



Do more than detect vulnerabilities. Manage them end to end.

Ornis Vista brings together vulnerability data from different security products, penetration testing findings and manually entered records in one central platform. It maps findings to assets, assigns them to the appropriate team, tracks them through to closure against SLAs and provides management with measurable reports. It runs on your organization's own server.

VISIBILITY

VULNERABILITY

VULNERABILITY

From fragmented findings to one traceable process

Every finding enters the same lifecycle. Automated steps reduce record-keeping effort so teams can focus on remediation.



Finding sources and matching

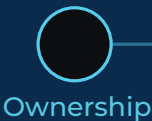
- ✓ Supported sources and formats: Nessus API/.nessus, OpenVAS XML, Qualys XML, CSV, Excel and JSON.
- ✓ Import penetration testing reports and manual findings; automatically recognize Turkish/English column headers.
- ✓ Column-mapping preview for CSV and Excel; report skipped rows with reasons.
- ✓ Display each source with a colour-coded label.
- ✓ Link to assets by IP, hostname, FQDN or URL; automatically create servers and web applications missing from inventory.
- ✓ Prevent a second record for the same vulnerability using asset, plugin ID, port, protocol and CVE fingerprints.

Secure and controlled import

- ✓ Reject macro-enabled Office files and read XML reports with a secure parser.
- ✓ Accept up to 100,000 rows in a single file.
- ✓ Preview findings from an incorrectly uploaded file and roll them back with confirmation, without affecting existing findings.
- ✓ Compare scan, host and severity counts in the source file against platform records.
- ✓ List findings that were not imported individually; show skipped or invalid rows with reasons.

One Owner

Every finding is assigned to a team and, when needed, an individual. If the team changes, findings and work orders move together.



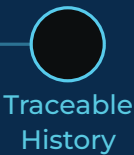
One Deadline

A remediation period runs according to severity; it pauses only in defined states and for a limited time.



One History

Assignment, status, severity, comment and SLA changes record who made them and when.



In Ornis Vista, every finding has an owner, a deadline and a history.

The right priority, owner and deadline for every finding

Scanner severity is only the starting point. Ornis Vista reassesses risk using asset importance and environmental conditions, preserving the rationale behind every decision.

Severity and context-based risk

- ✓ Critical, High, Medium, Low and Informational levels; finding and asset risk scores are refreshed nightly.
- ✓ Internet exposure, remote exploitability, active exploit, CISA KEV, EPSS, sensitive data and compensating-control impact.
- ✓ Administrators define weights and thresholds; history, SLA and risk are updated when the scanner reclassifies a finding.

Duplicate prevention and decision retention

- ✓ A fingerprint generated from the asset, plugin ID, port, protocol and CVE identifies the same vulnerability.
- ✓ A new scan does not create another record; last seen, occurrence count, scanner output and CVSS are updated.
- ✓ A false positive or manually closed finding is not reopened; it can be reopened manually and the SLA restarts.
- ✓ During full sync, unworked findings no longer reported may close only for assets that were rescanned.

Defined lifecycle

Open

In Progress

Pending (Third Party)

Risk Mitigated

Resolved

Risk Accepted

False Positive

Closed

Reopened

A justification is mandatory for closure and False Positive actions; evidence files may be attached. When all findings linked to a work order are closed, the work order is resolved automatically.

Assignment and routing

- ✓ Responsible asset team and owner; automatic assignment using people and teams in the penetration test file.
- ✓ Priority-ordered rules based on severity, asset type/tag, source-specific check ID/family and CVE.
- ✓ Assign critical and high findings to the team lead and others to the member with the lowest workload; test with samples before saving.
- ✓ Tiered authority for own team, other teams or the entire organisation; reasoned routing with "Not ours" and notification to the target team.

SLA policy and notifications

- ✓ Organisation-defined day-based periods for Critical, High, Medium and Low; when a period changes, only affected open findings and linked work orders are recalculated.
- ✓ Rule-based, limited pauses in In Progress and Pending (Third Party); a reason is mandatory for third-party waiting, and time restarts when the limit is exceeded.
- ✓ Hourly overdue marking; permanent storage of breach time and delay duration;
- ✓ SLA score from 1 to 5.
- ✓ Warnings in the final days, urgent notice on breach, and unassigned findings sent to the team lead; channel and quiet-hours preferences.
- ✓ Report open overdue and late-closed findings separately; calculate compliance consistently across the organisation. One daily digest replaces per-finding e-mail traffic; team-score thresholds are configurable.

Work orders synchronised with findings

- ✓ Open, In Progress, Pending, Resolved and Closed states; resolution description and closure reason are mandatory.
- ✓ Derive the due date from the finding SLA and add Pending time to the end.
- ✓ Open manually, in bulk, from asset details or automatically; two-way synchronisation of resolution and closure with findings.
- ✓ My Work Orders, Assigned to My Group, Created by Me and All; bulk status or assignment and Excel output.
- ✓ Views for open, in-progress and resolved work orders; SLA breaches, average resolution time and weekly trends.

Risk Acceptance Approval

An authorised manager approves requests opened with justification, validity and evidence; requesters cannot approve their own requests. Bulk approval and export.

Timeline

Status, assignment, severity, comments, attachments and SLA breaches; previous comments remain in the audit record.

Bulk Actions, Filters and Output

Filter by severity, status, CVSS, SLA, team, owner, asset or type, source, tag and date. A shared link opens the same view. Bulk-action notes are written separately to each finding's history; unauthorised records are skipped and reported. 22-column Excel/CSV/PDF output with formula-injection protection.

Assets, findings and work orders in one operational chain

Ornis Vista builds inventory from scans and carries ownership into findings and work orders. Planning and penetration testing are tracked on the same screen.



Inventory and ownership

- ✓ Servers, workstations, network devices, databases, web and mobile applications, cloud resources, containers and IoT devices.
- ✓ Criticality: Critical/High/Medium/Low; status: Active/Passive/Maintenance/Disabled. Preserve the history of deleted assets.
- ✓ Automatically identify Windows, Linux, macOS, iOS and Android families; assign types in bulk to filtered items with old and new values in the audit record.
- ✓ Assign responsible team and owner individually or in bulk and notify the assignee. Move open findings and work orders when the team changes; inherit ownership for new findings.

Asset visibility and data scope

- ✓ All assets or only team assets according to role scope; block link-based access to out-of-scope assets.
- ✓ Reflect ownership changes in findings and work orders; new findings inherit the team and owner from the asset.
- ✓ Block access to out-of-scope assets even when a link is shared.
- ✓ Preserve finding, work-order and audit history for deleted assets.

Bulk import and export

Excel, CSV or JSON template; update by IP or hostname, while blank cells leave existing data intact. Edit the team column and upload again for bulk assignment.

Authorisation register

SSH, RDP and VPN access; privileged, administrator, local/domain users and service accounts; sudo, database and backup permissions. Every update is audited.

Port analysis

Asset view by port, protocol and service; classify RDP, Telnet, SMB and database ports with the built-in risk catalogue and export to Excel.

ASSET DETAILS PAGE

Summary

Network, system, ownership, cloud, last scan, CVE and SLA

Findings

Severity/status, CVSS, port and first detected

Work Orders

One click for critical/high; SLA due date

Audit

Creation, update, bulk action and permissions

Planning: four views, five tabs

- ✓ Board (Kanban), List, Calendar and Timeline; All, Assigned to Me, My Team, Overdue and Archive tabs.
- ✓ Drag and drop across Open, In Progress, Pending and Resolved columns; open a new task from a column.
- ✓ Type, severity, team and owner filters; track findings and work orders on the same board.
- ✓ To-do list, colour-coded labels, file attachments and change history; assign to an individual.
- ✓ 10 MB per attachment; block executable file types for security.

Penetration testing: from report to closure

- ✓ Company/customer, 10 test types, project, technical/business owner, date and status; automatic project tag.
- ✓ Eight scope items including IP, IP block, domain, URL, mobile application and API; environment/criticality and import preview for Excel/CSV.
- ✓ Archive five report types, including initial test, retest, final and customer reports, plus raw XLSX/CSV findings within the project.
- ✓ Plan test rounds on a timeline with date, status and notes; show open, closed and reopened findings.
- ✓ Customer/project/date filter, severity/status, monthly trend, project and team on the pentest dashboard; PDF, Excel and CSV output.

The right view for everyone, from analyst to executive

The dashboard adapts to role and data scope. Management, teams and analysts see the portion of the same data that falls within their responsibility.

VISTA OVERVIEW

ILLUSTRATIVE INTERFACE AND DATA

OPEN FINDINGS

1.248

SLA BREACHES

84

RISK ACCEPTANCE

26

CLOSED

936



● Critical	42
● High	176
● Closed on time	%89

Dashboard and ready-made reports

- ✓ Cards for assets/findings, open, reopened, risk accepted, closed and SLA-breached items; open a filtered list from a card. Role management determines which cards each role sees.
- ✓ SLA compliance, MTTR, incoming/closed trend for the past 12 weeks, severity/status, finding age, risky assets, common CVEs, team performance, integrations and unassigned records.
- ✓ Sixteen reports: Executive Summary, SLA Compliance, Team Performance, process/MTTR/ageing/work order/closure/scan/usage, plus Trend and Top 10.

Executive and scheduled reporting

- ✓ Generate a branded Word/PDF executive report for the selected month with one click and compare it with the previous month: risk, vulnerability distribution, critical/high, trends, SLA, risky assets, teams, closed and new findings.
- ✓ Daily, weekly, fortnightly or monthly PDF/Excel/CSV reports; separate email for each team.
- ✓ Monthly critical/high summary; freeze team and individual SLA performance at the start of the month to create an immutable record.
- ✓ Live refresh of activity, connected users, new findings and logs; brute-force warning after repeated failed logins.

Ready-made report catalogue

Executive	SLA	Team	Process	Trend/Top 10
Assets, open items, SLA, scores and period activity	Compliance by severity; on-time/breach distribution	Open/closed, late-closed, SLA and MTTR	Ageing, work orders, closure, scans and usage	Risky assets, CVEs, urgent SLA and oldest open

Identity, directory and authorisation

- ✓ Email/password; hash passwords with Argon2. Google/Microsoft Authenticator TOTP; display the organisation name in the app.
- ✓ LDAP/Active Directory login and automatic account creation at first login; import organisational unit, department, team and manager relationships.
- ✓ Deactivate disabled directory accounts; preserve history through objectGUID/entryUUID even when name or email changes.
- ✓ Map LDAP groups to roles while preserving roles manually granted or removed by an administrator.
- ✓ Ten ready-made roles and custom organisational roles; module/action, menu/dashboard card and own/team/all data scope. Permission changes take effect without a new login.

Application security, audit and SIEM

- ✓ Password: at least 8 characters with upper/lower case, number and special character; reject common passwords. 30-minute reset window and hashed reset key.
- ✓ Reset passwords by email; store the 30-minute key in hashed form in the database.
- ✓ Close inactive sessions after 30 minutes; revoke the session key on logout or password change. HSTS, X-Frame-Options and Referrer-Policy; redirect HTTP to HTTPS when a certificate is configured; TLS 1.2/1.3 only.
- ✓ Encrypt TOTP secrets. Record login, failed attempt, password/MFA, user/role, asset, finding, work order, scan and report actions with who/when/IP.
- ✓ Record unauthorised attempts with missing permission/address/IP; filters, details and Excel. Default retention is five years and configurable.
- ✓ Log API create/update/delete operations with user, source IP and result; write audit and web access to separate LEEF 2.0 files. Mask passwords/tokens, omit request bodies, and forward to QRadar/SIEM through a shared request ID and rsyslog.

Audit chain from identity to SIEM

Identity	Authority	Trace	Correlation	Forwarding
LDAP/AD, email/password, TOTP	Role, action and data scope	Who, when and from which IP	Shared request ID	Separate LEEF 2.0 files, rsyslog

A secure, auditable architecture running on premises

The application and database are hosted on the organisation's Linux server. Updates are uploaded through the interface without requiring an internet connection.

On-premises deployment

- ✓ System service with PostgreSQL, Redis and Nginx; no Docker required.
- ✓ The installation script checks resources; optional SSL, firewall, SSH, file permissions and fail2ban.
- ✓ SLA checks, reports and scanner synchronisations are scheduled within the application without an additional job-queue service.

Encrypted offline updates

- ✓ Upload the AES-256 encrypted release package from System > Update.
- ✓ Automatic database backup first; roll back to the previous version if the update fails.
- ✓ Track progress, live logs and release notes on the same screen.

Self-maintenance

- ✓ Restart stopped services, check disk usage and rotate logs nightly and on restart.
- ✓ Weekly database backup.
- ✓ Connect application, database and Redis health endpoints to the organisation's monitoring tools.

Integrations and notifications

- ✓ Import data from security products via APIs or supported file formats; validate findings and map them to assets.
- ✓ Organisation SMTP (TLS/SSL): branded HTML templates for vulnerability, work order, asset, SLA, risk acceptance and system events.
- ✓ Webhook: send finding, work order, asset and scan events to Teams, Slack or an HTTP endpoint with an HMAC-SHA256 signature.
- ✓ SIEM: forward LEEF 2.0 audit and web access logs through rsyslog.

Corporate identity and usability

- ✓ White label: product name, company information, logo, favicon and login screen; the same identity in email and PDF.
- ✓ Turkish and English interface; switch language without refreshing the page.
- ✓ Light/dark theme; responsive on tablet and phone screens.
- ✓ Activation through the central portal or a signed offline licence for disconnected installations.

Deployment

Linux · PostgreSQL · Redis · Nginx · No Docker

Hardware

4 GB RAM · 20 GB disk · 2 cores recommended

Outputs

PDF · Excel · CSV · Word/PDF executive · LEEF 2.0

Who benefits from Ornis Vista?

Enterprise IT

Manage findings from different security products through a traceable workflow with clear ownership instead of Excel.

SOC and Security

Bring scan results, penetration testing findings and manual findings into a shared risk, SLA and closure workflow.

Penetration Test/ Audit

Move penetration testing findings into a workflow covering project management, retesting and verified closure.

Management and Performance

Provides an on-premises audit trail, monthly reports and frozen performance records.



Try it with your own data.

Ornis Vista runs in a 30-day trial mode without a licence key. Contact the İşNet team for installation and proof-of-concept (PoC) work.

Experience Ornis Vista in your organisation's security operations.

Demo and further information:

ornis.com.tr

info@ornis.com · 0850 290 0 290

