SEYA
TECH

CYBERSECURITY · ARTIFICIAL INTELLIGENCE

Cyber defence for the AI era.

Services, white-label platforms and advanced attack simulation, from the team that has spent a decade on the front line.

A decade on the front line of cyber defence.

SEYA Tech has operated in cybersecurity for a decade, building deep experience across services, products and the people who run security inside large organisations. We combine both sides: senior hands-on services and our own platforms, delivered as one accountable partner.

EXPERIENCE

10 years in cyber

Defence, testing, response and governance for regulated, high-risk organisations.

LEADERSHIP

Led by a former CISO

Our cyber practice is headed by a former CISO of multiple organisations, with years of experience running security programmes.

PORTFOLIO

15 services · 15 platforms

From 24/7 MDR to red teaming, plus off-the-shelf and white-label products.

DEPLOYMENT

Cloud to air-gapped

Every platform runs in the cloud, in your private environment or fully air-gapped.

AI made attackers faster, cheaper and more convincing.

Generative AI removed the effort from reconnaissance, phishing and impersonation. Attacks are now more frequent, more personalised and move from first access to full compromise in minutes.

+89%

more operations by AI-enabled adversaries, year over year

CROWDSTRIKE 2026

29 min

average eCrime breakout time, with the fastest at just 27 seconds

CROWDSTRIKE 2026

16%

of breaches involved attackers using AI, mostly phishing (37%) and deepfakes (35%)

IBM 2025

82%

of detections were malware-free: attackers log in rather than break in

CROWDSTRIKE 2026

Sources: CrowdStrike 2026 Global Threat Report (Feb 2026); IBM Cost of a Data Breach Report 2025.

Your own AI is now part of the attack surface.

Employees paste sensitive data into public tools, AI agents receive broad permissions, and models can be manipulated. Most organisations adopted AI faster than they secured it.

- Data leakage into public LLMs and unsanctioned tools
- Prompt injection and jailbreaks against your chatbots
- Over-permissioned AI agents acting on real systems
- Deepfake voices and video approving payments

20%

of breaches involved shadow AI, adding about **$670,000** to the average breach cost

IBM 2025

97%

of organisations that reported an AI model or application breach lacked proper AI access controls

IBM 2025

63%

of breached organisations had no AI governance policy in place

IBM 2025

Source: IBM Cost of a Data Breach Report 2025 (with Ponemon Institute).

We fight AI with AI, and put experienced people in charge of it.

seya://simulate

SIMULATE

Attack like the adversary

AI-driven attack-simulation models that emulate today's advanced attackers, across network, cloud, identity, phishing and AI systems, and prove what is really exploitable.

seya://defend

DEFEND

Detect and respond at machine speed

An AI-assisted SOC and 24/7 MDR that triage every alert in seconds, with senior analysts approving every high-impact action.

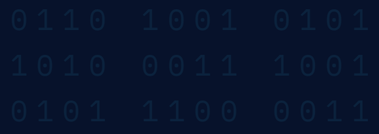
seya://govern

GOVERN

Secure the AI you adopt

An LLM firewall, agent permissions, AI red-teaming and governance, so the business can use AI without opening new doors.

Every automated action is logged, explainable and, where it matters, approved by a human analyst.



Advanced attack simulation, powered by AI models.

Our SEYA Specter platform and red team run continuous, intelligence-led attack simulations the way a real adversary would, then prove the impact and verify the fix. It is safe, controlled and repeatable after every change, not once a year.

01

Recon

Map exposed assets, leaked credentials and people as an attacker sees them.

02

Emulate

AI models reproduce real adversary techniques across network, cloud, identity and phishing.

03

Prove

Show the true attack path and business impact with evidence, not scanner noise.

04

Detect

Measure whether your SOC and controls actually caught each step.

05

Verify

Re-run the attack after remediation to confirm it is closed.

- Ransomware path validation
- Deepfake & vishing simulation
- AI / LLM red-teaming
- Purple-team exercises
- MITRE ATT&CK mapped

Round-the-clock defence, run by specialists.

24/7

Managed Detection & Response

Monitoring, threat hunting and containment across endpoint, network, identity and cloud. We act as your extended SOC.

BUILD · RUN

SOC-as-a-Service

Design, build and operation of a security operations centre, or a fully managed SOC with SIEM/SOAR engineering.

RETAINER · SLA

Digital Forensics & Incident Response

Rapid containment, forensic investigation, evidence handling and recovery, with defined response SLAs.

INDUSTRIAL

OT / ICS Security

Asset discovery, IEC 62443 segmentation and passive monitoring for plants, utilities, ports and buildings.

INTELLIGENCE

Threat Intelligence

Dark-web, credential-exposure and brand monitoring, turned into prioritised alerts and takedowns.

CONTINUOUS

Attack Surface & Vulnerability Mgmt

Continuous discovery of what you expose, with findings ranked by real exploitability.

Find the gaps first, then close them.

TEST

Penetration Testing

Web, mobile, API, network, cloud and wireless, with risk-rated findings and retest.

TEST

Red Team & Adversary Emulation

Objective-based, intelligence-led simulation across digital, human and physical layers.

RESILIENCE

Ransomware Readiness

Attack-path review, recovery testing, crisis playbooks and an executive exercise.

ARCHITECT

Cloud Security

AWS, Azure and GCP posture, identity and Kubernetes hardening.

ARCHITECT

Zero Trust Architecture

Identity-first access, micro-segmentation and a phased rollout to NIST SP 800-207.

ARCHITECT

AppSec & DevSecOps

Threat modelling, secure code and security built into CI/CD.

GOVERN

Regulatory Compliance & GRC

NCA, SAMA, UAE IA, CBUAE, DORA, NIS2, ISO 27001, SOC 2, PCI DSS.

GOVERN

vCISO & Advisory

Fractional CISO leadership, strategy, risk and board reporting.

PEOPLE

Awareness & Training

Phishing and deepfake simulations, role-based training and board drills.

Ready-to-deploy products, built by us.

sentry.triage

AI SOC

SEYA Sentry

An autonomous AI analyst that triages, investigates and contains alerts in seconds.

specter.attack

OFFENSIVE

SEYA Specter

A continuous AI adversary that proves what is exploitable and verifies the fix.

horizon.secure

CLOUD

SEYA Horizon

CNAPP for AWS, Azure, GCP and Kubernetes, with attack-path prioritisation.

identity.guard

IDENTITY

SEYA Identity

ITDR that stops credential theft, MFA bypass and lateral movement.

mailguard.filter

EMAIL

SEYA Mailguard

Behavioural defence against phishing, BEC and invoice fraud.

guardrail.protect

AI SECURITY

SEYA Guardrail

An LLM firewall, agent permissions and continuous AI red-teaming.

beacon.hunt

DIGITAL RISK

SEYA Beacon

Finds impersonation, phishing sites and leaks, then takes them down.

verify.human

DEEPFAKE

SEYA Verify

Detects deepfakes at onboarding, login and inside live calls.

Beyond the perimeter: fraud, intelligence and sovereign AI.

FRAUD

SEYA Aegis

Real-time fraud decisioning for every transaction, login and payee change.

FIN-INTEL

SEYA Nexus

A privacy-preserving risk network shared between institutions.

CRYPTO

SEYA Chain

Cross-chain tracing, wallet risk scoring and court-ready evidence.

OSINT

SEYA Prism

Hundreds of sources fused into one investigative graph.

NARRATIVE

SEYA Signal

Detects bot networks and coordinated disinformation campaigns.

AWARENESS

SEYA Sentinel

A live map of real-world events, with fake footage filtered out.

SOVEREIGN AI

SEYA Cortex

LLMs and agents that run entirely inside your own infrastructure.

ONE SUITE

Integrated or standalone

Every platform works alone or shares signals with the rest of the suite.

Your brand. Our engine.

Our platforms are available as white-label products. MSSPs, telcos, banks, system integrators and government agencies can offer advanced cyber protection to their own customers under their own name, without building it.

- MSSPs & MSPs
- Telcos & ISPs
- Banks (for their clients)
- System integrators
- National CERTs & agencies

BRAND

Fully rebranded

Your logo, colours, domain and reports. Your customers see you.

SCALE

Multi-tenant

Manage many customers from one console, each fully isolated.

SOVEREIGN

Deploy anywhere

Our cloud, your data centre or air-gapped, with data kept in-country.

ENABLE

Backed by our team

Training, pre-sales support and a Tier-3 SOC behind you.

Trusted where the stakes are highest.

Our clients include banks around the world, insurers, investment firms and government institutions, organisations that face the most capable attackers and the strictest regulators.

FINANCIAL

Banks worldwide

24/7 SOC, fraud and mule detection, red teaming and central-bank compliance.

FINANCIAL

Insurance

Cloud security, customer-data protection and readiness for regulatory audits.

FINANCIAL

Investment & asset managers

Executive and deepfake protection, BEC defence and due-diligence intelligence.

PUBLIC SECTOR

Government institutions

Sovereign SOC, sovereign AI, threat intelligence and disinformation monitoring.

CRITICAL

Critical infrastructure

OT/ICS security for energy, water, ports and transport.

ENTERPRISE

Enterprises & technology

Zero trust, AppSec, AI security and managed detection.

One accountable partner, from assessment to operation.

01

Assess

Risk, maturity and exposure, measured against recognised frameworks.

02

Architect

A target design and roadmap built around what you already own.

03

Build

Our engineers deploy, integrate and tune.

04

Deploy

Cloud, private or air-gapped, with handover and training.

05

Operate

24/7 managed service with clear SLAs and reporting.

MANAGED

MDR and SOC-as-a-Service with 24/7 coverage and SLAs.

PROJECT

Fixed-scope tests, assessments and architecture work.

RETAINER

On-call incident response and red-team capacity.

ADVISORY

vCISO, GRC and compliance leadership.

Aligned with the frameworks your regulator expects.

We map controls once and reuse the evidence across every framework that applies to you, so compliance becomes a continuous programme, not an annual scramble.

REGIONAL REGULATION

- NCA ECC
- SAMA CSF
- UAE IA
- CBUAE
- DORA
- NIS2

INTERNATIONAL STANDARDS

- ISO/IEC 27001
- SOC 2
- PCI DSS
- NIST CSF
- NIST SP 800-207
- IEC 62443

METHODOLOGY

- MITRE ATT&CK
- OWASP
- PTES
- CIS Benchmarks

Six reasons organisations choose us.

01

A decade of experience

Ten years of cyber work for demanding, regulated clients.

02

CISO-level leadership

Led by a former CISO who has sat in your seat.

03

Services and products together

Our own platforms, run by our own people. One partner, one SLA.

04

AI on both sides

We simulate AI-driven attacks and secure the AI you deploy.

05

Sovereign by design

Cloud, private or air-gapped, with your data staying where it must.

06

White-label ready

Resell our platforms under your brand, with our team behind you.

0110 1001 0101 1100 0011 1010 0110 1001 0101 1100 0011 1010

SEYA
TECH

NEXT STEP

Let's secure what comes next.

Book a briefing, a threat assessment or an attack-simulation demo, or ask about becoming a white-label partner.

EMAIL

info@seya-group.com

WEB

seya-tech.com/Cyber

CONFIDENTIAL · FOR DISCUSSION PURPOSES