POWERSHELL IDENTITY AUTOMATION WITH MIM

DUSTIN DORTCH

PRESENTER

- Dustin Dortch
  - DustinDortch.com
  - GitHub.com/DustinDortch
- Microsoft Cloud Engineer
  - Office 365
  - Enterprise Mobility + Security
  - Azure

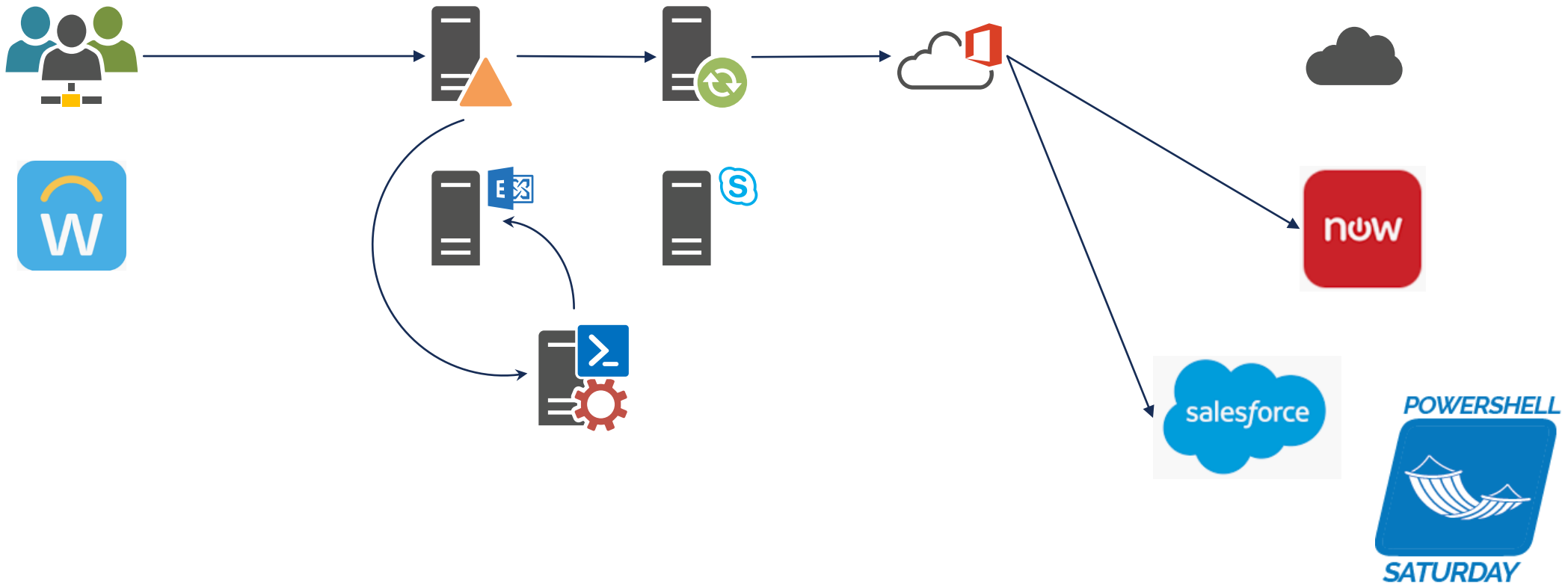
AGENDA

- Identity Lifecycle
- MIM Overview
- The Code
- Q&A

IDENTITY LIFECYCLE MATURITY

- Level 0: The "Nerf" ball method
- Level 1: Checklists
- Level 2: Scripts
- Level 3: Semi automated
- Level 4: Fully automated identities
- Level 5: Level 4, plus updates, roles, profiles, etc.

IDENTITY LIFECYCLE LANDSCAPE



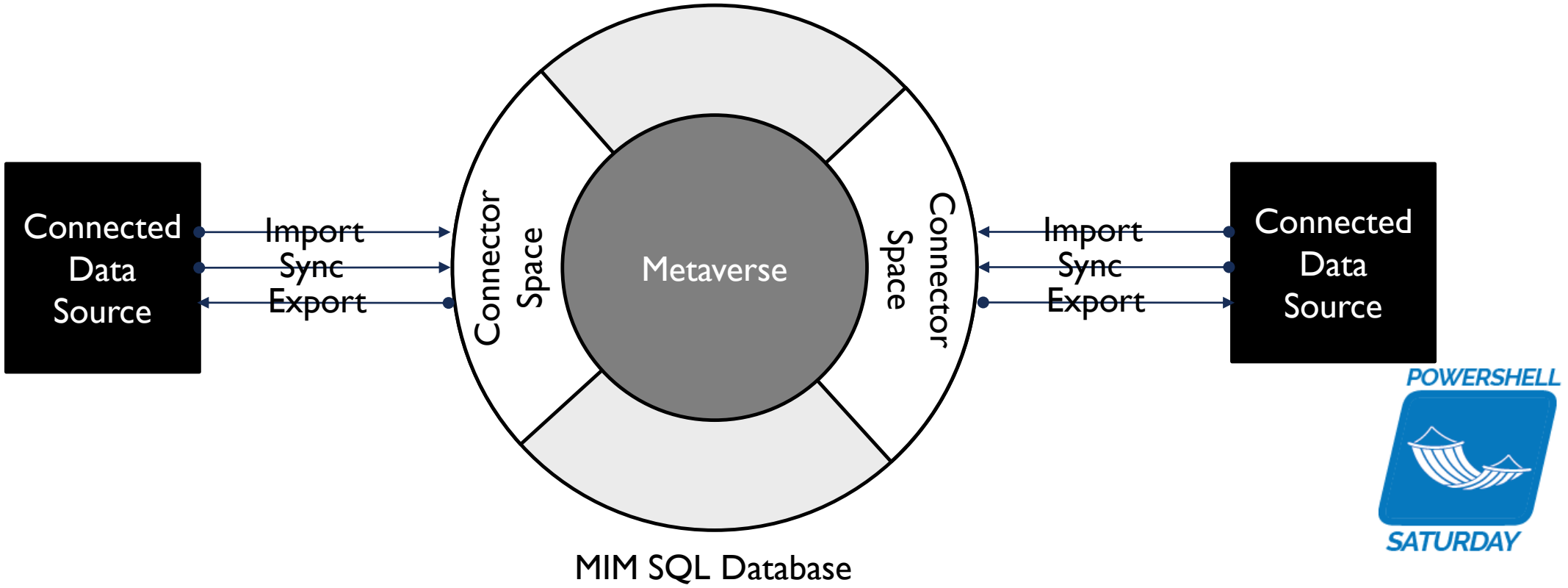
WHAT IS MIM?

- Originally known as ZoomIt Via, acquired by Microsoft in 1999
- Rebranded as Microsoft Metadirectory Server, used by MCS, in 1999
- Completely rewritten and renamed to Microsoft Identity Integration Server, in 2003 (current Sync Service)
- Certificate Management added on, rebranded to Identity Lifecycle Manager, in 2007
- SharePoint Portal bolted on for Group Management and Password Reset, rebranded to Forefront Identity Manager, in 2010
- Minor updates and rebranded to Microsoft Identity Manager, in 2016

WHERE HAVE YOU USED MIM (AND NOT REALIZED IT)?

- GAL Sync
- Exchange Edge Subscription (EdgeSync)
- Azure AD Connect (formerly DirSync and Azure AD Sync)
- Heavily utilized for automation in the backend of Office 365 services (Exchange Online, SharePoint Online, and Skype for Business Online are not accessing Azure AD, directly)

IDENTITY LIFECYCLE MIM



POWERSHELL SATURDAY

NORMAL SYNCHRONIZATION

- Directly copy attribute value from source to target (e.g. displayName)
- Manipulate attribute value from source and set in target (e.g. msExchRecipientTypeDetails)
  - Think Excel macros (I will show an example when we get to the code)
- Anything else requires an extension and custom code…
- Like the PowerShell Connector!

THE CODE STRUCTURE

- Common module
- Schema: Microsoft.MetadirectoryServices.Schema
- Partition: List[Microsoft.MetadirectoryServices.Partition]
- Hierarchy: List[Microsoft.MetadirectoryServices.HierarchyNode]
- Import
  - Begin Import
  - Import: Microsoft.MetadirectoryServices.GetImportEntriesResults
  - End Import
- Export
  - Begin Export
  - Export
  - End Export

THE CODE PRECAUTIONS

- Keep the code clean
- There is no interactive session, must log the output
- Only output the defined object
- Only output the defined object
- Only output the defined object

THE CODE

WALKTHROUGH

Q & A

FINAL THOUGHTS

EXAMPLE USE CASES

- Provision mailboxes
- Licensing (although, avoid this in favor of Azure AD Group-based licensing)
- Room lists
- Deprovisioning users
- Assigning policies, quotas, or other per-object configuration values
- Use another system to tell MIM to take action (e.g. Service Now)