VIOE Product Owner & Business User Guide

Vulnerability Intelligence & Ownership Engine

Version 1.0 | 1/13/2026

1. Introduction

What VIOE Does (Business Value)

VIOE (Vulnerability Intelligence & Ownership Engine) is an AI-powered security operations platform that helps organizations identify, manage, and resolve security vulnerabilities faster and more efficiently. The platform automatically assigns vulnerabilities to the right teams, predicts potential security threats, and ensures your organization maintains compliance with industry standards.

Key Business Benefits:
ï¿½ Reduce Security Risk: Identify and fix vulnerabilities before attackers exploit them
ï¿½ Save Time: AI automatically assigns work to the right teams, eliminating manual triage
ï¿½ Ensure Compliance: Automated mapping to regulatory frameworks (SOC 2, ISO 27001, NIST, CIS)
ï¿½ Proactive Protection: Predict and prevent future threats using AI threat intelligence

Who This Guide Is For

This guide is designed for:
ï¿½ Product Owners who need to understand system capabilities
ï¿½ Business Operators managing day-to-day security operations
ï¿½ Security Managers overseeing vulnerability programs
ï¿½ Executives making strategic security decisions

No programming or security engineering knowledge is required to use this guide or operate VIOE.

Problems VIOE Solves

Traditional Challenge: Organizations receive hundreds of security alerts daily, but lack the resources to manually review and assign each one. This leads to delays, missed critical issues, and unclear accountability.

VIOE Solution: AI automatically reviews every security finding, assigns it to the appropriate team with high confidence, and prioritizes remediation based on actual risk to your business.

Before VIOE:
ï¿½ Manual vulnerability triage takes days or weeks
ï¿½ Unclear ownership leads to vulnerabilities falling through cracks
ï¿½ Compliance audits require weeks of manual evidence gathering
ï¿½ Security teams react to incidents instead of preventing them

With VIOE:
ï¿½ Instant AI-powered triage and assignment
ï¿½ Clear ownership with confidence scoring
ï¿½ Automated compliance evidence collection
ï¿½ Proactive threat hunting prevents incidents

2. Getting Started

Accessing the Application

Step 1: Open your web browser (Chrome, Firefox, Safari, or Edge recommended)
Step 2: Navigate to your organization's VIOE URL (typically: https://your-company.vioe.app)
Step 3: Bookmark this page for quick access in the future

Note: Contact your IT administrator if you don't have your organization's VIOE URL.

Login Process

1. Enter your company email address in the Email field
2. Enter your password in the Password field
3. Click the 'Sign In' button
4. If two-factor authentication is enabled, enter the 6-digit code from your authenticator app
5. You'll be directed to the main Dashboard

Important: Your login credentials are the same as your company email system.

Password Reset

If you've forgotten your password:
1. Click 'Forgot Password' on the login screen
2. Enter your email address
3. Check your email for a password reset link
4. Click the link and create a new password
5. Return to VIOE and log in with your new password

Password Requirements: Minimum 8 characters, including uppercase, lowercase, and numbers.

First-Time User Setup

Upon your first login, complete these quick setup steps:

1. Profile Verification:
   ï¿½ Confirm your full name is correct
   ï¿½ Verify your role and team assignment
   ï¿½ Update your profile picture (optional)

2. Notification Preferences:
   ï¿½ Choose how you want to receive alerts (email, in-app, or both)
   ï¿½ Set your working hours for intelligent notification timing
   ï¿½ Select which types of alerts are most important to you

3. Dashboard Customization:
   ï¿½ The system will show you a brief tour of key features
   ï¿½ You can customize which widgets appear on your dashboard
   ï¿½ Set your default views and filters

This setup takes approximately 3-5 minutes and greatly improves your experience.

3. Core Application Overview

Dashboard - Your Command Center

What it is: The Dashboard is your home screen that provides an at-a-glance view of your organization's security posture.

Why it matters: It helps you quickly identify what needs attention and track progress over time.

When to use it: Check the Dashboard daily (typically first thing in the morning) to stay informed about your security status.

Key Metrics Shown:
ï¿½ Open Vulnerabilities: Current security issues requiring attention
ï¿½ Critical & High Priority Items: Most urgent issues
ï¿½ AI Auto-Assignment Rate: How effectively AI is routing work
ï¿½ Noise Reduction: How many low-priority alerts were filtered out

Vulnerabilities Module

What it is: A centralized view of all security vulnerabilities discovered in your environment.

Why it matters: This is where you track, prioritize, and manage security issues from discovery to resolution.

When to use it:
ï¿½ Daily: Review newly discovered vulnerabilities
ï¿½ Weekly: Check progress on remediation efforts
ï¿½ Monthly: Analyze trends and patterns

Key Features:
ï¿½ Filter by severity, status, team, or environment
ï¿½ View AI-assigned ownership with confidence scores
ï¿½ See remediation recommendations
ï¿½ Track resolution progress

Remediation Tasks Module

What it is: Actionable work items created to fix vulnerabilities.

Why it matters: Transforms security findings into trackable work with clear owners and deadlines.

When to use it:
ï¿½ Assign specific remediation work to team members
ï¿½ Track completion status
ï¿½ Generate reports for stakeholders
ï¿½ Integrate with project management tools like Jira

Key Features:
ï¿½ AI-estimated effort and complexity
ï¿½ Subtask breakdown for complex fixes
ï¿½ Integration with existing ticketing systems
ï¿½ Policy compliance checking

Incident Response Module

What it is: Coordinated response to active security incidents.

Why it matters: When a security incident occurs, quick and organized response minimizes damage.

When to use it:
ï¿½ When a vulnerability is actively exploited

ï¿½ During security alerts requiring immediate action
ï¿½ To coordinate response across multiple teams

Key Features:
ï¿½ AI-powered triage and prioritization
ï¿½ Automated containment recommendations
ï¿½ Incident timeline tracking
ï¿½ Response playbook suggestions

Threat Hunting Module

What it is: Proactive search for hidden threats and vulnerabilities.

Why it matters: Identifies security issues before they're exploited, staying ahead of attackers.

When to use it:
ï¿½ Weekly: Run automated threat analysis
ï¿½ After major system changes
ï¿½ When new threat intelligence emerges
ï¿½ For proactive security assessments

Key Features:
ï¿½ AI-powered pattern detection
ï¿½ Behavioral anomaly identification
ï¿½ Threat correlation across assets
ï¿½ Predictive vulnerability identification

Compliance Module

What it is: Automated compliance tracking and evidence generation for regulatory frameworks.

Why it matters: Ensures you meet industry requirements (SOC 2, ISO 27001, NIST, CIS) without manual work.

When to use it:
ï¿½ Monthly: Generate compliance reports
ï¿½ Before audits: Collect evidence packages
ï¿½ Quarterly: Review compliance scores
ï¿½ When policies need updates

Key Features:
ï¿½ Automated control mapping
ï¿½ Evidence generation
ï¿½ Gap analysis
ï¿½ Policy update recommendations

Asset Management Module

What it is: Central inventory of all IT assets (servers, applications, cloud resources).

Why it matters: You can't protect what you don't know about. Asset visibility is foundational to security.

When to use it:
ï¿½ Track which assets have vulnerabilities

ï¿½ Assess risk by asset criticality
ï¿½ Link security issues to specific systems
ï¿½ Prioritize protection for critical assets

Key Features:
ï¿½ Asset criticality scoring
ï¿½ Vulnerability mapping
ï¿½ Risk score calculation
ï¿½ Ownership tracking