CYBERARK®

Roles & Responsibilities

Best Practices

Documentation Information

Document No.	CAUSPS0016
Document Type	Best Practices
Classification	Unrestricted (internal and all external)
Intended Audience	PAS Customers
Author	Kevin Naglich, Senior Security Advisor
Date Authored	8/26/15
Abstract	This document describes common support roles associated with successful CyberArk deployments. The purpose of the document is to provide customers with a representative sample of how to consider building their own CyberArk support team to ensure the best level of service and scalability as the Privileged Account Security program grows.

Revision History

Revision Number	Author	Revision Summary
201508-01	K. Naglich	Final Draft

Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Table of Contents

Description

As CyberArk deployments expand it is important to build a team around the product with a ‘program’ as opposed to ‘project’ mentality. This means that privileged account security should be seen as continually evolving and a persistant presence at an organization. To efficiently support that program it is important to structure the CyberArk team with long term growth in mind. Creating different roles as outlined in this document will allow customers to have highly specialized groups responsible for certain elements of the program which allows greater focus and a reduction in what can traditionally be a bottleneck in many deployments (i.e. vault administrators being tasked with everything thereby slowing down implementation).

Common Roles & Responsibilities

Role 1: Subject Matter Expert (SME)

The CyberArk SME is responsible for helping to design and architect all aspects and phases of the solution rollout. Whenever new projects arise in the organization, the SME can be utilized to help answer how CyberArk can be leveraged and map out the required steps. These SME's can/will be used to interact with your internal customers as they look to get onboard your Privileged Account Management initiative.

SMEs can be thought of as in house consultants which can be utilized in many situations including the following:

- New platform onboarding
    - Cisco devices, Oracle, etc.
- Safe design (Segregation of Duties)
- Onboarding additional modules
    - PSM, OPM, AIM

SMEs can be part time or dedicated resources depending on the level of activity in your organization. Typically for smaller or very new rollouts the SME role can be combined with the Vault Admin role.

Role 2: Vault Administrator

The Vault Administrators are responsible for maintaining the application layer of the CyberArk PIM Suite. Their activities will typically include:

- Ensuring full operability of the application
    - Ensure CPM is running, LDAP integration is configured, etc.
- Creation of policies as defined by Risk/Audit/IT Security
- Execution of project tasks defined by the SME in the design/architecture phase

The Vault Admins are the *executors* of your CyberArk support team and will work closely with the SMEs to understand and carry out any activities that arise as part of new organizational initiatives or onboarding of new CyberArk modules.

Vault Administrators can be part or full time employees and typically most organizations will have two such admins serving in a primary/backup configuration.

Role 3: Operations

The Operations role is responsible for the underlying OS and hardware that is supporting the CyberArk software. This team will ensure the hardware and OS is operating within specifications, monitor services, perform backup procedures, and help troubleshoot any infrastructure issues. This team will also be involved in any upgrades/migrations as well as any OS patching required throughout the lifespan of the tool.

This role will typically manifest itself as part of an existing SecOps or SecAdmin team in your organization and likely does not require full time dedicated resources.

Role 4: Data Administrator

The Data Administrator role exists to perform the more repetitive and day to day tasks involved in Administering the CyberArk solution. Activities can include things such as:

- Safe Creation
- Account/Password Uploads
- Application Definition (AIM)

This role operates in an inbox/outbox fashion where internal clients will submit requests to have activities to be performed (e.g. "I need a new safe for the Unix PCI Root accounts") and this team will fulfill those requests. They will not typically need to know or be involved in the overall strategy of the tool, but rather just carry out basic tasks.

Leveraging an existing team such as an Access Control Administrators group is usually a preferred method of implementing this role.