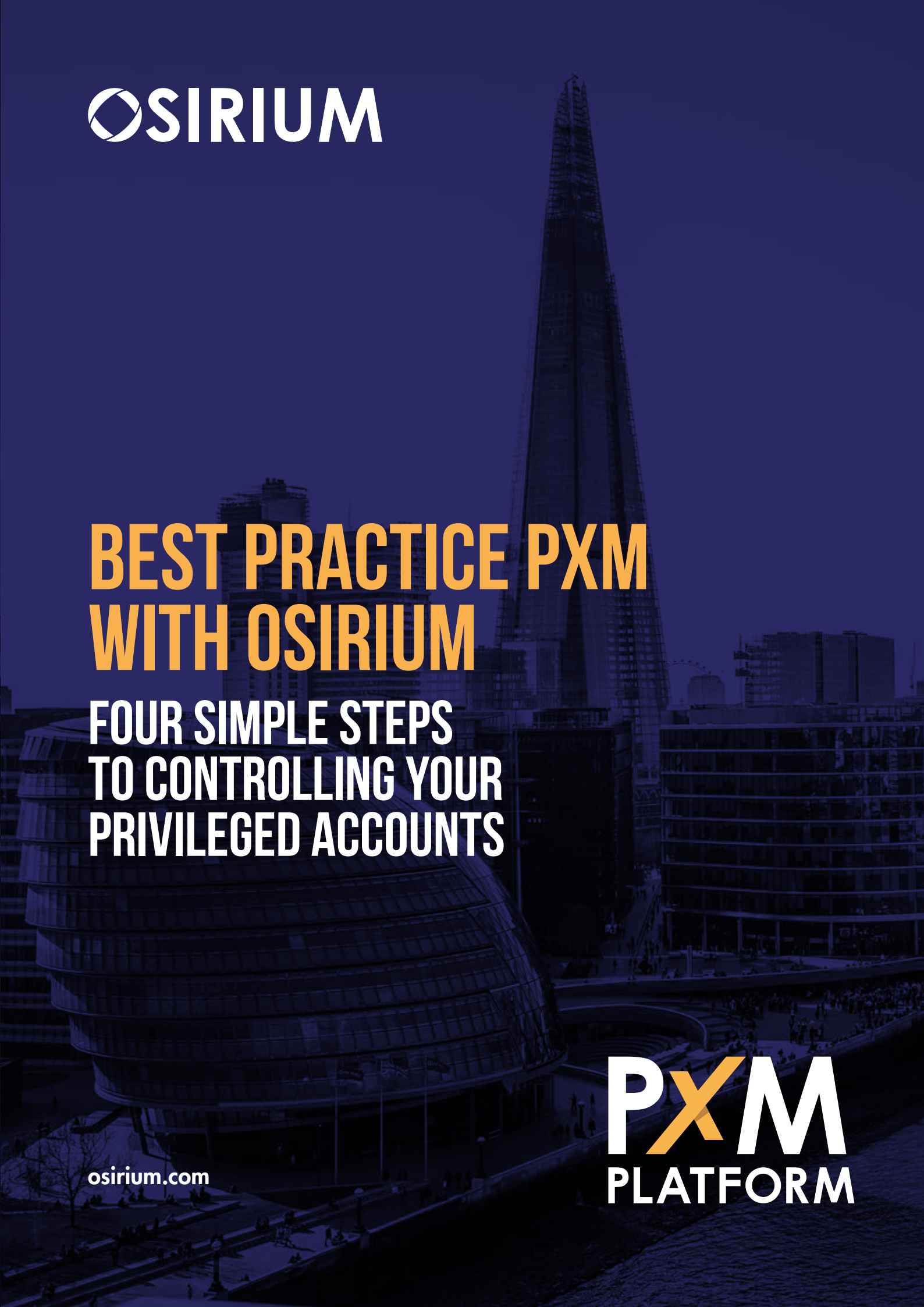
OSIRIUM

BEST PRACTICE PXM WITH OSIRIUM

FOUR SIMPLE STEPS TO CONTROLLING YOUR PRIVILEGED ACCOUNTS



osirium.com

PXM PLATFORM

BEST PRACTICE PXM WITH OSIRIUM

Four Simple Steps to Controlling Your Privileged Accounts

OSIRIUM

INTRODUCTION

PxM is the embodiment of just in time least privileged security models.
This paper discusses how to implement these using Osirium's PxM Platform.

AN OVERVIEW OF OSIRIUM'S SOLUTION TO PRIVILEGED ACCESS MANAGEMENT

PxM is the embodiment of just in time least privileged security models.
This paper discusses how to implement these using Osirium's PxM Platform.

Step 1: Reduce

Reducing the number of privileged accounts you have across your IT estate will significantly reduce your attack surface. It also makes it much easier to reason about what security you have where.

Although it may fly in the face of conventional wisdom, here we're going to suggest that removing personalised privileged accounts is a good idea. As an aside, Osirium's PxM Platform is great at dealing with the life-cycle of personalised privileged accounts, it can create and remove these on demand. With account mapping it can take over existing personalised privileged accounts. However, the PxM Platform's profiles and logging schemes mean that is it perfectly acceptable to have many users going through the same privileged account with full accountability. Here are the simple steps...

- Use Osirium's PxM Platform to gain control of your existing personalised privileged accounts
- Work out what roles are needed for each system (dealing with those that represent the most risk first)
- Create one account for each of the roles
- Determine which users need which roles
- Place those users in Profiles with the right role based accounts for the devices
- Use the PxM Platform to bulk disable the personalised privileged accounts (thus significantly reducing the attack surface)
- Wait for errata, those odd requirements that were never documented
- Iterate the above
- Use the PxM Platform to bulk delete personalised privileged accounts.

At this stage you have the least number of privileged accounts required to operate the system and a fully accountable mapping of who can use which role and when.

Step 2: Task automation

If you can remove a users access to a privileged account the attack surface reduces again. In particular the inside threat is reduced along with the probability of human error. Here are the simple steps...

- Determine the most common operations on any system, or even across systems of a similar type
- Build these tasks into the PxM Platform, this is most likely a case of modifying existing tasks in the Osirium Template Library
- Add these tasks to the profiles in the Reduce section (step 1).

At this stage you have reduced to a minimum the number of users able to engage in privileged sessions on systems. You have therefore also reduced the possibility of human error to a minimum. This is the stage that really drives business value. By deploying tasks you can get things done faster, more accurately and delegate to the level most connected to the need in the first place.

Step 3: Session management

Now that we have reduced the number of sign-on sessions to systems we will have reduced the volume of sessions that we need to record. For example you could decide that 'read-only' sessions need not be recorded. If you can reduce the data set to only the sessions that represent risk or learning you've made it easier to reason across this data. Here are the simple steps...

- Evaluate your profiles, would the sessions going through these profiles represent risk or the opportunity to learn. Third party sessions on your systems would be a great example of both. They are inherently risky and there's always a reason that you asked a third party to look at an issue
- Periodically review your Privileged Behaviour Management (PBM) reports for signs of risk building.

At this stage you have all your accounts under control, you've built workflow that benefits business operations and you're now feeding data into automated risk analysis.

Step 4: Iteration

When we analyse data breaches, we find three scenarios:

- The front door was open, they virtually walked in, filled their disks and sat waiting for more. 86% of passwords are stolen at the desktop and a further 10% are phished from unwitting employees
- The front door had a complex lock with a flaw. They knew the flaw and used it to compromise a privileged account
- The system compromised had a trust relationship with a lower system or series of systems. These systems were easier to compromise and were used as a route to the valuable data.

Therefore, you should go back to step 1 and work your way through your IT estate to create security cells.

At this stage you're a very comfortable and accomplished CISO. You can reason about all the security in your organisation. When the inevitable complex attack happens you'll see it quicker and know exactly how far it can travel and just what to remediate. Osirium's PxM Platform makes all this possible.

About Osirium

Osirium is a UK software development team that has pioneered the concept of a virtual air gap for privileged account access. The team have delivered a virtual appliance that can recognise an incoming identity, create a connection to a system, device or application, perform single sign-on and enterprise class password life cycle management, and then hand the pre-prepared session back to the incoming request ready for system management.

The session can be recorded, subject to time windows and device group separation. Osirium has delivered millions of privileged tasks and sessions for many of our blue chip clients. Osirium currently has four patents pending.

NOTES

OSIRIUM

11-13 High Street, Theale
Reading RG7 5AH

0118 324 2444
osirium.com