VIOE - Vulnerability Intelligence & Orchestration Engine

Roles & Permissions Matrix

Document Version: 1.0 **Classification:** Internal / Security Sensitive **Last Updated:** January 2026

Table of Contents

1. Document Purpose

This document defines the role-based access control (RBAC) model for VIOE. It serves as the authoritative reference for:

- Understanding what each role can do
- Making role assignment decisions
- Ensuring compliance with access control requirements
- Supporting audit activities

Critical for:

- Security compliance

- User provisioning
- Access reviews
- Audit preparation

---

2. Role Definitions

2.1 Administrator

Purpose: Full system control and configuration

Intended Users:

- Security Operations Manager
- Platform Administrator
- IT Security Lead

Description: Administrators have unrestricted access to all VIOE features including system configuration, user management, and all operational capabilities. This role should be limited to essential personnel only.

Key Responsibilities:

- System configuration and maintenance
- User and team management
- Integration setup
- Security policy enforcement
- Audit log review

2.2 Security Manager

Purpose: Strategic oversight and incident response leadership

Intended Users:

- Chief Information Security Officer (CISO)
- Security Director
- Security Operations Center (SOC) Manager

Description: Security Managers have elevated access for strategic decision-making and oversight. They can view all data, manage incidents, and access analytics but cannot modify system configuration.

Key Responsibilities:

- Security posture oversight
- Incident response coordination
- Strategic planning
- Executive reporting
- Compliance oversight

2.3 Security Analyst

Purpose: Day-to-day vulnerability management and triage

Intended Users:

- Security Analyst
- Vulnerability Analyst
- Application Security Engineer

Description: Security Analysts perform the core vulnerability management activities including triage, assignment, and task creation. They have access to operational features but not administrative functions.

Key Responsibilities:

- Vulnerability triage and validation
- AI assignment review
- Task creation and tracking
- Import management
- Threat investigation

2.4 Team Lead

Purpose: Team-scoped vulnerability management

Intended Users:

- Engineering Team Lead

- Development Manager
- Platform Team Lead

Description: Team Leads have access to vulnerabilities and tasks assigned to their team. They can manage team workload and track team performance but cannot access other teams' data.

Key Responsibilities:

- Team workload management
- Assignment validation for team
- Task prioritization
- Performance tracking
- Escalation handling

2.5 Compliance Officer

Purpose: Compliance and governance focus

Intended Users:

- Compliance Manager
- GRC Analyst
- Audit Coordinator

Description: Compliance Officers have read access to vulnerability data and full access to compliance features. They can generate reports and collect evidence but cannot modify operational data.

Key Responsibilities:

- Compliance report generation
- Evidence collection
- Framework assessment
- Audit support
- Policy review

2.6 Remediation Engineer

Purpose: Fix implementation and task management

Intended Users:

- Software Developer
- DevOps Engineer
- System Administrator

Description: Remediation Engineers focus on implementing fixes. They have access to assigned tasks and can update status but have limited access to broader vulnerability data.

Key Responsibilities:

- Task execution
- Status updates
- Jira synchronization
- Fix implementation
- Policy compliance

2.7 View Only

Purpose: Read-only access for stakeholders

Intended Users:

- Executive Leadership
- External Auditors (temporary)
- Stakeholder Observers

Description: View Only users can see dashboards and reports but cannot make any changes. Suitable for stakeholders who need visibility without operational involvement.

Key Responsibilities:

- Dashboard review
- Report consumption
- Status monitoring

3. Permission Categories

3.1 Category Overview

Category	Code	Description
View	V	Read/display data
Create	C	Add new records
Update	U	Modify existing records
Delete	D	Remove records
Execute	E	Trigger actions/processes
Configure	CFG	Modify system settings
Export	EXP	Download/extract data

3.2 Permission Notation

In the permission matrix:

- ✓ = Full permission
- **T** = Team-scoped only (own team's data)
- **R** = Read/View only
- **—** = No access

4. Complete Permission Matrix

4.1 Vulnerability Management

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View all vulnerabilities	✓	✓	✓	T	R	T	R
View vulnerability detail	✓	✓	✓	T	R	T	R
Create vulnerability (manual)	✓	✓	✓	—	—	—	—
Update vulnerability status	✓	✓	✓	T	—	T	—
Mark as false positive	✓	✓	✓	T	—	—	—
Delete vulnerability	✓	—	—	—	—	—	—
Bulk actions	✓	✓	✓	T	—	—	—
Export vulnerability data	✓	✓	✓	T	✓	—	—

4.2 AI Ownership & Assignment

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View assignments	✓	✓	✓	T	R	T	R
Trigger AI triage	✓	✓	✓	—	—	—	—
Accept AI assignment	✓	✓	✓	T	—	—	—
Reassign vulnerability	✓	✓	✓	T	—	—	—
Bulk triage	✓	✓	✓	—	—	—	—
View ownership history	✓	✓	✓	T	R	T	R
Configure AI settings	✓	—	—	—	—	—	—

4.3 Remediation Tasks

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View all tasks	✓	✓	✓	T	R	T	R
Create task	✓	✓	✓	T	—	T	—
Update task status	✓	✓	✓	T	—	T	—
Delete task	✓	✓	—	—	—	—	—
Create Jira issue	✓	✓	✓	T	—	T	—
Sync Jira status	✓	✓	✓	T	—	T	—
Trigger policy check	✓	✓	✓	T	R	T	—
Generate auto-fix	✓	✓	✓	T	—	T	—
Create pull request	✓	✓	✓	T	—	T	—

4.4 Asset Management

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View all assets	✓	✓	✓	T	R	T	R
Create asset	✓	✓	✓	—	—	—	—
Update asset	✓	✓	✓	—	—	—	—
Delete asset	✓	—	—	—	—	—	—
Update risk scores	✓	✓	✓	—	—	—	—
Export asset data	✓	✓	✓	—	✓	—	—

4.5 Team Management

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View all teams	✓	✓	R	T	R	R	R
Create team	✓	✓	—	—	—	—	—
Update team	✓	✓	—	—	—	—	—
Delete team	✓	—	—	—	—	—	—
View team performance	✓	✓	—	T	R	—	R
Assign users to team	✓	✓	—	—	—	—	—

4.6 Incident Response

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View incidents	✓	✓	✓	R	R	—	R
Create incident	✓	✓	✓	—	—	—	—
Update incident status	✓	✓	✓	—	—	—	—
Close incident	✓	✓	—	—	—	—	—
View AI assessment	✓	✓	✓	R	R	—	R
Manage containment	✓	✓	✓	—	—	—	—
Update timeline	✓	✓	✓	—	—	—	—
Generate playbook	✓	✓	✓	—	—	—	—
Generate incident report	✓	✓	✓	—	R	—	R

4.7 Threat Intelligence

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View threat alerts	✓	✓	✓	—	R	—	R
Acknowledge alerts	✓	✓	✓	—	—	—	—
View hunting sessions	✓	✓	✓	—	R	—	R
Create hunting session	✓	✓	✓	—	—	—	—
Trigger threat detection	✓	✓	✓	—	—	—	—
View predictive analysis	✓	✓	✓	—	R	—	R
Generate predictions	✓	✓	✓	—	—	—	—
View threat models	✓	✓	✓	—	R	—	R
Generate threat model	✓	✓	✓	—	—	—	—

4.8 Compliance & Reporting

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View compliance reports	✓	✓	R	R	✓	—	R
Generate compliance report	✓	✓	—	—	✓	—	—
View evidence	✓	✓	R	R	✓	—	R
Generate evidence	✓	✓	—	—	✓	—	—
View policy suggestions	✓	✓	—	—	✓	—	R
Generate policy updates	✓	✓	—	—	✓	—	—
Export compliance data	✓	✓	—	—	✓	—	—

4.9 Codebase Analysis

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View analysis results	✓	✓	✓	T	R	T	R
Trigger analysis	✓	✓	✓	—	—	—	—
View architectural findings	✓	✓	✓	T	R	T	R
View dependency issues	✓	✓	✓	T	R	T	R
View logic flaws	✓	✓	✓	T	R	T	R
Export analysis	✓	✓	✓	T	✓	—	—

4.10 Dashboard & Analytics

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View main dashboard	✓	✓	✓	✓	✓	✓	✓
View advanced dashboard	✓	✓	✓	R	✓	—	R
View trend analysis	✓	✓	✓	T	✓	T	R
View KPIs	✓	✓	✓	T	✓	T	✓
Export dashboard data	✓	✓	✓	T	✓	—	—

4.11 Data Import

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
Import vulnerabilities	✓	✓	✓	—	—	—	—
Upload files	✓	✓	✓	—	—	—	—
View import history	✓	✓	✓	—	R	—	—

4.12 Settings & Configuration

Permission	Admin	Manager	Analyst	Lead	Compliance	Engineer	View
View settings	✓	R	—	—	—	—	—
Manage suppression rules	✓	—	—	—	—	—	—
Configure AI settings	✓	—	—	—	—	—	—
Manage integrations	✓	—	—	—	—	—	—
Configure notifications	✓	—	—	—	—	—	—
View audit logs	✓	R	—	—	R	—	—

5. Restricted Actions

The following actions are restricted and require elevated privileges:

5.1 Administrator-Only Actions

Action	Justification
Delete vulnerability records	Prevents accidental data loss
Delete asset records	Maintains audit integrity
Delete team records	Preserves organizational structure
Modify system configuration	Protects platform stability
Manage integrations	Controls external access
Configure AI settings	Affects all assignments
Create suppression rules	Could hide security issues
View all audit logs	Contains sensitive information

5.2 Manager-and-Above Actions

Action	Justification
Close incidents	Ensures proper review
Delete remediation tasks	Maintains task integrity
Create/modify teams	Organizational control
Generate compliance reports	Official documentation
Bulk operations (unrestricted)	Performance impact

5.3 Prohibited Actions (All Roles)

Action	Status
Modify audit logs	Prohibited
Bypass authentication	Prohibited
Access other users' credentials	Prohibited
Export all data without filtering	Prohibited
Disable security controls	Prohibited

6. Logged Actions

All actions below are automatically logged for audit purposes:

6.1 Always Logged

Action Category	Logged Fields
Authentication	User, timestamp, success/failure, IP
Vulnerability changes	User, action, before/after values, timestamp
Assignment changes	User, old team, new team, confidence, timestamp
Task operations	User, action, task ID, timestamp
Status transitions	User, old status, new status, entity, timestamp
Incident operations	User, action, incident ID, timestamp
Configuration changes	User, setting, old value, new value, timestamp
Report generation	User, report type, parameters, timestamp
Data exports	User, data type, filters, timestamp
Import operations	User, file, record count, timestamp

6.2 Log Retention

Log Type	Retention Period
Authentication logs	2 years
Configuration changes	5 years
Data modification	3 years
Access logs	1 year
Export logs	3 years

6.3 Log Access

Role	Log Access
Administrator	Full access
Security Manager	Read-only
Compliance Officer	Read-only (filtered)
Other roles	No access

7. Admin Override Rules

7.1 Override Capabilities

Administrators can override certain restrictions:

Override	Conditions
Reassign from any team	Always allowed
Access team-scoped data	Always allowed
Modify resolved vulnerabilities	With justification
Unsuppress findings	With justification
Reset user access	With authorization

7.2 Override Logging

All administrative overrides are logged with:

- Administrator identity
- Action taken
- Reason/justification
- Timestamp
- Affected records

7.3 Override Restrictions

Even administrators cannot:

- Modify completed audit logs
- Delete audit records
- Bypass multi-factor authentication
- Grant themselves additional roles

7.4 Emergency Access

In emergency situations:

1. Emergency access requires documented justification
2. All emergency actions are flagged in logs
3. Post-incident review required within 72 hours
4. Notification to security leadership required

---

8. Role Assignment Guidelines

8.1 Minimum Privilege Principle

- Assign the lowest role that enables job function
- Review assignments quarterly
- Remove unnecessary elevated access promptly

8.2 Role Assignment Matrix

Job Function	Recommended Role
Security Operations Manager	Administrator
Platform Administrator	Administrator
CISO / Security Director	Security Manager
SOC Manager	Security Manager
Security Analyst	Security Analyst
Application Security Engineer	Security Analyst
Engineering Team Lead	Team Lead
Compliance Manager	Compliance Officer
GRC Analyst	Compliance Officer
Software Developer	Remediation Engineer
DevOps Engineer	Remediation Engineer
Executive Leadership	View Only

8.3 Multi-Role Considerations

- Users can have multiple roles
- Highest privilege applies when roles conflict
- Team-scoped roles apply independently per team
- Document justification for multiple roles

8.4 Temporary Elevated Access

For temporary needs:

1. Document business justification
2. Set explicit expiration date
3. Review at expiration
4. Automatic revocation if not renewed

9. Audit & Compliance

9.1 Access Review Schedule

Review Type	Frequency	Owner
Administrator access	Monthly	Security Manager
All user access	Quarterly	Administrator
Service account access	Quarterly	Administrator
Integration credentials	Semi-annually	Administrator

9.2 Compliance Mapping

Framework	Relevant Controls
SOC 2	CC6.1, CC6.2, CC6.3
ISO 27001	A.9.1, A.9.2, A.9.4
GDPR	Article 32
PCI DSS	Requirement 7, 8

9.3 Audit Evidence

This document, combined with system logs, provides evidence for:

- Access control implementation
- Principle of least privilege
- Segregation of duties
- Audit trail maintenance

9.4 Exception Management

Access control exceptions must:

1. Be documented with business justification
2. Be approved by Security Manager or above
3. Have defined expiration date

4. Be reviewed at each audit cycle

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document contains security-sensitive information and should be handled accordingly.

VIOE - Vulnerability Intelligence & Orchestration Engine *Roles & Permissions Matrix*