Management Consulting Services

Expert guidance to help security and engineering leaders build, scale, and mature secure development practices, application security programs, and DevSecOps capabilities.

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

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

Management Consulting Services Portfolio

Application Security Program Design

Overview

Our **Application Security Program Design** service helps organizations build, scale, and mature their application security practices. We work directly with security and engineering leaders to design programs that fit your SDLC, engineering culture, and business goals.

This service covers:

- Current program maturity assessment
- AppSec governance, policies, and control frameworks
- Secure SDLC and process integration
- Tooling, automation and workflow alignment

Why It Matters

Without a structured program, application security efforts become reactive and inconsistent. A well-designed program:

- Enables proactive risk management
- Aligns security with fast-paced delivery
- Reduces friction between security and engineering
- Builds a sustainable foundation for continuous improvement

Objectives

- Assess your current AppSec maturity and needs
- Define program structure, governance, and roles
- Integrate security practices and tooling into engineering workflows
- Establish clear KPIs and reporting for measuring program success

Service Options

- **AppSec Program Assessment & Design:** Comprehensive assessment of the current state and delivery of a **tailored program design** aligned with your organization's risk appetite and priorities.
- **Program Rollout Support:** Guidance on operationalizing the program, including roadmap execution, adoption strategies, and metrics tracking.

Deliverables

- Executive-level program assessment and target maturity goals
- Detailed AppSec program roadmap (short, mid, and long-term)
- Governance model, processes, and integration recommendations
- Optional enablement sessions for leadership and engineering teams

Code Security Program Design

Overview

Our **Code Security Program Design** service helps organizations embed security into the software development lifecycle by defining secure coding practices, integrating automation, and building developer capabilities.

We work with security and engineering leaders to create sustainable, shift-left approaches that reduce risk early in the development cycle.

We cover:

- Secure coding standards and guidelines
- SAST tools and code review workflows
- Developer enablement programs (training, playbooks)
- Code risk scoring and measurement models

Why It Matters

Most vulnerabilities originate from insecure coding practices that automated scanners alone cannot catch.

By proactively integrating secure coding standards and developer-friendly processes:

- Vulnerabilities are caught early, reducing cost and impact
- Engineering teams can deliver secure software at speed
- Organizations build a culture of secure coding that scales

Objectives

- Define organization-specific secure coding guidelines and standards
- Integrate SAST tools and manual review into developer workflows
- Develop training and playbooks for developers and reviewers
- Establish metrics and scoring models to measure code quality and risk

Service Options

- **Code Security Assessment & Design:** Review current practices and design a tailored program for secure coding, review processes, and tooling.
- **Developer Enablement & Rollout:** Support the implementation of secure coding guidelines, tools, and workflows, including workshops and coaching.

Deliverables

- Secure coding guidelines and standards document
- Recommended SAST and review workflow integration plan
- Developer training materials and/or workshops
- Metrics and scoring models for ongoing improvement

DevSecOps & CI-CD Architecture

Overview

Our **DevSecOps & CI/CD Architecture** service helps organizations design and implement secure, automated CI/CD pipelines.

We embed security controls, testing, and policy enforcement directly into the delivery workflow — ensuring security becomes a natural part of your engineering process.

We cover:

- Secure CI/CD pipeline architecture
- Pipeline threat modeling and workflow analysis
- Integration of security gates, scanning, and secrets management
- IaC and container security controls

Why It Matters

Without integrated security, CI/CD pipelines can become attack vectors and allow insecure code, misconfigurations, or secrets to flow into production.

A DevSecOps approach:

- Reduces vulnerabilities early and automatically
- Ensures compliance without slowing release cycles
- Builds trust and repeatability into your software delivery

Objectives

- Assess current CI/CD pipelines for security gaps
- Design secure, automated workflows aligned with engineering culture
- Integrate security scanning, policy enforcement, and secrets management
- Implement IaC and container security best practices
- Enable continuous monitoring and improvement of DevSecOps maturity

Service Options

- **Pipeline Assessment & Secure Design:** Review current CI/CD practices, identify risks, and design a secure DevSecOps architecture.
- **Implementation & Automation Support:** Help teams integrate scanning, secrets hygiene, and security controls into CI/CD pipelines with minimal disruption.

Deliverables

- Secure CI/CD architecture design
- Integration plan for security gates, automation, and monitoring
- Recommendations for secrets management, IaC security, and compliance
- Optional enablement workshop for DevOps and engineering teams

Security Policy & Standards Development

Overview

Our **Security Policy & Standards Development** service helps organizations establish clear, actionable, and enforceable policies and standards that guide secure software development and governance. We collaborate closely with stakeholders to ensure policies are tailored, practical, and aligned with both regulatory requirements and engineering culture.

We cover:

- Secure SDLC policies and standards
- Coding and deployment policies
- Governance and compliance frameworks
- Implementation playbooks and guidance

Why It Matters

Policies and standards set the foundation for consistent, repeatable security practices. Without well-designed and up-to-date guidance:

- Security efforts become fragmented and reactive
- Regulatory requirements are harder to meet
- Teams lack clarity on expectations and processes

Well-defined, engineering-aligned policies bridge this gap by embedding clear expectations into everyday workflows.

Objectives

- Assess current policies, standards, and procedures
- Develop or update secure SDLC and AppSec standards
- Ensure alignment with regulations and industry best practices
- Provide practical guidance for adoption and enforcement

Service Components

- Policy Framework Design
- Secure SDLC & Coding Standards
- Governance and Regulatory Alignment
- Playbooks and Implementation Guidance

Deliverables

- Comprehensive policy and standards documentation
- Gap analysis of existing policies
- Recommendations for governance, processes, and implementation
- Optional workshops with leadership and engineering teams to drive adoption

Application Security Maturity Action Plan

Overview

Our **Application Security Maturity Action Plan** service helps organizations assess the maturity of their Application Security and DevSecOps capabilities and define a structured roadmap for improvement. We benchmark your current state against industry-recognized models (BSIMM, SAMM) and design a phased plan to align people, processes, and technology with business goals.

We cover:

- AppSec and DevSecOps maturity assessments
- Gap analysis and prioritization
- Roadmap creation and progress tracking
- Metrics and governance model design

Why It Matters

Organizations often have fragmented security practices without a clear vision of where they stand or how to progress.

A structured maturity assessment:

- Provides objective visibility into strengths and gaps
- Establishes a prioritized roadmap tied to business goals
- Enables continuous improvement and measurable progress

Objectives

- Assess current AppSec and DevSecOps maturity using BSIMM/SAMM
- Identify key gaps and areas for improvement
- Define a phased, actionable roadmap aligned with risk appetite
- Establish KPIs and a measurement framework for ongoing improvement

Service Components

- Maturity Benchmarking (BSIMM/SAMM)
- Gap Analysis and Prioritized Roadmap
- KPIs, Metrics and Governance
- Continuous Improvement and Tracking

Deliverables

- Detailed maturity assessment report (AppSec & DevSecOps)
- Gap analysis and prioritized roadmap
- Metrics and governance framework
- Optional workshops to align stakeholders and plan execution

Architecture Risk Analysis & Threat Modeling

Overview

Our **Architecture Risk Analysis & Threat Modeling** service addresses security early in the design phase, when it is most cost-effective to fix weaknesses.

We analyze system architectures, perform contextual threat modeling, and assess the resilience of designs, components, and integrations before deployment.

We cover:

- Contextual threat modeling
- Secure architecture and design reviews
- Risk analysis of operational, procedural, and technical controls

Why It Matters

Most critical vulnerabilities originate in the design stage, long before code is written.

By embedding security into architecture decisions:

- Risks are addressed before implementation, saving time and cost
- Weaknesses are caught that cannot be discovered by traditional testing
- Teams build systems with security by design

Objectives

- Identify risks and weaknesses in system design and architecture
- Model likely attacker paths and abuse cases
- Recommend security patterns and controls to address risks
- Align architectures with secure design principles and best practices

Service Components

- **Threat Modeling:** Contextual modeling of potential attacker paths, abuse cases, and design-level risks.
- **Secure Design Review:** Assessment of architecture against best practices, security controls, and industry patterns.
- **Risk Analysis:** Evaluation of technical, procedural, and operational controls to prioritize risk mitigation.

Deliverables

- Threat modeling diagrams and risk register
- Secure design review findings
- Recommendations and remediation strategies for identified risks
- Optional architecture workshop with architects, engineers, and security teams