seceon
SECURITY FOR EONS

Seceon aiDAST360

Dynamic Application Security Testing

Integrated web & API vulnerability assessment for the Seceon Open Threat Management (OTM) Platform

At a Glance

- **Multi-engine DAST**: OWASP ZAP + Nuclei + 80+ custom OWASP/API/GraphQL checks
- **Native to Seceon CCE** - unified with network VA, aiSIEM ingestion, and compliance reporting
- **MSSP-ready**: multi-tenant operations, scheduled scans, ASM-driven auto-assessment
- **On-premises deployment with air-gapped support** - your data stays in your environment

Product Overview

Seceon aiDAST360 delivers enterprise-grade Dynamic Application Security Testing as an integrated module of the Seceon Open Threat Management (OTM) Platform. It continuously assesses web applications and APIs for exploitable vulnerabilities from an attacker's perspective, without requiring source code access.

Deployed on-premises via Seceon CCE alongside network vulnerability assessment (OpenVAS) and aiSIEM event correlation, aiDAST360 helps security teams, MSSPs, and regulated organizations maintain continuous web application security with compliance-ready reporting.

Highlights

PASSIVE OT VISIBILITY & ASSET DISCOVERY

Non-intrusive identification of every PLC, RTU, HMI, SCADA server, and IIoT device. Deep packet inspection across 60+ industrial protocols delivers a real-time, accurate asset inventory.

AI-POWERED THREAT DETECTION

Patented AI/ML and behavioral analytics detect zero-day attacks, ICS malware, unauthorized PLC programming, and lateral movement without requiring manual rule writing.

SAFE FOR PRODUCTION

One-way SPAN/TAP-based passive monitoring at the cell area zone. Zero impact on PLCs, RTUs, or process safety. Purdue Model-aligned architecture.

CONTINUOUS COMPLIANCE

Built-in mapping to IEC 62443, NIST 800-82, NERC CIP, NIS 2, NCIIPC, and CMMC 2.0 with automated audit reporting and continuous posture monitoring.

Key Capabilities

- Top 100+ -check vulnerability catalog covering OWASP Web Top 10 (2021) and API Security Top 10 (2023)
- GraphQL security testing and business-logic checks (IDOR, mass assignment, rate limiting)
- SPA crawler and OpenAPI-driven API scan profiles for modern JavaScript and microservice apps
- 10+ authentication methods: OAuth2, OIDC, SAML, JWT, Kerberos, NTLM, form, basic, API key, mTLS
- ML-assisted false-positive reduction with an analyst feedback loop and periodic auto-retrain
- Blind SSRF / out-of-band (OOB) detection for advanced attack scenarios
- HAR-based request/response evidence, CVSS v3 scoring, CWE mapping, and remediation code snippets

Scan Profiles

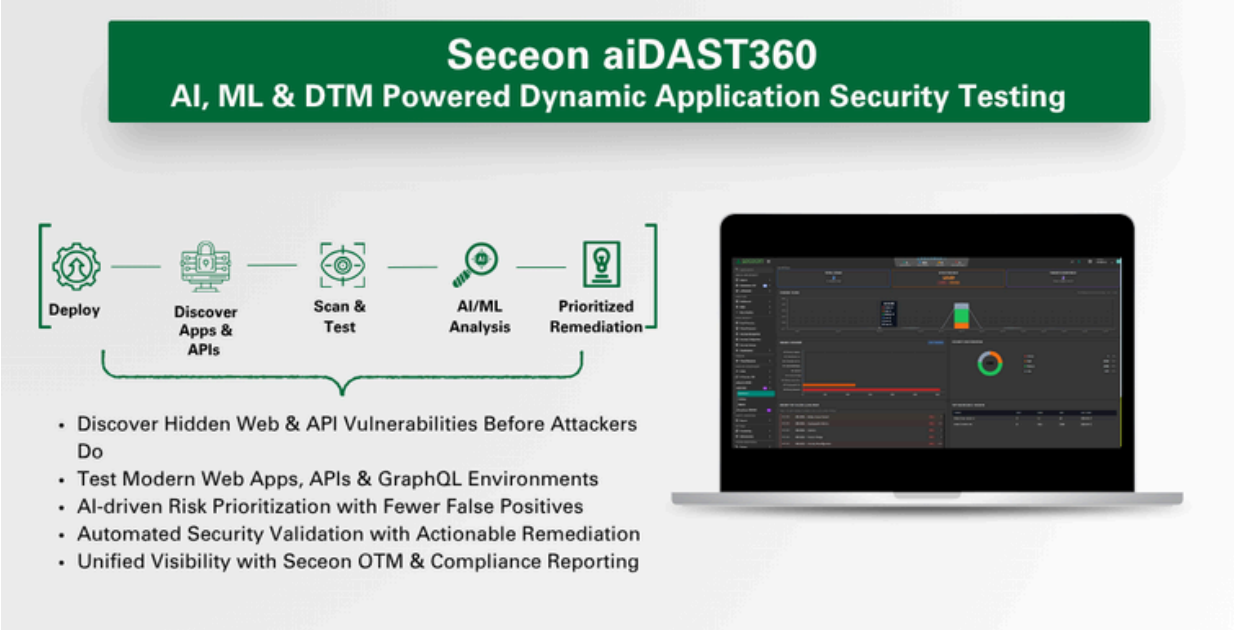
Profile	Duration	Description
Quick	30 minutes	Rapid smoke assessment for change validation
Standard	45 minutes	Balanced coverage for most web applications
Deep	90 minutes	Maximum crawl depth and active testing
API	30 minutes	OpenAPI/Swagger specification-driven API testing

OTM Platform Integration

- Co-deployed on Seceon CCE alongside OpenVAS network vulnerability assessment
- Findings stream via Seceon Event Format (SEF) to aiSIEM / SAPE for threat correlation
- MITRE ATT&CK mapping — T1190 (Exploit Public-Facing Application)
- ASM asset catalog sync with automatic scan triggering on new web/API assets
- Cross-tenant MSSP dashboard with risk scoring, open critical/high counts, and SLA aging
- Scheduled cron-based recurring scans with encrypted credential vault

Compliance & Reporting

- Automated control mapping: PCI DSS v4, ISO 27001:2022, NIST 800-53, NIST CSF 2.0, NIST SP 800-115
- HIPAA, CERT-In, and OWASP ASVS alignment per finding
- PDF compliance reports and full-assessment reports with optional tenant branding
- Finding aging / SLA reports with severity-based remediation targets
- JSON and CSV export for ticketing systems and GRC workflows



Seceon aiDAST360 continuously monitors web applications and APIs to detect exploitable vulnerabilities, validate security posture, and prioritize remediation using patented AI/ML-driven analytics.

Supported Compliance Frameworks

Framework	Mapping Scope
PCI DSS v4	Application security testing requirements (Req. 6 & 11)
ISO 27001:2022	Secure development, architecture, and security testing controls
NIST 800-53 / CSF 2.0	Vulnerability monitoring, input validation, and flaw remediation
NIST SP 800-115	Technical security testing guidance
HIPAA	Technical safeguards and risk analysis
CERT-In	Indian national cyber security guidance
OWASP ASVS	Application Security Verification Standard

Ideal Use Cases

- Web Application Security — continuous assessment of external and internal web properties
- API Security — REST, GraphQL, and microservice endpoint vulnerability testing
- MSSP Operations — multi-tenant DAST as a managed service on Seceon CCE
- Regulated Industries — PCI, HIPAA, and CERT-In compliance evidence and audit-ready reports
- Attack Surface Validation — pair ASM discoveries with automated DAST confirmation
- Pre-Production Gates — scheduled scans on staging environments before production release

Why Seceon aiDAST360

- Platform unity — one vendor for DAST, network VA, SIEM, and compliance (not disconnected SaaS tools)
- Beyond open-source ZAP — extended check library, Nuclei integration, and ML false-positive scoring
- Data sovereignty — on-premises CCE appliance; scan traffic and findings remain in your environment
- Lower TCO — incremental DAST on existing CCE estates without new vendor contracts
- Operational MSSP features — built-in multi-tenancy, scheduling, and cross-tenant risk visibility

Technical Highlights

- Runtime: cce-dast-zap + cce-dast-server containers on Seceon CCE host (loopback-secured control plane)
- Scan pipeline: ZAP spider → passive drain → active scan → Nuclei → custom Python check modules
- API gateway: REST endpoints for targets, scans, schedules, findings, reports, credentials, and ASM sync
- Evidence format: Seceon Event Format (SEF) with tenant_id, scan_id, compliance_tags, and confidence_score

About Seceon

Seceon simplifies cybersecurity for MSPs, MSSPs, and IT teams by reducing risk and complexity. Our AI and ML-powered aiSIEM and aiXDR platform provides comprehensive threat detection and response. By integrating data from logs, identity management, networks, endpoints, clouds, and applications, we deliver real-time, accurate alerts and automated remediation. Trusted by over 850 partners, Seceon supports more than 9,800 clients with efficient, high-margin security services and continuous compliance.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/