siberninja

Security Consulting Services

Comprehensive security testing and advisory services to identify vulnerabilities, validate exploitability, and strengthen your security posture across modern attack surfaces.

Contact:
Phone: +44 744 501 1912
Email: info@siberninja.com
Web: www.siberninja.com

Version 1.0

About Siber Ninja

Elite Offensive Security. Trusted by Industry Leaders.

Siber Ninja is a specialized cybersecurity consultancy and technology partner founded by experienced researchers and practitioners.

We provide a comprehensive portfolio that combines:

- **Security Consulting:** Advanced penetration testing, adversary simulation, application and cloud security services
- **Management Consulting:** Security program design, secure SDLC and DevSecOps transformation, risk and governance advisory
- **Security Training:** Instructor-led trainings, workshops, and custom enablement programs for engineering and leadership teams
- **Security Platforms:** AI-driven platforms for vulnerability intelligence, continuous attack surface monitoring, and application risk ranking

We work with organizations in highly regulated and security-critical industries such as finance, telecommunications, e-commerce, and public services.

How We Work?

Our approach goes beyond traditional testing and compliance:

- **Uncover complex, real-world attack paths** rather than surface-level findings
- **Validate exploitability and business impact** so you can prioritize what matters
- **Deliver clear, actionable, developer-friendly insights** without slowing down innovation

Why Siber Ninja?

We are more than a testing company — we are a long-term security partner.

- **Hands-on expertise:** All services are led by senior consultants; no outsourcing
- **Proven methodologies:** Real-world adversary simulation and continuous improvement of techniques and tools
- **Actionable results:** Business-aligned insights that reduce risk quickly and efficiently
- **Recognized leadership:** Speakers and contributors at DEF CON, Black Hat, and international security research communities

With 500+ successful engagements across 10+ countries, our work is trusted by enterprises, scale-ups, and public institutions that need to build, operate, and scale securely.

For more information, visit www.siberninja.com.

Table of Contents

About Siber Ninja **2**

Table of Contents **3**

Security Consulting Services Portfolio **4**

Web Application & API Security Testing 4

Network Security Testing 5

Mobile Application Security Testing 6

Secure Code Review and Secret Scanning 7

Red Teaming and Adversarial Security Testing 8

Thick Client Security Testing 9

Cloud Security Testing 10

Security Consulting Services Portfolio

Web Application & API Security Testing

Overview

Our **Web Application & API Security Testing** service helps organizations identify vulnerabilities in modern applications and backend services before attackers do.

We combine manual, goal-driven testing with industry-standard methodologies (OWASP Top 10, NIST 800-63) to uncover real risks — beyond what automated tools can detect.

We cover:

- Web applications (single-page apps, complex business portals)
- REST, GraphQL and SOAP APIs
- Microservices and backend integrations

Why It Matters

Web applications and APIs form the backbone of digital business. A single overlooked flaw can lead to data breaches, regulatory impact, and financial loss.

Our testing approach reveals real exploitability and business impact, not just a list of technical findings.

Objectives

- Discover and exploit vulnerabilities in applications and APIs
- Validate real-world exploitability and assess business impact
- Provide **clear, prioritized reports** with actionable remediation guidance
- Support security compliance with OWASP Top 10, NIST, PCI-DSS and other standards

Service Options

- **Standard:** Time-boxed penetration testing with manual and automated coverage for common vulnerabilities.
- **Comprehensive:** In-depth time-boxed testing, adding business logic abuse scenarios and advanced exploitation techniques.
- **Incremental:** Version-based testing focused on new releases, features, and related security implications.

Deliverables

- Executive summary for leadership
- Detailed technical findings with risk rating
- Prioritized remediation guidance
- Optional retrospective session with developers

Network Security Testing

Overview

Our **Network Security Testing** service identifies weaknesses across your internal and external network environments.
We combine automated scanning with manual exploitation and validation to uncover risks such as misconfigurations, outdated systems, and insecure network services that attackers can leverage.

We cover:

- External-facing infrastructure (internet perimeter)
- Internal networks, segmentation and privilege escalation paths
- Supporting services (DNS, VPN, VoIP/UC, etc.)

Why It Matters

A single exposed or misconfigured network service can be a gateway to lateral movement and compromise of critical systems.

This service helps organizations strengthen network defenses, reduce attack surface, and meet compliance requirements.

Objectives

- Discover vulnerabilities in internal and external networks
- Validate risks through manual testing and exploitation
- Provide clear, prioritized reporting with remediation guidance
- Verify compliance with industry standards such as PCI-DSS, ISO 27001, and regulatory requirements

Service Options

- **Standard:** Time-boxed assessment of internal or external networks, combining automated vulnerability scanning with manual penetration testing.
- **Custom:** Tailored testing that can include:
    - Wireless network security
    - VoIP/UC infrastructure testing
    - Social engineering components
    - Custom-defined attack scenarios

Deliverables

- Executive summary highlighting key exposures
- Technical findings with evidence and impact analysis
- Prioritized recommendations
- Optional readout session with IT/security teams

Mobile Application Security Testing

Overview

Our **Mobile Application Security Testing** service is designed to uncover vulnerabilities in iOS and Android applications, their backend services, and APIs.

We combine manual testing techniques with industry-recognized standards (OWASP Mobile Top 10, MASVS, NIST 800-63) to identify security weaknesses that automated tools often miss.

We cover:

- Native and hybrid mobile applications (iOS, Android)
- Mobile app APIs (REST/SOAP/GraphQL)
- Backend services and integrations (payment systems, authentication services)

Why It Matters

Mobile apps carry sensitive personal and business data. Weaknesses in mobile apps or backend APIs can lead to account takeovers, data breaches, and regulatory impact.

Our approach highlights real risks and exploit paths that affect both application users and your organization.

Objectives

- Identify vulnerabilities in mobile apps, backend services, and APIs
- Assess security controls against OWASP MASVS and Mobile Top 10
- Provide clear, actionable guidance to fix weaknesses
- Validate resilience against insecure storage, weak cryptography, and authentication flaws

Service Options

- **Standard:** Time-boxed mobile application security testing that includes automated analysis and manual validation.
- **Comprehensive:** A deep-dive engagement that adds business logic abuse scenarios, advanced cryptographic review, and backend API chaining.

Deliverables

- Executive summary with business impact
- Detailed findings with risk ratings
- Prioritized remediation guidance
- Optional session with development teams to accelerate fixes

Secure Code Review and Secret Scanning

Overview

Our **Secure Code Review & Secret Scanning** service provides a white-box perspective on the security of your applications.

Through a combination of manual code review, automated static analysis (SAST), and secret scanning, we identify vulnerabilities early in the SDLC, reducing remediation costs and improving overall code quality. We cover:

- Source code for web, mobile, API, and backend applications
- Authentication, authorization, and cryptographic implementations
- Hardcoded secrets, API keys, tokens, and misconfigurations

Why It Matters

Finding vulnerabilities in production is costly and time-consuming. A secure code review helps shift security left, detecting flaws in design and implementation before they become exploitable in production environments.

Objectives

- Identify vulnerabilities that automated tools miss, including:
  - Authentication & authorization flaws
  - Business logic weaknesses
  - Insecure coding patterns
- Detect and remediate hardcoded secrets and credentials
- Provide developer-friendly reporting that shortens time-to-remediation
- Improve code quality and resilience through early feedback

Service Options

- **Standard:** Time-boxed secure code analysis with automated SAST and targeted manual review of critical components.
- **Comprehensive:** Deep-dive secure code review that includes:
  - Complete manual code review of core modules
  - Automated SAST and secret scanning
  - Business logic assessment and design-level review

Deliverables

- Executive summary with risk insights
- Detailed findings with examples from source code
- Prioritized, actionable remediation steps
- Optional developer workshop to address recurring issues

Red Teaming and Adversarial Security Testing

Overview

Our **Red Teaming & Adversarial Security Testing** service simulates real-world, multi-vector attacks to assess how well your organization can prevent, detect, and respond to advanced threats. This engagement is goal-oriented rather than scope-limited: we act like a determined adversary to achieve agreed-upon objectives such as unauthorized access, data exfiltration, or privilege escalation.

We cover:

- Advanced attack simulations combining technical, physical, and social engineering vectors
- Testing organizational detection and response capabilities
- Lateral movement and chained attack path identification

Why It Matters

Standard penetration tests focus on finding vulnerabilities in specific systems.

Red teaming looks at the big picture — how an attacker can combine weaknesses across people, processes, and technology to compromise your business-critical assets.

Objectives

- Assess the true resilience of your organization against realistic adversaries
- Identify blind spots in detection and response capabilities
- Test technical, procedural, and human defenses under controlled conditions
- Provide actionable recommendations to strengthen resilience

Service Options

- **Red Teaming:** A multi-phase, custom engagement that includes reconnaissance, exploitation, lateral movement, and goal-driven attack paths, agreed upon with the client.
- **Adversarial Simulation:** Targeted adversary emulation using specific threat actor tactics, techniques, and procedures (TTPs) relevant to your sector.

Deliverables

- Executive report for leadership: key attack paths, business impact, and resilience gaps
- Detailed technical report of actions taken and findings
- Prioritized, actionable roadmap to strengthen defenses
- Optional readout session and workshop with security and leadership teams

Thick Client Security Testing

Overview

Our **Thick Client Security Testing** service focuses on the unique security challenges of desktop, standalone, and client-server applications.

We perform deep manual testing of application logic, communication protocols, and server-side components to uncover vulnerabilities often missed by standard testing approaches.

We cover:

- Desktop applications (Windows, macOS, Linux)
- Standalone or client-server enterprise software
- Communication channels between client and server components

Why It Matters

Thick client applications often manage sensitive data and interact directly with core systems. Due to their complexity, traditional web or network testing methodologies are insufficient to find flaws like insecure local storage, weak communication security, or code execution vulnerabilities.

Objectives

- Conduct in-depth analysis of client-side logic and server interactions
- Identify vulnerabilities such as:
  - Insecure local data storage
  - Weak encryption or obfuscation
  - Reverse engineering risks
  - Privilege escalation opportunities
- Provide actionable guidance for secure client-server architecture

Service Options

- **Thick Client Penetration Testing:** Comprehensive testing tailored for thick client architectures, including:
  - Manual analysis of internal logic and local storage
  - Assessment of communication protocols for tampering and interception
  - Review of server-side interactions and business logic vulnerabilities

Deliverables

- Executive summary highlighting high-risk weaknesses
- Detailed technical report including exploit scenarios
- Prioritized remediation roadmap
- Optional review session with development and architecture teams

Cloud Security Testing

Overview

Our **Cloud Security Testing** service addresses the unique security challenges of cloud environments. We perform in-depth assessments of cloud infrastructure, services, and applications to identify misconfigurations, vulnerabilities, and weaknesses in security controls.

Both manual techniques and automated cloud-specific tools are used to ensure a thorough evaluation.

We cover:

- Public, private, and hybrid cloud environments
- Cloud-native services (compute, storage, databases, IAM)
- Applications deployed on AWS, Azure, GCP and multi-cloud architectures

Why It Matters

Cloud environments introduce new attack surfaces and shared responsibility risks.

Misconfigurations, overly permissive roles, and insecure integrations are common causes of breaches. Proactive cloud security testing is critical to prevent data leaks and ensure compliance with standards.

Objectives

- Identify vulnerabilities and misconfigurations in cloud services
- Assess resilience against real-world attack scenarios
- Verify compliance with cloud security best practices (CIS Benchmarks, NIST, ISO 27017)
- Provide actionable recommendations to strengthen cloud posture

Service Options

- **Cloud Infrastructure Assessment:** In-depth review of cloud configurations, IAM roles, exposed services, and architectural weaknesses.
- **Cloud Penetration Testing:** Controlled exploitation of cloud environments, simulating real-world attack scenarios including privilege escalation, lateral movement, and data exfiltration.

Deliverables

- Executive summary focusing on key risks and business impact
- Technical findings with evidence and remediation guidance
- Prioritized roadmap to improve cloud security
- Optional cloud security workshop for engineering and DevOps teams