VIOE - Vulnerability Intelligence & Orchestration Engine

Security & Compliance Overview

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

Table of Contents

1. Executive Summary

1.1 Purpose

This document provides a comprehensive overview of VIOE's security architecture and compliance posture. It is intended for security evaluators, auditors, compliance officers, and enterprise clients assessing the platform's security controls.

1.2 Security Commitment

VIOE is designed with security as a foundational principle. The platform:

- Protects sensitive vulnerability and security data
- Implements defense-in-depth security controls
- Supports enterprise compliance requirements
- Maintains comprehensive audit capabilities
- Follows industry security best practices

1.3 Compliance Summary

Framework	Alignment Status	Key Controls
SOC 2 Type II	Aligned	Access control, encryption, audit
ISO 27001	Aligned	ISMS, risk management
GDPR	Aligned	Data protection, privacy
PCI DSS	Aligned	Access, encryption, logging
HIPAA	Aligned (as applicable)	PHI protection

---

2. Security Architecture

2.1 Defense in Depth

VIOE implements multiple security layers:

```
[Diagram Placeholder: Defense in Depth Architecture]

Layer 1: Network Security
├── TLS/HTTPS encryption
├── Web Application Firewall
├── DDoS protection
└── Network segmentation

Layer 2: Application Security
├── Authentication
├── Authorization (RBAC)
```

```
├── Input validation
└── Session management

Layer 3: Data Security
├── Encryption at rest
├── Encryption in transit
├── Access controls
└── Data classification

Layer 4: Monitoring & Response
├── Audit logging
├── Anomaly detection
├── Incident response
└── Security monitoring
```

2.2 Security Boundaries

Boundary	Protection
External to Application	TLS 1.3, WAF, rate limiting
Application to Database	Encrypted connections, parameterized queries
Application to Integrations	OAuth, API keys, encrypted transport
User to Application	MFA, session management, RBAC

2.3 Secure Development

VIOE follows secure development practices:

Practice	Implementation
Secure coding standards	OWASP guidelines
Code review	Required for all changes
Dependency scanning	Automated vulnerability checks
Security testing	SAST, DAST in CI/CD
Penetration testing	Annual third-party assessment

---

3. Authentication Model

3.1 Authentication Methods

Primary Authentication:

- Username (email) and password
- Password complexity requirements enforced
- Account lockout after failed attempts

Multi-Factor Authentication (MFA):

- TOTP-based authentication supported
- Recommended for all users
- Required for administrator accounts

Single Sign-On (SSO):

- SAML 2.0 support
- OAuth 2.0 / OpenID Connect
- Integration with enterprise identity providers

3.2 Authentication Controls

Control	Description
Password Policy	Minimum length, complexity, history
Account Lockout	5 failed attempts = 30-minute lockout
Session Timeout	30 minutes of inactivity
Secure Transmission	Credentials only over HTTPS
Password Storage	Bcrypt hashing with salt

3.3 Session Management

Feature	Implementation
Session Tokens	Cryptographically random
Token Storage	Secure HTTP-only cookies
Token Expiry	Configurable timeout
Concurrent Sessions	Limited per user
Session Termination	Logout invalidates token

3.4 Identity Provider Integration

Provider	Support Level
Okta	Full integration
Azure AD	Full integration
Google Workspace	Full integration
Custom SAML	Supported

---

4. Access Control Principles

4.1 Role-Based Access Control (RBAC)

VIOE implements comprehensive RBAC:

Principles Applied:

- Least privilege: Users receive minimum necessary access
- Separation of duties: Critical functions require multiple roles
- Need-to-know: Data access limited by role and scope

Available Roles:

Role	Access Level	Primary Purpose
Administrator	Full	System configuration
Security Manager	Elevated	Strategic oversight
Security Analyst	Standard	Vulnerability management
Team Lead	Team-scoped	Team management
Compliance Officer	Compliance focus	Reporting and evidence
Remediation Engineer	Task focus	Fix implementation
View Only	Read-only	Observation

4.2 Data Access Controls

Control Type	Implementation
Role-based filtering	Data visibility by role
Team-based scoping	Access limited to assigned team
Environment filtering	Production/staging/development
Feature-based access	Functions enabled by role

4.3 Administrative Controls

Control	Description
Admin account limitation	Minimum necessary administrators
Admin action logging	All admin actions recorded
Privileged access review	Monthly admin access review
Admin MFA requirement	MFA mandatory for admins

4.4 Access Review Process

Review Type	Frequency	Owner
User access review	Quarterly	Security Manager
Admin access review	Monthly	CISO
Role assignment review	Quarterly	Administrator
Integration access review	Semi-annually	Administrator

---

5. Data Protection & Encryption

5.1 Data Classification

Classification	Description	Examples
Confidential	Highly sensitive	Credentials, tokens
Internal	Business sensitive	Vulnerability data
Restricted	Limited distribution	Compliance reports
Public	No restrictions	Product documentation

5.2 Encryption Standards

Encryption in Transit:

Protocol	Standard	Usage
HTTPS	TLS 1.3	All web traffic
API Communications	TLS 1.3	All API calls
Database Connections	TLS	Backend connections
Integration Traffic	TLS 1.2+	External services

Encryption at Rest:

Data Type	Encryption	Key Management
Database	AES-256	Cloud provider KMS
File Storage	AES-256	Cloud provider KMS
Backups	AES-256	Separate key hierarchy
Logs	AES-256	Log service encryption

5.3 Key Management

Aspect	Implementation
Key Generation	Cryptographically secure random
Key Storage	Hardware Security Module (HSM)
Key Rotation	Annual rotation schedule
Key Access	Role-based, audited

5.4 Data Handling

Process	Security Control
Data Input	Validation, sanitization
Data Processing	Least privilege access
Data Storage	Encryption, access control
Data Transmission	TLS encryption
Data Deletion	Secure deletion procedures

5.5 Sensitive Data Protection

Data Type	Protection Measures
API Keys	Encrypted storage, masked display
User Credentials	Hashed, never stored in plain text
Integration Tokens	Encrypted, short-lived
Vulnerability Data	Access-controlled, encrypted

---

6. Audit & Logging

6.1 Logging Scope

Events Logged:

Category	Events
Authentication	Login success/failure, logout, MFA events
Authorization	Access denied, permission changes
Data Access	Create, read, update, delete operations
Configuration	Settings changes, integration updates
Administrative	User management, role changes
Security	Suspicious activity, policy violations

6.2 Log Content

Each log entry contains:

Field	Description
Timestamp	UTC time with millisecond precision
User ID	Authenticated user identifier
Action	Operation performed
Resource	Target of the operation
Result	Success or failure
Source IP	Client IP address
User Agent	Browser/client information
Details	Additional context

6.3 Log Protection

Control	Implementation
Integrity	Write-once, append-only
Confidentiality	Encrypted storage
Availability	Redundant storage
Retention	Minimum 2 years
Access	Administrator only

6.4 Log Retention

Log Type	Retention Period
Security logs	3 years
Audit logs	3 years
Access logs	2 years
Application logs	1 year
Debug logs	30 days

6.5 Monitoring & Alerting

Monitoring Type	Implementation
Real-time monitoring	Security event correlation
Anomaly detection	Baseline deviation alerts
Threshold alerting	Configurable thresholds
Dashboard	Security operations visibility

---

7. Compliance Framework Alignment

7.1 SOC 2 Type II

Trust Service Criteria Coverage:

Category	Coverage
Security (CC)	Full
Availability (A)	Full
Processing Integrity (PI)	Full
Confidentiality (C)	Full
Privacy (P)	Applicable controls

Key Controls:

Control ID	Description	VIOE Implementation
CC6.1	Logical access security	RBAC, authentication
CC6.2	Access provisioning	Role assignment process
CC6.3	Access removal	Offboarding procedures
CC6.6	Access review	Quarterly reviews
CC7.1	Vulnerability management	Core functionality
CC7.2	Change management	Controlled releases

7.2 ISO 27001

Annex A Control Coverage:

Domain	Coverage
A.5 Information Security Policies	Documented
A.6 Organization of Information Security	Implemented
A.7 Human Resource Security	Applicable
A.8 Asset Management	Implemented
A.9 Access Control	Full
A.10 Cryptography	Full
A.12 Operations Security	Full
A.13 Communications Security	Full
A.14 System Development	Full
A.16 Incident Management	Full
A.18 Compliance	Applicable

7.3 GDPR

Applicable Requirements:

Article	Requirement	Implementation
25	Privacy by Design	Built-in controls
32	Security of Processing	Encryption, access control
33	Breach Notification	Incident response procedures
35	Data Protection Impact	Assessment process

Data Protection Measures:

- Encryption of personal data
- Access controls limiting exposure
- Audit logging of data access
- Data retention policies
- Right to deletion support

7.4 PCI DSS

Applicable Requirements:

Requirement	Description	Implementation
3	Protect stored data	Encryption at rest
4	Encrypt transmission	TLS everywhere
7	Restrict access	RBAC implementation
8	Identify users	Authentication system
10	Track access	Comprehensive logging
12	Security policies	Documented procedures

---

8. Security Controls Matrix

8.1 Preventive Controls

Control	Purpose	Implementation
Authentication	Verify identity	Username/password, MFA
Authorization	Limit access	RBAC, team scoping
Input validation	Prevent injection	Parameterized queries, sanitization
Encryption	Protect data	TLS, AES-256
Rate limiting	Prevent abuse	API throttling

8.2 Detective Controls

Control	Purpose	Implementation
Audit logging	Record activity	Comprehensive logging
Monitoring	Detect anomalies	Real-time alerting
Access review	Identify issues	Regular reviews
Vulnerability scanning	Find weaknesses	Automated scanning

8.3 Corrective Controls

Control	Purpose	Implementation
Incident response	Address breaches	Documented procedures
Backup/restore	Recover data	Regular backups
Patch management	Fix vulnerabilities	Regular updates
Account lockout	Stop attacks	Automated lockout

8.4 Control Effectiveness

Control Area	Maturity Level
Access Management	Advanced
Data Protection	Advanced
Audit & Monitoring	Advanced
Incident Response	Mature
Configuration Management	Mature

9. Incident Response Capability

9.1 Incident Response Process

Phase	Activities
Preparation	Plans, training, tools
Detection	Monitoring, alerting, reporting
Analysis	Triage, scope assessment
Containment	Limit damage, preserve evidence
Eradication	Remove threat
Recovery	Restore operations
Post-Incident	Review, improve

9.2 Incident Classification

Severity	Criteria	Response Time
Critical	Data breach, service compromise	Immediate
High	Security control failure	1 hour
Medium	Policy violation	4 hours
Low	Minor security event	24 hours

9.3 Communication Procedures

Stakeholder	Communication Method	Timing
Internal security	Direct notification	Immediate
Management	Escalation process	Based on severity
Customers	Notification process	As required
Regulators	Compliance notification	Within requirements

---

10. Third-Party Security

10.1 Integration Security

Integration	Security Measures
Vulnerability Scanners	API keys, encrypted transport
Jira	OAuth, encrypted connection
Slack	OAuth, scoped permissions
Directory Services	Secure LDAP, SSO

10.2 Vendor Assessment

Criteria	Evaluation
Security certifications	SOC 2, ISO 27001
Data handling	Privacy policies
Incident response	Notification procedures
Access controls	Least privilege

10.3 Data Sharing Controls

Control	Implementation
Data minimization	Share only necessary data
Purpose limitation	Define permitted uses
Access restriction	Scoped API access
Audit	Log all data sharing

---

11. Security Governance

11.1 Security Policies

Policy	Scope
Information Security Policy	Overall security framework
Access Control Policy	User access management
Data Protection Policy	Data handling requirements
Incident Response Policy	Security event handling
Acceptable Use Policy	User responsibilities

11.2 Security Responsibilities

Role	Responsibility
CISO	Overall security strategy
Security Manager	Operational security
Administrator	Platform security configuration
Users	Follow security policies

11.3 Security Assessment Schedule

Assessment	Frequency	Owner
Vulnerability assessment	Continuous	Security team
Penetration testing	Annual	Third party
Security audit	Annual	Internal audit
Compliance assessment	Annual	Compliance team
Access review	Quarterly	Security manager

11.4 Continuous Improvement

Activity	Purpose
Security metrics	Measure effectiveness
Incident analysis	Learn from events
Industry monitoring	Track emerging threats
Control updates	Improve protections

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document contains security-sensitive information for authorized review only.