ScienceLogic

Event Details Report Instruction Manual and Use Cases

Documented by: Bob Ahmadi

16/02/2026

Table of Contents

Introduction

The **Event Details Report PowerPack** is designed to provide valuable insights into events and incidents noise, helping organizations identify sources of noise and optimize system performance. This PowerPack includes a collection of reports and a dashboard that offer a comprehensive view of event volumes, incident trends, and automation triggers over selected time periods.

With dedicated reports analyzing events and incidents frequency, as well as those focusing on triggered automations, users can gain a deeper understanding of operational noise and its impact. The included **Event and Incident Dashboard** further enhances visibility by showcasing the noise level, its sources, and the ratio of events and incidents to active devices.

By leveraging these insights, organizations can fine-tune event policies, adjust system thresholds, and optimize settings to **reduce Mean Time to Repair (MTTR) and operational costs**. This PowerPack empowers teams to take proactive measures in noise reduction, ensuring a more efficient and stable IT environment.

Key challenges

Without having the visibility, organizations struggle to effectively manage event and incident noise, leading to several operational challenges. A lack of visibility in event volumes and sources makes it difficult to pinpoint and address the root causes of excessive noise, resulting in longer **Mean Time to Repair (MTTR)** and increased operational costs. Without proper insights, teams may experience alert fatigue, where overwhelming event volumes cause critical alerts to be missed or delayed. Additionally, without automated tracking of incident-triggering events, organizations may face inefficiencies in troubleshooting and automation optimization. The inability to analyze event/incident-to-active device ratios further complicates resource allocation and system fine-tuning, leading to ineffective event policies and threshold settings. Ultimately, these challenges contribute to reduced system stability, slower issue resolution, and unnecessary operational expenses, making proactive event management a significant hurdle.

Purpose of the Document

The purpose of this document is to provide an overview of the **Event Details Report PowerPack**, highlighting its features, benefits, and with their individual use cases. It explains how the included reports and dashboards offer valuable insights into events and incidents noise, enabling organizations to optimize their event management strategies. This document serves as a guide to understanding how the PowerPack can help reduce MTTR, improve operational efficiency, and fine-tune system settings to minimize unnecessary noise.

Audience

SL1 Admins, Operation Engineers, Operation Manager.

Important Notes to Remember

- Reports cannot replace the event page, The event page provides real time information about events and incidents while reports are for event and incident analysis and can't provide real time information. Please avoid using reports for real time events and incidents management.
- Any changes in a live and production environment must comply with the organization's change policy.
- ScienceLogic strongly recommends implementing any changes first in your lab environment and then transitioning it into production.
- Always backup your configuration before making any changes within your environment.

Key Business benefits

- **Reduced MTTR & Operational Costs** – Gain insights into event and incident noise to quickly identify and resolve issues, minimizing downtime and resource expenses.
- **Improved Event Management & Noise Reduction** – Identify the sources of excessive noise and fine-tune event policies, system thresholds, and settings for a more efficient IT environment.
- **Enhanced Automation Optimization** – Understand which events trigger automations, allowing teams to refine workflows and improve overall system efficiency.
- **Better Visibility & Decision-Making** – Leverage detailed reports and dashboards to monitor event trends, enabling proactive decision-making and more effective IT operations.

Pre-requisites

To use this solution you need to download, import and install the latest version of **Event Details Report and Dashboards** PowerPack from this link.

The PowerPack contains:

1- Reports:
   a. Active Events – Incidents.
   b. Event Details Report – Lean Severity.
   c. Event Details Report – First Occurrence V2.
   d. Event Details Report - Last Occurrence V2.
   e. Event Details Report – Lean (Policy ID&EID).
   f. Event Policy Report.
   g. Number of Cleared Events per Device per Org.
   h. Number of Cleared Incidents per Device per Org.
   i. Active Event to Active Device Ratio.
   j. Active Incidents to Active Device Ratio.
   k. Cleared Event to Active Device Ratio.
   l. Cleared Incident to Active Device Ratio.

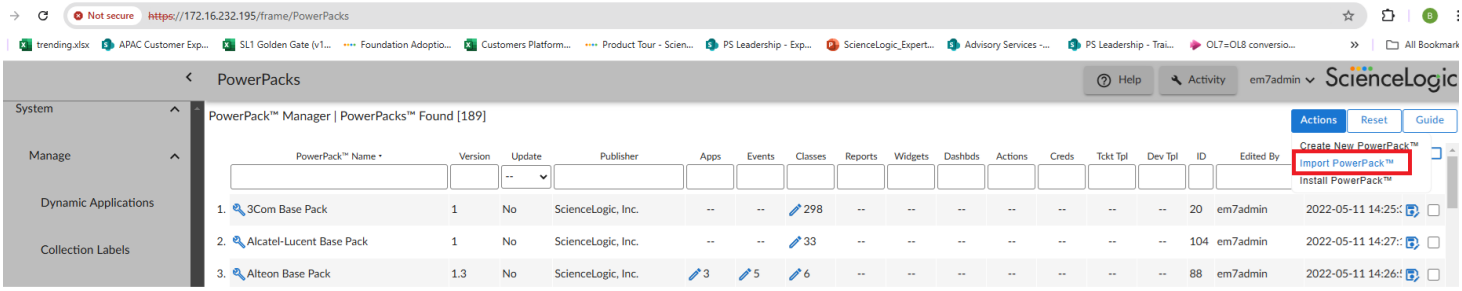
2- Dashboard:
   a. Events and Incidents Details Dashboard. (Classic)

PowerPack Import and Install

Download the PowerPack from provided link.

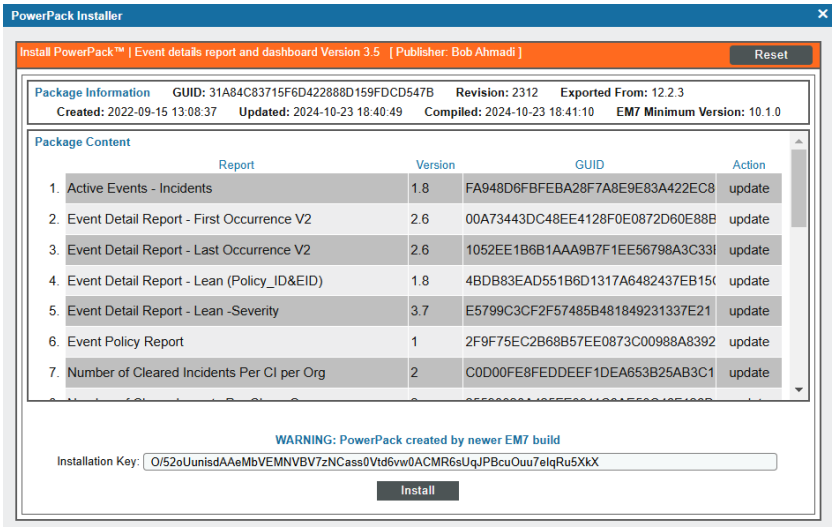
1- In the AP2 UI go to System -> Manage -> PowerPacks

2- Click on the "Actions" button on the top right corner of the screen and click import.



3- On the Import PowerPack Window, Click Browse, navigate to the location of the downloaded PowerPack, select the PowerPack, click open and select Import.

4- In the PowerPack Installer window, select Install and click Ok.



Reports and Use Cases.

1. Active Events/Incidents Report

The purpose of this report is to provide detailed information about active events and incidents. The information in this report is similar to the event page in your SL1 platform.

Use Case:

Use this report when you need to review details of current active events and incidents. It is particularly useful for assessing the volume of events/incidents in real time and for performing resource management, capacity management, and aged ticket planning.

2. Event Details Report – Lean Severity

This report is the best tool for managing events, incidents, and noise in the environment. It provides essential and valuable insights into both cleared and active events/incidents over a selected time period.

Use Case:

If your primary goal is to reduce noise volume in the SL1 platform, this is the report you need. There are multiple options for running the report, including filtering by Organization, Event Policy, Severity, Time Span, Event or Incident Type, and Date Type.

There are three types of date filters available:

a. Last Occurrence

- If you run the report based on Last Occurrence, SL1 uses the selected report span and matches that date with the date_last field in the events table of the database.

  When to use: This option is useful when you want to analyze the most recent occurrences of events/incidents and understand their frequency or patterns. It helps in identifying ongoing issues that may require immediate attention.

b. Date Active

- If you run the report based on Date Active, SL1 uses the selected Date Span to match the date with the date_active field in the database.
  When to use: Choose this option when you need to examine events/incidents that were active during that specific date. It is particularly helpful for trend analysis and tracking the duration of active incidents.

c. Date Delete

- If you run the report based on Date Delete, SL1 uses the selected Date Span to match the date with the date_del field in the database.

  When to use: This option is valuable when you need to track and analyze incidents that have been removed or cleared from the system. It helps in understanding resolution trends, cleanup efforts, and event lifecycles.

3. Event Details Report – First Occurrence and Last Occurrence

Both reports serve the same purpose: providing insightful information about Runbook Automations (RBAs) triggered by events or incidents.

- First Occurrence Report: Runs the report based on the date_active field in the event table.
- Last Occurrence Report: Runs the report based on the date_last field in the event table.

Use Case:

First Occurrence Report (date_active)

- When to use:
  - When you need to identify when an event or incident was first detected in the system.
  - Useful for analyzing root causes and understanding when a specific type of event or incident started appearing.
  - Helps in tracking new or emerging issues and assessing how long they persist in the system before resolution.

Last Occurrence Report (date_last)

- When to use:
  - When you want to analyze the most recent instance of an event or incident.
  - Helps in identifying ongoing or recurring issues that require immediate attention.
  - Useful for tracking how frequently an event occurs and whether it has been resolved or is still active.

Summary

- Use the First Occurrence Report to investigate when a problem initially appeared in the system.
- Use the Last Occurrence Report to track the latest instance of the event, helping in active issue resolution and trend analysis.

4. Event Policy Report.

This report generates a list of existing event policies, their settings and their statuses.

Use Case:

- If you need to **review existing event policies** and their configurations.
- When planning for **policy optimization**, ensuring that event rules are correctly set up and aligned with operational needs.
- To **audit and troubleshoot** event policies, identifying outdated, misconfigured, or redundant policies.

5. Number of Cleared Events/Incidents per Device per Organization.

The purpose of this report is to provide detailed insights into the total number of cleared events or incidents for each device within an organization over a selected time span. Below is a snapshot of this report:

Device Name	Number of the Events	Organization Name
System	2668	System
Study	1626	Organization 1
172.16.232.194	343	Organization 1
172.16.232.43	232	Organization 1
172.16.232.66	141	Organization 1
172.16.232.141	134	Organization 1
172.16.232.159	134	Organization 1
172.16.232.72	134	Organization 1
adfs.home.local	134	Organization 1
Srv-ex01.home.local	134	Organization 1
CentreAP	131	Organization 1
SRV01.home.local	131	Organization 1
srv01	90	Organization 1
Meraki Root	70	Cloud X

Use Cases:

- **Noise Management & Optimization:** If you want to manage the volume of noise in your environment and identify the noisiest devices on your platform, this report is essential. It helps in planning noise reduction strategies and improving incident and problem management.
- **Organizational Event Analysis:** If you need to determine which organization within your platform generates the most events or incidents, this report provides valuable insights. It also assists in calculating the cost to serve for each organization, helping in resource allocation and cost optimization.
- **Device Performance Monitoring:** By analyzing which devices frequently generate incidents, you can identify potential performance issues, faulty hardware, or misconfigurations that may need attention.
- **Capacity Planning & Resource Allocation:** Understanding the volume of cleared events/Incidents per device helps in forecasting resource needs and optimizing system capacity to ensure efficient operations.
- **Compliance & Auditing:** This report can also support compliance efforts by tracking incident resolution trends and ensuring that service-level agreements (SLAs) are met.

6. Active Events/Incidents to Active Device Ratio.

The purpose of this report is to provide insights into the active events/incidents ratio for active devices within each organization. This report is particularly useful when performing event/incident tuning and helps identify which organizations have a higher active events/incidents ratio relative to their active devices.

The goal is to maintain an Active Events/Incidents Ratio ≤ 1, meaning that for every active device, there is at most one event or incident.

- **Ratio > 1** indicates a higher volume of events/incidents per device, leading to increased operational costs and potential system inefficiencies.
- **Ratio < 1** suggests optimized operations, fewer incidents, higher uptime, and better overall efficiency.

Below is a snapshot of the report:

Organization ID	Organization N	Number of Current Active Devices	Number of Active Events	Event Ratio to Active Cis
1	Organization 1	22	50	2.27
4	Cloud X	2	1	0.5
3	ABC company	63	3	0.05
2	Pre-discovery	1	0	0
0	System	0	68	

Use Cases:

- **Event/Incident Volume Management:** Helps teams identify organizations with high event/incident generation and take action to reduce unnecessary noise and improve system stability.
- **Operational Cost Optimization:** By tracking event-to-device ratios, organizations can assess the cost to serve and make data-driven decisions to improve operational efficiency.
- **Service Reliability & Uptime Monitoring:** A lower ratio indicates higher system uptime and stability, allowing teams to proactively address issues before they impact performance.
- **Capacity Planning & Infrastructure Scaling:** Helps forecast resource needs by analyzing event trends per active device, ensuring scalable and cost-effective operations.
- **Automation & Incident Reduction Strategies:** Organizations can use this report to fine-tune automation rules, optimize alert thresholds, and reduce unnecessary incidents through better event correlation.

7. Cleared Events/Incidents to Active Device Ratio.

The Cleared Events/Incidents to Active Device Ratio report provides insights into the number of cleared events or incidents relative to the total number of active devices within each organization. This metric helps assess how effectively incidents and events are being resolved and whether organizations are successfully managing and mitigating system noise, operational inefficiencies, and recurring issues.

A well-balanced ratio ensures that incident resolution keeps pace with the volume of active devices, contributing to operational stability.

- **Ratio > 1** indicates higher noise levels, meaning that more events/incidents are being cleared relative to the number of active devices. This suggests excessive event generation, which may require event filtering, suppression, or better incident tuning to reduce operational overhead.
- **Ratio ≤ 1** suggests less noise and a more optimized environment, where event generation and resolution are balanced, leading to higher system efficiency, fewer distractions, and better operational performance.

This report is useful for identifying organizations with **high event noise** and helps implement strategies to optimize event resolution, improve efficiency, and reduce unnecessary alerts.

Use Cases:

1. **Event Noise Reduction & Optimization.** Helps identify organizations generating excessive event/incident noise that could overwhelm incident response teams. It Enables teams to fine-tune alerting thresholds, suppression rules, and event correlation to minimize unnecessary alerts.
2. **Incident Management & Operational Efficiency.** Ensures that events/incidents are being resolved at a pace that aligns with system demands. A low ratio (≤1) suggests effective incident management, while a high ratio (>1) may indicate unnecessary operational noise.
3. **IT Operations & Monitoring Strategy Improvement.** If an organization has a consistently high cleared event ratio, it may signal too many low-priority or redundant alerts, requiring changes in alerting policies and automation strategies. Also, it helps to evaluate monitoring effectiveness and adjust configurations to reduce distractions from non-critical alerts.
4. **Cost Optimization & Resource Allocation.** A high cleared event ratio suggests increased operational costs due to excessive event resolution efforts. It helps organizations determine where to reduce unnecessary event resolution workload and focus resources on more critical issues.
5. **System Stability & Proactive Maintenance.** By reducing event noise, organizations can improve system reliability, reduce downtime risks, and increase efficiency. It also helps pinpoint recurring issues that need root-cause analysis and long-term fixes rather than repeated short-term resolutions.

8. Event Suppression Report.

The Event Suppression report provides insights about suppressed events on Devices or Device Groups. This Report helps to identify which events are suppressed across the platform.

Use Cases:

- **Audit the Event Policies.** Helps to identify which events are suppressed across the platform to make sure no un-necessary suppression applied to devices/device groups to mitigate unwanted outages due to suppressed events.

Sample output for suppressed events for device groups:

Events Suppression report — Date:04/28/2025

Device Group Name ID	Device Group Name	IP Address	Event Policy Name	Event ID	Severity	Modified BY	Modified Date
48	ABC - Router Group1		Poller: Availability Check Failed	1205	Critical	em7admin	2-11-11 15:22:23
11	Home-PC		Support: Appliance Validation Not Mor	2561	Major	em7admin	5-04-28 03:27:26
49	ABC - Router Group2		Support: Appliance Validation Not Mor	2561	Major	em7admin	5-04-28 03:27:26
82	SL1: Linux Servers		Support: Appliance Validation Not Mor	2561	Major	em7admin	5-04-28 03:27:26

Sample output for suppressed events for device

Events Suppression report — Date:04/28/2025

Device Name ID	Device Name	IP Address	Event Policy Name	Event ID	Severity	Modified BY	Modified Date
555	adfs.home.local	172.16.232.144	Poller: Availability Check Failed	1205	Critical	em7admin	3-10-04 05:37:50
18	mail.mylabs.au	172.16.232.195	Support: Appliance Validation Not Mor	2561	Major	em7admin	4-05-14 11:20:22
18	mail.mylabs.au	172.16.232.195	Support: Appliance Validation Minimur	2563	Major	em7admin	4-05-14 11:20:33

9. Operational Cost & Automation Impact Report (Cost per Device & Organization)

The Operational Cost & Automation Impact report provides a clear view of operational workload and estimated support costs across devices and organizations. It combines alert volumes with configurable cost assumptions to estimate handling effort and highlight the value of automation.

The report helps users understand where operational effort is concentrated, how effectively automation reduces manual work, and which areas present opportunities for optimization.

This report is designed to:

- Identify devices generating the highest operational cost.
- Estimate labor effort associated with alerts.
- Demonstrate the value and impact of automation.
- Distinguish between alert noise and true operational issues.
- Support prioritization of remediation and automation efforts.

Date:02/16/2026
From : UTC 2026-02-16 00:00:00 To : UTC 2026-02-17 00:00:00
Date span is based on column: Last Occurrence

Device Name	Organization	Event Count	Incident Cou	Active Devices	Event Ratio	Incident Rati	Avg. Duration(min	Hourly Rate	Minutes per Event	Minutes per Incident	Minutes saved p	Handling Minute	Handling Cost	EST. Automatio	EST. Automation Sa	Net Cost
[0] System	System	4752	0	3	1584	0	18.14	100	0.5	10	5	2376	3960	0	0	3960
[454] Study.home.local	Organization1	410	0	14	29.2857	0	92.76	100	0.5	10	5	205	341.67	337	2808.33	-2466.67
[1177] trial-message	System	285	0	3	95	0	76	100	0.5	10	5	142.5	237.5	0	0	237.5
[1147] ABC-WA-AP-01	ABC Company	268	0	52	5.1538	0		100	0.5	10	5	134	223.33	0	0	223.33
[558] NSW-VIC-L3-DC	Organization1	268	0	14	19.1429	0		100	0.5	10	5	134	223.33	0	0	223.33
[1188] ABC-SA-AP-01	ABC Company	268	0	52	5.1538	0		100	0.5	10	5	134	223.33	0	0	223.33
[1233] SRV-DC02.mylabs.au	Organization1	268	0	14	19.1429	0		100	0.5	10	5	134	223.33	0	0	223.33
[76] Meraki Root	Cloud X	268	0	1	268	0		100	0.5	10	5	134	223.33	0	0	223.33
[1181] HomeFW01	Organization1	268	0	14	19.1429	0		100	0.5	10	5	134	223.33	0	0	223.33
[1232] SRV-DC01.mylabs.au	Organization1	268	0	14	19.1429	0		100	0.5	10	5	134	223.33	0	0	223.33

Run Quick Report: [Operational Cost & Automation Impact, version 1]

Organizations
All Organizations
Organizations
ABC Company
Cloud X
INBAN
Organization1
System

Report Span
Daily
Weekly
Monthly
Starting
This month
2026 / Feb / 1
Duration
1 month

Select The Severity
Critical
Major
Minor
Notice
Healthy

Date span based on:
Select the date type
Last Occurence
Date Active
Date Delete

Events/Incidents
Select the Type
Event
Incident
Both

Cost Assumption Window
Hourly Rate
100
Minutes per Event
0.5
Minutes per Incident
10
Minutes Saved per Automation run
0

Output Control
Top N Devices
10

Sort By:
Estimated Cost

Use Cases

- **Operational Optimization**

  Identify devices or environments generating excessive alerts relative to their size.

- **Automation Value Demonstration**

  Show estimated cost savings achieved through automation.

- **Executive Reporting**

  Provide a high-level operational cost overview for service owners and leadership.

- **Prioritization of Remediation**

  Highlight devices with high incident ratios or long durations that indicate real service impact.

Report Summary

For each device within an organization, the report shows:

- Event and incident volumes
- Number of active devices for context
- Ratios indicating operational noise vs impact
- Estimated manual handling effort and cost
- Estimated automation savings
- Net operational cost after automation

Field Explanations

- ### Organization

The organization to which the device belongs.

Device Name

The device generating alerts, shown as [Device ID] Device Name for clarity.

- ### Event Count

Total number of events generated by the device during the selected time period.

What it means:
Frequent events may indicate alert noise or unstable conditions.

- ### Incident Count

Total number of incidents generated by the device during the selected time period.

What it means:
Incidents represent alerts that required escalation or ticket creation.

- ## Active Devices in Organization

  Number of active devices within the organization.

  What it means:
  Provides context for comparing alert volumes across organizations of different sizes.

- ## Event Ratio

  Shows how many events this device generates relative to the number of active devices in the organization.

  How it is calculated:

  Event Count ÷ Active Devices in Organization

  How to interpret:

  - ≤ 1 → healthy alert volume
  - 1 → potential alert noise or misconfiguration

- **Incident Ratio**

  Shows how many incidents this device generates relative to the number of active devices in the organization.

  How it is calculated:

  Incident Count ÷ Active Devices in Organization

  How to interpret:

  - Low → stable environment
  - High → increased operational risk

- **Avg Duration (Minutes)**

  Average time alerts remain active before being cleared.

  What it means:

  - Short duration → transient or self-resolving issues
  - Long duration → potential outages or slow resolution

- **Hourly Rate**

  The estimated hourly cost of operational staff.

  What it means:
  Used to estimate the labor cost of handling alerts.

- **Minutes per Event**

  Estimated time required to manually handle a single event.

- **Minutes per Incident**

  Estimated time required to manually handle a single incident.

- **Minutes Saved per Automation**

  Estimated time saved when automation resolves an alert.

- **Handling Minutes**

  Estimated total manual effort required to handle alerts.

  How it is calculated:

  (Event Count × Minutes per Event) + (Incident Count × Minutes per Incident)

- ### Handling Cost

  Estimated labor cost for handling alerts.

  How it is calculated:

  Handling Minutes ÷ 60 × Hourly Rate

- ### Automation Runs

  Estimated number of times automation handled alerts.

  What it means:
  Represents alerts where automation is configured to respond.

- ### Automation Savings

  Estimated labor cost avoided due to automation.

  How it is calculated:

  Automation Runs × Minutes Saved per Automation ÷ 60 × Hourly Rate

- ### Net Cost

  Estimated operational cost after accounting for automation savings.

  How it is calculated:

  Handling Cost – Automation Savings

  How to interpret:

  - Positive value → manual effort still dominates
  - Zero → automation fully offsets manual effort
  - Negative value → automation saves more effort than estimated manual handling time

How to Use This Report

Use this report to:

- Identify devices that generate the most operational cost
- Evaluate the effectiveness of automation
- Compare operational load across organizations
- Prioritize remediation and automation efforts
- Demonstrate automation value to stakeholders

Dashboard.

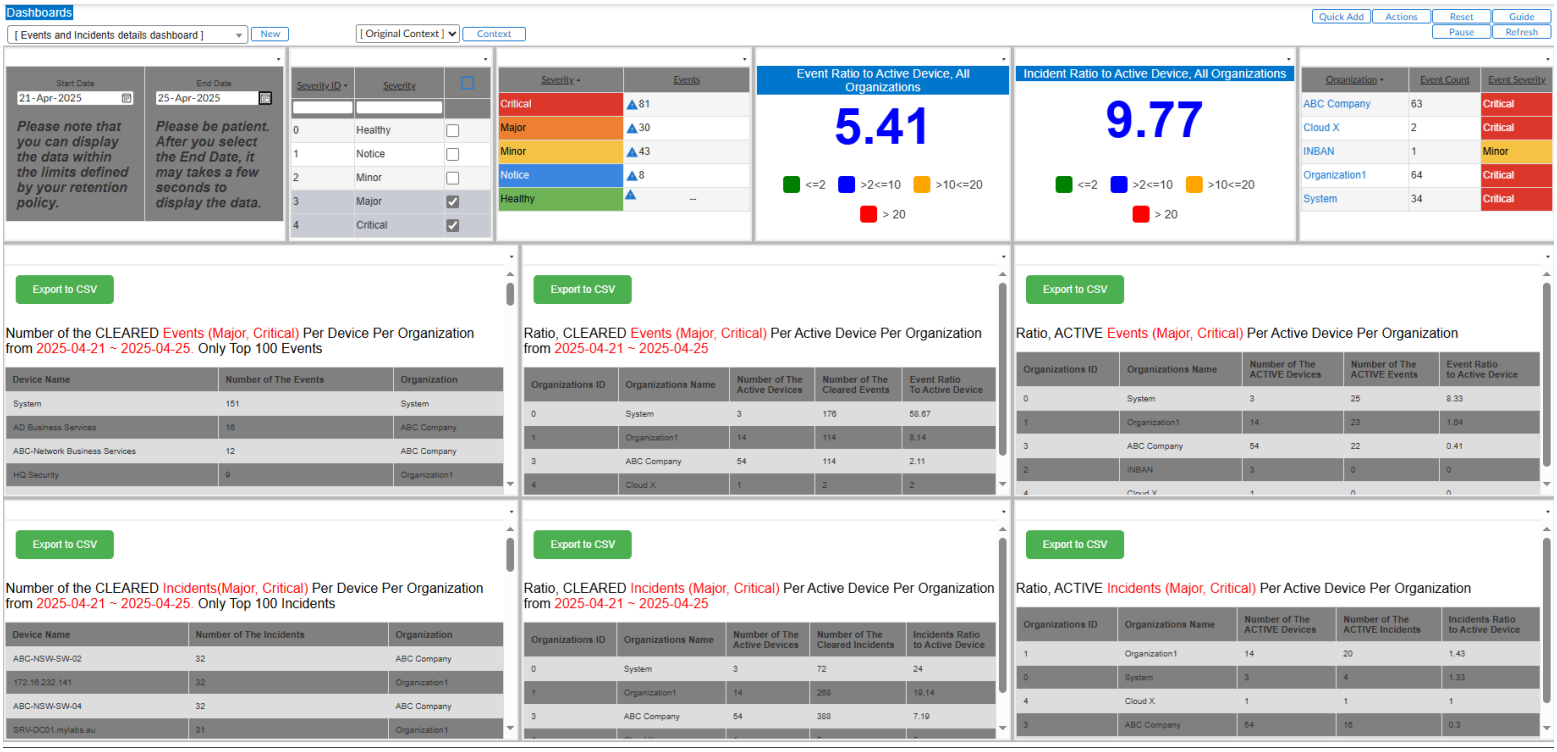
- **Events and Incidents Details Dashboard.**

  The event details report and dashboard, contain a dashboard to show the real-time information for:

  - Event Ratio to Active Device .
  - Incident Ratio to Active Device.
  - Active Events/Incidents ratio to active device.
  - Cleared Events/Incidents ratio to active device.
  - Number of cleared events per device per organization.
  - Number of cleared incidents per device per organization.

  You can export the data of each widget to csv file for further analysis.

  Below is a snapshot of the dashboard:



By leveraging these reports, organizations can gain valuable insights into their event and incident management processes, helping to optimize system performance, reduce noise, and enhance operational efficiency. Whether tracking active event ratios, monitoring cleared incidents, or assessing overall incident resolution effectiveness, these reports serve as essential tools for proactive IT operations, cost optimization, and strategic decision-making.

Regularly analyzing these metrics enables teams to identify trends, mitigate risks, and fine-tune monitoring strategies to ensure a stable, efficient, and cost-effective IT environment. By utilizing the insights provided in these reports, organizations can drive continuous improvement, enhance service reliability, and create a more resilient infrastructure.

For any questions or further assistance in interpreting these reports, please reach out to your dedicated CSM or CSA.