VIOE - Vulnerability Intelligence & Orchestration Engine

Data & Reporting Guide

Document Version: 1.0 **Classification:** Internal / Business User **Last Updated:** January 2026

Table of Contents

1. Introduction

1.1 Purpose

This guide helps stakeholders understand the data VIOE collects, how metrics are calculated, and how to accurately interpret reports. Understanding these details ensures informed decision-making and prevents misinterpretation of security posture.

1.2 Who Should Read This

- Security Managers needing accurate metrics for leadership
- Compliance Officers preparing audit evidence
- Product Owners tracking operational efficiency
- Executives reviewing security dashboards
- Analysts validating data accuracy

1.3 Data Integrity Commitment

All data in VIOE is:

- **Timestamped:** Every record includes creation and modification times
- **Attributed:** Changes linked to users or systems
- **Auditable:** Full history available for review
- **Consistent:** Calculations use standardized logic

---

2. Data Collected by VIOE

2.1 Vulnerability Data

Data Field	Source	Description
Title	Scanner/Import	Vulnerability name or description
CVE ID	Scanner/Import	Standard vulnerability identifier
CVSS Score	Scanner/Import	Severity score (0-10 scale)
Severity	Derived	Critical/High/Medium/Low/Info
Status	System	Open/In Progress/Resolved/False Positive
Environment	Import/Manual	Production/Staging/Development
Asset	Import/Manual	Affected system or component
Description	Scanner/Import	Full technical description
Remediation	Scanner/Import	Recommended fix approach
Created Date	System	When first imported
Modified Date	System	Last update timestamp

2.2 Assignment Data

Data Field	Source	Description
Assigned Team	AI/Manual	Responsible team
Confidence Score	AI	Assignment certainty (0-100%)
Triage Status	System	Pending/Triaged
Assignment History	System	Audit trail of changes

2.3 Remediation Data

Data Field	Source	Description
Task Title	User	Task name
Task Status	User/System	Todo/In Progress/In Review/Completed/Blocked
Priority	User	Task urgency level
Jira Issue Key	Integration	Linked Jira ticket
Policy Status	System	Compliance check result
Created Date	System	Task creation time
Completed Date	System	Task completion time

2.4 Operational Data

Data Field	Source	Description
Import Records	System	File uploads, record counts
Suppression Stats	System	Filtered findings count
Integration Logs	System	Sync operations, errors
User Actions	System	Audit trail entries

---

3. Key Performance Indicators (KPIs)

3.1 Primary KPIs

These are the most critical metrics for assessing security operations:

KPI	Definition	Target	Frequency
Open Vulnerabilities	Total unresolved findings	Decreasing trend	Daily
Critical Findings	Unresolved Critical severity	Near zero	Daily
Mean Time to Remediate (MTTR)	Average days to resolve	Decreasing	Weekly
SLA Compliance Rate	% resolved within SLA	>90%	Weekly
AI Assignment Rate	% auto-assigned by AI	>80%	Weekly

3.2 Secondary KPIs

KPI	Definition	Purpose
Noise Reduction Rate	% findings suppressed	Measure efficiency gains
Team Resolution Rate	% resolved per team	Identify performance variance
Asset Risk Score	Weighted risk by asset	Prioritize asset attention
Compliance Score	Framework alignment %	Track compliance posture
False Positive Rate	% marked as false positive	Measure scanner accuracy

3.3 KPI Calculation Formulas

Open Vulnerabilities:

```
Count(status IN ['open', 'in_progress'])
```

Critical Findings:

```
Count(severity = 'critical' AND status NOT IN ['resolved', 'false_positive'])
```

Mean Time to Remediate:

```
Average(resolved_date - created_date) for resolved items in period
```

SLA Compliance Rate:

```
(Count(resolved within SLA) / Count(resolved total)) × 100
```

AI Assignment Rate:

```
(Count(assigned_team IS NOT NULL) / Count(total)) × 100
```

---

4. Dashboard Metrics

4.1 Main Dashboard KPI Cards

Card 1: Open Vulnerabilities

- **What it shows:** Total count of open and in-progress items
- **Color coding:** Red if increasing, Green if decreasing
- **Trend indicator:** Arrow showing week-over-week change
- **Drill-down:** Click to view vulnerability list

Card 2: Critical & High

- **What it shows:** Combined count of Critical and High severity unresolved
- **Breakdown:** Shows Critical count / High count
- **Target:** Minimize Critical to zero
- **Alert threshold:** Any Critical triggers alert

Card 3: AI Auto-Assigned %

- **What it shows:** Percentage of vulnerabilities with AI team assignment
- **Calculation:** (Assigned count / Total count) × 100
- **Target:** Above 80% indicates effective AI configuration
- **Note:** Includes high, medium, and low confidence

Card 4: Noise Reduced

- **What it shows:** Count of findings suppressed by rules
- **Value:** Represents analyst time saved
- **Calculation:** Count(is_suppressed = true)
- **Review:** Periodic check that suppression isn't hiding issues

4.2 Trend Charts

Vulnerability Trend (Time Series)

- **X-axis:** Time periods (daily/weekly/monthly)
- **Y-axis:** Vulnerability count
- **Lines:** Open, Closed, Net (Open - Closed)
- **Anomaly markers:** Highlight unusual spikes

Severity Distribution

- **Chart type:** Stacked area or bar
- **Categories:** Critical, High, Medium, Low
- **Purpose:** Track severity mix over time
- **Good trend:** Shift toward lower severity

Team Distribution

- **Chart type:** Bar chart
- **Data:** Vulnerability count per team
- **Sorting:** Highest count first
- **Purpose:** Identify workload imbalances

Asset Distribution

- **Chart type:** Bar chart
- **Data:** Vulnerability count per asset
- **Sorting:** Highest count first
- **Purpose:** Identify problematic assets

4.3 Ownership Confidence Distribution

Chart type: Pie or donut chart

Segment	Definition	Color
High Confidence	>= 90%	Green
Medium Confidence	70-89%	Yellow
Low Confidence	< 70%	Orange
Unassigned	No team	Red

Interpretation:

- High percentage of High Confidence = AI working well
- High Unassigned = Review AI configuration

---

5. Standard Reports

5.1 Executive Summary Report

Purpose: High-level security posture for leadership

Contents:

- Total vulnerability count
- Severity breakdown
- Week-over-week trend
- Top 5 risks
- Remediation progress
- Key wins and concerns

Recommended frequency: Weekly

5.2 Team Performance Report

Purpose: Compare team effectiveness

Contents per team:

Metric	Description
Assigned Count	Total vulnerabilities assigned
Resolved Count	Successfully closed
Resolution Rate	% resolved vs assigned
Average Resolution Time	Mean days to resolve
Open Critical/High	Unresolved high-severity
SLA Compliance	% within target time

Recommended frequency: Weekly/Monthly

5.3 Asset Risk Report

Purpose: Identify highest-risk assets

Contents per asset:

Metric	Description
Asset Name	System identifier
Asset Type	Category
Criticality	Business importance
Vulnerability Count	Total findings
Critical Count	Critical severity
Risk Score	Calculated risk level

Recommended frequency: Monthly

5.4 SLA Compliance Report

Purpose: Track remediation timeliness

Contents:

Severity	SLA Target	Resolved	Within SLA	Compliance %
Critical	7 days	[count]	[count]	[%]
High	30 days	[count]	[count]	[%]
Medium	60 days	[count]	[count]	[%]
Low	90 days	[count]	[count]	[%]

Recommended frequency: Weekly/Monthly

5.5 Import Activity Report

Purpose: Track data ingestion

Contents:

Period	Files Imported	Records Added	AI Assigned	Failed
[date]	[count]	[count]	[count]	[count]

---

6. Compliance Reports

6.1 Framework Compliance Report

Available Frameworks:

- SOC 2 (Service Organization Controls)
- ISO 27001 (Information Security Management)
- GDPR (General Data Protection Regulation)
- PCI DSS (Payment Card Industry Data Security Standard)

Report Structure:

Section 1: Executive Summary

- Overall compliance score (0-100%)
- Per-framework scores
- Key gaps identified
- Priority recommendations

Section 2: Gap Summary

Gap Level	Count	Description
Critical	[n]	Immediate action required
High	[n]	Address within 30 days
Medium	[n]	Address within 60 days

Section 3: Detailed Findings Per finding:

- Control reference
- Finding description
- Severity level
- Evidence status
- Remediation recommendation

Section 4: Remediation Roadmap

Phase	Timeline	Actions	Expected Impact
Immediate	0-30 days	[actions]	+X% compliance
Short-term	30-90 days	[actions]	+Y% compliance
Long-term	90+ days	[actions]	+Z% compliance

6.2 Evidence Package

Purpose: Audit-ready documentation

Contents per control:

Element	Description
Control ID	Framework reference
Control Description	Requirement text
Compliance Status	Compliant/Partial/Non-Compliant
Evidence Items	Supporting documentation
Evidence Strength	Strong/Adequate/Weak/Missing

6.3 Policy Recommendations

Output per recommendation:

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

---

7. Calculation Logic

7.1 Severity Classification

VIOE maps CVSS scores to severity:

CVSS Score	Severity	Color
9.0 - 10.0	Critical	Red
7.0 - 8.9	High	Orange
4.0 - 6.9	Medium	Yellow
0.1 - 3.9	Low	Blue
0.0	Info	Gray

7.2 Risk Score Calculation

Asset risk scores (0-100) are calculated using:

```
Risk Score = (Critical × 25) + (High × 15) + (Medium × 5) + (Low × 1)
           × Criticality Multiplier
           × Environment Multiplier
```

```
Capped at 100
```

Criticality Multipliers:

Level	Multiplier
Critical	2.0
High	1.5
Medium	1.0
Low	0.5

Environment Multipliers:

Environment	Multiplier
Production	1.5
Staging	1.0
Development	0.5

7.3 Confidence Score Interpretation

Range	Level	Meaning
90-100%	High	Multiple data sources agree strongly
70-89%	Medium	Most sources agree
50-69%	Low	Some disagreement between sources
<50%	Very Low	Insufficient data or high disagreement

7.4 SLA Timeline Calculation

SLA countdown starts from:

- **Created Date** for new findings
- **Reopened Date** for reactivated findings

SLA pauses when:

- Status = False Positive
- Status = Blocked (with documented reason)

7.5 Trend Calculation

Week-over-Week Change:

```
((Current Week Count - Previous Week Count) / Previous Week Count) × 100
```

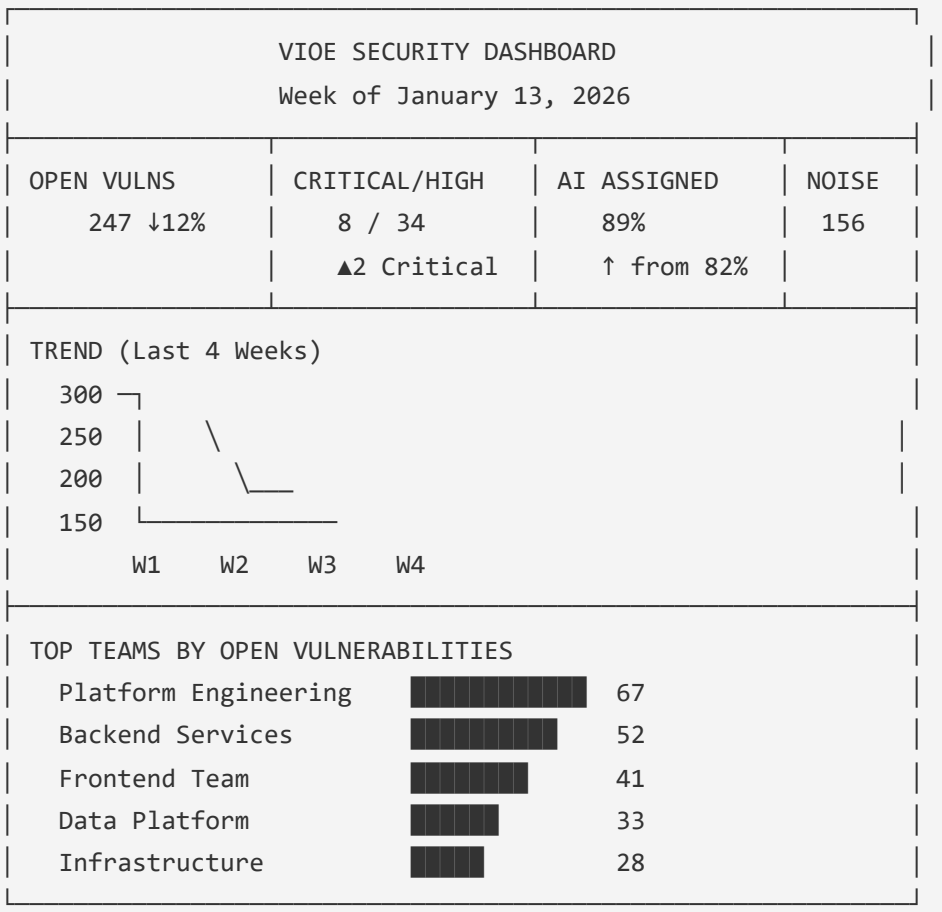
Anomaly Detection:

```
Anomaly if current value > (Historical Average + 2 × Standard Deviation)
```

---

8. Sample Reports

8.1 Sample Executive Dashboard



8.2 Sample Team Performance Summary

```
TEAM PERFORMANCE REPORT - January 2026

Team: Platform Engineering
──────────────────────────────────────────────────

Total Assigned:           147
Resolved This Month:       80
Resolution Rate:          54%
Avg Resolution Time:      12 days

Severity Breakdown:
  Critical:     2 (1 open)
  High:        23 (8 open)
  Medium:      67 (31 open)
  Low:         55 (27 open)

SLA Performance:
  Within SLA:   72/80 (90%)
  Exceeded SLA: 8/80 (10%)

Trend: ↓ 15% reduction in open items from last month
```

8.3 Sample Compliance Summary

```
COMPLIANCE REPORT - SOC 2 Type II

Overall Compliance Score: 78%

Framework Breakdown:
  ┌──────────────────────┬───────┬──────────┐
  │ Category             │ Score │ Status   │
  ├──────────────────────┼───────┼──────────┤
  │ Security             │  82%  │ Good     │
  │ Availability         │  85%  │ Good     │
  │ Processing Integ.    │  74%  │ Fair     │
  │ Confidentiality      │  71%  │ Fair     │
  │ Privacy              │  76%  │ Fair     │
  └──────────────────────┴───────┴──────────┘

Gap Summary:
  Critical Gaps:  3 (require immediate attention)
  High Gaps:      7 (30-day remediation)
```

```
  Medium Gaps:   12 (60-day remediation)

Top Priority Items:
  1. [CC6.1] Access control for critical systems
  2. [CC7.2] Vulnerability management process
  3. [CC3.1] Risk assessment documentation
```

---

9. Interpretation Tips

9.1 Reading Trends Correctly

Increasing Open Vulnerabilities:

- Could indicate more scanning (good)
- Could indicate slower remediation (concern)
- Check: Compare import rate vs. resolution rate

Decreasing Critical Count:

- Usually positive
- Verify: Not due to reclassification
- Confirm: Actual remediation occurred

High Noise Reduction:

- Positive if appropriate rules in place
- Concern if too aggressive
- Review: Sample suppressed items periodically

9.2 Context Matters

Consider when interpreting:

- Recent scanner deployment = expected spike
- Team changes = temporary metric shifts
- New product launch = new attack surface
- Compliance deadline = prioritization shift

9.3 Comparative Analysis

Compare metrics to:

- Previous period (trend)
- Other teams (benchmark)
- Industry standards (maturity)
- Historical baseline (progress)

9.4 Leading vs. Lagging Indicators

Leading Indicators (Predictive):

- Import volume increasing
- AI confidence dropping
- SLA approaching alerts

Lagging Indicators (Historical):

- Resolution rate
- MTTR
- Compliance score

---

10. Common Misreads

10.1 Misread: "Zero Critical = We're Secure"

Reality: Zero critical vulnerabilities is good, but:

- High severity items still pose significant risk
- New critical items could appear tomorrow
- Security is continuous, not a destination

Correct interpretation: Focus on trends and overall posture

10.2 Misread: "High AI Assignment = Problem Solved"

Reality: High AI assignment rate means ownership is automated, but:

- Confidence levels vary
- Assignments may need validation
- Remediation still required

Correct interpretation: AI helps efficiency, not security outcomes

10.3 Misread: "Low Vulnerability Count = Good Security"

Reality: Low counts could indicate:

- Insufficient scanning coverage
- Over-aggressive suppression
- Actually good security

Correct interpretation: Validate scanning coverage first

10.4 Misread: "Team X Has Most Vulnerabilities = Worst Team"

Reality: High count could indicate:

- More assets under management
- More scanning of their systems
- Larger codebase

Correct interpretation: Compare resolution rates, not raw counts

10.5 Misread: "Compliance Score = Security Level"

Reality: Compliance frameworks address specific controls:

- May not cover all threats
- Point-in-time assessment
- Documentation vs. implementation

Correct interpretation: Use as one input among many

10.6 Misread: "False Positives Are Scanner Problems"

Reality: False positives can indicate:

- Scanner misconfiguration
- Context not provided to scanner
- Actually a real issue misunderstood

Correct interpretation: Investigate root cause, improve scanner config

---

11. Report Customization

11.1 Filtering Options

Reports can be filtered by:

Filter	Options
Time Period	Custom date range
Severity	Select specific severities
Environment	Production/Staging/Development
Team	Specific teams
Asset Type	Server/Application/etc.
Status	Open/Resolved/etc.

11.2 Export Formats

Format	Use Case
PDF	Formal reports, printing
Excel	Data analysis, custom charts
CSV	Data integration, custom processing

11.3 Scheduled Reports

Reports can be scheduled for automatic delivery:

Frequency	Typical Use
Daily	Operations team
Weekly	Management review
Monthly	Executive reporting
Quarterly	Board/Audit purposes

11.4 Custom Dashboards

Advanced users can create custom dashboard views:

- Select specific metrics
- Arrange widgets
- Save and share configurations
- Set refresh frequency

Document Control

Version	Date	Author	Changes
1.0	January 2026	Documentation Team	Initial release

This document helps stakeholders accurately interpret VIOE data and reports.

VIOE - Vulnerability Intelligence & Orchestration Engine *Data & Reporting Guide*