Vulnerability Analysis Visualization Guide

Plugin History Analysis Tool

Version 2.0 - December 2024

Vulnerability Analysis Visualization Guide

This guide documents all visualizations available in the Plugin History Analysis Tool, explaining their purpose, data inputs, interpretation methods, and cybersecurity value.

Table of Contents

Risk Tab

CVSS Score Distribution

What it shows: Histogram displaying the distribution of CVSS v3 base scores across all findings. Bars are color-coded by severity:
- **Critical** (red): 9.0+
- **High** (orange): 7.0-8.9
- **Medium** (yellow): 4.0-6.9
- **Low** (green): 0-3.9

Data Inputs:
- `cvss3_base_score` from vulnerability scan data

Cybersecurity Value:
Helps identify the overall risk profile of your environment. A distribution skewed toward higher scores indicates systemic security issues requiring immediate attention. Use this to prioritize remediation efforts and justify security investments to leadership.

How to Interpret:
- Peak location shows typical vulnerability severity in your environment
- Wide spread suggests diverse risk levels requiring varied response strategies
- Right-skewed distributions (more high scores) are concerning and warrant investigation
- Compare against industry benchmarks for your sector

Available Filters: Severity, Status, Date Range, Environment

Mean Time to Remediation (MTTR)

What it shows: Bar chart showing average days to resolve vulnerabilities grouped by severity level. Only includes resolved findings.

Data Inputs:
- `days_open` - Calculated as: current_date - first_observed_date (from scanner output)
- `severity_text` - Severity classification
- `status` - Must be "Resolved"

Cybersecurity Value:
Key metric for security operations effectiveness. Compare against SLA targets to identify compliance gaps. Critical and High MTTR exceeding SLAs indicates remediation process failures that may require resource reallocation or process improvement.

How to Interpret:
- Lower bars = faster remediation (better)
- Critical should have lowest MTTR (highest priority)
- Compare to your SLA targets:
- Critical: 15 days
- High: 30 days
- Medium: 60 days
- Low: 90 days

Available Filters: Severity, Date Range, Environment

Findings by Age

What it shows: Stacked bar chart showing active findings bucketed by age:
- 0-30 days (newest)
- 31-60 days
- 61-90 days
- 90+ days (aging)

Data Inputs:
- `days_open` - Calculated as: current_date - first_observed_date (from scanner output)
- `status` - Active findings only

Cybersecurity Value:
Aging vulnerabilities represent increased risk exposure. Findings over 90 days likely indicate process failures, lack of ownership, or technical barriers. Use for compliance reporting and risk acceptance decisions with leadership.

How to Interpret:
- Most findings should be in 0-30 day bucket
- Large 90+ day bucket indicates remediation backlog requiring management attention
- Track this over time to show remediation velocity improvement

Available Filters: Severity, Status, Environment

Top Risky Hosts

What it shows: Horizontal bar chart showing hosts with highest cumulative risk scores, colored by environment type:
- **Production** (green)
- **PSS/Pre-Production** (blue)
- **Shared** (yellow)

Data Inputs:
- `hostname` - Asset identifier
- `severity_value` - Numeric severity weight (Critical=4, High=3, Medium=2, Low=1)
- `environment_type` - Derived from hostname pattern

Cybersecurity Value:
Identifies assets requiring immediate security attention. Production hosts with high risk scores should be prioritized. Helps target penetration testing and security assessments. Use for asset-centric remediation planning.

How to Interpret:
- Focus remediation on top hosts first
- Consider isolating high-risk production systems
- Environment coloring helps prioritize based on business impact
- A single host with extreme risk may indicate compromise or critical misconfiguration

Available Filters: Severity, Status, Environment, Host Type

Timeline Tab

Total Findings by Period

What it shows: Line chart showing total vulnerability count over time, grouped by selected interval (daily, weekly, monthly). Includes trend indicator.

Data Inputs:
- `scan_date` - When vulnerability was detected
- Finding counts aggregated by period

Cybersecurity Value:
Shows overall security posture trajectory. Increasing trend indicates growing attack surface or inadequate remediation. Flat or decreasing trend suggests security program effectiveness.

How to Interpret:
- Upward trend = increasing risk exposure
- Spikes may indicate:
- New vulnerability scanner deployment
- Expanded scan scope
- Major vulnerability disclosures (e.g., Log4j)
- Compare to security events or infrastructure changes

Available Filters: Date Range, Severity, Environment

Findings by Severity Over Time

What it shows: Multi-line chart tracking Critical, High, Medium, Low findings over time. Each severity has distinct color for easy tracking.

Data Inputs:
- `scan_date` - Detection timestamp
- `severity_text` - Severity classification

Cybersecurity Value:
Monitors severity distribution changes. Sudden Critical/High spikes may indicate zero-days or new attack vectors. Helps demonstrate remediation progress by severity tier to stakeholders.

How to Interpret:
- Critical/High lines should trend downward over time
- Watch for correlation between severity levels
- Diverging trends may indicate prioritization issues (e.g., only remediating low severity)
- Sudden spikes warrant immediate investigation

Available Filters: Date Range, Environment

New vs Resolved

What it shows: Grouped bar chart comparing:
- **New findings** discovered per period (red)
- **Findings resolved** per period (green)
- Net change shown

Data Inputs:
- `scan_changes` table - New/Resolved status transitions

Cybersecurity Value:
Core metric for security program health. Resolved > New indicates reducing risk. Persistent deficit suggests inadequate resources or process issues requiring management escalation.

How to Interpret:
- Green bars (resolved) should exceed red bars (new)
- Calculate velocity: Resolved/New ratio
- Ratio > 1.0 = improving posture
- Ratio < 1.0 = falling behind
- Ratio = 1.0 = treading water

Available Filters: Date Range, Severity, Environment

Cumulative Risk Score

What it shows: Area chart showing total severity-weighted risk score over time.

Calculation:

```
Risk Score = Σ (severity_value for all active findings)
where:
  Critical = 4 points
  High = 3 points
  Medium = 2 points
  Low = 1 point
```

Cybersecurity Value:
Single metric capturing overall organizational risk. Use for executive reporting and risk trending. Enables comparison across time periods and business units.

How to Interpret:
- Downward slope = risk reduction
- Plateaus indicate stagnation
- Sharp increases require immediate investigation
- Set target risk score thresholds for alerts

Available Filters: Date Range, Environment

SLA Tab

SLA Compliance Overview

What it shows: Stacked bar chart showing:
- **Compliant** (green) - On track to meet SLA
- **At-Risk** (yellow) - Approaching deadline (within 25%)
- **Breached** (red) - Past SLA deadline

Grouped by severity level.

Data Inputs:
- `severity_text` - Severity classification
- `sla_status` - Calculated from days_open vs SLA targets

SLA Targets (Configurable):
Severity	Days
Critical	15
High	30
Medium	60
Low	90

Cybersecurity Value:
Critical for compliance reporting and audit evidence. SLA breaches may trigger contractual penalties or regulatory findings. Track for continuous improvement initiatives.

How to Interpret:
- Focus on reducing red segments, especially for Critical/High
- Yellow segments need proactive attention before breach
- 100% green is the goal

Available Filters: Severity, Environment

SLA Breaches by Severity

What it shows: Bar chart showing count of SLA-breached findings per severity level.

Data Inputs:
- `severity_text` - Severity classification
- `days_open` - Current age of finding
- `sla_targets` - Configured thresholds

Cybersecurity Value:
Direct compliance risk indicator. High breach counts require escalation and resource allocation. Document for audit trail and management reporting.

How to Interpret:
- Critical breaches are highest priority
- Zero breaches is the goal
- Track month-over-month improvement
- Investigate root causes for persistent breaches

Available Filters: Date Range, Environment

SLA Approaching Deadline

What it shows: List/bar of findings within warning threshold of SLA deadline (typically within 25% of remaining time).

Data Inputs:
- `severity_text` - Severity classification
- `days_open` - Current age
- `sla_targets` - Configured thresholds
- `warning_threshold` - Typically 25%

Cybersecurity Value:
Early warning system for potential breaches. Enables proactive remediation before SLA violation. Helps resource planning and workload distribution.

How to Interpret:
- These findings need immediate attention
- Sort by days remaining
- Assign owners and track daily
- Use for daily standup prioritization

Available Filters: Severity, Environment

Days to SLA Deadline

What it shows: Distribution chart showing days remaining until SLA deadline.
- Positive values = time remaining
- Negative values = days overdue

Data Inputs:
- `sla_deadline` - Calculated from first_seen + SLA days
- `current_date` - Today

Cybersecurity Value:
Visualizes remediation urgency across entire portfolio. Helps identify systemic issues (e.g., all Critical findings overdue).

How to Interpret:
- Distribution should be right-skewed (most findings have time remaining)
- Left tail (negative values) represents breaches
- Bimodal distribution may indicate batch remediation patterns

Available Filters: Severity, Status, Environment

OPDIR Tab

OPDIR Coverage

What it shows: Pie chart showing:
- Findings mapped to OPDIR directives
- Unmapped findings

Data Inputs:
- `opdir_number` - OPDIR directive reference (presence indicates mapping)

Cybersecurity Value:
OPDIR directives are authoritative remediation requirements. Unmapped findings may lack official guidance. Coverage indicates compliance posture with mandated security requirements.

How to Interpret:
- Higher mapped percentage = better compliance coverage
- Unmapped findings need manual assessment
- Low coverage may indicate new vulnerability types not yet in OPDIR guidance

Available Filters: Severity, Status

OPDIR Compliance Status

What it shows: Donut chart showing:
- **Overdue** (red) - Past OPDIR deadline
- **Due Soon** (yellow) - Approaching deadline
- **On Track** (green) - Meeting timeline

Data Inputs:
- `opdir_due_date` - Mandated remediation deadline
- `current_date` - Today

Cybersecurity Value:
Direct compliance measurement against authoritative directives. Overdue findings may result in audit findings or security incidents. Critical for regulatory compliance.

How to Interpret:
- Minimize red (overdue) segment
- Yellow indicates upcoming deadlines needing attention
- Green shows compliant items
- Track weekly improvement

Available Filters: Date Range, Environment

OPDIR Finding Age Distribution

What it shows: Histogram of days since discovery for OPDIR-mapped findings.

Data Inputs:
- `first_seen` - Discovery date
- `opdir_number` - Must have OPDIR mapping

Cybersecurity Value:
Shows remediation velocity for mandated vulnerabilities. Long-standing OPDIR findings indicate serious compliance issues requiring escalation.

How to Interpret:
- Distribution should skew left (newer findings)
- Long tail indicates remediation challenges
- Investigate outliers for root cause

Available Filters: OPDIR Status, Severity

Findings by OPDIR Year

What it shows: Grouped bar showing findings by OPDIR directive release year.

Data Inputs:
- `opdir_number` - Year extracted from directive number

Cybersecurity Value:
Older directives with open findings suggest persistent compliance gaps. Helps identify historical remediation debt requiring special attention.

How to Interpret:
- Findings from older years indicate long-standing issues
- Recent years should have fewer findings (newer directives)
- Large counts for old years = technical debt

Available Filters: Status, Severity

Efficiency Tab

Scan Coverage Consistency

What it shows: Distribution of hosts by number of scans they appear in.

Data Inputs:
- `hostname` - Asset identifier
- `scan_date` - Unique scans per host count

Cybersecurity Value:
Identifies gaps in vulnerability scanning program. Hosts scanned infrequently may harbor undetected vulnerabilities creating blind spots.

How to Interpret:
- Peak should be at high scan counts (consistent coverage)
- Left tail indicates under-scanned assets
- Investigate hosts with low scan counts

Available Filters: Date Range, Host Type

Vulnerability Reappearance

What it shows: Chart showing vulnerabilities that were resolved but reappeared in subsequent scans.

Data Inputs:
- `scan_changes` - Status transitions tracking Resolved → New

Cybersecurity Value:
Indicates ineffective remediation or regression. High reappearance suggests root cause not addressed or change management issues requiring process improvement.

How to Interpret:
- Lower is better
- Recurring findings need root cause analysis
- May indicate:
- Patch rollback
- Configuration drift
- Incomplete remediation
- Re-imaging with old images

Available Filters: Severity, Date Range

Vulnerabilities per Host

What it shows: Distribution showing how vulnerabilities are spread across hosts.

Data Inputs:
- `hostname` - Asset identifier
- Finding count per host

Cybersecurity Value:
Identifies concentration risk. Few hosts with many vulnerabilities are high-value targets for attackers. May indicate compromised or misconfigured systems.

How to Interpret:
- Right-skewed = few problematic hosts (concentrate efforts)
- Flat distribution = systemic issues (need broad remediation)
- Identify outliers for investigation

Available Filters: Severity, Environment, Host Type

Resolution Velocity

What it shows: Distribution of time-to-resolution for remediated vulnerabilities.

Data Inputs:
- `days_open` - For resolved findings only

Cybersecurity Value:
Measures remediation efficiency. Compare to industry benchmarks and SLA targets. Use for process improvement and resource planning.

How to Interpret:
- Peak location shows typical remediation time
- Long tail indicates outliers needing investigation
- Track shift leftward over time (faster remediation)

Available Filters: Severity, Date Range, Environment

Network Tab

Top Subnets by Vulnerability

What it shows: Horizontal bar chart showing network subnets with most vulnerabilities.

Data Inputs:
- `ip_address` - Subnet extracted (first 3 octets)

Cybersecurity Value:
Identifies network segments requiring security focus. May indicate:
- Vulnerable applications
- Outdated infrastructure
- Inadequate segmentation
- Shadow IT

How to Interpret:
- Focus network security efforts on top subnets
- Consider additional segmentation for high-risk segments
- Investigate common vulnerability patterns

Available Filters: Severity, Status, Environment

Subnet Risk Scores

What it shows: Risk-weighted view of network segments using severity scoring.

Data Inputs:
- `ip_address` - Subnet identifier
- `severity_value` - Weighted score

Cybersecurity Value:
Prioritizes network segments by actual risk, not just count. Critical vulnerabilities weight higher than informational. Better for risk-based prioritization.

How to Interpret:
- High-risk subnets need immediate attention regardless of count
- May justify network redesign or additional controls
- Compare risk density (risk per host)

Available Filters: Severity, Status

Host Criticality Distribution

What it shows: Distribution of cumulative risk scores across hosts.

Data Inputs:
- `hostname` - Asset identifier
- `severity_value` - Summed per host

Cybersecurity Value:
Visualizes risk concentration across infrastructure. Tail represents high-value targets requiring immediate attention or isolation.

How to Interpret:
- Right tail hosts are critical priority
- Average line shows typical risk level
- Investigate hosts above 2 standard deviations

Available Filters: Environment, Host Type

Environment Distribution

What it shows: Pie/bar chart showing findings by environment type:
- Production
- PSS (Pre-Production)
- Shared
- Unknown

Data Inputs:
- `hostname` → `environment_type` mapping

Cybersecurity Value:
Production vulnerabilities have highest business impact. Shared infrastructure affects multiple environments, creating broader risk exposure.

How to Interpret:
- Production findings need prioritization
- Shared findings may have broader impact
- PSS can be used for patch testing

Available Filters: Severity, Status

Plugin Tab

Top 15 Most Common Plugins

What it shows: Horizontal bar chart showing most frequently detected vulnerability types (by Plugin ID).

Data Inputs:
- `plugin_id` - Unique vulnerability identifier
- `plugin_name` - Human-readable name
- Count of occurrences

Cybersecurity Value:
Identifies systemic vulnerabilities affecting many hosts. These are often:
- Misconfigurations
- Missing patches
- Default credentials
- Outdated software

Single remediation action can affect many hosts (high ROI).

How to Interpret:
- Top plugins may have single remediation action
- High count + high severity = critical priority
- Look for patterns (same application, same OS)

Available Filters: Severity, Status, Environment

Findings by Severity

What it shows: Bar chart showing total findings per severity level.

Data Inputs:
- `severity_text` - Severity classification

Cybersecurity Value:
Quick view of severity distribution. Critical and High counts drive risk posture. Use for executive dashboards.

How to Interpret:
- Healthy: Pyramid shape (more Low, fewer Critical)
- Concerning: Inverted pyramid
- Track ratios over time

Available Filters: Status, Environment

Plugins Affecting Most Hosts

What it shows: Plugins ranked by number of unique hosts affected.

Data Inputs:
- `plugin_id` - Vulnerability identifier
- `hostname` - Unique count per plugin

Cybersecurity Value:
Wide-spread vulnerabilities indicate systemic issues. High host count + high severity = critical priority requiring immediate action.

How to Interpret:
- Top plugins affect most infrastructure
- Single fix can reduce risk across many assets
- Prioritize by (host_count × severity_weight)

Available Filters: Severity, Status

Plugins with Longest Average Age

What it shows: Plugins ranked by average days open.

Color Coding:
- **Red**: >90 days average
- **Orange**: >30 days average
- **Green**: <30 days average

Data Inputs:
- `plugin_id` - Vulnerability identifier
- `days_open` - Averaged per plugin

Cybersecurity Value:
Long-standing vulnerability types may indicate:
- Remediation barriers (no patch available)
- False positives needing tuning
- Process failures
- Resource constraints

How to Interpret:
- Red items need investigation
- May be unfixable or require significant effort
- Consider risk acceptance for very old items

Available Filters: Status, Environment

Priority Tab

Remediation Priority Matrix

What it shows: Scatter plot with:
- **X-axis**: CVSS score (severity)
- **Y-axis**: Days open (age)
- **Point color**: Severity level

Data Inputs:
- `cvss3_base_score` - Numeric severity
- `days_open` - Age of finding
- `severity_text` - Color coding

Cybersecurity Value:
Visual prioritization tool combining severity and urgency.

Quadrant Analysis:
Quadrant	CVSS	Age	Priority
Upper-Right	High	Old	CRITICAL - Fix immediately
Lower-Right	High	New	HIGH - Fix soon

| Upper-Left | Low | Old | MEDIUM - Plan remediation |
| Lower-Left | Low | New | LOW - Schedule later |

How to Interpret:
- Focus on upper-right quadrant first
- Track movement toward lower-left over time

Available Filters: Severity, Status, Environment

Priority Distribution

What it shows: Pie chart showing findings by calculated priority bucket:
- **Urgent** - High severity + old
- **High** - High severity OR old
- **Medium** - Moderate risk
- **Low** - Low severity + new

Data Inputs:
- `priority_score` - Calculated from CVSS + age

Cybersecurity Value:
Summary view for resource planning. Urgent items need immediate attention and dedicated resources.

How to Interpret:
- Track urgent reduction over time
- Healthy distribution has small urgent slice (<10%)
- Large urgent slice requires escalation

Available Filters: Severity, Status

Top 10 Priority Findings

What it shows: List of highest priority findings based on CVSS score and age combination.

Data Inputs:
- `priority_score` - Ranking metric
- `plugin_name` - Vulnerability description
- `hostname` - Affected asset

Cybersecurity Value:
Action list for remediation teams. These should be assigned and tracked daily in standups.

How to Interpret:
- Start remediation from top
- Check for common threads:
- Same host (concentrate remediation)
- Same vulnerability (single fix, multiple hosts)
- Update daily

Available Filters: Environment, Host Type

Priority Score by Severity

What it shows: Average priority score grouped by severity level.

Data Inputs:
- `priority_score` - Calculated metric
- `severity_text` - Grouping

Cybersecurity Value:
Shows if high-severity items are being addressed quickly.

How to Interpret:
- Critical should have LOWEST priority score (newest = being fixed fast)
- Higher bars for Critical/High = aging high-severity items = BAD
- Investigate if Critical bar > Low bar

Available Filters: Status, Environment

Host Tracking Tab

Missing Hosts

What it shows: Hosts not seen in recent scans that previously appeared.

Data Inputs:
- `hostname` - Asset identifier
- `last_seen_date` - Most recent scan appearance

Cybersecurity Value:
Missing hosts may be:
- Decommissioned (verify with CMDB)
- Renamed (update records)
- Dropped from scan scope (configuration error)
- Network isolated (may need agent-based scanning)

Security risk if active but unscanned!

How to Interpret:
- Verify status of each missing host
- Update inventory or scan configuration
- Document decommissioned hosts

Available Filters: Date Range, Environment

Hosts per Scan Over Time

What it shows: Line chart showing unique host count per scan over time.

Data Inputs:
- `scan_date` - Scan timestamp
- `hostname` - Unique count per scan

Cybersecurity Value:
Monitors scan scope consistency. Changes may indicate:
- Infrastructure changes
- Scanner issues
- Network problems
- Credential failures

How to Interpret:
- Stable line is good
- Sudden drops need investigation
- Gradual increase = growing infrastructure

Available Filters: Date Range

Declining Scan Coverage

What it shows: Hosts showing decreased scan frequency or intermittent coverage.

Data Inputs:
- `hostname` - Asset identifier
- Scan appearance frequency calculation

Cybersecurity Value:
Intermittent scanning creates blind spots. Attackers can exploit gaps in visibility. Critical hosts should have consistent coverage.

How to Interpret:
- Investigate cause for each declining host
- May need scanner configuration changes
- Consider agent-based scanning for mobile assets

Available Filters: Date Range, Environment

Host Status Overview

What it shows: Distribution of hosts by scanning status:
- **Active** - Seen in recent scans
- **Intermittent** - Inconsistent appearance
- **Missing** - Not seen recently

Data Inputs:
- `hostname` - Asset identifier
- Scan frequency classification

Cybersecurity Value:
Quick health check of vulnerability management program coverage. High missing percentage indicates scanning program issues.

How to Interpret:
- Maximize Active percentage
- Minimize Missing percentage
- Set thresholds based on scan schedule

Available Filters: Environment, Host Type

Metrics Tab

Remediation vs Active by Severity

What it shows: Grouped bar comparing:
- **Resolved** (green) findings per severity
- **Active** (red) findings per severity

Data Inputs:
- `severity_text` - Severity classification
- `status` - Active or Resolved

Cybersecurity Value:
Shows remediation progress across severity tiers. Higher resolved:active ratio is better. Use for monthly reporting.

How to Interpret:
- Green should exceed red, especially for Critical/High
- Calculate ratio per severity
- Track improvement over time

Available Filters: Date Range, Environment

Organization Risk Trend

What it shows: Line chart showing overall risk score over time with trend line.

Data Inputs:
- `scan_date` - Timestamp
- `severity_value` - Summed risk score

Cybersecurity Value:
Executive-level metric for security program effectiveness. Use for board reporting and budget justification.

How to Interpret:
- Downward trend shows improvement
- Flat indicates stagnation
- Rising requires action and escalation

Available Filters: Date Range

SLA Compliance by Severity

What it shows: Stacked percentage bar showing SLA compliance rate per severity.

Data Inputs:
- `severity_text` - Severity classification
- `sla_status` - Compliance status

Cybersecurity Value:
Compliance metric for regulatory and contractual requirements. Target 100% compliance, especially for Critical.

How to Interpret:
- Track improvement over time
- Identify severity levels with compliance issues
- Set improvement targets

Available Filters: Date Range, Environment

Vulnerabilities per Host Trend

What it shows: Average vulnerabilities per host over time.

Calculation:

```
Vulns per Host = Total Findings / Unique Hosts
```

Cybersecurity Value:
Normalized metric accounting for infrastructure growth. Better for comparison across time periods and organizations.

How to Interpret:
- Decreasing trend shows per-asset risk reduction
- Compare to industry benchmarks
- Use for maturity assessment

Available Filters: Date Range, Environment

Advanced Charts

Vulnerability Density Heatmap

What it shows: Grid showing vulnerability density by host and severity. Darker cells = more findings.

Data Inputs:
- `hostname` - Row identifier
- `severity_text` - Column identifier
- Count - Cell value

Cybersecurity Value:
Visual pattern recognition for concentrated risk areas. Quickly identify problematic hosts.

How to Interpret:
- Dark cells are priority
- Patterns across rows = systemic host issues
- Patterns down columns = severity-specific issues

Available Filters: Severity, Status, Environment

Bubble Chart

What it shows: Multi-dimensional visualization:
- **X-axis**: CVSS score
- **Y-axis**: Age (days open)
- **Bubble size**: Hosts affected
- **Color**: Severity

Cybersecurity Value:
Rich visualization for executive presentations. Shows multiple risk dimensions in single view.

How to Interpret:
- Large red bubbles in upper-right = critical priorities
- Focus on reducing bubble count and size
- Track movement toward origin (lower-left)

Available Filters: Severity, Status

Lifecycle Flow (Sankey)

What it shows: Flow diagram showing vulnerability progression:
- Discovery → Active
- Active → Resolved
- Resolved → Reappeared

Data Inputs:
- Status transitions over time

Cybersecurity Value:
Process visualization for remediation workflow analysis. Identifies bottlenecks and inefficiencies.

How to Interpret:
- Thick flows to Resolved = good
- Thin flows to Resolved = bottleneck
- Flows to Reappeared = remediation quality issue

Available Filters: Date Range, Severity

Category Treemap

What it shows: Hierarchical view of vulnerabilities by plugin family/category.

Data Inputs:
- `plugin_family` - Category grouping
- Count per category
- Severity weighting

Cybersecurity Value:
Identifies vulnerability categories requiring attention. Helps focus remediation by vulnerability type.

How to Interpret:
- Large tiles represent significant categories
- Color indicates severity mix
- Click to drill down

Available Filters: Severity, Status

SLA Breach Prediction

What it shows: Forecast of upcoming SLA breaches based on current trajectory.

Data Inputs:
- `days_to_sla` - Time remaining
- `remediation_velocity` - Historical fix rate

Cybersecurity Value:
Proactive risk management. Plan resources before breaches occur. Enables preventive action.

How to Interpret:
- Rising line = increasing future breaches
- Take action before predicted breach
- Use for resource planning

Available Filters: Severity

Period Comparison

What it shows: Side-by-side comparison of metrics between two time periods.

Metrics Compared:
- Total findings
- Risk score
- MTTR
- SLA compliance
- New vs Resolved ratio

Cybersecurity Value:
Demonstrates program improvement for reporting and audits. Shows trend direction.

How to Interpret:
- Green indicators = improvement
- Red indicators = regression
- Use for quarterly/annual reporting

Available Filters: Date Range Selection

Smart Filtering

Overview

Smart filtering automatically overrides the UI status filter for specific visualizations that require certain data regardless of user selection. This ensures accurate metrics even when the user has filtered to view only Active or Remediated findings.

Why Smart Filtering Matters

Some metrics can only be calculated with specific data:
- **Remediation Rate**: Requires BOTH Active and Remediated findings to calculate the percentage
- **MTTR (Mean Time to Remediation)**: Requires only Remediated findings (can't measure time to fix if not fixed)
- **Reopen Rate**: Requires both statuses to track findings that were remediated then reappeared

Without smart filtering, viewing only "Active" findings would show 0% remediation rate, which is misleading.

Visualizations Using Smart Filtering

Visualization	Smart Filter	Reason
MTTR by Severity	Remediated Only	Can only calculate fix time for fixed items
Remediation Rate	Both Statuses	Need both to calculate Active vs Remediated ratio
Remediation Status by Severity	Both Statuses	Compares Active vs Remediated counts
Reopen Rate	Both Statuses	Tracks remediated items that became active again
Resolution Velocity	Remediated Only	Distribution of time-to-fix

Filter Behavior

When smart filtering is active:
- **Date Range**: Still respected (metrics are within selected date range)
- **Severity Filter**: Still respected (can filter to Critical only, etc.)
- **Environment Filter**: Still respected (can filter to Production only)
- **Status Filter**: Overridden to ensure accurate metrics

User Experience

Smart filtering is automatic and transparent. When viewing a chart that uses smart filtering:
1. The data shown reflects accurate metrics regardless of the Status filter selection
2. Other filters (date, severity, environment) still apply normally
3. No user action is required - the system handles this automatically

This ensures that executive dashboards and compliance reports always show accurate remediation metrics, even if an analyst has temporarily filtered to view only active findings for triage work.

Environment Filtering

Environment Types

The tool supports classification of hosts by environment:

Environment	Description	Priority
Production	Live business systems	Highest
PSS	Pre-production/staging	Medium
Shared	Infrastructure used by multiple environments	High (broad impact)
Unknown	Unclassified hosts	Review needed

Hostname Detection

Environments are detected from hostname patterns (9-character format: LLLLTTCEP):

- Position 8: Letter (A-Z) = Production, Number (0-9) = PSS
- Custom mappings can override auto-detection

Configuration

Access environment configuration via the gear icon next to the Environment filter.
Options include:
- Custom environment types
- Explicit hostname mappings
- Pattern-based rules

Using the Visualizations

Interaction Features

All Charts:
- **Double-click**: Open enlarged pop-out view
- **Hover**: See detailed tooltips

Pop-out Windows:
- **Zoom**: +/- buttons for magnification
- **Pan**: Click and drag to move view
- **Labels toggle**: Show/hide data labels
- **Status filter**: Active/Resolved/All
- **Mode filter**: Filtered/All Data/Unique
- **Date filter**: Custom date range
- **Copy to Clipboard**: Save chart image
- **Info button**: View chart documentation

Best Practices

1. **Start with Risk Tab** - Understand overall posture
2. **Use Timeline Tab** - Identify trends and patterns
3. **Check SLA Tab** - Verify compliance status
4. **Drill into Plugin Tab** - Find systemic issues
5. **Review Host Tracking** - Ensure complete coverage

Reporting Recommendations

Weekly:
- New vs Resolved trend
- SLA approaching findings
- Top risky hosts

Monthly:
- MTTR by severity
- Risk trend
- Environment distribution

Quarterly:
- Period comparison
- OPDIR compliance
- Category treemap

Technical Reference

Data Sources

Table	Description
`historical_findings`	All findings with metadata
`finding_lifecycle`	Status and age tracking
`scan_changes`	New/Resolved events
`host_presence`	Scan coverage tracking

Date Field Clarification

Important distinction:
- `first_observed_date`: The timestamp when the vulnerability was first detected by the scanner (from scan output). Used for calculating `days_open`.
- `scan_date`: The date of the scan report. Used for filtering and timeline visualizations.

`days_open` **Calculation:**

```
days_open = current_date - first_observed_date
```

- Uses the scanner's first observation timestamp, NOT the report date
- Date only, no time-of-day consideration
- More accurate representation of actual exposure duration

Severity Values

Severity	Value	SLA (days)
Critical	4	15
High	3	30
Medium	2	60
Low	1	90

Risk Score Calculation

```
Host Risk = Σ severity_value for all active findings on host
Org Risk = Σ severity_value for all active findings
```

Document generated from chart_descriptions.py
For questions or feedback, consult your security team or tool administrators.