Scope of Work

Project Title:

HQ357_Privilege Access Management Systems

Project Location(s):

HQ Portland /Global

Background:

The cost of cyber-insurance for Mercy Corps (MC) has increased over the last three years, and last year many of our applications were rejected by insurance providers. Unrestricted local administrative rights were specifically noted as a reason for this rejection. Continuing use of this practice has made it difficult and expensive to obtain cyber-insurance.

For the purposes of this statement of work, the term "Project" means the acquisition, implementation, and establishment of initial maintenance procedures for a Privilege Access Management (PAM) system to mitigate the associated risks.

Mercy Corp is seeking a supplier that will implement and establish a Privilege Access Management System to mitigate risk.

Purpose / Project Description:

The project will seek to remove these elevated rights, yet still allow users to perform necessary tasks safely on their computers, by using a Privilege Access Management (PAM) system. The PAM system will help protect against cyberthreats by exerting control over and monitoring the elevated ("privileged") access and permissions for users, accounts, processes, and systems across an IT environment. The PAM system will control, monitor and act on the user's behalf to perform high security tasks such as software installation.

Once implemented, a PAM administrator will use the PAM portal to define methods to access the privileged accounts across various applications and enterprise resources. The credentials of privileged accounts (such as their passwords) will be stored in a special-purpose and highly secure password vault that is deeply integrated into the PAM system. The PAM administrator will use the PAM portal to define the policies of who can assume access to these privileged accounts and under what conditions. Privileged users will log in through the PAM and request privileged access, or immediately assume access to the privilege's user account, depending on context and case. This access will be logged and remain temporary for the exclusive performance of specific tasks. To ensure security, the PAM user should be asked to provide a business justification for using the account. The user shouldn't be granted access to the actual passwords used to log into the applications but instead be provided access via the PAM. Additionally, the PAM will ensure that passwords frequently change, ideally automatically, either at regular intervals or after each use. The PAM administrator should be able to monitor user activities through the PAM portal and even manage live sessions in real time, if needed.

Objectives:

The objective of the Project is to acquire, implement, and establish the maintenance of a Privilege Access Management (PAM) system that meets the minimum requirements as established in the Project Charter.

Deliverables:

- Preparation of PAM implementation plan based on chosen vendor's solution and identification of current system gaps.

Scope of Work

Vendor / Solution Requirements:

- The PAM System must be able to standardize all endpoint users to a set of configurable, minimal, standard privileges.
    - This should include restrictions on software installation, usage, and OS configuration changes.
    - This should include the ability to allow users to add printers and other peripheral devices.
- The PAM System must automatically manage the routine privilege escalations of users who require privileged access to carry out specific tasks or use specific applications.
- The user should be able to inject credentials directly with the PAM System.
    - The user should never have to manually type administrative credentials.
    - The PAM System should be able to supply this functionality without displaying the privileged credentials to the user.
- The PAM System should allow an endpoint user to submit a reason / business case when requesting non-routine temporary elevated access.
- The PAM system must tie into our existing SSO (Single-Sign On) technologies (Okta) and not require a separate log-in.
    - If the PAM system must become the initial log-in due to its design, it must allow Team Members to use MFA (Multi Factor Authentication).
- The end-user user interface must be intuitive and easy to use to best facilitate user adoption and mitigate workaround attempts.
- Passwords and secrets (passwords) on the local workstation should be rotated. Rotation should be able to be automatic, scheduled, and based on use.
- Password policies should be enforced by the PAM system, as it handles the rotation of the passwords, and governs aspects of passwords such as complexity, uniqueness, expiration, and the elimination of default passwords.
- Passwords must be securely stored and encrypted in a tamper-resistant safe/vault.
- The PAM System should passively track and analyze user behavior by collecting, storing, and indexing application use, session recordings, and other privileged events.
- The PAM System should be able to terminate or suspend any privileged account sessions that are deemed to be suspicious either automatically or upon review.
    - If a privileged account session is deemed suspicious, the PAM system should enable a rapid orchestration of security responses to stop or mitigate the detected threats.
- The PAM System must be able to be centrally administered / managed for policies, passwords, sessions, reporting, auditing, etc.
- The access control provided by the PAM System must be granular.
    - There is a need to be able to target groups and users.
    - There should be an ability to allow exceptions to existing policies.
- The PAM System must provide the ability to implement trust-based application whitelisting, with the flexibility to set both broad and granular rules.
- The PAM System must not require any additional third-party tools or potentially dangerous dependencies and should instead utilize native tools (example: MSTSC, PuTTY) and standard protocols for connections (example: RDP, HTTP/S, SSH, SAML, RADIUS) instead.
- The PAM System should include the ability to push agent updates to endpoints.
- The PAM System should be able to manage credentials across various platforms.
    - This must include Windows and Mac devices.
    - This must include cloud and web application credentials.
    - This would ideally include network and other devices such as Firewalls.
- The PAM System should allow flexible deployment options.
    - Hardware appliances
    - Virtual appliances

  - Software.
- The deployment should be agent-based and be able to be included in a system image for an image-based deployment to endpoints.
- Strong Reporting Capabilities
  - How privileged credentials are being used.
  - Privileged session activity.
- Strong Auditing Capabilities.
  - Track any changes to critical policy, system, application, and data files.
  - Unauthorized action attempts including detected workarounds.
- The PAM System cannot rely exclusively on, or even primarily, Active Directory alone. Mercy Corps does not utilize on-premises Active Directory.

Timeframe / Schedule: February 2023 – June 2023

Evaluation:

An evaluation will be done by checking responsiveness to our requirements (proposals) and a follow up interview for a demo from the shortlisted firms.

Payment Schedule:

Ensure to add a payment scheme to your proposal.

The vendor will be managed by: Errol Sigler, Senior Director – Global Infrastructure and Support

The vendor will work closely with: Errol Sigler, Amber Lovell, Brian Arthur, Jesus Ruiz, Jerry Kessler