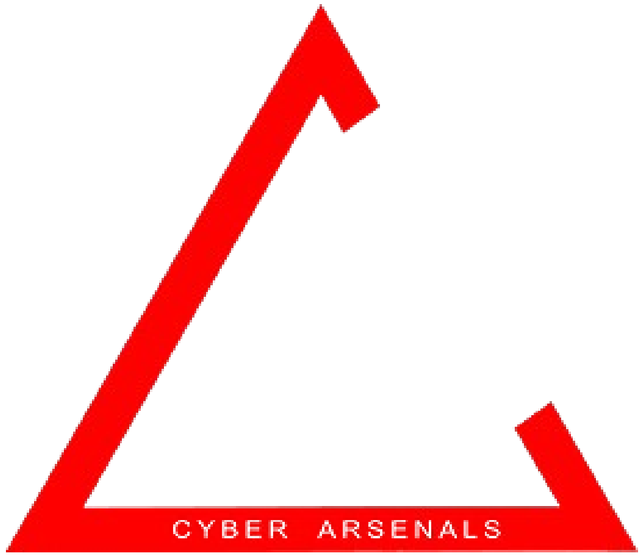



Empowering businesses through

comprehensive technology and cyber security solutions

# COMPANY PROFILE

# Cyber Arsenals (Private) Limited

# About Us

## Transforming the Way You Protect Your Digital World!

We believe that great digital experiences and strong cybersecurity should go hand in hand. We not only work in shaping cyber security for you but also maturing it. Which means shifting from reacting to threats to anticipating them. It is the discipline of strengthening behaviors, processes, and systems so that security becomes an integrated business capability - not an afterthought. We drive that transformation with clarity, confidence, and purpose.

Strengthening cybersecurity begins with reinforcing every layer people, processes, and technology. We help organizations develop robust defenses, elevate awareness, and adopt smarter, more secure digital practices.

**It's about building resilience, which is not a choice but necessity.**

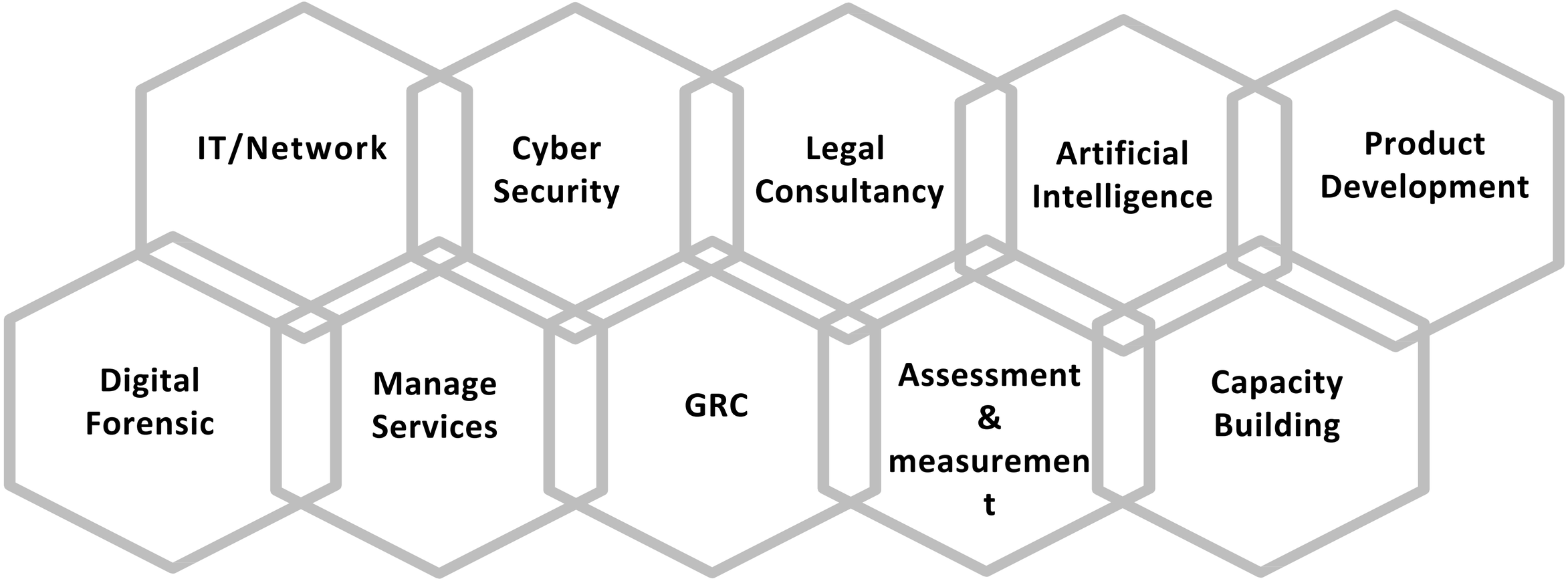
# Our Mission

Our mission is to shape a proactive cybersecurity mindset, empowering people to think critically, act responsibly, and make security an instinctive part of everyday digital life.

To transform cybersecurity mindsets by empowering individuals and organizations to think proactively, act responsibly, and embed security into every digital decision.

We strive to build a culture of awareness, resilience, and confidence, where cybersecurity is not just a practice but a shared mindset that drives safer, smarter digital experiences.

# Our Cyber Security Solutions & Services



# What We Do

## IT/Network

- Set up and manage firewalls, routers, and switches
- Monitor all network traffic around the clock
- Block unauthorized access before it causes harm
- Secure your internet connections and internal systems
- Fast response when network threats are detected

## Cyber Security

- Find weaknesses in your systems before hackers do
- Train your team to recognize and avoid cyber threats
- Respond quickly and effectively when attacks happen
- Keep sensitive business and customer data safe
- Build a strong, long-term security posture for your organization

## Legal Consultancy

- Advice on cybersecurity and data protection laws
- Help you meet local and international legal requirements
- Review contracts, agreements, and privacy policies
- Support during cyber incidents and legal disputes
- Guidance on GDPR, PDPL, and other data regulations

## Artifical Intelligence

- Automatically detect threats using intelligent algorithms
- Monitor your systems 24/7 without human fatigue
- Predict attacks before they happen using data patterns
- Automate routine security tasks to save time and cost
- Get smart insights from your security data instantly

## Product Development

- Develop software and apps with security built in from the start
- Thorough security testing before any product goes live
- Regular updates to keep your product protected over time
- Custom-built solutions designed for your specific business needs
- Comply with industry security standards throughout development

## Digital Forensic

- Investigate cyber crimes and security incidents thoroughly
- Collect and preserve digital evidence the right way
- Understand exactly what happened and how it was done
- Provide expert support for legal and court proceedings
- Recover lost or stolen data after an attack

# What We Do

## Manage Services

- 24/7 monitoring and support from our expert security team
- Proactive threat detection and immediate incident response
- Regular reports keeping you informed of your security status
- Flexible service plans that grow with your business
- More cost-effective than building an in-house security team

## GRC

- Build strong security policies and governance frameworks
- Identify, assess, and manage your business risks clearly
- Meet compliance requirements: ISO 27001, GDPR, PCI-DSS, PDPL
- Regular audits to ensure your policies are being followed
- Clear reporting for leadership and board-level decisions

## Capacity Building

- Security awareness training for all staff levels
- Hands-on workshops and real-world scenario exercises
- Phishing simulation campaigns to test and build awareness
- Specialized training for IT and security teams
- Ongoing learning programs to keep skills sharp and current

## Assessment & Measurement

- Comprehensive review of your current security posture
- Penetration testing to simulate real-world attacks
- Vulnerability scanning across all systems and applications
- Gap analysis with a clear, prioritized action plan
- Maturity assessments aligned to global frameworks (NIST, CMMI)

# Cyber Security – Solutions

## Z E R O T R U S T

### Network Security

- NG Firewalls
- Web Application Firewalls
- Email Security
- Anti - DDoS
- Network Admission Control

### Identity and Access

- Privilege Access Management (PAM)
- Identity and Access Management (IAM)
- Identity Governance (IGA)
- Zero Trust Network Access (ZTNA)
- Mobile Device Management (MDM)
- Network Admission Control (NAC)

### Detection and Response

- SIEM and SOAR
- End Point Protection (EPP)
- End point detection and Response (EDR)
- Extended Detection and Response (XDR)
- Network Detection and Response (NDR)
- Threat Intel

### Data Security

- Data Loss Prevention
- Database protection and Encryption
- Database insights
- Data Discovery and Classification

### Application Security

- Dynamic Application Security Testing DAST
- Static Application Security Testing SAST
- API Security
- Vulnerability Management

### GRC

- Compliance Management
- IS Governance
- Risk Management
- External Attack Surface Management
- Internal Risk management
- Awareness and Phishing Simulations

# Legal Portfolio - Cyber Crime & Digital Fraud



*CEO-led legal practice combining legal expertise with cyber security experience*

### Cyber Crime Litigation

Legal representation and case handling in cyber crime matters, with a focus on digital evidence, cyber offences, investigation support and court proceedings.

### Financial & Digital Fraud

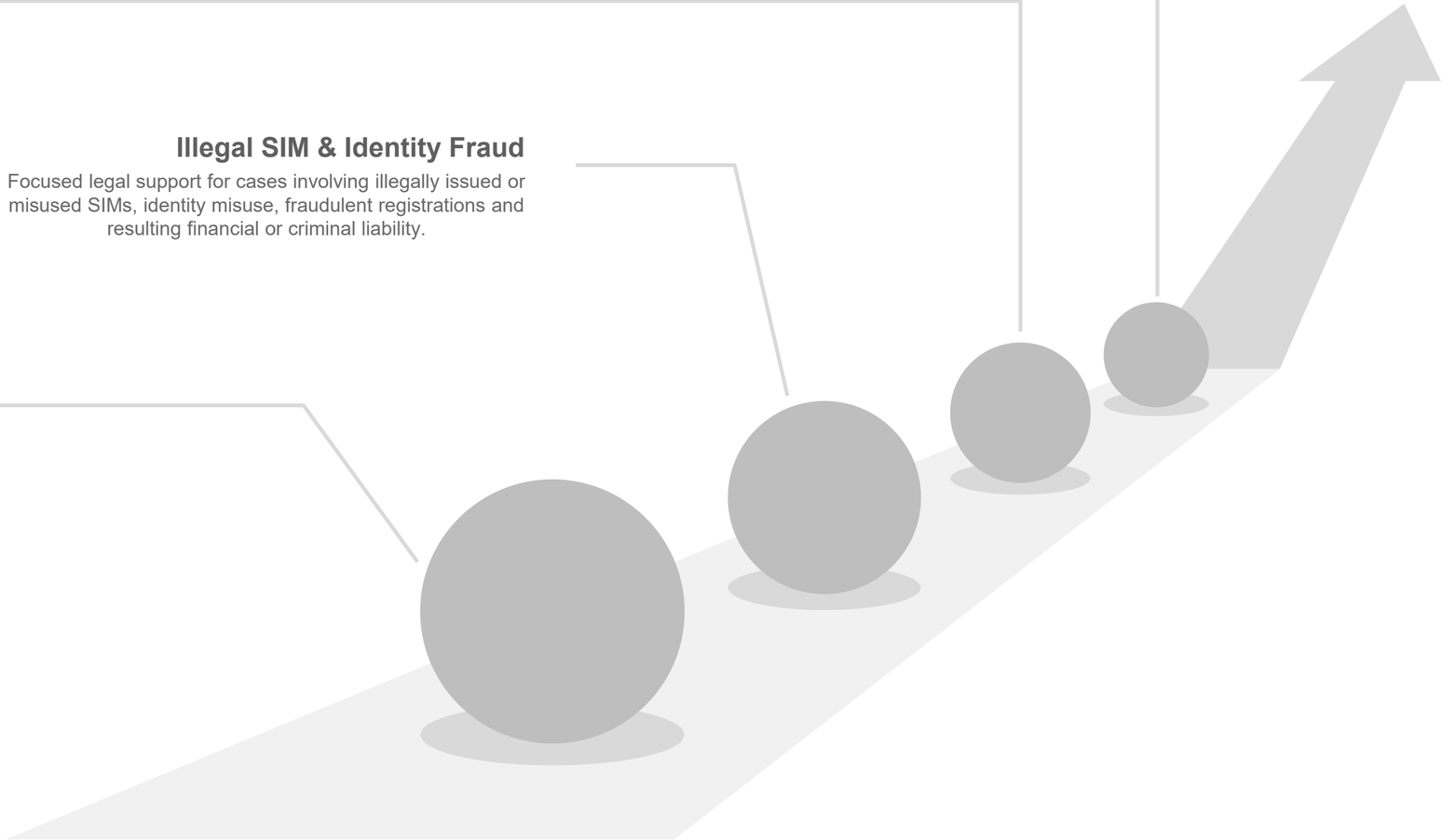
Legal assistance in financial fraud, online scams, unauthorized digital transactions, account misuse and other technology-enabled financial crimes.

### Illegal SIM & Identity Fraud

Focused legal support for cases involving illegally issued or misused SIMs, identity misuse, fraudulent registrations and resulting financial or criminal liability.

### Cyber Law Advisory & Evidence

Legal and technical guidance on cyber laws, digital evidence, incident documentation, regulatory matters and coordination with relevant investigative authorities.



# Critical Market Need - Our Benchmarks



## Data Management

Cyber Arsenals has developed its own frameworks on data governance, data quality, data architecture, data modeling, referencing and tagging etc.

## Data Discovery and Classification

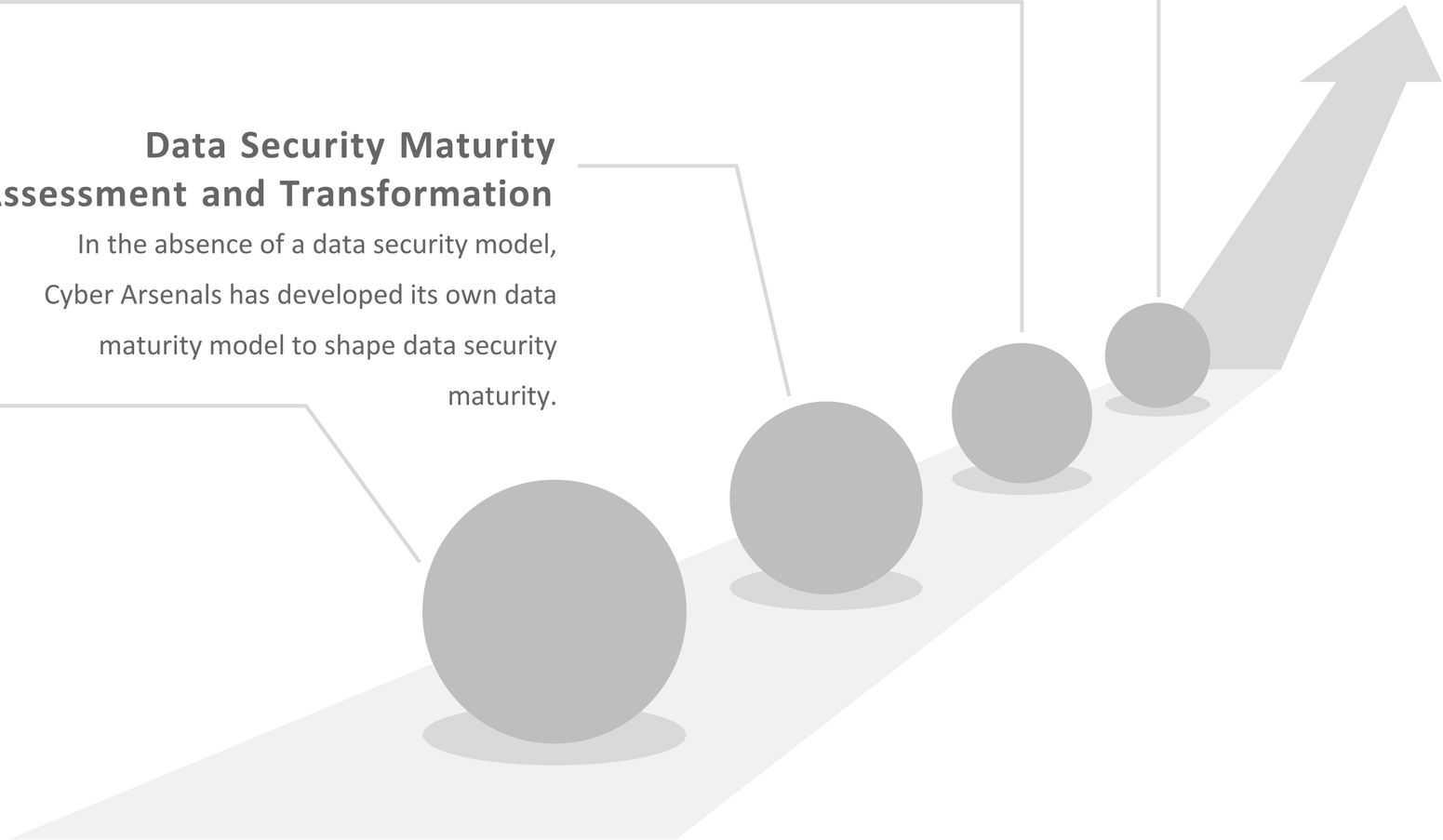
Coping the big challenge of formulizing and shaping data discovery and classification, Cyber Arsenals phased approved is the need of organizations.

## Data Security Maturity Assessment and Transformation

In the absence of a data security model, Cyber Arsenals has developed its own data maturity model to shape data security maturity.

## SOC Maturity Assessment and Transformation

Experts in CMMI. Cyber Arsenals has developed its own extended model on top of CMMI to measure maturity of all the functions integrated with a security operations center.



# Cyber Security - Services



## Consultancy

- Data Management
- Data Discovery & Classification
- Data Security
- Security Architecture
- Cloud Security
- Zero Trust
- Identity Security
- Zero Trust
- IS Risk Mitigation Plan

## Managed SOC

- 24 x 7 Managed
- Hybrid
- Digital Forensics and Incident Response
- Threat Hunting
- Malware Analysis and Reverse Engineering

## Managed DevOps

- Monitoring / 24 x 7 Support
- CI / CD Pipeline Management
- Containerization and Orchestration
- Trainings
- Infrastructure as code implementation
- Automated Quality Assurance

## Managed DevSecOps

- Static Application Security Testing SAS
- Dynamic Application Security Testing DAS
- Public Key Infrastructure PKI
- Secure CI / CD Automation
- Policy as a Code implementation
- Threat Modeling and Vulnerability Management
- Compliance Assurance

## Audit and Compliance

- AD Security
- ISO 27000
- HIPAA
- PCI-DSS
- GDPR
- PDPL
- HI-Trust
- SOC2

## Security Assessment and Testing

- Risk Assessment
- Vulnerability Assessment
- Penetration Testing
- OT Penetration Testing
- Secure Code Review
- NIST CSF
- Compromise Assessment
- Digital Forensics

## Maturity Assessment and Transformation

- Cyber Security
- Security Operations Center
- Data Security
- Data Governance
- Data Quality
- DevSecOps
- Operational Technology

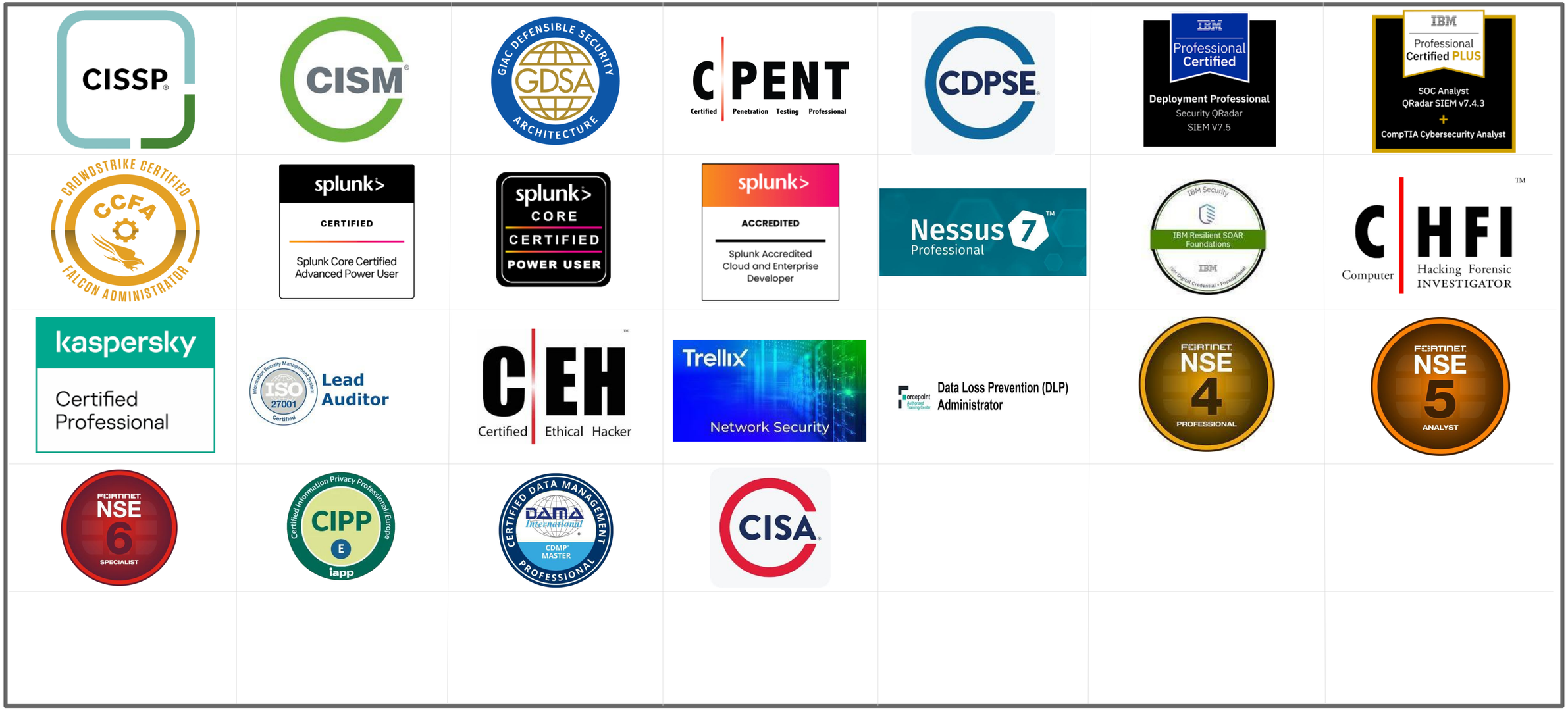
# Our OEM Partnerships



| | | | | | | |
|---|---|---|---|---|---|---|
| IBM | corelight | DECE | f5 | SECHARD Complete Zero Trust | kaspersky | cywift |
| ZEROWL | ivanti | paloalto NETWORKS | CISCO splunk> | FORTINET | RAPID7 | SkyGuard |
| LOGPOINT | ORACLE | COHESITY | VORTEX GLOBAL | FORCEPOINT | NUTANIX | Logsign |
| LogRhythm | SOPHOS | SOCRadar® | Trellix | Delinea | DRATA | segura |
| tenable | TREND MICRO | Samsung Knox | trio | PRODAFT | PhishRod Addressing Human Risk | Symantec |

# Our Certifications





# Managed SOC Services



## Incident Monitoring

- Continuous Monitoring
- Event Analysis
- Incident Analysis
- SOC Triage and Escalation
- Alert Categorization
- KPI Monitoring
- False Positive Analysis
- System Health Monitoring

## Incident Response Management

- Root Cause Analysis
- Attack vector Identification
- Threat Management
- Stake Holder Coordination
- L2 Triage
- Incident Response
- Integrations and normalization
- MITRE Mapping
- Rule fine Tuning
- IOC Ingestion

## DF & Solution Enrichment

- Digital Forensics
- Malware Analysis
- Reverse Engineering
- SOC Engineering
- Solution Enrichment
- Threat Intelligence
- Threat Hunting
- Use Case Management
- Use Case Management
- Automation and Orchestration

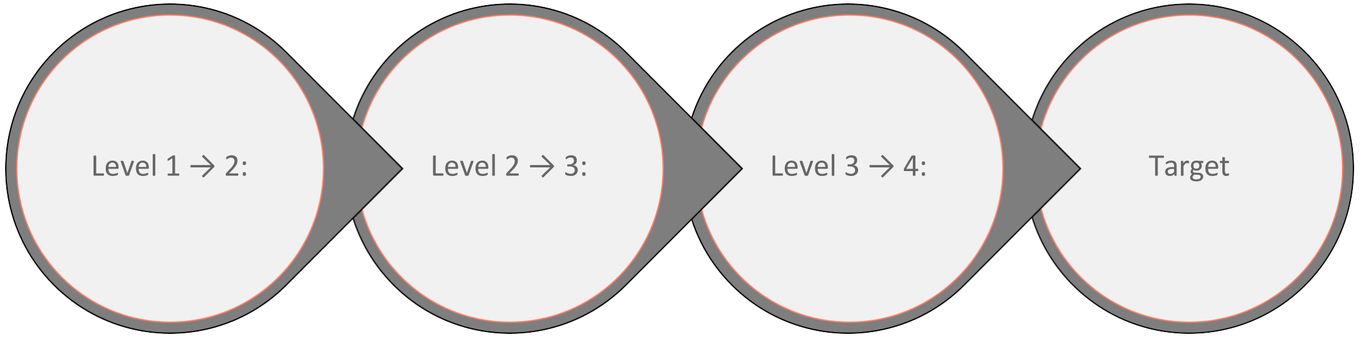
## SOC Governance

- Risk Alignment
- SOC Charter Development and enforcement
- SOC Governance Program Development Enforcement
- SOC Process enforcement
- RACI Enforcement
- SOC Service Delivery
- ROI Management
- Compliance Management

# Maturity Transformation



## LIFECYCLE



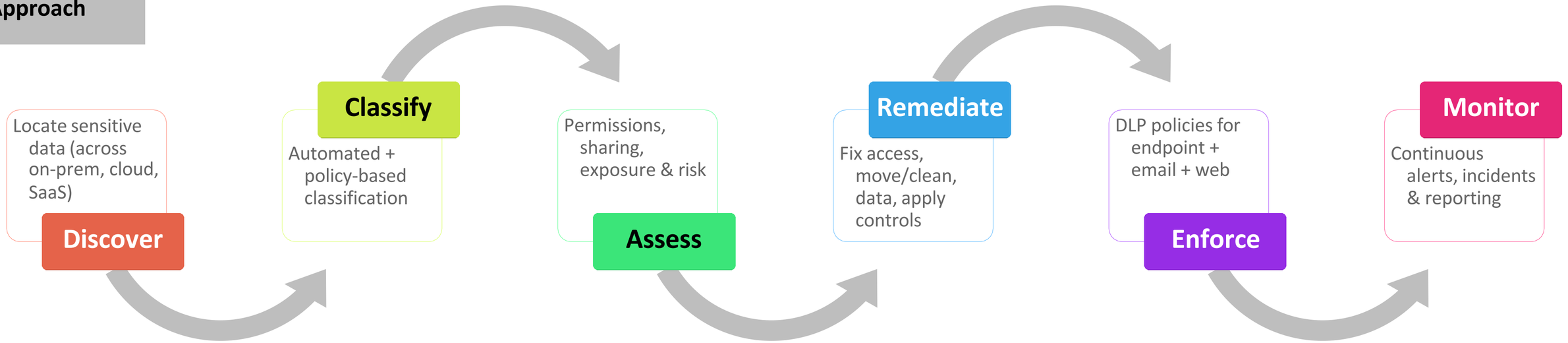

### Transformation Enablers:

- Executive sponsorship and governance
- Cross-functional team formation
- Technology platform integration
- Continuous improvement processes

# Recommended Data Security Approach (Lifecycle + Zero Trust)



## Approach




## How the tools map to the lifecycle

### DSPM

- Discover & classify sensitive data
- Assess exposure: sharing, permissions, ROT
- Orchestrate remediation actions

### DLP

- One policy across channels
- Prevent/monitor email, web, endpoint exfil
- Support discovery & endpoint controls

### Security Hardening

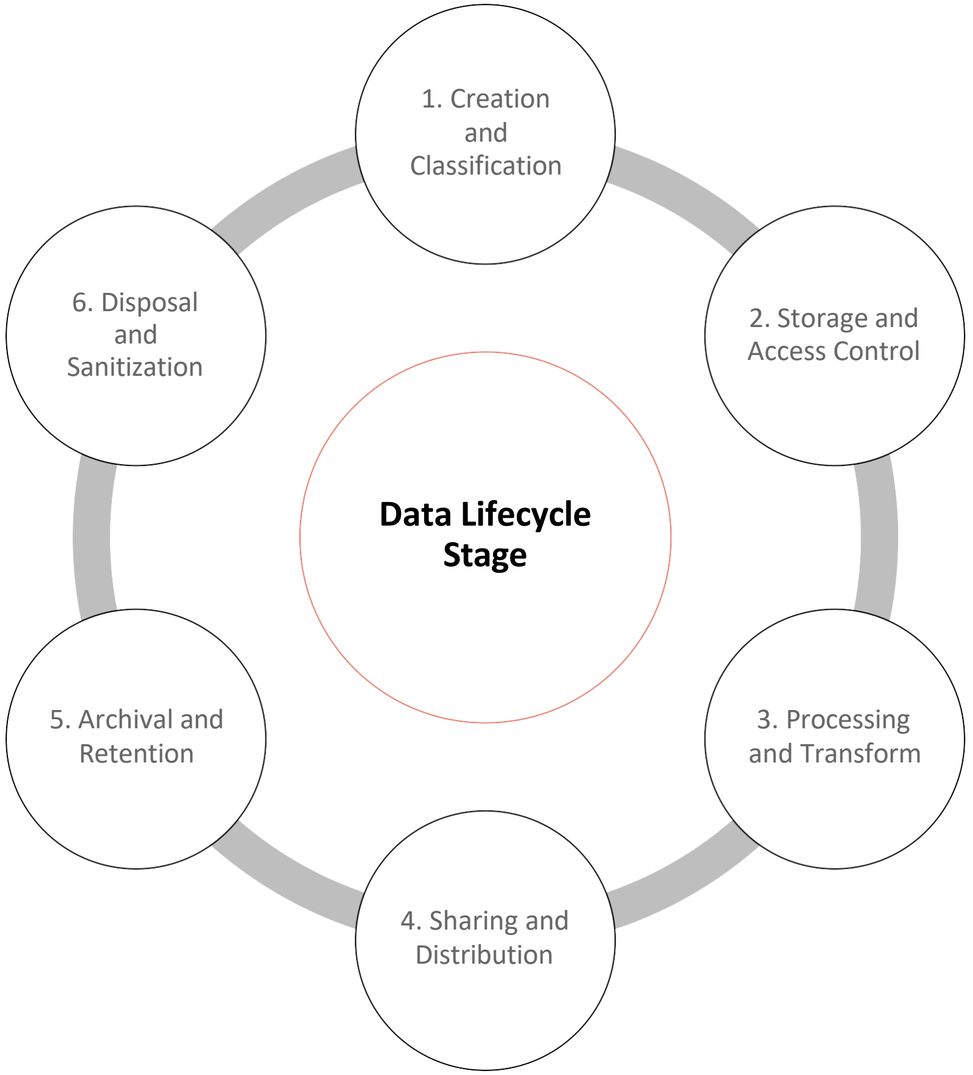
- Hardening audits + scoring
- Automated remediation & configuration control

# Data Remediation & Lifecycle Automation



**AUTOMATED REMEDIATION CAPABILITIES**

- Real-time encryption of sensitive data
- Dynamic data masking for non-production environments
- Automated redaction of PII in documents
- Intelligent data retention policy enforcement
- Secure deletion and sanitization workflows



# SOC Maturity Assessment and Transformation

| Maturity Assessment | Finding and Recommendation | Optimization | Transformation |
|---|---|---|---|
| **Phase 1**<br>SOC capability and maturity assessment across 5 domains.<br>That is business, processes, people, technology and service | **Phase 2**<br>Identify SOC capability and maturity gaps. Provide recommendations and optimization through transformation roadmap | **Phase 3**<br>Apply SOC capability and maturity recommendation for SOC optimization. | **Phase 4**<br>Execution of transformation program |

Maturity Tool

SOC Governance Program


SOC Charter

SOC Assessment Report

# Data Discovery and Classification Approach

| Formulization | Discovery | Classification |
|---|---|---|
| **Phase 1**<br>1. Establish a steering committee<br>2. Formulize data classification policy | **Phase 2**<br>1. Plan data discovery efforts<br>2. Implement data discovery plan | **Phase 3**<br>1. Classify the data<br>2. Maintain and optimize program |

Data Classification Inventory Tool

Steering Committee Charter
Classification Policy
Classification Standard
Data Classification RACI
User Data Handling Requirements

Develop a Classification Program

Data Discovery Interview Tracking

Incorporate human and technology-based tools to simplify discovery

Inventory Tool
Verification Tool
Metrics Tracking Tool
Awareness Pamphlet
Awareness Poster

Implement the classification program to ensure appropriate levels of protection

# Our CoreTeam



**CEO**
**Farhan Habib, MS(IS), LLB, TE**


**COO**
**Komal Batool, PhD Malaysia**

**CTO**
**Imran Makhdoom, PhD Aus**

**Technical Lead**
**Assad Anwaar**

**Business Development**
**Ayyda Sajid**

**Consultant**
**Abdul Rasheed, PhD China**

# THANK YOU ☺