VIOE - Vulnerability Intelligence & Orchestration Engine

Core Functional Specification

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

Table of Contents

1. Document Overview

1.1 Purpose

This Core Functional Specification serves as the single source of truth for VIOE functionality. It defines what each feature does, how it behaves, and the business rules governing system operations.

1.2 Audience

- Product Owners
- Business Analysts
- QA Teams
- Enterprise Clients
- Implementation Partners

1.3 Scope

This document covers all user-facing functionality of VIOE version 1.0. Technical implementation details are excluded; focus is on functional behavior and business outcomes.

---

2. System Overview

2.1 Product Description

VIOE (Vulnerability Intelligence & Orchestration Engine) is an enterprise vulnerability management platform that automates the identification, assignment, and remediation of security vulnerabilities through artificial intelligence.

2.2 Core Modules

Module	Primary Function
Vulnerability Management	Track and manage security findings
AI Ownership Assignment	Automatic team assignment
Remediation Management	Task tracking and workflow
Asset Management	IT resource inventory
Team Management	Organizational structure
Incident Response	Security event handling
Threat Intelligence	Proactive threat detection
Compliance & Governance	Framework alignment
Reporting & Analytics	Metrics and insights
Settings & Configuration	System administration
Data Import	Scanner integration

2.3 System Access

- **Authentication:** Required for all access
- **Authorization:** Role-based access control
- **Session Management:** Automatic timeout after inactivity

---

3. Vulnerability Management Module

3.1 Feature: Vulnerability List View

Description: Displays all vulnerability findings in a searchable, filterable list.

Inputs:

- User navigation to Vulnerabilities page
- Filter selections (optional)
- Search query (optional)

Outputs:

- List of vulnerability cards
- Pagination controls
- Filter summary
- Total count indicator

Filters Available:

Filter	Options
Severity	Critical, High, Medium, Low, Info
Status	Open, In Progress, Resolved, False Positive
Environment	Production, Staging, Development
Team	All configured teams
Confidence	High, Medium, Low, Unassigned
Triage Status	Pending, Triaged
Suppression	Active, Suppressed

Display Modes:

- Grid view (default): Cards in responsive grid
- List view: Tabular format with more details

Business Rules:

- Only non-suppressed vulnerabilities shown by default
- Results sorted by severity (Critical first), then by date
- Maximum 50 items per page

3.2 Feature: Vulnerability Detail View

Description: Comprehensive view of a single vulnerability finding.

Inputs:

- Vulnerability selection (click on card)

Outputs:

- Full vulnerability details panel

- Ownership information panel
- Remediation tasks list
- Action buttons

Information Displayed:

Field	Description
Title	Vulnerability name/description
CVE ID	Common Vulnerabilities and Exposures identifier
CVSS Score	Severity score (0-10)
Severity	Critical/High/Medium/Low/Info
Status	Current resolution status
Environment	Where the vulnerability exists
Asset	Affected system or component
Assigned Team	Owning team
Confidence Score	AI assignment confidence
Created Date	When first detected
Description	Full technical description
Remediation	Recommended fix approach

Available Actions:

- Accept Assignment: Confirm team ownership
- Reassign: Change owning team
- Update Status: Change resolution status
- Create Task: Generate remediation task
- Mark as False Positive: Remove from active tracking
- View History: See ownership changes

3.3 Feature: Vulnerability Triage

Description: Process of reviewing and prioritizing vulnerability findings.

Inputs:

- Vulnerability in "Pending" triage status
- Triage action trigger (button click)

Process:

1. System invokes AI analysis
2. AI determines likely team ownership
3. Confidence score calculated
4. Team assignment applied
5. Triage status updated to "Triaged"

Outputs:

- Updated team assignment
- Confidence score
- Ownership history record
- Status change notification

Business Rules:

- Triage can only be performed on "Pending" items
- AI assignment respects configured confidence threshold
- Manual override always allowed
- All changes logged to ownership history

3.4 Feature: Status Management

Description: Track vulnerability resolution progress through defined states.

Status Values:

Status	Description	Next States
Open	Newly identified	In Progress, False Positive
In Progress	Being addressed	Resolved, Open, False Positive
Resolved	Fix verified	Open (reopen if needed)
False Positive	Not a real issue	Open (if reassessed)

Status Transition Rules:

- Open → In Progress: When remediation begins
- In Progress → Resolved: When fix is verified
- Any → False Positive: When determined not actionable
- Resolved → Open: If vulnerability reoccurs
- False Positive → Open: If determination changes

---

4. AI Ownership Assignment Module

4.1 Feature: Automatic Team Assignment

Description: AI-powered determination of which team should own a vulnerability.

Inputs:

- Vulnerability data (affected files, asset, description)
- Configured AI data sources
- Team definitions

Process:

1. Analyze vulnerability metadata
2. Query enabled data sources:
    - Git commit history (who modified affected code)
    - CODEOWNERS file mappings
    - Directory integration (organizational structure)
3. Correlate findings to teams
4. Calculate confidence score
5. Apply assignment if above threshold

Outputs:

- Team assignment
- Confidence score (0-100%)
- Assignment rationale

Confidence Calculation:

Factor Agreement	Confidence Level
All sources agree	90-100% (High)
Most sources agree	70-89% (Medium)
Sources disagree	Below 70% (Low)
No data available	0% (Unassigned)

4.2 Feature: Bulk Triage

Description: Process multiple vulnerabilities simultaneously.

Inputs:

- Selection of multiple vulnerabilities
- Bulk triage action trigger

Process:

1. Queue selected vulnerabilities
2. Process each through AI assignment
3. Apply assignments based on threshold
4. Generate summary report

Outputs:

- Assignment count (successful)
- Low confidence count (requires review)
- Failed count (no assignment possible)

Constraints:

- Maximum 100 items per bulk operation
- Processing is sequential (not parallel)
- Low confidence items flagged for manual review

4.3 Feature: Manual Reassignment

Description: Override AI assignment with manual team selection.

Inputs:

- Vulnerability identifier
- Target team selection
- (Optional) Reassignment reason

Outputs:

- Updated team assignment
- Ownership history record
- Notification to new team

Business Rules:

- Any user with appropriate permissions can reassign
- Original assignment retained in history
- Manual assignments marked as "Manual Override"
- System may learn from manual corrections

4.4 Feature: Ownership History

Description: Complete audit trail of ownership changes.

Recorded Data:

Field	Description
Timestamp	When change occurred
Previous Team	Team before change
New Team	Team after change
Change Type	AI Assignment / Manual Reassignment
Confidence Score	AI confidence at time of assignment
Changed By	User who made change (for manual)

---

5. Remediation Management Module

5.1 Feature: Task Creation

Description: Generate remediation tasks from vulnerabilities.

Inputs:

- Source vulnerability
- Task details (title, description, priority)
- Assigned team (inherited or specified)

Outputs:

- New remediation task record
- Link to source vulnerability
- Task card in Remediation Tasks list

Task Fields:

Field	Description	Required
Title	Task name	Yes
Description	What needs to be done	Yes
Priority	Urgency level	Yes
Assigned Team	Responsible team	Yes
Status	Current progress	Auto-set
Vulnerability Link	Source vulnerability	Auto-set
Jira Issue Key	External ticket (if synced)	No
Policy Check Status	Compliance verification	Auto-set

5.2 Feature: Task Status Tracking

Description: Monitor remediation progress through defined states.

Status Values:

Status	Description	Color
Todo	Not yet started	Gray
In Progress	Work underway	Blue
In Review	Fix awaiting verification	Yellow
Completed	Successfully resolved	Green
Blocked	Cannot proceed	Red

Transition Rules:

- Todo → In Progress: Work begins
- In Progress → In Review: Fix submitted
- In Review → Completed: Fix verified
- Any → Blocked: Impediment identified
- Blocked → In Progress: Impediment resolved

5.3 Feature: Jira Integration

Description: Bidirectional synchronization with Jira.

Create Jira Issue:

- Inputs: Task data, Jira project configuration
- Process: Create issue in configured Jira project
- Outputs: Jira issue key, link to issue

Sync Jira Status:

- Inputs: Task identifier, sync trigger
- Process: Query Jira for current status, update VIOE
- Outputs: Updated task status, sync timestamp

Field Mapping:

VIOE Field	Jira Field
Title	Summary
Description	Description
Priority	Priority
Status	Status
Assigned Team	Assignee/Team

5.4 Feature: Policy Compliance Check

Description: Verify remediation meets organizational policies.

Inputs:

- Completed remediation task
- Policy check trigger

Process:

1. Evaluate fix against defined policies
2. Check for required approvals
3. Verify documentation completeness
4. Assess risk acceptance (if applicable)

Outputs:

- Policy Check Status: Passed / Warning / Failed / Pending
- Compliance notes
- Required actions (if any)

5.5 Feature: Auto-Fix Generation

Description: AI-generated code fixes for vulnerabilities.

Inputs:

- Vulnerability details
- Affected code location
- Auto-fix trigger

Process:

1. Analyze vulnerability type
2. Generate remediation code
3. Present fix for review
4. Create pull request (if approved)

Outputs:

- Generated fix code
- Confidence assessment
- Pull request (optional)

Constraints:

- Available for supported vulnerability types only
- Requires human review before application
- May not address all vulnerability variants

---

6. Asset Management Module

6.1 Feature: Asset Inventory

Description: Central registry of IT assets tracked by VIOE.

Asset Fields:

Field	Description	Values
Asset Name	Unique identifier	Text
Asset Type	Category	Server, Workstation, Cloud Resource, Database, Application, Software License
Criticality	Business importance	Critical, High, Medium, Low
Environment	Deployment context	Production, Staging, Development
Risk Score	Calculated risk level	0-100
Vulnerability Count	Associated findings	Integer

6.2 Feature: Asset Creation

Description: Add new assets to the inventory.

Inputs:

- Asset details (name, type, criticality, environment)

Outputs:

- New asset record
- Initial risk score calculation

Validation Rules:

- Asset name must be unique
- All required fields must be populated
- Environment must match valid values

6.3 Feature: Risk Score Calculation

Description: Automated risk assessment per asset.

Calculation Factors:

Factor	Weight
Critical vulnerability count	High
High vulnerability count	Medium
Medium/Low vulnerability count	Low
Asset criticality	Multiplier
Environment	Multiplier

Risk Score Ranges:

Score	Risk Level	Color
0-25	Low	Green
26-50	Medium	Yellow
51-75	High	Orange
76-100	Critical	Red

6.4 Feature: Asset Filtering

Description: Filter asset inventory view.

Available Filters:

- Asset Type
- Criticality Level
- Environment
- Risk Score Range
- Search (name)

---

7. Team Management Module

7.1 Feature: Team Creation

Description: Define organizational teams for vulnerability ownership.

Inputs:

Field	Description	Required
Team Name	Display name	Yes
Lead Email	Team lead contact	Yes
Slack Channel	Notification channel	No

Outputs:

- New team record
- Team available for assignments

7.2 Feature: Team Performance Analytics

Description: Metrics showing team vulnerability management effectiveness.

Metrics Displayed:

Metric	Description
Total Vulnerabilities	All assigned to team
Critical Count	Critical severity assigned
High Count	High severity assigned
Open Count	Unresolved items
Resolved Count	Successfully closed
Resolution Rate	% resolved vs. total

7.3 Feature: Team Notifications

Description: Alert team members of new assignments.

Notification Triggers:

- New vulnerability assigned
- Critical vulnerability assigned
- SLA approaching
- Low confidence assignment

Channels:

- Email to team lead
- Slack channel post (if configured)

---

8. Incident Response Module

8.1 Feature: Incident Tracking

Description: Monitor and manage security incidents.

Incident Fields:

Field	Description
Incident ID	Unique identifier
Severity	Critical / High
Status	Detection through closure
Detection Time	When identified
Affected Assets	Systems impacted
AI Assessment	Automated analysis

8.2 Feature: Incident Status Flow

Status Progression:

Status	Description	Next Status
Detected	Initial identification	Investigating
Investigating	Analysis underway	Containing
Containing	Mitigation in progress	Resolved
Resolved	Threat eliminated	Closed
Closed	Post-mortem complete	-

8.3 Feature: AI Assessment

Description: Automated incident analysis.

Assessment Components:

Component	Description
Threat Level	Severity assessment
Blast Radius	Potential impact scope
Potential Impact	Business consequences
Recommended Actions	Containment suggestions

8.4 Feature: Containment Actions

Description: Track mitigation activities.

Action Fields:

Field	Description
Action Description	What needs to be done
Status	Pending, In Progress, Completed, Failed
Assigned To	Responsible party
Completion Time	When finished

8.5 Feature: Incident Timeline

Description: Chronological record of incident events.

Timeline Entry Fields:

Field	Description
Timestamp	When event occurred
Event Type	Action, Update, Note
Description	Event details
Actor	Who performed action

---

9. Threat Intelligence Module

9.1 Feature: Threat Hunting

Description: Proactive search for security threats.

Functions:

Function	Description
Detect Threats	Analyze patterns for active threats
Predict Vulnerabilities	Forecast emerging risks
Create Hunt	Custom hunting session

9.2 Feature: Threat Alerts

Description: Notifications of detected threats.

Alert Fields:

Field	Description
Detection Time	When identified
Severity	Critical / High
Status	New / Acknowledged / Resolved
Alert Details	Threat information

9.3 Feature: Predictive Analysis

Description: AI-powered vulnerability forecasting.

Prediction Outputs:

Output	Description
Emerging Threats	Not yet in portfolio, likely to appear
Vulnerability Patterns	Trends in finding types
Architectural Risks	System areas at risk
Recommendations	Proactive actions

Prediction Periods:

- 30 days
- 60 days
- 90 days

9.4 Feature: Threat Modeling

Description: STRIDE-based threat analysis.

STRIDE Categories:

Category	Description
Spoofing	Identity/authentication threats
Tampering	Data modification threats
Repudiation	Audit/accountability threats
Information Disclosure	Confidentiality threats
Denial of Service	Availability threats
Elevation of Privilege	Authorization threats

Model Outputs:

Output	Description
Risk Matrix	Critical/High/Medium/Low counts
Attack Vectors	Potential attack methods
Trust Boundaries	Security perimeters
Mitigations	Recommended controls

---

10. Compliance & Governance Module

10.1 Feature: Compliance Reporting

Description: Assessment against security frameworks.

Supported Frameworks:

Framework	Description
SOC 2	Service Organization Controls
ISO 27001	Information Security Management
GDPR	Data Protection Regulation
PCI DSS	Payment Card Industry Standard

10.2 Feature: Compliance Assessment

Description: Evaluate vulnerability data against framework controls.

Outputs:

Output	Description
Overall Score	0-100% compliance
Framework Scores	Per-framework assessment
Gap Summary	Critical/High/Medium gaps
Findings	Specific non-compliance items
Remediation Roadmap	Prioritized action plan

10.3 Feature: Evidence Collection

Description: Gather proof of compliance.

Evidence Package Contents:

Element	Description
Control ID	Framework control reference
Control Description	What the control requires
Compliance Status	Compliant / Partial / Non-Compliant
Evidence Items	Supporting documentation
Evidence Strength	Strong / Adequate / Weak / Missing

10.4 Feature: Policy Recommendations

Description: Suggest organizational policy updates.

Recommendation Fields:

Field	Description
Policy Area	Affected policy domain
Current Gap	What's missing
Recommendation	Suggested improvement
Priority	Implementation urgency
Expected Impact	Compliance improvement

---

11. Reporting & Analytics Module

11.1 Feature: Dashboard KPIs

Description: Key performance indicators displayed on main dashboard.

KPI Definitions:

KPI	Calculation	Target
Open Vulnerabilities	Count(status IN ['open', 'in_progress'])	Decreasing
Critical & High	Count(severity IN ['critical', 'high'] AND status != 'resolved')	Minimize
AI Auto-Assigned %	(assigned_team count / total) * 100	>80%
Noise Reduced	Count(is_suppressed = true)	Track trend

11.2 Feature: Trend Analysis

Description: Time-series visualization of vulnerability data.

Trend Types:

Trend	Description
Vulnerability Trend	Count over time
Severity Trend	Distribution over time
Team Trend	Per-team counts
Asset Trend	Per-asset counts

Anomaly Detection:

- Compares current period to historical baseline
- Highlights unusual spikes or drops
- Provides trend summary

11.3 Feature: Advanced Analytics

Description: Deep-dive analytical capabilities.

Analytics Components:

Component	Description
Resolution Rate	% resolved vs. identified
Risk Reduction	Security posture improvement
Severity-Criticality Heatmap	Cross-correlation analysis
Attack Vector Distribution	Vulnerability type breakdown

11.4 Feature: Ownership Confidence Distribution

Description: Visualization of AI assignment confidence levels.

Distribution Categories:

Category	Criteria
High	Confidence >= 90%
Medium	70% <= Confidence < 90%
Low	Confidence < 70%
Unassigned	No team assigned

---

12. Settings & Configuration Module

12.1 Feature: Suppression Rules

Description: Configure automatic filtering of findings.

Rule Types:

Type	Description
Environment	Filter by environment
Asset Pattern	Regex match on asset
Severity + Environment	Combined filter
Duplicate	Same CVE in same asset
Age-Based	Findings older than threshold

Rule Fields:

Field	Description
Name	Rule identifier
Type	Rule category
Conditions	Filter criteria
Active	Enabled/disabled
Suppressed Count	Items filtered

12.2 Feature: AI Configuration

Description: Configure AI ownership assignment behavior.

Configuration Options:

Option	Description
Git Commit Analysis	Analyze code history
CODEOWNERS Parsing	Use CODEOWNERS files
Directory Integration	Use Okta/AD mapping
Confidence Threshold	Minimum acceptance level

12.3 Feature: Integration Management

Description: Configure external system connections.

Supported Integrations:

Integration	Purpose
Snyk	Vulnerability import
SonarQube	Code analysis import
Checkmarx	SAST import
Qualys	Infrastructure scanning
Tenable	Vulnerability scanning
Rapid7	Security assessment
Jira	Task management
Slack	Notifications

12.4 Feature: Notification Preferences

Description: Configure alert settings.

Notification Types:

Type	Description	Default
New Critical Vulnerability	Immediate alert	ON
SLA Approaching	48-hour warning	ON
Low Confidence Assignment	Review required	ON
Daily Summary	Daily digest	ON

---

13. Data Import Module

13.1 Feature: File Upload

Description: Import vulnerability data from files.

Supported Formats:

Format	Extensions
CSV	.csv
JSON	.json
Excel	.xlsx, .xls
PDF	.pdf

13.2 Feature: Import Processing

Description: Parse and process uploaded data.

Processing Steps:

Step	Progress	Description
Upload	0-10%	File transfer
Extract	10-30%	Data parsing
Process	30-90%	AI ownership + creation
Complete	100%	Summary display

13.3 Feature: AI Ownership During Import

Description: Automatic team assignment during bulk import.

Process:

1. Extract vulnerability records
2. For each record, invoke AI analysis
3. Assign team based on confidence threshold
4. Create vulnerability record with assignment

Outputs:

- Import count (total)
- Assigned count (AI successful)
- Needs Review count (low confidence)

13.4 Feature: Deduplication

Description: Prevent duplicate vulnerability records.

Deduplication Logic:

- Match on CVE ID + Asset combination
- Skip if exact match exists
- Update if partial match with new data

---

14. User Flows

14.1 Flow: Daily Vulnerability Review

```
Start → Dashboard
  ↓
Review KPIs → Identify priority items
  ↓
Navigate to Vulnerabilities
  ↓
Filter by severity (Critical, High)
  ↓
Select vulnerability → View detail
```

```
  ↓
Review AI assignment → Accept or Reassign
  ↓
Create remediation task (if needed)
  ↓
Update status → Move to next item
  ↓
End
```

14.2 Flow: Vulnerability Import

```
Start → Vulnerabilities page
  ↓
Click Import button
  ↓
Drag/drop or browse for file
  ↓
System uploads file
  ↓
System extracts data
  ↓
System processes with AI assignment
  ↓
View completion summary
  ↓
Navigate to vulnerabilities list
  ↓
End
```

14.3 Flow: Incident Response

```
Start → Incident detected (notification)
  ↓
Navigate to Incidents page
  ↓
Click incident card → View details
  ↓
Review AI assessment
  ↓
Begin investigation (status update)
  ↓
Review affected assets
```

```
  ↓
Execute containment actions
  ↓
Document in timeline
  ↓
Mark as resolved when complete
  ↓
End
```

14.4 Flow: Compliance Reporting

```
Start → Compliance Reports page
  ↓
Select framework(s)
  ↓
Click Generate Report
  ↓
System analyzes data
  ↓
View overall score
  ↓
Review gap summary
  ↓
View specific findings
  ↓
Review remediation roadmap
  ↓
Generate evidence (optional)
  ↓
End
```

---

15. Business Rules

15.1 Vulnerability Rules

Rule	Description
VR-001	All vulnerabilities must have a severity
VR-002	Status transitions follow defined state machine
VR-003	False positive status bypasses remediation
VR-004	Suppressed items excluded from active counts
VR-005	Critical severity triggers immediate notification

15.2 Ownership Rules

Rule	Description
OR-001	AI assignment respects confidence threshold
OR-002	Manual reassignment always overrides AI
OR-003	All changes logged to ownership history
OR-004	Low confidence items flagged for review
OR-005	One team per vulnerability at any time

15.3 Remediation Rules

Rule	Description
RR-001	Tasks inherit team from source vulnerability
RR-002	Status transitions follow defined workflow
RR-003	Jira sync is bidirectional when enabled
RR-004	Completed tasks trigger policy check
RR-005	Blocked status requires impediment description

15.4 SLA Rules

Rule	Description
SR-001	Critical severity: 7 day SLA (default)
SR-002	High severity: 30 day SLA (default)
SR-003	Medium severity: 60 day SLA (default)
SR-004	Low severity: 90 day SLA (default)
SR-005	SLA approaching alert at 48 hours

15.5 Suppression Rules

Rule	Description
SUP-001	Only active rules suppress findings
SUP-002	Suppressed items retain audit trail
SUP-003	Multiple rules can apply to same finding
SUP-004	Suppression does not delete data
SUP-005	Rule changes do not retroactively unsuppress

---

16. Constraints & Limitations

16.1 System Constraints

Constraint	Description
SC-001	Maximum 100 items per bulk operation
SC-002	Maximum 50 items per page in list views
SC-003	File upload limit: 50MB
SC-004	Concurrent users: Based on deployment
SC-005	Data retention: Configurable per policy

16.2 Functional Limitations

Limitation	Description
FL-001	Auto-fix available for supported types only
FL-002	AI accuracy depends on data quality
FL-003	Compliance scoring based on mapped controls
FL-004	Predictive analysis requires historical data
FL-005	Real-time sync may have latency

16.3 Integration Limitations

Limitation	Description
IL-001	Jira sync requires API access
IL-002	Slack integration requires workspace auth
IL-003	Scanner APIs may have rate limits
IL-004	Directory sync is periodic, not real-time
IL-005	PDF parsing may have accuracy limitations

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document is the single source of truth for VIOE functionality.

VIOE - Vulnerability Intelligence & Orchestration Engine *Core Functional Specification*