VIOE - Vulnerability Intelligence & Orchestration Engine

Product Owner & Business User Guide

Document Version: 1.0 **Classification:** Internal / Client-Facing **Last Updated:** January 2026

Table of Contents

1. Executive Summary

VIOE (Vulnerability Intelligence & Orchestration Engine) is an enterprise-grade security management platform that transforms how organizations identify, assign, and remediate security vulnerabilities. The platform leverages artificial intelligence to automatically assign vulnerability ownership, reduce noise from false positives, and accelerate the remediation lifecycle.

Key Business Outcomes:

- **80% reduction** in manual triage time through AI-powered ownership assignment
- **Significant noise reduction** via intelligent suppression rules
- **Accelerated remediation** through Jira integration and automated workflows
- **Compliance readiness** with built-in framework mapping (SOC 2, ISO 27001, GDPR, PCI DSS)

- **Predictive capabilities** to anticipate emerging threats before they materialize

---

2. What VIOE Does - Business Value

2.1 Core Value Proposition

VIOE solves the critical challenge of vulnerability management at scale. Traditional approaches require security teams to manually review thousands of findings, determine ownership, and track remediation—a process that is slow, error-prone, and unsustainable.

Before VIOE:

- Manual review of each vulnerability finding
- Hours spent determining which team should fix each issue
- Spreadsheets and emails to track remediation status
- No visibility into compliance posture
- Reactive response to emerging threats

With VIOE:

- AI automatically assigns vulnerabilities to the correct team
- Intelligent filtering removes false positives and non-actionable findings
- Integrated workflow tracks remediation from discovery to resolution
- Real-time compliance dashboards show framework alignment
- Predictive analysis anticipates threats before they impact the organization

2.2 Who Uses VIOE

User Type	Primary Activities
Security Analysts	Review vulnerabilities, validate AI assignments, create remediation tasks
Development Teams	Receive assigned vulnerabilities, implement fixes, track task status
Team Leads	Monitor team performance, review high-priority findings, manage workload
Compliance Officers	Generate compliance reports, track framework alignment, collect evidence
Security Managers	Executive dashboards, incident response, strategic planning
Administrators	Configure settings, manage teams, set up integrations

2.3 Key Capabilities Overview

Vulnerability Management

- Centralized view of all security findings across the organization
- Multi-source import (Snyk, SonarQube, Checkmarx, Qualys, Tenable, Rapid7)
- Severity-based prioritization (Critical, High, Medium, Low)

AI-Powered Ownership

- Automatic team assignment based on code ownership patterns
- Confidence scoring (High/Medium/Low) for transparency
- Git commit analysis and CODEOWNERS file parsing
- Directory integration (Okta, Active Directory)

Remediation Orchestration

- Task creation and tracking
- Bidirectional Jira synchronization
- Policy compliance checks
- Auto-fix generation with pull request workflows

Threat Intelligence

- Predictive vulnerability forecasting (30/60/90 days)
- STRIDE-based threat modeling
- Proactive threat hunting
- Incident response orchestration

Compliance & Governance

- Framework mapping (SOC 2, ISO 27001, GDPR, PCI DSS)
- Evidence collection and management
- Gap analysis and remediation roadmaps
- Policy recommendation engine

---

3. Getting Started

3.1 Accessing VIOE

Login Process:

1. Navigate to your organization's VIOE URL
2. Enter your credentials (email and password)
3. Complete multi-factor authentication if configured
4. You will be directed to the main Dashboard

[Screenshot Placeholder: Login screen with email and password fields]

First-Time Login:

- Your administrator will provide initial credentials
- You will be prompted to set a new password on first login
- Review and accept the terms of use

3.2 Navigation Overview

VIOE uses a left-side navigation panel with the following sections:

Navigation Item	Purpose
Dashboard	Main overview with key metrics and priority items
Advanced Dashboard	Deep analytics and strategic insights
Vulnerabilities	Browse and manage all vulnerability findings
Remediation Tasks	Track fix tasks and Jira integration
Assets	IT asset inventory with risk scoring
Teams	Team management and performance analytics
Incidents	Security incident response management
Threat Hunting	Proactive threat detection
Predictive Analysis	AI-powered forecasting
Threat Modeling	STRIDE analysis and attack vectors
Compliance Reports	Framework-based compliance assessment
Codebase Analysis	Source code security review
Settings	Configuration and administration

[Screenshot Placeholder: Main navigation panel showing all menu items]

3.3 Understanding Your Role

Your experience in VIOE depends on your assigned role:

If you are a Security Analyst:

- Focus on the Vulnerabilities page for daily triage
- Use the Dashboard to identify priority items
- Create remediation tasks for confirmed findings

If you are a Team Lead:

- Monitor your team's performance in the Teams section
- Review vulnerabilities assigned to your team
- Ensure remediation tasks are progressing

If you are a Compliance Officer:

- Generate compliance reports from the Compliance Reports section
- Track framework alignment scores
- Collect and manage evidence

If you are an Administrator:

- Configure suppression rules in Settings
- Manage teams and user assignments
- Set up scanner integrations

---

4. Core Workflows

4.1 Daily Vulnerability Review Workflow

Step 1: Start at the Dashboard

- Review the "Open Vulnerabilities" count
- Note any increase in Critical or High severity items
- Check the "Needs Review" section for items requiring attention

Step 2: Review Priority Vulnerabilities

- Click on any vulnerability card to view details
- Priority items are those with Critical or High severity that are unresolved

Step 3: Validate AI Assignment

- For each vulnerability, review the assigned team
- Check the confidence score (High = 90%+, Medium = 70-89%, Low = <70%)
- Accept the assignment or manually reassign if needed

Step 4: Create Remediation Tasks

- For confirmed vulnerabilities, create a remediation task
- Link to Jira if your organization uses Jira integration
- Set appropriate priority and due date

Step 5: Track Progress

- Monitor task status in the Remediation Tasks page
- Follow up on overdue or blocked items

[Diagram Placeholder: Flowchart showing the daily vulnerability review workflow from Dashboard to Task Creation]

4.2 Importing New Vulnerability Scans

Step 1: Navigate to Import

- From the Vulnerabilities page, click the "Import" button

Step 2: Upload Scan Results

- Drag and drop your scan file (CSV, JSON, Excel, or PDF)
- Or click to browse and select the file

Step 3: Processing

- VIOE will parse the file and extract vulnerability data
- AI will analyze each finding and suggest team ownership
- Progress bar shows: Upload (10%) → Extract (30%) → Process (60-90%)

Step 4: Review Results

- Upon completion, you'll see a summary of imported items
- Navigate to Vulnerabilities to review the new findings

Supported Formats:

- CSV files from most vulnerability scanners
- JSON exports from API-based tools
- Excel spreadsheets with vulnerability data
- PDF reports (text will be extracted)

4.3 Generating Compliance Reports

Step 1: Navigate to Compliance Reports

- Select "Compliance Reports" from the navigation menu

Step 2: Select Framework

- Choose the compliance framework: SOC 2, ISO 27001, GDPR, or PCI DSS
- Multiple frameworks can be selected for comparative analysis

Step 3: Generate Report

- Click "Generate Report"
- VIOE will analyze your vulnerability data against the framework controls

Step 4: Review Results

- **Overall Score:** Percentage of compliance (0-100%)
- **Gap Summary:** Count of Critical, High, and Medium gaps
- **Findings:** Specific non-compliance items with severity
- **Remediation Roadmap:** Prioritized actions to close gaps

Step 5: Export Evidence

- Generate an evidence package for auditors
- Evidence is organized by control with supporting documentation

4.4 Responding to Incidents

Step 1: Incident Detection

- New incidents appear in the Incidents page
- Critical incidents trigger immediate notifications

Step 2: Begin Investigation

- Click on the incident to view details
- Review AI assessment including threat level and blast radius
- Note affected assets and their isolation status

Step 3: Containment

- Review recommended containment actions
- Mark actions as completed as you progress
- Update status: Investigating → Containing

Step 4: Resolution

- Once the threat is mitigated, mark as Resolved
- Document findings in the incident timeline
- Complete post-incident review

---

5. Dashboard & Metrics Interpretation

5.1 Main Dashboard KPIs

Open Vulnerabilities

- *What it shows:* Total count of vulnerabilities with status "Open" or "In Progress"
- *Good trend:* Decreasing over time
- *Action if increasing:* Review import volume and remediation capacity

Critical & High Severity

- *What it shows:* Count of unresolved Critical and High severity vulnerabilities
- *Target:* Minimize to zero for Critical; manage High actively
- *Action if high:* Prioritize immediate remediation

AI Auto-Assigned %

- *What it shows:* Percentage of vulnerabilities automatically assigned by AI
- *Target:* 80%+ indicates effective AI configuration
- *Action if low:* Review AI settings and confidence thresholds

Noise Reduced

- *What it shows:* Count of findings suppressed by rules

- *Value:* Represents time saved by not reviewing false positives
- *Review periodically:* Ensure suppression rules aren't hiding real issues

5.2 Trend Analysis

Vulnerability Trend Chart

- Shows daily/weekly/monthly vulnerability counts over time
- Anomaly detection highlights unusual spikes
- Use to identify patterns and plan capacity

Severity Distribution

- Breakdown of Critical/High/Medium/Low over time
- Shift toward lower severity indicates improving security posture

Team Trends

- Which teams have the most vulnerabilities assigned
- Helps identify teams needing additional resources or training

Asset Trends

- Which assets have the most vulnerabilities
- Prioritize upgrades or replacements for problematic assets

5.3 Ownership Confidence Distribution

This chart shows the breakdown of AI assignment confidence:

Confidence Level	Meaning	Action
High (90%+)	AI is confident in team assignment	Accept assignment
Medium (70-89%)	Reasonable confidence, review recommended	Validate and adjust if needed
Low (<70%)	AI uncertain, manual review required	Manually assign to correct team
Unassigned	No team assigned yet	Immediate triage required

5.4 Advanced Dashboard Insights

The Advanced Dashboard provides deeper analytics:

Resolution Rate

- Percentage of vulnerabilities resolved vs. total identified
- Target: Consistently above 70%

Risk Reduction

- Measures improvement in overall security posture
- Calculated from resolved Critical/High items

Severity-Criticality Heatmap

- Cross-correlation of vulnerability severity with asset criticality
- Red zones require immediate attention

Attack Vector Analysis

- Distribution of vulnerabilities by attack type
- Helps prioritize security investments

---

6. Reports & Alerts

6.1 Available Reports

Compliance Reports

- Framework-specific compliance assessment
- Gap analysis with prioritized remediation steps
- Evidence packages for audit purposes

Team Performance Reports

- Vulnerabilities per team
- Resolution rates and response times
- Trend analysis

Asset Risk Reports

- Risk scores per asset
- Vulnerability counts by asset type
- Environment-based breakdown

Predictive Analysis Reports

- 30/60/90 day vulnerability forecasts
- Emerging threat predictions
- Recommended proactive actions

6.2 Alert Configuration

VIOE supports the following alert types:

Alert Type	Trigger	Default Timing
New Critical Vulnerability	Critical severity finding imported	Immediate
SLA Approaching	Remediation deadline nearing	48 hours before
Low Confidence Assignment	AI assignment below threshold	Immediate
Daily Summary	Digest of activity	Daily (configurable)

Configuring Alerts:

1. Navigate to Settings → Notifications
2. Toggle each alert type on or off
3. Alerts are delivered via the configured channel (email, Slack)

6.3 Interpreting Alert Messages

"Critical Vulnerability Detected"

- Meaning: A new Critical severity finding has been imported
- Action: Review immediately; Critical items have shortest SLA

"SLA Approaching for [Vulnerability Name]"

- Meaning: Remediation deadline is 48 hours away
- Action: Check task status; escalate if blocked

"Low Confidence Assignment for [Vulnerability Name]"

- Meaning: AI is uncertain about team ownership
- Action: Manually review and assign to correct team

---

7. Common Mistakes & Fixes

7.1 "I can't find a vulnerability I know exists"

Possible Causes:

1. The vulnerability may be suppressed by a rule
2. Filters may be hiding the item
3. The item may not have been imported yet

Fix:

- Clear all filters on the Vulnerabilities page
- Check Settings → Suppression Rules for matching rules
- Verify the scan file was successfully imported

7.2 "AI assigned a vulnerability to the wrong team"

This is normal and expected occasionally.

Fix:

1. Open the vulnerability detail page
2. Review the current assignment and confidence score
3. Click "Reassign" and select the correct team
4. The system will learn from this correction over time

7.3 "My dashboard shows zero vulnerabilities but I know we have issues"

Possible Causes:

1. No scan data has been imported
2. All vulnerabilities have been suppressed
3. All vulnerabilities have been resolved

Fix:

- Check if import has been completed successfully
- Review suppression rules in Settings
- Adjust filters to show resolved items

7.4 "Jira task status doesn't match VIOE"

Possible Cause: Synchronization delay or configuration issue

Fix:

1. Click "Sync Status" on the remediation task
2. Wait for sync to complete
3. If issue persists, check Jira integration settings

7.5 "Compliance report shows lower score than expected"

Possible Causes:

1. Open vulnerabilities affecting compliance controls
2. Missing evidence for certain controls
3. Recent findings not yet remediated

Fix:

- Review gap analysis to identify specific issues
- Remediate high-priority gaps first
- Ensure evidence is properly documented

7.6 "I'm seeing too many low-priority vulnerabilities"

Fix:

1. Create suppression rules for known acceptable risks
2. Use filters to focus on Critical and High severity
3. Consider environment-based suppression for non-production

---

8. Glossary of Business Terms

Term	Definition
Asset	Any IT resource (server, workstation, application, database) tracked in VIOE
Blast Radius	The potential scope of impact from a security incident
Compliance Framework	A set of security controls and requirements (e.g., SOC 2, ISO 27001)
Confidence Score	AI's certainty level (0-100%) when assigning vulnerability ownership
Critical Severity	Highest risk level; requires immediate attention
CVE	Common Vulnerabilities and Exposures; a unique identifier for security flaws
CVSS	Common Vulnerability Scoring System; standardized severity rating (0-10)
Evidence	Documentation proving compliance with a specific control
False Positive	A finding that appears to be a vulnerability but is not actually a risk
Gap	A deficiency in compliance with a framework control
High Severity	Serious risk requiring prompt remediation
Incident	A confirmed security event requiring response
Low Severity	Minor risk that can be addressed in normal cycles
Medium Severity	Moderate risk requiring planned remediation
Noise	Findings that are not actionable (false positives, duplicates, etc.)
Ownership	The team responsible for remediating a vulnerability
Remediation	The process of fixing or mitigating a vulnerability
Risk Score	A calculated value representing overall risk level of an asset
SLA	Service Level Agreement; the target timeframe for remediation
STRIDE	Threat modeling framework (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
Suppression Rule	A configuration that filters out certain findings from active tracking

Term	Definition
Threat Hunting	Proactive search for security threats not yet detected
Triage	The process of reviewing and prioritizing vulnerability findings
Vulnerability	A security weakness that could be exploited by attackers

---

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document is confidential and intended for authorized users only.

VIOE - Vulnerability Intelligence & Orchestration Engine *Transforming Security Operations Through Intelligent Automation*