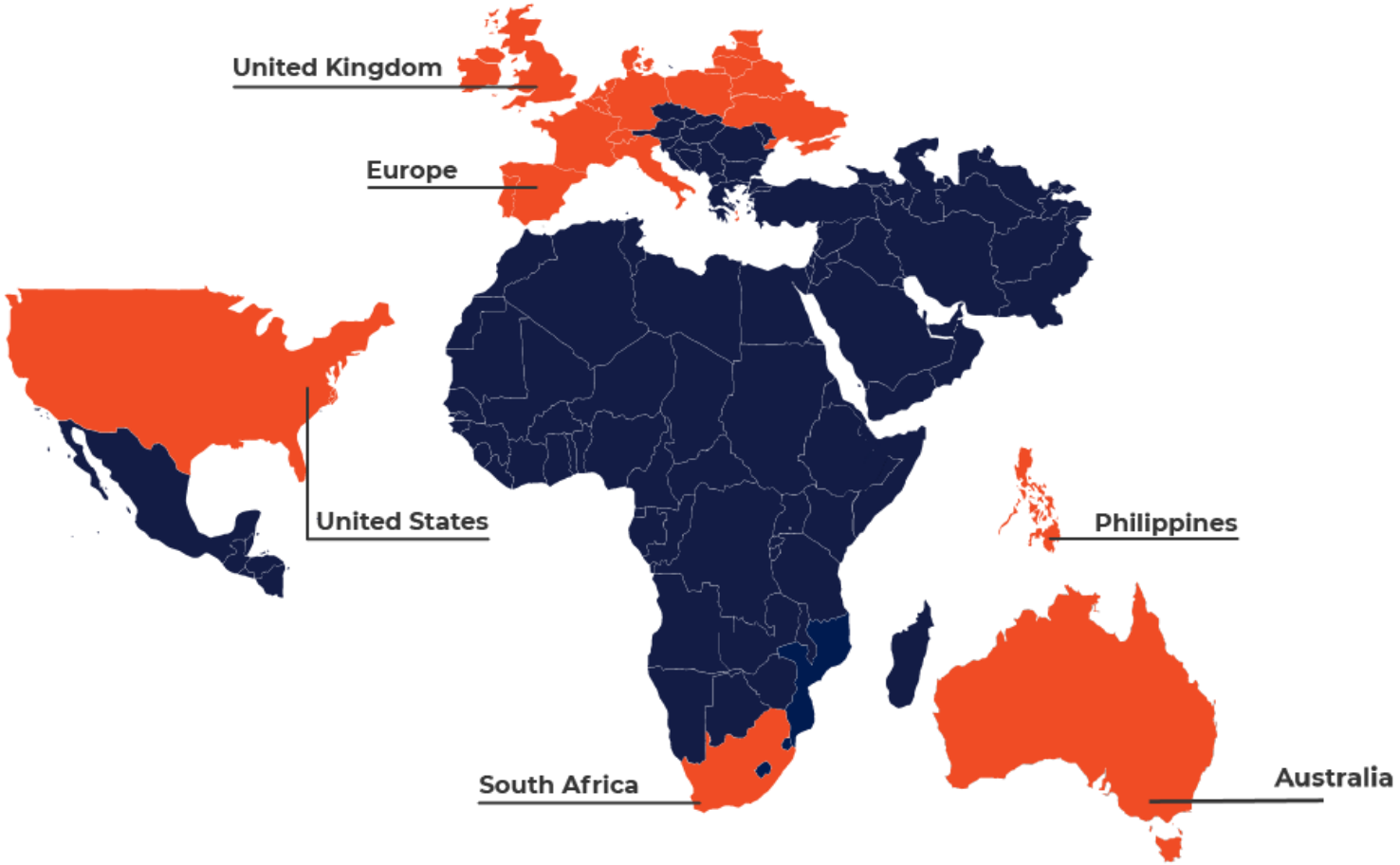
CyberIAM

G-Cloud-15
CyberIAM Advisory Services

Where Are We Based

About CyberIAM

CyberIAM was founded in 2017. We are
a leading Managed Cybersecurity Services company.
We have the industry's top Access, Identity and Privileged Management Experts across our vendor partner's market-leading technologies. From advisory services to Professional Services to support, we can assist you wherever your business is, on your identity journey.



What We Do

Our Services

Advisory Services

Our business consulting services take care of strategy, architecture, solution delivery and development for a range of both bespoke and vendor products.

Professional Services

We offer a team of highly trained professionals to manage and run your project as part of our Professional Services offering.

Managed Services

CyberIAM Managed Services help run and manage your BAU identity implementation beyond project completion. Our team of highly skilled experts will maintain your Identity Platform.

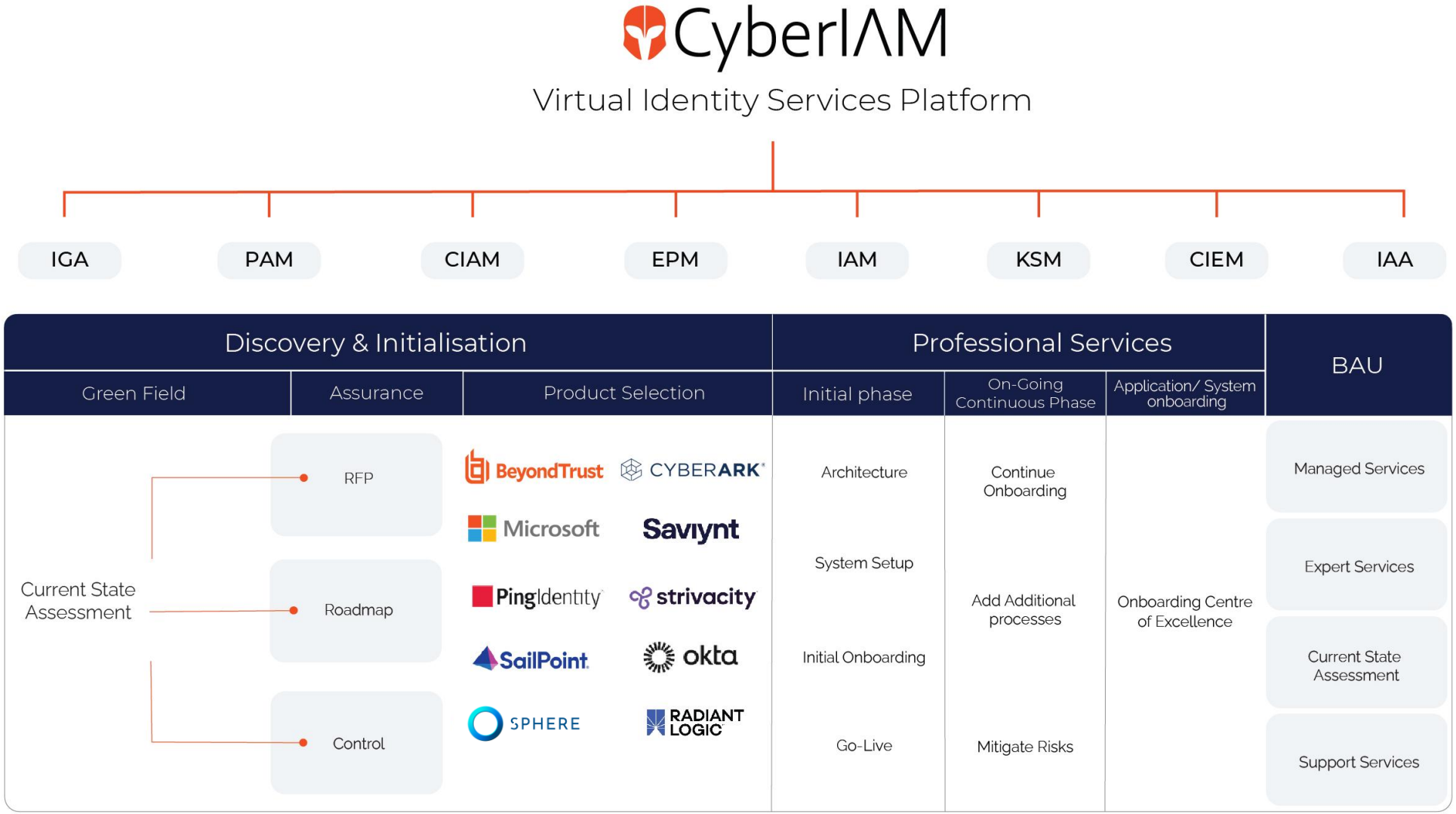
Support Services

Our support packages provide a pool of hours delivered by our skilled engineers to assist your team with resolving any bugs and issues.

Expert Services

Our Expert Services are an insurance policy beyond project completion, we provide service hours that can be drawn on to assist with business-as-usual (BAU) tasks.

Virtual Identity



Advisory Service

We offer Advisory Services to guide you, wherever you are on your Identity journey. Whether greenfield or experienced, we can advise you on a multitude of things including best practices and which software vendors are best for your business needs, using our highly trained experts.

Benefits:

- We are vendor agnostic which means we help you select the best solution based on your business needs.

- We boast a team of highly skilled IAM and PAM experts with extensive years of experience and vendor training. They are here to expertly guide you and provide well-informed solution proposals tailored to your infrastructure.

- With experience working across various vendors, our advisory services can help you optimise your investment with the best solution.

Why CyberIAM

What we do

- CyberIAM offers specialised expertise in the design and implementation of sophisticated identity and access management systems
- Our approach integrates both technical and business acumen for each project, recognising that successful outcomes require addressing both technological and business needs
- We employ a technology-agnostic strategy, leveraging partnerships with leading IAM and PAM vendors as recommended by industry analysts
- Our delivery methodology prioritises long-term collaboration with clients, encompassing strategic advisory services and comprehensive hands-on technical implementation

Our Differentiators

- **Specialised focus**: Exclusive dedication to IAM, PAM, and CIAM solutions
- **Flexible engagement models**: Adaptable to client's specific requirements and budget constraints
- **Proven track record**: Demonstrated success in managing enterprise IAM and PAM deployments
- **Local presence**: In-depth understanding of global markets, enabling us to provide localised support and services
- **Commitment**: Our technical consultants work together with our business consultants to ensure successful project outcomes

Our Experience

130+ successful deployments

Rich and in-depth experience & knowledge of the vendor and products

Consultants are dual trained in both IAM and PAM technologies

We grow our consultant's knowledge using our own graduate program

Always aligning with best practices to ensure top-tier delivery for customers

Small to large projects from new installs to managing environment

Certification & Awards

Certifications

SailPoint

346+

SailPoint courses completed by CyberIAM Employees

12 SailPoint Engineer Certifications	**2** SailPoint Architect Certifications

14

Total Certifications

BeyondTrust

17 BeyondTrust Password Safe Certifications	**6** BeyondTrust Advanced Password Safe Certifications
13 BeyondTrust Privileged Remote Access Certifications	**2** BeyondTrust Advanced Privileged Remote Access Certifications
3 BeyondTrust Remote Support Certifications	**2** BeyondTrust Advanced Remote Support Certifications

CYBERARK

303+

CyberArk Certifications Acquired by CyberIAM Employees

23 CyberArk Defender Certifications	**15** CyberArk Sentry Certifications
5 CyberArk Guardian Certifications	**14** Privileged Cloud Delivery Engineers

Joint 2nd in EMEA and Joint 3rd Globally for Guardians outside of CyberArk

CyberIAM Partner Awards

Delivery Admiral- Software

Fulfilling the award criteria means that we had over 3 successful new deployments and vastly surpassed the minimum certified IdentityNow engineers and professionals and IdentityIQ engineers and architects. Admiral Top Delivery Partners must also maintain a very high standard of customer satisfaction.

Delivery Admiral- SaaS

To achieve this, we successfully carried out 4 new deployments, acquired 4 certified IdentityNow engineers and secured 2 certified IdentityIQ architects.

CyberArk Advanced Partner

This is a notable step, reflecting substantial investment and commitment in obtaining valuable and demonstrable skills in the Privileged Access Management discipline.

CyberArk EMEA Services Delivery Partner of the year

CyberArk, has awarded us with the EMEA Services Delivery Partner of the Year award! This comes as we always go above and beyond to ensure customers deploy, utilise and maximise CyberArk's platform.

CyberIAM Partner Awards

BeyondTrust's EMEA 2024 Ecosystem Partner of the Year Award

This award highlights the partners who have fully integrated into the BeyondTrust partner ecosystem and contribute consistently to its growth and success. It holds substantial significance for our company by validating our expertise, enhancing our reputation, and motivating us to excel. It affirms our proficiency in implementing BeyondTrust's solutions to address the complex identity access challenges faced by organizations across the EMEA region. This recognition solidifies our status as a trusted advisor and solutions provider in the identity space. Being recognised as the EMEA 2024 Ecosystem Partner of the Year serves as a testament to our capabilities and strengthens our position as a preferred partner for organisations seeking identity solutions and services. It inspires us to continue striving for excellence and innovation in all our endeavours.

Accredited Certification to ISO 27001:2013

ISO/IEC 27001:2013 Information Security Management System.

CyberIAM, multi-award-winning, implementation partner of leading IAM and PAM vendors, has obtained the Accredited Certification for Information Security Management System ISO 27001:2013. Being accredited by the International Organisation for Standardisation (ISO) is a result of CyberIAM's commitment to offering our clients market-leading solutions that are delivered by world class consultants.

PERRY JOHNSON REGISTRARS, INC.

UKAS MANAGEMENT SYSTEMS 0105

CYBER ESSENTIALS CERTIFIED

CyberIAM Secure Spot in Financial Times 1000: Europe's Fastest Growing Companies Report Two Years Running

FT Financial Times 1000 Europe's Fastest Growing Companies 2022 - 2024

The FT 1000 is the result of a joint initiative by the Financial Times and Statista, which conducted months of research, public calls for participation, intensive database research and directly contacted tens of thousands of companies.

In 2022, we won the title of Fastest Growing Company in Europe in the Cybersecurity category and this year we have been recognised again. To be recognised by the FT:1000 for two years running is incredibly exciting for us and illustrates our talent, skill and dedication to our company and the demand for the unique services we offer across Europe for Identity and Privileged Access Management security solutions to protect businesses.

Security Check (SC)

SC Consultants

SC Consultants

CyberIAM over **40** Security Cleared consultants

NATIONAL NPPV 3 WITH SC

CyberIAM has been aiding and offering services to **11** Police Forces over the last 7 years

We hold over 730 Identity Certifications covering Privileged Access Management (PAM),Identity Governance Management (IGA) & Access Management (AM)

Our Partners

Partners

Case Studies

Customer Testimonial

During our latest engagement, everything was very smooth and easy. Your team were always willing to get stuck into the issues, not once did I hear 'it's your problem let us know when it's fixed'. Reporting was clear and concise, any problems/issues were called out early and included suggestions to address it.

Large Global Healthcare Provider

Offshore Drilling Company

Problem Statement

BeyondTrust Application Custom Platform

- 1 Month time window
- Delivery BeyondTrust Password Safe custom platform to manage passwords of Oracle Application accounts
- Accounts in scope are
  - Database
  - Application
  - Administrative
  - Application user

CyberIAM Approach

- Out of the box thinking to create a compact but efficient platform
- Proof of concept lab testing to ensure correct and reliable solution was identified, ensuring the customer could adopt the best solution
- Development of scripts to gather all account credentials required for a successful execution
- All four account in scope were onboarded into BeyondTrust Password Safe
- During development and testing CyberIAM ensured security with no production assets or accounts were accessible
- Full testing in Three environments before deployment to production environment
- Documentation and walkthroughs to the organisation

Client Benefits

- Log files and output from the Oracle Application utility were interrogated to confirm the success or failure of the request ensuring the customer was aware of what was going on in the solution
- Confirmation email were created and generated to the Support Team informing them of results
- The Oracle Application account rotated on check-in after each use allowing the Client to demonstrate regulatory/audit compliance
- Careful planning of test cycles ensured that any disruption was restricted to only the lower environment allowing the organisation to continue to operate as normal
- Shadowing by the organisations team of the CyberIAM team ensured valuable information and knowledge was passed over
- All work completed within the change management approval time frames

International Health Insurance and Healthcare Group

Problem Statement

- User questionnaire proved that CyberArk had a lack of PSM connectors for ADM accounts, resulting in passwords being copied out, stopping potential session monitoring.
- Lack of capacity and capability on the PSM infrastructure.
- Requirement of fully automated credentialed scanning across organization and elimination of hardcoded credentials.
- Deficiency in user experience and training.
- Remove hardcoded credentials from critical business applications.

CyberIAM Approach

- Reviewed the existing PSM infrastructure providing a detailed approach of improvements with granular calculations.
- Designed and built a range of PSM connectors for an extensive range of platforms.
- Configured AAM with added layers of security to support automated Nessus scanning with daily credential rotation.
- Provided detailed technical and operational documentation to support new integrations.
- Removed hardcoded credentials using Python API with CCP.
- Implemented PTA to report multiple suspicious activities and indicators of compromise.
- Reviewed existing onboarding procedure and made changes to improve overall efficiency.
- Provided expert CyberArk knowledge to assist in the design and configuration of solutions to address specific control deficiency use cases.

Client Benefits

- Detailed documentation enabled a smooth handover from the project to the BAU team.
- Identified highest risk areas and “quick wins” for the programme.
- Reduced the time needed to onboard accounts through automation and additionally reduced the likelihood of human error.
- Users were forced to go through PSM as all connector capabilities were satisfied.
- PoC provided for future Oracle database account onboarding.
- Detailed analysis allowed for the key risk areas to be identified and discrepancies in data sources to be highlighted early on.
- Privileged access to the Vault during irregular hours and suspected credentials theft managed and detected through PTA.

UK Subsidiary of a Global Telecommunications Company

Problem Statement

- Previous consultancy ceased activity halfway through phase one of the project. This led to the PAM tool having a poor reputation across the user base
- New government legislation and internal Cybersecurity targets were not being met
- Under resourced BAU team, who were unable to meet demands of the project and an overall lack of user experience and training within the company
- Extremely complex network due to growth via acquisition
- Inaccurate, out of date CMDB and ownership of many systems was unknown
- Limited amount of recertification of Privileged Access
- Large number of legacy systems which required integration, with no enterprise tooling to assist in discovery
- Personal accounts being used for privileged activities

CyberIAM Approach

- Comprehensive Health Check of existing PAM platform to fully understand the start state
- Designed and built a range of CPM and PSM plug-ins for an extensive range of platforms
- Created a scalable engagement model so multiple CyberIAM teams could engage multiple client teams simultaneously
- Changed the strategic direction of the client from a Personal Privileged Model to a Generic Privileged Model
- Deployed reconciliation accounts across the entire estate
- Initiated pilots of application credential rotation and removal of hardcoded credentials
- Provided detailed technical and operational documentation to support new integrations
- Reviewed existing onboarding and offboarding procedures and introduced automation
- Provided expert knowledge to assist in the configuration of the PAM solution and integration with various platforms (inc. Windows/Linux servers, Databases and Out of Band access)

Client Benefits

- Client able to meet internal and externally mandated targets
- Net reduction of privileged accounts (reducing risk)
- Close working relationship with BAU team allowed for smooth handover
- Structured the project phases to target highest risk areas which enabled quick wins and risk reduction
- CyberIAM trusted to steer the strategic direction of the PAM programme across the UK and globally
- Scalable approach allowed for accelerated delivery
- The reputation of the PAM tool was significantly improved during the lifetime of the programme due to increased engagement, how-to guides and prompt fixing of issues
- Detailed analysis allowed for the key risk areas to be identified and discrepancies in data sources to be highlighted early on
- An improved and more accurate CMDB was defined with owners identified for servers and services

Luxury Fashion House

Problem Statement

- Our client had several outstanding audit points arising from the lack of visibility into “who has access to what”.
- Existing manual Joiner, Mover and Leaver controls were ineffective and time consuming
- Attempts to have one single system IAM solution were unsuccessful
- Manual, or non-existing provisioning with certain critical business applications
- Data quality inconsistency

CyberIAM Approach

- As part of the project initiation, CyberIAM helped the client define strategic target state with clear objectives and outcomes
- Conducted workshop to map out current (or As-Is) IAM controls and processes, followed by detailed workshop to define To-Be processes
- Delivered the foundation phase of IdentityNow in 6 months which included onboarding of HR and Active Directory sources, automated Joiner, Mover and Leaver controls with basic birth right role provisioning
- Performed data quality assessment to identify data mismatch, orphan and dormant accounts
- Worked in partnership with the internal audit and SecOps team to build list of their crown jewel applications with on-boarding priority
- Define approach for SAP applications on-boarding in partnership with Enterprise Arch
- On-boarded over 45 applications using read/write connectors, of which 15 were SAP apps in year one

Client Benefits

- Delivered a centralised IAM solution, which provided a complete visibility of user accounts and access information
- Automated identity management processes, such as joiner, mover and leaver
- Enabled certification campaigns for verifying granted accesses
- Provided self-service and easy request and approval process to replace existing manual requests
- Supplied required reports and history tracking
- Assisted in delivering critical IAM controls to the crown jewel applications

UK Law Enforcement

Problem Statement

- The nationwide programme required our clients in this agency (multiple entities within the agency) to migrate away from traditional ways of working and adapt new standards that would enable collaborations between different entities.
- Improve their current security controls around Identity and Access Management.
- The IAM process was not managed centrally, resulting in disparate controls and process within the different entities.
- Outdated IAM tools requiring heavy manual interventions resulting in slow provisioning and inadequate compliance for Joiner and Leavers.
- Different technologies and architecture resulted in cross entity collaboration slow and difficult.
- Authoritative sources such as HR and Active Directory managed by different third parties, resulting in inconsistent data across system.

CyberIAM Approach

- Reviewed ‘As-Is’ IAM controls and processes, to help design ‘To-Be’ processes in-line with the government standards.
- Reviewed and updated architecture design to streamline and define authoritative data source for different critical information.
- Performed data quality assessment to identify data mismatch, orphan and dormant accounts.
- Automate Joiner Mover and Leaver capability using IdentityNow, along with implementation of basic birth right roles.
- Delivered automated B2B design using Azure and IdentityNow for collaboration among different entities.
- Optimised role and assignment management approach.
- Developed a staged delivery plan to merge the processes across different entities in a manner that allows the containment and control of risk.

Client Benefits

- Improved accuracy in JML processes and reduced complexity in peripheral systems and data movement leading to reduced support costs.
- Migrated from legacy regional Active Directory to central AD clean-up and improved security on Active Directory data.
- Compliance with national governance standards.
- Streamlined sharing and collaboration across entities.

Australian Multinational Retailer

Problem Statement

PAM Onboarding Project

- Our client required a dedicated team of engineers to onboard applications to newly deployed CyberArk Privileged Cloud.
- Client team did not have engineering expertise for PAM application onboarding.
- Applications historically onboarded to CyberArk On Prem were not effectively designed and deployed to apply controls for risk reduction.

CyberIAM Approach

- Project Management structure was put in place to manage the progress of application onboarding.
- Defined roles and responsibilities across the hybrid client and CyberIAM onboarding team.
- Defined new risk reduction PAM policies which dictated onboarding configurations.
- Onboarded accounts as ‘managed’ by default to ensure passwords stored in vaults are correct and rotated. Moving away from ‘static’ passwords.
- Apply Session Management where possible.
- CyberIAM engineers provided education and guidance for client BA’s during requirements gathering.
- JIRA used as project management tool to track tasks during Discovery, Design, Deployment and Warranty. Kanban boards for daily standups and tickets for task assignments across the team.
- Created templates for documenting requirements, high-level and low-level designs.
- Dashboards developed using JIRA to provide real time status updates to the senior leadership team.

Client Benefits

- Defined centralised PAM application onboarding team.
- Consistent level of delivery for application teams.
- Triage function to prioritise applications and set expectations with application owners.
- Well defined PAM end to end onboarding process.
- All accounts onboarded to PAM are at a minimum verified.
- Password rotation applied for onboarded human shared accounts.
- Session monitoring applied for all critical accounts.

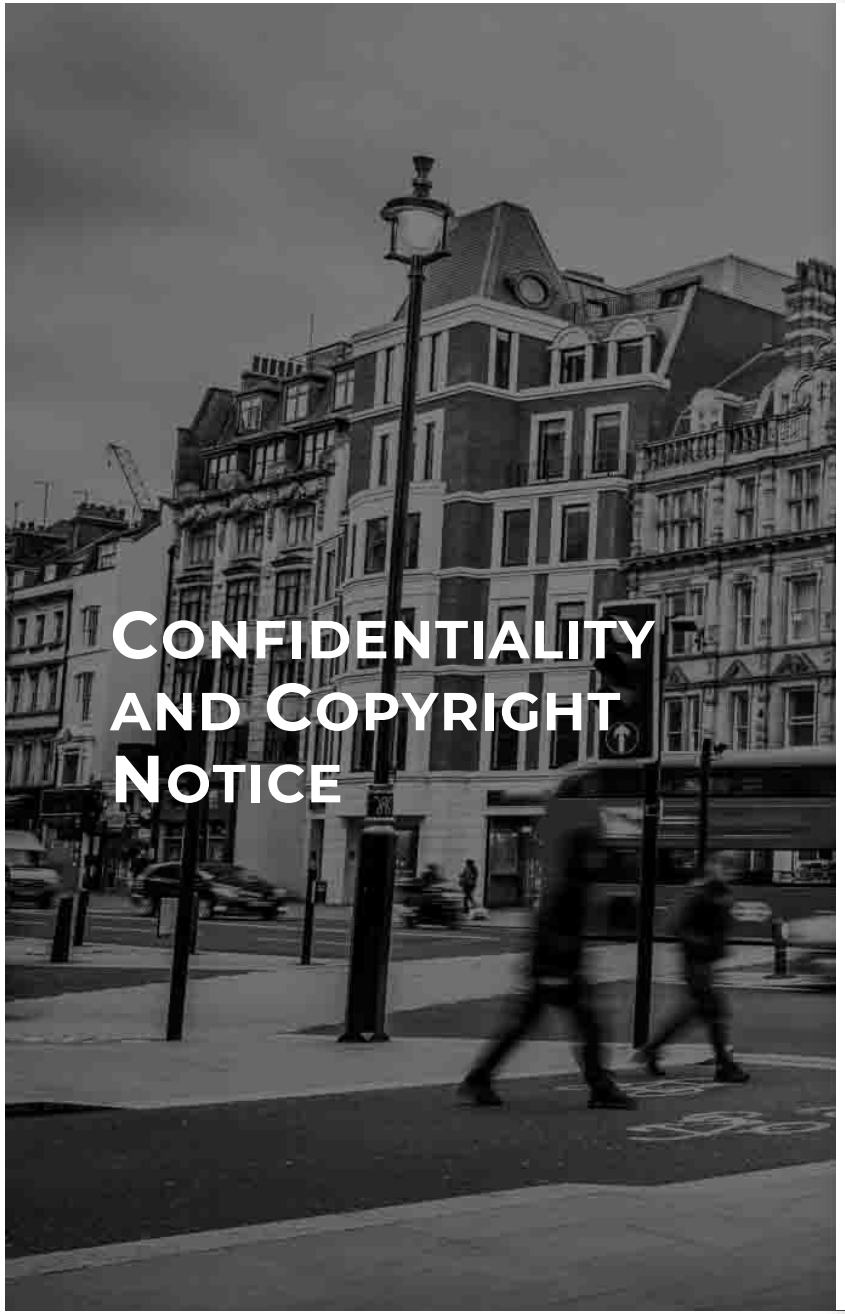
CyberIAM

Contact Details

Feel free to contact us.

Company

+44 (0)844 335 0012
info@cyberiam.com
www.cyberiam.com



Confidentiality and Copyright Notice

The content of this presentation is intended solely for the recipient/s and may contain confidential information.

Please note that no part of this presentation may be reproduced, stored in a retrieval system of any nature, or transmitted, in any form or by any means including photocopying and recording, without the prior written permission of CyberIAM, the copyright owner. Licenses issued by the Copyright Licensing Agency, or any other reproduction rights organisation do not apply. If any unauthorised acts are carried out in relation to this copyright work, a civil claim for damages may be made and/or a criminal prosecution may result. All further rights remain strictly reserved.

All the information contained in this presentation may be subject to change and is not intended to bind the parties to any agreement.