

**PAS Program Template**

Prepared for CIII Capital Partners

## 1-3 months

Recommendation: Randomize Built in Backdoor Admin passwords

* Built In Local Administrators
* Root
* Oracle SYS/System
* MSSQL SA
* Enable
* HP iLO

Benefits: Remove the risk of lateral movement through the enterprise via default or backdoor accounts. Provide a strong foundation to build a PAS program upon.

Recommendation: Utilize CyberArk integrations to protect high-value service accounts used for discovery/vulnerability management

* Vulnerability Management
  + QualysGuard
  + Rapid7
  + Tenable Nessus
  + McAfee Vulnerability Manager
* Discovery
  + Service-Now Discovery
  + HP Universal Discovery
  + ForeScout CounterAct

Benefits: Immediately protect high-value accounts that are frequently targeted in penetration tests *and* live attacks

Recommendation:Control and monitor all direct access to domain controllers

* Isolate credentials use and prevent credential theft with Privileged Session Manager
* Monitor behavior of privileged accounts on Domain Controllers with Privileged Threat Analytics
* Apply local Privilege Management and Application Control functionality for Domain Controllers and workstations for high-value users.

Benefits: Prevent the spread of malware from high-value workstations to domain controllers and prevent unknown applications from running on the most critical user desktops or directly on Domain Controllers.

## 4-6 months

Recommendation: Utilize CyberArk integrations to protect high-value database and cloud accounts

* Secure database accounts embedded in free text in XML files on application servers, such as WebSphere, JBOSS, Tomcat & WebLogic
* Secure sensitive cloud credentials (e.g. AWS secret access keys) embedded in free text in DevOps scripts

Benefits: Immediately protect high-value accounts that are frequently targeted in attacks

Recommendation: Establish credential boundaries in domain (e.g. dedicated accounts for Tier 0, Tier 1 & Tier 2)

* Identify and classify assets into tiers
* Create dedicated accounts for each tier, using role-based ID’s for administration
* PSM/PSMP/PTA/VF for Tier 1 assets

Benefits: Utilizing dedicated, role-based accounts via a jump server prevents the spread of malware from the workstation environment to the Tier 1 assets.

Recommendation: Utilize CyberArk integrations with malware analytics products.

* Check Point ThreatCloud Incident Response
* FireEye Threat Analytics Platform (TAP)
* Palo Alto WildFire

Benefits: Each of these products integrates with CyberArk Viewfinity for inspection and analysis of potentially malicious software in your environment. Viewfinity will identify suspicious applications and flag them for inspection by the relevant malware analytics product.

Recommendation: Define policies and procedures for newly created accounts in the environment

* What happens when a new service account is needed?
* What is the frequency in which a privileged account should be changed?
* Automate the provisioning of operating system accounts with existing CyberArk functionality.

Benefits:At this point we have addressed many of the most critical of accounts in the environment and it makes sense to spend the time determining the policies and procedures that are necessary to maintain a healthy environment of privileged accounts in the enterprise. The recommended approach is to have a demarcation line where any new accounts are immediately on boarded into CyberArk.

## 6-12 months

Recommendation:Continue to expand PAS program to Tier 2 assets

* Privilege management/ Application Control for workstations/tier 2 Windows servers
* Granular privilege control for Unix environment
* PSM for vendor access

Benefits: Expanding functionality to lower tier environments further solidifies the enterprise infrastructure from APT attacks that frequently begin at lower tiers. Centrally managing granular privilege in UNIX environments. Isolation and recording all vendor sessions into the environment thus mitigating preventing risk of attacks that begin with trusted vendor access.

## 12-24 months

Recommendation:Focus on high-risk service/application ID’s.

* Identify the top 10 – 20 existing accounts based on risk level.
* Work with application team to confirm all usages are accounted for.
* Define appropriate scope for service accounts, reducing privilege or splitting privilege into multiple lower risk accounts as needed.
* Application identity Management to replace hard-coded passwords or SSH Keys in application code or scripts.

Benefits: Managing the scope and applying frequent password changes to non-human accounts with the highest risk further enhances corporate security posture and minimizes the risks of PtH inherent with Windows operating systems. Applying Application Identity Management to your SDLC process prevents the inclusion of hard-coded credentials in code.