IronProbe

CAPABILITY BROCHURE 2026

COMPREHENSIVE CYBERSECURITY & AI ASSURANCE

PROBE. HARDEN. DEFEND.

Offensive-led security, AI assurance, and governance for organizations defending intelligent systems against real-world adversaries.

OSCP · CREST CPSA/CRT · CISM · CRTP · NIST AI RMF · OWASP

WWW.IRONPROBE.NET

WHO WE ARE

01

OSCP

CREST CPSA/CRT

CISM · CRTP

We break systems the way real adversaries do.

IronProbe is an offensive-led security practice safeguarding applications, cloud environments, and machine-learning pipelines against adversarial attacks, data poisoning, and compliance gaps. We pair ethical AI frameworks such as the NIST AI RMF with hands-on technical defense — hardening cloud-hosted models, auditing training data for bias, and shutting down prompt-injection exploits before they reach production. Continuous dark web, brand, and Shadow AI monitoring keeps that visibility running between engagements.

Offensive-led

Red-team operators simulating real-world threat actors across the full kill chain.

AI-native

Specialised testing for LLMs, agents, and MCP integrations, plus discovery of unsanctioned Shadow AI across the enterprise.

Continuously monitored

Dark web, leak-site, and brand-impersonation monitoring that turns exposure into early warning.

Governance-aligned

Findings mapped to NIST AI RMF, OWASP, ISO 27001, SOC 2, PCI-DSS, and GCC and Indian regulatory frameworks.

13

SPECIALISED PRACTICES

12

FRAMEWORKS MAPPED

CREDENTIALS

OSCP · CREST CPSA/CRT · CISM · CRTP · NIST AI RMF · OWASP

02 · OUR APPROACH

Your future, our expertise.

We deliver measurable outcomes in security and compliance — helping organizations proactively assess their defenses and stay resilient against ever-emerging threats.

01 Highest standards
Tailored solutions that meet the strictest cybersecurity and compliance benchmarks.

02 Proactive defense
Assess and strengthen defense mechanisms before attackers find the gaps.

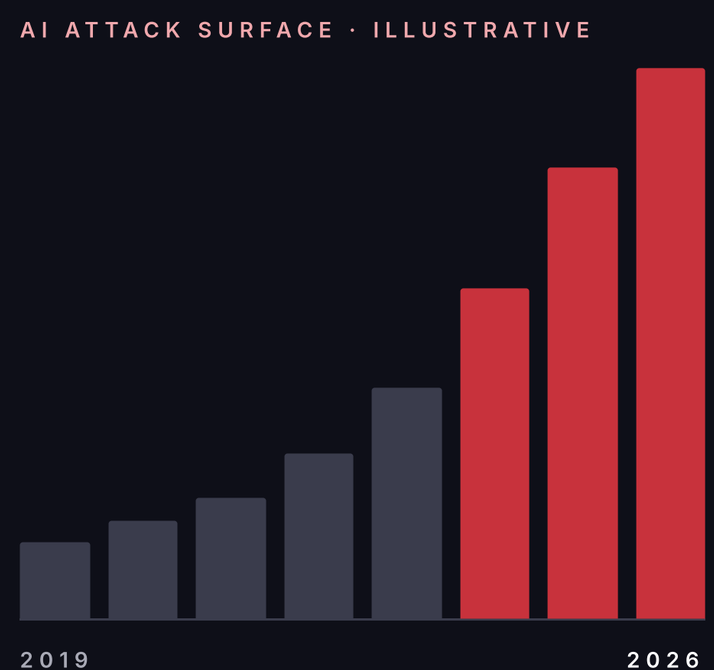
03 Real-world simulation
Red-team assessments that test the true effectiveness of your controls.

04 Operational continuity
Prevent attacks from disrupting the business and minimise costly downtime.

05 Hidden risk discovery
Surface and remediate vulnerabilities before they can be exploited.

06 Exposure management
World-class support to prioritise, patch, and remediate across your attack surface.

Enterprise adoption of generative AI is expanding the attack surface faster than traditional security can cover.



13 Our services

Thirteen specialised practices spanning offensive testing, AI assurance, continuous threat monitoring, cloud defense, compliance, and data privacy — deployed individually or as an integrated program.

04	AI Security Services	LLM · MCP · GOVERNANCE
05	Shadow AI Detection	NEW DISCOVERY · POLICY · ISO 42001
06	Blue Teaming & Secure Coding	SIEM · SDLC · HARDENING
07	Cloud Security Services	AWS · AZURE · GCP
08	Red Teaming & Adversary Simulation	MITRE ATT&CK
09	Incident Response & Insider Threat	DFIR · UEBA · DLP
10	Dark Web & Data Leakage Monitoring	DARK WEB · BREACH · RANSOMWARE
11	Brand Monitoring & Protection	NEW DOMAINS · IMPERSONATION · TAKEDOWN
12	Web Application Security	OWASP · API · DAST
13	Mobile Application Security	IOS · ANDROID · RASP
14	Compliance & Auditing	ISO · SOC 2 · GCC · DPDP
15	Cyber Due Diligence NEW	M&A · FUNDRAISING
16	DPDP Compliance NEW	CONSENT · RIGHTS · BREACH

PRACTICE

04

AI Security Services

We protect AI systems from adversarial attack, ensure compliance with global standards, and fortify the intelligence infrastructure underneath.

ASSESSMENT COVERAGE

- AI Agent & LLM Security Testing
- AI Red Teaming & Adversarial Testing
- AI Runtime Monitoring & Incident Readiness
- MCP & Tool Integration Security Assessment
- AI Security Risk Assessment
- AI Governance & Compliance Assessment
- AI Vendor & Third-Party Risk Assessment
- AI Architecture Security Review
- Secure AI Development (AI SDLC) Review
- RAG & Data Pipeline Security Assessment

WHERE AI BREAKS

INPUT
Prompt injection, jailbreaks & adversarial inputs

OUTPUT
Data leakage, unsafe & biased responses

MODEL
Poisoning, theft & supply-chain risk

AGENTS
Excessive agency & tool-integration abuse

NIST AI RMF

OWASP LLM TOP 10

ISO/IEC 42001

PRACTICE

05

NEW

Shadow AI Detection & Governance

Find every AI tool, model, and agent in use across the business, including the ones nobody approved. We map where sensitive data flows into public GenAI services and bring unsanctioned use under policy.

WHAT WE DISCOVER

Unsanctioned GenAI tools

Public chatbots, copilots and AI browser extensions used without approval.

Embedded SaaS AI

AI features switched on inside approved SaaS platforms and their data-sharing terms.

Rogue agents & MCP servers

Self-built agents, automations and MCP connectors with access to internal systems.

Exposed AI API keys

LLM provider keys in code repositories, CI pipelines and endpoints.

Sensitive data in prompts

Source code, PII, client and financial data sent to external models.

Unmanaged cloud AI

Model endpoints, notebooks and vector stores spun up outside governance.

TELEMETRY

- Proxy & DNS logs
- CASB / SSE
- Endpoint & browser
- SaaS OAuth grants
- Code repositories
- Cloud accounts

01 AI inventory

A living register of tools, models, owners and data classes.

02 Risk scoring

Each use case rated by data sensitivity, vendor terms and access.

03 Policy & controls

Acceptable-use policy, sanctioned alternatives and DLP rules.

ISO/IEC 42001

NIST AI RMF

DLP · CASB · SSE

PRACTICE

06

Blue Teaming & Secure Coding

Defensive services that detect, mitigate, and prevent threats — combining security monitoring, threat intelligence, and secure development to minimise vulnerabilities and build resilience.

COMPONENTS TESTED

Threat Detection & Monitoring

SIEM & real-time log analysis · UEBA validation · coverage across cloud, endpoints & networks · false-positive reduction.

Incident Response & Forensics

Rapid identification & containment · digital forensics & root-cause analysis · breach-impact assessment · recovery planning.

Secure Configuration & Hardening

Secure baselines · patch management & vulnerability mitigation · CIS benchmark alignment · continuous posture monitoring.

Endpoint & Identity Protection

Multi-factor authentication · EDR solutions · conditional-access policy assessment · Zero Trust identity controls.

Secure Coding Practices

Secure SDLC integration · threat modeling & code review · software composition analysis · secrets detection · secure API & input validation.

OUTCOME

A hardened, continuously-monitored environment where threats are caught early and remediated fast.

SIEM · UEBA · EDR

CIS BENCHMARKS

SECURE SDLC

PRACTICE

07

Cloud Security Services

End-to-end protection for AWS, Azure, and multi-cloud environments — threat detection, compliance automation, and Zero Trust architecture that secure everything from customer PII to AI training data.

Data Protection at Scale

Encryption, DLP & access governance for business-critical data.

Multi-Cloud Complexity

Centralised visibility & unified controls across AWS, Azure, GCP & hybrid.

Regulatory Compliance

Automated compliance checks, audits & policy enforcement.

CAPABILITIES

- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Mgmt (CIEM)
- IAM Governance & Privileged Access
- Container & Kubernetes Security
- Cloud Workload Protection (CWPP)
- API & Serverless Security
- Security Monitoring & Threat Hunting
- Compliance Automation & Audit Readiness
- Data Encryption & Key Management
- Incident Response & Forensics

AWS · AZURE · GCP

CIS · CSA CCM

ZERO TRUST

PRACTICE

08

Red Teaming & Adversary Simulation

We replicate real-world adversaries to assess your ability to prevent, detect, and respond — measuring true detection and response maturity across the full kill chain.

THE KILL CHAIN WE WALK

01	02	03	04	05	06	07
Recon	Initial Access	Execution	Persistence	Privilege Escalation	Lateral Movement	Impact & Exfiltration

ENGAGEMENT OBJECTIVES

01	Emulate Advanced Persistent Threats (APTs)
02	Validate security controls across the kill chain
03	Measure detection & response maturity (SOC capability)
04	Identify exploitable attack paths to critical assets
05	Test resilience against targeted, covert attacks

TECHNIQUES & FRAMEWORKS

MITRE ATT&CK TTP mapping	Cyber Kill Chain methodology
Threat-intelligence-driven scenarios	Identity & access attacks (AD, IAM abuse)
Endpoint & EDR evasion techniques	Cloud exploitation & misconfiguration
Web application & API exploitation	Threat hunting

MITRE ATT&CK

CYBER KILL CHAIN

TIBER-EU ALIGNED

SAMA FEER ALIGNED

PRACTICE

09

Incident Response & Insider Threat

Swiftly detect, contain, and remediate incidents while mitigating risk from malicious or negligent insiders — through rapid response, behavioral analytics, and proactive threat mitigation.

KEY FOCUS AREAS

01	**Threat Identification & Anomaly Detection**	AI-driven analytics to detect unusual activity and deviations, with behavioral alerts that flag insider threats early.
02	**Incident Response & Containment**	Rapid isolation of compromised systems to prevent lateral movement, plus automated real-time attack mitigation.
03	**Insider Threat Monitoring**	Continuous monitoring of privileged users and access patterns; detection of unauthorized data access and exfiltration.
04	**Endpoint Security & Hardening**	Proactive endpoint protection against unauthorized actions, integrated with Zero Trust and adaptive access controls.
05	**Data Loss Prevention (DLP)**	Real-time tracking of sensitive data movement, blocking unauthorized file transfers and email leaks.

DFIR

UEBA

DLP · ZERO TRUST

PRACTICE

10

EXPANDED

Dark Web & Data Leakage Monitoring

Continuous monitoring across the surface, deep, and dark web — turning exposed credentials and sensitive data into proactive threat intelligence before attackers exploit them.

Credential Leak Detection

Exposed employee, customer, admin & privileged account credentials.

Infostealer Log Monitoring

Session cookies and saved passwords harvested from infected employee and contractor devices.

Breach Database Monitoring

Leaked customer records, PII, financial data, source code & files.

Ransomware Leak-Site Monitoring

Detect if your organization or a key supplier appears on extortion or leak portals.

Initial Access Broker Tracking

Listings selling VPN, RDP or cloud access to your environment.

VIP & Executive Exposure

Track credential leaks and targeted exposure of executives & privileged users.

MONITORING CHANNELS

TOR MARKETPLACES

LEAK FORUMS

RANSOMWARE PORTALS

TELEGRAM & MESSAGING

PASTE SITES

CODE REPOSITORIES

01 Collect

Automated crawling plus analyst access to closed sources.

02 Validate

Analysts confirm each finding and remove noise and duplicates.

03 Alert

Prioritised alerts with context on source, actor and data affected.

04 Respond

Reset playbooks, takedown support and a monthly intelligence report.

IRONPROBE

PRACTICE

11

NEW

Brand Monitoring & Protection

Detect and remove the lookalike domains, fake profiles, cloned apps, and phishing campaigns that trade on your name — before customers and staff fall for them.

WHAT WE WATCH

Lookalike & Typosquat Domains

New registrations, homoglyphs and certificate issuance that imitate your domains.

Phishing Kits & Sites

Cloned login pages and kits targeting your customers or employees.

Social Media Impersonation

Fake brand pages, support accounts and fraudulent advertising.

Rogue Mobile Apps

Counterfeit or repackaged apps in official and third-party app stores.

Executive Impersonation

Fake executive profiles used for fraud, recruitment scams and BEC.

Brand Abuse in Fraud

Fake offers, tickets, loyalty schemes and customer-support numbers.

TAKEDOWN & RESPONSE

Evidence packs, registrar and hosting abuse reports, platform takedown requests, and tracking until each threat is removed.

BUILT FOR HIGH-IMPERSONATION SECTORS

Telecom, aviation, BFSI and retail brands where customer-facing fraud carries direct financial and reputational loss.

DOMAIN MONITORING

IMPERSONATION

TAKEDOWN

PRACTICE

12

Web Application & API Security

We simulate real-world attacks to uncover vulnerabilities, assess business impact, and deliver actionable remediation — black-box, grey-box and authenticated testing across the OWASP Top 10 and the OWASP API Security Top 10.

METHODOLOGY

01	In-depth analysis of services for vulnerabilities & misconfigurations	02	Exploiting vulnerabilities to assess impact on business data
03	Dynamic Application Security Testing (DAST)	04	Authenticated & business-logic testing
05	Vulnerable software component identification	06	OWASP Top 10 & OWASP API Security Top 10 analysis
07	Detailed reporting with risk ratings & remediation guidance	08	Prioritisation by severity & potential business impact
09	Collaboration on remediation planning & implementation	10	Recommended security controls & best practices

SEVERITY	SEVERITY	SEVERITY	SEVERITY
Critical	High	Medium	Low

OWASP TOP 10 · API

DAST · SCA

CVSS RATED

IRONPROBE

PRACTICE

13

Mobile Application Security

End-to-end protection for iOS, Android, and cross-platform frameworks — automated scanning plus manual penetration testing, then hardening with RASP, anti-tampering, and real-time threat monitoring in production.

Comprehensive Coverage

Real-time threat detection & protection for live mobile applications.

Code & Runtime Protection

Advanced code hardening & Runtime Application Self-Protection (RASP).

Production Monitoring

Continuous threat intelligence for apps in development and in production.

VULNERABILITY DISCOVERY

- Reverse-engineering vulnerabilities
- Runtime tampering & code injection
- Hardcoded secrets
- Certificate-pinning bypass
- Insecure API communication
- Rooted / jailbroken device exploitation

IOS · ANDROID

OWASP MASVS

RASP · ANTI-TAMPER

IRONPROBE

PRACTICE

14

EXPANDED

Compliance & Auditing

We help businesses navigate complex security frameworks, assess risk, and implement best practices — with detailed assessments, gap analysis, and actionable recommendations to meet global and regional regulatory requirements.

GLOBAL FRAMEWORKS

ISO 27001
Information Security Management System

ISO 27701
Privacy Information Management System

SOC 2
Service Organization Control — Security & Privacy

GDPR
General Data Protection Regulation

HIPAA
Health Insurance Portability & Accountability Act

PCI-DSS
Payment Card Industry Data Security Standard

GCC & INDIA

UAE IAS · Dubai ISR
UAE Information Assurance Standards and Dubai Information Security Regulation

Saudi NCA ECC
National Cybersecurity Authority Essential Cybersecurity Controls

SAMA
SAMA Cyber Security Framework and red-teaming requirements

DPDP Act
India Digital Personal Data Protection Act readiness

RBI
Cybersecurity and IT governance directions for regulated entities

SEBI CSCRF
Cybersecurity & Cyber Resilience Framework, including VAPT

Outcomes: reduced compliance risk & audit failures · improved governance & control maturity · faster audit readiness & certification · stronger data privacy & regulatory alignment · enhanced customer trust & confidence.

ISO 27001 · 27701

SOC 2 · PCI-DSS

GDPR · HIPAA

UAE IAS · NCA ECC

DPDP · RBI · SEBI

PRACTICE

15

NEW

Cyber Due Diligence

Technical evidence of a target company’s security posture for acquirers, investors, and their advisors — combining offensive testing with a dark web and leak scan to surface risks that affect valuation and deal terms.

ASSESSMENT SCOPE

External Attack Surface

Internet-facing assets, exposed services and misconfigurations.

Targeted Penetration Test

Testing of the systems that carry the deal value: core apps, cloud and identity.

Dark Web & Leak Scan

Leaked credentials, breached data and prior ransomware listings.

Brand & Domain Exposure

Impersonation, lookalike domains and active fraud campaigns.

AI & Shadow AI Review

How the target uses AI and where proprietary data has left the business.

Compliance Posture

Gaps against ISO 27001, SOC 2, DPDP and sector regulation.

ALIGNED TO THE DEAL TIMELINE

Pre-LOI

Outside-in scan with no access to the target required.

Confirmatory diligence

Scoped testing and evidence review under NDA.

Post-close

100-day remediation plan and integration risk review.

Deliverable: a board-ready risk memo that ranks findings by deal impact, alongside the full technical report.

M&A

FUNDRAISING

PRE-INVESTMENT

PRACTICE

16

NEW

DPDP Compliance Readiness

End-to-end readiness for India's Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025 — mapping personal data, closing consent and governance gaps, and proving your security safeguards hold up under real-world attack.

WHAT WE DELIVER

Personal Data Mapping

Inventory of personal data across apps, cloud, SaaS and vendors, mapped to purpose and owner.

Notice & Consent

Itemised notices, consent and withdrawal journeys, plus Consent Manager readiness.

Safeguards Validation

Encryption, access control, logging and backups — tested by our offensive team.

Breach Readiness

Board and user breach intimation playbooks, aligned with CERT-In timelines.

Processor Governance

DPDP clauses, due diligence and ongoing oversight of vendors processing personal data for you.

Rights & Retention

Access, correction, erasure and grievance workflows, with retention schedules.

HOW WE ENGAGE

Assess

Gap review against the Act and Rules, with a risk-ranked register.

Remediate

Policies, consent flows, contracts and controls built with your teams.

Assure

Safeguard testing, breach drills and audit-ready evidence on file.

Deliverable: a board-ready DPDP readiness report and remediation roadmap, backed by technical evidence.

DPDP ACT 2023

DPDP RULES 2025

ISO 27701 · CERT-IN

02 Our products

Two platforms we built and run ourselves — they turn our brand monitoring and DPDP compliance practices into continuous, client-facing tools.

01

BrandWatch

BRAND MONITORING · THREAT INTELLIGENCE

Finds lookalike domains, phishing sites, impersonation and leaked credentials, and scores every finding from 0 to 100.

Sources monitored	13, from certificate logs to dark-web feeds
Alerts	Email, Slack, Teams, webhooks
Pairs with	Practices 10 & 11

SEE PAGE 19 →

02

Praman

DPDP ACT 2023 · READINESS

Measures DPDP readiness, tracks every gap to closure, keeps the evidence, and runs data-principal requests against a 30-day SLA.

Coverage	23 controls across 9 DPDP domains
Attack surface	Scans of client-verified domains only
Pairs with	Practice 16

SEE PAGE 20 →

BUILT BY PRACTITIONERS

The same team that delivers our services builds these platforms, so they reflect how we actually test, monitor and assess.

IRONPROBE

PRODUCT

01

IN-HOUSE

BrandWatch

Our brand monitoring and threat intelligence platform — it finds lookalike domains, phishing sites, impersonation and leaked credentials, and scores every finding.

WHAT IT DOES

01 Lookalike domain discovery

Typosquats, homoglyphs and TLD swaps, enriched with DNS, WHOIS and TLS data.

02 Phishing detection

Login forms, credential posting, parked pages and reputation checks on suspect sites.

03 Mentions & exposure

News, social, code and threat feeds for brand, executive and credential leaks.

04 Explainable risk scoring

Every finding scored 0–100, with the reason behind each point.

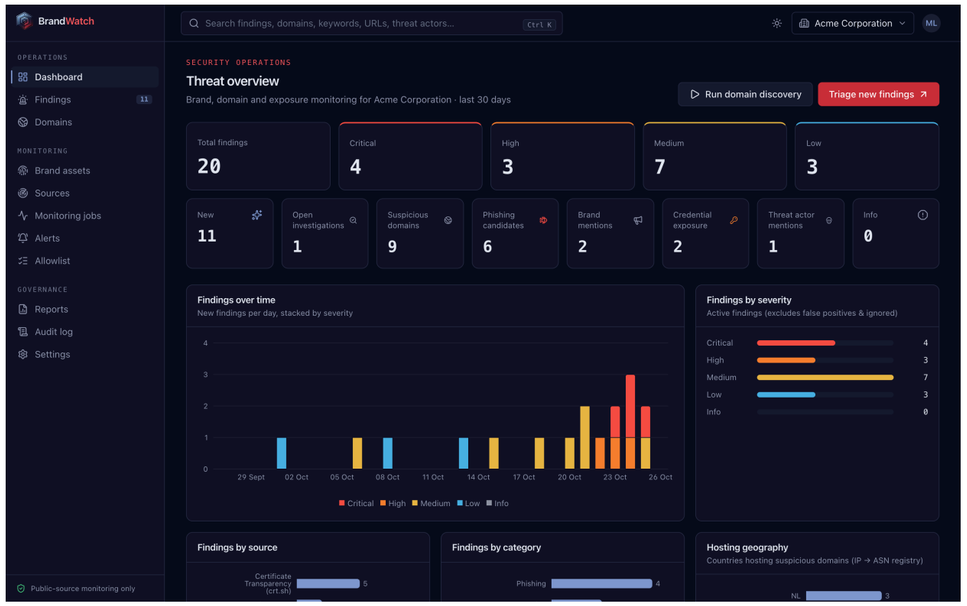
05 Analyst workflow

Triage, assignment, notes, evidence, a relationship graph and a full audit trail.

06 Alerts & reports

Email, Slack, Teams and webhook alerts; reports in PDF, CSV or JSON.

LIVE DASHBOARD



BrandWatch threat overview, shown with demo data for a fictional organisation.

SECURE BY DESIGN

Tenant isolation, role-based access, SSRF-safe fetching, encrypted secrets and a full audit log.

BRAND MONITORING

THREAT INTELLIGENCE

PHISHING DETECTION

IRONPROBE

PRODUCT

02

IN-HOUSE

Praman

Our DPDP Act 2023 readiness platform — measure compliance, close the gaps, keep the evidence, and answer data-principal requests on time.

WHAT IT COVERS

01 Readiness assessment
23 controls across 9 DPDP domains, scored into an overall readiness view.

02 Gaps & remediation
Every gap becomes a tracked remediation task, from open to done.

03 Evidence locker
Policies, notices and test results stored as proof of each control.

04 Data principal rights
Access, correction and erasure requests with a 30-day SLA countdown.

05 Readiness report
A board-ready summary of scores, priority gaps and progress.

06 Attack surface scan
Subdomain discovery, exposure scanning and credential-leak checks.

LIVE DASHBOARD



Praman compliance readiness dashboard, shown with demo data for a fictional organisation.

SCANS ONLY WHAT YOU OWN

Every scan is gated by a DNS ownership check, and each organisation's data is isolated from every other.

Pairs with: Practice 16, DPDP Compliance Readiness. Praman gives clients a live view of the gaps our assessment finds, and tracks them to closure.

DPDP ACT 2023

READINESS SCORING

ATTACK SURFACE

Trusted where the stakes are high.

From India’s financial services leaders to UAE fintechs, SaaS platforms and genetics labs, IronProbe secures the systems that hold customer money and patient data — against real adversaries and regulators alike.

INDIA · FINANCIAL SERVICES

Mahindra Finance

Red Teaming & Adversary Simulation

Red team engagement simulating real-world threat actors to test the organisation’s ability to prevent, detect and respond to targeted attacks across the kill chain.

DELIVERED

UAE · FINTECH

Gidea

Security Posture & CBUAE Compliance

Ongoing programme to strengthen Gidea’s cybersecurity posture and bring its controls in line with Central Bank of the UAE (CBUAE) regulatory standards.

ONGOING

UK & INDIA · LIFE SCIENCES

Datar Cancer Genetics

FDA Audit & Compliance

Security and compliance cover for Datar’s UK and India labs, with a complete audit conducted as per FDA guidelines and support in making the organisation FDA compliant.

FINTECH · SAAS

Finastra

End-to-End SaaS Security & PCI Compliance

Complete end-to-end ownership of security for Finastra’s SaaS product, with thorough compliance as per the latest PCI standards.

REGULATED-SECTOR EXPERIENCE

Offensive testing, audit and compliance for financial institutions and life-sciences labs.

ADVERSARY-GRADE DEPTH

Red-team capability proven against a large Indian financial services group.

ONE TEAM, MULTIPLE MARKETS

Delivery across India, the UK and the GCC, mapped to local and global regulators.

Led by practitioners.

Hands-on offensive security expertise, from the people who founded IronProbe and still lead its engagements.



FOUNDER

Sahib Oberoi

8 years across application security, DevSecOps, red teaming and compliance readiness, helping organisations find and fix what attackers would exploit.

OSCP · CREST CRT · CISM



FOUNDER

Pranjal Aswal

Specialises in offensive security tooling and offensive security operations, building the tools and running the engagements that test defences the way real adversaries do.

OSCP · CREST CRT · CRTP

IRONPROBE

Technical depth you can sell under your name.

For GRC, audit, and advisory firms: IronProbe adds red teaming, AI and LLM security, Shadow AI detection, mobile testing, and continuous dark web and brand monitoring to your existing client work. We don’t compete for your advisory engagements.

01

White-label delivery

IronProbe performs the testing under your brand. You own the client relationship and the report.

02

Co-branded offering

Joint propositions such as AI Governance + AI Red Team, sold and delivered together.

03

Mutual referral

Each side refers clients whose needs fall in the other’s core practice.

04

Joint bids

Combined teams for larger RFPs that need advisory and technical depth.

RECURRING REVENUE

Dark web, brand and Shadow AI monitoring as ongoing managed services.

SPECIALIST ADD-ONS

Red team and AI assurance attached to GRC, audit and CISO-advisory work.

GETTING STARTED

Mutual NDA, a one-page joint offering, and one named pilot.

LET'S TALK

Secure the future of your business.

Don't wait for an incident to expose the gaps. Talk to IronProbe about a tailored assessment across your applications, cloud, and AI systems.

EMAIL

business@ironprobe.net

PHONE

+91 74175 82987

WEB

www.ironprobe.net

OFFICE

Khasra no. 275, Westend Marg, Saidulajab, Saiyad Ul Ajaib Extension, Saket, New Delhi 110030