Privileged Identity Management Best Practices

Abstract

The threat landscape today requires continuous monitoring of risks – be it industrial espionage, cybercrime, cyber-attacks, Advanced Persistent Threat (APT), Ongoing Targeted Attacks and cyber-warfare - the terminology is irrelevant. Add to this the fact that trusted insiders (such as IT administrators) have access to both highly sensitive information and mission-critical resources. Accidental (or deliberate) misuse of a shared credential leads to a breach, and the compromised credential is abused either by insiders, disgruntled employees or cybercriminals.

The field of security that deals with this exact problem, called Privileged Identity Management (PIM), has been around for some time now. Some IT executives have a tough time working out a plan of action, figuring out what to look for in potential solution. This paper aims at collating PIM best practices in a single space for ease-of-access and reference. The paper is targeted at IT decision makers and security personnel and intends to share some of the industry best practices for PIM solutions.

Let us briefly introduce PIM solutions

Almost regularly now, we keep hearing news about data breaches and compromised IT systems of organizations or government agencies. It seems no one, big or small, state or corporate, is beyond reach. It has been identified that some 83% of these cases are because of the malice or ignorance of privileged insiders. PIM systems exist to fill exactly this niche within a company's security infrastructure. PIM solutions are employed to

- Secure, manage and track privileged accounts
- Isolate, control and monitor privileged sessions
- Report business as usual and alert on deviations

On any device in the datacenter – hosted, on premise, managed, or in the cloud – of your complete IT infrastructure.

But despite all this, we are yet to see mass adoption of PIM solution within the industry. The ones who are already doing it are touted as progressive. Also, there is limited differentiation between PIM and Identity Access Management (IAM) solutions. IAM solutions generally don't provide PIM capabilities, as privileged identities are associated with software and hardware assets, not with the individual user identities controlled by IAM. PIM solutions monitor, secure, and audit privileged credentials used by administrators, computer services, and applications for accessing sensitive information and computing resources.

In this paper we aim to provide a one-stop access to the information needed for PIM deployments. We'll try to touch on all the PIM best practices possible by giving the reasoning behind them.

What is the objective of implementing a PIM solution?

The PIM solutions objective is to create a continuous cycle that can be represented in four phases:

- Isolate and record all critical IT assets, their privileged accounts and interdependencies wherever present on any hardware or software platform.
- Assign access to only appropriate personnel, using least privilege required, with documented purpose, so that the credentials can be used to login to IT assets in a timely manner at designate times
- Enforce rules for password complexity, diversity, and change frequency, synchronizing changes across all dependencies to prevent service disruptions.
- Audit and report so that the requester, purpose, and duration of each privileged access request is documented. Alerts can also be configured for management to be aware of unusual events.

What are the best practices?

Whether getting started on PIM, or upgrading existing implementations, it's best to work with a checklist. Based on industry experiences and case studies, the following are recommended as key incorporations of best practices.

1. Isolate and record -
   key systems, application and databases, and the privileged account(s) that exist in each one. An itemized list would help better organize the complex IT infrastructure landscape of the modern data center. Also,this step needs to be incorporated into the ongoing (de)provisioning processes for all assets. This keeps the list updated as a single source of truth.

2. Prepare the existing setup -
   Correct any improperly conceived account names and assignments. With a list from the earlier step, this is pretty easy to identify. For example, ensure that every database service account is assigned a different domain login to release credentials with limited scope.

3. Avoid the mistake of simply automating poor prior practices -
   This is very dangerous trap, and must be avoided at all costs. If privileged users end up sharing their unique credentials and using the system as an automated session and password manager, it defeats the whole idea of PIM.

4. **Classify who should have access to these accounts -**
   With a list of all assets and their privileged accounts compiled, which can be cross-referenced again roles & responsibilities of admins, this is the easy part.

5. **Uncover who does have access to these accounts-**
   This is the hard part as disclosure of unauthorized access is scary for employees. One way to get around this is to grant a one-time free pass to everyone when asking for this information. Another is to change privileged passwords in a phased manner, notifying all to approach the PIM team for further access.

6. **Enforce Privileged Account Lifecycle Process –**
   Privileged account creation, modification and deletion should be entertained via well-established process. As far as possible the system should be automated to handle any such request post necessary approvals. It's a good practice to create privileged account with a predefined expiry period where such accounts are created for ad-hoc work.

7. **Use templates for permissions –**
   Create user groups and define permissions for the group. While on-boarding an individual (s)he should be mapped to appropriate group. This way individuals will be provided only those permissions which are absolutely required for them.

8. **Outline policies for privileged access to key systems –**
   Ensure the policies are designed to be:
   a. As specific as possible (time- bound access, dual-Control authorization, password modifications)
   b. As granular as possible (down to session and command level policies)

9. **Default to Least Privilege -**
   This saves from disclosing logins that have broad, elevated permission to make changes across the enterprise. Same holds true with all other types of privileged accounts; better governance involves organizing these credentials to limit the scope of access.

10. **Multi-Factor Authentication (MFA) for Privileged users –**
    Implement MFA for the privileged users who require access to the sensitive data /resources. Such processes will require user to provide additional authentication (Like randomly generated token or One Time Password) along with their normal credentials.

11. **Explicit Authorization –**
    Any access to the critical resource or data should be explicitly authorized.It should not be the case that by only authenticating self to any application user gains unrestricted access to all the underlying components.

12. Automatic Policy Enforcement - Employ processes to apply policy definitions automatically. This can be done manual by the IT department based on regular audits, or automated with the help of dedicated managed services.

13. Record and Audit – Organizations should record/log all the user activities for the privileged accesses and plan for a regular audit. This not only creates a sense of accountability across the users but also help faster investigations of any breaches.

14. Monitor and Alert – Last but not the least, proactive monitoring of the activities help to protect from any intentional or unintentional unauthorized access. Such findings should then be immediately propagated to concerned team as alerts.

So how will you benefit by implementing a PIM solution?

The obvious (and some not so obvious) values of a PIM solution are mostly appreciable in its absence. It's usually the case after a breach, when the security policies are under scrutiny that we remember how some action in the past might have prevented the incident. Fortunately, like the best practices, here is a list of the advantages of a PIM deployment. Some of these benefits are quantifiable, some not, but they are definitely common to properly deployed PIM solutions across the board.

benefit	...which means
policy based restriction	Full audit trail and accountability of the actual operators
monitor and audit activity	view activity and define policies and workflows (via an interface - web, or thin client) session recording - for compliance and regulatory purposes.
business continuity	Secure password versioning (in case of loss or break-ins)
limited investment	integrate with existing IT authentication systems (in cloud or on-premise)
compliances	Legal and Regulatory Compliance

Conclusion

As IT auditors become more aware of the threats posed by unmanaged privileged identities, your organization could face increasing pressures to bring these powerful logins under control. Hackers have also taken notice, increasing the frequency of attacks that exploit shared, elevated credentials to gain control of victim organizations networks.

Fortunately, privileged identity management software can help you continuously secure privileged credentials throughout your network and provide an authoritative audit trail of their access. A successful implementation can also save IT staff time by providing login credentials instantly and on-demand, reducing the need for manual processes to discover, change, and document the accounts.

About ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched inidentifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.