



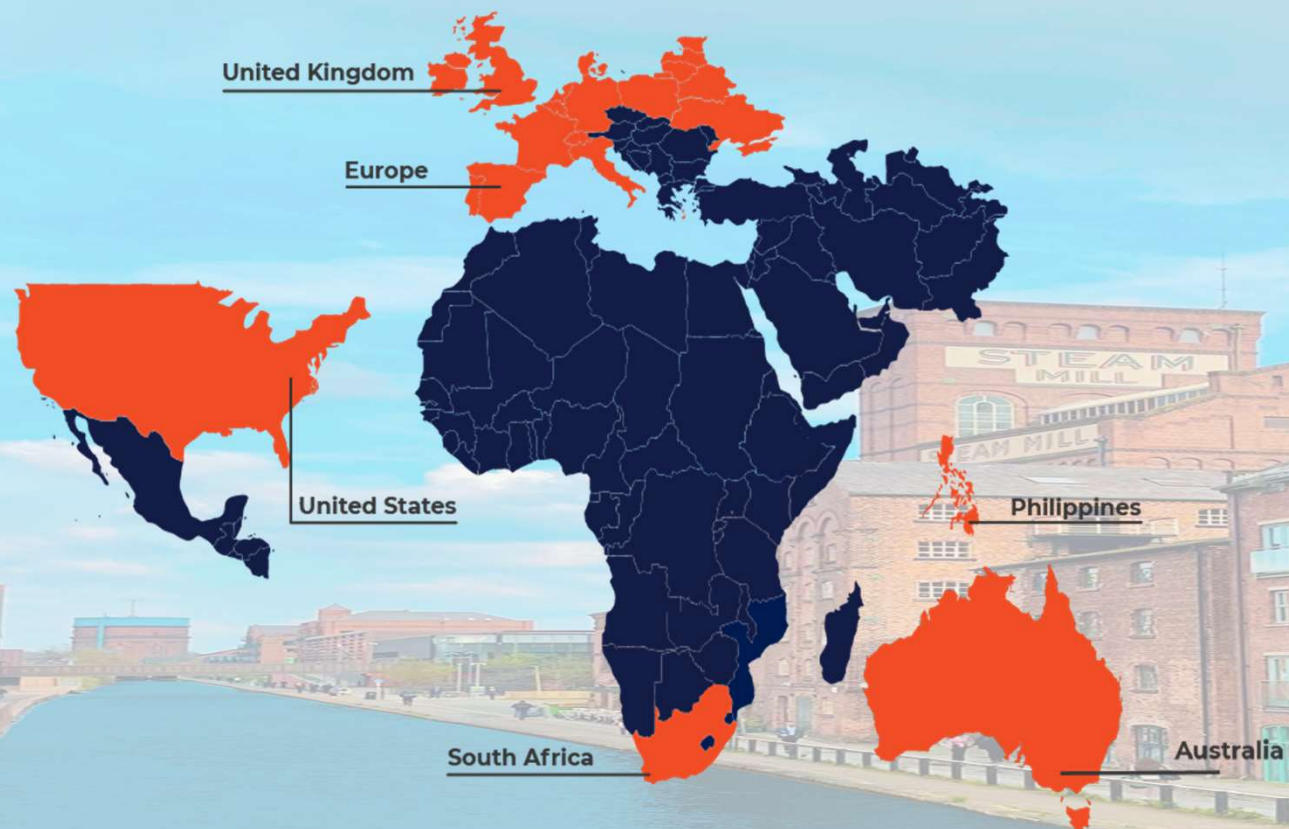
G Cloud 14

Date: 2024

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.



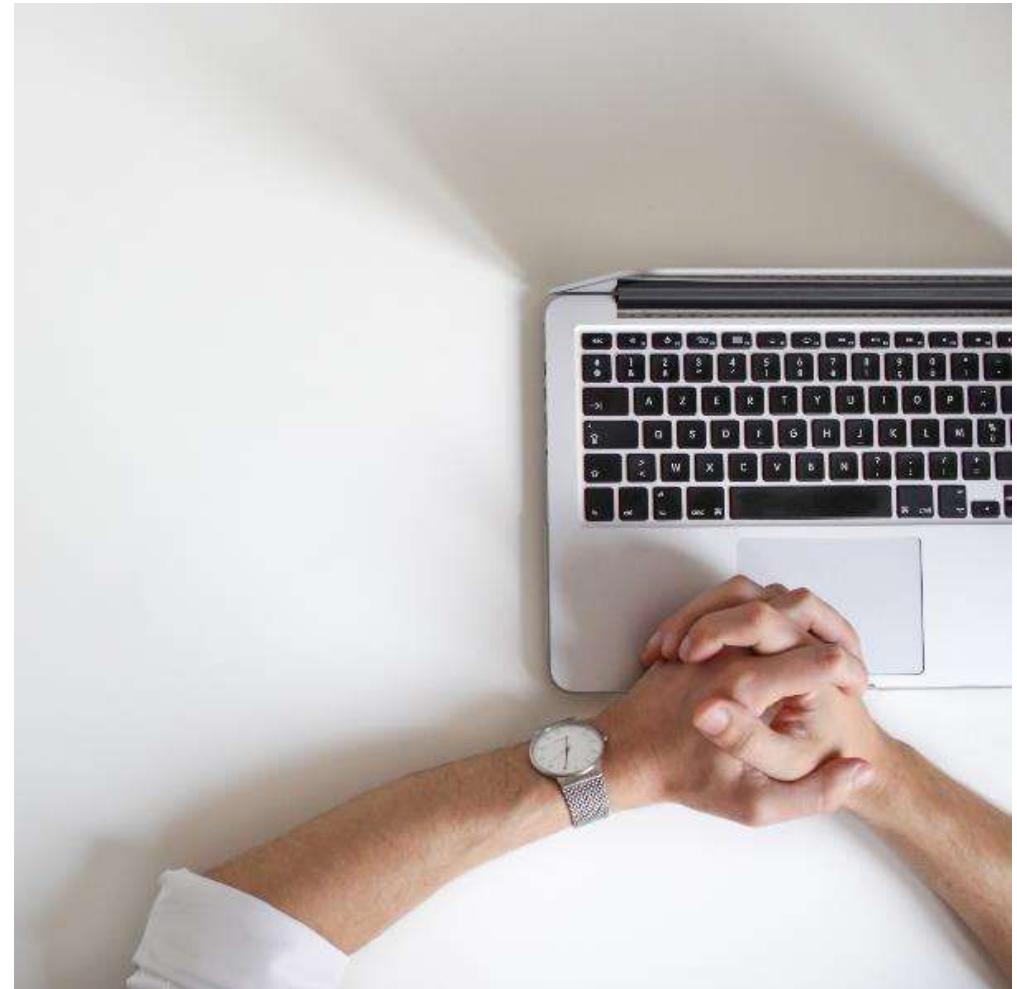
Support Services

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

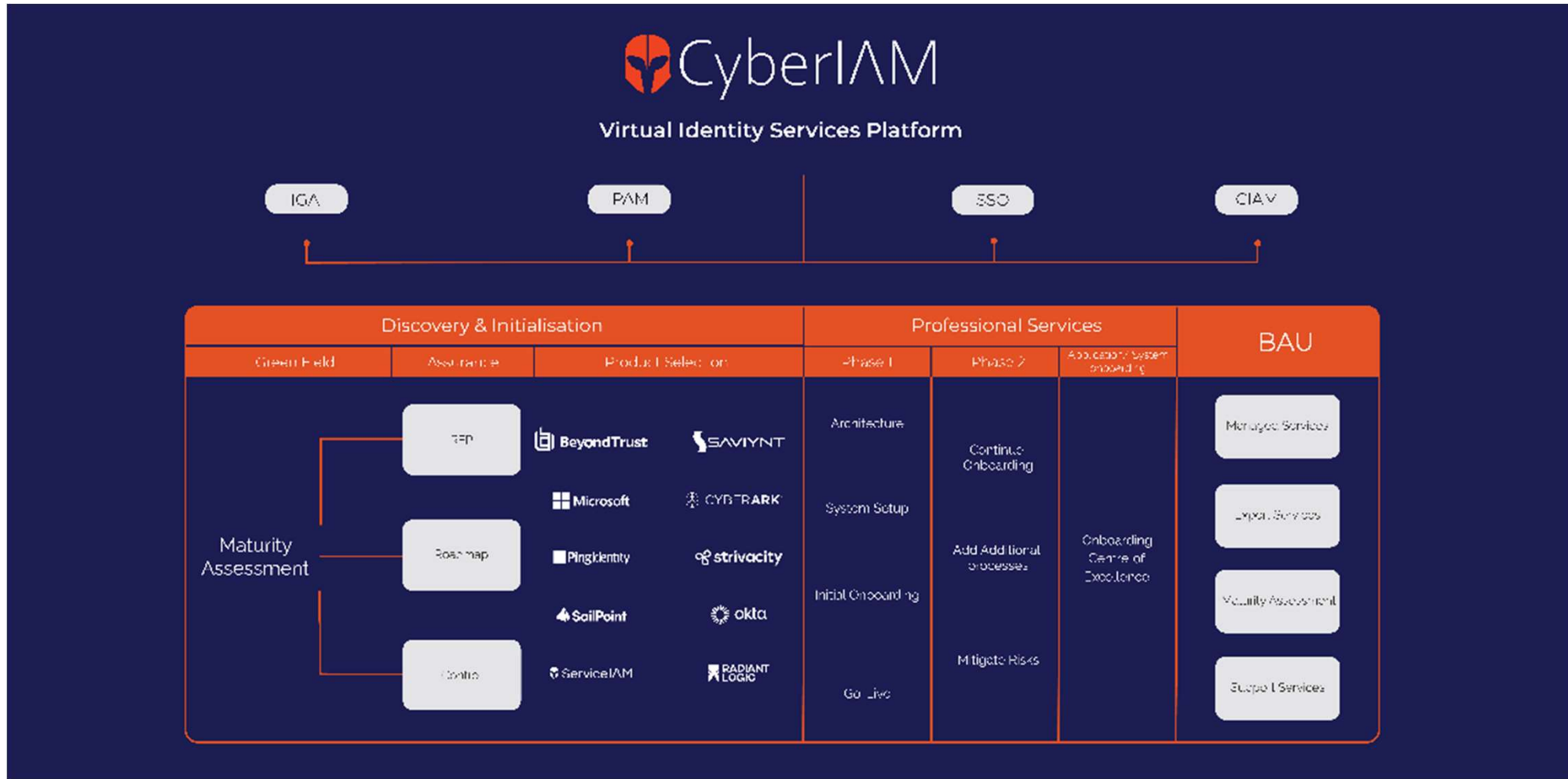


Expert Services

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.



Business slide



Why CyberIAM?



What we do

- CyberIAM provides the expertise needed for the design and implementation of complex identity and access management systems.
- We provide a blend of technical and business expertise for each project engagement because we understand that a successful project addresses both the technology and the business requirements.
- Technology-agnostic approach based on partnerships with the market-leading IAM and PAM vendors that are recommended by the analysts.
- Delivery methodology that emphasises sustained partnership with customers, ranging from strategic advisory services to 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

Managed Services

CyberIAM Managed Services can help run and manage your business-as-usual privileged access implementation beyond project completion. Our team of highly skilled experts will take on the responsibility of maintaining your identity implementation.

Our team will ensure that your solution runs seamlessly and without interruption. Managed Services allows your business to focus on its core objectives, giving you access to the latest technology and industry experts in order to maintain a competitive edge in your respective industry.



Copyright © CyberIAM Holdings Limited 2024.

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



A grayscale background photograph showing a team of people working at a desk. In the foreground, a person's hands are visible typing on a laptop. A pair of glasses and some papers are also on the desk. The image is slightly blurred, creating a professional and collaborative atmosphere.

Our Team

Certification



190+

SailPoint courses completed by CyberIAM Employees

10	2
SailPoint Engineer Certifications	SailPoint Architect Certifications

12

Total Certifications



40+

BeyondTrust Certifications Acquired

15	5
BeyondTrust Password Safe Certification	BeyondTrust Remote Support Certification

15

BeyondTrust
Privileged Remote
Access Certifications



75+

CyberArk Certifications Acquired by CyberIAM Employees

16	9
CyberArk Defender Certifications	CyberArk Sentry Certifications

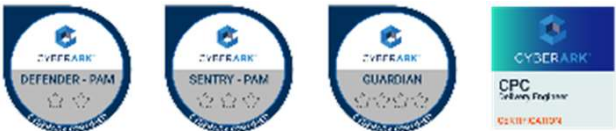
5

CyberArk Guardian
Certifications

7

Privileged Cloud
Delivery Engineer

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



Graduate Program



2023 UK Business Tech Award
Rising Star Nomination

45+

Gone through the
program



CyberIAM
Grad Program

10+

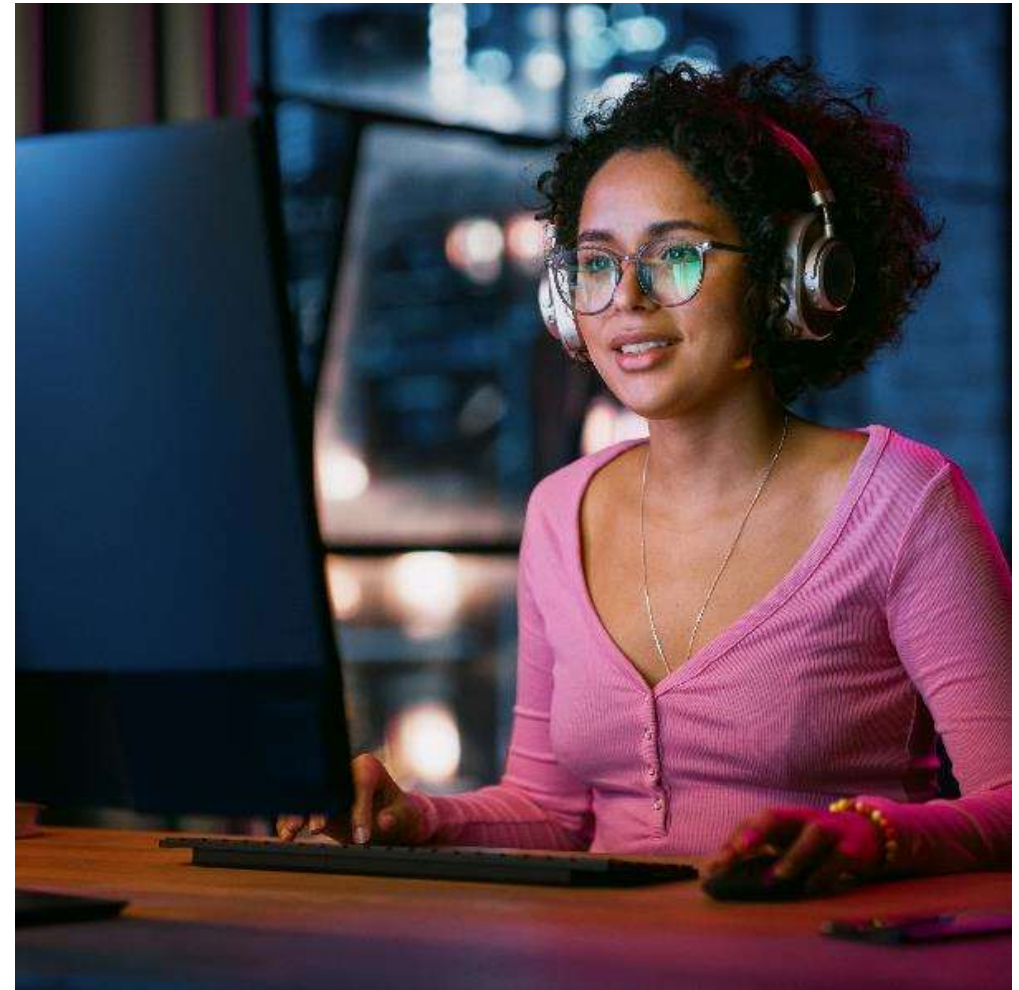
Current Grad
Program

35+

Career promotion
progression

2019

Started in



The Consultants



Business Consultants

4 Associate

8 Consultant

8 Senior



Technical Consultants

20 Associate

14 Consultant

14 Senior



Master Consultants

9 Solution Architects

8 Principal Consultants

7 Managing Consultant



Total number of Identity
Certifications held by CyberIAM

145+



Certification & Awards

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.



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.



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



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.

A grayscale background image showing a group of people in an office setting. In the foreground, a person's hands are visible typing on a laptop. A pair of glasses and some papers are on the desk. In the background, other people are blurred, suggesting a busy work environment.

Our Partners





Case Studies

International Health Insurance and Healthcare Group

Client Issues

- 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.

“

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.

”

- Customer Testimonial
Large Global Healthcare Provider

Global Investment Management Company

Client Issues

- Audit requirement to secure privileged access across the company.
- Complex Active Directory estate with more than ten domains and complicated group nesting.
- Large amount of privileged users using their elevated access for day to day tasks.
- Privileged access mostly held by outsourced manage service providers.
- CyberArk in place for a number of years but underused.

CyberIAM Approach

- Reviewed the current estate and designed tactical and strategic roadmaps to address immediate audit findings and long-term requirements.
- Designed a safe model, naming convention and automated the onboarding of accounts into CyberArk, including the safe and associated Active Directory (AD) group creation.
- Onboarded network device root accounts and several key applications defined by the client.
- Reviewed the Unix estate, created an onboarding approach and onboarded root accounts with associated logon accounts.
- Ran workshops with platform teams to gather requirements and defined access use cases.
- Assessed extracts of data from various sources to determine the scale of the estate and the privileged accounts that exist.
- Designed a revised access model to reduce risk and simplify permissions.
- Detailed documentation of platform design, onboarding processes and access model.

Client Benefits

- 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.
- An audit requirement was satisfied, and privileged account risk was reduced for critical applications.
- Any use of root accounts for Unix machines is now logged and recorded, improving the auditability of these accounts.
- Platform teams were engaged from the beginning, which allowed for better acceptance of the new ways of working.
- Detailed analysis allowed for the key risk areas to be identified and discrepancies in data sources to be highlighted early on.
- The revised access model reduces permission complexity and allows for easier re-certification of access.
- Detailed documentation enabled a smooth handover from the project to the BAU team.

UK Subsidiary of a Global Telecommunications Company

Client Issues

- 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



UK

Contact Details

Feel free to contact us.

Company

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





SA

Contact Details

Feel free to contact us.

Company

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





NL

Contact Details

Feel free to contact us.

Company

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





AUS

Contact Details

Feel free to contact us.

Company

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



USA

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.





Sub Header

Sub Header



Sub Header

Sub Header



Sub Header

A background photograph showing a group of people sitting around a long wooden table in a meeting or workshop. The image is slightly blurred and has a warm, sunlit atmosphere. In the foreground, a person's hands are visible, writing in a notebook. Another person's arm and hand are visible on the right side of the table. The text 'Sub Header' is overlaid on the left side of the image.

Sub Header

Sub Header

