

VIOE - Vulnerability Intelligence & Orchestration Engine

Operational Playbook

Document Version: 1.0 **Classification:** Internal - Operations **Last Updated:** January 2026

Table of Contents

1. [Playbook Overview](#)
 2. [Daily Operations](#)
 3. [Weekly Operations](#)
 4. [Monthly Operations](#)
 5. [User Onboarding Process](#)
 6. [Data Quality Checks](#)
 7. [Operational Workflows](#)
 8. [Incident Handling Overview](#)
 9. [Escalation Procedures](#)
 10. [Maintenance Windows](#)
 11. [Operational Checklists](#)
-

1. Playbook Overview

1.1 Purpose

This Operational Playbook provides step-by-step procedures for day-to-day operations of VIOE. Following these procedures ensures consistent, reliable, and efficient vulnerability management operations.

1.2 Intended Users

- Security Operations Center (SOC) Staff
- Security Analysts
- Operations Managers
- Team Leads
- Administrators

1.3 How to Use This Playbook

- Follow procedures in order unless otherwise noted
- Document any deviations and reasons
- Update playbook when processes change
- Report issues to playbook owner

2. Daily Operations

2.1 Morning Standup Checklist

Time: Start of business day (recommended 9:00 AM) **Duration:** 15-30 minutes **Owner:** Security Operations Lead

Procedure:

Step	Action	Expected Outcome
1	Log into VIOE Dashboard	Access confirmed
2	Review overnight alerts	Understand new issues
3	Check Critical vulnerabilities	Identify immediate priorities
4	Review SLA approaching items	Plan urgent remediation
5	Check import status	Verify data freshness
6	Assign daily priorities	Team aligned

2.2 Critical Vulnerability Triage

Trigger: Any new Critical severity vulnerability **Response Time:** Within 2 hours of detection **Owner:** Senior Security Analyst

Procedure:

Step	Action	Notes
1	Open vulnerability detail	Review full information
2	Validate severity is correct	Check CVSS, exploit availability
3	Confirm AI team assignment	Accept or reassign
4	Create remediation task	Set priority as Critical
5	Notify team lead	Via Slack or direct message
6	Document in daily log	Record action taken
7	Set follow-up reminder	Track to resolution

2.3 Daily Import Verification

Time: After each scheduled import **Owner:** Security Analyst

Procedure:

Step	Action	Expected Outcome
1	Navigate to Import History	View recent imports
2	Verify import completed	Status = Complete
3	Check record count	Within expected range
4	Review error count	Should be minimal
5	Spot-check new items	Quality verification
6	Log import statistics	Maintain records

2.4 End-of-Day Review

Time: End of business day **Duration:** 15 minutes **Owner:** Security Operations Lead

Procedure:

Step	Action	Purpose
1	Review day's resolution	Track progress
2	Check Critical status	Ensure no new Critical unaddressed
3	Update daily log	Document activities
4	Set overnight alerts	Enable notifications
5	Hand off to next shift	If applicable

3. Weekly Operations

3.1 Weekly Metrics Review

Day: Monday morning **Duration:** 1 hour **Owner:** Security Operations Manager

Procedure:

Step	Action	Deliverable
1	Generate weekly dashboard	Export metrics
2	Calculate week-over-week change	Trend analysis
3	Identify top 10 risks	Prioritization list
4	Review team performance	Performance data
5	Document insights	Weekly summary
6	Distribute to stakeholders	Email/presentation

3.2 Team Performance Check

Day: Tuesday **Duration:** 30 minutes per team **Owner:** Team Lead

Procedure:

Step	Action	Purpose
1	Navigate to Teams page	Access performance data
2	Review team's open items	Understand workload
3	Check resolution rate	Compare to target
4	Identify blockers	Remove impediments
5	Adjust assignments if needed	Balance workload
6	Document in team log	Track trends

3.3 Suppression Rule Review

Day: Wednesday **Duration:** 30 minutes **Owner:** Security Analyst + Admin

Procedure:

Step	Action	Purpose
1	Navigate to Settings → Suppression	Access rules
2	Review active rules	Verify appropriateness
3	Check suppression counts	Volume assessment
4	Sample 5-10 suppressed items	Quality check
5	Adjust rules if needed	Maintain accuracy
6	Document any changes	Audit trail

3.4 Integration Health Check

Day: Thursday **Duration:** 30 minutes **Owner:** Administrator

Procedure:

Step	Action	Expected Outcome
1	Check scanner sync status	All syncs successful
2	Verify Jira connectivity	Test sync operation
3	Confirm Slack delivery	Test notification
4	Review integration logs	No errors
5	Document any issues	Track for resolution

3.5 Weekly Report Generation

Day: Friday **Duration:** 1 hour **Owner:** Security Operations Manager

Procedure:

Step	Action	Deliverable
1	Generate executive summary	PDF report
2	Generate team reports	Per-team metrics
3	Generate SLA report	Compliance status
4	Compile weekly narrative	Context and insights
5	Distribute to leadership	Email delivery

4. Monthly Operations

4.1 Monthly Security Review

Timing: First week of month **Duration:** Half day **Participants:** Security Manager, Team Leads, Admin

Agenda:

Time	Topic	Owner
0:00-0:30	Review previous month metrics	Manager
0:30-1:00	Discuss trends and anomalies	All
1:00-1:30	Team performance review	Team Leads
1:30-2:00	Process improvement discussion	All
2:00-2:30	Action item assignment	Manager
2:30-3:00	Next month planning	All

4.2 Compliance Assessment

Timing: Second week of month **Duration:** 2-4 hours **Owner:** Compliance Officer

Procedure:

Step	Action	Deliverable
1	Generate compliance reports	All frameworks
2	Review gap changes	Month-over-month
3	Update evidence packages	Current evidence
4	Identify new risks	Risk register update
5	Create remediation plan	Gap closure plan
6	Report to leadership	Summary presentation

4.3 User Access Review

Timing: Third week of month **Duration:** 2 hours **Owner:** Administrator

Procedure:

Step	Action	Purpose
1	Export user list	Current state
2	Review role assignments	Verify appropriateness
3	Identify inactive users	Cleanup candidates
4	Verify admin accounts	Limit admin access
5	Document findings	Audit evidence
6	Implement changes	Remove/modify as needed

4.4 Configuration Audit

Timing: Fourth week of month **Duration:** 2 hours **Owner:** Administrator + Security Manager

Procedure:

Step	Action	Verification
1	Review suppression rules	Still appropriate
2	Check AI settings	Optimal configuration
3	Verify integrations	All functioning
4	Review notifications	Correct recipients
5	Document configuration	Backup settings
6	Plan any changes	Change requests

5. User Onboarding Process

5.1 New User Onboarding Workflow

Duration: 1-2 business days **Owner:** Administrator + Team Lead

Phase 1: Account Setup (Day 1)

Step	Action	Owner	Time
1	Receive access request	HR/Manager	-
2	Verify authorization	Administrator	15 min
3	Create user in identity provider	IT Admin	30 min
4	Assign to team(s)	Administrator	15 min
5	Set role permissions	Administrator	15 min
6	Send welcome email	Administrator	10 min

Phase 2: Orientation (Day 1-2)

Step	Action	Owner	Time
7	Schedule orientation meeting	Team Lead	15 min
8	Provide documentation access	Team Lead	10 min
9	Conduct orientation session	Team Lead	1 hour
10	First login verification	User	15 min
11	Practice vulnerability review	User	30 min
12	Confirm access working	Administrator	15 min

5.2 New User Welcome Email Template

Subject: Welcome to VIOE - Your Access is Ready

Dear [User Name],

Welcome to VIOE (Vulnerability Intelligence & Orchestration Engine). Your account has been created and you are ready to begin.

ACCESS INFORMATION:

URL: [Your VIOE URL]

Username: [Your organizational email]

Role: [Assigned Role]

Team(s): [Assigned Team(s)]

GETTING STARTED:

1. Log in using the URL above with your organizational credentials
2. Complete any first-time setup (password change, MFA if required)
3. Navigate to the Dashboard to see current status
4. Review the Product Owner Guide (attached)

NEXT STEPS:

Your Team Lead [Name] will schedule an orientation session with you.

SUPPORT:

Technical Issues: [Support Contact]

Process Questions: [Team Lead]

Access Issues: [Administrator Contact]

Best regards,
[Administrator Name]
VIOE Administrator

5.3 User Offboarding Workflow

Trigger: User departure or role change **Duration:** Same day **Owner:** Administrator

Step	Action	Verification
1	Receive offboarding request	Written request
2	Disable user account	Account inactive
3	Reassign open items	No orphan work items
4	Remove from teams	Team updated
5	Audit recent activity	Security check
6	Document completion	Offboarding log

6. Data Quality Checks

6.1 Daily Data Quality Checks

Check	Procedure	Expected Result
Import completeness	Compare import count to scanner	Within 5%
Severity accuracy	Sample 10 items	All correctly classified
Assignment rate	Check dashboard KPI	>80% assigned
Duplicate check	Search for duplicate CVEs	Minimal duplicates

6.2 Weekly Data Quality Checks

Check	Procedure	Expected Result
Stale data review	Find items >90 days unchanged	Explain or update
False positive rate	Calculate FP %	<15%
Suppression accuracy	Sample suppressed items	No real issues hidden
Asset accuracy	Verify asset names/types	Correctly categorized

6.3 Monthly Data Quality Checks

Check	Procedure	Expected Result
Data completeness	Check for empty fields	<5% incomplete
Historical consistency	Compare to last month	Explainable changes
Scanner coverage	Verify all systems scanned	100% coverage
Team mapping accuracy	Verify team assignments	Correct ownership

6.4 Data Quality Issue Resolution

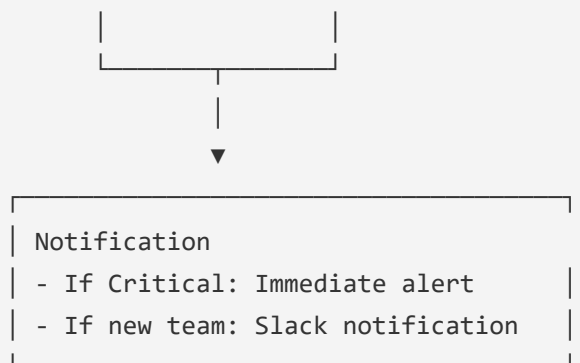
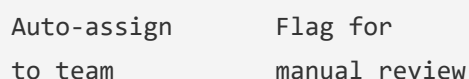
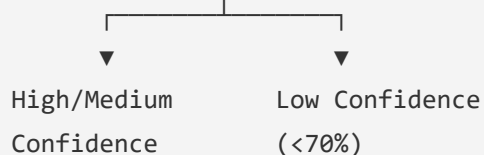
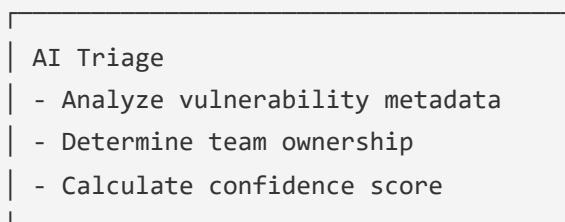
If data quality issue found:

Severity	Response Time	Escalation
Critical (security impact)	Immediate	Manager + Admin
High (operational impact)	Same day	Team Lead
Medium (reporting impact)	Within week	Analyst
Low (cosmetic)	Next sprint	Backlog

7. Operational Workflows

7.1 New Vulnerability Processing Workflow

START: New vulnerability imported



▼
COMPLETE

7.2 Remediation Task Workflow

START: Task created from vulnerability



Status: TODO

- Task assigned to team
- Notification sent



Status: IN PROGRESS

- Engineer begins work
- Optional: Create Jira issue



Normal
progress

Blocked
(impediment)

Document blocker
Escalate if needed



Status: IN REVIEW

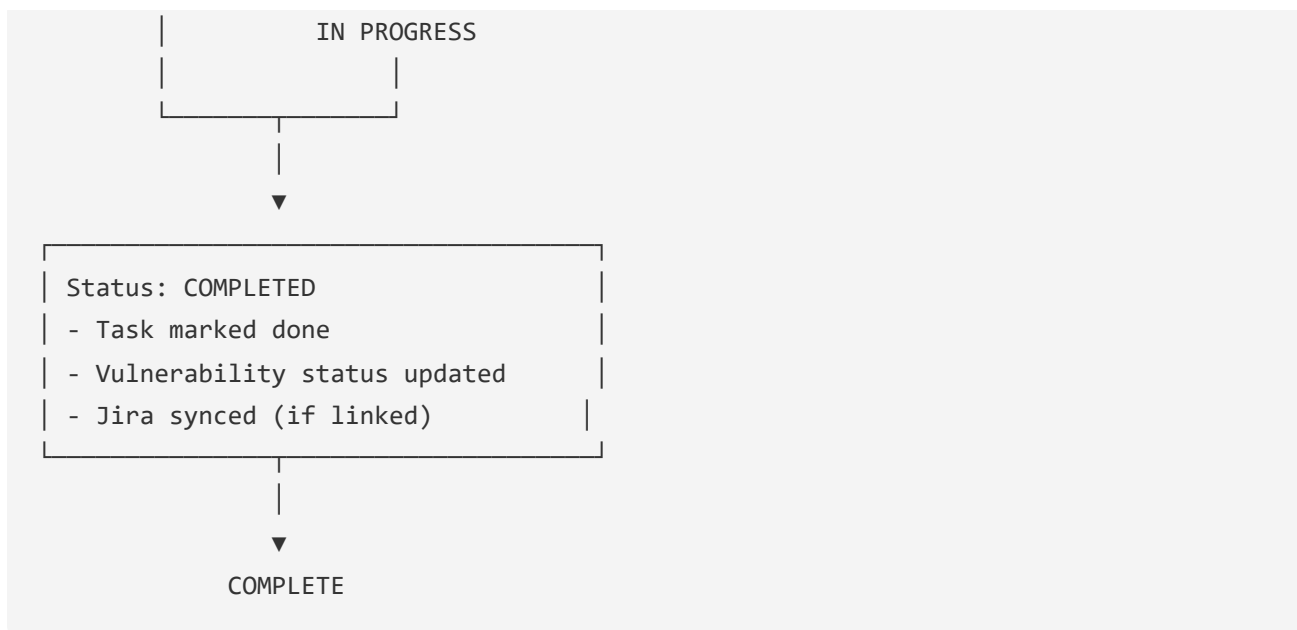
- Fix submitted
- Policy check triggered
- Verification pending



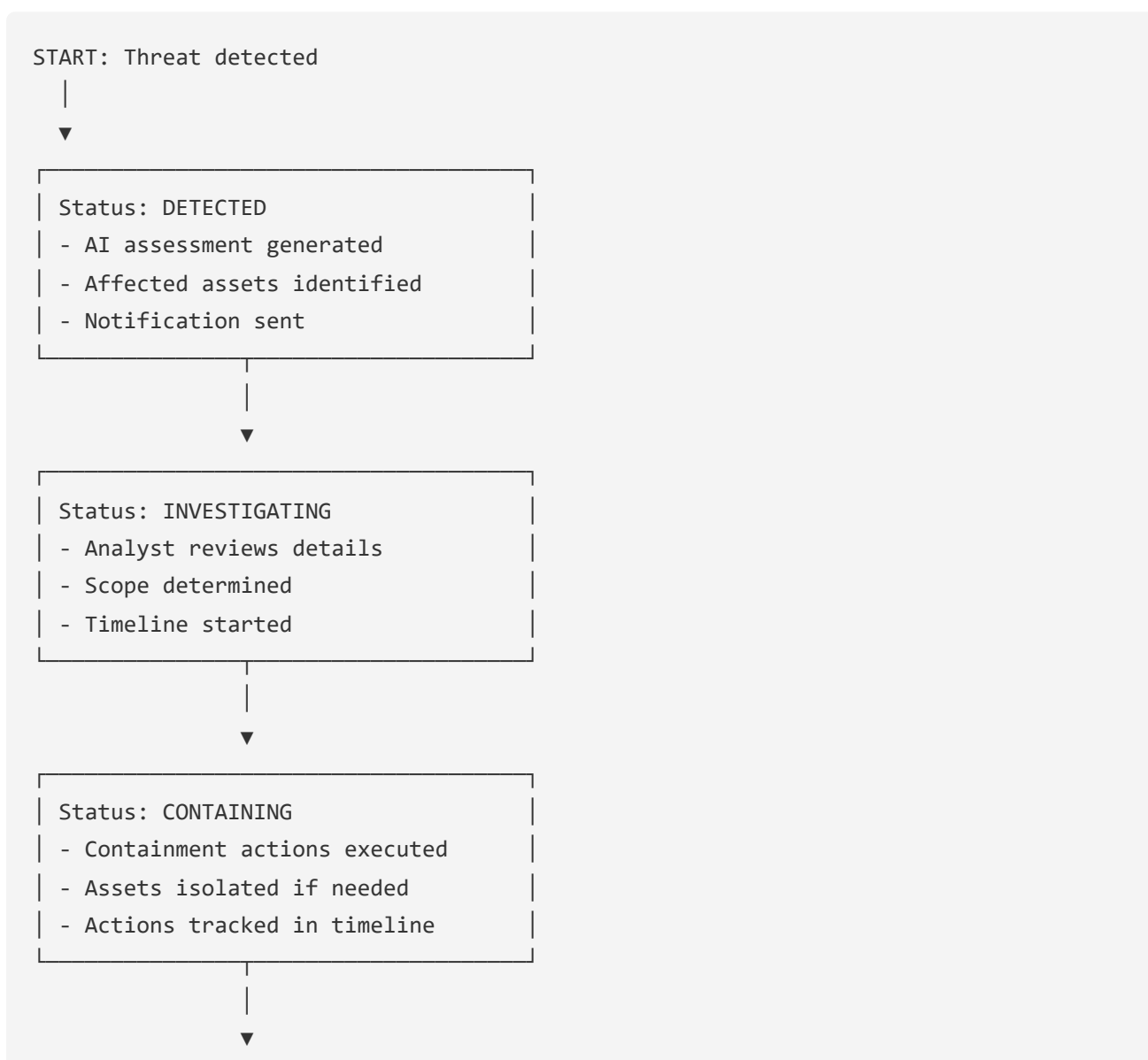
Policy PASS

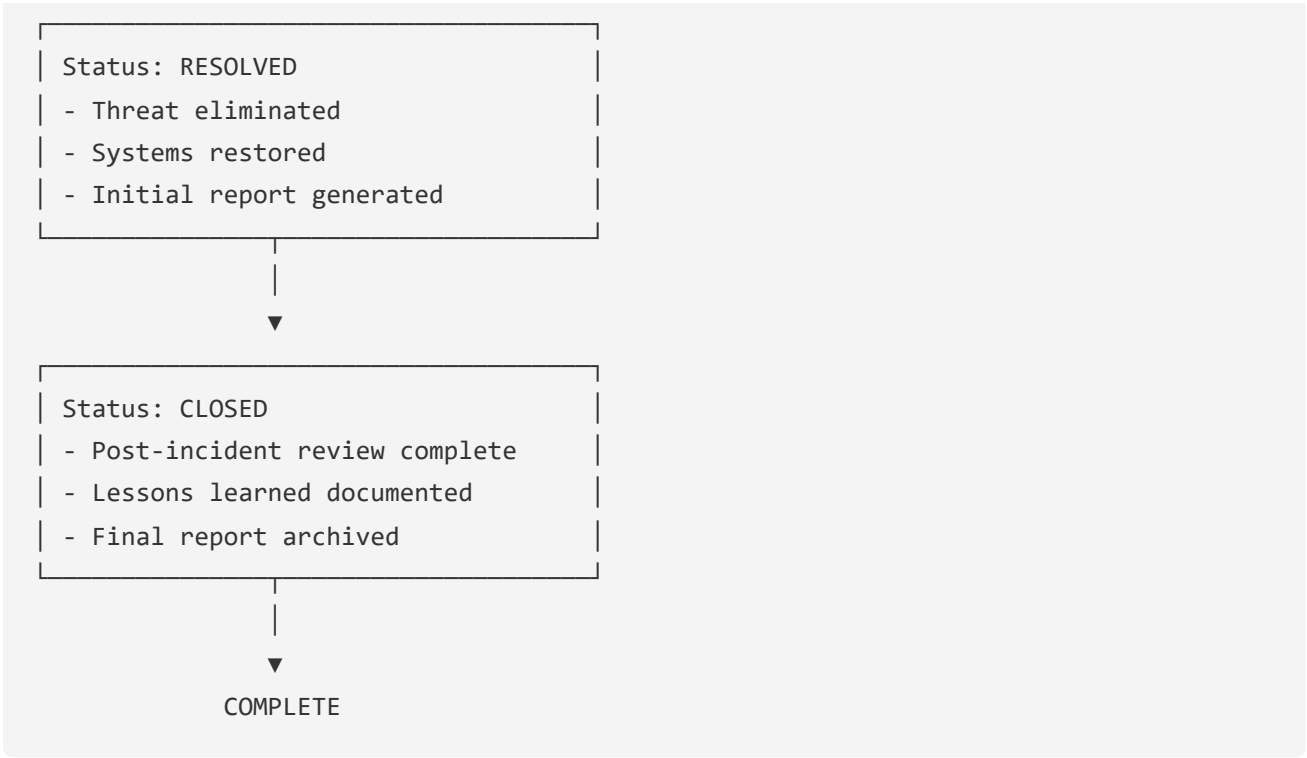
Policy FAIL

Return to



7.3 Incident Response Workflow





8. Incident Handling Overview

8.1 Incident Classification

Severity	Criteria	Response Time
Critical	Active breach, data loss imminent	Immediate
High	Significant threat, potential impact	Within 1 hour
Medium	Contained threat, monitoring needed	Within 4 hours
Low	Minor issue, no immediate risk	Within 24 hours

8.2 Initial Response Checklist

For all incidents:

Step	Action	Owner
1	Acknowledge incident in VIOE	First responder
2	Assess severity level	First responder
3	Notify appropriate parties	First responder
4	Begin documentation	First responder
5	Start investigation	Assigned analyst

8.3 Communication Matrix

Severity	Notify Immediately	Update Frequency
Critical	CISO, Security Manager, IT Leadership	Every 30 minutes
High	Security Manager, Team Lead	Every 2 hours
Medium	Team Lead	Daily
Low	Document only	On resolution

8.4 Post-Incident Activities

Activity	Timing	Owner
Initial report	Within 24 hours	Incident lead
Root cause analysis	Within 1 week	Senior analyst
Lessons learned	Within 2 weeks	Team
Process improvements	Within 1 month	Manager

9. Escalation Procedures

9.1 Escalation Triggers

Trigger	Escalation Level
Critical vulnerability unassigned >2 hours	Team Lead → Manager
SLA breach imminent	Analyst → Team Lead
Blocked task >24 hours	Analyst → Team Lead
System outage	Admin → Manager → Leadership
Security incident	Analyst → Manager → CISO

9.2 Escalation Path

```

Level 1: Security Analyst
  |
  ▼ (If unresolved after 4 hours)
Level 2: Team Lead
  |
  ▼ (If unresolved after 8 hours)
Level 3: Security Manager
  |
  ▼ (If business impact)
Level 4: CISO / Security Director
  |
  ▼ (If executive decision needed)
Level 5: Executive Leadership

```

9.3 Escalation Communication Template

ESCALATION NOTICE

Priority: [Critical/High/Medium]
 Issue: [Brief description]
 Current Status: [What's happening now]
 Time in Current State: [Duration]
 Impact: [Business impact]
 Actions Taken: [What's been tried]
 Requested Action: [What you need]
 Contact: [Your name and phone]

Timeline:

[Timestamp] - [Event]
[Timestamp] - [Event]

10. Maintenance Windows

10.1 Scheduled Maintenance

Type	Frequency	Duration	Notification
System updates	Monthly	2-4 hours	1 week advance
Database maintenance	Weekly	30 min	24 hours advance
Integration updates	As needed	1 hour	48 hours advance

10.2 Maintenance Procedure

Pre-Maintenance:

Step	Action	Owner
1	Send maintenance notification	Admin
2	Verify backup completed	Admin
3	Document current state	Admin
4	Pause scheduled imports	Admin

During Maintenance:

Step	Action	Owner
1	Execute maintenance tasks	Admin
2	Verify each step	Admin
3	Document any issues	Admin
4	Test functionality	Admin

Post-Maintenance:

Step	Action	Owner
1	Verify system operational	Admin
2	Resume imports	Admin
3	Monitor for issues	Admin
4	Send completion notice	Admin

11. Operational Checklists

11.1 Daily Opening Checklist

- ☐ Log into VIOE
- ☐ Check overnight alerts
- ☐ Review Critical vulnerabilities (action within 2 hours)
- ☐ Check SLA approaching items
- ☐ Verify import completed
- ☐ Review assignments needing attention
- ☐ Check integration status
- ☐ Update daily log

11.2 Daily Closing Checklist

- ☐ Review day's resolutions
- ☐ Verify no Critical items unaddressed
- ☐ Update task statuses
- ☐ Document any blockers
- ☐ Set overnight alerts
- ☐ Update daily log
- ☐ Hand off to next shift (if applicable)

11.3 Weekly Checklist

- ☐ Generate weekly metrics
- ☐ Review team performance
- ☐ Check suppression rules
- ☐ Verify integration health

- ☐ Generate weekly report
- ☐ Distribute to stakeholders
- ☐ Plan next week priorities

11.4 Monthly Checklist

- ☐ Conduct monthly security review
- ☐ Generate compliance reports
- ☐ Perform user access review
- ☐ Audit configuration
- ☐ Review and update processes
- ☐ Plan next month activities
- ☐ Archive monthly reports

11.5 Incident Response Checklist

- ☐ Acknowledge incident
- ☐ Assess severity
- ☐ Notify appropriate parties
- ☐ Begin investigation
- ☐ Document timeline
- ☐ Execute containment
- ☐ Track to resolution
- ☐ Complete post-incident review

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This playbook should be reviewed and updated quarterly or when significant process changes occur.

VIOE - Vulnerability Intelligence & Orchestration Engine Operational Playbook