PBM

Privileged Behaviour Management

See at a glance which users are the most suspicious and take appropriate action. Changes in behaviour, especially in privileged users, are flagged so that you can quickly narrow down a search for suspicious activity. Easily see which users are using the devices they have been assigned and remove any that are no longer needed, remove the damage that a rouge employee or cyber hacker can do.

ADAPTIVE PREEMPTIVE THREAT DETECTION

Statistical analyses create a series of behavioural baselines for users.

- User behaviour can be automatically categorised.
- Through the PxM Platform's use of profiles, other users are treated as behavioural peers.
- Behaviours that are considered abnormal are preemptively flagged and reported.

REAL-TIME MONITORING & INTERACTIVE ANALYSES

Montior user activities as they happen, whenever they happen.

- Fully integrated metrics and reporting system - visualise correlations in user tendencies in real-time.
- Automatically produce comprehensive data sets in a variety of user-friendly formats.

INTELLIGENTLY ASSIGNED RISK SCORES

Privileged users gain risk scores reflecting behavioural baselines.

- SysAdmins can then use these scores to prioritise and address security risks.
- Deprovision over-privileged users that have been granted legacy access rights.
- Remove any ambiguity surrounding access rights.

USE PAST DATA TO MANAGE FUTURE RISK

Correlate privileged user data - preemptively display clear cases of exposed risks to infrastructure.

- Give users the access rights that fit their use patterns - never under-privilege, never over-privilege.
- Baselines constantly adapt and update to mirror user patterns.

ADAPTIVE THREAT PROFILE BASED ON LOGIN ADDRESS

The PxM Platform creates a use profile for each privileged user in your organisation.

- Visualise whenever a user's access address differs from preexisting baselines.
- The more frequently a user logs in from a given address, the lower their suspicion becomes.

IDENTIFY LATENT THREAT WITHIN YOUR ORGANISATION

Privilege-creep arises through users gaining privileges in excess of their requirements.

- Identify and prevent latent threat within your organisation.
- Provision and deprovision users flexibly, give them access to what they need, when they need it.

WHAT IS PRIVILEGED BEHAVIOUR MANAGEMENT?

Because Osirium's PxM Platform maps identities to roles, it already goes a long way in delivering 'Active Compliance'. This means that we can automatically close the loop between audit and action.

Within the PxM Platform's UI it's easy to visualise the accounts that already exist on systems, not just Windows and Linux but a wide range of systems, applications and devices - for example Cisco switches, storage area networks and mobiles. The identities (i.e the users) that can be mapped into roles. The relationships between the users, the roles and systems that they can use along with the time windows and the status of session recordings.

Delivering a consistent, irrefutable audit trail is undeniably invaluable, but what if could use this data to predict potential wrongdoing before it even occurs?

ACTIVE THREAT VS. LATENT RISK

The PxM Platform's Privileged Behaviour Management (PBM) capability brings a depth of analytical features to an IT infrastructure, the most important being predicting unusual behaviour by privileged users.

Privileged Behaviour Management is machine learning that creates a series of baselines against which privileged user actions are measured. With PBM, a user's posture is about when and where they execute tasks and interactive sessions. PBM learns each privileged user "baseline" alongside their peers. Simply put, if a privileged user does roughly the same as their peers, their risk profile diminishes.

Our PxM platform creates user profiles that define which tools and tasks privileged users can access on which systems or devices. Therefore, a privileged user that starts to do something out of the ordinary gains a higher threat profile based on their unusual behaviour.

INFRASTRUCTURE & SYSTEM REQUIREMENTS (PXM PLATFORM)

Virtualisation:	VMware 5 through 6, Xen, Hyper-V, Azure, AWS.
Osirium appliance allocations:	IP Address, 40GB storage, 2 x CPU cores, 8GB RAM.
Desktop Client Requirements:	Microsoft Windows & Microsoft .NET Framework v4.5.2 / macOS 10.9 or later
Minimum Browser & Plugins:	Internet Explorer 10 / Chrome 50