DATASHEET

Osirium PAM POC Plan

Privileged Access Management Proof of Concept Plan

OSIRIUM PAM

r8.0.3

Contents

1 Introduction and Purpose

The Osirium PAM Proof of Concept (POC) allows organisation to test Osirium PAM in their own environment.

The primary purpose of Osirium PAM is to control access to devices using privileged credentials. Osirium PAM's main features are listed below. The checkbox can be selected for those relevant to your environment. Specific use cases can be detailed if required.

- ☐ Manage credentials of Local Admins across Windows Servers and/or Unix Servers.
- ☐ Manage credentials of Domain Administrator accounts.
- ☐ Manage credentials of Network infrastructure accounts, on devices such as routers, switches and firewalls.
- ☐ Manage credentials of databases and other applications such as HR, marketing and Payroll systems.
- ☐ Proxy and record sessions established by privileged accounts.
- ☐ Grant access to management tools to control access, such as ADUC, GPO and DSA. Etc MMC connections.
- ☐ Management of Tasks that require a specific level of privilege for Windows, EG, reset Domain Account passwords, lock Domain accounts, etc.
- ☐ Management of Tasks that require a specific level of privilege for Network devices, e.g., opening ports, flushing arp cache.
- ☐ Management of other service desk level tasks.
- ☐ Control and monitor access by external and/or 3rd party and/or contractor access.

The purpose of this document is to record the work carried out during the POC, which will have been scoped during pre-POC calls.

Before the start of the POC, the primary contact will need to review the POC objectives and complete the POC scope of objectives table.

Weekly cadence calls will be scheduled to track POC progress. The typical duration of a POC is 30 days, and Osirium will provide regular knowledge transfer to onsite staff during the POC.

2 POC Objectives

The below table documents the list of deliverables that will be configured and proved over the duration of the POC.

2.1 Day One Activities

No.	Activity	Outcome	Applicable	Tick
1	Install PAM Server.	PAM Server successfully installed on an on-premise or cloud platform.	☐	☐
2	(Optional) Install PAM UI Server.	PAM UI server successfully installed on an on-premise or cloud platform.	☐	☐
3	Install MAP Server.	MAP Server software installed successfully on an on-premise or cloud platform and integrated with the PAM Server.	☐	☐
4	Osirium PAM with Active Directory (AD).	a) Provision an AD in Osirium PAM using LDAPS to connect to a/some Domain Controllers.	☐	☐
		b) Osirium PAM will create an OU of which to store accounts into, unless previously specified and created.	☐	☐
		c) Specify a 'Group of Interest' to demonstrate that Osirium PAM can discover privileged accounts in AD.	☐	☐
		d) Provision users with AD authentication and optional configure 'inbound' AD user groups to sync members from.	☐	☐
5	Osirium PAM can integrate with Two Factor authentication systems.	Users successfully able to authenticate to Osirium PAM with a RADIUS challenge.	☐	☐
6	Onboard target devices into Osirium PAM and add them to a Profile with the Users.	Within the PAM UI, search the granted list of devices on keyword, hostname, or IPs to find them.	☐	☐
7	Osirium PAM provides Privileged Session Management (PSM) access to Windows servers using Remote Desktop (RDP), and recording the session.	Within the PAM UI, launch a PSM RDP session to a Windows server using Remote Desktop. Notice the session recording within the browser tab.	☒	☐

8	Osirium PAM provides Privileged Session Management (PSM) access to Linux/Unix/Networking servers using SSH and recording the session.	Within the PAM UI, launch a PSM SSH session to a Linux/Unix/Networking device using SSH. Notice the session recording within the browser tab.	☐	☐
9	Osirium PAM can automate tasks to provide a least privileged model.	Within the PAM UI, the Users can run some privileged tasks on the target devices. Tasks communicate over WinRM or SSH.	☐	☐
10	Osirium PAM can rotate credentials of target accounts.	A test account within AD has been discovered by Osirium PAM through Group of Interest membership and password rotated after 'Refresh Account Credentials' has been selected on the account.	☐	☐
11	Osirium PAM provides a detailed audit trail of all device connections.	Show the device access report. Review searching and filtering by keystroke, date, user, device etc. Session shadowing should also be reviewed.	☐	☐

2.2 Day Two Activities

No.	Activity	Outcome	Applicable	Tick
12	Osirium PAM allows users to PSM to web browser-based applications.	Provision a device to a browser-based template. Add to a profile. User should access web application from PAM UI.	☐	☐
13	Osirium PAM allows users to PSM to thick client management applications.	Provision a device to a thick client-based template. Add to a profile. User should access thick client from PAM UI.	☐	☐
14	Osirium PAM can provide mapped connections to target devices if a secondary, named Domain Admin account model is used.	Configure an account mapping appended with the appropriate account naming convention, e.g., %accountusername%_adm users can then access devices with the mapped account providing the account is Known by Osirium PAM and access configured in a profile.	☐	☐
15	Run a backup of Osirium PAM.	Run the backup task against Osirium PAM device and download the file. Automatic backups can also be configured.	☐	☐

16	[Amend/add use cases as required] Client requested use case number 1.	TBD	☐	☐
17	[Amend/add use cases as required] Client requested use case number 2.	TBD	☐	☐

3 Contact Information

Contact details of the staff involved are below;

Role	Name	Title	Contact Number	Email
Osirium Support	https://osirium.com/register	Osirium Support	0118 324 2442	supportdesk@osirium.com
Osirium Pre-Sales Technical	<Osirium SE>			
Osirium Commercial Contact	<Osirium AE>			
Company POC Contact	<Company> contact			

4 Timelines

Date	Event	Location
	Day one activities	Customer site
	Day two activities & fill out POC deployment acceptance	Remote or customer site
	Cadence call 1	Remote
	Cadence call 2	Remote
	Cadence call 3	Remote
	Cadence call 4, POC close + fill out POC success table	Remote

5 POC Progress Summary

5.1 POC Deployment Summary

To be completed after successful POC installation.

POC Deployment Summary	
Contact Name	
Date	
Comments and Feedback	

5.2 POC Use Case Success

To be completed at end of POC.

Use Case Success	
Contact Name	
Date	
Comments and Feedback	

6 Ensuring a Trouble-Free POC

Osirium PAM is lightweight and quick to deploy. To ensure a successful POC, we recommend the following pre-requisites are met.

- Access for the Osirium engineer to environment where the installation will take place.
- The availability of a supported virtual platform, and access to a member of staff with permissions to install the virtual appliances (Using VHD or OVA files).
- An Osirium Support account should be requested from here prior to the POC. This will allow downloading of the necessary Osirium PAM software.
- The availability of network and Active Directory support staff, in the event of any unexpected local environment issues.
- No more than 10 target servers and/or devices to test with during the POC. Device connection details and credentials must be available.
- Groups of users for testing if required.
- All other requirements as per the Osirium PAM System Requirements Guide.