PowerShell Conference Asia

Secure your Environment by Automation

Jaap Brasser

jaapbrasser.com/about

- PowerShell Conf EU/Asia
- Dutch PowerShell User Group
- Blogging
- PowerShell Gallery
- TechNet Forums/Gallery

@Jaap_Brasser

Agenda


Security challenges
Remote PowerShell
Current threats
Demos!

Microsoft

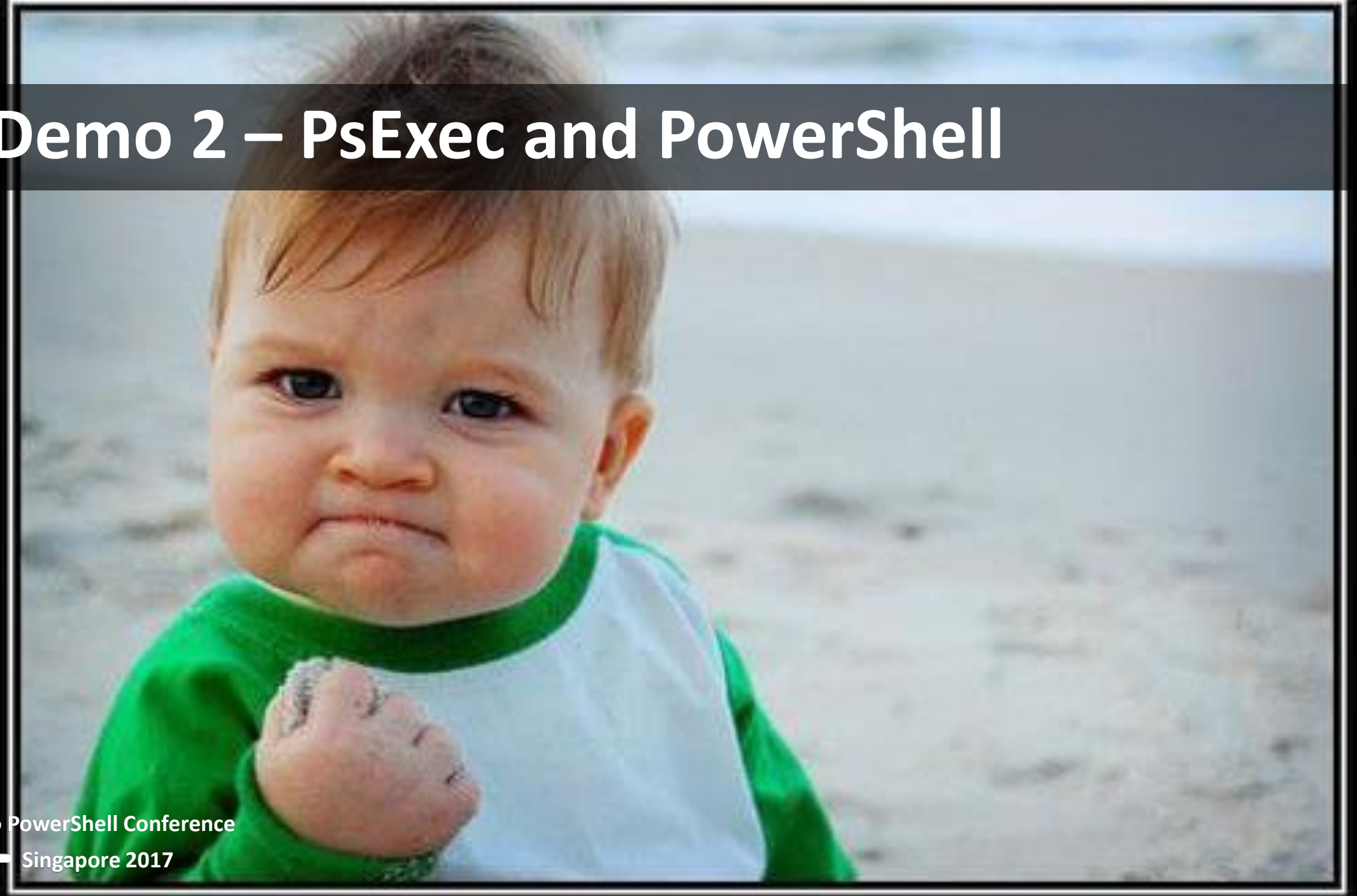
State of IT Security

Demo 1 – PowerShell Remoting

Demo 1 - Summary

- Used PowerShell Remote
- Showed Invoke-Command
- Retrieved HotFix information

Demo 2 – PsExec and PowerShell



Demo 2 - Summary

- Redirect PsExec error stream
- Use –NoBanner
- Get Text Output
- Store on network share
- Convert output to base64
- Convert base64 to PSObjects

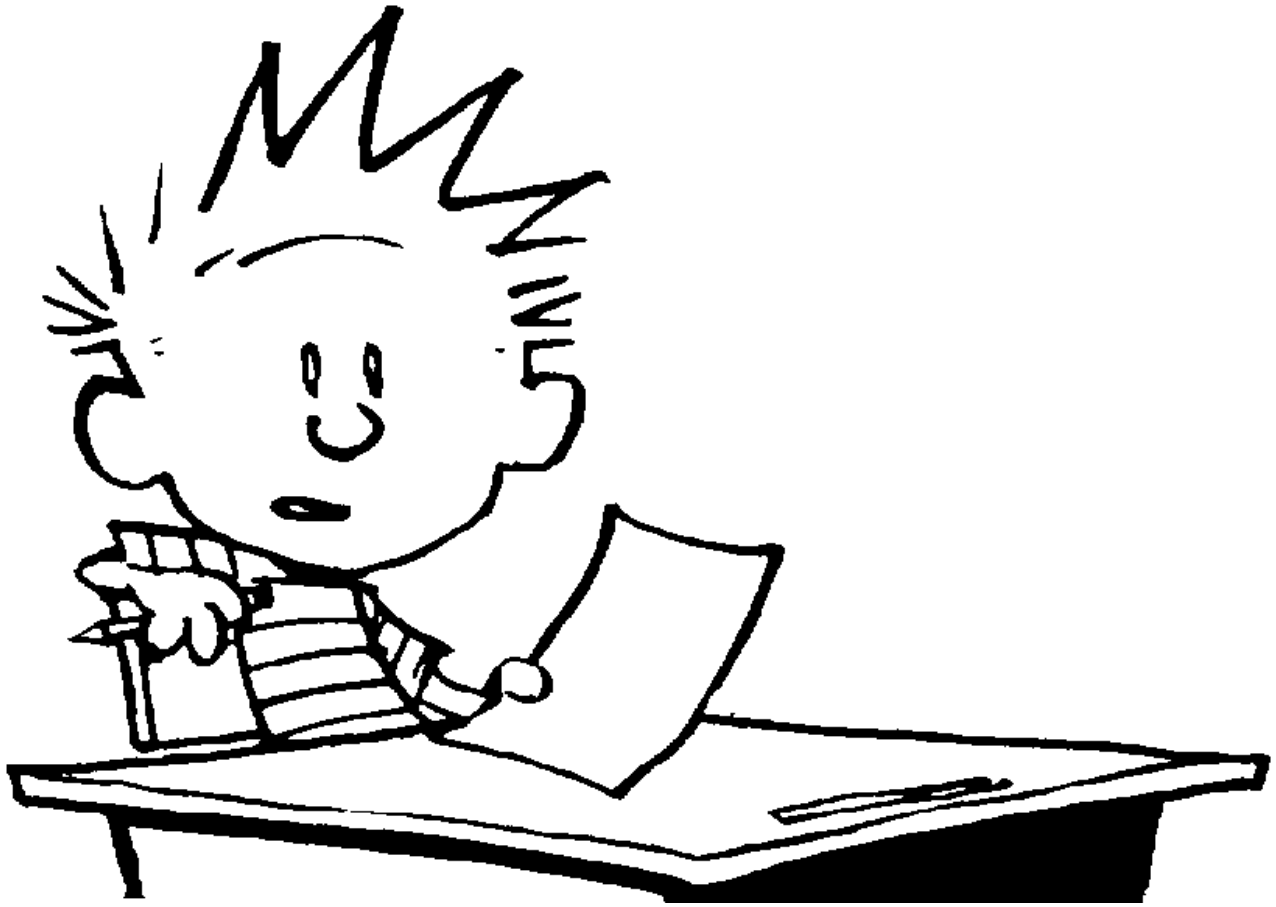
Demo 3 – Wmi and PowerShell

Demo 3 - Summary

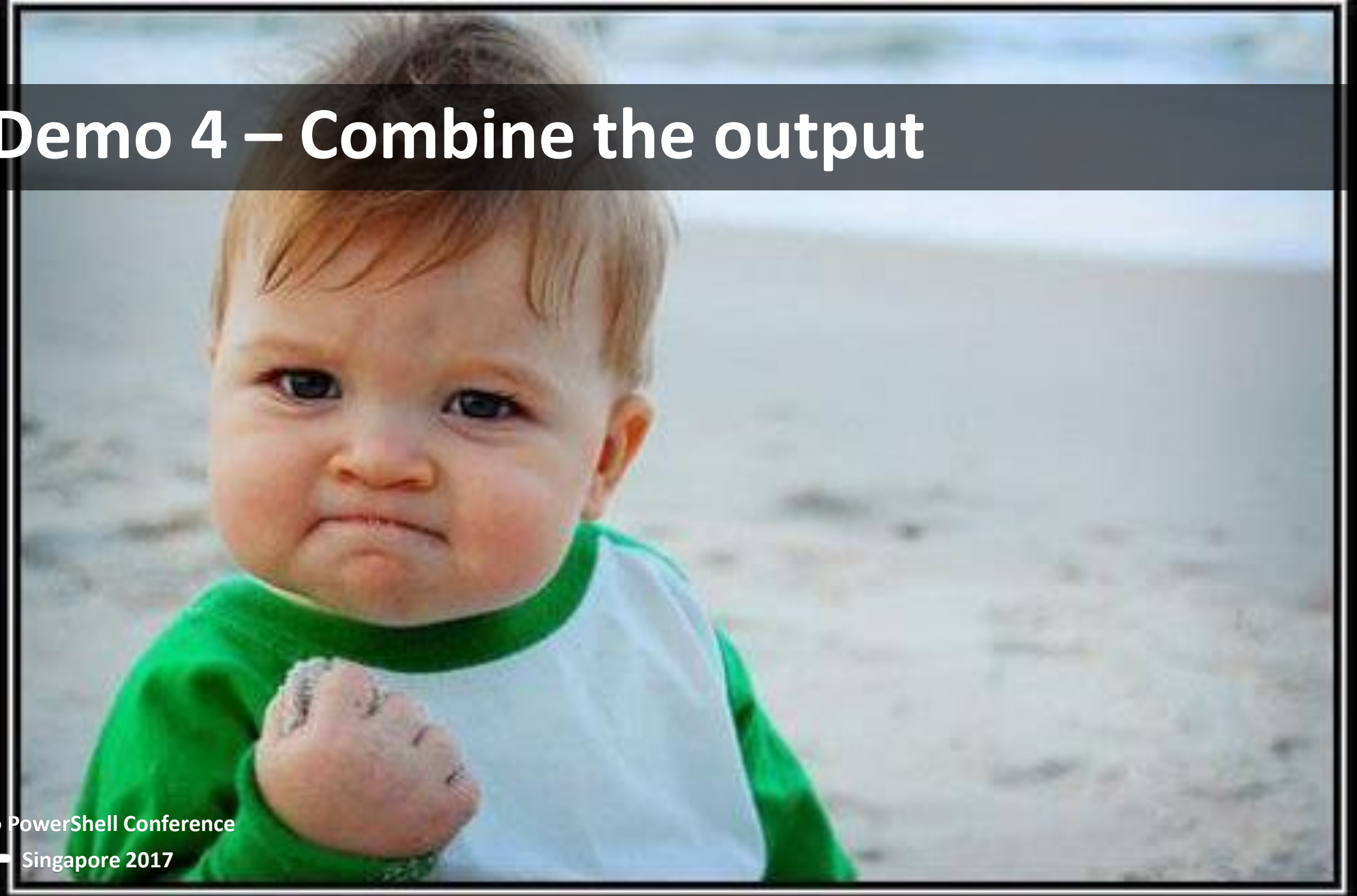
- [wmisearcher]
- [wmiclass]
- Type-accelerator performance
- Output on disk

- Store binary output in registry
- Wmi to query registry
- Recreate PSObject from binary

Why are we doing this



Demo 4 – Combine the output



Demo 4 - Summary

- Created static functions
- Generate the identical output
- Can be used to execute code / tools

What comes next?

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