AD Preparedness

Activity Directory Hygiene

Activity	Difficulty	Value
Consolidate domains	Hard	High
Reduce domain admins	Easy	Medium
Clean up GPOs	Medium	High
Password complexity for domain admins	Easy	High
Disable SID filtering	Easy	High
Remove unnecessary services from DCs	Easy	High
Patch DC and maintain at N or N-1	Easy	High
Audit and remediate ADCS	Medium	High
Understand and rationalise trusts	Medium	High
M&A – require domain consolidation	Easy	High

Preparation

Activity	Difficulty	Value
Implemented Tier Model and PAWs	Hard	High
Implement Privileged Access Management	Hard	High
Install the tools your IR provider requires	Medium	High
Snapshot and ‘deep freeze’ a DC	Easy	High
Whitelist Internet access for all servers	Medium	High
Practice changing Kerberos password	Medium	High
Practice breaking trusts	Medium	High
Document and prepare to isolate the network	Easy	Medium
Practice isolating the network	High	High
Inventory of allowed remote access methods for all applications. Block others	Easy	High
Inventory of allowed cloud storage. Block others.	Easy	High
Mimikatz, Impacket etc. playbooks	Easy	High
Model threat actor having domain admin privilege	Easy	High

Sample of Indicators

SIEM / Security Console detectable	Comments
Mimikatz, credential harvesting tools detected	Leading indicator
High number of failed logins	Leading indicator
ProcessHacker.exe detected	Leading indicator
Net User (domain enumeration) detected	Leading indicator
Unexpected GPO changed	Trailing indicator
Unexpected domain admin account change	Trailing indicator
Unexpected ADCS change	Trailing indicator

License