EJN LABS

G-Cloud 15 – Service Definition Document

Lot 3: Cloud Support for Continuous Threat Intelligence Monitoring: Proactive Data Leak Protection

bidteam@ejnlabs.com https://www.ejnlabs.com +44 020 4577 1740
EJN Labs, 44-45, Beaufort Court, Admirals Way, London E14 9XL

Table of Contents

Company Overview

EJN Labs are a UK cyber security company specialising in the delivery of AI enhanced offensive security services and threat intelligence. We offer flexible engagement models for individual projects and fully managed services through a unified and automated client portal.

Our focus is to support organisations of all sizes to strengthen their cyber resilience and respond effectively to emerging threats. EJN Labs can support clients across regulated sectors and critical infrastructure, as well as non-regulated businesses that recognise the importance of proactive defence. By prioritising accessibility and efficiency, we help organisations avoid unnecessary time investments and ensure cyber protection is within reach, regardless of budget or complexity. Every solution is tailored to fit our client's unique risk profile, operational demands, and long-term goals.

Services Offered

Our service portfolio includes:

- Penetration Testing and Vulnerability Assessments
- Red Teaming, Purple Teaming and Adversary Simulation
- AI-Augmented Threat Modelling
- **Managed Services:**
  - Bug Bounty Programmes
  - **Breach Hunter Threat Intelligence and Take Down Monitoring Managed Service (for companies, HNWIs and persons of interest)**
  - Attack Surface Monitoring (ASM) Managed Service
  - Purple Teaming Managed Service

Mission

Our mission is to reshape the future of cyber defence by combining cutting-edge technology with research led expertise to deliver outcomes that are not only smarter but leaner and faster. By applying clarity, precision and continuous innovation, we help organisations achieve intelligent, adaptive and resilient security strategies that reduce operational complexity, lower costs, and save valuable time. Every solution is designed to accelerate response, streamline resources and strengthen cyber posture.

Contact Us

Please contact us at EJNLabs.com or bidteam@ejnlabs.com for a demo of our platform or more information.

1. Continuous Threat Intelligence Monitoring

EJN Labs delivers continuous Cyber Threat Intelligence Monitoring Managed Service that eliminates the risk of missed data leaks. Our service provides daily scanning across clear, deep, and dark web sources, ensuring ongoing visibility of emerging threats. Unlike traditional periodic checks, we offer proactive alerts, enriched intelligence, and expert guidance to help organisations act before incidents escalate.

Combined with optional Takedown Support and Attack Surface Monitoring (ASM), these additional managed services give you peace of mind and measurable risk reduction.

EJN Labs is committed to strengthening your security posture and protecting both corporate and individual assets from emerging threats. Our managed service ensures continuous visibility, expert guidance, and measurable risk reduction.

1.1 Pricing and Commercials

EJN Labs Continuous Threat Intelligence Monitoring services is on a Subscription Model. Our Annual managed service starts at £3,500/year and for the same scope we offer a multi-year discount at £9,000/year for 3-year contracts.

- Optional Takedown Service: Priced separately based on scope (phishing/impersonation takedowns and data broker removals).
- Optional Attack Surface Monitoring (ASM): Priced separately based on scope.
- Optional Consultancy: Available at £1,000/day for bespoke threat modelling, integration workshops, or advisory sessions.
- All Prices: Exclude VAT and expenses.
- Invoicing & Payment: Annual or agreed milestones; 30-day terms aligned to G-Cloud Call-Off Contract

Service	1 Year	3 Years
TI Monitoring Managed Service (Up to 5 emails) *Sample Reports available	£3,500	£9,000
Per additional emails includes onboarded	£25 per email	£75 per email
Optional Consultancy (per day)	£1,000	£1,000
Optional Takedown Service	Priced separately based on scope	
Optional Attack Surface Monitoring (ASM)	Priced separately based on scope	

1.2 Key Service Offering and Benefits

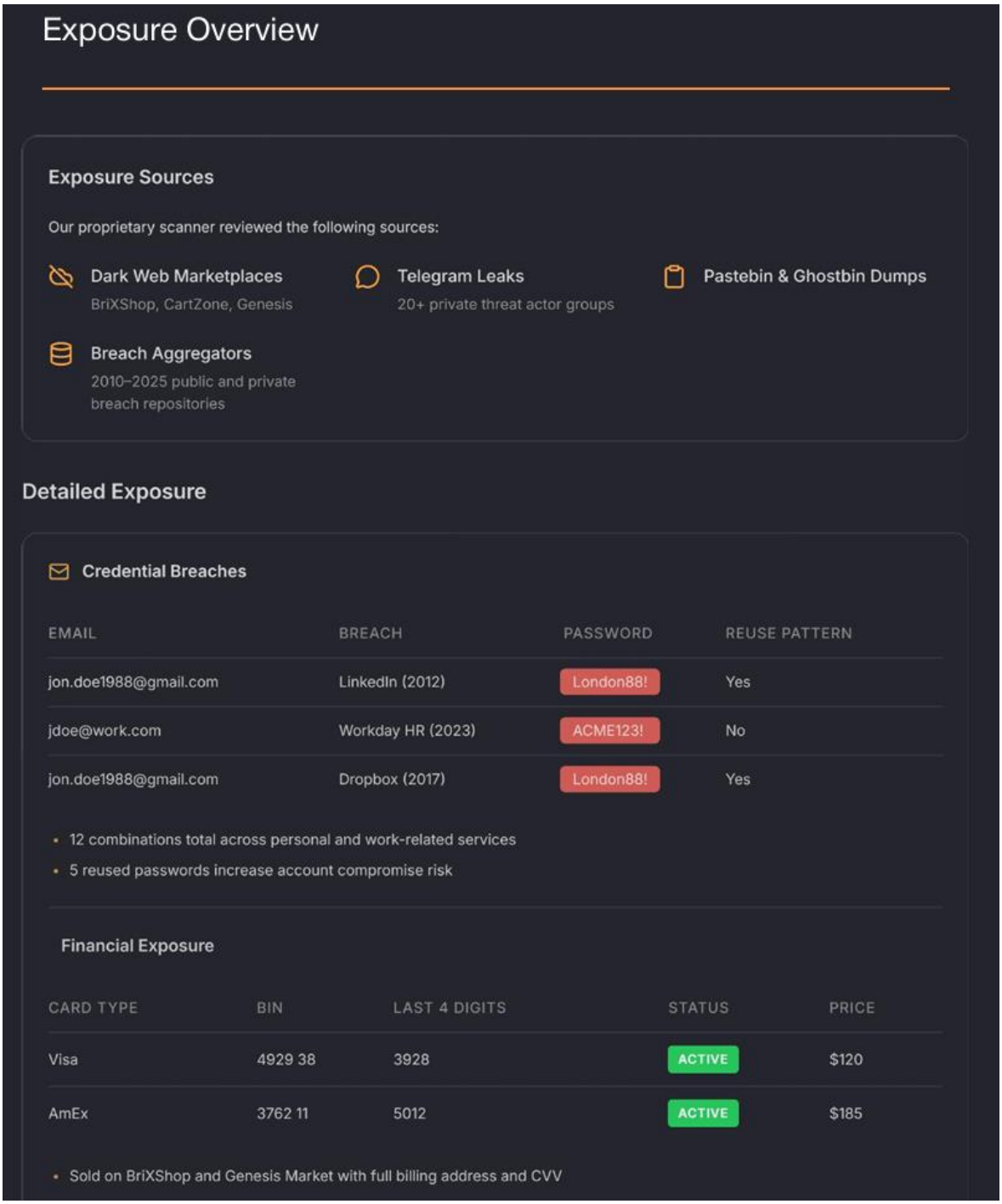
- **Continuous monitoring** of domains, IP ranges, email addresses, and identifiers to provide ongoing visibility into external threats.
- **Daily scans and contextual enrichment** to validate findings and reduce false positives.
- **Alerts for leaked credentials and sensitive data**, enabling early detection of breaches and impersonation attempts.
- **Threat intelligence correlation across multiple sources** (clear web, dark web, paste sites) for actionable insights and risk reduction.
- **Executive and technical reporting** to support strategic decision-making and operational response.
- **Integrated advisory support** for remediation steps and alignment with organisational risk priorities.
- **Secure client portal** offering centralised access to alerts, dashboards, and historical reports.
- **Flexible onboarding** via structured scoping questionnaire to ensure tailored monitoring scope.
- **Compliance alignment** with ISO 27001, GDPR, and NCSC principles for assurance and governance.
- **Optional:**
    - **Takedown Service**:
        - Erase personal information from 420+ data brokers.
        - Automate hundreds of removals to reduce exposure to scams and fraud.
        - Support phishing and impersonation takedown requests to minimise reputational damage.
    - **Attack Surface Monitoring (ASM) -** See Section 2.2

1.3 Delivery Process

1. **Scope & SoW**: Define monitored assets (domains, IP ranges, email addresses, staff identifiers, social handles) plus optional Takedown and Attack Surface Monitoring (ASM) requirements.
2. **Kick-Off:** Complete Scoping Questionnaire, confirm rules of engagement, set up secure portal access, and agree alerting/reporting cadence.
3. **Monitoring:** Continuous daily scans across clear web, dark web, paste sites, and threat intelligence feeds; enrichment and validation of findings.
4. **Reporting:** Monthly summary reports and quarterly executive reports; ad-hoc reports for critical exposures (to be confirmed by client).
5. **Advisory Support:** Ongoing guidance on remediation steps and risk prioritisation.
6. **Close-Out:** Export of all reports and alerts, transfer of watchlists, and secure deletion of client data.

1.4 SLAs and Working Terms

- Office Hours: Monday to Friday 09:00–17:30 (UK) excluding national holidays
- Consultant Working Day: 8 hours (excluding travel/lunch)
- Support Hours: Mon–Fri, 08:30–17:30 (UK); 1-hour response in hours; reasonable-effort out of hours (unless 24/7 agreed at call-off)
- Travel & Subsistence: remote default; on-site by request, charged at cost
- Professional Indemnity Insurance: included in day rates



2. Managed TI & ASM Approach

2.1 Threat Intelligence (TI) and Take Down Monitoring Managed Service

Threat intelligence helps organisations anticipate, detect and defend against emerging cyber threats. EJN Labs provides actionable intelligence by tracking malicious actors, identifying indicators of compromise and transforming raw threat data into meaningful insights.

Optional Take Down is also available as a managed service, and includes removal of Online personal information on legal sites only:

- Erase personal information from 420+ data brokers
- Run hundreds of removals on autopilot
- Reduce exposure to spam, scams & fraud

2.1.1 What This Service Is

Our threat intelligence service delivers curated, relevant information about threats that matter to your organisation. This can include tactical indicators for detection, operational insight into campaigns, and strategic trends to support risk decisions and security investment.

2.1.2 What We Assess

- Indicator and campaign tracking relevant to your sector and technology stack
- TTP analysis and mapping to defensive controls
- Prioritised alerts and reporting tailored to your risk profile
- Support for incident response and threat hunting activities
- Recommendations to improve detection and resilience based on observed threats

2.1.3 How the Work Is Performed

We collect and analyse threat data from multiple sources, enrich and validate it, and deliver outputs in formats that integrate into security operations. Where needed, we provide guidance on how to operationalise intelligence for detection, response and prevention.

2.1.4 Why This Matters

Good intelligence reduces uncertainty and helps teams focus on credible risk. It supports earlier detection of compromise, improves hunting and response, and helps organisations stay aligned with evolving attacker methods.

2.2 Optional Attack Surface Monitoring (ASM) Managed Service

Attack surface monitoring continuously discovers, inventories and monitors external-facing assets to find dangerous exposures before attackers do. The service tracks newly created hosts, certificates, misconfigurations and public data leaks, and delivers prioritised alerts and remediation guidance.

2.2.1 What This Service Is

Attack surface monitoring provides ongoing visibility into your organisation's digital footprint. It identifies unknown or unmanaged assets, monitors changes, and helps ensure exposures are addressed promptly and consistently.

2.2.2 What We Assess

- Continuous external asset discovery and inventory management
- Monitoring for new hosts, subdomains, certificates and exposed services
- Identification of misconfigurations and publicly accessible data exposure
- Alerting for high-risk changes and newly discovered exposures
- Prioritised remediation guidance to reduce time-to-fix

2.2.3 How the Work Is Performed

We continuously monitor your footprint and surface changes and exposures with actionable alerts. Findings are prioritised to help teams address the most important risks first, and to reduce the chance that unknown assets become attack paths.

2.2.4 Why This Matters

Organisations change constantly, and attackers look for what is new, forgotten or misconfigured. Continuous monitoring helps reduce blind spots, improve hygiene, and lower the risk of opportunistic compromise.

2.3 Accreditations & Memberships

EJN Labs hold the below accreditations and memberships

- ISO 27001, ISO 9001
- CREST aligned delivery
- Cyber Essentials (Basic) and Cyber Essentials Plus
- UK Cyber Security Council member

EJN LABS

bidteam@ejnlabs.com
https://www.ejnlabs.com
+44 020 4577 1740
EJN Labs, 44-45, Beaufort Court, Admirals Way, London E14 9XL