seceon
SECURITY FOR EONS

Seceon Vulnerability Assessment (VA)

Seceon Vulnerability Assessment (VA) is a native vulnerability scanning engine built into the Seceon CCE platform. It discovers assets across IP, range, and CIDR targets; detects network and service vulnerabilities; performs safe exploit probes; runs built-in web application security checks; and supports authenticated assessment of Linux, Windows, and Active Directory environments. Findings are enriched with threat intelligence (NVD, EPSS, CISA KEV), mapped to major compliance frameworks, prioritized by risk, and delivered as actionable PDF and CSV reports with remediation guidance

- **Unified scanning** for network, web, authenticated OS, Active Directory, containers, and cloud instance metadata, in a single pipeline
- **Threat-informed prioritization** using CVSS, EPSS, and CISA Known Exploited Vulnerabilities (KEV)
- **Built-in web application scanning** without a separate WAS product for basic coverage
- **Compliance-aware** findings mapped to CIS, PCI DSS, NIST CSF, ISO 27001, HIPAA, and SOC 2 Prescriptive remediation with solution and verification guidance
- **Native integration** with Seceon APE for multi-tenant job orchestration, progress, and report delivery

What Seceon VA Scans & Detects

Domains Covered in a Single Scan Pipeline

- Network services, ports, and protocol hardening (SSH, SSL/TLS, SMB, databases)
- Web applications and APIs discovered on HTTP/HTTPS services.

Highlights

Unified Multi-Domain Scanning

Network, web application, authenticated OS, Active Directory, container, and cloud posture checks run from one engine and one job pipeline.

Threat-Informed Prioritization

CVSS severity is combined with EPSS exploitlikelihood scoring and CISA KEV status to surface what actually needs attention first.

Authenticated Deep Assessment

SSH, SMB/WMI, and LDAP/LDAPS credentials enable kernel, patch, configuration, and identityhygiene checks beyond surface scanning.

Built-in Web App Security

Automatic OWASP-style DAST coverage injection, XSS, SSRF, XXE, and more runs the moment HTTP/HTTPS services are found.

Compliance-Ready Reporting

Every finding is tagged to CIS, PCI DSS, NIST CSF, ISO 27001, HIPAA, and SOC 2 for audit-ready scorecards.

- Authenticated Windows hosts via SMB/WMI patches, shares, settings
- Active Directory domain controllers via LDAP/LDAPS
- Containers Docker and Podman workloads, privilege and mount posture
- Cloud instance metadata AWS, Azure, and GCP IMDS posture

Safe, Non-Destructive Exploit Probes

Coverage includes Heartbleed, POODLE, DROWN, ROBOT, Log4Shell, Spring4Shell, EternalBlue, BlueKeep, SMBGhost, ZeroLogon, ProxyShell, and selected F5, Citrix, vCenter, SSH, and LDAP Log4Shell conditions

Web Application Checks (Auto-Triggered)

- SQL & command injection, reflected and DOM XSS, SSRF, XXE
- Local file inclusion / path traversal, CRLF injection, open redirect, SSTI
- Security headers, CSP, CORS misconfiguration, insecure cookies
- CSRF heuristics, JWT weaknesses, SRI gaps, WAF/WebSocket detection
- Sensitive file exposure, directory listing, WordPress/CMS checks

Active Directory Identity Hygiene

- Kerberoasting & AS-REP roasting exposure
- Unconstrained delegation, reversible encryption
- Privileged accounts with password never expires
- Weak domain password policy, anonymous LDAP bind

Containers & Cloud Posture

- Privileged containers, Docker socket exposure, root/dangerous capabilities
- AWS IMDSv1 vs IMDSv2 posture, hardcoded cloud credentials detection
- Azure & GCP instance metadata posture; optional cloud API auditors

VULNERABILITY ASSESSMENT CAPABILITIES	Network Scan	Web App Scan	Authenticated Scan
Asset discovery IP, range, CIDR, large target sets	✓		✓
Service fingerprinting & CVE correlation	✓		✓
SSL/TLS, SMB, and protocol hardening checks	✓		
Safe, non-destructive exploit probes	✓		
OWASP-style injection, XSS, SSRF, XXE testing		✓	
Security headers, CSP, CORS, cookie & JWT checks		✓	
Linux kernel, package & patch-level CVE audit			✓
Windows patch, share & security settings review			✓
Active Directory identity-hygiene checks			✓
Container workload & privilege posture			✓
Cloud IMDS & credential exposure posture			✓
CVSS + EPSS + CISA KEV risk enrichment	✓	✓	✓

VULNERABILITY ASSESSMENT CAPABILITIES	Network Scan	Web App Scan	Authenticated Scan
Compliance mapping (CIS, PCI, NIST, ISO, HIPAA, SOC 2)	✓	✓	✓
PDF, CSV & NDJSON reporting with remediation guidance	✓	✓	✓

Technical Highlights

Engine	Native Seceon VA scanner
Discovery	IP, range, CIDR with alive host probing — up to 4,096 hosts
Port Profiles	Quick / Full-Fast (default) / Full (TCP 1–65535)
Auth Methods	SSH, SMB/WMI, LDAP/LDAPS (Active Directory)
Web Checks	Built-in WAS, auto-triggered on discovered HTTP/HTTPS
Intelligence	NVD, EPSS, CISA KEV via Seceon Threat Intelligence
Risk Model	Severity + exploit signal + asset context + correlation (0–100 score)
Outputs	PDF, CSV, NDJSON
Orchestration	Seceon APE / Kafka job pipeline, multi-tenant

Compliance Frameworks Mapped

CIS Controls v8 PCI DSS NIST CSF ISO 27001 HIPAA Security Rule SOC 2 Trust Services Criteria

Reporting & Remediation

PDF report — executive summary, host/authentication summary, SLA-oriented prioritization, compliance scorecard, and detailed findings with CVSS, CWE, EPSS, CISA KEV, and remediation
CSV export — full finding inventory for SIEM, ticketing, or spreadsheet workflows
NDJSON log export — machine-readable records for SIEM ingestion
OS-aware remediation guidance — package, KB/WSUS/SCCM, and service-specific solution and verification text

Ideal Use Cases

Periodic internal & perimeter vulnerability assessments

Authenticated deep assessment of Linux and Windows estates

Active Directory identity risk discovery

Lightweight web app exposure checks alongside network VA

Container and cloud IMDS hardening reviews

Risk-based remediation planning using EPSS and CISA KEV

Compliance-oriented reporting for audit stakeholders

Multi-tenant VA delivery for MSP / MSSP operations

- Safe exploit probes are designed to be non-destructive assessment checks.
- Compliance mappings support reporting and gap analysis; they do not constitute formal certification.
- Web application scanning provides broad OWASP-style coverage for discovered web services; deep application penetration testing may still be performed with dedicated DAST where required.

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/