EJN LABS

G-Cloud 15 – Pricing 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

Why Choose EJN Labs for 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, this service gives 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**.

Key differentiators include:

- Continuous monitoring of domains, IP ranges, email addresses, and identifiers.
- Contextual enrichment and prioritisation to reduce false positives.
- Integrated advisory support for remediation and strategic risk decisions.
- Optional automated takedown service for phishing and data broker removals.
- Secure client portal for alerts, dashboards, and historical reports.
- Compliance alignment with ISO 27001, GDPR, and NCSC principles.

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.

Annual Pricing:

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

- **Daily monitoring of domains, IPs, emails, identifiers** providing continuous visibility into external threats
- **Alerts for leaked credentials and sensitive data** providing early detection of credential leaks and impersonation
- **Threat intelligence correlation across multiple sources** reducing risk through actionable intelligence
- **Executive and technical reporting** supporting strategic decision-making
- **Optional takedown support** to help minimises reputational damage
- **Advisory on threat intelligence scope** to align monitoring with organisational risk
- **Secure client portal** providing centralised access to alerts and reports
- **Flexible onboarding via scoping questionnaire** to ensure tailored monitoring scope

Terms, SLA's and Delivery Process

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

Pricing and Commercials

- Subscription Model: Annual managed service at £3,500/year; 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).
- Additional 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

Delivery Process

1. Scope & SoW: Define monitored assets (domains, IP ranges, email addresses, staff identifiers, social handles) and optional takedown 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.

Accreditations & Memberships

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

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