MindHug

Your Mind, Your Journey, Our Innovation

Elevate your Wellbeing with

MindHug

DSbD

Privacy Preserving Technologies

Project Number:
DiScribe – RC-MN1164X

Our Starting Point

MindHug

Key Achievement : A MCC (Multi Compartment Computation) based Key Derivation Function framework prototype

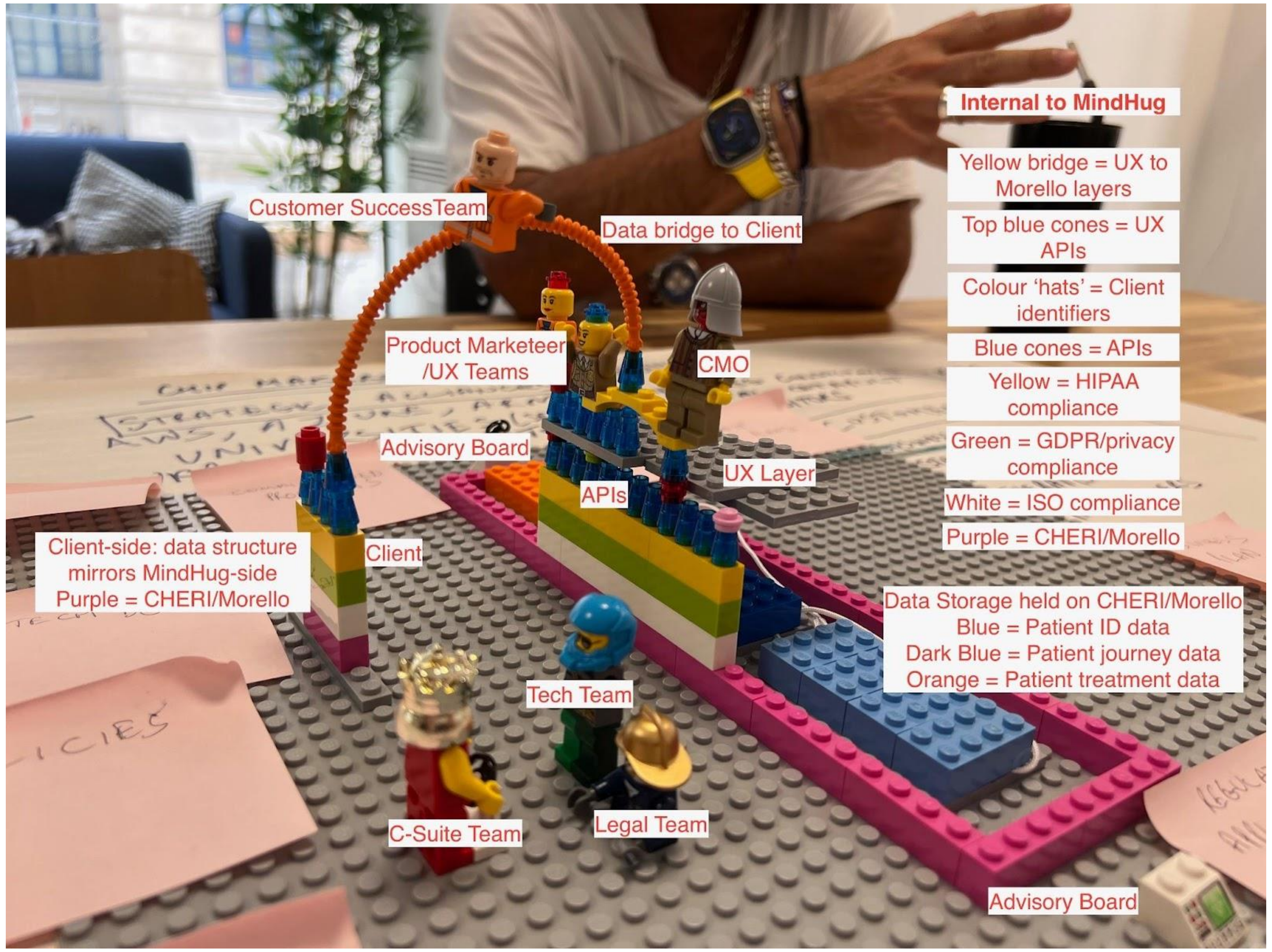
Deliverables completed

Password based Compartmentalised key derivation framework

- **ParallelisationFactor (p) - Compartment A**
  - PBKDF2 based generation of initial 128*BlockSizeFactor*p bytes of data (based on compartment's parallelisationFactor)
  - Resulting array of p elements, (each entry being blocksize bytes) invokes Compartment B parallelly
- **memoryCostFactor (m) - Compartment B**
  - Mixes each incoming block capability in m Costfactor times using ROMix function
- **salsaCore - Compartment C**
  - a non-collision resistant core compartment that derives a hash function from 64-octet capability from B to 64-octet capability.

Beta CRM Architecture for benchmarking and testing

Where want to get to


Internal to MindHug
Yellow bridge = UX to Morello layers
Top blue cones = UX APIs
Colour 'hats' = Client identifiers
Blue cones = APIs
Yellow = HIPAA compliance
Green = GDPR/privacy compliance
White = ISO compliance
Purple = CHERI/Morello
Customer SuccessTeam
Data bridge to Client
Product Marketeer /UX Teams
CMO
Advisory Board
UX Layer
APIs
Client-side: data structure mirrors MindHug-side Purple = CHERI/Morello
Client
Data Storage held on CHERI/Morello
Blue = Patient ID data
Dark Blue = Patient journey data
Orange = Patient treatment data
Tech Team
C-Suite Team
Legal Team
Advisory Board

Credits**: Royal Holloway, University of London** (Lizzie Coles Kemp, Claude Heath, Laura Shipp), **Queensland University of Technology** (Mark Burdon) & **MindHug** (Anthony Ioannou, Rajpal Gujral and Chitraj Singh)

The LEGO model: Brainstorming session of the end state, full stack product, data and technology solution that MindHug wants to offer, including the potential to License Healthcare Software. While we considered the use of CHERI/Morello hardware shown as a ring of purple bricks surrounding stored patient and client data … there is an Elephant in the Room!

Research Question

“While CHERI and Morello continue to remain off-market, and given the budget and technical limitations of startups - what are the security and governance steps a HealthTech startup can take to mimic elements of compartmentalisation on the cloud, and meet privacy and regulatory standards?

Research Methodology

Technology and Security Design: Convert our regulatory research into technical specifications and governance requirements, analyse current gaps, complete research to ensure needs of market and vulnerable individuals considered, and map our technology API endpoints.

Incorporate security measures into a scaled version of our technology stack that can mimic some of the benefits of 'compartmentalised' and 'enclave' based security capabilities within the current limitations of traditional cloud computing. This could for instance distribute data across multiple nodes, use encryption at rest and in-transit, use Enclaves to retrieve and recompute data, and use Virtual Private Cloud (VPC) subnet storage. Other methodologies may also be considered.

Integration and Testing: Test API endpoints to ensure Modules, AI Engine and Security and Privacy Techniques integrate.

Build **Legal and Governance Pipelines**, Controls, Terms and Processes to meet **non technical** requirements

Scope

The Security Philosophy

Access monitoring (continuous):

- Full Enrolment / MFA on all devices and logins (Internal and Platform Users)
- Enforced 30 day Password changes (internal MindHug Users)
- Microsoft defender at all end points
- Multi level risk and threat monitoring and Alerting (login , email , location and data access)
- Microsoft Purdue or Similar constant compliancy scanning

Data storage and access:

•All data behind VPC/VPN and fully segmented and encrypted at source and in transit. Our aim is to segment the user data into 3 separate encrypted at rest data stores thus significantly reducing the risk of data breaches

  - Personal Data (PII)
  - Medical information
  - Journey information (user experience etc)

•Full MFA on all portal logins
•Access to data will be fully role based
•Constant Stack checking and security patching – proactive approach to security
•All infrastructure as code (Full CI/CD) and containerisation. Ensuring configurations are never manually applied
•Source code scanning for security best practice and library patches etc (sonar cloud)
•AWS Guard duty , AWS cloud trail , AWS Waf, AWS Secret manager

Continual privacy , compliance and threat monitoring to the following standards:
ISO 27001, and ISO 27701, CIS-AWS v1.3.0, PCIv3.2.1, SOC v2, HIPAA v1, GDPR V1, CIS Azure v1.3.0, CIS Docker v1.2.0., OWASP top 10 2021

Legal Terms and Privacy Policies reflect these standards and requirements

Making it more specific

Microsoft 365 / Google Workplace

- Full Enrollment / MFA on all devices and logins
- Enforced 90 day Password changes
- Microsoft defender at all end points
- Multi level risk and threat monitoring and Alerting (login , email , location and data access)
- Microsoft Purdue compliancy scanning

Cloud and Application

- All data behind VPC/VPN and fully segmented
- Full MFA on all portal logins
- Constant Stack checking and security patching
- All infrastructure as code (Full CI/CD) and containerisation.
- Source code scanning for security best practice and library patches etc (sonar cloud)
- AWS Guard duty , AWS cloud trail , AWS Waf, AWS Secret manager

Enhanced Monitoring

Continual privacy , compliance and threat monitoring / dashboarding , to all the following standards :

- ISO 27001
- CIS-AWS v1.3.0
- PCIv3.2.1
- SOC v2
- HIPPA v1
- GDPR V1
- CIS Azure v1.3.0
- CIS Docker v1.2.0
- OWASP top 10 2021

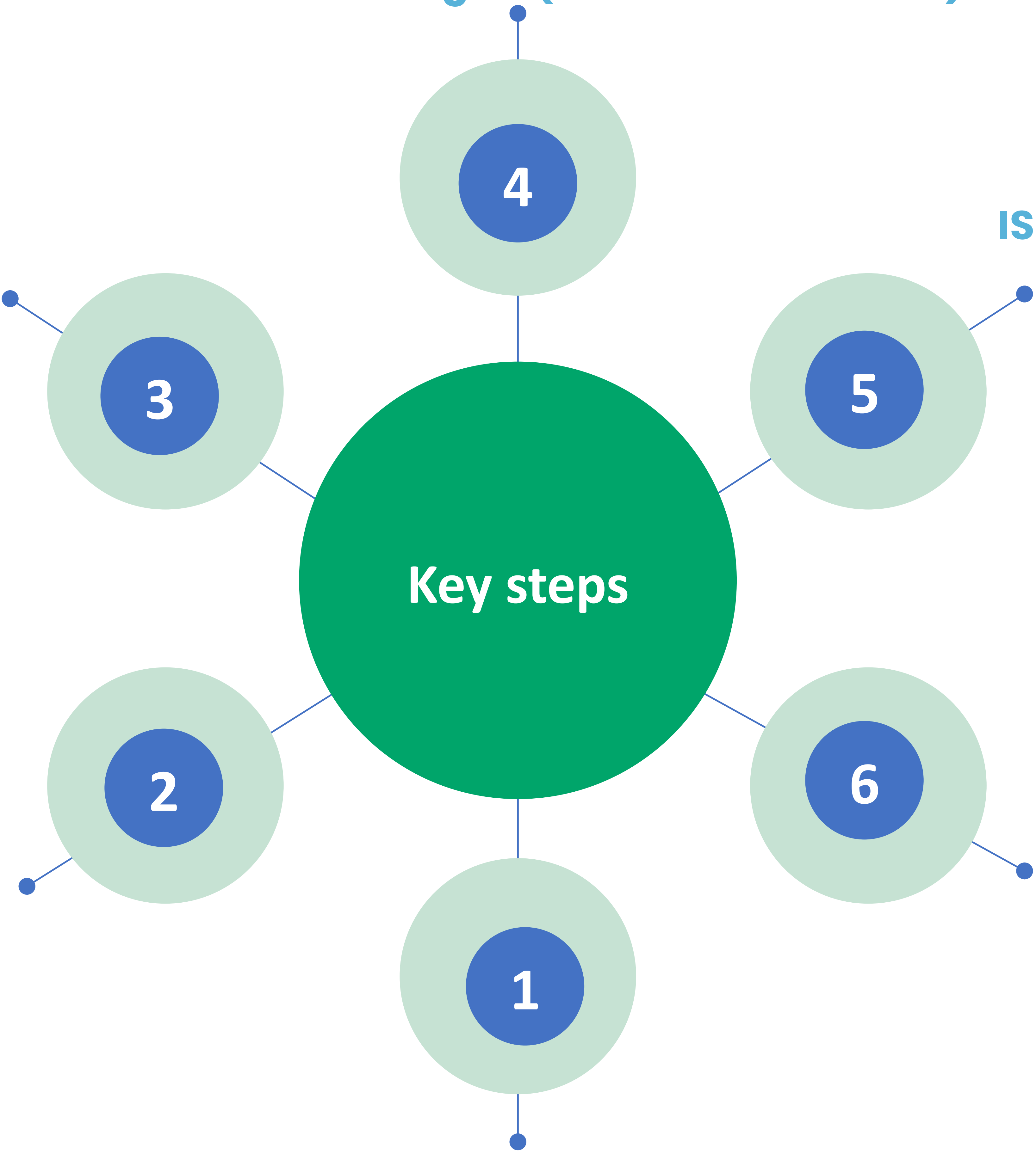
MindHug 6 step approach

ISO27001 Stage 1 (Document Audit)

ISO 27001 Stage 2 (Certification Audit)

GDPR Compliance

ISO27001 compliance



DPO Training , ISMS Lead Training . Internal stage 1 and stage 2 audit

ISO 27001, key person s training and certification

Enhanced PII and PIMS development

ISMS Document creation

ISMS Documentation tooling , Gap assessments , pen tests

ISO 27701, training and certification

HIPPA Data in Transit Compliance

Technological Infrastructure and Monitoring incl live dashboards

ISO27701 compliance

Why ISO?

- ISO 27001 is a standard and GDPR is a regulation. ISO27001 is clear direction / framework for ensuring our technological implementation , processes and documentation are all at the same monitorable and auditable baseline for confidentiality, integrity and availability.
- It is based around the 3 Pillars of People, Process, Technology
- It gives us management assurance and outward facing trust / credibility.
- ISO 27001 is the only auditable international standard that defines the requirements of an information security management system (ISMS).

Types of ISO Controls

- Information Security Policies (2)
- Organisation of Information Security (7)
- Human Resources Security (6)
- Asset Management (10)
- Access Control (14)
- Cryptography (2)
- Physical and Environmental Security (15)
- Operational Security (14)
- Communications Security (7)
- System Acquisition, Development and Maintenance (13)
- Supplier Relationships (5)
- Information Security Incident Management (7)
- Information Security Aspects of Business Continuity Management (4)
- Compliance (8)

MindHug

Making it more specific

Microsoft 365 / Google Workplace

- Full Enrollment / MFA on all devices and logins
- Enforced 90 day Password changes
- Microsoft defender at all end points
- Multi level risk and threat monitoring and Alerting (login , email , location and data access)
- Microsoft Purdue compliancy scanning

Cloud and Application

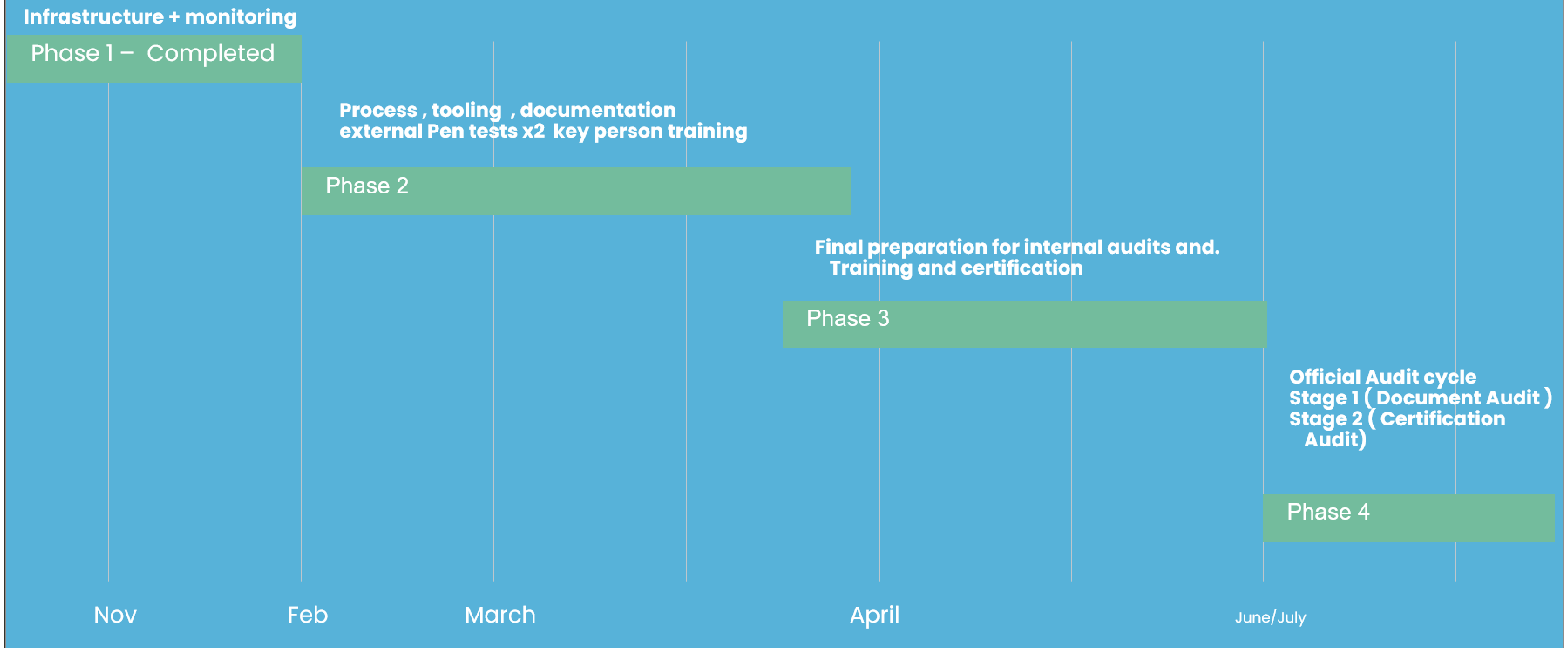
- All data behind VPC/VPN and fully segmented
- Full MFA on all portal logins
- Constant Stack checking and security patching
- All infrastructure as code (Full CI/CD) and containerisation.
- Source code scanning for security best practice and library patches etc (sonar cloud)
- AWS Guard duty , AWS cloud trail , AWS Waf, AWS Secret manager

Enhanced Monitoring

Continual privacy , compliance and threat monitoring / dashboarding , to all the following standards :

- ISO 27001
- CIS-AWS v1.3.0
- PCIv3.2.1
- SOC v2
- HIPPA v1
- GDPR V1
- CIS Azure v1.3.0
- CIS Docker v1.2.0
- OWASP top 10 2021

Path to ISO 27001 and ISO27701 Compliance (2023/24)


Infrastructure + monitoring

Phase 1 – Completed

Process , tooling , documentation
external Pen tests x2 key person training

Phase 2

Final preparation for internal audits and.
Training and certification

Phase 3

Official Audit cycle
Stage 1 (Document Audit)
Stage 2 (Certification Audit)

Phase 4

Q&A

MindHug

Thank You For Your Support
Give Yourself a MindHug :)

Contact Us

MindHug

MindHug
UCL BaseKX
103c Camley Street,
London N1C 4PF
+442038702691

Chitraj (Raj) Singh, CEO and Founder
EMAIL: raj@mindhug.io
WEBSITE: www.mindhug.io