

Finite State Next-Generation Platform Data Imports

Take advantage of leading AppSecOps visibility with data imports

Updated November 2023

The Finite State Next-Generation Platform supports out-of-the-box data imports from over 150 common security tools. See below for the currently supported formats for each tool.

Tool	Scan Format
Acunetix360 Scan	Acunetix360 JSON format
Acunetix Scan	XML format
Anchore Engine Scan	Anchore-CLI JSON vulnerability report format
Anchore Enterprise Policy Check	Anchore-CLI JSON policy check report format
Anchore Grype	A vulnerability scanner for container images and filesystems. JSON report generated with '-o json' format
AnchoreCTL Policies Report	AnchoreCTLs JSON policies report format
AnchoreCTL Vuln Report	AnchoreCTLs JSON vulnerability report format
Aqua Scan	Aqua Scanner results in JSON format
Arachni Scan	JSON report format
AppSpider Scan	Use the VulnerabilitiesSummary.xml file found in the zipped report download
AuditJS Scan	AuditJS Scanning tool using Sonatype OSSIndex database with JSON output format
AWS Prowler Scan	Export of AWS Prowler in CSV or JSON format
AWS Prowler V3	Export of AWS Prowler JSON V3 format
AWS Scout2 Scan	JS file in scout2-report/inc-awsconfig/aws_config.js.
AWS Security Finding Format (ASFF) Scan	AWS Security Finding Format (ASFF)
AWS Security Hub Scan	AWS Security Hub exports in JSON format
Azure Security Center Recommendations Scan	Microsoft Defender for Cloud (formerly known as Azure Security Center) recommendations in CSV format
Bandit Scan	JSON report format

Tool	Scan Format
BlackDuck API	BlackDuck findings can be directly imported using the Synopsys BlackDuck API
Blackduck Component Risk	Upload the zip file containing the security.csv and files.csv.
Blackduck Hub Scan	Upload the zip file containing the security.csv and components.csv for Security and License risks
Brakeman Scan	Import Brakeman Scanner findings in JSON format
Bugcrowd API Import	Bugcrowd submissions can be directly imported using the Bugcrowd API
BugCrowd Scan	BugCrowd CSV report format
Bundler-Audit Scan	bundler-audit check' output (in plain text)
Burp Enterprise Scan	Burp Enterprise Edition findings in HTML format
Burp GraphQL API	Burp Enterprise Edition findings from the GraphQL API in JSON format
Burp REST API	Burp REST API scan data in JSON format (/scan/[task_id] endpoint)
Burp Scan	When the Burp report is generated the recommended option is Base64 encoding both the request and response fields. These fields will be processed and made available in the 'Finding View' page
CargoAudit Scan	JSON output for cargo audit scan report
Checkmarx OSA	Checkmarx Open Source Analysis for dependencies (json). Generate with `jq -s . CxOSAVulnerabilities.json CxOSALibraries.json`
Checkmarx Scan	Detailed Report. Import all vulnerabilities from checkmarx without aggregation
Checkov Scan	JSON reports of Infrastructure as Code vulnerabilities
Clair Klar Scan	JSON reports of Docker image vulnerabilities from clair klar client
Clair Scan	JSON reports of Docker image vulnerabilities in JSON format
Cloudsploit Scan	Cloudsploit report file can be imported in JSON format (option --json)
Cobalt.io API Import	Cobalt.io findings can be directly imported using the Cobalt.io API
Cobalt.io Scan	CSV Report

Tool	Scan Format
Codechecker Report native	Import Codechecker Report in native JSON format
Contrast Scan	CSV Report
Coverity API	Coverity API view data in JSON format (/api/viewContents/issues endpoint)
Crashtest Security JSON File	XML Report
CredScan Scan	CSV output of CredScan scan report
CycloneDX	CycloneDX v1.4 JSON
DawnScanner Scan	Dawnscanner (-j) output file can be imported in JSON format
Dependency Check Scan	OWASP Dependency Check output can be imported in Xml format
Dependency Track Finding Packaging Format (FPF) Export	The Finding Packaging Format (FPF) from OWASP Dependency Track can be imported in JSON format. See here for more info on this JSON format
Detect-secrets Scan	JSON output for detect-secrets scan report
docker-bench-security Scan	JSON reports of Docker CIS benchmark scans
Dockle Scan	JSON output for Dockle scan report
DrHeader JSON Importer	Result of DrHeader JSON output
DSOP Scan	Import XLSX findings from DSOP vulnerability scan pipelines
Edgescan Scan	Edgescan findings can be imported by API or JSON file
ESLint Scan	JSON report format
Finite State SBOM	Finite State SBOM Listing document
Fortify Scan	Findings from XML file format
Generic Findings Import	Generic findings in CSV or JSON format
Ggshield Scan	Import Ggshield Scan findings in JSON format
Github Vulnerability Scan	Vulnerabilities from Github API GraphQL query in JSON format
GitLab API Fuzzing Report Scan	GitLab API Fuzzing Report report file can be imported in JSON format (option --json)
GitLab Container Scan	GitLab Container Scan report file can be imported in JSON format (option --json)
GitLab DAST Report	GitLab DAST Report in JSON format (option --json)
GitLab Dependency Scanning Report	GitLab SAST Report vulnerabilities in JSON format

Tool	Scan Format
GitLab SAST Report	GitLab SAST Report vulnerabilities in JSON format.
GitLab Secret Detection Report	GitLab Secret Detection Report file can be imported in JSON format (option --json)
Gitleaks Scan	Gitleaks Scan findings in JSON format
Gosec Scanner	Gosec Scanner findings in JSON format
Govulncheck Scanner	Import Govulncheck Scanner findings in JSON format
HackerOne Cases	HackerOne cases findings in JSON format
Hadolint Dockerfile check	Hadolint Dockerfile check findings in JSON format
Harbor Vulnerability Scan	Vulnerabilities from Harbor API in JSON format
Horusec Scan	JSON output of Horusec cli
HuskyCI Report	Import HuskyCI Report vulnerabilities in JSON format
Hydra Scan	Hydra Scan can be imported in JSON format
IBM AppScan DAST	XML file from IBM App Scanner
Immuniweb Scan	XML Scan Result File from Imuniweb Scan
IntSights Report	IntSights report file can be imported in JSON format
JFrog Xray API Summary Artifact Scan	Xray findings in JSON format from the JFrog Xray API Summary/Artifact JSON response
JFrog Xray Scan	Xray findings in JSON format
JFrog Xray Unified Scan	Xray Unified (i.e. Xray version 3+) findings in JSON format
KICS Scan	JSON output for KICS scan report
Kiuwan Scan	Kiuwan Scan in CSV format. Export as CSV Results on Kiuwan
kube-bench Scan	JSON reports of Kubernetes CIS benchmark scans
Logic Bomb	Logic Bomb Issues Listing document
Meterian Scan	Meterian JSON report output file can be imported
Microfocus Webinspect Scan	XML report
MobSF Scan	MobSF results in JSON format (use the API api/v1/report_json)
Mobsfscan Scan	JSON report for mobsfscan report file
Mozilla Observatory Scan	JSON report
Netsparker Scan	Netsparker JSON format

Tool	Scan Format
NeuVector (compliance)	Imports compliance scans returned by REST API
NeuVector (REST)	description: Use the full XML export template from Nexpose
Nexpose Scan	Use the full XML export template from Nexpose
Nikto Scan	XML output or JSON output
Nmap Scan	XML output (use -oX)
Node Security Platform Scan	Node Security Platform (NSP) output file can be imported in JSON format
NPM Audit Scan	NPM Audit Scan json output up to v6 can be imported in JSON format
Nuclei Scan	Import JSON output for nuclei scan report
OpenScap Vulnerability Scan	Import OpenScap Vulnerability Scan in XML formats
OpenVAS CSV	Import OpenVAS Scan in CSV format. Export as CSV Results on OpenVAS
ORT evaluated model Importer	Outpost24 endpoint vulnerability scan in XML format
OssIndex Devaudit SCA Scan Importer	OssIndex Devaudit SCA Scan in JSON format
Outpost24 Scan	Outpost24 endpoint vulnerability scan in XML format
PHP Security Audit v2	PHP Security Audit v2 Scan in JSON format
PHP Symfony Security Check	Results from the PHP Symfony Security Checker by Sensiolabs in JSON format
pip-audit Scan	pip-audit JSON scan report
PMD Scan	CSV Report
Popeye Scan	Popeye report file can be imported in JSON format
PWN SAST	pwn_sast Driver findings in JSON format
Qualys Infrastructure Scan (WebGUI XML)	Qualys WebGUI output files can be imported in XML format
Qualys Scan	Qualys WebGUI output files can be imported in XML format
Qualys Webapp Scan	Qualys WebScan output files can be imported in XML format
Retire.js Scan	Retire.js JavaScript scan (--js) output file can be imported in JSON format
Rubocop Scan	Import Rubocop JSON scan report (with option -f json)
Rusty Hog Scan	Rusty Hog Scan - JSON Report
SARIF	SARIF report file can be imported in SARIF format

Tool	Scan Format
Scantist Scan	Scantist Dependency Scanning Report vulnerabilities in JSON format
Scout Suite Scan	JS file in scoutsuite-results/scoutsuite_results_*.js.
Semgrep JSON Report	Semgrep output (--json)
SKF Scan	Output of SKF Sprint summary export in CSV format
Snyk Scan	Snyk output file (snyk test --json > snyk.json) can be imported in JSON format
Solar Appscreeener Scan	Solar Appscreeener report file can be imported in CSV format from Detailed_Results.csv
SonarQube Scan	SonarQube output file can be imported in HTML format
Sonatype Application Scan	Sonatype results in JSON format
SPDX	SPDX JSON (up to v2.3)
SpotBugs Scan	XML report of textui cli.
SSL Labs Scan	JSON Output of sslabs-scan cli.
Sslscan	XML output of sslscan report
SSLyze Scan (JSON)	XML report of SSLyze version 2 scan
StackHawk HawkScan	StackHawk webhook event can be imported in JSON format
Talisman Scan	JSON format
Tenable Scan	CSV or .nessus (XML) report formats
Terrascan Scan	JSON output for Terrascan scan report
Testssl Scan	CSV output of testssl scan report
TFSec Scan	JSON output for TFSec scan report
Trivy Operator Scan	Import trivy-operator JSON scan report
Trivy Scan	trivy scan report in JSON format
Trufflehog3 Scan	JSON Output of Trufflehog3 a fork of TruffleHog located at https://github.com/feeltheajf/truffleHog3
Trufflehog Scan	JSON Output of Trufflehog. Supports version 2 and 3 of https://github.com/trufflesecurity/trufflehog
Trustwave Fusion API Scan	Trustwave Fusion API report file can be imported in JSON format
Trustwave Scan (CSV)	CSV output of Trustwave vulnerability scan
Twistlock Image Scan	JSON output of twistcli image scan or CSV

Tool	Scan Format
VCG Scan	VCG output can be imported in CSV or Xml formats
Veracode Scan	Detailed XML Report
Veracode SourceClear Scan	Veracode SourceClear CSV or JSON report format
Vulners	Import Vulners Audit reports in JSON
Wapiti Scan	XML report
Wazuh	Wazuh
WFuzz JSON report	WFuzz findings in JSON format
Whispers Scan	Whispers report file can be imported in JSON format (option --json)
WhiteHat Sentinel	WhiteHat Sentinel output from api/vuln/query_site can be imported in JSON format
Whitesource Scan	JSON report
Wpscan	JSON report
Xanitizer Scan	XML findings list report preferably with parameter 'generateDetailsInFindingsListReport=true'
Yarn Audit Scan	Yarn Audit Scan output file can be imported in JSON format
ZAP Scan	ZAP XML report format