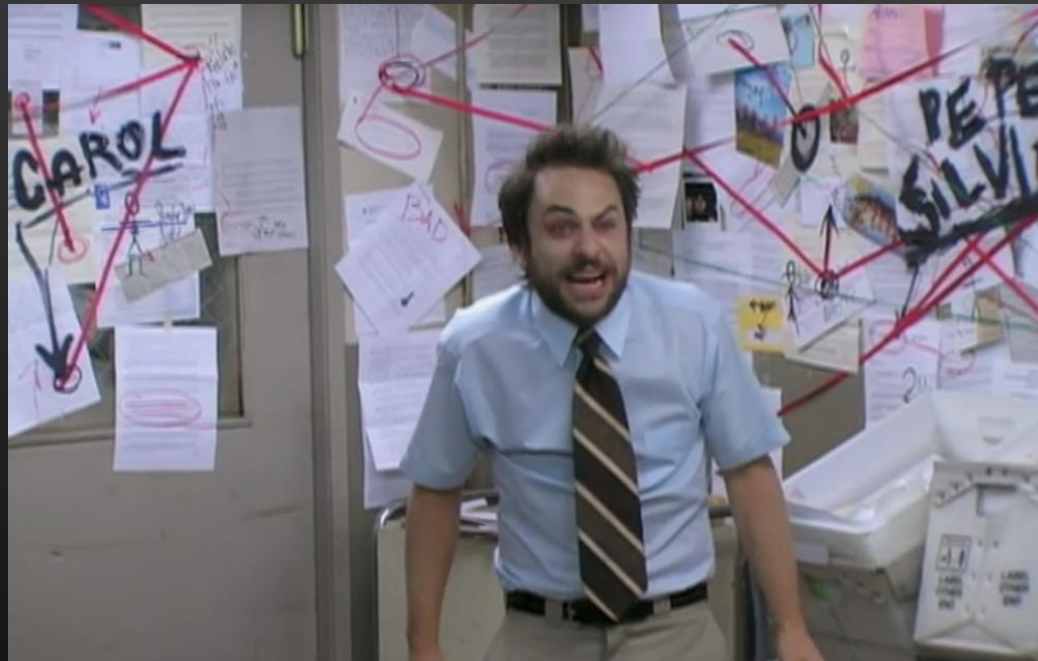
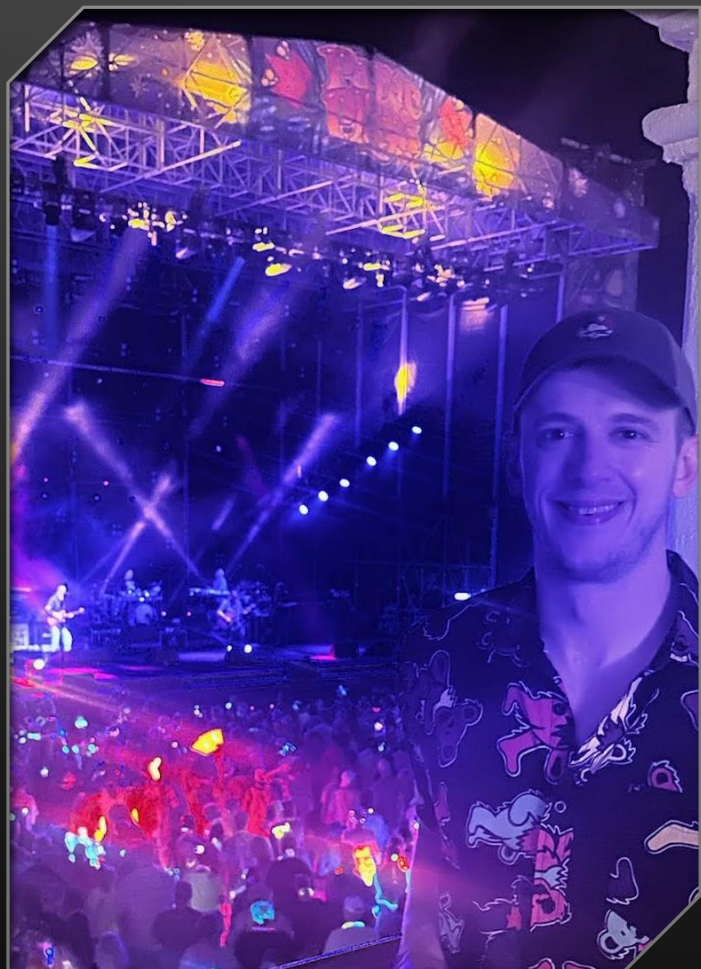


AD HARDENING: STRATEGIES FOR TIERED INFRASTRUCTURE & MINIMIZING PRIVILEGES



SAINTCON 2024

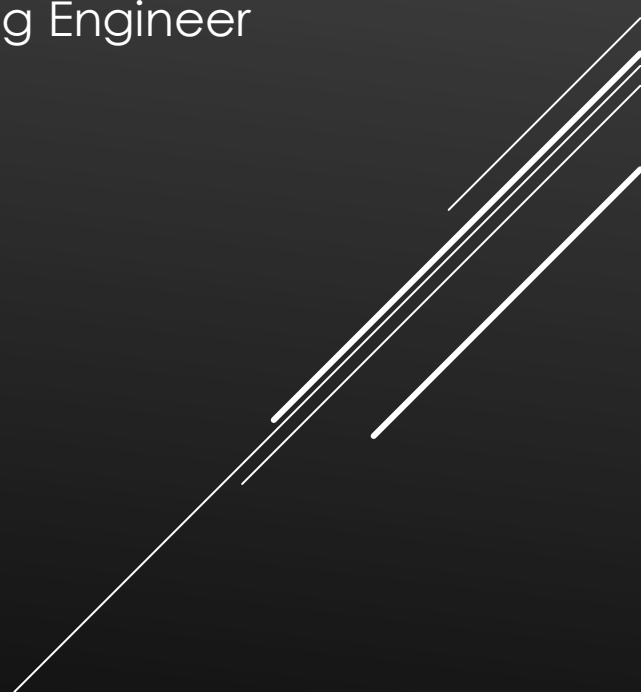


MIKE VENTURELLI

Staff Incident Response & Threat Hunting Engineer

Henry Schein One

OSCP, CISSP



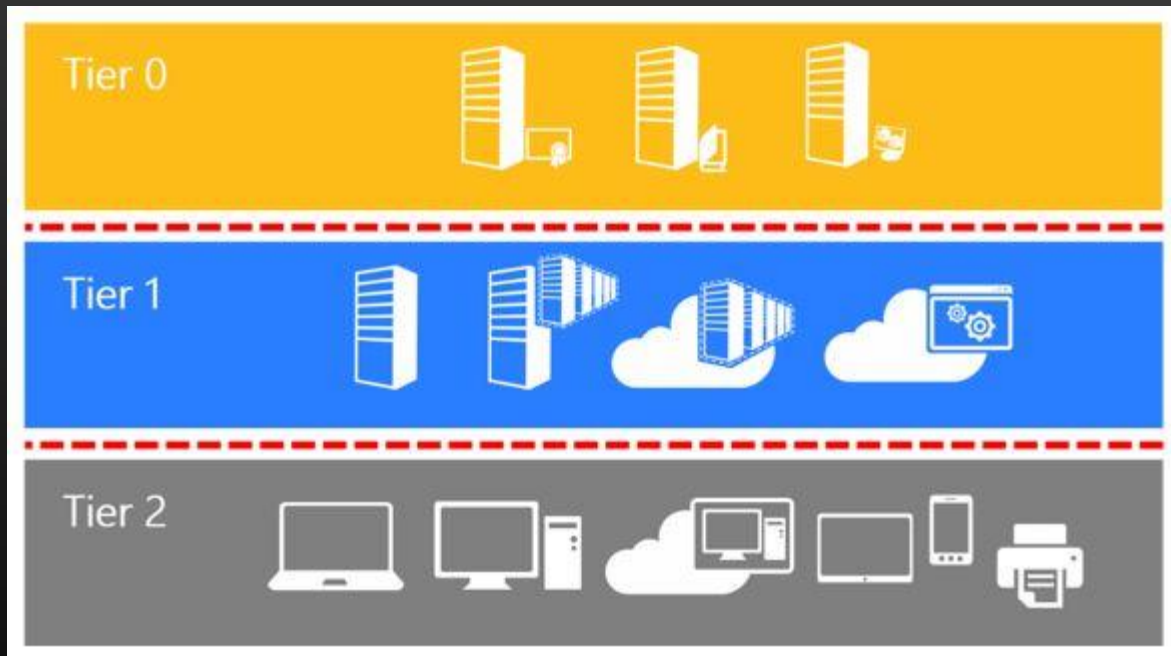
WHY?

- Reduce “blast radius” if an incident occurs
 - Becomes “more expensive”/raises the bar
 - Each tier becomes their own boundary
- Identity is the new edge
- “BYO” Privileged Access Management (PAM)
 - Lift to go to PAM solution(s) significantly reduced
- Asset Management – start, review, re-certify
- Implementing “step-up” MFA
- Reporting/auditing
- Risk discussions with management (yay!)



BLEEPINGCOMPUTER

DEFINE TIERS & PLAN



End-to-end Protection For Privileged Sessions		Enterprise Security	Specialized Security	Privileged Security
		Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
Session	Role Recommendation For privileged access role	<div>Standard users</div> <div>High impact users / developers</div> <div>IT Operations</div>		
	Device Physical device initiating session Profile Summary	Enterprise Device <i>Protect existing attack surface</i> <ul style="list-style-type: none">Centrally Managed PoliciesProductivity & Admin AppsEndpoint Detection and Response (EDR)Monitor app and browser activity	Specialized Device <i>Limit new attack surface</i> Enterprise Security Plus... <ul style="list-style-type: none">No local admin privilegesBlock unexpected applications	Privileged Access Workstation (PAW) <i>Highly Restricted attack surface</i> Specialized Security Plus... <ul style="list-style-type: none">Restricted applications (limited or no productivity apps)Restricted web browsing
	Account with access to resources			
	Intermediary Remote Access / Admin Broker			
	Interface Controlling resource access			

TIER ZERO/PRIVILEGED

- **Access to “crown jewels”**
 - Domain admin & access to DCs
- **Controls**
 - Named accounts that can be tied back to a person
 - Built-in security groups
 - Tier 0-specific fine-grained password policy (48+) & strong MFA required
 - Restrict from logging into any non-tier 0 asset
 - Privileged access workstations (PAWS)
 - Service accounts
- **Change Impact**
 - Critical risk to the org, lowest risk to disruption



TIER ZERO TABLE

SPECTEROPS

- <https://github.com/SpecterOps/TierZeroTable/>
- <https://specterops.github.io/TierZeroTable/>

TierZeroTable

Table of AD and Azure assets and whether they belong to Tier Zero.

Description of table columns and additional resources can be found here: <https://github.com/SpecterOps/TierZeroTable>

Hint: Click on a header to sort the table alphabetically.

Name	Type	IdP	Identification	Description	Known Tier Zero compromise by default configuration	Known Tier Zero compromise by common (mis)configuration	Is Tier Zero	Reasoning	Microsoft: Privileged access security roles	AdminSDHolder protected	What is Tier Zero episode	External links
Account Operators	DC group	Active Directory	SID: S-1-5-32-548	The Account Operators group grants limited	YES - Takeover	N/A - Compromise by default	YES	The Account Operators group has GenericAll	YES	YES	1	https://learn.microsoft.com/en-us/windows-
Administrator	AD user	Active Directory	SID: S-1-5-21- <domain>-500	The Administrator account is a default	YES - Takeover	N/A - Compromise by default	YES	The built-in Administrator account	YES	YES	2	https://learn.microsoft.com/en-us/previous-
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators group	YES - Takeover	N/A - Compromise by default	YES	The Administrators group has full control	YES	YES	1	https://learn.microsoft.com/en-us/windows-
AdminSDHolder	AD container	Active Directory	DistinguishedName: CN=AdminSDHolder,C	The purpose of the AdminSDHolder object	YES - Takeover	N/A - Compromise by default	YES	The permissions configured on	NO	YES	2	https://learn.microsoft.com/en-us/windows-
Allowed RODC Password Replication	AD group	Active Directory	SID: S-1-5-21- <domain>-571	The purpose of this security group is to	NO	YES - Takeover	NO	The Allowed RODC Password Replication	NO	NO	2	https://posts.specterops.io/at-the-edge-of-
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup Operators	YES - Takeover	N/A - Compromise by default	YES	The Backup Operators group has the	YES	YES	1	https://learn.microsoft.com/en-us/windows-

TIER ONE/SPECIALIZED

- **Administrative access to tier 1 assets**
 - Servers: app, web, database, etc.
- **Controls**
- Named accounts that can be tied back to a person
 - (SRV-admin, SRV-patching/services)
 - Tier 1-specific fine-grained password policy (36+) & strong MFA
 - Restrict from logging into any non-tier 1 asset/alerting if boundary crossed
- **Change Impact**
 - High risk to the org, low-to-medium disruption risk, additional pre-work/planning required
 - Asset management
 - Communication



TIER TWO/ENTERPRISE (SHORT-TERM)

- **Administrative access to tier 2 assets**

- Workstation admins, install software, etc.
- Depending on environment/use case, could also be “user”-level access to Tier1 assets (CanRDP)

- **Controls**

- Named accounts that can be tied back to a person/owner
- Tier 2-specific fine-grained password policy (24+) & strong MFA
- Unable to access higher tiers

- **Change Impact**

- High impact, high risk of disruption



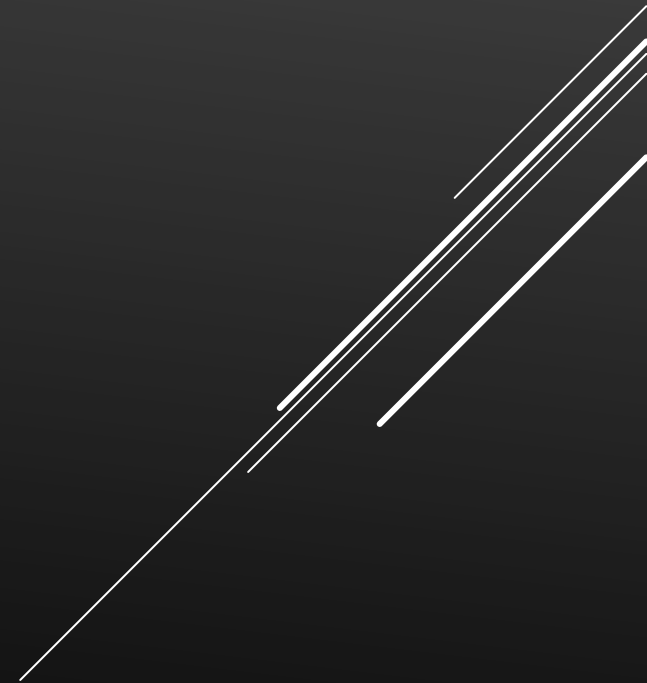
TIER TWO/ENTERPRISE (LONG-TERM)

- Local Administrator Password Solution (LAPSv2)/InTune Admin
- Centralized management/cataloging/asset management




End User

- Company Portal/share – approved software catalog
- Golden images/virtual desktops
- Domain password policy (15+)



ALL TIERS/GROUPS

- Lifecycle management – utilize a field in AD (extattr) to “link accounts” for a user
 - Service accounts
 - MSA(single)/gMSA(multi)
 - Password managers
 - "Productivity apps" limited to non-admins
 - Cloud/Hybrid Admins
 - Net-new requests after process established & agreed upon
- 
- A series of several parallel white lines of varying lengths and slopes, located in the bottom right corner of the slide, creating a modern, abstract graphic element.

ENVIRONMENT ASSESSMENT


- **Active Directory**

- BloodHound (CE or Enterprise) [On-Prem/Active Directory & Cloud]
 - Community: <https://github.com/SpecterOps/BloodHound>
 - Enterprise: <https://bloodhoundenterprise.io/>
- PingCastle (Netwrix) <https://www.pingcastle.com/>
- PurpleKnight (Semperis) <https://www.semperis.com/purple-knight/>

- **Hybrid/Cloud**

- SCuBA (CISA) <https://github.com/cisagov/ScubaGear>
- Monkey365 (silverhack) <https://github.com/silverhack/monkey365>
- ScoutSuite (NCCGroup) <https://github.com/nccgroup/ScoutSuite>
- ROADTools (dirkjanm) <https://github.com/dirkjanm/ROADtools>

ADDITIONAL HYGIENE

- **Third party/vendors/external**
 - **Endpoint file type associations**
 - .js, .jse, .bat, .cmd, .ps1, .iso, .hta, .vbs, .vbe, .wsf, .wsh
 - **Active Directory Certificate Services (ADCS)**
 - BloodHound, LockSmith
 - **RMM, file transfer, backup apps**
 - **Browser settings/extensions**
- 
- A series of four parallel white lines of varying lengths, slanted diagonally upwards from left to right, located in the bottom right corner of the slide.

PROTOCOLS

- Disable:
 - LLMNR
 - NBNS
 - mDNS
 - IPv6
 - WPAD
 - WebDav
 - SMBv1
- To Harden:
 - SMB(v2-3)
 - LDAP(S)

Resources:

Disabling NTLMv1 - https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/active-directory-hardening-series-part-1-disabling-ntlmv1/ba-p/3934787?WT.mc_id=5003815

Disabling SMBv1 - <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/active-directory-hardening-series-part-2-removing-smbv1/ba-p/3988317>

Configure SMB Signing with confidence - <https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102>

PUSHBACK

“This is impossible, we’re never going to be able to do this!”

“How am I/others supposed to remember which account to use?”

“My password needs to be HOW LONG?! I’ll never remember that!”

“I prefer SMS/email for MFA, I don’t like:

- push notifications & having to enter a number
- Having to use a hardware key for my MFA.”

“Just using a bastion host for accessing servers solves the problem.”

RESOURCES

- ADSecurity - <https://adsecurity.org/>
- CIS Top 18 - <https://www.cisecurity.org/controls/cis-controls-list>
- Microsoft's Privileged Access strategy - <https://docs.microsoft.com/en-us/security/compass/privileged-access-strategy>
- Rapid Modernization Plan - <https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan>
- Short Videos - <https://docs.microsoft.com/en-us/security/compass/administration-videos-and-decks>
 - More involved slide deck: <https://docs.microsoft.com/en-us/microsoft-365/downloads/security-compass-presentation.pptx>
- Securing devices overview - <https://docs.microsoft.com/en-us/security/compass/privileged-access-devices>

RESOURCES

- “Initially Isolate Tier 0 Assets with GPOs to start Administrative Tiering” - <https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/initially-isolate-tier-0-assets-with-group-policy-to-start/ba-p/1184934>
 - “Prevent lateral movement in AD with authentication policies” - <https://blog.improsec.com/tech-blog/preventing-lateral-movement-in-active-directory-with-authentication-policies>
 - “Securing Windows Environments” - <https://blog.improsec.com/tech-blog/securing-windows-environments>
 - SpecterOps blog - <https://specterops.io/blog/>
- 
- A series of three parallel white lines of increasing length, slanted upwards from left to right, located in the bottom right corner of the slide.