G-Cloud 15 – Service Definition Document

Lot 3: Cloud Support for Red, Purple & Adversary Simulation

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

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
- AI-Augmented Threat Modelling
- **Red Teaming and Purple Teaming and Adversary Simulation**
- Advanced Testing and Monitoring Services
  - Attack Surface Monitoring (ASM) Managed Service
  - Bug Bounty Programmes
  - 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 testing platform or more information.

Advanced Testing Services

EJN Labs adopts hybrid methodology that combines advanced AI-driven tooling with deep manual expertise. Our technology is built to support, not replace, the work of experienced security testers. By incorporating behavioural analytics, predictive modelling, and contextual intelligence, we help clients detect vulnerabilities with greater precision, speed, and strategic relevance. This blend of technical depth and intelligent automation delivers tailored security programmes aligned to each organisations risk landscape. All services follow recognised global standards such as OWASP, NIST, CREST and CHECK, and are delivered by seasoned professionals with deep operational expertise.

Please refer to Sections 1–4 for a detailed overview of our Red, Purple & Adversary Simulation Services and descriptions of each of the services listed below.

Section	Type	Service
1.	Adversary Simulation & Detection (Red and Purple Teaming)	• Red Teaming • Purple Teaming
2.	Managed Bug Bounty (Cloud)	• Managed Bug Bounty Programme
3.	Managed TI & ASM	• Threat Intelligence (TI) and Take Down Monitoring Managed Service • Attack Surface Monitoring (ASM) Managed Service

Our Service Advantages

- Free Unlimited Retesting to verify fixes and confirm remediation effectiveness
- Free unlimited rescheduling to accommodate development timelines & operational changes
- Ongoing expert support to clarify findings and provide guidance beyond the final report
- No extra charge for out-of-hours work. where required, to minimise business disruption
- No cancellation fees, allowing you to plan security testing without commercial pressure

What You Receive

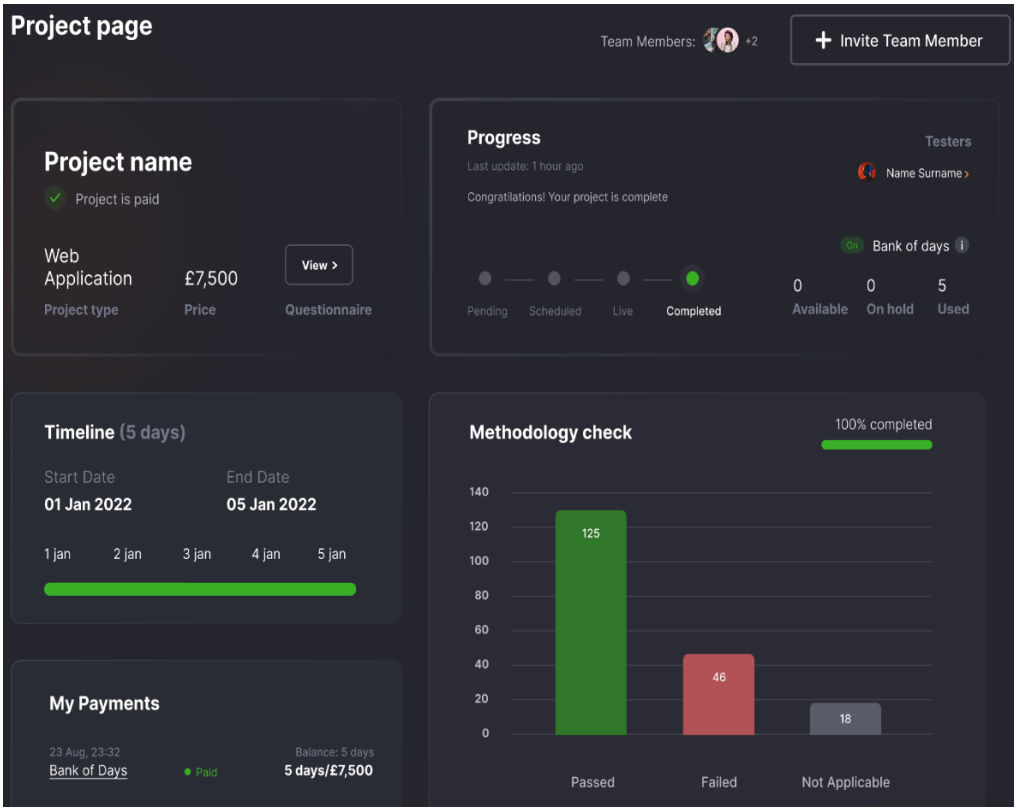
EJN Labs provide **24-hour turnaround of 3x tailored actionable reports** (Management, Technical and Client facing). Our reports include:

- An executive summary outlining overall risk and key findings
- Clear scope and methodology notes for assurance and audit purposes
- Detailed descriptions of identified issues (or observations), written for technical and non-technical stakeholders
- Evidence and reproduction steps where applicable
- Risk ratings based on real-world impact and likelihood
- Prioritised remediation guidance and recommended next steps

Service Delivery

EJN Labs is committed to excellence, transparency and agility in every engagement we offer:

- **A fully integrated client portal** providing threat prioritisation dashboards and complete test visibility and **Onboarding and initiation of testing within 24 hours**



1. Benefits of EJN Labs Red, Purple & Adversary Simulation Services

EJN Labs' Red Teaming, Purple Teaming, and Adversary Simulation engagements are engineered to provide measurable uplift across an organisation's detection, response, resilience, and overall cyber defence maturity. By combining deep offensive tradecraft with collaborative defensive enhancement, our approach ensures that security teams are tested rigorously and empowered to continuously improve.

Each of the benefits below reflects our commitment to delivering intelligence-led, technically robust, and outcome-driven exercises tailored to your operational environment and strategic objectives.

1.1 Key Benefits

- **Real-Time Collaboration (Purple Teaming):** We work alongside your defensive teams during Purple Team engagements, enabling immediate feedback loops, contextual learning, and iterative optimisation of detections, playbooks, and response processes. This ensures security teams develop and validate detection logic in real time.
- **Threat-Led Red Teaming (Adversary Simulation / Red Team):** Our Red Teaming engagements emulate realistic threat actors using current, sector-specific intelligence, attacker TTPs, and MITRE ATT&CK mapping. This provides an authentic simulation of advanced adversaries, beyond generic penetration testing and enabling organisations to understand true resilience across people, processes, and technology.
- **Full Attack Chain Coverage:** Our engagements span the full lifecycle of adversary behaviour ensuring organisations gain end-to-end visibility of exposures, blind spots, and response capability.
    - Reconnaissance & OSINT
    - Social engineering & human compromise
    - Initial access
    - Privilege escalation
    - Lateral movement
    - Persistence
    - Objective execution
    - Data exfiltration simulation (safe & controlled)
- **Continuous Assurance & Improvement:** To supports long-term resilience rather than one-off testing at EJN Labs our Red and Purple Team engagements include:
    - Free retesting to validate remediation
    - Unlimited advisory throughout the engagement
    - Flexible scheduling around operational constraints
    - Post-engagement workshops to ensure uplift is embedded
- **Strategic & Actionable Insight:** Our reporting combines deep technical detail with clear executive-level interpretation allowing technical teams and senior leadership to make informed, risk-based decisions. Deliverables include:

- MITRE ATT&CK coverage and detection matrix
- Threat narrative and kill-chain walk-through
- Targeted remediation roadmap
- Risk-aligned recommendations
- Maturity scoring & capability benchmarking

- **Scalable, Modular & Repeatable Programmes:** EJN Labs offers flexibility and alignment to your roadmap, SOC evolution, and control maturity goals as our Red, Purple, and Adversary Simulation services can be delivered as:
  - One-off assessments
  - Quarterly assurance cycles
  - Annual maturity uplift programmes
  - Continuous Purple Team subscriptions

1.2 EJN Labs Tooling & Technology Integration

EJN Labs leverages a modern ecosystem of offensive security tooling, automation, and intelligence platforms to ensure precision, efficiency, and realism throughout engagements. Our approach blends proprietary tooling with industry-standard frameworks.

- **EJN Breach Hunter (Threat Intelligence & Adversary Mapping):** Our in-house Breach Hunter platform ensures Red and Purple Team engagements are intelligence-led and aligned with credible adversary behaviours and enriching security testing with:
  - Real-time threat intelligence correlation
  - Actor profiling and TTP mapping
  - External footprint enrichment
  - Command-and-control visibility (safe simulation)
- **AI-Augmented Threat Modelling:** We leverage machine learning models to transform threat modelling into a dynamic, data-driven process to:
  - Identify likely attack paths
  - Prioritise based on impact, exploitability, and defensive visibility
  - Highlight choke points in your environment
  - Support faster and more accurate remediation planning
- **Adversary Simulation Frameworks:** For Red Teaming and adversary simulation engagements, to ensure realistic but controlled replication of hostile behaviours EJN Labs integrate:
  - Custom TTP automation
  - Safe C2 channels
  - Malware-less execution
  - Endpoint-evasive techniques
  - MITRE ATT&CK alignment
- **Attack Surface Management (ASM) Integration – Optional Add-On:** To enable a holistic understanding of both internal and external attack paths EJN Labs optional ASM platform provides:
  - Continuous external reconnaissance
  - Exposure and misconfiguration discovery
  - Monitoring for shadow assets, cloud drift, or leaked credentials
  - Integration with Red/Purple Team findings

1.3 Tailored to Your Security Maturity

Our **Core, Pro, and Enterprise** tiers offer scalable, threat-led engagements that align with your existing tooling, team structure, and business objectives and help you uncover blind spots, validate assumptions, and accelerate your security maturity through collaborative, real-time testing.

EJN Labs Tiered Services	
Core Level 1:	**Baseline Validation**
Estimated Duration:	10–12 Days (£12,500 - £15,000 + VAT)
Target Audience:	Organisations building foundational detection capabilities.
Scope:	➢ Limited MITRE ATT&CK TTPs ➢ Focus on visibility and basic detection validation ➢ Training-oriented engagement for blue teams
Technical Focus:	➢ Credential access, privilege escalation, basic lateral movement ➢ Endpoint and identity telemetry validation
Deliverables:	➢ Technical findings report ➢ Detection coverage map ➢ Remediation guidance
Pro Level 2:	**Capability Enhancement**
Estimated Duration:	20–24 Days (£25,000 - £30,000 + VAT)
Target Audience:	Organisations with operational SOC or IR functions.
Scope:	➢ Broader TTP coverage across the kill chain ➢ Sector-specific threat modelling
Technical Focus:	➢ Full kill chain simulation ➢ Playbook validation and automation readiness
Deliverables:	➢ Combined technical and strategic report ➢ Detection effectiveness metrics ➢ Recommendations for playbook refinement ➢ Retest validation roadmap
Enterprise Level 3:	**Strategic Resilience**
Estimated Duration:	30–36 Days (£37,500 - £45,000 + VAT)
Target Audience:	Mature organisations with advanced detection and response capabilities.
Scope:	➢ Deep adversary emulation across multiple threat scenarios ➢ Use of Breach Hunter TI platform and ASM insights ➢ Focused testing on stealth, persistence, and evasion techniques
Technical Focus:	➢ Advanced lateral movement, data staging, exfiltration ➢ Cloud and hybrid infrastructure coverage ➢ Threat actor simulation based on real-world campaigns ➢ Anti-Virus Bypass Exercises
Deliverables:	➢ Executive-level debrief and thematic analysis ➢ Strategic and operational recommendations ➢ Technical report detailing TTPs, detection outcomes, and response quality ➢ Business risk reduction summary

2. Red Teaming, Purple Teaming & Adversary Simulation Methodology

EJN Labs delivers threat-led, outcome-driven exercises that validate and uplift organisational cyber resilience across people, process, and technology.

Our unified methodology ensures realism (adversary emulation), safety (strict RoE), collaboration (purple loop), and measurable improvement against recognised frameworks (e.g., MITRE ATT&CK, CBEST/GBEST principles, TIBER-EU/UK, and NCSC guidance).

- Red Teaming,
- Purple Teaming
- Adversary Simulation

While each service has distinct goals and operating modes, all follow the same structured lifecycle, adapted to covert versus collaborative needs and agreed business objectives. Our approach is designed to be scalable, measurable, and repeatable, delivering strategic insights, technical depth, and continuous assurance.

2.1 Planning & Objectives (All Services)

- **Define business-aligned outcomes** and measurable criteria (e.g., MTTD, MTTR, dwell time, alert fidelity, containment time, data access prevention).
- **Establish Rules of Engagement (RoE):** legal authorisations, change freezes, test windows, safety breakpoints, stop conditions, escalation paths.
- **Scope & constraints:** in-scope systems/cloud tenants, third-party dependencies, operational constraints, out-of-bounds systems.
- **Communication model:**
  - Red/Adversary Simulation: covert by default; minimal-need escalation channel agreed.
  - Purple: collaborative by design; daily touchpoints and live feedback loops.

2.2 Threat Intelligence, Modelling & ATT&CK Alignment (All Services)

- **Adversary selection:** sector-relevant actors (state-sponsored, cyber-criminal, insider, hacktivist) with current TTPs.
- **Kill-chain mapping**: prioritise techniques across identity, endpoint, network, SaaS/M365, and cloud (Azure/AWS/GCP) layers.
- **Hypothesis-driven design:** define and test hypotheses (e.g., credential access paths, lateral movement routes, exfiltration vectors, privilege escalation choke points).
- **EJN Labs capabilities:**
  - Breach Hunter TI Platform for real-time enrichment, actor profiling, and TTP mapping.
  - AI-Augmented Threat Modelling to prioritise likely attack paths by likelihood, impact, and defensive visibility.

2.3 Reconnaissance, OSINT & Attack Path Development (All Services)

- **Digital footprinting & OSINT:** emails, domains, exposed services, leaked credentials, shadow IT, cloud footprints.
- **External attack surface:** optional **ASM integration** to validate exposures, misconfigurations, orphaned assets.
- **Initial access planning:** phishing/social engineering design (where authorised), cloud identity abuse routes, third-party vectors, supply-chain considerations.
- **Operational playbooks:** prepare technique chains and safety controls for stealth, evasion, and rollback.

2.4 Telemetry Baseline & Detection Readiness (Primarily Purple; Optional in Red/Adversary)

- **Document current telemetry:** EDR/EPP, SIEM, NDR, identity, cloud logs; validate ingestion, parsing, time sync, and alert routing.
- **Baseline alert behaviour:** distinguish signal vs noise; map detections against planned ATT&CK techniques.
- **Readiness gates:** confirm that safety monitoring and emergency contacts are active before execution.

2.5 Controlled Execution (Service-Specific Modes)

- **Red Teaming (Covert, Goal-Oriented):**
  - Initial access (phishing, credential abuse, external footholds).
  - Privilege escalation (exploits, misconfigurations, token abuse).
  - Lateral movement (AD abuse, remote execution, cloud pivots).
  - Persistence (scheduled tasks, SSO/refresh tokens, authorised C2).
  - Objective execution (domain dominance, data access, controlled exfiltration simulations).
  - Evasion (living-off-the-land, low-and-slow, artefact minimisation).
- **Adversary Simulation (Scripted Emulation):**
  - Pre-selected TTPs executed to mirror a named actor or campaign.
  - Focus on fidelity to adversary tradecraft, timing, and sequencing.
  - May be **overt or covert** depending on objectives.
- **Purple Teaming (Collaborative, Transparent):**
  - Execute TTPs in **phased steps** with the Blue Team present.
  - Observe detections in real time; tune SIEM/SOAR/EDR rules; iterate.
  - Validate playbooks and runbooks end-to-end.
  - All execution is **non-destructive**, safety-checked, and adheres strictly to the agreed RoE.

2.6 Collaboration (Purple Teaming)

The below is for Purple Teaming, however, in Red/Adversary exercises, this loop can be run post-engagement or with a limited audience to preserve realism.

- **Real-time feedback:** defenders share visibility; EJN iterates TTPs to confirm detection/coverage.
- **Detection engineering:** develop/tune rules, analytics, and enrichment; reduce false positives; improve response speed.

- **Knowledge transfer:** walkthroughs, "show-your-work" artefacts, and micro-workshops to embed learning.

2.7 Analysis, Reporting & Business Translation (All Services)

- **Technical deep-dive:** full kill-chain narrative, artefacts, and evidence.
- **ATT&CK mapping:** techniques executed, detections observed, and gaps identified.
- **Risk & remediation:** prioritised fixes, hardening guidance, and dependency mapping.
- **Metrics & outcomes:** MTTD/MTTR deltas, dwell time, coverage %, alert fidelity improvements.
- **Executive summary:** business risk language, impact on critical services, maturity uplift roadmap.

2.8 Assurance, Retesting & Continuous Uplift (All Services)

- **Free retesting** to validate remediation outcomes.
- **Follow-on Purple sessions** to convert Red/Adversary findings into detections and playbooks.
- **Quarterly/annual cycles** or **continuous Purple** programmes to maintain assurance.

2.9 Governance, Legal & Safety Controls (All Services)

- **Authorisation to Test (ATT)** and legal approvals.
- **Safety breakpoints & emergency comms** are always in place.
- **Data handling:** non-destructive test data; safe exfiltration simulations; no persistence beyond test windows.
- **Quality & compliance:** aligned to ISO 27001/9001, CREST, CE/CE+, and G-Cloud terms.

2.10 3. Service Variants & When to Use Them

Red Teaming – Covert, outcome-driven:

- Use when you need a realistic resilience assessment across people/process/tech without alerting defenders, to measure true detection & response capability and business impact.

Adversary Simulation – Fidelity to a specific actor:

- Use when you want to rehearse against the TTPs of a named threat group/campaign (overt or covert), evaluate defensive posture against a credible scenario, and validate readiness.

Purple Teaming – Collaborative uplift:

- Use when you want to accelerate detection engineering, validate playbooks, and iteratively mature SOC performance with live feedback.

2.11 Metrics & Success Criteria (examples)

Detection & Response:

- MTTD ↓, MTTR ↓, dwell time ↓
- % ATT&CK coverage ↑ (by tactic and technique)
- Alert fidelity ↑ (precision/recall), false positive rate ↓

Process & Readiness:

- Playbook adherence %, escalation accuracy %, containment time ↓
- Control effectiveness scores (EDR, SIEM, identity, cloud) ↑

Business Impact:

- Risk reduction narrative tied to critical services and data classes
- Maturity scoring vs baseline and target state

2.12 Prerequisites

- **Commercial & Communications**

- Signed **SoW** and **PO**.
- **Authorisation to Test** covering all in-scope environments.
- Named **Client PoC** and escalation contacts (24/7 if required).
- Preferred report formats (executive/technical/PDF).
- Agreement on **covert vs overt** engagement model and notification windows.

- **Technical**
  - **For Purple/Overt:** telemetry access (EDR/SIEM/NDR/identity/cloud), log parsing validation, time sync verified.
  - **For Red/Covert:** minimal prerequisites; may require IP ranges or safe channels pre-authorised for emergency comms.
  - **General:** test laptop/VM where required, optional representative credentials (for validation), cloud tenant details where in scope, any third-party constraints.

2.13 Deliverables

- **Executive Report:** business risk summary, outcomes vs objectives, strategic recommendations.
- **Technical Report:** kill-chain narrative, evidence, ATT&CK mapping, detection gaps, remediation roadmap.
- **Detection Engineering Pack (Purple/Follow-up):** rules, parsers, analytics, dashboards, runbooks.
- **Coverage Matrix & Metrics:** before/after scores, KPIs (MTTD/MTTR, dwell time, coverage %).
- **Workshops & Debriefs:** stakeholder walkthroughs, Q&A, and knowledge transfer.
- **Retest Results:** validation outputs and updated maturity scoring.

2.14 EJN Labs Tooling & Integration

- **Breach Hunter TI Platform:** real-time enrichment, actor/TTP mapping, external signal correlation to keep scenarios intelligence-led.
- **AI-Augmented Threat Modelling:** prioritises attack paths by likelihood/impact/visibility for efficient, high-value testing.
- **Optional ASM Integration:** continuous external exposure validation, shadow asset discovery, and alignment with internal findings.

3. Managed Bug Bounty

3.1 Managed Bug Bounty Programme

Bug bounties provide continuous, real-world testing across live environments by incentivising ethical hackers to find vulnerabilities before malicious actors do. EJN Labs helps organisations design and run managed bug bounty programmes that attract high-quality security researchers.

3.1.1 What This Service Is

A managed bug bounty programme defines scope, rules and rewards for responsible disclosure, then supports ongoing triage and remediation. The goal is to create a scalable, controlled way to uncover vulnerabilities over time, with clear handling of researcher submissions.

3.1.2 What We Assess

- Programme scoping and rules-of-engagement design
- Triage, validation and prioritisation of submissions
- Researcher communication and disclosure workflow management
- Risk assessment and remediation guidance for verified issues
- Reporting and metrics to track trends and progress

3.1.3 How the Work Is Performed

We help establish or refine your programme, then manage operational workflows including submission review, verification, severity assessment, and coordination with engineering teams. Our focus is on high signal-to-noise and fast, safe remediation.

3.1.4 Why This Matters

Bug bounty programmes extend testing coverage, provide diverse attacker perspectives, and help identify issues that may not appear during periodic assessments. A managed approach ensures quality, reduces operational burden, and supports responsible handling of findings.

4. Managed TI & ASM

4.1 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

4.1.1 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.

4.1.2 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

4.1.3 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.

4.1.4 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.

4.2 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.

4.2.1 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.

4.2.2 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

4.2.3 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.

4.2.4 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.

EJN LABS

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