SYSTEM
SOLVE IT

SSIT Security Audit

Security teams do not need another scanner.
They need actionable intelligence.

One Platform. One Security Score. One Remediation Workflow.

Unified security assessments, risk prioritization, AI remediation, and workflow automation for modern software teams.

Start a free scan — systemsolveit.com/security-audit

02 Executive Summary

SSIT is not a scanner. SSIT is a Security Audit Operating System.

Modern software security is fragmented. Organizations run point tools that each generate separate reports, conflicting priorities, and thousands of alerts — while executives still lack a single view of risk.

SSIT Security Audit unifies detection, correlation, scoring, automation, and reporting into one platform. The result: one deduplicated finding catalog, one prioritized security score, and one remediation workflow your entire organization can follow.

This brochure opens with an executive overview for leadership and procurement teams. A Technical Deep Dive follows for engineers who need orchestrator, admin UI, and domain-level detail.

Key outcomes at a glance

- Reduced alert fatigue through intelligent finding correlation
- Faster remediation with AI guidance and AK-Bakery automation
- Centralized reporting for developers, auditors, and the board
- Enterprise deployment options including on-premises and air-gapped

Table of Contents

04 Why SSIT Exists

The problem with fragmented security tooling

- Security findings scattered across disconnected tools and dashboards
- The same vulnerability reported repeatedly by different scanners
- Developers spend hours triaging alerts instead of fixing root causes
- Executives lack a single, trustworthy view of organizational risk
- Compliance evidence spread across exports that do not align
- Security assessments that are slow, expensive, and hard to scale

SSIT was built to replace tool sprawl with a Security Audit Operating System — one workflow from assessment to remediation.

05 SSIT's Core Differentiator

Intelligent Finding Correlation

Problem

Security teams run many detection technologies. Each produces its own alerts. The same SQL injection may appear four times — from static analysis, dynamic testing, and multiple rule engines — creating alert fatigue and wasted effort.

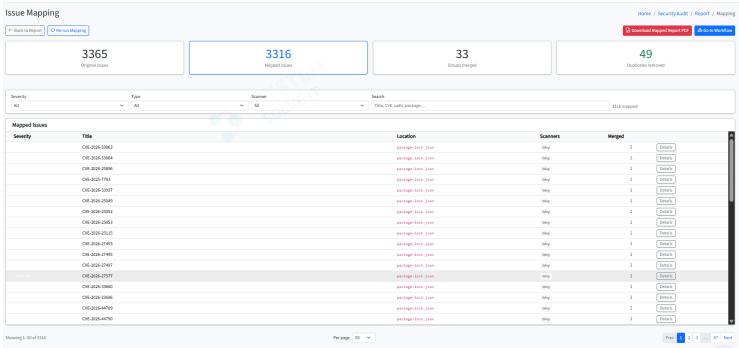
Solution

SSIT correlates findings from every integrated source into one verified issue catalog. One vulnerability. One priority. One remediation path.

Benefits

- Reduced alert fatigue — fix once, close once
- Faster triage — security teams focus on unique risk
- Better prioritization — severity reflects true exposure, not duplicate counts
- Improved remediation efficiency — developers receive clear, deduplicated guidance

Finding correlation flow — multiple scanner alerts unified into one canonical issue



Cross-scanner mapping in the admin UI

06 Real Security Outcomes

What organizations achieve with SSIT — beyond running scans

Reduced Duplicate Findings

Cross-scanner correlation eliminates redundant alerts so teams address unique risk.

Faster Remediation

Prioritized catalog, AI guidance, and workflow automation shorten time-to-fix.

Centralized Reporting

One score, one report, one export pipeline for every stakeholder.

Simplified Compliance Prep

SBOM, audit PDFs, and evidence packages ready for auditors and regulators.

Improved Security Visibility

16-category scoring gives executives and boards a clear posture metric.

Reduced Tool Sprawl

One unified platform replaces the cost and complexity of managing many point tools.

07 Why Security Teams Choose SSIT

The operational difference of a unified security platform

Without SSIT	With SSIT
• Multiple disconnected security tools	One unified security platform
• Multiple conflicting reports per assessment	One security score across 16 categories
• Duplicate findings across scanners	One deduplicated issue catalog
• Manual export and report assembly	One workflow automation engine (AK-Bakery)
• Alert fatigue and slow triage	One reporting system for every audience
• Remediation blocked by unclear priorities	Automated remediation workflows and AI guidance

08 How SSIT Works

From source code to actionable intelligence

GitHub Repo / Source Code
Shallow clone, stack detection, authorized live URLs and cloud credentials

↓

SSIT Orchestrator
Tiered execution with pause, resume, and per-tool status

↓

Integrated Detection
Orchestrated security technologies across code, cloud, and runtime

↓

Finding Correlation Engine
Deduplication into a canonical mapped catalog

↓

Risk Scoring Engine
0–100 score and 16-category prioritization

↓

AK-Bakery Automation
Visual workflows for alerts, exports, and integrations

↓

Reports & Remediation
PDF exports, AI guidance, SBOM, and DefectDojo JSON

09 Why SSIT Is Different

Not a scanner aggregator — a Security Audit Operating System

Finding Correlation

Maps duplicate alerts into one verified issue — not a raw feed from each tool.

Security Scoring

16-category 0–100 score executives and auditors understand immediately.

AI Remediation

Per-issue guidance explaining impact, exploit paths, and stack-specific fixes.

AK-Bakery Automation

Visual workflows — no scripting — for tickets, webhooks, and exports.

Public GitHub Audit

Prove value in minutes with a free tier — no enterprise sales cycle required.

Enterprise On-Prem Deployment

Licensed Docker inside your network; source code never leaves your boundary.

Mapped Audit Reports

Deliverables built from deduplicated catalogs, not noisy raw scanner output.

Unified Finding Catalog

One prioritized backlog for developers, security, and leadership.

10 Enterprise Security & Trust

Built for government, healthcare, banking, and regulated industries

- Air-gapped deployment for environments with no external connectivity
- Licensed on-premises Docker — full platform inside your network
- Internal-only source code processing — data ownership stays with you
- Local scanner execution — assessments run within your security boundary
- Persistent audit trails — reports, issues, AI logs, and settings in MongoDB
- Enterprise compliance readiness — SBOM, license compliance, and audit PDF evidence

SSIT meets the deployment and data-sovereignty requirements of organizations that cannot send source code to third-party SaaS platforms.

11 The Future of Security Auditing

Beyond scanning — toward security intelligence

SSIT is evolving beyond point-in-time scanning into continuous security intelligence.

The platform combines risk prioritization, correlated findings, AI-assisted remediation, and workflow-driven security operations — so teams spend less time managing tools and more time reducing risk.

- Risk prioritization over raw finding counts
- Correlated findings as the system of record
- AI-assisted remediation at the point of triage
- Workflow-driven SecOps via AK-Bakery
- Enterprise security intelligence for boards and regulators

SSIT is a Security Audit Operating System — not a security scanner platform.

12 One Platform. One Security Score. One Remediation Workflow

Unified security assessments for modern software teams

Organizations no longer need to choose between depth and simplicity. SSIT replaces disconnected dashboards with a unified assessment lifecycle — from first scan to executive report and automated follow-through.

Whether you are a startup evaluating a GitHub repository, an agency delivering client audits, or an enterprise securing regulated workloads, SSIT delivers correlated intelligence, prioritized risk, and actionable remediation in one place.

Technical Deep Dive

For security engineers, architects, and technical evaluators

14 Application Security

Identify coding vulnerabilities before attackers do

- Static Application Security Testing (SAST)
- Source code analysis
- Injection vulnerability detection
- Authentication and authorization weaknesses
- Security anti-pattern detection

Powered by

Semgrep CodeQL

SSIT runs Semgrep and CodeQL against cloned repositories, surfaces injection and auth flaws with file/line precision, and folds SAST into your unified score and mapped catalog.

How the orchestrator handles it

- Orchestrator shallow-clones the repo, detects languages (Node, Python, Go, Java, PHP, etc.), and selects applicable SAST rulesets.
- Semgrep runs on the public tier; CodeQL runs on enterprise admin when enabled.
- Findings include severity, CWE, code snippet, and scanner rule ID for audit evidence.
- Cross-scanner mapping merges duplicate SAST hits with DAST or SCA findings on the same vulnerability.

Admin UI & workflow

- Toggle Semgrep and CodeQL independently in Scan Target scanner options.
- Report issue list filters by severity, category, and scanner source.
- Issue detail page: full description, affected file path, highlighted snippet, and AI remediation panel.
- Export full or mapped audit PDF with SAST findings severity-ordered.

What SSIT delivers

- SAST findings in Full Audit PDF
- Mapped issue catalog
- Per-issue AI fix report
- DefectDojo JSON import

15 Dependency & Supply Chain Security

Modern applications depend on hundreds of third-party packages

- Known CVEs
- Malicious packages
- Supply-chain risks
- Vulnerable transitive dependencies
- Outdated components
- SBOM cross-check via Syft and OSV-Scanner

Powered by

Trivy | Snyk | OSV-Scanner | Socket | npm audit

SSIT orchestrates SCA and supply-chain intelligence so CVEs, malicious packages, and transitive risks appear once in your prioritized catalog — not in five separate tool dashboards.

How the orchestrator handles it

- Trivy and npm audit run on every applicable repo; Snyk and Socket activate when API keys are configured.
- OSV-Scanner cross-references lockfiles and SBOM components against the OSV database.
- Orchestrator deduplicates the same CVE reported by multiple SCA tools into one mapped issue.
- Severity reflects CVSS, exploitability, and reachability where scanners provide it.

Admin UI & workflow

- Dependency findings grouped under Vulnerabilities & SCA category in the score chart.
- Issue detail shows package name, version, fixed version, and all scanner sources.
- Configure Snyk and Socket API keys in admin settings for commercial intelligence.
- Download CycloneDX SBOM from report actions for supply-chain transparency.

What SSIT delivers

- SBOM CycloneDX
- SCA section in audit PDF
- DefectDojo JSON
- AI remediation for upgrade paths

16 Secret Detection

Prevent exposed credentials from becoming breaches

- API keys
- Access tokens
- Database credentials
- Cloud secrets
- Private certificates

Powered by

Gitleaks | TruffleHog | Trivy Secret Scanner

SSIT scans git history and working tree for leaked credentials, deduplicates across Gitleaks, TruffleHog, and Trivy secret rules, and flags critical findings for immediate rotation.

How the orchestrator handles it

- Gitleaks runs on public and enterprise tiers; TruffleHog is optional on enterprise admin.
- Trivy secret scanner adds container and filesystem secret detection.
- Mapping merges identical secrets found by multiple engines into one issue with all line references.
- High-severity secrets impact the Secrets category score disproportionately.

Admin UI & workflow

- Secrets appear in dedicated category with red severity badges.
- Issue detail redacts partial secret values while showing file, line, and rule type.
- Filter report by Secrets category for focused remediation sprints.
- AK-Bakery templates can webhook critical secret findings to Slack or ticketing systems.

What SSIT delivers

- Secret findings in audit PDF
- Mapped secret catalog
- Immediate-rotation checklist via AI assistant

17 Dynamic Application Security Testing

Security does not stop at source code

- SQL Injection
- Cross-Site Scripting
- Authentication weaknesses
- Misconfigurations
- Information disclosure
- API vulnerabilities

Powered by

OWASP ZAP | Nuclei | Nikto

Enterprise admin runs DAST against authorized live URLs via OWASP ZAP sidecar, Nuclei templates, and Nikto — with partial-result recovery if a scan is interrupted.

How the orchestrator handles it

- Provide a live website URL in Scan Target; DAST tier runs after repo scanners complete.
- ZAP runs in Docker sidecar with spider and active scan phases; partial results persist on timeout.
- Nuclei executes community and custom templates for known CVEs and misconfigs.
- Nikto adds legacy web server checks; DAST findings map to SAST issues when the same vuln is confirmed statically and dynamically.

Admin UI & workflow

- Enable ZAP, Nuclei, and Nikto toggles in scanner options for admin scans.
- Orchestrator shows DAST tier status separately from repo tiers.
- Issue detail links DAST evidence (URL, parameter, request) alongside code findings.
- Public tier does not run full DAST — enterprise required for live URL testing.

What SSIT delivers

- DAST findings in Full Audit PDF
- Mapped cross-scanner confirmation
- Executive summary of live exposure

18 SBOM Generation

Software Bill of Materials for supply-chain transparency

- CycloneDX SBOM export
- Component inventory across languages
- OSV database cross-check
- Transitive dependency visibility
- Audit-ready artifact for compliance

Powered by

Syft OSV-Scanner

SSIT generates CycloneDX SBOMs via Syft and cross-checks every component against OSV-Scanner so compliance teams receive machine-readable inventory plus vulnerability correlation.

How the orchestrator handles it

- Syft runs during the Repo tier on every scan with lockfiles or package manifests.
- SBOM includes name, version, type, and purl for each component.
- OSV-Scanner consumes the SBOM or lockfiles to flag known vulnerabilities per component.
- SBOM download is available from report export actions independent of PDF generation.

Admin UI & workflow

- Download SBOM (CycloneDX JSON) from report header export menu.
- SBOM-related findings appear under SBOM and SCA categories in the score chart.
- Issue detail references the affected SBOM component and upgrade path.

What SSIT delivers

- CycloneDX SBOM file
- SBOM-linked findings in audit PDF
- Compliance evidence package

19 IaC & Misconfiguration Security

Catch Terraform, Docker, and Kubernetes misconfigs before deploy

- Terraform and CloudFormation policies
- Dockerfile and compose misconfigs
- Kubernetes manifest compliance
- CIS and NSA framework checks
- Policy-as-code violations

Powered by

Terrascan | Checkov | Kubescape | Trivy IaC

SSIT scans infrastructure-as-code in your repository with Terrascan, Checkov, Kubescape, and Trivy IaC — surfacing misconfigs that become production incidents if unaddressed.

How the orchestrator handles it

- Stack detection finds Terraform, Dockerfile, docker-compose, and K8s YAML in the repo.
- Terrascan and Kubescape run on public tier when IaC files are detected; Checkov on enterprise admin.
- Findings include resource ID, policy rule, and remediation guidance from the scanner.
- IaC issues contribute to the IaC & Misconfigs score category.

Admin UI & workflow

- IaC findings show file path, resource name, and failed policy check.
- Filter by IaC category to review infra team backlog separately from app code.
- Map IaC findings with container or cloud findings when they reference the same resource.

What SSIT delivers

- IaC section in audit PDF
- Policy violation catalog
- Mapped infra + app correlation

20 Cloud Posture Security

Secure AWS, Azure, and GCP environments

- Multi-cloud misconfiguration detection
- IAM and storage exposure
- Network and logging gaps
- Compliance framework mapping
- Continuous posture assessment

Powered by

Prowler Scout Suite

Enterprise admin connects cloud credentials so Prowler and Scout Suite audit AWS, Azure, and GCP posture — IAM misconfigs, public buckets, and logging gaps feed your unified score.

How the orchestrator handles it

- Provide cloud credentials in Scan Target; Infra tier runs Prowler and/or Scout Suite.
- Prowler checks hundreds of CIS-aligned controls per cloud provider.
- Scout Suite delivers multi-cloud visualization and rule-based findings.
- Cloud findings appear in Cloud Posture category separate from IaC repo scans.

Admin UI & workflow

- Cloud credential fields in Scan Target with provider selection.
- Orchestrator Infra tier shows Prowler and Scout Suite completion status.
- Issue detail includes cloud resource ARN, region, and remediation CLI where available.

What SSIT delivers

- Cloud posture section in audit PDF
- Compliance mapping evidence
- Executive cloud risk summary

21 Container & Kubernetes Security

Modern applications rely heavily on containers

- Container image vulnerabilities
- Runtime hardening
- CIS benchmark compliance
- Kubernetes attack paths
- Deployment misconfigurations

Powered by

Trivy | kube-bench | kube-hunter | Kubescape | Docker Bench

SSIT combines image CVE scanning, CIS benchmarks, and cluster attack-path analysis so container and K8s risk is visible in one report — not scattered across four tools.

How the orchestrator handles it

- Trivy scans container images referenced in Dockerfiles and compose files.
- kube-bench runs CIS Kubernetes benchmarks when cluster config is provided (enterprise).
- kube-hunter probes for cluster attack paths; Kubescape validates manifests against NSA/CIS frameworks.
- Docker Bench Security checks host-level container hardening on infra targets.

Admin UI & workflow

- Container and K8s findings split across Container Security and Kubernetes Security categories.
- Issue detail shows image digest, CVE list, or benchmark control ID.
- Toggle kube-bench, kube-hunter, and Docker Bench in scanner options.

What SSIT delivers

- Container/K8s sections in audit PDF
- CIS benchmark evidence
- Image vulnerability catalog

22 API Security

APIs are among the most targeted attack surfaces

- OpenAPI implementation validation
- Schema compliance
- Authentication weaknesses
- Input validation flaws
- Unexpected behavior detection

Powered by

Schemathesis

When you provide a live API URL and OpenAPI spec, Schemathesis property-based fuzzing validates schema compliance and finds auth and input flaws automated scanners miss.

How the orchestrator handles it

- Live URL tier runs Schemathesis against the OpenAPI document in the repo or supplied URL.
- Fuzzing generates edge-case inputs from schema definitions.
- Failures include HTTP status, response body snippet, and operation ID.
- API findings map to DAST and SAST issues when the same endpoint is affected.

Admin UI & workflow

- Provide API base URL and spec path in Scan Target.
- API Security category in score chart tracks OpenAPI fuzz results.
- Issue detail shows endpoint, method, and reproduction steps.

What SSIT delivers

- API findings in audit PDF
- OpenAPI compliance report section

Discover externally exposed services before attackers do

- Open ports
- Running services
- Network exposure
- Misconfigured infrastructure

Powered by

Nmap

Enterprise admin runs authorized Nmap scans against live targets to discover open ports and services that expand your attack surface.

How the orchestrator handles it

- Nmap runs in Live URL tier when a hostname or IP is authorized in Scan Target.
- Service detection identifies running daemons and versions.
- Findings feed Network Scanning category in the 16-category score.

Admin UI & workflow

- Enable Nmap in scanner toggles; provide authorized target in live URL field.
- Issue detail lists port, protocol, service name, and version banner.
- Combine with DAST findings for exposed admin panels or debug endpoints.

What SSIT delivers

- Network exposure section in audit PDF
- Port/service inventory

24 TLS, SSL & Web Security

Evaluate the security posture of public-facing applications

- TLS configuration and cipher strength
- Certificate validity and chain trust
- HTTP security header grades
- Content-Security-Policy and HSTS gaps
- Browser security protections via securityheaders.com

Powered by

testssl.sh SecurityHeaders

SSIT analyzes live URLs with testssl.sh for TLS weaknesses and securityheaders.com for HTTP header grades — both run automatically when a URL is supplied on public and enterprise tiers.

How the orchestrator handles it

- testssl.sh checks cipher suites, protocol versions, certificate expiry, and known TLS vulnerabilities.
- securityheaders.com integration grades CSP, HSTS, X-Frame-Options, and related policies.
- TLS and Security Headers contribute to separate score sub-categories under Web Security.
- Public tier includes both when visitor adds a website URL to their GitHub audit.

Admin UI & workflow

- Live URL field on Scan Target and public audit form triggers TLS and header analysis.
- Findings show grade, missing headers, and recommended policy values.
- Issue detail links to testssl.sh evidence and header scan results.

What SSIT delivers

- TLS/header findings in audit PDF
- Public preview includes sample web security results

25 License Compliance

Avoid legal risk from dependency license violations

- Copyleft license detection
- Unknown and prohibited licenses
- Dependency license policies
- Multi-ecosystem support (npm, Maven, PyPI, Go)
- Policy violation reporting

Powered by

license-checker FOSSA Trivy License Scanner

SSIT flags GPL, AGPL, and policy-violating licenses across your dependency tree using license-checker, FOSSA (when configured), and Trivy license policies.

How the orchestrator handles it

- license-checker runs on Node projects during Extended tier.
- FOSSA API integration adds commercial license intelligence when keys are configured.
- Trivy reports license metadata alongside CVE data for container and OS packages.
- Violations appear in License Compliance score category.

Admin UI & workflow

- License findings show package, declared license, and policy rule triggered.
- Configure FOSSA API key in admin settings for enhanced coverage.
- Filter report by License Compliance for legal review workflows.

What SSIT delivers

- License section in audit PDF
- Compliance evidence for legal teams
- SBOM with license metadata

Identify suspicious files and malicious payloads

- YARA rule matching
- ClamAV scanning
- Suspicious binary detection
- Embedded payload analysis

Powered by

YARA ClamAV

Enterprise admin optionally scans artifacts with YARA rules and ClamAV to detect suspicious binaries and embedded malware in repositories and build outputs.

How the orchestrator handles it

- YARA rules run against files matching size and extension heuristics.
- ClamAV provides signature-based malware detection on scanned artifacts.
- Findings are high severity by default and isolated in Malware & Artifacts category.

Admin UI & workflow

- Enable YARA and ClamAV in optional scanner toggles on enterprise scans.
- Issue detail shows matched rule, file hash, and file path.
- Recommended action: quarantine, remove, or verify with security team.

What SSIT delivers

- Malware findings in audit PDF
- Incident-ready artifact references

Kubernetes runtime threat detection with Falco

- Falco rule pack evaluation
- Runtime syscall anomalies
- Container escape indicators
- Policy-as-code for K8s runtime
- Enterprise optional scanner

Powered by

Falco

When Falco rule packs are enabled, SSIT evaluates Kubernetes runtime policy bundles to detect anomalous syscalls, privilege escalations, and container escape patterns.

How the orchestrator handles it

- Falco rules run as optional Admin-tier scanner when policy bundles are configured.
- Rules align with community and custom Falco feeds for K8s threat detection.
- Findings contribute to Runtime Policy score category.

Admin UI & workflow

- Toggle Falco in scanner options for enterprise assessments.
- Issue detail shows triggered rule, priority, and Kubernetes context.
- Combine with kube-hunter and Falco for defense-in-depth cluster coverage.

What SSIT delivers

- Runtime policy section in audit PDF
- K8s threat detection evidence

28 The SSIT Security Score

Security data is only useful when it is understandable

SSIT transforms thousands of raw findings into a clear security score from 0 to 100, calculated across 16 security categories.

Organizations gain immediate insight into overall security posture, critical risk areas, compliance readiness, and maturity trends.

The 0–100 score and letter grade translate complex multi-scanner output into a metric executives, clients, and auditors understand immediately.

How the orchestrator handles it

- Sixteen categories each receive a weighted sub-score based on finding severity and count.
- Critical and high findings penalize categories more than informational items.
- Overall score aggregates category scores with configurable weighting.
- Public tier shows score and charts; enterprise shows full finding catalog behind the score.

Admin UI & workflow

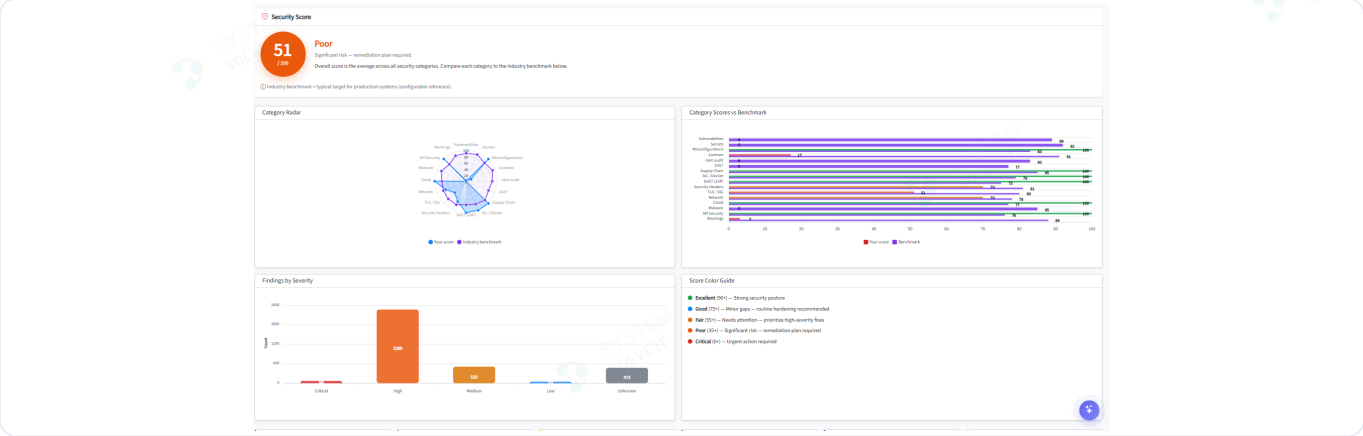
- Report header displays score, grade, and trend indicators.
- Interactive category charts drill down to findings per domain.
- Public audit layout mirrors enterprise score UX for consistent client experience.

What SSIT delivers

Score overview in all PDF exports

Category charts in Full Audit PDF

Public preview PDF with sample findings per category



Enterprise report — unified score and category breakdown

AK-Bakery Security Automation

Security findings should drive action — no coding required

Send alerts and generate reports automatically

Create tickets and trigger webhooks

Export findings and sync with security platforms

Generate AI remediation plans from visual workflows

AK-Bakery is SSIT's visual automation layer — connect triggers, issues, AI, exports, and webhooks without writing scripts.

How the orchestrator handles it

- Built-in templates: CVE Alert, DefectDojo Sync, AI Brief, Ticket Creator, Single Issue Fix Report.
- Node palette: triggers, Get Issue, Issue AI, Export, Webhook, Condition, and more.
- Run controls: execute, pause, view logs, and auto-download exports.
- Workflows operate on mapped issue catalog for accurate automation input.

Admin UI & workflow

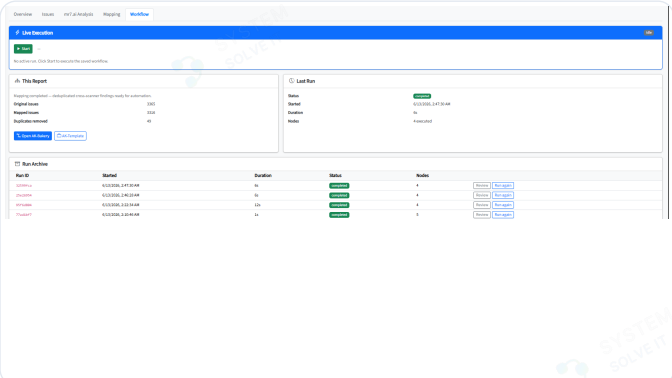
- Workflow dashboard lists templates and custom workflows with last run status.
- Canvas editor: drag nodes, connect edges, configure parameters per node.
- Execution panel shows step-by-step output and errors.

What SSIT delivers

Workflow Export CSV/Excel/PDF

Single Issue Fix Report PDF

Webhook payloads to Slack/Jira/custom endpoints



Workflow dashboard and template library

Visual workflow canvas with execution panel

30 AI-Assisted Remediation

Finding vulnerabilities is only half the battle

- What the issue means and why it matters
- How attackers exploit it in practice
- Recommended fixes and secure coding alternatives
- Remediation guidance tailored to your technology stack

AIKit provides per-issue remediation in the admin dashboard — explaining impact, exploit scenarios, and stack-specific fix steps powered by your codebase context.

How the orchestrator handles it

- AI analysis runs per issue from issue detail or AK-Bakery Issue AI node.
- Prompts include finding metadata, snippet, and detected stack for relevant guidance.
- AI logs persist in MongoDB for audit trail and re-generation.
- Aggregated AI output exports as AI Recommendations PDF.

Admin UI & workflow

- AI assistant panel on every issue detail page — expand for full remediation output.
- Regenerate analysis after code changes or false-positive review.
- AK-Bakery Issue AI node batch-processes top findings in workflows.

What SSIT delivers

- AI Recommendations PDF
- Single Issue Fix Report PDF
- mr7.ai authorized attacker narrative PDF

31 Reporting Designed for Every Audience

Professional deliverables for developers, auditors, clients, and board members

- Executive Security Reports
- Technical Audit Reports
- Compliance Evidence Packages
- SBOM Documentation (CycloneDX)
- DefectDojo Exports
- AI Remediation Reports
- Security Review PDFs

SSIT generates branded PDFs and structured exports so every stakeholder receives the right level of detail without manual report assembly.

How the orchestrator handles it

- Full Audit PDF: executive summary, charts, methodology, severity-ordered catalog.
- Mapped Audit PDF: same format from deduplicated catalog post-mapping.
- ZIP Audit splits very large catalogs into summary + findings PDFs.
- Public Preview PDF: score, sample findings, upsell — gated by email on public tier.

Admin UI & workflow

- Export menu on report page: Full PDF, Mapped PDF, ZIP, SBOM, DefectDojo JSON, AI PDF.
- Brochure PDF available from landing page for marketing.
- AK-Bakery Export node generates CSV, Excel, or PDF with SSIT branding.

What SSIT delivers

- Full Audit PDF
- Mapped Audit PDF
- ZIP Audit
- Public Preview PDF
- Platform Brochure PDF
- SBOM
- DefectDojo JSON

Deployment Options

Public Security Audit

Submit a GitHub repository and receive an immediate security assessment. No account required.

Enterprise Cloud

Full-featured security platform hosted and managed by SSIT with unified detection, mapping, and AK-Bakery.

Licensed On-Premises

Complete data ownership, air-gapped deployment, internal-only source code processing, and unlimited internal assessments.

SSIT scales from free public GitHub audits to licensed Docker on-premises — same orchestrator, same UI, your choice of data boundary.

How the orchestrator handles it

- Public: shallow clone, core detection tier, score + preview PDF, optional live URL for TLS/headers.
- Enterprise cloud: full orchestration, mapping, DAST, cloud, AK-Bakery, and complete exports.
- On-prem: licensed Docker bundle runs entirely inside your network; no source code leaves your boundary.

Admin UI & workflow

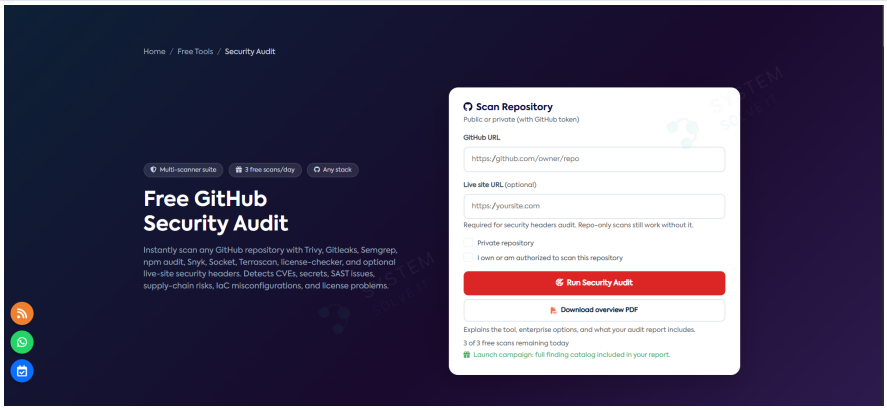
- Public flow at systemsolveit.com/security-audit — paste GitHub URL, authorize, view score.
- Enterprise admin dashboard: full scan configuration, reports, workflows, settings.
- On-prem install uses same admin UI against local MongoDB and scanner toolchain.

What SSIT delivers

Public preview PDF

Enterprise full audit suite

Air-gapped compliance deployments



Free public audit — score, grade, and category charts

33 Built for Every Industry

SSIT supports organizations across regulated and high-growth sectors

Financial Services & Fintech	**Healthcare & Life Sciences**
Government & Defense	**SaaS & Technology**
E-Commerce & Retail	**Manufacturing & IoT**
Education & Nonprofits	**Agencies & Consultancies**
Enterprise DevSecOps Teams	**Technology Startups**

Regulated industries need evidence; startups need speed — SSIT delivers both with the same platform.

How the orchestrator handles it

- Financial and healthcare: on-prem deployment, SBOM, license compliance, audit PDFs for regulators.
- Agencies: white-label reports, client GitHub audits via public tier, full enterprise for engagements.
- SaaS and startups: free tier proves value; enterprise scales to CI/CD integration.

Admin UI & workflow

- Branded PDF exports suitable for client delivery and board presentations.
- Industry-specific scanner toggles (e.g., Falco for K8s-heavy healthcare SaaS).
- Consultation scheduling from public preview upsell page.

What SSIT delivers

Client-ready audit PDFs

Compliance evidence packages

SSIT hands-on remediation from $1,000 USD

Why SSIT for Technical Teams

Platform capabilities for security engineers and architects

- Unified detection orchestration across every major security domain
- Unified risk scoring across 16 categories
- Cross-scanner correlation and deduplication
- AI-powered remediation per finding
- Workflow automation via AK-Bakery
- Executive and technical PDF exports
- On-premises deployment for regulated environments
- Enterprise scalability from free tier to licensed Docker

All delivered through a single Security Audit Operating System designed for technical depth and operational clarity.

SSIT replaces a toolchain of disconnected products with one platform — practitioner-built, not resold.

How the orchestrator handles it

- Breadth: SAST, DAST, SCA, secrets, IaC, containers, cloud, API, network, TLS, SBOM, licenses, malware, runtime — one orchestrated run.
- Clarity: mapping and 16-category scoring replace alert fatigue.
- Action: AK-Bakery and AI remediation turn findings into tickets, fixes, and reports automatically.

Admin UI & workflow

- Free public tier removes sales friction — see your score in minutes.
- Enterprise and on-prem scale to regulated workloads without changing workflow.
- Partnership tier: SSIT senior engineers fix what scanners find.

What SSIT delivers

- Complete platform brochure
- Schedule consultation at systemsolveit.com

35 Scanner Reference — Integrated Detection Technologies

Integrated tools orchestrated in every enterprise assessment

Trivy SCA / CVE	**npm audit** SCA	**Gitleaks** Secrets	**Semgrep** SAST
Snyk SCA	**Socket** Supply chain	**CodeQL** SAST	**Syft** SBOM
OSV-Scanner SCA	**Kubescape** IaC / K8s	**TruffleHog** Secrets	**YARA** Malware
ClamAV Malware	**Falco** Policy	**Terrascan** IaC	**license-checker** License
Security Headers HTTP	**Checkov** IaC	**FOSSA** License	**OWASP ZAP** DAST

Scanner Reference — Integrated Detection Technologies (continued)

testssl.sh
TLS

Nuclei
DAST

Nikto
DAST

Nmap
Network

Schemathesis
API

Docker Bench
Cloud

kube-bench
K8s

kube-hunter
K8s

Scout Suite
Cloud

Prowler
Cloud

Capability Coverage Matrix

Platform capabilities — professional reference

Capability	SSIT
SAST	**Supported** Semgrep, CodeQL
DAST	**Supported** OWASP ZAP, Nuclei, Nikto
SCA / Dependency Scanning	**Supported** Trivy, Snyk, OSV-Scanner, npm audit
Secret Detection	**Supported** Gitleaks, TruffleHog, Trivy
SBOM Generation	**Supported** Syft, CycloneDX
IaC Security	**Supported** Checkov, Terrascan, Kubescape
Container Security	**Supported** Trivy, Docker Bench
Kubernetes Security	**Supported** kube-bench, kube-hunter, Kubescape
Cloud Posture	**Supported** Prowler, Scout Suite
API Security	**Supported** Schemathesis
Malware Analysis	**Supported** YARA, ClamAV
AI Remediation	**Supported** AIKit per-issue guidance
Workflow Automation	**Supported** AK-Bakery visual workflows
Reporting & Exports	**Supported** Audit PDF, SBOM, DefectDojo JSON
On-Premises Deployment	**Supported** Licensed Docker, air-gapped

Get In Touch

Security audits · DevOps · Enterprise integration · Hands-on remediation

WEBSITE
systemsolveit.com

EMAIL
info@systemsolveit.com

WHATSAPP
+201503883394

SCHEDULE MEETING
Book a consultation