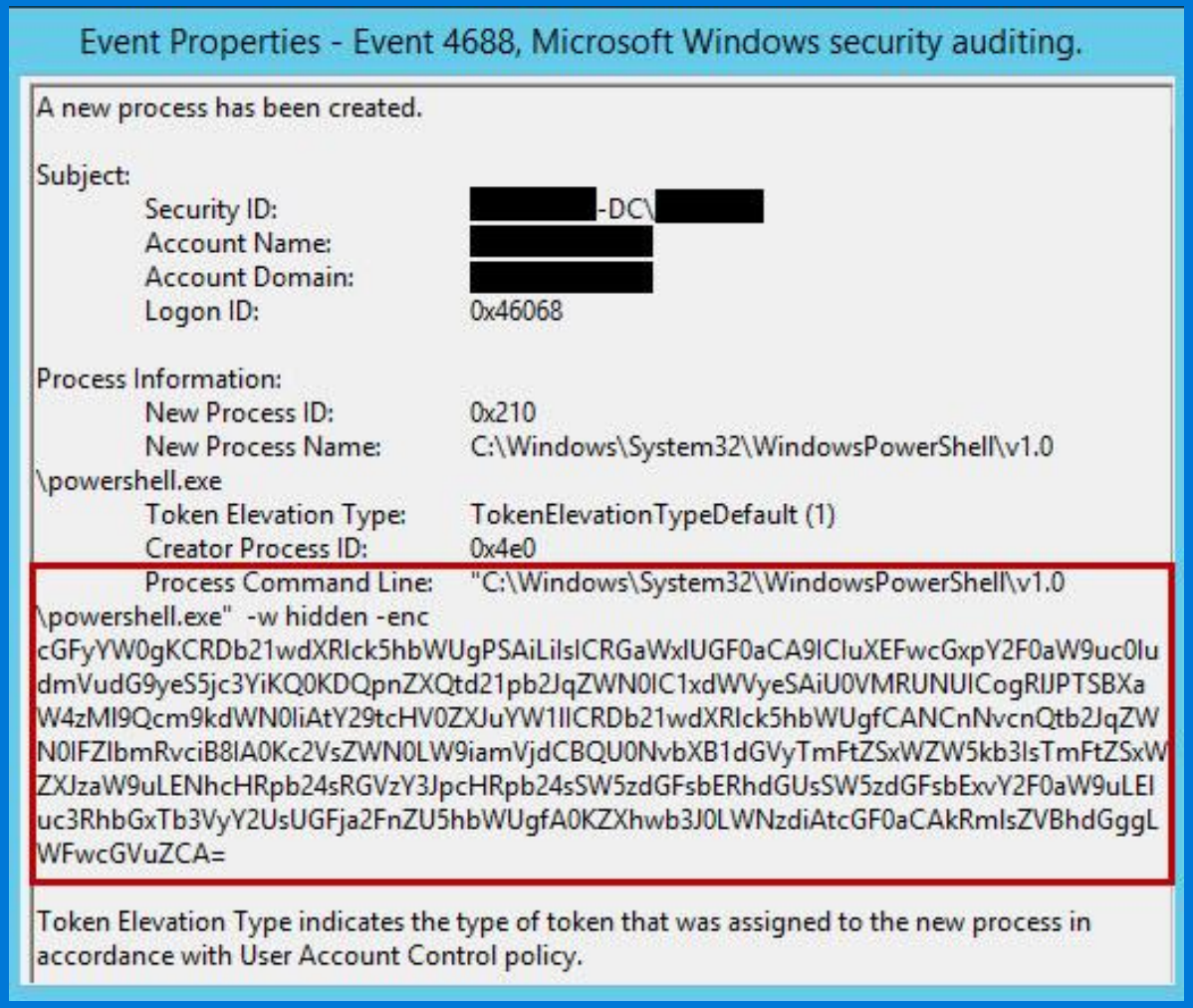
PowerShell Remoting – Bottom Line

The improvements in **WMF 5.0** make PowerShell the worst tool of choice for a hacker when you enable script block logging and system-wide transcription.

Hackers will leave **fingerprints** *everywhere*, unlike popular CMD utilities.

For this reason, PowerShell should be the *only* tool you allow for remote administration.

Logging


Event Properties - Event 4688, Microsoft Windows security auditing.
A new process has been created.
Subject:
Security ID: [redacted]-DC\[redacted]
Account Name: [redacted]
Account Domain: [redacted]
Logon ID: 0x46068
Process Information:
New Process ID: 0x210
New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Creator Process ID: 0x4e0
Process Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -enc
cGFyYW0gKCRDb21wdXRlck5hbWUgPSAiLilsICRGaWxlUGF0aCA9ICIuXEFwcGxpY2F0aW9uc0IudmVudG9yeS5jc3YiKQ0KDQpnZXQtd21pb2JqZWN0IC1xdWVyeSAiU0VMRUNUICogRlJPTSBXaW4zMl9Qcm9kdWN0IiAtY29tcHV0ZXJuYW1lICRDb21wdXRlck5hbWUgfCANCnNvcnQtb2JqZWN0IFZlbmRvciB8IA0Kc2VsZWN0LW9iamVjdCBQU0NvbXB1dGVyTmFtZSxWZW5kb3IsTmFtZSxWZXJzaW9uLENhcHRpb24sRGVzY3JpcHRpb24sSW5zdGFsbERhdGUsSW5zdGFsbExvY2F0aW9uLEluc3RhbGxTb3VyY2UsUGFja2FnZU5hbWUgfA0KZXhwb3J0LWNzdiAtcGF0aCAkRmlsZVBhdGggLU5vVHlwZUluZCA=
Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Logging

Module Logging

Transcription Logging

ScriptBlock Logging

Module Logging

- records pipeline execution details, including variable initialization and command invocations.
- Available since PowerShell v3
- events are written to Event ID **EID 4103**

Transcription

- creates a unique record of every PowerShell session
- includes all input and output, exactly as it appears in the session
- very storage-efficient; stored **in files.**

Script Block Logging

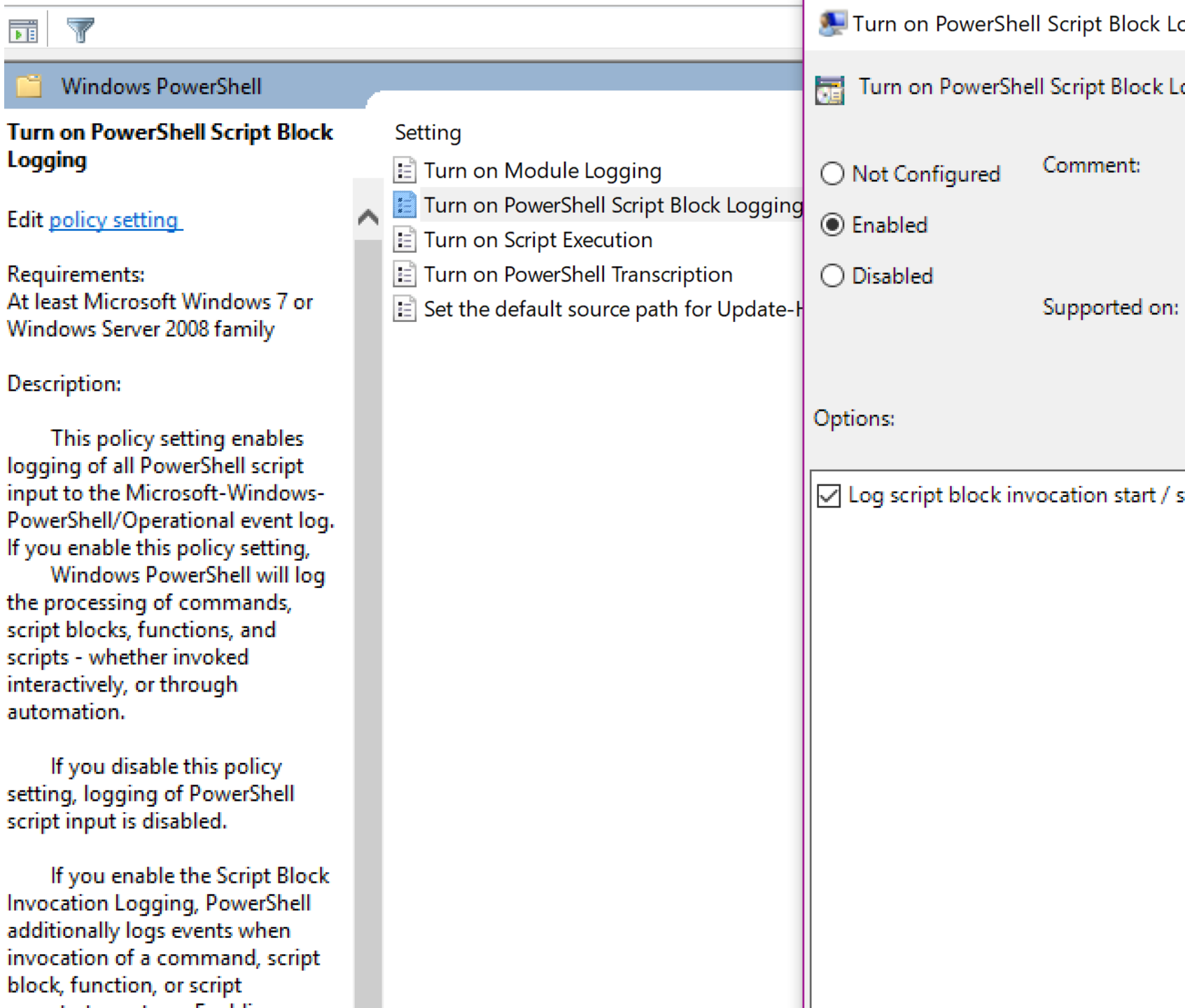
- logging records blocks of code as they are executed by the PowerShell engine
- capturing the full contents of code executed by an attacker, including scripts + commands
- also records **de-obfuscated code** logging events are recorded in Event ID **EID 4104**

Logging – Best Practice

In environments with PowerShell 5.0, organizations should consider, at a minimum, aggregating and monitoring suspicious script block logging events, EID 4104 with level "warning", in a SIEM or other log monitoring tool.

attacker commands and code execution.

Configuration GPOs / MDM



ConstrainedLanguage
Applocker
Device Guard

Constrained Language Mode

allows only core PowerShell functionality

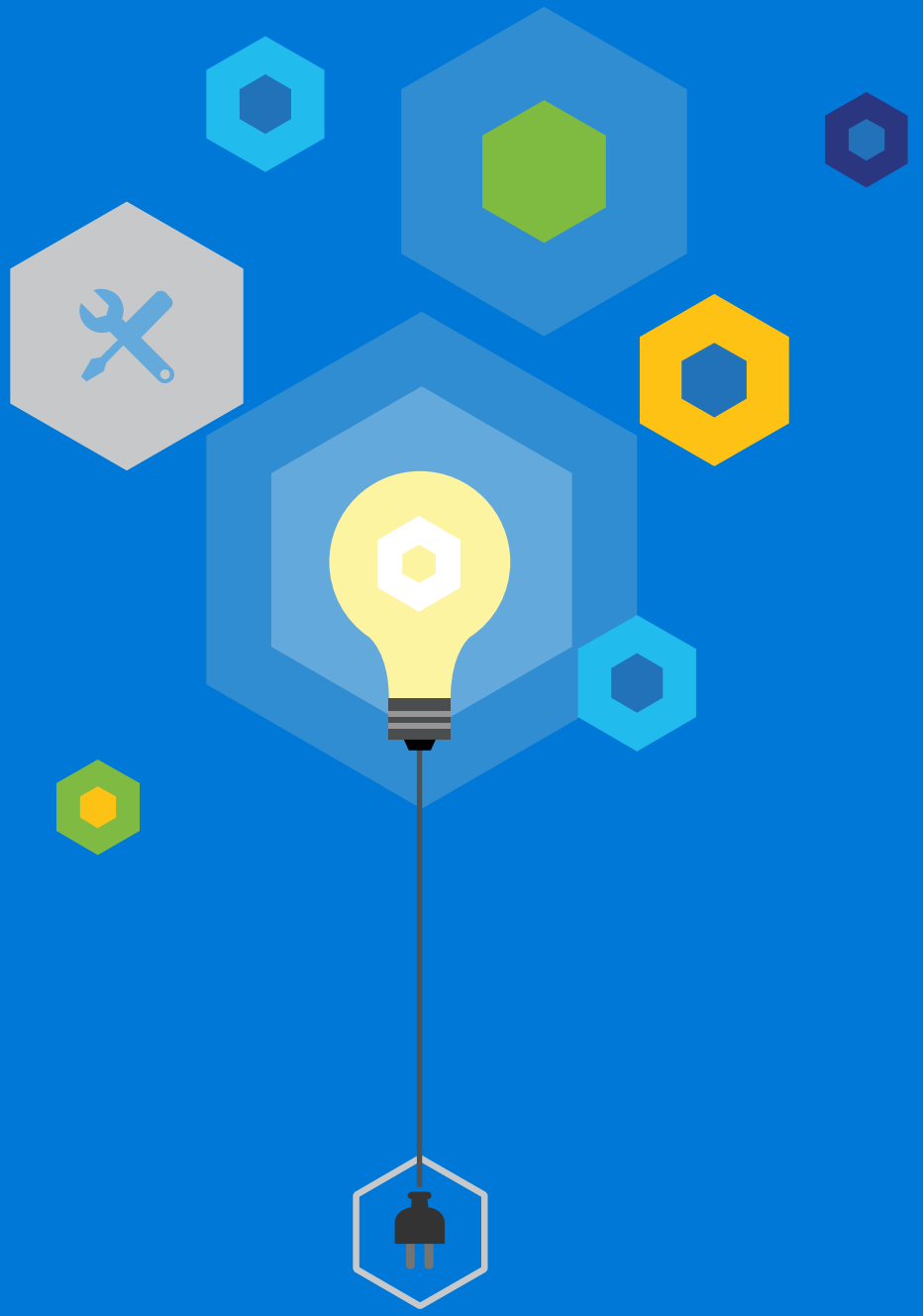
prevents execution of the extended language features often used by offensive PowerShell tools

direct .NET scripting

invocation of Win32 APIs via the Add-Type cmdlet

interaction with COM objects

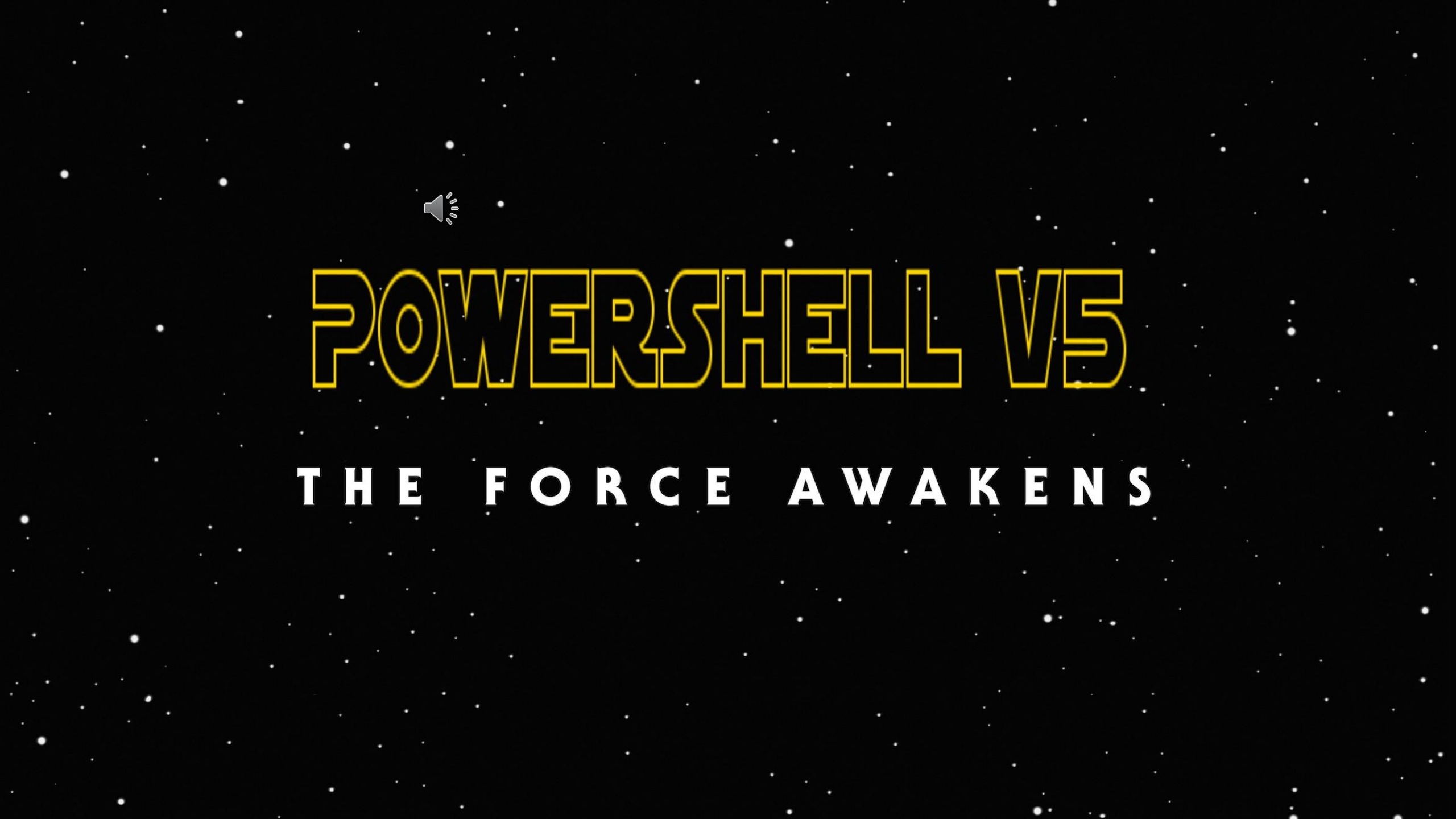
Demo - ConstrainedLanguage



PowerShell v5 changes everything

```
PS C:\Users\dadasnev> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.16288.1
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.16288.1
CLRVersion                     4.0.30319.42000
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1
```


POWERSHELL V5
THE FORCE AWAKENS

May the enforce be with you

PowerShell v5

Constrained Language

AppLocker in Allow Mode

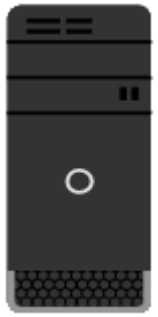
Device Guard with enforced UMCI

Applocker / DeviceGuard + PowerShell v5

Will need internal repositories and new processes

Just Enough Administration

JEA



Endpoint

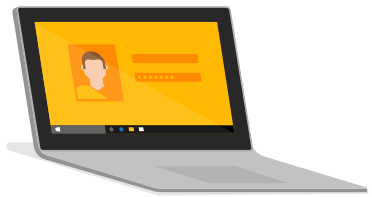
Role Capabilities

PSRemoting

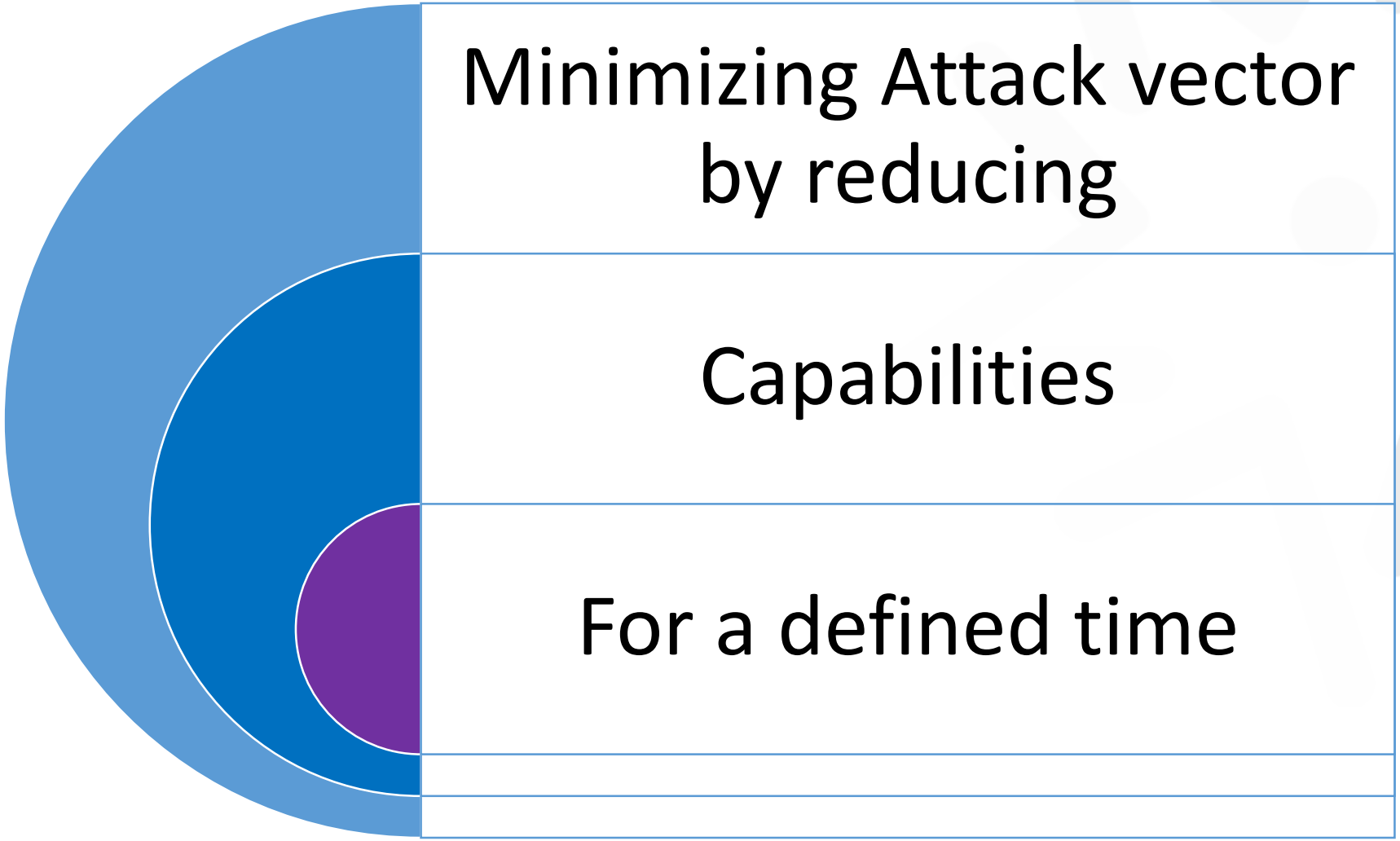
Authentication
Authorization

Server

Client
User without Admin rights



JEA


Minimizing Attack vector by reducing
Capabilities
For a defined time

Windows 10 Features
Server 2016 Features

Windows 10 / Server 2016 brings some more

Future

Enforced Constrained Language is a very secure hardening

PowerShell is becoming unattractive for pentesting companies and hackers

Summary

- 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.

Links

https://blogs.msdn.microsoft.com/daviddasneves/2017/05/25/powershell-security-at-enterprise-customers/

Don’t Forget!

- Fill in your survey in Mobile app – it’s how we do better!
- Don’t lose you badge! You need it for the Social Events
- Grab the Speakers for a chat – they all have time for you!
- Let everyone know what they are missing on Social Media

  #PowerShell

  #PSConfAsia

Photos of Marina Bay Credit: Sebastian Szumigalski