G-Cloud 15 – Service Definition Document

Lot 3: Cloud Support for Penetration Testing

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
- 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 pen testing platform or more information.

Penetration 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 penetration 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.

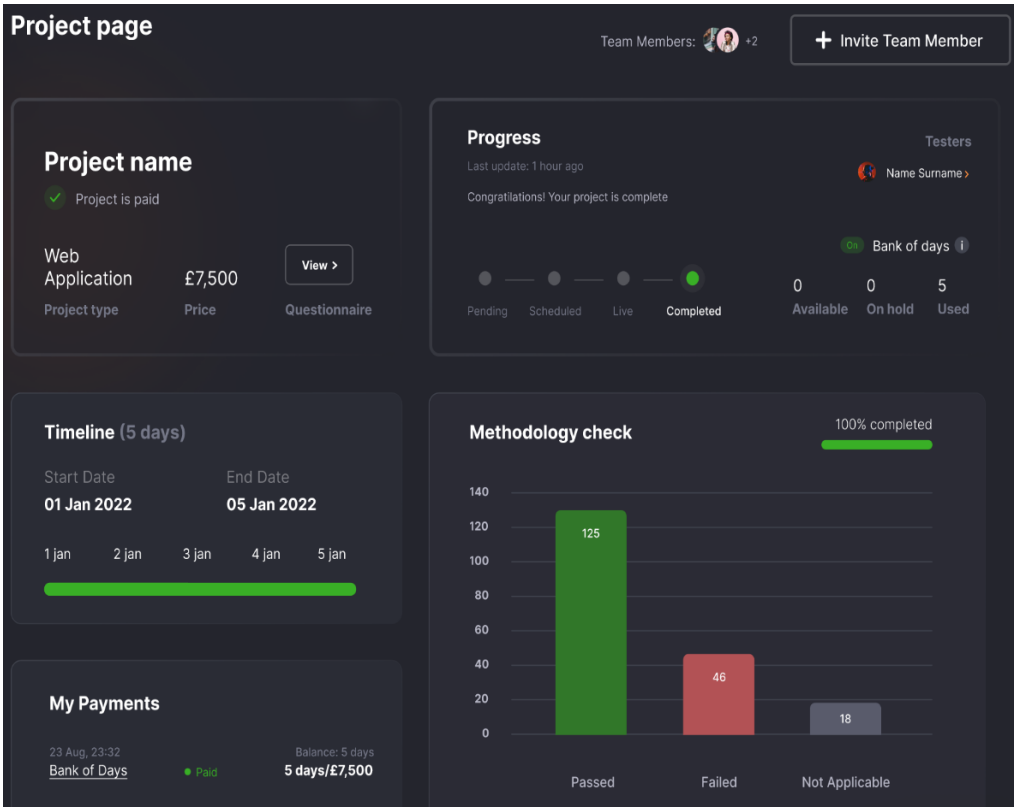
Please refer to Sections 1–10 for a detailed overview of our methodology and description of each of the below penetration tests. These sections outline the service scope, typical assessment areas, and the key outcomes you can expect from every engagement

Section	Type	Test
1.	Application and API Security Testing:	• Web Application Penetration Testing • API Penetration Testing • Thick Client Penetration Testing
2.	Mobile Device & Mobile Application Testing	• Mobile Application Penetration Testing • Mobile and Device Testing
3.	Network and Infrastructure Testing	• External Infrastructure Penetration Testing • Internal Infrastructure Testing • Identity & Access Security
4.	Cloud Security Testing (Amazon, Azure, Google)	• Amazon Web Services (AWS) Cloud Security Review • Azure Cloud Security Review • Google Cloud Platform (GCP) Cloud Security Review
5.	Social Engineering & Phishing	• Social Engineering (Non-Physical) • Phishing Assessments
6.	Advanced & Emerging Technology Testing	• AI Security Testing • Code Reviews (secure development focus) • AI-Augmented Threat Modelling • Blockchain Security Assessment • Cryptocurrency Security Assessment
7.	Comprehensive Vulnerability Assessment	• Vulnerability Assessment and Penetration Testing (VAPT)
8.	Adversary Simulation & Detection (Red and Purple Teaming)	• Red Teaming • Purple Teaming
9.	Managed Bug Bounty (Cloud)	• Managed Bug Bounty Programme
10.	Managed TI & ASM	• Threat Intelligence (TI) and Take Down Monitoring Managed Service • Attack Surface Monitoring (ASM) Managed Service

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**



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

1. Application and API Security Testing

1.1 Web Application Penetration Testing

Web application penetration testing is a structured security assessment designed to identify and validate vulnerabilities within web-based systems before they can be exploited. EJN Labs provides comprehensive web application penetration testing services that help organisations understand real-world risk and reduce the likelihood of data breaches, service disruption, and regulatory non-compliance.

1.1.1 What This Service Is

Our web application penetration testing simulates realistic attack scenarios against your application. Using a blend of manual testing and industry-standard tooling, we assess how an attacker could gain unauthorised access, manipulate data, bypass authentication controls, or otherwise compromise the confidentiality, integrity, or availability of the service.

1.1.2 What We Assess

- Authentication and session management mechanisms
- Authorisation and access control enforcement
- Input validation issues and injection vulnerabilities
- Business logic and workflow vulnerabilities
- Client-side security controls
- API endpoints and third-party integrations
- Configuration and deployment weaknesses

1.1.3 How the Work Is Performed

Testing is conducted in a controlled and responsible manner, aligned with recognised industry guidance such as the OWASP Testing Guide. Each engagement is tailored to the technology stack, architecture, and business context of the application under assessment. Where appropriate, we perform both authenticated and unauthenticated testing to reflect different threat perspectives.

1.1.4 Why This Matters

Web applications are frequent targets due to their accessibility and exposure to the internet. Regular penetration testing helps organisations proactively identify weaknesses before they are exploited, protect sensitive data, maintain customer trust, and meet regulatory or contractual security requirements. Our focus is on delivering meaningful insight that supports practical remediation and long-term resilience.

1.2 API Penetration Testing

Modern applications rely on APIs to connect services, share data and power user experiences. EJN Labs helps organisations secure APIs by identifying and validating weaknesses in endpoint design, authentication and data handling before attackers can exploit them.

1.2.1 What This Service Is

Our API penetration testing assesses REST, GraphQL, and RPC interfaces to identify vulnerabilities that lead to data exposure, authorisation bypass, account compromise, or service abuse. We focus on both technical weaknesses and logic flaws unique to API-driven systems.

1.2.2 What We Assess

- Authentication mechanisms (tokens, keys, sessions) and implementation flaws
- Authorisation and object-level access control (including IDOR-style issues)
- Input validation, injection risks, and schema weaknesses
- Rate limiting, abuse controls, and anti-automation protections
- Error handling, information disclosure, and security headers where relevant
- Business logic vulnerabilities and insecure workflows

1.2.3 How the Work Is Performed

Testing is tailored to your API architecture and usage patterns. We validate issues through controlled exploitation and provide clear, prioritised remediation guidance so your teams can strengthen the API ecosystem with minimal friction.

1.2.4 Why This Matters

APIs often expose high-value data and enable sensitive actions. A focused assessment helps prevent data leakage and account compromise, and supports secure integration across services, partners and third-party clients.

1.3 Thick Client Penetration Testing

Desktop and rich client applications often combine local logic with networked services, making them valuable targets for attackers. EJN Labs helps organisations secure thick client software by uncovering vulnerabilities in compiled binaries, local storage, and communications channels.

1.3.1 What This Service Is

Thick client penetration testing simulates attacks against desktop or rich client software to identify weaknesses in the executable, local storage, and network interfaces. This supports protection of intellectual property, prevents data theft, and strengthens trust in distributed applications.

1.3.2 What We Assess

- Anti-tamper and binary protections (obfuscation, packing, anti-debug)
- Local data security (plaintext secrets, weak encryption, file permissions)
- Protocols and network communications (encryption, authentication, MITM risks)
- Runtime manipulation and fuzzing to uncover memory corruption and logic flaws
- Installer/update mechanisms and deployment security
- Third-party and dependency risks (known as CVEs and insecure integrations)
- User interface security (injection points, debug panels, data leakage)

1.3.3 How the Work Is Performed

We combine static binary analysis (reverse engineering and pattern-based review of compiled code) with runtime testing and fuzzing. This reveals how the application is built and how it behaves under malicious conditions, including local manipulation and hostile inputs.

1.3.4 Why This Matters

Thick client applications create multiple avenues for exploitation across local execution and online services. Robust testing helps harden applications against tampering and reverse engineering, protect sensitive device-resident data, and reduce the risk of client-side compromise.

2. Mobile Device & Application Testing

2.1 Mobile Application Penetration Testing

Mobile applications are a primary touchpoint for users and an increasingly attractive target for attackers. EJN Labs helps organisations secure iOS and Android applications by identifying and validating critical vulnerabilities before they can be exploited.

2.1.1 What This Service Is

Our mobile application penetration testing simulates real-world attacks against your mobile app and its supporting services. We assess client-side security controls, back-end interactions, and how sensitive data is handled, with the goal of preventing unauthorised access, data leakage, and abuse of application functionality.

2.1.2 What We Assess

- Authentication and session handling within the mobile client
- Authorisation and access control enforcement (including API interactions)
- Secure storage of sensitive data on device
- Transport security and protection against interception and tampering
- Client-side validation, jailbreak/root detection, and anti-tamper controls
- Business logic and workflow vulnerabilities
- Third-party SDK and dependency risks

2.1.3 How the Work Is Performed

Testing combines manual analysis and targeted tooling to identify both common and complex vulnerabilities. Where appropriate, we perform dynamic testing on real devices or controlled environments, and assess how the application behaves under hostile conditions such as traffic interception and local manipulation.

2.1.4 Why This Matters

Mobile apps often handle authentication tokens, personal data, and payment-related workflows, making them high-value targets. A security assessment helps ensure mobile defences are effective, reduces the risk of compromise, and supports compliance and user trust.

2.2 Mobile and Device Testing

Mobile devices and endpoints are critical access points to corporate systems and data. EJN Labs helps organisations secure laptops, mobiles, and managed devices against misuse and compromise.

2.2.1 What This Service Is

Mobile and device testing assesses the security posture of end-user devices, including configuration, management controls, and exposure to attack. The goal is to prevent device-level compromise from leading to broader organisational impact.

2.2.2 What We Assess

- Endpoint configuration and hardening controls
- Device encryption and secure storage enforcement
- Mobile device management (MDM) and policy effectiveness
- Local privilege escalation and credential exposure risks
- Remote access, VPN, and device trust mechanisms
- Patch levels and exposure to known vulnerabilities

2.2.3 How the Work Is Performed

We assess device configurations and management policies, and perform controlled testing where agreed. Findings are mapped to practical remediation actions that improve endpoint resilience without disrupting users.

2.2.4 Why This Matters

Compromised devices often provide attackers with persistent access. Regular testing helps reduce endpoint risk, support secure remote working, and limit the impact of lost or compromised devices.

3. Network and Infrastructure Testing

3.1 External Infrastructure Penetration Testing

External infrastructure penetration testing simulates real-world attacks against your publicly accessible assets. This helps prevent initial compromise, data theft, and service disruption by identifying weaknesses that can be exploited from the internet.

3.1.1 What This Service Is

We assess internet-facing systems such as VPNs, remote access gateways, web services, exposed management interfaces, and perimeter controls. The objective is to understand what an external attacker can discover, access, and exploit, and provide clear remediation guidance.

3.1.2 What We Assess

- External asset discovery and exposure analysis
- Network services, ports, and protocol-level weaknesses
- Authentication controls and remote access mechanisms
- Misconfigurations and insecure default settings
- Known vulnerability exposure and patching gaps
- Privilege escalation and lateral movement pathways (where in-scope)

3.1.3 How the Work Is Performed

Our approach combines reconnaissance and exposure analysis with controlled exploitation. We validate findings to confirm real impact, prioritise issues based on exploitability, and provide practical fixes that can be applied with confidence.

3.1.4 Why This Matters

Internet-facing assets are often the first point of entry for attackers. External testing helps organisations understand and reduce their real-world exposure, improve hardening, and lower the likelihood of an initial foothold.

3.2 Internal Infrastructure Penetration Testing

Internal infrastructure penetration testing evaluates security controls from the perspective of an attacker who already has a foothold within the network. EJN Labs helps organisations understand the real impact of internal compromise and reduce the risk of widespread lateral movement and privilege escalation.

3.2.1 What This Service Is

This service simulates attacks originating from inside the network, such as a compromised user device or malicious insider. The objective is to identify weaknesses that allow attackers to escalate privileges, move laterally, and access sensitive systems or data.

3.2.2 What We Assess

- Internal network segmentation and trust boundaries
- Active Directory and domain security controls
- Privilege escalation paths and credential exposure
- Lateral movement techniques and service misconfigurations
- Internal services, management interfaces, and legacy systems
- Endpoint and network security control effectiveness

3.2.3 How the Work Is Performed

Testing is performed in a controlled manner using realistic attacker techniques while respecting agreed scope and safety constraints. Findings are validated to confirm impact and prioritised based on risk to the organisation.

3.2.4 Why This Matters

Many successful breaches escalate after an initial compromise. Internal testing helps organisations identify how far an attacker could realistically progress, enabling targeted improvements to containment and detection.

3.3 Identity and Access Security

Identity systems are central to modern security architectures. EJN Labs helps organisations strengthen identity and access controls to prevent account compromise, privilege abuse, and unauthorised access.

3.3.1 What This Service Is

Identity and access security assessments evaluate how identities are created, managed, authenticated, and authorised across systems. The focus is on preventing misuse of credentials and ensuring least-privilege access is enforced.

3.3.2 What We Assess

- Authentication mechanisms and multi-factor enforcement
- Authorisation models and privilege assignment
- Identity lifecycle management and account hygiene
- Federation, SSO, and third-party identity integrations
- Privileged access management and role separation
- Monitoring and alerting for identity misuse

3.3.3 How the Work Is Performed

We review architecture, configurations, and workflows across identity platforms and connected systems. Where appropriate, controlled testing is used to validate real-world exploitability of weaknesses.

3.3.4 Why This Matters

Compromised identities are a leading cause of breaches. Strengthening identity and access controls reduces attack surface, limits blast radius, and improves detection of suspicious behaviour.

4. Cloud Security Testing (AWS, Azure, GCP)

Cloud platforms underpin critical business services, but misconfigurations and weak controls can expose sensitive data and workloads. EJN Labs provides comprehensive cloud security testing across Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP). Our approach combines manual architecture review, automated checks, and targeted exploitation to validate real-world risk and deliver actionable remediation guidance. All engagements align with OWASP, NIST, CREST, and MITRE ATT&CK frameworks to ensure compliance and resilience.

4.1 Amazon Web Services (AWS) Cloud Security Review

AWS powers vast numbers of services daily, yet misconfigurations or gaps in controls can expose critical assets. EJN Labs helps secure AWS environments by identifying permission issues, insecure service settings and architectural weaknesses before they lead to incidents.

4.1.1 What This Service Is

An AWS Cloud Security Review inspects your cloud setup to uncover misconfigurations, permission gaps and insecure service deployments. It is designed to help prevent lateral movement, data leakage and regulatory violations across your AWS account.

4.1.2 What We Assess

- Identity and access management (IAM users, roles, policies, MFA and key hygiene)
- Network security (VPC design, security groups, NACLs and segmentation)
- Storage permissions and encryption (e.g., S3 access controls and KMS policies)
- Monitoring and logging configuration (e.g., CloudTrail and alerting)
- Container and serverless security (EKS/Lambda)
- Exposure of management interfaces and insecure defaults

4.1.3 How the Work Is Performed

We examine architecture and configuration across identity, networking and core services, then apply automated checks and targeted testing to validate benchmark drift and common misconfiguration exploitation paths. Findings are prioritised with practical remediation steps.

4.1.4 Why This Matters

Cloud misconfigurations can create high-impact exposure very quickly. A security review helps enforce least privilege, harden critical services, and reduce the likelihood of compromise as your AWS footprint evolves.

4.2 Azure Cloud Security Review

As organisations increasingly rely on Azure for infrastructure, applications and data, misconfigurations or gaps in controls can expose critical assets. EJN Labs helps secure Azure environments by identifying configuration drift, permission issues and architectural weaknesses before they lead to incidents.

4.2.1 What This Service Is

An Azure Cloud Security Review assesses your Azure setup to uncover misconfigurations, permission gaps and insecure service deployments. It is designed to prevent lateral movement, data leakage and compliance violations across your Azure subscriptions.

4.2.2 What We Assess

- Identity and access management (roles, conditional access, privileged access)
- Network security (segmentation, firewall rules, exposed services)
- Compute, container and serverless configuration hardening
- Storage security and encryption settings
- Logging, monitoring and alerting coverage
- Infrastructure-as-code and CI/CD security controls (where applicable)

4.2.3 How the Work Is Performed

We combine manual architecture and configuration review with automated checks and targeted testing. Using custom scripts and industry-standard tools, we identify drift from security benchmarks, validate exploitable misconfigurations, and provide prioritised guidance for remediation.

4.2.4 Why This Matters

Cloud environments change quickly, and small configuration mistakes can lead to major exposure. A security review helps maintain a hardened posture, supports compliance requirements, and reduces risk as your Azure footprint grows.

4.3 Google Cloud Platform (GCP) Cloud Security Review

GCP offers a wide array of services, but misconfigurations or gaps in controls can expose sensitive workloads. EJN Labs helps secure GCP environments by uncovering permission issues, network weaknesses and insecure service settings before they lead to incidents.

4.3.1 What This Service Is

A GCP Cloud Security Review examines your Google Cloud setup to discover misconfigurations, over-permissive roles and insecure service deployments. The goal is to prevent privilege escalation, data exfiltration and regulatory non-compliance across your GCP projects.

4.3.2 What We Assess

- IAM roles, service accounts, bindings and key management
- VPC networks, firewall rules, segmentation and egress controls
- Data protection and encryption for storage and managed services
- Logging and monitoring (Audit Logs, VPC Flow Logs, SCC findings)

- Infrastructure-as-code security (Terraform/Deployment Manager/Cloud Build)
- Container and serverless security (GKE, Cloud Run, Cloud Functions)
- Data services configuration (e.g., BigQuery datasets and access controls)

4.3.3 How the Work Is Performed

We analyse your project structure, networking and IAM, and assess resource policies for insecure defaults. We then apply automated checks and targeted testing to identify benchmark drift and attempt controlled exploitation of common misconfigurations. This provides a complete view of both design and operational risk.

4.3.4 Why This Matters

Maintaining a secure GCP footprint is essential for resilience, compliance and business continuity. A review helps identify weaknesses early, enforce least privilege, and strengthen detection and response through improved logging and policy enforcement.

5. Social Engineering & Phishing

5.1 Social Engineering (Non-Physical)

Social engineering attacks exploit human behaviour rather than technical flaws. EJN Labs helps organisations assess and reduce susceptibility to non-physical social engineering techniques.

5.1.1 What This Service Is

This service evaluates how attackers could manipulate staff through digital or verbal interaction, without physical presence. The aim is to identify weaknesses in awareness, verification processes, and response.

5.1.2 What We Assess

- Email-based social engineering beyond standard phishing
- SMS and messaging platform manipulation attempts
- Voice-based attacks such as vishing scenarios
- Impersonation of internal or trusted third parties
- User verification and escalation processes
- Reporting and response workflows

5.1.3 How the Work Is Performed

Scenarios are carefully designed and agreed in advance to ensure ethical and responsible testing. Engagements focus on learning outcomes rather than individual blame, with clear guidance for improvement.

5.1.4 Why This Matters

Attackers frequently bypass technical controls by targeting people. Social engineering testing helps improve awareness, strengthen verification procedures, and reduce the likelihood of successful manipulation.

5.2 Phishing Assessments

Phishing remains one of the most common and effective attack methods used to steal credentials, deliver malware and gain unauthorised access. EJN Labs phishing assessments simulate realistic phishing scenarios to uncover weaknesses, raise employee awareness and strengthen overall security posture.

5.2.1 What This Service Is

A phishing assessment evaluates your organisation's resilience to social engineering by running controlled phishing simulations and measuring how users respond. The goal is to identify patterns of risk, validate defensive controls and support practical improvements in awareness and reporting.

5.2.2 What We Assess

- User susceptibility and behavioural patterns across realistic phishing scenarios

- Email and security control effectiveness (filtering and detection)
- Reporting workflows and response readiness
- Credential harvesting and unsafe link interaction risks (simulated)
- Targeted scenarios aligned to roles, departments or threat models (where agreed)

5.2.3 How the Work Is Performed

We design phishing simulations that align with your organisation's context and risk appetite. Campaigns are executed responsibly, with clear rules of engagement. Results are analysed to provide actionable recommendations for training, control tuning and process improvement.

5.2.4 Why This Matters

Even strong technical controls can be bypassed through human error. Phishing assessments help reduce risk by improving awareness, strengthening reporting culture, and validating the effectiveness of existing controls and processes.

6. Advanced & Emerging Technology Testing

6.1 AI Security Testing

As AI becomes integral to decision-making, automation, and customer experiences, adversaries are rapidly developing methods to exploit model weaknesses, training data, and supporting interfaces. EJN Labs identifies and validates security risks unique to AI and machine learning systems.

6.1.1 What This Service Is

Our AI penetration testing evaluates AI-enabled applications, model interfaces, and surrounding infrastructure to uncover risks such as prompt injection, sensitive data leakage, insecure model access, and abuse of AI-driven workflows. We focus on both security and safety-relevant vulnerabilities that could lead to real-world harm or loss.

6.1.2 What We Assess

- Model and application interfaces (including LLM prompts, inputs, and output handling)
- Data exposure risks (training data leakage, memorisation, sensitive context disclosure)
- Access controls around model endpoints, keys, and permissions
- Abuse scenarios such as prompt injection and tool/plugin misuse
- Supply-chain and dependency risks in ML pipelines
- Monitoring, logging, and incident response readiness for AI abuse

6.1.3 How the Work Is Performed

We combine manual adversarial testing with structured evaluation techniques aligned to emerging AI security practices. Engagements are tailored to your model type (LLM, predictive, custom ML pipelines) and your deployment environment.

6.1.4 Why This Matters

AI systems introduce new attack paths and failure modes that traditional testing may not cover. A dedicated assessment helps ensure systems are trustworthy, reduces the risk of data leakage or manipulation, and supports compliance and governance requirements.

6.2 Code Reviews (secure development focus)

Security-focused code reviews identify vulnerabilities that can lead to real-world exploits. Unlike conventional code reviews that focus on style or performance, EJN Labs reviews target security flaws such as injection risks, authentication weaknesses and insecure data handling.

6.2.1 What This Service Is

A security code review is a manual analysis of your source code to find vulnerabilities early and reduce risk before deployment. By reviewing implementation details directly, we can identify issues that may not be observable through black box testing alone.

6.2.2 What We Assess

- Input validation and injection risks
- Authentication and session management implementation weaknesses
- Authorisation logic and access control correctness
- Cryptographic use and secret management practices
- Sensitive data handling and privacy concerns
- Error handling, logging and information disclosure risks
- Security controls around dependencies and third-party integrations

6.2.3 How the Work Is Performed

We review code with a security-first methodology, focusing on high-risk components, trust boundaries and critical workflows. Findings are contextualised to your architecture and development practices, with clear remediation guidance suitable for engineering teams.

6.2.4 Why This Matters

Finding vulnerabilities at code level helps prevent defects reaching production, reduces remediation cost, and improves secure development maturity. A review also provides assurance for high-risk features and helps teams align with secure coding best practices.

6.3 AI-Augmented Threat Modelling

Threat modelling is a proactive approach to identifying and mitigating security risks during system design and evolution. EJN Labs enhances traditional threat modelling by augmenting it with AI-assisted analysis to improve coverage, consistency, and insight.

6.3.1 What This Service Is

AI-augmented threat modelling combines structured threat modelling techniques with AI-assisted analysis to identify potential attack paths, design weaknesses, and misuse scenarios across applications, infrastructure, and business workflows. The goal is to identify risk early and support informed architectural decisions.

6.3.2 What We Assess

- System architecture and trust boundaries
- Data flows, assets, and sensitive information handling
- Threat scenarios aligned to attacker capabilities and motivations
- Misuse and abuse cases, including insider and automation-driven threats
- Control gaps and compensating security measures
- Risk prioritisation based on impact and likelihood

6.3.3 How the Work Is Performed

We work collaboratively with your technical and business stakeholders to model systems and workflows. AI-assisted analysis is used to explore threat scenarios, validate assumptions, and surface overlooked risks. Findings are reviewed and refined by experienced consultants to ensure accuracy and relevance.

6.3.4 Why This Matters

Addressing security risks early is significantly more effective than fixing issues post-deployment. AI-augmented threat modelling helps organisations design more resilient systems, reduce downstream remediation costs, and make informed security decisions as architectures evolve.

6.4 Blockchain Security Assessment

Blockchain-based systems introduce unique security challenges due to decentralisation, immutability, and complex trust assumptions. EJN Labs helps organisations identify and mitigate risks across blockchain platforms, smart contracts, and supporting infrastructure.

6.4.1 What This Service Is

A blockchain security assessment evaluates the security of blockchain implementations, including smart contracts, nodes, wallets, and integration points with traditional systems. The objective is to identify vulnerabilities that could lead to financial loss, service disruption, or loss of trust.

6.4.2 What We Assess

- Smart contract logic and vulnerability classes
- Consensus and protocol-related risks (where applicable)
- Key management and wallet security
- Node configuration and network exposure
- Integration points with off-chain services and APIs
- Monitoring, upgrade, and incident response readiness

6.4.3 How the Work Is Performed

We review architecture, smart contract code, and operational controls using a combination of manual analysis and targeted tooling. Testing focuses on realistic attack scenarios and prioritises issues based on exploitability and potential financial or operational impact.

6.4.4 Why This Matters

Blockchain systems often handle high-value assets and irreversible transactions. A security assessment helps reduce the risk of exploitation, protect user funds and data, and maintain confidence in decentralised applications and platforms.

6.5 Cryptocurrency Security Assessment

Cryptocurrency platforms and services are frequent targets for attackers due to the direct financial incentives involved. EJN Labs helps organisations secure cryptocurrency-related systems by identifying weaknesses that could lead to theft, fraud, or disruption.

6.5.1 What This Service Is

A cryptocurrency security assessment evaluates the security of systems involved in the storage, transfer, and management of digital assets. This includes exchanges, custodial services, wallets, payment platforms, and supporting infrastructure.

6.5.2 What We Assess

Assessments are tailored to your environment and objectives, but typically include the following areas:

- Wallet architecture and key management practices
- Transaction signing and authorisation workflows
- Hot and cold storage controls
- Exchange and platform access controls
- Fraud prevention and abuse detection mechanisms
- Operational security and incident response processes

6.5.3 How the Work Is Performed

We assess architecture, configurations, and operational workflows, and perform controlled testing where appropriate. Findings are validated to confirm real-world impact and prioritised to reduce the risk of asset loss or service compromise.

6.5.4 Why This Matters

Security failures in cryptocurrency systems can result in immediate and irreversible losses. Regular assessments help organisations protect assets, maintain user trust, and demonstrate strong security governance.

7. Comprehensive Vulnerability Assessment

7.1 Vulnerability Assessment and Penetration Testing (VAPT)

VAPT combines systematic vulnerability discovery with controlled exploitation testing to provide a complete view of your security posture. It identifies weaknesses in systems, applications and infrastructure, then validates real-world impact through safe exploitation.

7.1.1 What This Service Is

A VAPT engagement blends vulnerability assessment (broad discovery and prioritisation) with penetration testing (validation and exploitability analysis). This ensures you know where vulnerabilities exist and understand the risk they pose to your organisation.

7.1.2 What We Assess

- Vulnerability discovery across agreed assets and systems
- Validation and exploitation of high-risk findings to confirm impact
- Misconfigurations and insecure defaults
- Authentication and access control weaknesses
- Patch hygiene, exposed services and risky exposure paths

7.1.3 How the Work Is Performed

We begin with structured discovery to identify potential weaknesses, then validate key findings through controlled testing. Outcomes are prioritised by exploitability and business impact, with clear recommendations for remediation and risk reduction.

7.1.4 Why This Matters

A combined approach provides both breadth and depth. It reduces false positives, focuses remediation effort on issues that matter, and provides clear evidence for stakeholders and compliance requirements.

8. Adversary Simulation & Detection (Red and Purple Teaming)

8.1 Red Teaming

Red Teaming engagements simulate advanced, real-world attacks to evaluate your organisation's ability to detect, respond to and recover from sophisticated threats. This goes beyond vulnerability identification by emulating threat actors' tactics, techniques and procedures to test people, processes and technology under realistic conditions.

8.1.1 What This Service Is

A red team engagement is an objective-led attack simulation designed to assess defensive capability. The focus is on end-to-end outcomes such as gaining access, moving laterally, achieving persistence, and reaching agreed objectives, while monitoring detection and response throughout.

8.1.2 What We Assess

- Detection and response capability across realistic attack paths
- Security monitoring and alerting effectiveness
- Identity and access weaknesses leading to compromise
- Lateral movement and privilege escalation pathways (in-scope)
- Security operations processes and incident handling readiness

8.1.3 How the Work Is Performed

Engagements are planned with clear rules of engagement and safety controls. We emulate realistic threat behaviours and adapt tactics based on what is discovered, while ensuring testing remains controlled and aligned to agreed objectives. Outputs are prioritised and mapped to defensive improvements.

8.1.4 Why This Matters

Red teaming provides a realistic view of how an organisation withstands targeted attacks, highlights gaps in detection and response, and supports measurable improvements in resilience.

8.2 Purple Teaming

Purple Teaming combines offensive (red team) and defensive (blue team) security operations in a collaborative engagement. EJN Labs uses this approach to test and improve detection and response capabilities in real time whilst simulating realistic attack scenarios.

8.2.1 What This Service Is

A purple team engagement is a collaborative exercise where attackers and defenders work together to validate controls, improve detections and strengthen response workflows. It is ideal for organisations that want measurable defensive uplift rather than a standalone test report.

8.2.2 What We Assess

- Detection coverage for key attacker techniques
- Alert quality and triage effectiveness
- Logging and telemetry sufficiency
- Response playbooks and containment workflows
- Control tuning and defensive gaps across people, process and technology

8.2.3 How the Work Is Performed

We run structured attack scenarios and work side-by-side with your defenders to validate what is detected, what is missed and why. We then help tune controls and detections, and re-run scenarios to confirm improvements.

8.2.4 Why This Matters

Purple teaming accelerates security maturity by turning offensive findings into immediate defensive improvements, helping organisations build stronger monitoring, faster response, and clearer visibility.

9. Managed Bug Bounty

9.1 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.

9.1.1 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.

9.1.2 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

9.1.3 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.

9.1.4 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.

10. Managed TI & ASM

10.1 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

10.1.1 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.

10.1.2 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

10.1.3 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.

10.1.4 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.

10.2 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.

10.2.1 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.

10.2.2 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

10.2.3 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.

10.2.4 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