SAFETY4RAILS

Manual for crisis management and coordination of response teams

Deliverable 5.6

Lead Author: Elbit Systems C4I and Cyber Ltd.

Contributors: CuriX, MTRS, LDO

Dissemination level: Public

Security Assessment Control: passed

The project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883532.

D5.6 Manual for crisis management and coordination of response teams

Deliverable number:	D5.6	
Version:	1.2	
Delivery date:	13/12/2022	
Dissemination level:	Public	
Nature:	Report	
Main author(s)	Eli Ben Yizhak Ido Peled	Elbit Systems Otorio (Elbit's business partner)
Contributor(s)	Uli Siebold Gilad Rafaeli	CuriX MTRS
Internal reviewer(s)	Corinna Köpke Stephen Crabbe Atta Badii Uli Siebold Andreas Georgakopopoulos Antonio De Santiago Laporte	Fraunhofer Fraunhofer UREAD CuriX WINGS MDM
External reviewer(s)	Andre Samberg	

Document control

Version	Date	Author(s)	Change(s)
0.1	23/12/2021	Ido Peled	Preliminary
0.2	24/02/2022	Ido Peled	First release
0.3	21/03/2022	Eli Ben-Yizhak, Ido Peled	S4RIS format
0.5	14/06/2022	Eli Ben-Yizhak	Implement comments
0.6	17/06/2022	Eli Ben-Yizhak	Implement comments
1.0	17/06/2022	Stephen Crabbe	Creation of 1.0 from V0.6 and minor updates. Project coordinator decision on Security Assessment Control. (Some internal and external reviews for process, any further feedback into future work).
1.2	13/12/2022	Eli Ben-Yizhak	Railway assets reference (par. 4)

DISCLAIMER AND COPYRIGHT

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the views of its authors. Neither the authors nor the Research Executive Agency nor the European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

No part of this document may be copied, reproduced, disclosed, or distributed by any means whatsoever, including electronic without the express permission of the SAFETY4RAILS project Partners. The same applies to translation, adaptation or transformation, arrangement or reproduction by any method or procedure whatsoever.

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: **Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS**. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming even more important means of transportation given the need to address climate change. However, being such critical infrastructures turns metro and railway operators as well as related intermodal transport operators into attractive targets for cyber and/or physical attacks.**The SAFETY4RAILS project delivers methods and systems to increase the safety and recovery of track-based inter-city railway and intra-city metro transportation.** It addresses both cyber-only attacks (such as impact from WannaCry infections), physical-only attacks (such as the Madrid commuter trains bombing in 2004) and combined cyber-physical attacks, which an important emerging scenarios are given increasing IoT infrastructure integration.

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security, e.g. carry out a threat analysis, maintain situation awareness, establish crisis communication and response, and they have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENTS

Executive summary

This document is deliverable D5.6, led by Elbit Systems.

The S4RIS crisis management tools set, described at D5.5, aggregates the alerts received from all relevant S4RIS monitoring tools, to generate relevant insights and mitigation procedures for the railway operator and for the coordination of its response teams.

D5.6 document describes the User Manual of SAFETY4RAILS Decision Support System – RAM^2

The document outlines system features and interfaces, used by Elbit Systems to collaborate with S4RIS monitoring tools to produce relevant insights for the Operator, to address the Cyber and Cyber-Physical events for each scenario.

Elbit System used Otorio RAM^2 as a general Decision Support tool, and performed the design and modifications of its interfaces and infrastructure, to receive, fuse and analyse structured & unstructured data of various sensors and monitoring tools, to support the required modes of operation and demonstrated scenarios, performed by SAFETY4RAILS' consortium at different sites – Madrid, Ankara, Rome and Milan (Demonstration in Milan to follow after the scheduled closure date of this deliverable).

The content of this document is based on RAM^2 original user manual and it has been updated/revised to reflect the specifics and developments for SAFETY4RAILS

Since RAM^2 system supports divers use-case scenarios, some of the content of this manual may include different components, not directly related to railways.
Otorio is Elbit's business partner. The information included in this manual has copyrights by Otorio.

1. Introduction

1.1 Overview

Elbit Systems has chosen RAM^2, Otorio's Risk Assessment Monitoring & Management platform, for S4RIS Decision Support Platform. RAM^2 is an industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. It offers a comprehensive, centralized, and automated industrial cyber risk management solution. The content of this document is based on RAM^2 original user manual and it has been updated/revised to reflect the specifics and developments for SAFETY4RAILS

The platform easily tracks a variety of production floor data sources (e.g. OT, IT, security logs and network data) and provides actionable views of site assets and alerts, based on powerful machine analytics. Business Information Security Officers (BISO) and operations engineers can use the customized dashboard to more effectively carry out day-to-day tasks.

RAM^2 allows users to do the following:

- Manage all railway operator assets across multiple sites, through an easily navigable hierarchical structure
- Associate assets to Sub-units and Sub-units to stations.
- Collect information about operator physical assets, including critical changes that are happening
- Perform intelligent risk prioritization to better handle site threats: calculate the risk level for each asset, Sub-unit, and station based on the vulnerabilities discovered in the assets, and categorize impact levels
- Automatically generate alerts when abnormal events and vulnerabilities are found in assets
- Easily view KPIs and detailed information about the site network and its components

2. Terminology

2.1 Site Management

The RAM^2 system manages security for assets in the operational network.

It enables contextualization of the data by dividing the monitored network hierarchically into the following entities:

Site – a single business or industrial unit, that is monitored by a dedicated central Management appliance, and can be divided into multiple operational processes.

Operational units - default values are Station for the first level & Sub-unit for the second level:

- **Station** – an operational unit in which specific functional activities are performed.
- **Sub-unit** – an operational unit within a station that groups several machines and assets to perform a specific set of operational tasks.

Asset – a single endpoint machine or device that has at least one MAC or IP address within the monitored network. Information about assets in the assessed environment is received from different data sources to build the asset inventory. This inventory is updated based on one-off, periodic or continuous monitoring. The information includes details about technical, operational, and intelligence attributes. The central management server alerts users about newly discovered assets for the purposes of investigation and assignment to relevant units.

2.2 Risk Assessment

Risk level is calculated bottom up for each operational unit, meaning from the single asset to the whole network level. Risk is assessed based on the asset attributes, its behavior, relation to other assets and processes, network activities, and security posture, as well as identified vulnerabilities. Risk is aggregated based on the organizational hierarchy. This enables an effective drill down from the top level to the root cause, focused on the most critical areas of operations. The risk calculation takes into account the probability of attack, the severity of the attack, and the potential consequences and disturbance to the operational processes.

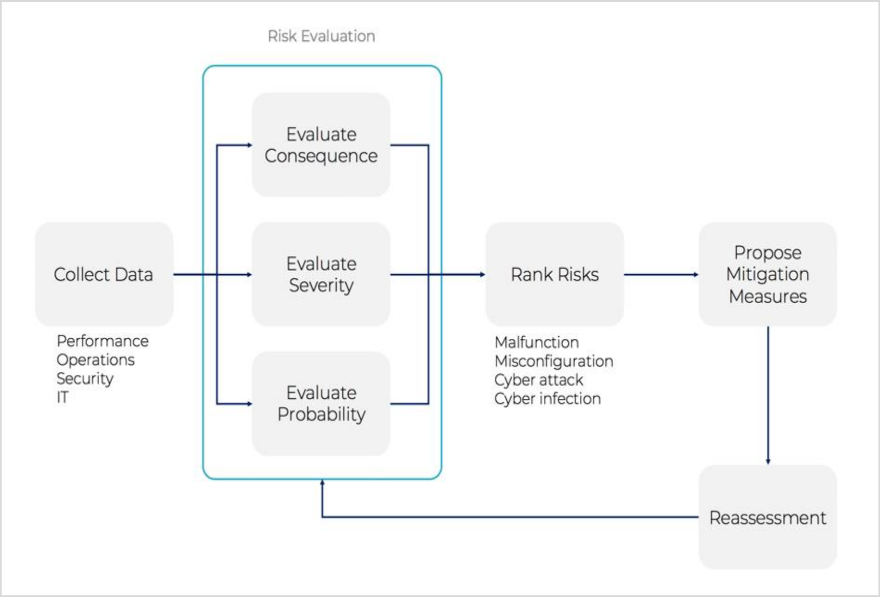


FIGURE 1: DIGITAL RISK ASSESSMENT PROCESS

2.3 Alerts

RAM^2 generates alerts automatically for security and operational issues it discovers. Each alert indicates the severity of the issue, as well as its details (such as the specific vulnerability for the issue). Alerts usually relate to a single event from a data source, and the affected asset characteristics.

Monitored events which have not reached a minimal severity threshold or do not bear a risk on their own are treated by the system as Invisible alerts that are not exposed to the user, in order to reduce the level of noise and false positive alerts. However, they are considered by the security engines' algorithms for the detection of suspicious patterns. These alerts may become visible and displayed as part of an insight if their threat severity increases or when correlated with additional alerts to identify a greater risk.

2.4 Insights

Alerts, vulnerabilities, asset details, operational data, security posture and other types of data are collected and monitored to detect suspicious patterns and needed configuration changes, which are presented to users as Insights. The goal of insights is to group together issues that are part of a bigger story, so that they can be investigated together within the same context.

Insights are a way for users to see the relationship between independent data points that might not be of interest on their own. By grouping multiple vulnerabilities and threats together, users can have a better view and understanding of the big picture. The insights connect the dots between events and data from multiple data sources, and assist in ensuring the environment is secure.

2.5 Vulnerabilities

Given S4RIS assets inventory details, reported by SecuRail, risk level for an asset is assessed using a list of publicly known vulnerabilities (CVE) compiled by the OTORIO threat intelligence research team or by S4RIS monitoring tools. The CVE is based on published open source vulnerabilities, industrial best practices, and other industry sources.

Users can view the list of vulnerabilities, and filter views and alerts according to specific vulnerabilities. Users have the capability of disabling specific vulnerabilities, in which case, alerts will not be generated for them. By default, all the vulnerabilities are active.

3. Getting Started

3.1 Login to the system

Connect to the system central management from a browser, with the URL for your central management server.

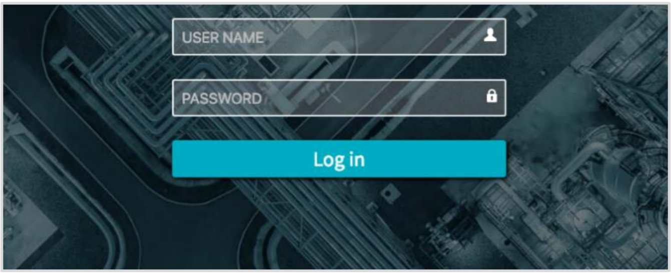


Figure 2 Login screen

Enter user name and password.

Once logged in, the Dashboard view will open.

3.1.1 Getting Started Overview

Upon initial login, there is no definition for the operational hierarchy. If assets have been discovered, they will appear on the list of Unassigned Assets.

Once assets are discovered, any risks that are discovered will be presented through the dashboard. Users can view and manage alerts and insights for assets, open cases for follow up, and get required information for risk mitigation.

3.2 The Central Management Main Dashboard

The Dashboard view provides a snapshot of risk status, top threats and issues that require attention. The dashboard is interactive and can be displayed for each of the operational levels and processes within the organization, allowing users to easily and immediately drill down from a site overview to the single alert level. It allows users to focus on the areas which are at greatest risk, for efficient investigation and mitigation.

3.2.1 Hierarchy navigation menu

The left navigation menu in the dashboard screen shows the organizational structure from corporate level to the Sub-unit level. When users click on a specific item in the menu, the dashboard is updated to present the information relating to that operational process.

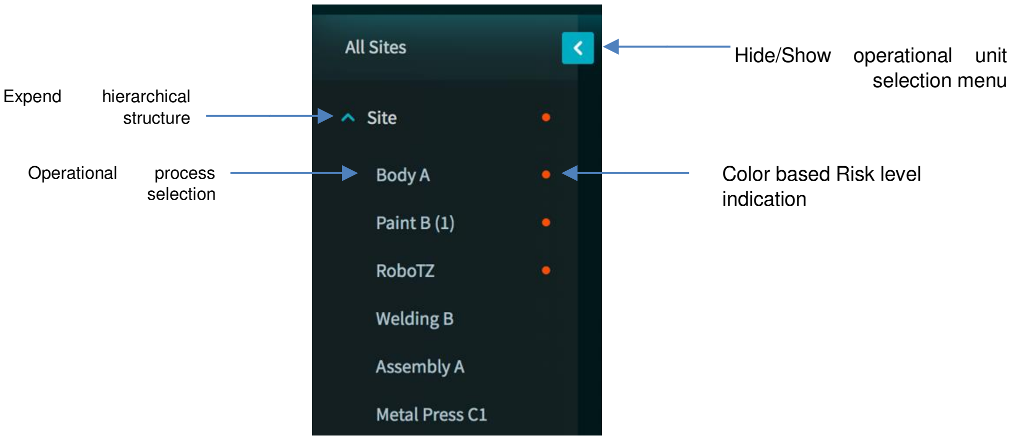

All Sites
Site
Body A
Paint B (1)
RoboTZ
Welding B
Assembly A
Metal Press C1
Expend hierarchical structure
Operational process selection
Hide/Show operational unit selection menu
Color based Risk level indication

Figure 3 Dashboard left navigation menu

Any operational process that is at risk will have a color-based indicator next to its name. The color of the dot reflects the risk level. The risk is aggregated within the organizational hierarchy, so the risk to a station will be affected by the risk of the Sub-units and assets under it.

3.2.2 Top Risk KPIs

Three main KPIs are displayed in the center area of the dashboard:

- **Risk Level –** Shows the overall risk level of the selected operational unit in two dimensions. The donut chart reflects the risk level state out of 100%, while the color reflects predefined risk levels: Critical, High, Medium, and Low.
- **Alerts –** number of alerts that are currently open for the selected operational unit. The donut chart reflects the distribution of alerts by severity.
- **Affected Assets –** number of assets with open alerts or insights, compared to the total number of assets identified in the system under the selected operational unit. The donut chart reflects the relative amount of affected assets out of the total number of assets under the operational unit in view.

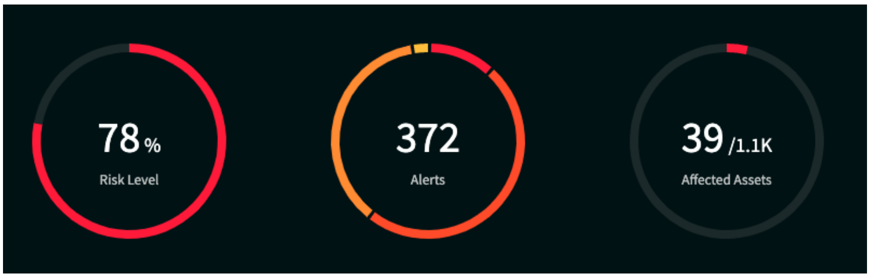


Figure 4 Dashboard view

3.2.3 Risk over time

The risk over time graph shows risk trends as they change over time. Select the timeframe for display (Last 7 days, Last 30 days or Last 90 days). Ideally, the general trend should show a reduction of the risk. When digital risk is under control and at an acceptable level, it means best practices are being implemented to improve the security posture. But your investment is also proportional to your operational investment and the business risk you would like to take.

When trends change, users can drill down through to understand the reason for the change. By drilling down to the Sub-unit and asset level, users can see the main contributor to the change in risk level, and the steps that should be taken to reduce and remove the risk.

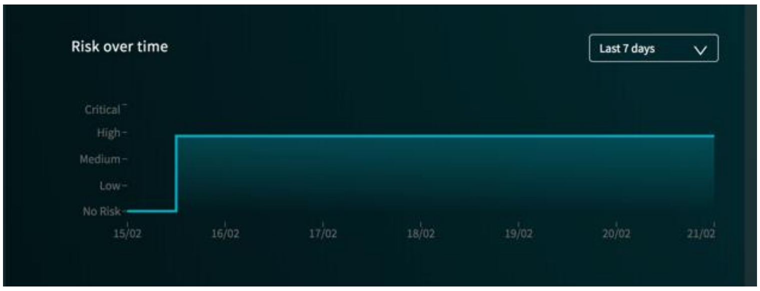


Figure 5 Risk over time

3.2.4 Details tabs

The right side of the dashboard contains several tabs that provide access to the risk breakdown and enable immediate drill down for investigation. These tabs are Station/Sub-unit (changes based on user navigation), Risk, Insights, Alerts, and Cases.

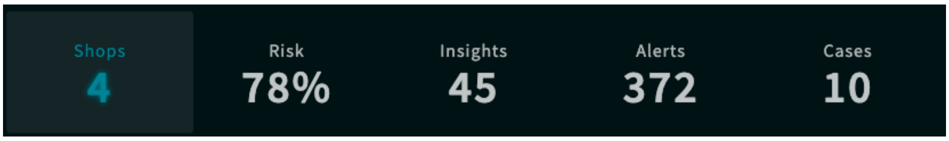


Figure 6 Details tabs

3.2.5 Operational Units Tab

The first table displays the top KPIs of the operational units under the selected operational level:

When the dashboard displays the site level, the tab title will be “Stations”, and it will include the list of stations within the site. When the dashboard displays one of the stations, the tab title will be “Sub-units”, and it will include the list of Sub-units within the selected station.

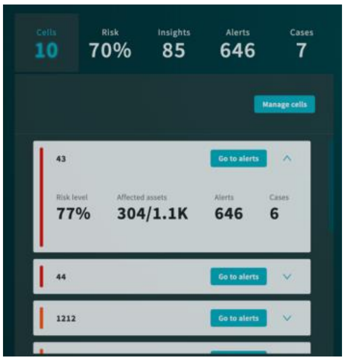


Figure 7 Sub-units tab under a selected operational unit

The operational units under this tab are sorted by risk level, so you can focus on units with higher severity first. For each Sub-unit or Stations in this tab the following

KPIs are displayed: Risk Level, affected assets, Alerts and number of open cases which are related to the operational unit - to be described below).

Click the “Go to alerts” button to drill down directly to the open alerts for the selected unit. The “Manage Sub-units” or “Manage stations” button will take you to the railway stations management screen, where you can create new operational units or update existing ones in the logical structure parallel to your actual operational structure.

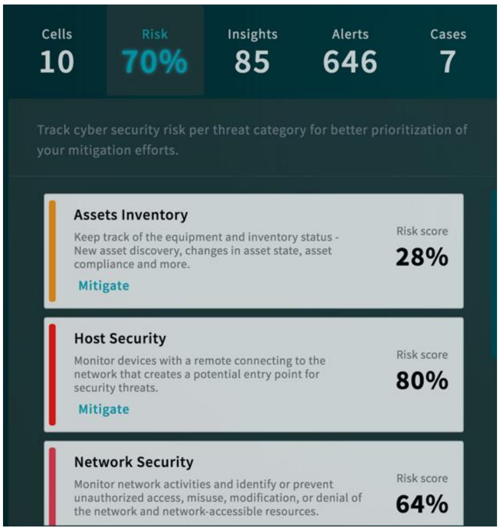
When the dashboard is set to display the Site level, the Stations tab will show the amount of unassigned assets compared to the total discovered assets. Assigning assets to operational units is important for proper asset inventory and visibility, and it is necessary for correct analysis of risk, generation of mitigation steps and detection of anomalies. Once all assets are assigned to operational processes, discovery of unassigned assets can be the result of a planned activity that should be acknowledged in the central management, or an indicator for a breach that should be handled immediately.

3.2.6 Risk tab

The Risk tab summarizes the sources of digital risk by threat categories. A risk level is calculated separately for each of the categories to provide a better understanding of the areas that require more attention.

The threat categories in this tab are: Assets Inventory, Host Security, Network Security, User Privileges and Behavior, Vulnerability Management and Threat Intelligence, and Remote Connection Activities. The threat categories add an additional dimension for investigation that must be taken into account to ensure improvement in all aspects of the security posture.

Click the “Mitigate” button on each category to go directly to the issues contributing to the risk level.



Track cyber security risk per threat category for better prioritization of your mitigation efforts.

Assets Inventory

Keep track of the equipment and inventory status - New asset discovery, changes in asset state, asset compliance and more.

Risk score 28%

Host Security

Monitor devices with a remote connecting to the network that creates a potential entry point for security threats.

Risk score 80%

Network Security

Monitor network activities and identify or prevent unauthorized access, misuse, modification, or denial of the network and network-accessible resources.

Risk score 64%

Figure 8 Risk tab in the dashboard – Threat categories

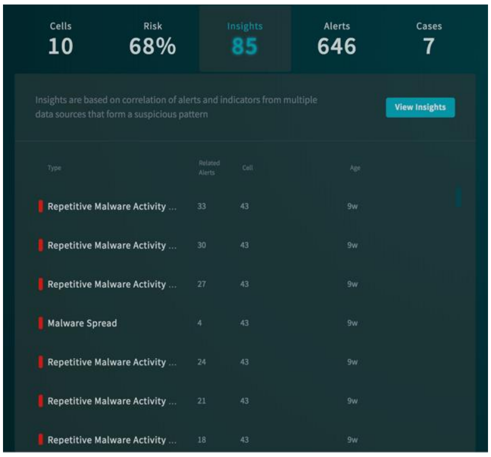
3.2.7 Insights tab

Insights are a combination of visible alerts and invisible alerts that the solution has tagged for additional investigation. Individually, these alerts may not seem to pose a threat, but when viewed as a group they require further investigation

The Insights tab contains the most critical insights related to the operational unit on display. Insights correlate groups of alerts that together pose a risk to operational continuity.

Each insight allows users to drill down to the details for a deeper investigation. This tab provides quick access to a prioritized list of insights. The insights act as an "Analyst in a box," empowering users to take action and reduce the mean time to repair (MTTR).

Click the "View insights" button to view the full list of insights. It will be filtered to the selected operational unit currently on display.



Insights are based on correlation of alerts and indicators from multiple data sources that form a suspicious pattern

Type	Related Alerts	Cell	Age
Repetitive Malware Activity ...	33	43	9w
Repetitive Malware Activity ...	30	43	9w
Repetitive Malware Activity ...	27	43	9w
Malware Spread	4	43	9w
Repetitive Malware Activity ...	24	43	9w
Repetitive Malware Activity ...	21	43	9w
Repetitive Malware Activity ...	18	43	9w

Figure 9 Insights tab in the dashboard

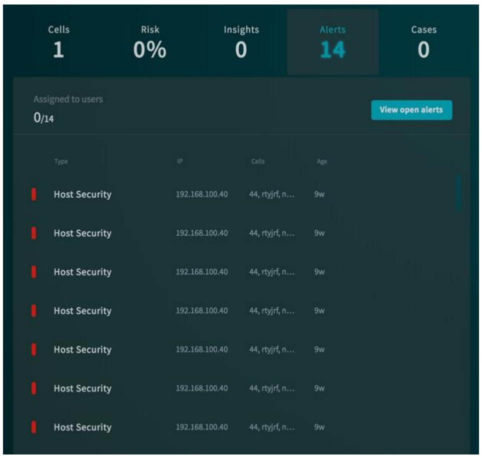
3.2.8 Alerts tab

Alerts are individual warnings that may require attention. They can be part of a larger insight, or stand alone. While insights should be reviewed first, the Alerts tab contains warnings for the operational unit on display.

The alerts tab lists the alerts that are currently active. They are color-coded and sorted by risk level and operational impact. It also shows the number of alerts that have been assigned to users to investigate, the Sub-units involved in the alert, and the age of the alert.

Users can drill down through each alert to see the details by clicking the "Go to Alert" button. Alerts that are unassigned or ones that have a high age expose the operation to a higher risk of disturbance to operational continuity.

The "View Open Alerts" button shows users the full list of alerts that are relevant to the selected operational unit.



Cells 1 | Risk 0% | Insights 0 | Alerts 14 | Cases 0

Assigned to users
0/14

	Type	IP	Cells	Age
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w
🟥	Host Security	192.168.100.40	44, rtyjrf, n...	9w

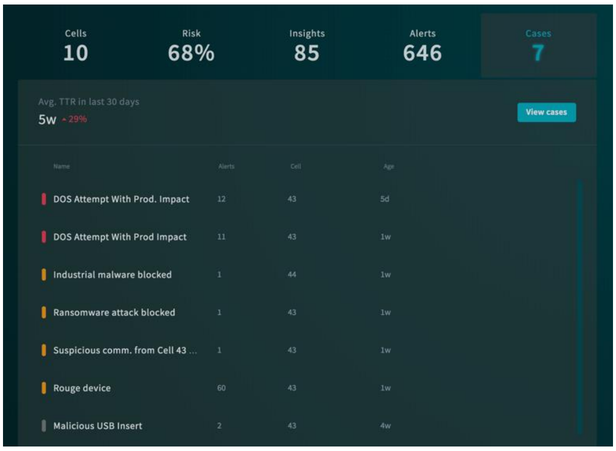
Figure 10 Alerts tab in the dashboard

3.2.9 Cases tab

Cases are insights, alerts or other vulnerabilities that have been assigned for investigation and resolution. They can be shared among different users, and handled by different stakeholders within the organization. The case management helps manage the communication both within the operational team and across units, allowing IT and cyber analyst involvement.

The Cases tab lists active cases. They are color-coded by severity and risk level. Users can drill down to see details of each case. The tab also shows the average time to resolution (TTR) for cases, providing a usable KPI for reporting purposes and allowing teams to estimate the required resources.

Click the “View Cases” button to see the full list of cases that are relevant to the selected operational unit.



Cells 10 | Risk 68% | Insights 85 | Alerts 646 | Cases 7

Avg. TTR in last 30 days
5w ▲29%

	Name	Alerts	Cell	Age
🟥	DOS Attempt With Prod. Impact	12	43	5d
🟥	DOS Attempt With Prod Impact	11	43	1w
🟧	Industrial malware blocked	1	44	1w
🟧	Ransomware attack blocked	1	43	1w
🟧	Suspicious comm. from Cell 43 ...	1	43	1w
🟧	Rouge device	60	43	1w
▮	Malicious USB Insert	2	43	4w

Figure 11 Cases tab in the dashboard

3.2.10 Navigation

The solutions Central Management was designed to allow users to easily navigate throughout the system. As mentioned earlier in this section, users can navigate through different stations, Sub-units and assets using the navigation menu on the left side of the screen. They can drill down into insights, alerts, and other elements using the tabs on the right side of the screen.

Additionally, users can navigate to any location at any time using the top navigation menu.

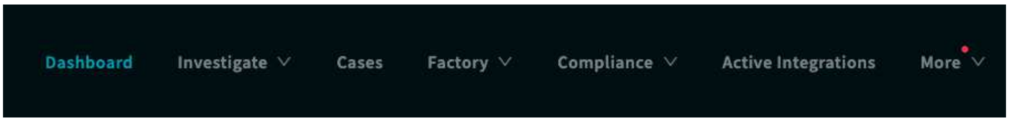


Figure 12 Top navigation menu of the application

- **Dashboard –** View overall system health, or drill down into individual stations, Sub-units, and assets
- **Investigate –** View the Alerts & Insights page or the Vulnerabilities page for full listings of risk indicators.
- **Cases –** View open cases.
- **Site –** Manage operational hierarchy and assets.
- **Compliance –** Manage ICS compliance (IEC 62443 & NIST 800-82 questionnaires)
- **Integrations –** Enable security and industrial data sources, and monitor their performance.
- **More –** View and change application settings, user management, troubleshooting and system updates.

4. Site Management

The operational organization is managed by dividing it hierarchically into multiple operational layers. These layers are **Site**, **Stations** and **Sub-units**.

The asset inventory is generated from information that is received from both 3rd party data sources available in the network, active and passive Network monitoring capabilities. Assets must be assigned to operational units at the lowest operational processes layer.

S4RIS relevant assets were managed by RAM^2 with the same operational layers (Site, Stations and Sub-units).

4.1 Site view

The Site hierarchy view allows users to create, modify, and delete operational units. Users can also search for operational units by name, filter them, and see the number of assets that have not been assigned to a unit.

Select *Stations* from the *Site* menu to see the different stations that have been defined. Each station in the system is displayed as a card.

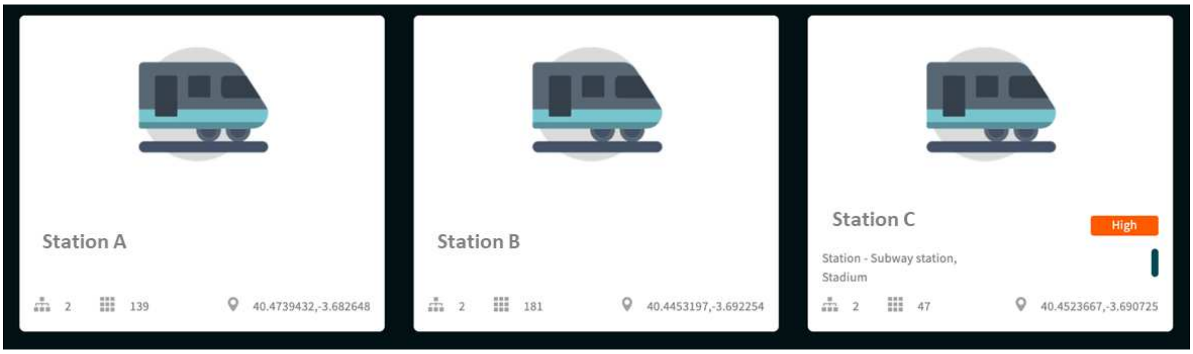


Figure 13 stations

In this view, each card shows the following information for the station:

- Name and description of the station
- Overall risk level (color coded)
- Number of Sub-units
- Number of assets
- Geographic location of the station

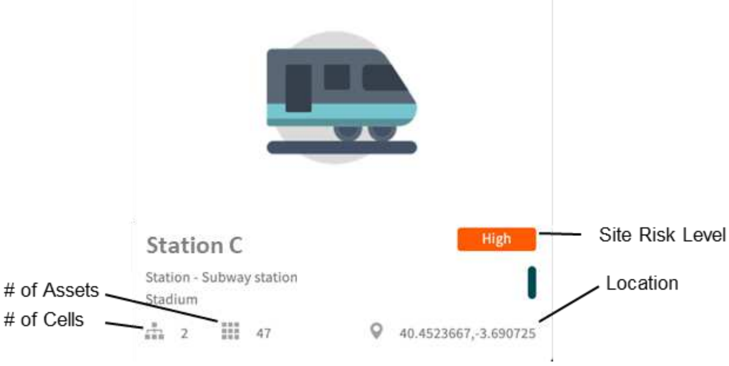
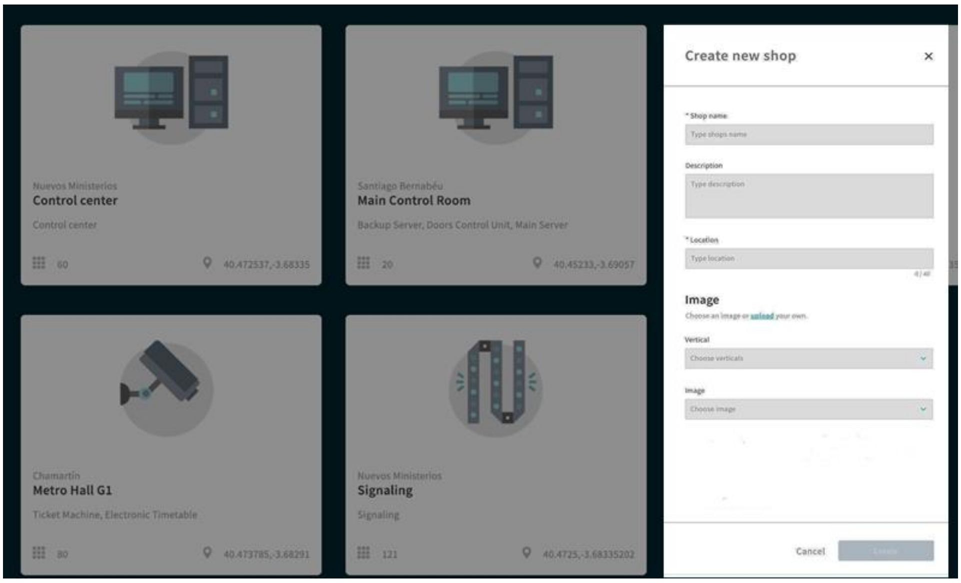


Figure 14 station card

4.1.1 Create a Station

To add a new Station:

1. Select *Station* from the top-level *Site* menu.
2. Click ⊕.
3. In the *Create New Station* panel, enter the following:
   a. **Station name & description** – the name for the station in central management, and a description of it; this is free text
   b. **Location** – the geographic location of the station
   c. **Image** – Choose an Image by vertical or upload your own image



Create new shop ×

* Shop name
Type shops name

Description
Type description

* Location
Type location

Image
Choose an image or upload your own.

Vertical
Choose verticals

Image
Choose image

Figure 15 Create new station

4. Click *Create*

A card for the new station will appear on the page.

4.1.2 Edit a station

To modify details for a station:

1. Open the station view. Hover the mouse over the station card to be modified & click the ⚙.

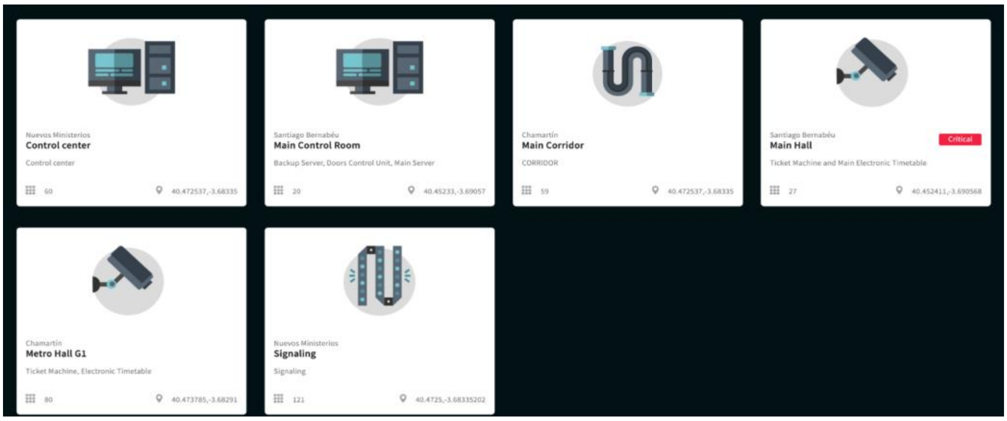
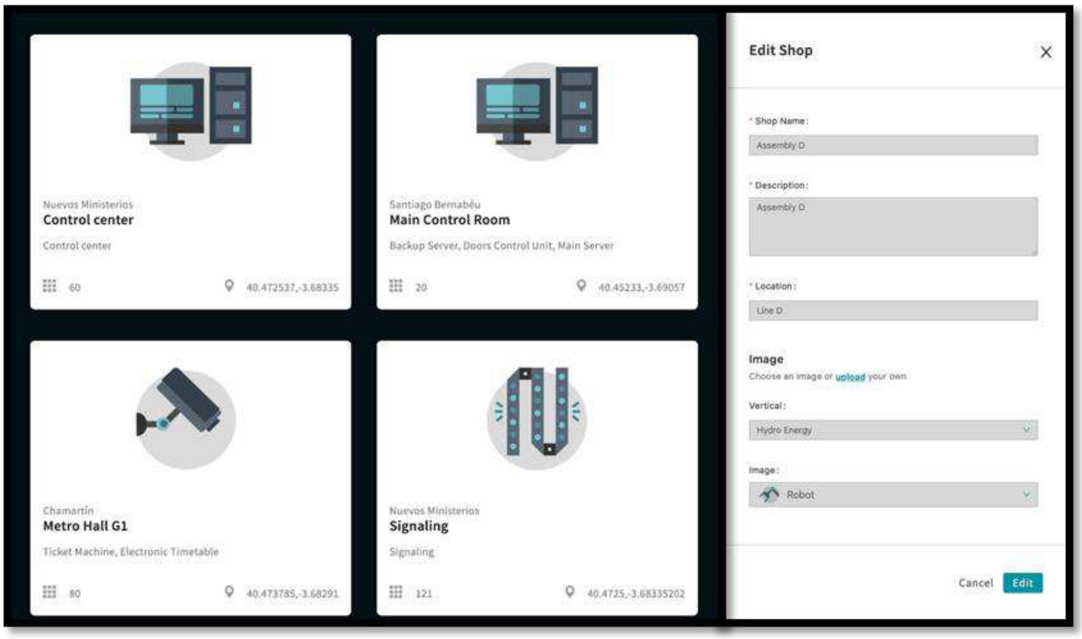


Figure 16 station card – show Station Sub-units

2. In the *Edit station* panel, make changes to the station details as necessary, and then click *Edit* to save.



Edit Shop

* Shop Name: Assembly D

* Description: Assembly D

* Location: Line D

Image

Choose an image or upload your own

Vertical: Hydro Energy

Image: Robot

Figure 17 Edit station

4.1.3 Filter or search for stations

Users can filter or search for specific stations in the station view.

Click ▼ to select the filter for the view. Filter by name or location of the station.

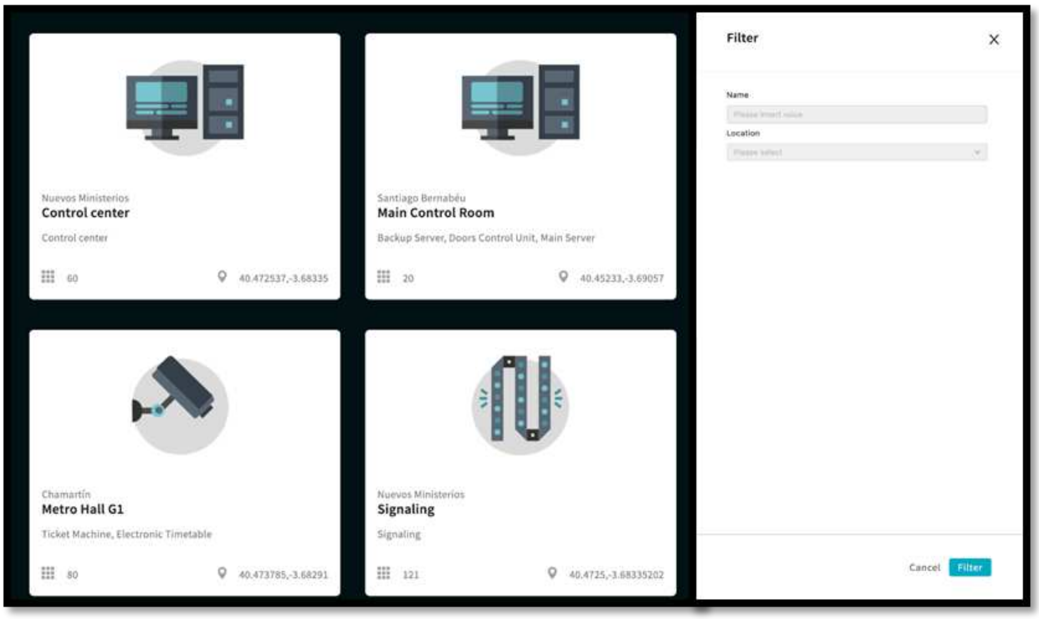


Figure 18 – Filter

Click 🔍 to search for a specific station by name.

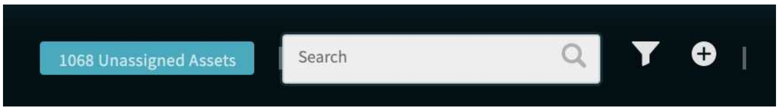


Figure 19 – search field

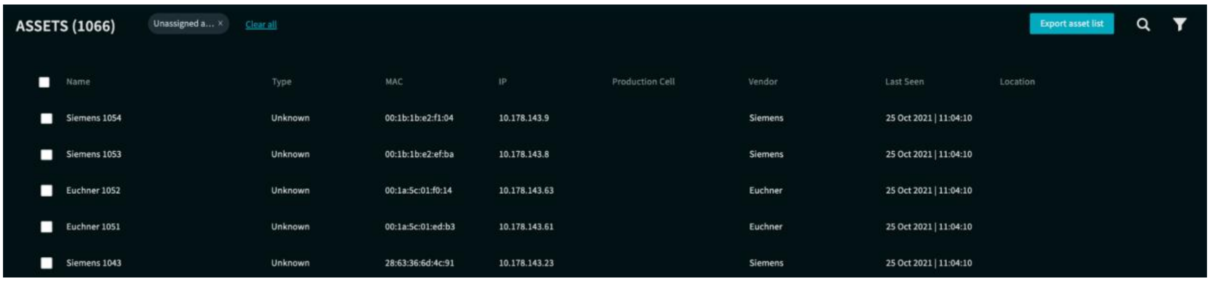
4.1.4 Delete a station

To delete a station, remove all Sub-units that are part of the station (move them to other stations).

Hover mouse over station card, and click 🗑. If there are Sub-units in the station, the station cannot be deleted.

4.1.5 Manage Unassigned Assets

Click 10 Unassigned Assets in the upper right to view a list of Unassigned Assets. From this list users can manage unassigned assets and assign them to Sub-units.



ASSETS (1066) Unassigned a... × Clear all Export asset list

☐	Name	Type	MAC	IP	Production Cell	Vendor	Last Seen	Location
☐	Siemens 1054	Unknown	00:1b:1b:e2:f1:04	10.178.143.9		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens 1053	Unknown	00:1b:1b:e2:ef:ba	10.178.143.8		Siemens	25 Oct 2021 | 11:04:10	
☐	Euchner 1052	Unknown	00:1a:5c:01:f0:14	10.178.143.63		Euchner	25 Oct 2021 | 11:04:10	
☐	Euchner 1051	Unknown	00:1a:5c:01:ed:b3	10.178.143.61		Euchner	25 Oct 2021 | 11:04:10	
☐	Siemens 1043	Unknown	28:63:36:6d:4c:91	10.178.143.23		Siemens	25 Oct 2021 | 11:04:10	

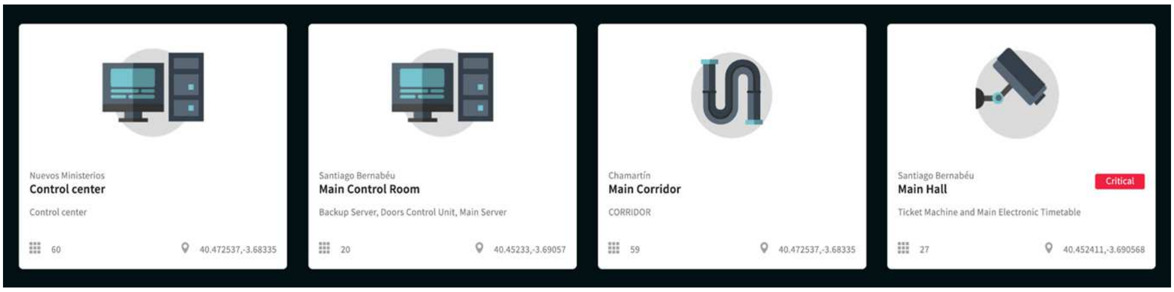
Figure 20 – Unassigned Asset List

4.2 Station Sub-unit

Station Sub-units are entities within stations. Sub-units contain assets. Sub-units can only be assigned to a single station but can have any number of assets assigned to it. Moreover, a single asset can be assigned to different Sub-units as assets may be part of several production units.

4.2.1 Sub-unit view

To navigate to the Sub-units view, either click on the station card to see all the Sub-units within this station, or select *Sub-units* from the top-level *Site* menu to see all the Sub-units in the site.



Nuevos Ministerios
Control center
Control center
60 40.472537,-3.68335

Santiago Bernabéu
Main Control Room
Backup Server, Doors Control Unit, Main Server
20 40.45233,-3.69057

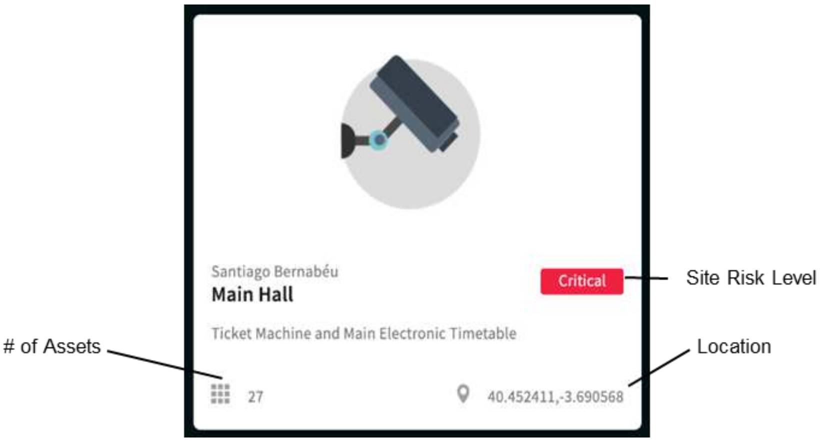
Chamartín
Main Corridor
CORRIDOR
59 40.472537,-3.68335

Santiago Bernabéu
Main Hall Critical
Ticket Machine and Main Electronic Timetable
27 40.452411,-3.690568

Figure 21 Station Sub-units

Sub-units are shown as cards. Each card contains the following information:

- Name and description of the Sub-unit
- Overall risk level (color coded)
- Number of assets
- Station where Sub-unit is located
- Owner of Sub-unit



Santiago Bernabéu
Main Hall
Critical
Ticket Machine and Main Electronic Timetable
27
40.452411,-3.690568

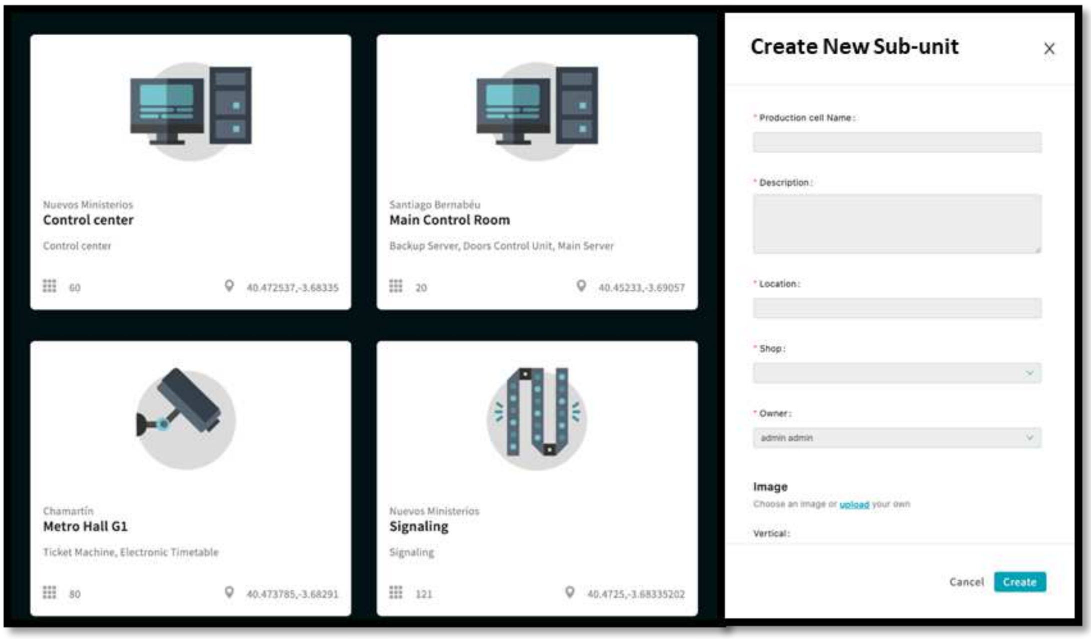
Figure 22 Sub-unit card

4.2.2 Create a Sub-unit

Sub-units can either be created through the Station Sub-units page or through the station page. When created through the Station Sub-units page users must assign the Sub-unit to a station. When created through the station page, the Sub-unit is automatically associated with the station.

To create a Sub-unit from the Station Sub-units page:

1. Select *Station Sub-units* from the top-level *Site* menu. The Sub-unit cards for the site are shown.
2. Click ⊕
3. In the *Create New Station Sub-unit* panel, enter the following details for the Sub-unit:
    a. **Sub-unit name & description** - the name for the Sub-unit and its description; this is free text
    d. **Location** - the geographic location of the Sub-unit
    e. **Station** – the station with which the Sub-unit will be associated (from a list). if the Sub-unit was created directly from a specific station, this field is field automatically
    f. **Image** – Choose an Image by vertical or upload your own image
    g. **Impact level** – (optional) Indicate the impact loss of this Sub-unit would have in the following areas: Financial, Safety, Productivity, Operational, Reputation, Regulatory. Select from *Insignificant, Minor, Moderate, Major,* or *Catastrophic* for each category.



Nuevos Ministerios
Control center
Control center
60 40.472537,-3.68335

Santiago Bernabéu
Main Control Room
Backup Server, Doors Control Unit, Main Server
20 40.45233,-3.69057

Chamartín
Metro Hall G1
Ticket Machine, Electronic Timetable
80 40.473785,-3.68291

Nuevos Ministerios
Signaling
Signaling
121 40.4725,-3.68335202

Create New Sub-unit

* Production cell Name:

* Description:

* Location:

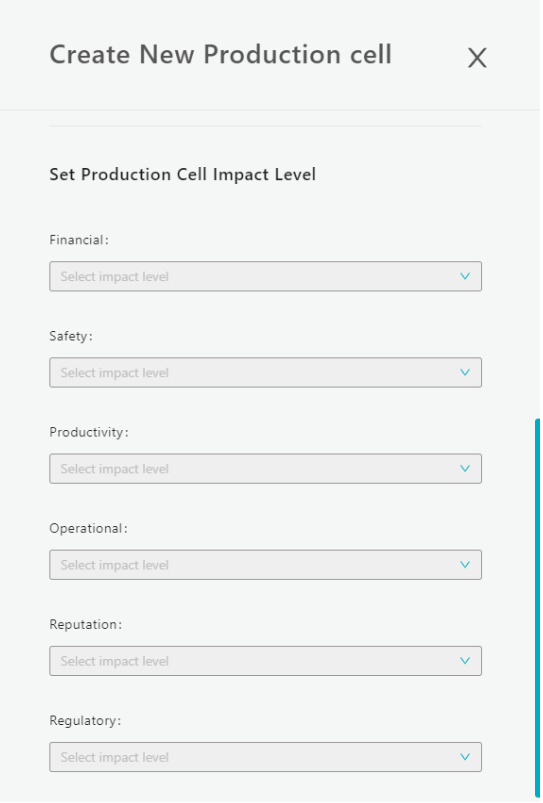
* Shop:

* Owner: admin admin

Image
Choose an image or upload your own

Vertical:

Figure 23 Create New Station Sub-unit



Create New Production cell

Set Production Cell Impact Level

Financial: Select impact level

Safety: Select impact level

Productivity: Select impact level

Operational: Select impact level

Reputation: Select impact level

Regulatory: Select impact level

Figure 24 Sub-unit impact level

4. Click *Create.*

A card for the Sub-unit will appear on the *Station Sub-units* page.

4.2.3 Edit Sub-units

To modify details for a Sub-unit, including station assignment.

1. Select *Station Sub-units* from the top-level *Site* menu.
2. Hover over the Sub-unit to be modified and click ⚙.
3. In the *Edit Station Sub-unit* panel, change details as necessary.
4. Click *Edit* to save the changes.

4.2.4 Filter or search for Sub-units

Users can filter or search for specific Sub-units in the Sub-unit view.

1. Click ▼ in the upper right to filter for Sub-units. Filter by name or location of the Sub-unit.
2. Click 🔍 to search for a specific Sub-unit by name.

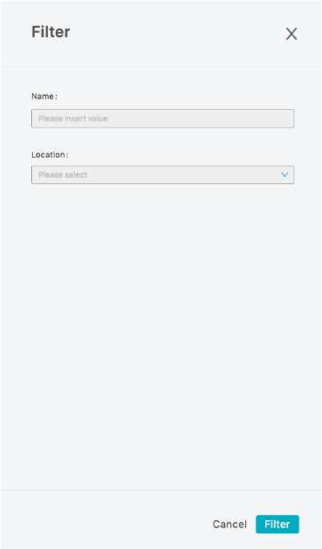


Figure 25 Filter Sub-units

4.2.5 Delete a Sub-unit

To delete a Station Sub-unit from a station, remove all assets from the Sub-unit (for example, move them to other Sub-units).

Hover the mouse over the Sub-unit card and click 🗑. Deleting Sub-unit is possible only if user approve that the assigned asset in this Sub-unit will move to be part of the unassigned asset list.

4.2.6 Navigation from the Sub-unit view

Users can navigate from a Sub-unit view to the list of assets in the Sub-unit, or to the list of Unassigned Assets.

Hover over a Sub-unit card, and then click Show Assets to show a list of the assets in the Sub-unit.

4.3 Assets

Assets are individual production-floor devices that have an IP address. They are discovered automatically based on multiple data sources. A production floor machine could represent several assets.

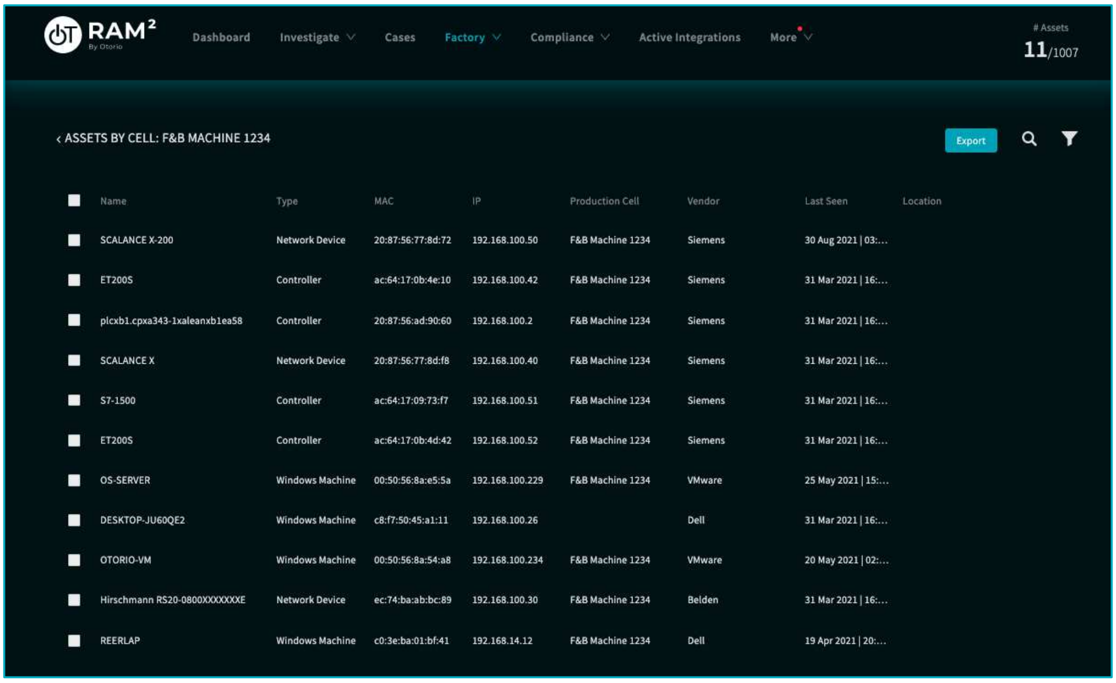
Once assets are discovered, users assign them to Station Sub-unit/s.

Once assets are in the system, risk is calculated for each asset.

Once assets are assigned to a Sub-unit, their issues contribute to the overall Risk Level of the assigned Sub-unit and station.

4.3.1 Assets view

To navigate to the Assets view, hover the mouse over the Sub-unit cards and click on Show Assets button to display the assets. Alternatively, select *Assets* from the top-level *Site* menu to see all the assets in the site. Click 2 Unassigned Assets from the Sub-unit or Station views to view all Unassigned Assets.



‹ ASSETS BY CELL: F&B MACHINE 1234

□	Name	Type	MAC	IP	Production Cell	Vendor	Last Seen	Location
□	SCALANCE X-200	Network Device	20:87:56:77:8d:72	192.168.100.50	F&B Machine 1234	Siemens	30 Aug 2021 | 03:...	
□	ET200S	Controller	ac:64:17:0b:4e:10	192.168.100.42	F&B Machine 1234	Siemens	31 Mar 2021 | 16:...	
□	plcxb1.cpxa343-1xaleanxb1ea58	Controller	20:87:56:ad:90:60	192.168.100.2	F&B Machine 1234	Siemens	31 Mar 2021 | 16:...	
□	SCALANCE X	Network Device	20:87:56:77:8d:f8	192.168.100.40	F&B Machine 1234	Siemens	31 Mar 2021 | 16:...	
□	S7-1500	Controller	ac:64:17:09:73:f7	192.168.100.51	F&B Machine 1234	Siemens	31 Mar 2021 | 16:...	
□	ET200S	Controller	ac:64:17:0b:4d:42	192.168.100.52	F&B Machine 1234	Siemens	31 Mar 2021 | 16:...	
□	OS-SERVER	Windows Machine	00:50:56:8a:e5:5a	192.168.100.229	F&B Machine 1234	VMware	25 May 2021 | 15:...	
□	DESKTOP-JU60QE2	Windows Machine	c8:f7:50:45:a1:11	192.168.100.26		Dell	31 Mar 2021 | 16:...	
□	OTORIO-VM	Windows Machine	00:50:56:8a:54:a8	192.168.100.234	F&B Machine 1234	VMware	20 May 2021 | 02:...	
□	Hirschmann RS20-0800XXXXXXXE	Network Device	ec:74:ba:ab:bc:89	192.168.100.30	F&B Machine 1234	Belden	31 Mar 2021 | 16:...	
□	REERLAP	Windows Machine	c0:3e:ba:01:bf:41	192.168.14.12	F&B Machine 1234	Dell	19 Apr 2021 | 20:...	

Figure 26 Site assets

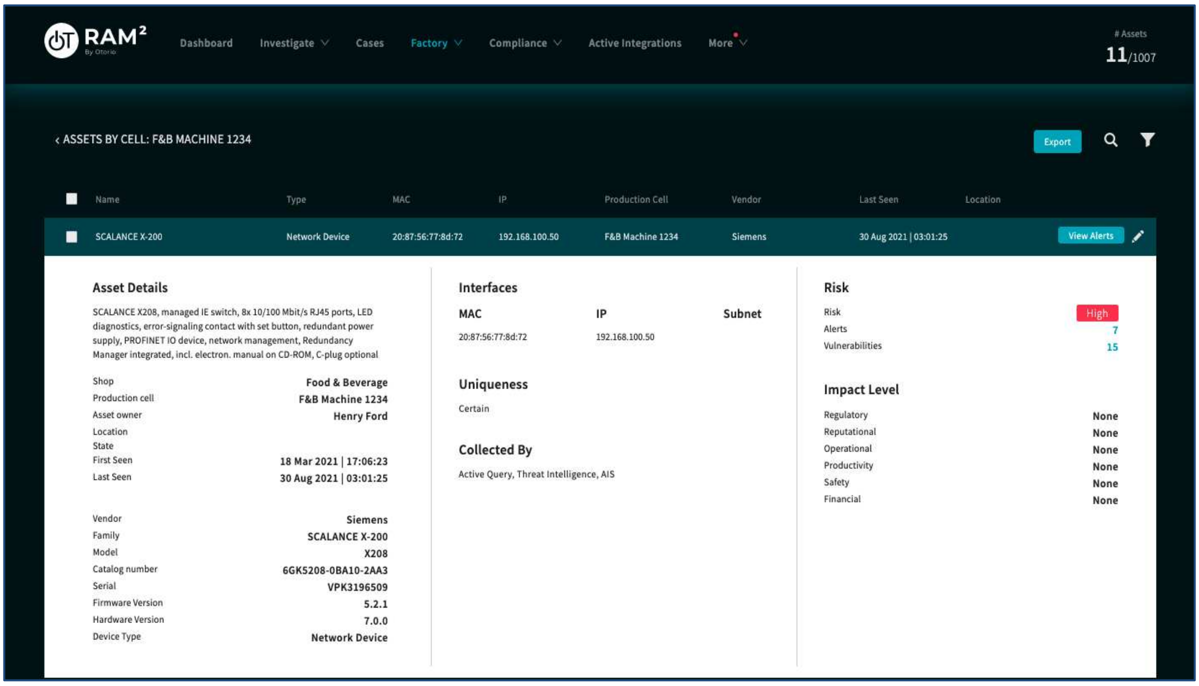
The Asset List includes the following information:

- **Asset name -** Either original asset name as provided by the plugins, or a generated name by the user
- **Asset type -** Controller, Network Device, etc.
- **MAC address -** One of the asset's MACs. If additional MACs are available, "+n" indication will appear. A tooltip with all network interfaces information is presented on hover.
- **Asset IP address -** One of the asset's IPs. If additional IPs are available, "+n" indication will appear. A tooltip with all network interfaces information is presented on hover.

- **Station Sub-unit -** Station Sub-unit/s to which the asset is assigned to
- **Vendor -** the vendor of the asset as it is detected by data source/s
- **Last Seen -** the last time the asset was seen
- **Location**

Click on an asset in the list to show more detail. This shows the following:

- **General asset details – the station, Sub-unit, location and description**
- **Interfaces - list of network interfaces including MAC, IP, Subnet**
- **Type and state, Hardware and Firmware version and more.**
- **Impacts Level**
- **Additional Info -** button to open additional information gathered at the asset level such as compliance information, network, etc.



‹ ASSETS BY CELL: F&B MACHINE 1234

Name	Type	MAC	IP	Production Cell	Vendor	Last Seen	Location
SCALANCE X-200	Network Device	20:87:56:77:8d:72	192.168.100.50	F&B Machine 1234	Siemens	30 Aug 2021 | 03:01:25	

Asset Details

SCALANCE X208, managed IE switch, 8x 10/100 Mbit/s RJ45 ports, LED diagnostics, error-signaling contact with set button, redundant power supply, PROFINET IO device, network management, Redundancy Manager integrated, incl. electron. manual on CD-ROM, C-plug optional

Shop	Food & Beverage
Production cell	F&B Machine 1234
Asset owner	Henry Ford
Location	
State	
First Seen	18 Mar 2021 | 17:06:23
Last Seen	30 Aug 2021 | 03:01:25
Vendor	Siemens
Family	SCALANCE X-200
Model	X208
Catalog number	6GK5208-0BA10-2AA3
Serial	VPK3196509
Firmware Version	5.2.1
Hardware Version	7.0.0
Device Type	Network Device

Interfaces

MAC	IP	Subnet
20:87:56:77:8d:72	192.168.100.50	

Uniqueness

Certain

Collected By

Active Query, Threat Intelligence, AIS

Risk

Risk	High
Alerts	7
Vulnerabilities	15

Impact Level

Regulatory	None
Reputational	None
Operational	None
Productivity	None
Safety	None
Financial	None

Figure 27 Asset detail

Note: user can export asset level report from the button “Export Report '' located at the top left corner of the ide panel. For more information, view the Report chapter in this manual.

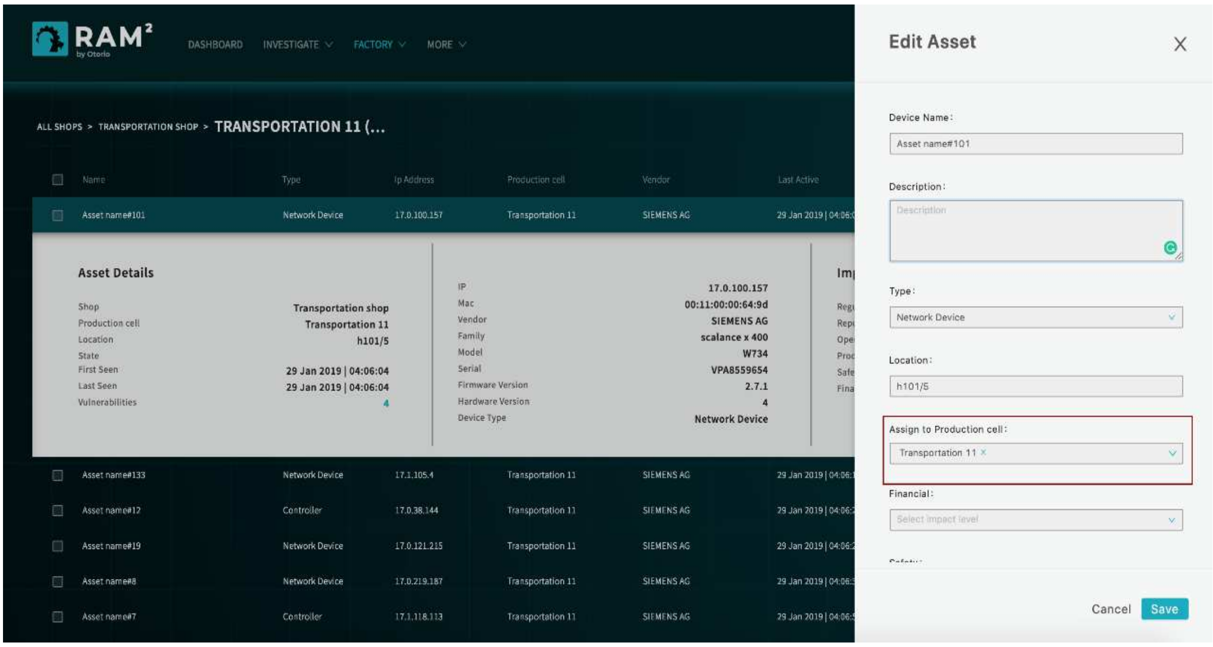
4.3.2 Assign assets to Sub-units

Assets need to be assigned to Sub-units & Sub-units are assigned to stations. Any alerts related to an asset can be seen at the station, Sub-unit and asset level.

Assets can be associated with Sub-units either individually or in bulk. You can assign assets to Sub-units from the *Assets* list view.

To assign a single asset to a Sub-unit:

1. Hover over the asset in the list.
2. Click (on the right side) to open the *Edit Asset* panel.



Name	Type	Ip Address	Production cell	Vendor	Last Active
Asset name#101	Network Device	17.0.100.157	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:0
Asset name#133	Network Device	17.1.105.4	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:1
Asset name#12	Controller	17.0.38.144	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:2
Asset name#19	Network Device	17.0.121.215	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:2
Asset name#8	Network Device	17.0.219.187	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:3
Asset name#7	Controller	17.1.118.113	Transportation 11	SIEMENS AG	29 Jan 2019 | 04:06:5

Asset Details

Shop	Transportation shop
Production cell	Transportation 11
Location	h101/5
State	
First Seen	29 Jan 2019 | 04:06:04
Last Seen	29 Jan 2019 | 04:06:04
Vulnerabilities	4

IP	17.0.100.157
Mac	00:11:00:00:64:9d
Vendor	SIEMENS AG
Family	scalance x 400
Model	W734
Serial	VPA8559654
Firmware Version	2.7.1
Hardware Version	4
Device Type	Network Device

Device Name: Asset name#101

Description: Description

Type: Network Device

Location: h101/5

Assign to Production cell: Transportation 11

Financial: Select impact level

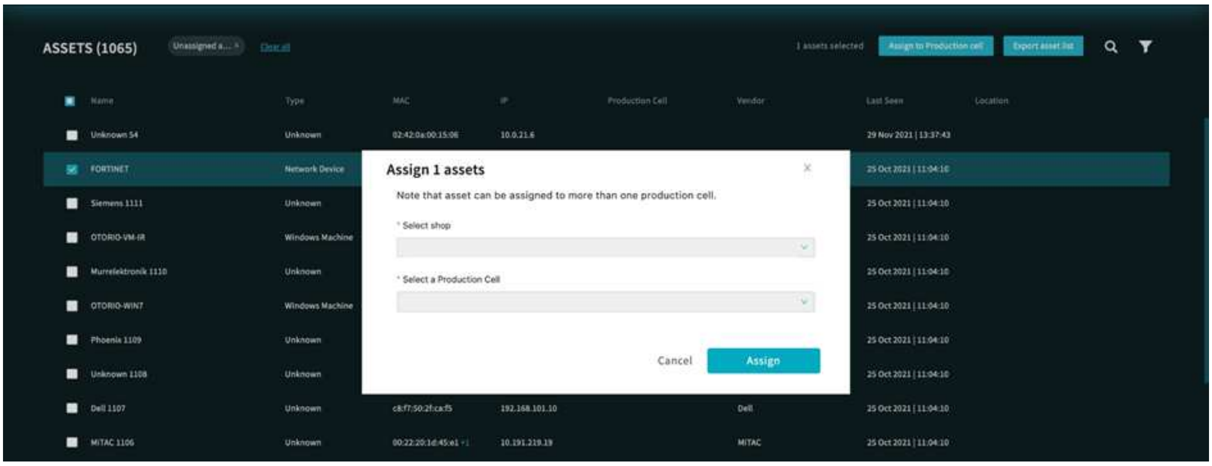
Figure 28 Assign an asset to a Sub-unit

3. In the *Edit Asset* panel, in the *Assign to Station Sub-unit* field, select the Station Sub-unit/s from the list.
4. Click *Save*.

4.3.3 Bulk assign assets to Sub-units

To assign multiple assets to a Station Sub-unit:

1. Select the assets in the list, and click Assign to Production cell in the upper right.



ASSETS (1065) Unassigned a... × Clear all

1 assets selected | Assign to Production cell | Export asset list | 🔍 | ▼

☐	Name	Type	MAC	IP	Production Cell	Vendor	Last Seen	Location
☐	Unknown 54	Unknown	02:42:0a:00:15:06	10.0.21.6			29 Nov 2021 | 13:37:43	
☑	FORTINET	Network Device					25 Oct 2021 | 11:04:10	
☐	Siemens 1111	Unknown					25 Oct 2021 | 11:04:10	
☐	OTORIO-VM-IR	Windows Machine					25 Oct 2021 | 11:04:10	
☐	Murrelektronik 1110	Unknown					25 Oct 2021 | 11:04:10	
☐	OTORIO-WIN7	Windows Machine					25 Oct 2021 | 11:04:10	
☐	Phoenix 1109	Unknown					25 Oct 2021 | 11:04:10	
☐	Unknown 1108	Unknown					25 Oct 2021 | 11:04:10	
☐	Dell 1107	Unknown	c8:f7:50:2f:ca:f5	192.168.101.10		Dell	25 Oct 2021 | 11:04:10	
☐	MITAC 1106	Unknown	00:22:20:1d:45:e1 +1	10.191.219.19		MITAC	25 Oct 2021 | 11:04:10	

Assign 1 assets ×

Note that asset can be assigned to more than one production cell.

* Select shop

* Select a Production Cell

Cancel | Assign

Figure 29 Assign multiple assets to a Sub-unit

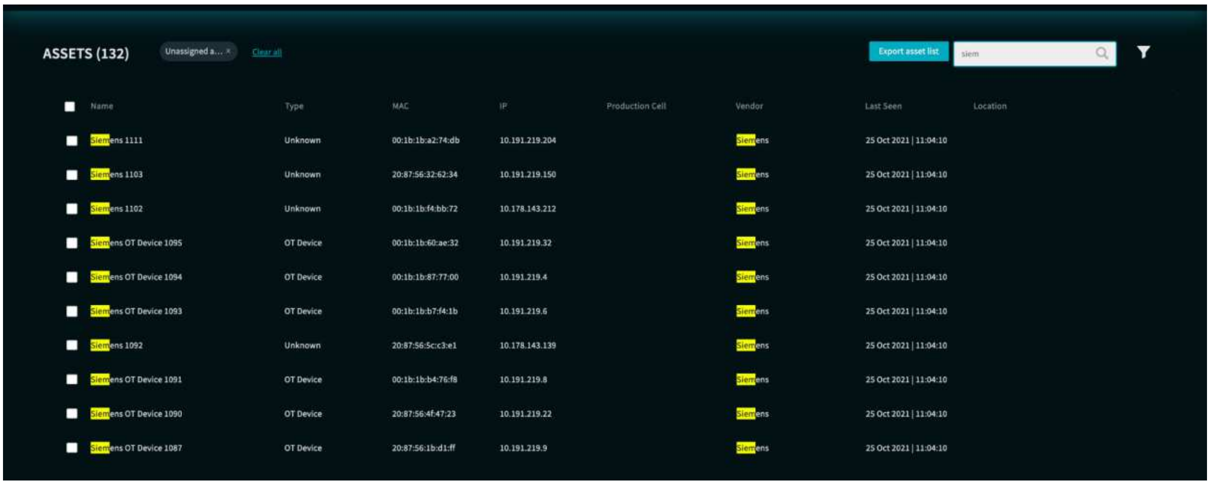
2. Select the Station from the drop down list.
3. Select the Station Sub-unit from the drop down list
4. Click *Assign*.

4.3.4 Filter or search for assets

Users can filter or search for specific assets in the Asset list view.

Click ▼ in the upper right to filter for assets. Filter by name, location, vendor, Sub-unit, IP address and more asset attributes.

Click 🔍 to search for a specific asset by name. The search is progressive: this list of matching assets is updated as more text is entered.



ASSETS (132) Unassigned a... × Clear all

Export asset list | siem 🔍 | ▼

☐	Name	Type	MAC	IP	Production Cell	Vendor	Last Seen	Location
☐	Siemens 1111	Unknown	00:1b:1b:a2:74:db	10.191.219.204		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens 1103	Unknown	20:87:56:32:62:34	10.191.219.150		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens 1102	Unknown	00:1b:1b:f4:bb:72	10.178.143.212		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1095	OT Device	00:1b:1b:60:ae:32	10.191.219.32		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1094	OT Device	00:1b:1b:87:77:00	10.191.219.4		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1093	OT Device	00:1b:1b:b7:f4:1b	10.191.219.6		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens 1092	Unknown	20:87:56:5c:c3:e1	10.178.143.139		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1091	OT Device	00:1b:1b:b4:76:f8	10.191.219.8		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1090	OT Device	20:87:56:4f:47:23	10.191.219.22		Siemens	25 Oct 2021 | 11:04:10	
☐	Siemens OT Device 1087	OT Device	20:87:56:1b:d1:ff	10.191.219.9		Siemens	25 Oct 2021 | 11:04:10	

Figure 30 Asset search

5. Investigation - Alerts

Note: The Investigate option on the navigation bar has three submenus. Alerts and Insights, which is discussed in this section, and vulnerabilities, which is discussed in the following section.

The **Alerts screen** is split into two tabs: **Alerts** and **Insights**.

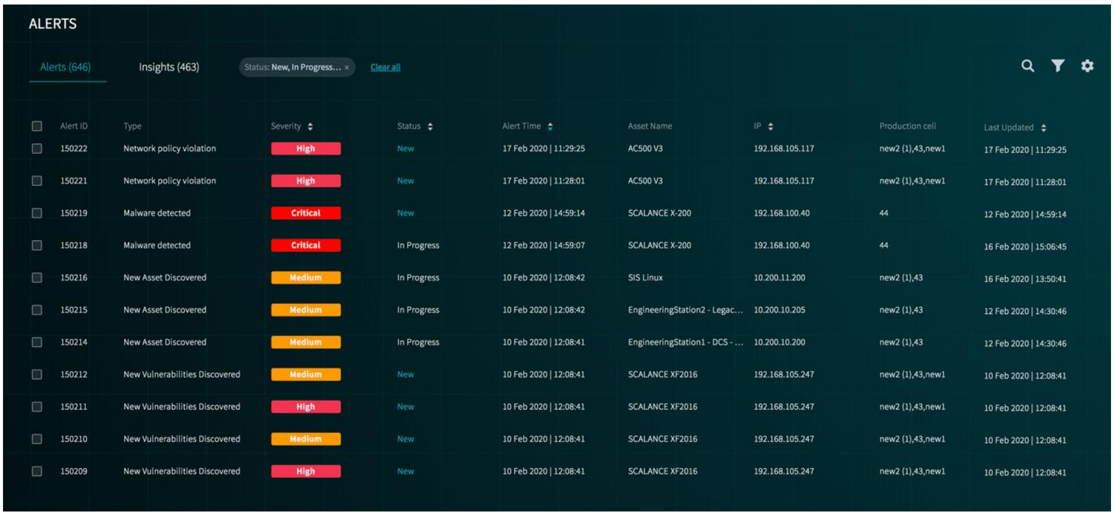
Under the Alerts tab, users can view all alerts that have been generated in the central management. Under the Insights tab, users can view the list of insights that were generated based on correlation of various alerts, and in combination with asset information.

5.1 Alerts tab

The Alerts tab contains a table with a list of all the alerts that were generated by the system. By default, the list is sorted by time of creation, with the newest alerts appearing at the top of the list. Also by default, the list only contains open alerts. Default settings can be changed in the settings for the page. Sorting can be set by a number of parameters, including severity.

Alerts enter the system in one of two ways. Some alerts are generated for events based on data sources that are integrated into the solution, while others are generated based on the internal central management security engines logic and take into account the operational context and impact of manifestation of the risk to the asset and the operational process.

Alerts that do not pass the minimal threshold are managed in the system's backend as invisible alerts and are not exposed in this view, to reduce unneeded noise and alert fatigue. If an invisible alert is correlated with other alerts to an insight, it will be transformed to a visible alert and exposed in this view.



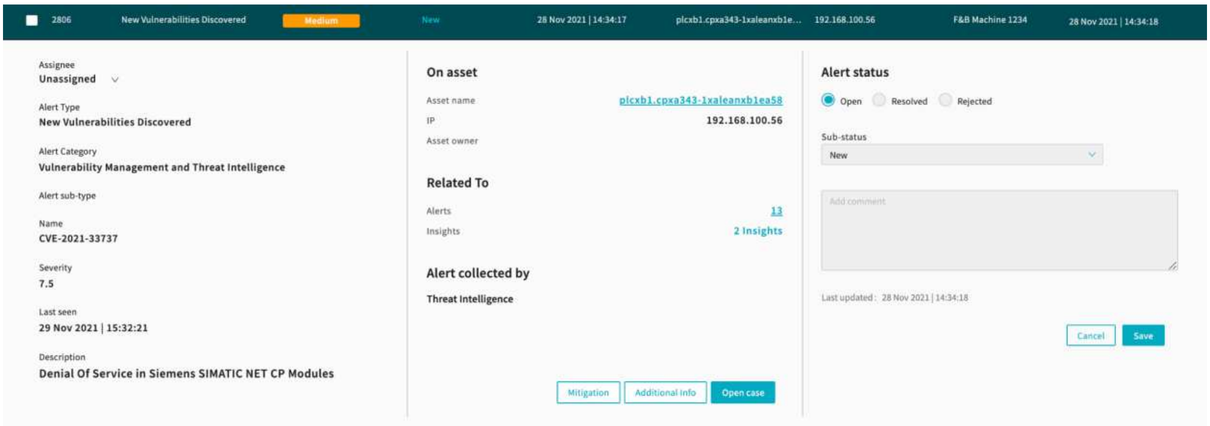
□	Alert ID	Type	Severity	Status	Alert Time	Asset Name	IP	Production cell	Last Updated
□	150222	Network policy violation	High	New	17 Feb 2020 | 11:29:25	AC500 V3	192.168.105.117	new2 (1),43,new1	17 Feb 2020 | 11:29:25
□	150221	Network policy violation	High	New	17 Feb 2020 | 11:28:01	AC500 V3	192.168.105.117	new2 (1),43,new1	17 Feb 2020 | 11:28:01
□	150219	Malware detected	Critical	New	12 Feb 2020 | 14:59:14	SCALANCE X-200	192.168.100.40	44	12 Feb 2020 | 14:59:14
□	150218	Malware detected	Critical	In Progress	12 Feb 2020 | 14:59:07	SCALANCE X-200	192.168.100.40	44	16 Feb 2020 | 15:06:45
□	150216	New Asset Discovered	Medium	In Progress	10 Feb 2020 | 12:08:42	SIS Linux	10.200.11.200	new2 (1),43	16 Feb 2020 | 13:50:41
□	150215	New Asset Discovered	Medium	In Progress	10 Feb 2020 | 12:08:42	EngineeringStation2 - Legac...	10.200.10.205	new2 (1),43	12 Feb 2020 | 14:30:46
□	150214	New Asset Discovered	Medium	In Progress	10 Feb 2020 | 12:08:41	EngineeringStation1 - DCS - ...	10.200.10.200	new2 (1),43	12 Feb 2020 | 14:30:46
□	150212	New Vulnerabilities Discovered	Medium	New	10 Feb 2020 | 12:08:41	SCALANCE XF2016	192.168.105.247	new2 (1),43,new1	10 Feb 2020 | 12:08:41
□	150211	New Vulnerabilities Discovered	High	New	10 Feb 2020 | 12:08:41	SCALANCE XF2016	192.168.105.247	new2 (1),43,new1	10 Feb 2020 | 12:08:41
□	150210	New Vulnerabilities Discovered	Medium	New	10 Feb 2020 | 12:08:41	SCALANCE XF2016	192.168.105.247	new2 (1),43,new1	10 Feb 2020 | 12:08:41
□	150209	New Vulnerabilities Discovered	High	New	10 Feb 2020 | 12:08:41	SCALANCE XF2016	192.168.105.247	new2 (1),43,new1	10 Feb 2020 | 12:08:41

Figure 31 Alerts view

Each alert contains the following details:

- **Alert ID –** unique alert identifier
- **Type –** from a list of predefined alert types
- **Severity –** risk level of the alert
- **Status –** new, in progress, resolved or rejected
- **Alert time –** time/date stamp when the alert occurred
- **Asset name –** the asset associated with the alert
- **IP –** Asset's IP address
- **Station Sub-unit –** Sub-unit containing the affected asset
- **Last updated –** Time/date stamp for last time there were any changes to the alert

Click on an alert to expand the row for more detailed information.



□	2806	New Vulnerabilities Discovered	Medium	New	28 Nov 2021 | 14:34:17	plcxb1.cpxa343-1xaleanxb1e...	192.168.100.56	F&B Machine 1234	28 Nov 2021 | 14:34:18

Assignee
Unassigned

Alert Type
New Vulnerabilities Discovered

Alert Category
Vulnerability Management and Threat Intelligence

Alert sub-type

Name
CVE-2021-33737

Severity
7.5

Last seen
29 Nov 2021 | 15:32:21

Description
Denial Of Service in Siemens SIMATIC NET CP Modules

On asset

Asset name: plcxb1.cpxa343-1xaleanxb1ea58
IP: 192.168.100.56
Asset owner

Related To

Alerts: 13
Insights: 2 Insights

Alert collected by

Threat Intelligence

Alert status

● Open ○ Resolved ○ Rejected

Sub-status: New

Last updated : 28 Nov 2021 | 14:34:18

Figure 32 Expended alert view

The expanded view includes the following information:

- **Alert type -** type of the alert
- **Alert Category –** scope of alert (shown in Risk tab)
- **Alert sub-type –** detailed alert classification
- **Description –** Root cause of alert and potential implications
- **Asset details –** asset name (clickable), asset owner
- **Related to –** Other alerts (clickable), insights (clickable)
- **Source –** the data source that contributed the event based on which the alert was generated.
- **Alert status –** open, resolve or reject the alert. Additional free text comment field for added documentation explaining alert status changes.

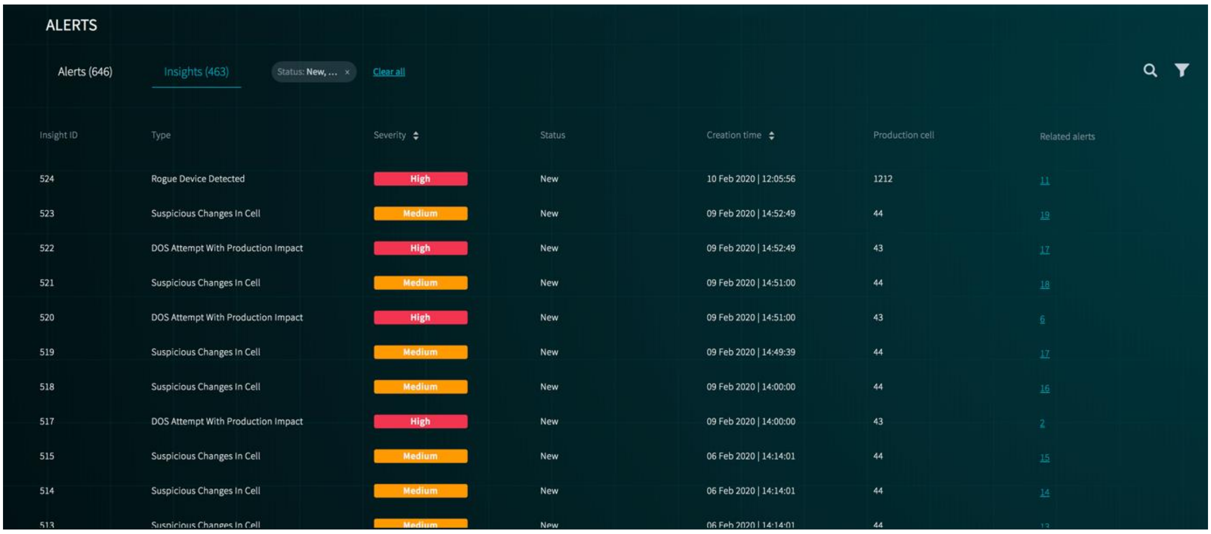
Users can close the alert directly from the expanded view. In addition, there are three additional options:

- **Open Case –** create a new case to manage alert with other stakeholders or team members within the organization
- **Mitigation Button –** click to display the needed mitigation actions for resolution of the problem.
- **Additional Info –** Investigate the raw data that was used to generate the alert. A cyber analyst can view this information including the original Syslog event or API response.

5.2 Insights tab

Insights are generated by correlating visible and invisible alerts, together with asset information. These insights create a wider view of risks impacting the system.

The insights act as “Cyber-analyst-in-a-box”. They identify patterns and suggest a playbook with step-by-step actions to take for quick mitigation. These empower the operational team to take action, as they reduce both the time and effort needed for resolution on the Security Operations Center (SOC) side. They bridge the knowledge gap and assist to ensure safe industrial growth.



ALERTS

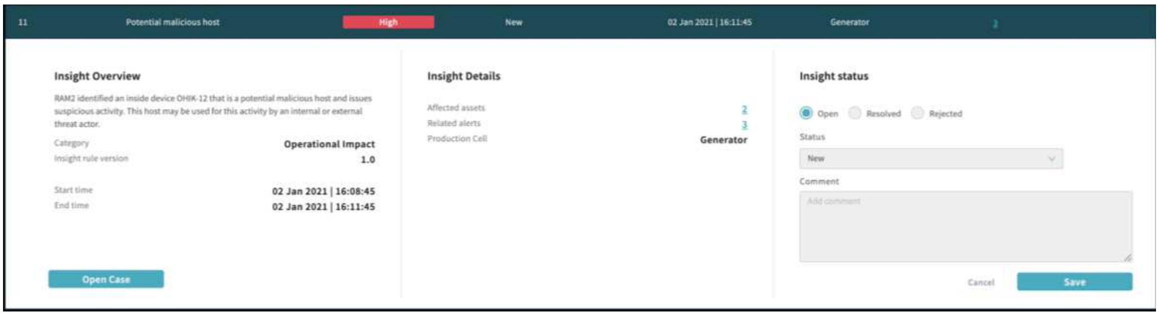
Insight ID	Type	Severity	Status	Creation time	Production cell	Related alerts
524	Rogue Device Detected	High	New	10 Feb 2020 | 12:05:56	1212	11
523	Suspicious Changes In Cell	Medium	New	09 Feb 2020 | 14:52:49	44	19
522	DOS Attempt With Production Impact	High	New	09 Feb 2020 | 14:52:49	43	17
521	Suspicious Changes In Cell	Medium	New	09 Feb 2020 | 14:51:00	44	18
520	DOS Attempt With Production Impact	High	New	09 Feb 2020 | 14:51:00	43	6
519	Suspicious Changes In Cell	Medium	New	09 Feb 2020 | 14:49:39	44	17
518	Suspicious Changes In Cell	Medium	New	09 Feb 2020 | 14:00:00	44	16
517	DOS Attempt With Production Impact	High	New	09 Feb 2020 | 14:00:00	43	2
515	Suspicious Changes In Cell	Medium	New	06 Feb 2020 | 14:14:01	44	15
514	Suspicious Changes In Cell	Medium	New	06 Feb 2020 | 14:14:01	44	14
513	Suspicious Changes In Cell	Medium	New	06 Feb 2020 | 14:14:01	44	13

Figure 33 Insights view

Each insight row includes:

- **Insight ID –** Unique insight identifier
- **Type –** from a list of predefined Insight types
- **Severity –** based on the risk of the alerts and the impact level of the Sub-unit
- **Status –** new, handled in case, resolved or rejected
- **Creation Time -** the creation of the insight
- **Station Sub-unit –** the Station Sub-unit at risk based on asset alerts
- **Related alerts -** the alerts that were involved in creating the Insight

Click on an Insight to expand the row for more detailed information



11	Potential malicious host	High	New	02 Jan 2021 | 16:11:45	Generator	2

Insight Overview

RAM2 identified an inside device OHIK-12 that is a potential malicious host and issues suspicious activity. This host may be used for this activity by an internal or external threat actor.

Category: Operational Impact
Insight rule version: 1.0

Start time: 02 Jan 2021 | 16:08:45
End time: 02 Jan 2021 | 16:11:45

Insight Details

Affected assets: 2
Related alerts: 3
Production Cell: Generator

Insight status

● Open ○ Resolved ○ Rejected

Status: New

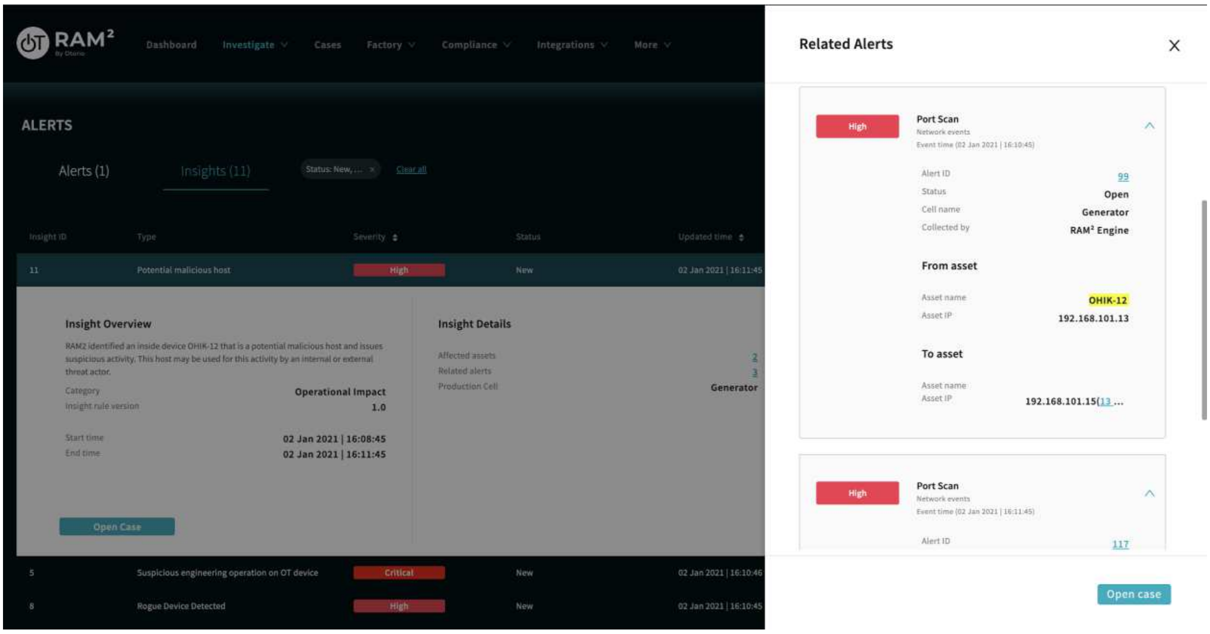
Comment: Add comment

Figure 34 Expanded Insight view

The expanded insight view includes:

- **Insight Overview –** details relating to the insight, the threat category and the impacted Station Sub-unit.
- **Insight Details -** the affected assets, related alerts and the time of the first and last alert in the insight.
- **Insight status –** open, resolve, or reject the insight. Additional free text comment field for added documentation explaining Insight Status changes.
- **Insight rule version -** Version of the insight rule that generated the insight.

Click on the related alerts (numbered link) to see all matched alerts on a timeline. Each alert is presented with the event time, current status, relevant Sub-unit and related assets. The anchor value, which unifies the alerts to the insight is yellow marked.



ALERTS

Insight ID	Type	Severity	Status	Updated time
11	Potential malicious host	High	New	02 Jan 2021 | 16:11:45
5	Suspicious engineering operation on OT device	Critical	New	02 Jan 2021 | 16:10:46
8	Rogue Device Detected	High	New	02 Jan 2021 | 16:10:45

Insight Overview

RAM2 identified an inside device OHIK-12 that is a potential malicious host and issues suspicious activity. This host may be used for this activity by an internal or external threat actor.

Category: Operational Impact
Insight rule version: 1.0

Start time: 02 Jan 2021 | 16:08:45
End time: 02 Jan 2021 | 16:11:45

Insight Details

Affected assets: 2
Related alerts: 3
Production Cell: Generator

Related Alerts

High — Port Scan
Network events
Event time (02 Jan 2021 | 16:10:45)

Alert ID: 99
Status: Open
Cell name: Generator
Collected by: RAM² Engine

From asset
Asset name: OHIK-12
Asset IP: 192.168.101.13

To asset
Asset name:
Asset IP: 192.168.101.15(13 ...

High — Port Scan
Network events
Event time (02 Jan 2021 | 16:11:45)

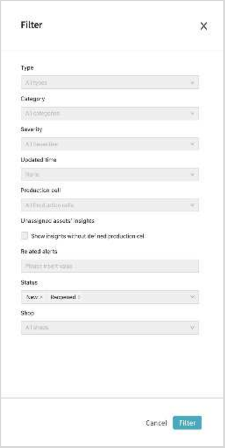
Alert ID: 117

Figure 35 - Alerts

BEST PRACTICE: When managing an insight and tracking the resolution of the alerts involved, users should open a case. This allows stakeholders to have a single point of communication, where all messages can be viewed, managed and documented. Effort toward resolution is tracked, giving full transparency across the organization. To start, click the Open Case button.

5.3 Filter or Search Alerts & Insights

- Click ▼ in the **upper** right to filter alerts. Filter by alert type, status, time, Sub-unit, vulnerability type, or severity. You can also filter for new or acknowledged alerts.
- Click 🔍 to search for alerts.



Filter ×

Type: All types

Category: All categories

Severity: All severities

Updated time: None

Production cell: All production cells

Unassigned assets' insights

□ Show insights without defined production cell

Related alerts: Please insert value

Status: New × Reopened ×

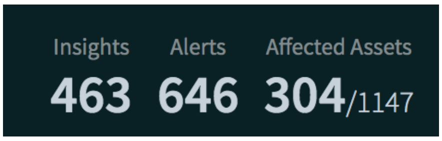
Shop: All shops

Cancel Filter

Figure 36 Filter alerts

5.4 Alert & Insights KPIs and Distribution

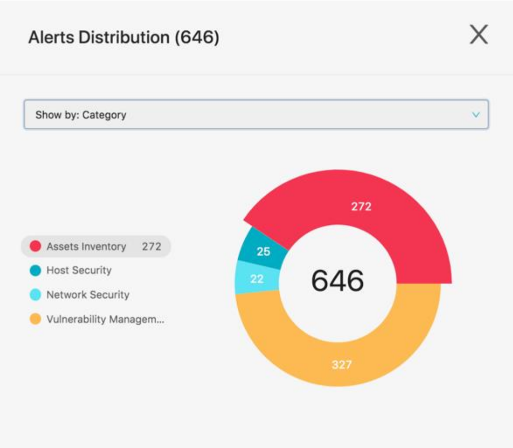
The top right corner of the Investigate screen shows the total number of open insights, alerts, and the number of site assets affected by alerts.



Insights	Alerts	Affected Assets
463	646	304/1147

Figure 37 Alerts screen KPIs

Click on the summary of alerts and affected assets in the upper right of the Alerts view to see a distribution of alerts according to type, category, status or Station Sub-unit.



Alerts Distribution (646)

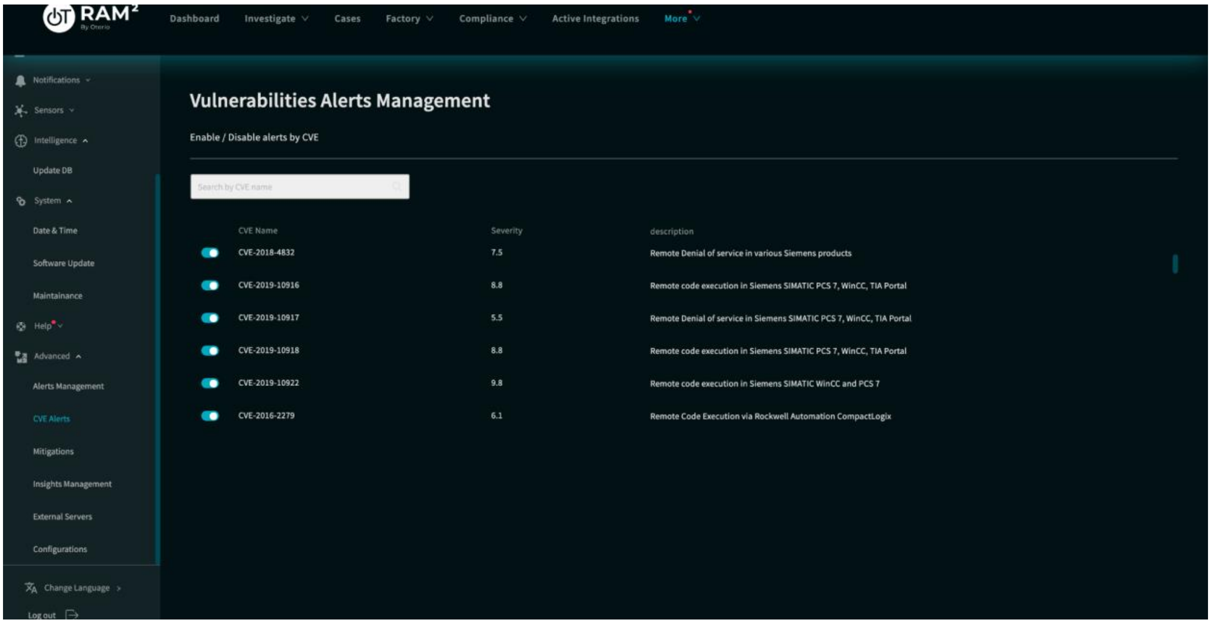
Show by: Category

Figure 38 Alert distribution by type

5.5 Disable vulnerabilities

One source for alerts is vulnerabilities. While most vulnerabilities need to be monitored, there may be some specific vulnerabilities that don’t require monitoring. Hence, the user can disable them to prevent them from creating alerts.
To disable these vulnerabilities:

1. In main menu *More/Settings/Advanced/CVE Alerts* page
2. In the *Vulnerabilities Alerts Management* page, disable alerts that are not relevant.



Vulnerabilities Alerts Management

Enable / Disable alerts by CVE

	CVE Name	Severity	description
●	CVE-2018-4832	7.5	Remote Denial of service in various Siemens products
●	CVE-2019-10916	8.8	Remote code execution in Siemens SIMATIC PCS 7, WinCC, TIA Portal
●	CVE-2019-10917	5.5	Remote Denial of service in Siemens SIMATIC PCS 7, WinCC, TIA Portal
●	CVE-2019-10918	8.8	Remote code execution in Siemens SIMATIC PCS 7, WinCC, TIA Portal
●	CVE-2019-10922	9.8	Remote code execution in Siemens SIMATIC WinCC and PCS 7
●	CVE-2016-2279	6.1	Remote Code Execution via Rockwell Automation CompactLogix

Figure 39 Vulnerabilities

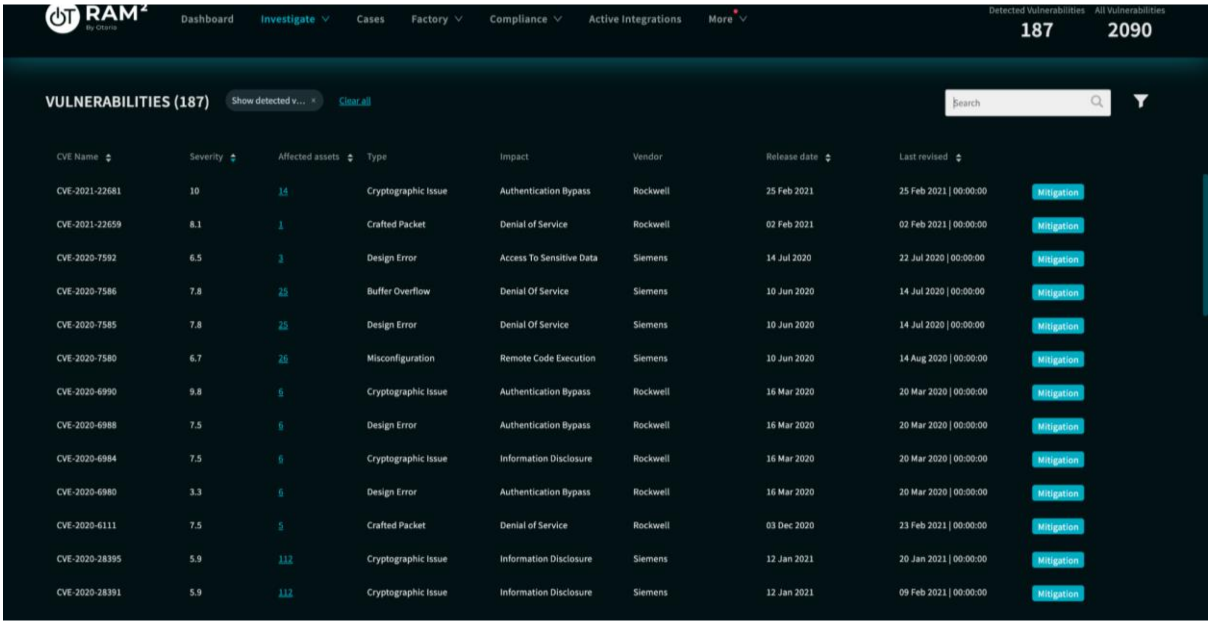
3. Once a vulnerability is disabled, future alerts for it will not be issued, and will not appear in the Alerts page.

6. Investigation - Vulnerabilities

Note: The Investigate option on the navigation bar has two submenus. Alerts, which was discussed in the previous section, and vulnerabilities, which is discussed in this section.

This screen provides access to OTORIO's dedicated vulnerabilities database that is managed by our threat intelligence team. The table in the screen includes information regarding each vulnerability, and the automatic mapping to actual assets within the network.

Use this view to save time on manual analysis of the common vulnerabilities and exposures (CVE) and matching the assets vendors, families and firmware versions to the conditions in the vendor advisories.



VULNERABILITIES (187)

CVE Name	Severity	Affected assets	Type	Impact	Vendor	Release date	Last revised	
CVE-2021-22681	10	14	Cryptographic Issue	Authentication Bypass	Rockwell	25 Feb 2021	25 Feb 2021 | 00:00:00	Mitigation
CVE-2021-22659	8.1	1	Crafted Packet	Denial of Service	Rockwell	02 Feb 2021	02 Feb 2021 | 00:00:00	Mitigation
CVE-2020-7592	6.5	3	Design Error	Access To Sensitive Data	Siemens	14 Jul 2020	22 Jul 2020 | 00:00:00	Mitigation
CVE-2020-7586	7.8	25	Buffer Overflow	Denial Of Service	Siemens	10 Jun 2020	14 Jul 2020 | 00:00:00	Mitigation
CVE-2020-7585	7.8	25	Design Error	Denial Of Service	Siemens	10 Jun 2020	14 Jul 2020 | 00:00:00	Mitigation
CVE-2020-7580	6.7	26	Misconfiguration	Remote Code Execution	Siemens	10 Jun 2020	14 Aug 2020 | 00:00:00	Mitigation
CVE-2020-6990	9.8	6	Cryptographic Issue	Authentication Bypass	Rockwell	16 Mar 2020	20 Mar 2020 | 00:00:00	Mitigation
CVE-2020-6988	7.5	6	Design Error	Authentication Bypass	Rockwell	16 Mar 2020	20 Mar 2020 | 00:00:00	Mitigation
CVE-2020-6984	7.5	6	Cryptographic Issue	Information Disclosure	Rockwell	16 Mar 2020	20 Mar 2020 | 00:00:00	Mitigation
CVE-2020-6980	3.3	6	Design Error	Authentication Bypass	Rockwell	16 Mar 2020	20 Mar 2020 | 00:00:00	Mitigation
CVE-2020-6111	7.5	5	Crafted Packet	Denial of Service	Rockwell	03 Dec 2020	23 Feb 2021 | 00:00:00	Mitigation
CVE-2020-28395	5.9	112	Cryptographic Issue	Information Disclosure	Siemens	12 Jan 2021	20 Jan 2021 | 00:00:00	Mitigation
CVE-2020-28391	5.9	112	Cryptographic Issue	Information Disclosure	Siemens	12 Jan 2021	09 Feb 2021 | 00:00:00	Mitigation

Figure 40 Vulnerabilities

Each CVE includes the following details:

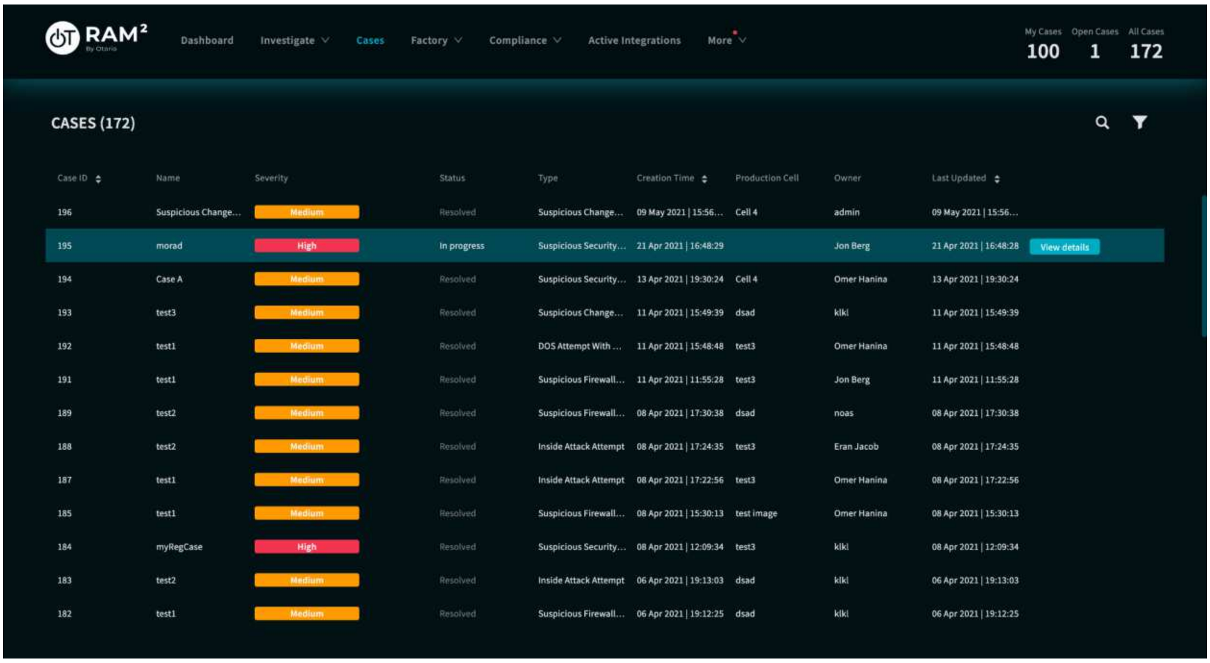
- **CVE Name**
- **Severity (CVSS)**
- **Affected assets –** number and a link to the list of assets
- **Type of vulnerability**
- **Potential impact of the vulnerability**
- **Affected vendor**
- **Release date**
- **Latest revised**
- **Mitigation –** Steps needed to take to mitigate the risk, taking limitations of the OT network into account

7. Cases

Cases are insights, alerts or other vulnerabilities that have been assigned for investigation and resolution. They can be shared among different users, such as operators, engineers, cyber analysts, IT technicians, or anyone else required for the resolution of the alert.

RAM² helps manage the communication both within the operational team and across units, allowing for full transparency across the organization.

Cases can be opened from an insight, alert, or group of alerts. Once a case is created, its resolution time is measured. The case has a default owner based on the affected assets. However, each of the alerts that are grouped by the case can have a different assignee based on the relevant function that is skilled to handle the issue.



CASES (172)

Case ID	Name	Severity	Status	Type	Creation Time	Production Cell	Owner	Last Updated
196	Suspicious Change...	Medium	Resolved	Suspicious Change...	09 May 2021 | 15:56...	Cell 4	admin	09 May 2021 | 15:56...
195	morad	High	In progress	Suspicious Security...	21 Apr 2021 | 16:48:29		Jon Berg	21 Apr 2021 | 16:48:28
194	Case A	Medium	Resolved	Suspicious Security...	13 Apr 2021 | 19:30:24	Cell 4	Omer Hanina	13 Apr 2021 | 19:30:24
193	test3	Medium	Resolved	Suspicious Change...	11 Apr 2021 | 15:49:39	dsad	klkl	11 Apr 2021 | 15:49:39
192	test1	Medium	Resolved	DOS Attempt With ...	11 Apr 2021 | 15:48:48	test3	Omer Hanina	11 Apr 2021 | 15:48:48
191	test1	Medium	Resolved	Suspicious Firewall...	11 Apr 2021 | 11:55:28	test3	Jon Berg	11 Apr 2021 | 11:55:28
189	test2	Medium	Resolved	Suspicious Firewall...	08 Apr 2021 | 17:30:38	dsad	noas	08 Apr 2021 | 17:30:38
188	test2	Medium	Resolved	Inside Attack Attempt	08 Apr 2021 | 17:24:35	test3	Eran Jacob	08 Apr 2021 | 17:24:35
187	test1	Medium	Resolved	Inside Attack Attempt	08 Apr 2021 | 17:22:56	test3	Omer Hanina	08 Apr 2021 | 17:22:56
185	test1	Medium	Resolved	Suspicious Firewall...	08 Apr 2021 | 15:30:13	test image	Omer Hanina	08 Apr 2021 | 15:30:13
184	myRegCase	High	Resolved	Suspicious Security...	08 Apr 2021 | 12:09:34	test3	klkl	08 Apr 2021 | 12:09:34
183	test2	Medium	Resolved	Inside Attack Attempt	06 Apr 2021 | 19:13:03	dsad	klkl	06 Apr 2021 | 19:13:03
182	test1	Medium	Resolved	Suspicious Firewall...	06 Apr 2021 | 19:12:25	dsad	klkl	06 Apr 2021 | 19:12:25

Figure 41 Cases screen

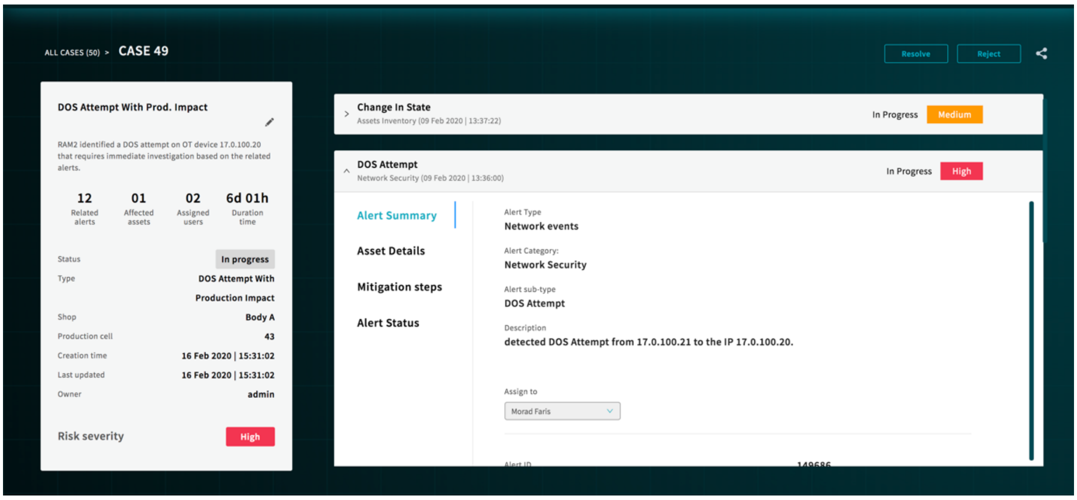
The Case screen includes the following information:

- **Case ID number**
- **Case name**
- **Severity level**
- **Status**
- **Type**
- **Creation Time**
- **Station Sub-unit**
- **Owner**
- **Last Updated**

Click on the “View details” button for an expanded view of the case. The expanded view includes:

- **Details about the alert**
- **Risk severity**
- **Change in state**
- **Alert Summary**
- **Asset Details**
- **Mitigation Steps**
- **Alert Status**

Click the share button to send the case details to any person within or outside the operational team, who needs to assist in managing the case for efficient resolution.



DOS Attempt With Prod. Impact

RAM2 identified a DOS attempt on OT device 17.0.100.20 that requires immediate investigation based on the related alerts.

12	01	02	6d 01h
Related alerts	Affected assets	Assigned users	Duration time

Status	In progress
Type	DOS Attempt With Production Impact
Shop	Body A
Production cell	43
Creation time	16 Feb 2020 | 15:31:02
Last updated	16 Feb 2020 | 15:31:02
Owner	admin
Risk severity	High

Change In State
Assets Inventory (09 Feb 2020 | 13:37:22)
In Progress Medium

DOS Attempt
Network Security (09 Feb 2020 | 13:36:00)
In Progress High

Alert Type
Network events

Alert Category:
Network Security

Alert sub-type
DOS Attempt

Description
detected DOS Attempt from 17.0.100.21 to the IP 17.0.100.20.

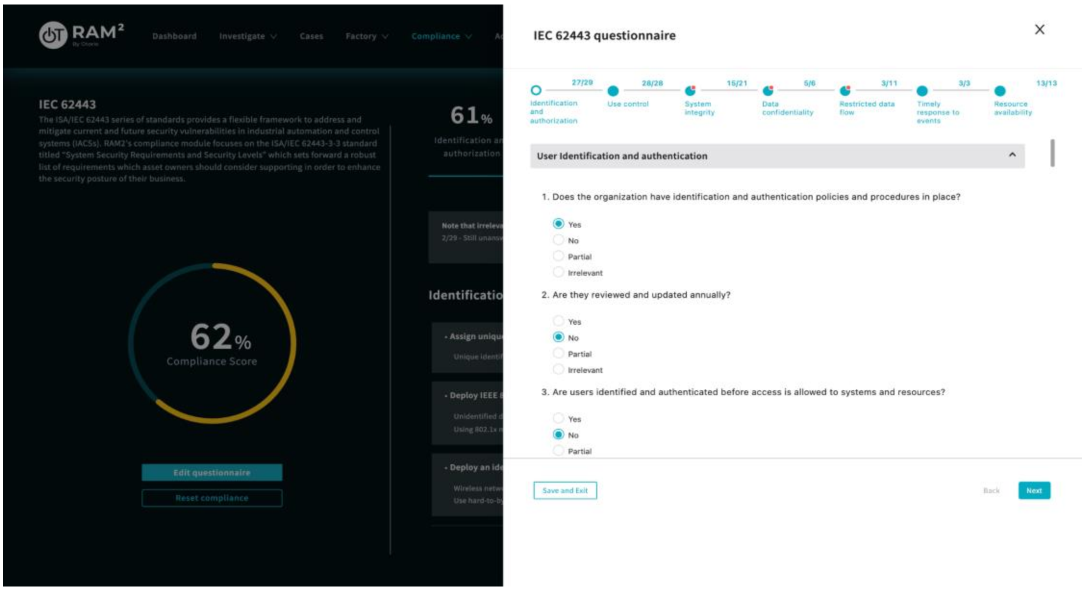
Assign to
Morad Faris

Alert ID 149686

Figure 42 case details screen

8. Compliance

The compliance module enables governance of the site's adherence to industry security standards. Built as an easy-to-understand questionnaire for each of the common standards, it helps in tracking the fulfillment of best practices and actions that lead to Cyber security risk reduction in industrial organizations. The Compliance module currently supports IEC 62443 and NIST 800-82 standards.



IEC 62443

The ISA/IEC 62443 series of standards provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). RAM2's compliance module focuses on the ISA/IEC 62443-3-3 standard titled "System Security Requirements and Security Levels" which sets forward a robust list of requirements which asset owners should consider supporting in order to enhance the security posture of their business.

IEC 62443 questionnaire

User Identification and authentication

1. Does the organization have identification and authentication policies and procedures in place?

● Yes
○ No
○ Partial
○ Irrelevant

2. Are they reviewed and updated annually?

○ Yes
● No
○ Partial
○ Irrelevant

3. Are users identified and authenticated before access is allowed to systems and resources?

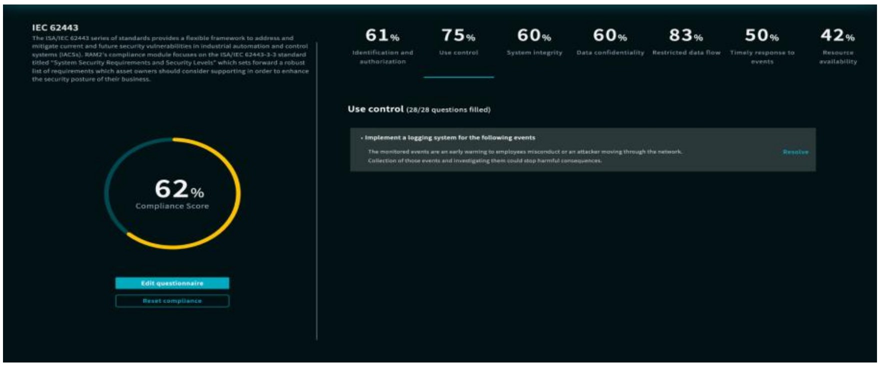
○ Yes
● No
○ Partial

Figure 43 IEC 62443 compliance questionnaire

The module simplifies the handling of these standards, presents a score for the whole compliance standard, breaks the score down by pillar, and suggests remediation actions to improve compliance levels.

In addition, the user can provide textual comments per question to in order to improve or provide:

- Clarifications regard answers provide
- record open issue
- Raise relevant gaps



IEC 62443

The ISA/IEC 62443 series of standards provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). RAM2's compliance module focuses on the ISA/IEC 62443-3-3 standard titled "System Security Requirements and Security Levels" which sets forward a robust list of requirements which asset owners should consider supporting in order to enhance the security posture of their business.

Use control (28/28 questions filled)

- Implement a logging system for the following events

The monitored events are an early warning to employees misconduct or an attacker moving through the network. Collection of those events and investigating them could stop harmful consequences.

Figure 44 Compliance questionnaire scoring and remediation suggestions

9. Reports

The reporting functionality allows organizations to generate ad-hoc reports for better analysis, as well as to share the digital risk posture with stakeholders across the organization.

The current report types user can generate are:

1. Risk overview report
2. Asset Inventory report
3. Vulnerability report
4. Confirmation of compliance reports for:
    a. IEC 62443
    b. NERC CIP
5. Detailed asset level compliance report

There are several location in which user can generate reports:

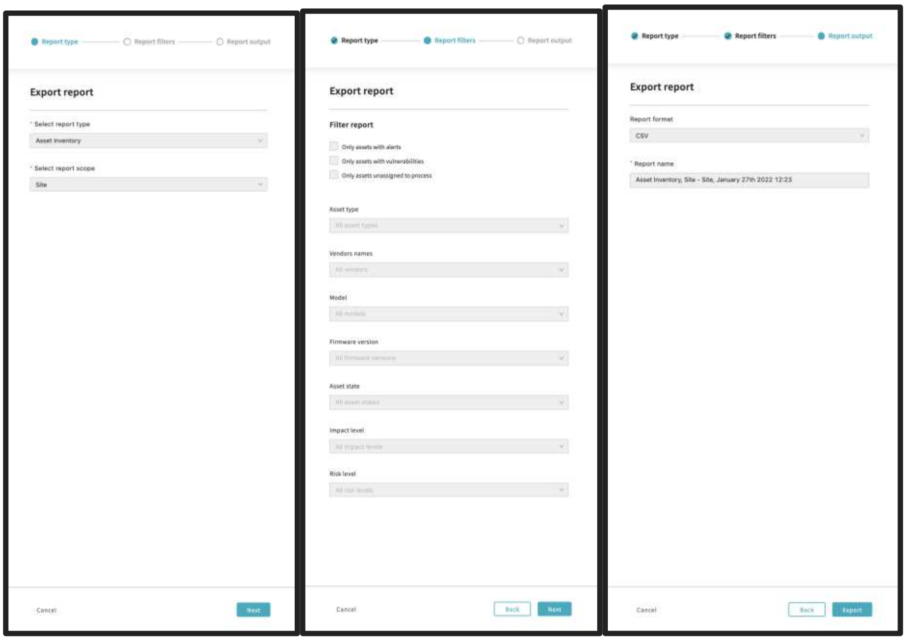
1. Via dashboard screen
2. Via specific entities such as asset, Sub-unit, station etc.

9.1 Via dashboard

Click on the Export report button on the Central Management dashboard to display the report configuration side panel. The system offers two types of reports. Select the required report:

- **Risk overview –** high level information regarding risk, assets, vulnerabilities, alerts and more. Available in PDF format.
- **Assets inventory –** A list of all the assets and their attributes for the selected process and filters. Available in CSV format. Asset is identified by the ID under the “Asset ID” column. A single asset may be presented by multiple lines, each referring to a specific asset interface; interface's index is under the “Interface Index” column.
- **Vulnerabilities overview-** A list of all detected vulnerabilities on selected assets (by filter: Station/Sub-unit/Vendor/Type/Severity/ and more. Available in CSV format.

Choose the scope of the report (Site, Station or Sub-unit where applicable), set the needed filters, and click the export button to download the report.



Export report

* Select report type: Asset Inventory

* Select report scope: Site

Export report

Filter report

□ Only assets with alerts
□ Only assets with vulnerabilities
□ Only assets unassigned to process

Asset type: All asset types

Vendors names: All vendors

Model: All models

Firmware version: All firmware versions

Asset state: All asset states

Impact level: All impact levels

Risk level: All risk levels

Export report

Report format: CSV

* Report name: Asset Inventory, Site - Site, January 27th 2022 12:23

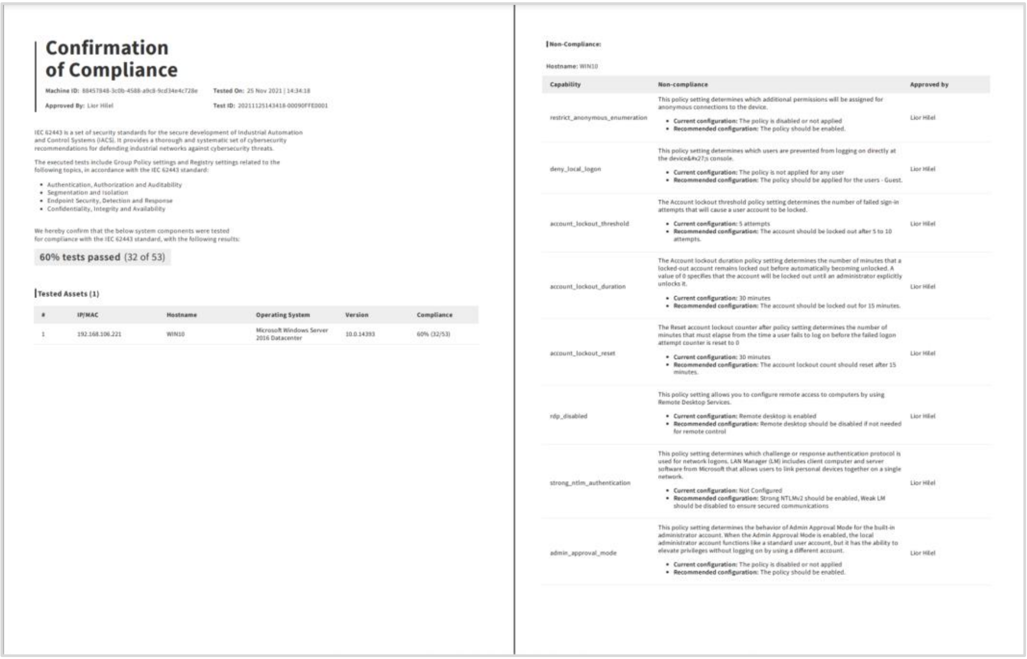
Figure 45 Report wizard - Export report configuration

9.2 Via specific entity

9.2.1 Asset

User can export 2 report types of a specific asset:

1. Asset inventory
2. **Vulnerability overview**
3. **Confirmation of compliance IEC 62443/NERC CIP report-** The following acts as an evidence of compliance of the asset in adherence to IEC 62443/NERC CIP standard (output as PDF). This report reveals all the non compliance issues exist on the asset.



Confirmation of Compliance

Machine ID: 88457848-3c0b-4588-a9c8-9cd34e4c728e **Tested On:** 25 Nov 2021 | 14:34:18

Approved By: Lior Hilel **Test ID:** 20211125143418-00090FFE0001

IEC 62443 is a set of security standards for the secure development of Industrial Automation and Control Systems (IACS). It provides a thorough and systematic set of cybersecurity recommendations for defending industrial networks against cybersecurity threats.

The executed tests include Group Policy settings and Registry settings related to the following topics, in accordance with the IEC 62443 standard:

- Authentication, Authorization and Auditability
- Segmentation and Isolation
- Endpoint Security, Detection and Response
- Confidentiality, Integrity and Availability

We hereby confirm that the below system components were tested for compliance with the IEC 62443 standard, with the following results:

60% tests passed (32 of 53)

Tested Assets (1)

#	IP/MAC	Hostname	Operating System	Version	Compliance
1	192.168.106.221	WIN10	Microsoft Windows Server 2016 Datacenter	10.0.14393	60% (32/53)

Non-Compliance:

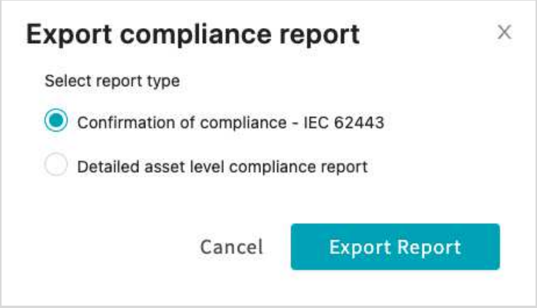
Hostname: WIN10

Capability	Non-compliance	Approved by
restrict_anonymous_enumeration	This policy setting determines which additional permissions will be assigned for anonymous connections to the device. • **Current configuration:** The policy is disabled or not applied • **Recommended configuration:** The policy should be enabled.	Lior Hilel
deny_local_logon	This policy setting determines which users are prevented from logging on directly at the device&#x27;s console. • **Current configuration:** The policy is not applied for any user • **Recommended configuration:** The policy should be applied for the users - Guest.	Lior Hilel
account_lockout_threshold	The Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. • **Current configuration:** 5 attempts • **Recommended configuration:** The account should be locked out after 5 to 10 attempts.	Lior Hilel
account_lockout_duration	The Account lockout duration policy setting determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked. A value of 0 specifies that the account will be locked out until an administrator explicitly unlocks it. • **Current configuration:** 30 minutes • **Recommended configuration:** The account should be locked out for 15 minutes.	Lior Hilel
account_lockout_reset	The Reset account lockout counter after policy setting determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0 • **Current configuration:** 30 minutes • **Recommended configuration:** The account lockout count should reset after 15 minutes.	Lior Hilel
rdp_disabled	This policy setting allows you to configure remote access to computers by using Remote Desktop Services. • **Current configuration:** Remote desktop is enabled • **Recommended configuration:** Remote desktop should be disabled if not needed for remote control	Lior Hilel
strong_ntlm_authentication	This policy setting determines which challenge or response authentication protocol is used for network logons. LAN Manager (LM) includes client computer and server software from Microsoft that allows users to link personal devices together on a single network. • **Current configuration:** Not Configured • **Recommended configuration:** Strong NTLMv2 should be enabled, Weak LM should be disabled to ensure secured communications	Lior Hilel
admin_approval_mode	This policy setting determines the behavior of Admin Approval Mode for the built-in administrator account. When the Admin Approval Mode is enabled, the local administrator account functions like a standard user account, but it has the ability to elevate privileges without logging on by using a different account. • **Current configuration:** The policy is disabled or not applied • **Recommended configuration:** The policy should be enabled.	Lior Hilel

Figure 46 Confirmation of compliance - IEC 62443

4. **Detailed asset level compliance report**-
   a detailed CSV report that consist all the compliance test performed on this asset, the mapping of those test to the various industry standards (currently in adherence of IEC 62443 & NERC CIP) ,as well as the result of each test

   Allocate the asset you want in the Site > Asset & extend the asset row.
   Press the “Additional Info” button to expand the side panel & press the export report button to reveal the report wizard which allows to generate the reports



Export compliance report

Select report type

● Confirmation of compliance - IEC 62443

○ Detailed asset level compliance report

Figure 47 Export asset level reports

Note:

- The aforementioned reports are available only if the asset was actually scanned for compliance (for additional information on how to scan for compliance see SCM User guide)
- You can easily allocate asset that underwent compliance test by the designated filter ▼ called inspected for compliance

☑ Inspected for compliance

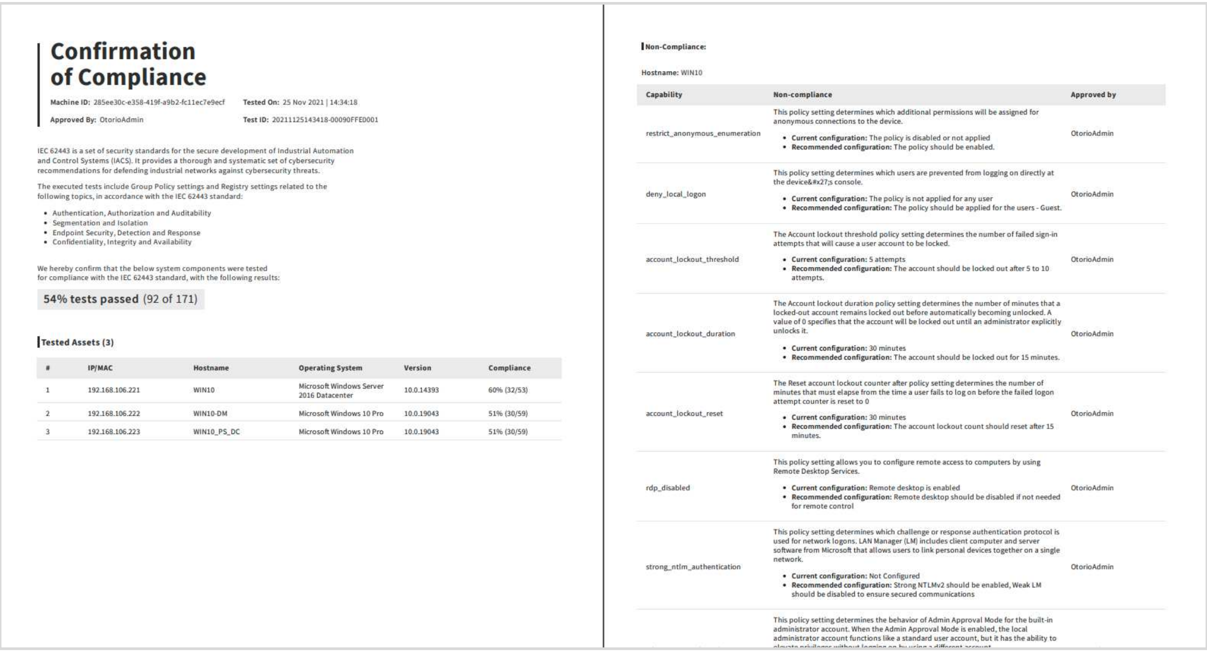
Figure 48 Inspected for compliance filter

9.2.2 Sub-unit (represent inspected machines on site)

User can export the following report types of a specific Sub-unit:

1. **Confirmation of compliance IEC 62443/NERC CIP report**-
   The following acts as an evidence of compliance of the assets in the Sub-unit in adherence to IEC 62443/NERC CIP standard (output as PDF). This report reveals all the non compliance issues exist on each asset in the Sub-unit.

Note: the report consists of only the asset in the Sub-unit that underwent compliance test



Confirmation of Compliance

Machine ID: 285ee30c-e358-419f-a9b2-fc11ec7e9ecf **Tested On:** 25 Nov 2021 | 14:34:18

Approved By: OtorioAdmin **Test ID:** 20211125143418-00090FFE0001

IEC 62443 is a set of security standards for the secure development of Industrial Automation and Control Systems (IACS). It provides a thorough and systematic set of cybersecurity recommendations for defending industrial networks against cybersecurity threats.

The executed tests include Group Policy settings and Registry settings related to the following topics, in accordance with the IEC 62443 standard:

- Authentication, Authorization and Auditability
- Segmentation and Isolation
- Endpoint Security, Detection and Response
- Confidentiality, Integrity and Availability

We hereby confirm that the below system components were tested for compliance with the IEC 62443 standard, with the following results:

54% tests passed (92 of 171)

Tested Assets (3)

#	IP/MAC	Hostname	Operating System	Version	Compliance
1	192.168.106.221	WIN10	Microsoft Windows Server 2016 Datacenter	10.0.14393	60% (32/53)
2	192.168.106.222	WIN10-DM	Microsoft Windows 10 Pro	10.0.19043	51% (30/59)
3	192.168.106.223	WIN10_PS_DC	Microsoft Windows 10 Pro	10.0.19043	51% (30/59)

Non-Compliance:

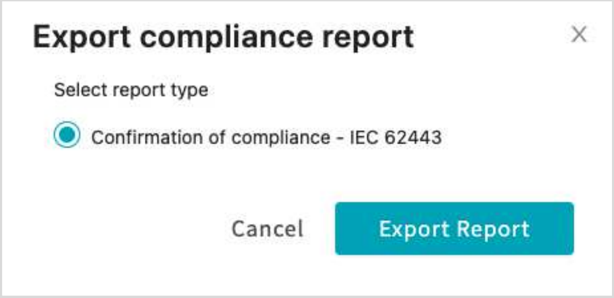
Hostname: WIN10

Capability	Non-compliance	Approved by
restrict_anonymous_enumeration	This policy setting determines which additional permissions will be assigned for anonymous connections to the device. • **Current configuration:** The policy is disabled or not applied • **Recommended configuration:** The policy should be enabled.	OtorioAdmin
deny_local_logon	This policy setting determines which users are prevented from logging on directly at the device&#x27;s console. • **Current configuration:** The policy is not applied for any user • **Recommended configuration:** The policy should be applied for the users - Guest.	OtorioAdmin
account_lockout_threshold	The Account lockout threshold policy setting determines the number of failed sign-in attempts that will cause a user account to be locked. • **Current configuration:** 5 attempts • **Recommended configuration:** The account should be locked out after 5 to 10 attempts.	OtorioAdmin
account_lockout_duration	The Account lockout duration policy setting determines the number of minutes that a locked-out account remains locked out before automatically becoming unlocked. A value of 0 specifies that the account will be locked out until an administrator explicitly unlocks it. • **Current configuration:** 30 minutes • **Recommended configuration:** The account should be locked out for 15 minutes.	OtorioAdmin
account_lockout_reset	The Reset account lockout counter after policy setting determines the number of minutes that must elapse from the time a user fails to log on before the failed logon attempt counter is reset to 0 • **Current configuration:** 30 minutes • **Recommended configuration:** The account lockout count should reset after 15 minutes.	OtorioAdmin
rdp_disabled	This policy setting allows you to configure remote access to computers by using Remote Desktop Services. • **Current configuration:** Remote desktop is enabled • **Recommended configuration:** Remote desktop should be disabled if not needed for remote control	OtorioAdmin
strong_ntlm_authentication	This policy setting determines which challenge or response authentication protocol is used for network logons. LAN Manager (LM) includes client computer and server software from Microsoft that allows users to link personal devices together on a single network. • **Current configuration:** Not Configured • **Recommended configuration:** Strong NTLMv2 should be enabled, Weak LM should be disabled to ensure secured communications	OtorioAdmin
	This policy setting determines the behavior of Admin Approval Mode for the built-in administrator account. When the Admin Approval Mode is enabled, the local administrator account functions like a standard user account, but it has the ability to elevate privileges without logging on by using a different account.	

Figure 50 Inspected for compliance filter

Allocate the Sub-unit you want in the Site > Station Sub-unit & hover on the Sub-unit card.

Press the 📄 to reveal a dialog box which allows to generate the report



Export compliance report

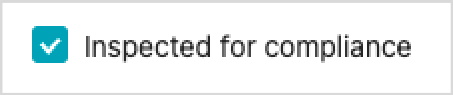
Select report type

● Confirmation of compliance - IEC 62443

Figure 51 Export asset level reports

Note:

- The aforementioned reports are available only if the asset was actually scanned for compliance (for additional information on how to scan for compliance see SCM User guide)
- You can shift the view from card to table by the designated toggle located at the right side of the screen (☰) for your convenience
- You can easily allocate asset that underwent compliance test by the designated filter ▼ called inspected for compliance



☑ Inspected for compliance

Figure 52 Inspected for compliance filter

10. Insight settings

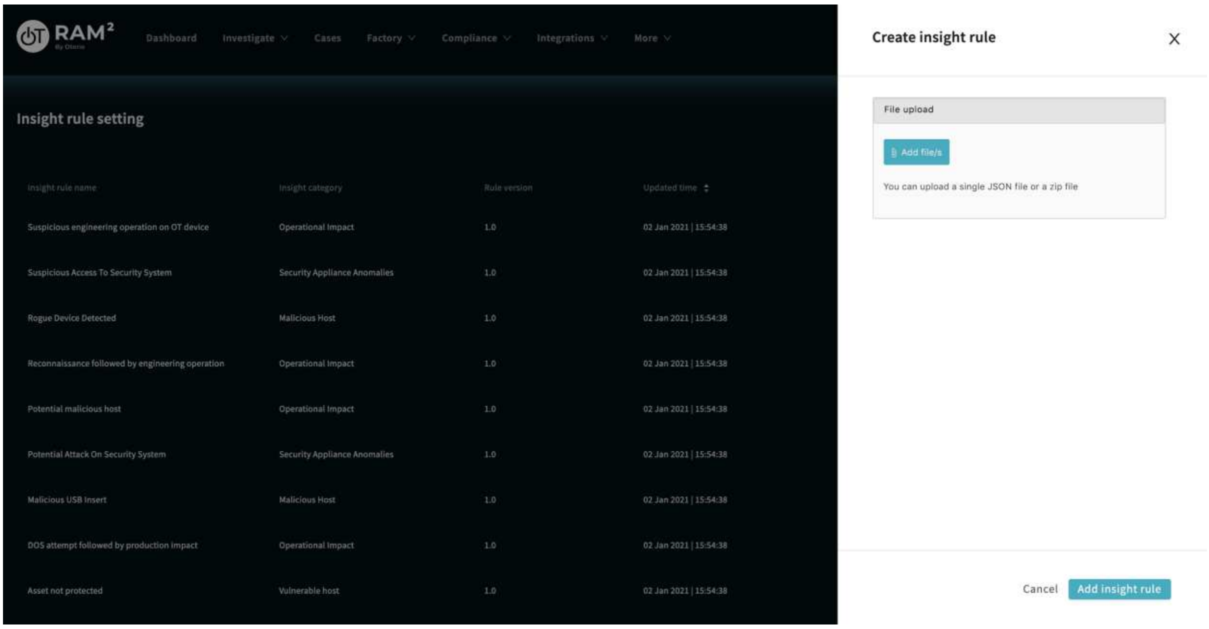
Admin users are able to define a new insight rule or update an existing one and upload it to the Central Management server. Once uploaded and enabled, insights will be generated when a proper alert arrives to the system.

10.1 Insight rule upload

A single insight rule is defined by a dedicated JSON file describing its unique name, the alerts to be considered for the insight and the logic that generates the insight. Each rule has a version number that identifies the specific combination of alerts and logic and presents the generated insight.

Insight rules are uploaded to the central management as a separated or zip file via More/Settings/Advanced->Insights Management ->add file/s button.

Once uploaded, each file is validated and the insight rule is available for use.



Insight rule setting

Insight rule name	Insight category	Rule version	Updated time
Suspicious engineering operation on OT device	Operational Impact	1.0	02 Jan 2021 | 15:54:38
Suspicious Access To Security System	Security Appliance Anomalies	1.0	02 Jan 2021 | 15:54:38
Rogue Device Detected	Malicious Host	1.0	02 Jan 2021 | 15:54:38
Reconnaissance followed by engineering operation	Operational Impact	1.0	02 Jan 2021 | 15:54:38
Potential malicious host	Operational Impact	1.0	02 Jan 2021 | 15:54:38
Potential Attack On Security System	Security Appliance Anomalies	1.0	02 Jan 2021 | 15:54:38
Malicious USB Insert	Malicious Host	1.0	02 Jan 2021 | 15:54:38
DOS attempt followed by production impact	Operational Impact	1.0	02 Jan 2021 | 15:54:38
Asset not protected	Vulnerable host	1.0	02 Jan 2021 | 15:54:38

Create insight rule

File upload

You can upload a single JSON file or a zip file

Figure 53 - insights

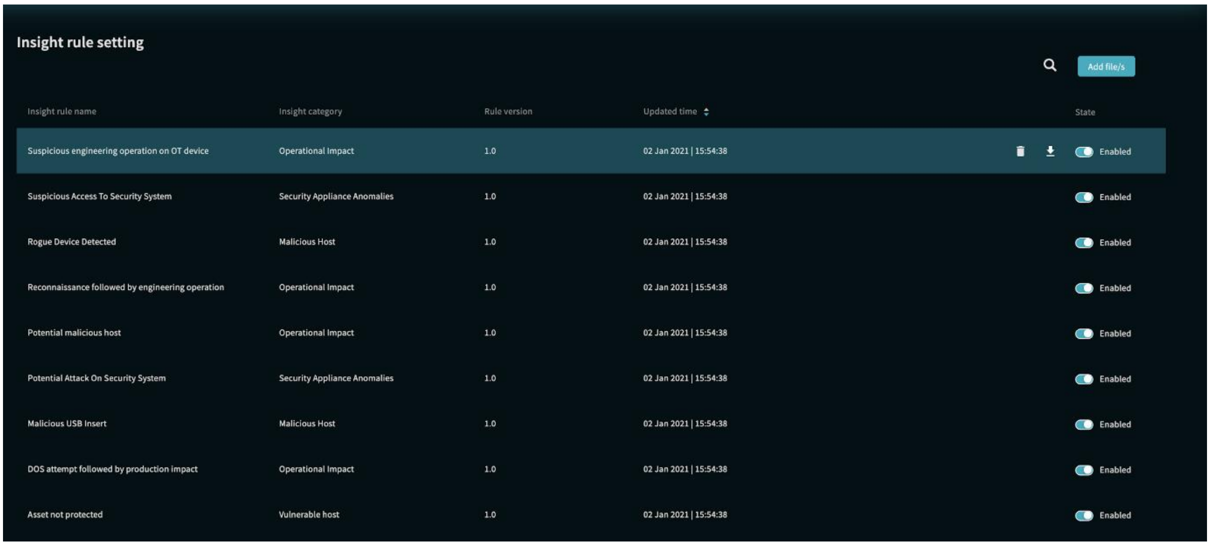
10.2 Insight rule setting

Insight rules may be enabled / disabled in the Insight rule setting page. Once enabled, each relevant alert will be matched with former alerts to generate the required insight, or extend an existing instance of it.

Generated insights are presented on the Investigate->Insights tab.

Insight rules may be disabled via the Insights Management settings page. In this case, generated insights are not affected, but new ones will not be created or extended.

Existing insight rule is available to download in order to perform specific updates on it. Version number should be in order to ensure successful rule update.



Insight rule setting

Insight rule name	Insight category	Rule version	Updated time	State
Suspicious engineering operation on OT device	Operational Impact	1.0	02 Jan 2021 | 15:54:38	Enabled
Suspicious Access To Security System	Security Appliance Anomalies	1.0	02 Jan 2021 | 15:54:38	Enabled
Rogue Device Detected	Malicious Host	1.0	02 Jan 2021 | 15:54:38	Enabled
Reconnaissance followed by engineering operation	Operational Impact	1.0	02 Jan 2021 | 15:54:38	Enabled
Potential malicious host	Operational Impact	1.0	02 Jan 2021 | 15:54:38	Enabled
Potential Attack On Security System	Security Appliance Anomalies	1.0	02 Jan 2021 | 15:54:38	Enabled
Malicious USB Insert	Malicious Host	1.0	02 Jan 2021 | 15:54:38	Enabled
DOS attempt followed by production impact	Operational Impact	1.0	02 Jan 2021 | 15:54:38	Enabled
Asset not protected	Vulnerable host	1.0	02 Jan 2021 | 15:54:38	Enabled

Figure 54 – insights rule setting

11. Users

Users require a username and password. New users can be added by the admin user.

11.1 User roles

Each user role has a different level of access to the system. The available user roles are:

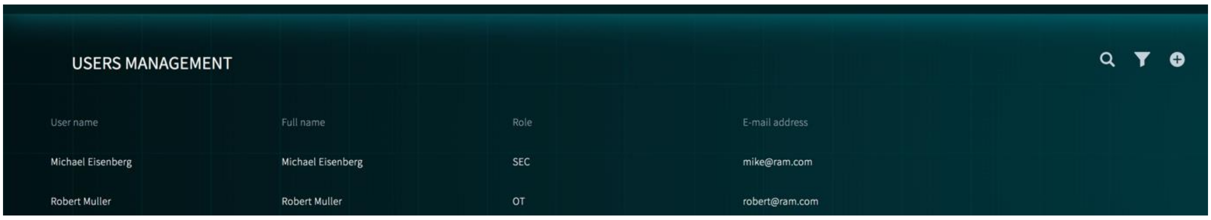
Admin – can access all pages in the central management UI, including the configuration and user management pages (can change settings and add users). Admin users can add or modify stations and Sub-units.

Operations – this user can view any page, define stations and Sub-units, and acknowledge alerts. This user cannot access the configuration pages or add/modify users.

11.2 Add users

To add a user:

1. From the top menu, select "*More/*/Settings and go to Users & Permissions/Users.
2. A list of all users and their roles are shown.

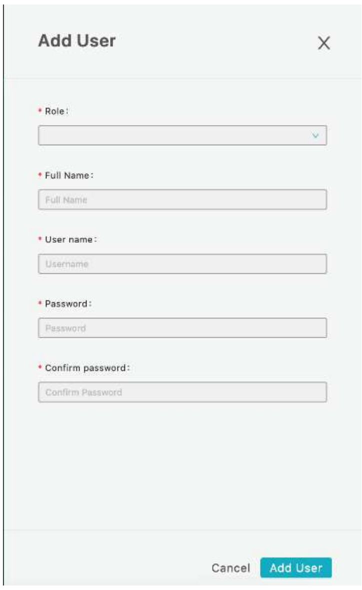


USERS MANAGEMENT

User name	Full name	Role	E-mail address
Michael Eisenberg	Michael Eisenberg	SEC	mike@ram.com
Robert Muller	Robert Muller	OT	robert@ram.com

Figure 55

3. Click ⊕ in the upper right.
4. Enter details for the new user and select the role. Note: it is suggested to provide a full name for each user as it is added to some reports when those are exported.
5. Click *Add User.*



Add User ×

* Role:
* Full Name: Full Name
* User name: Username
* Password: Password
* Confirm password: Confirm Password

Cancel | Add User

Figure 56 Add user

12. Site Configurations

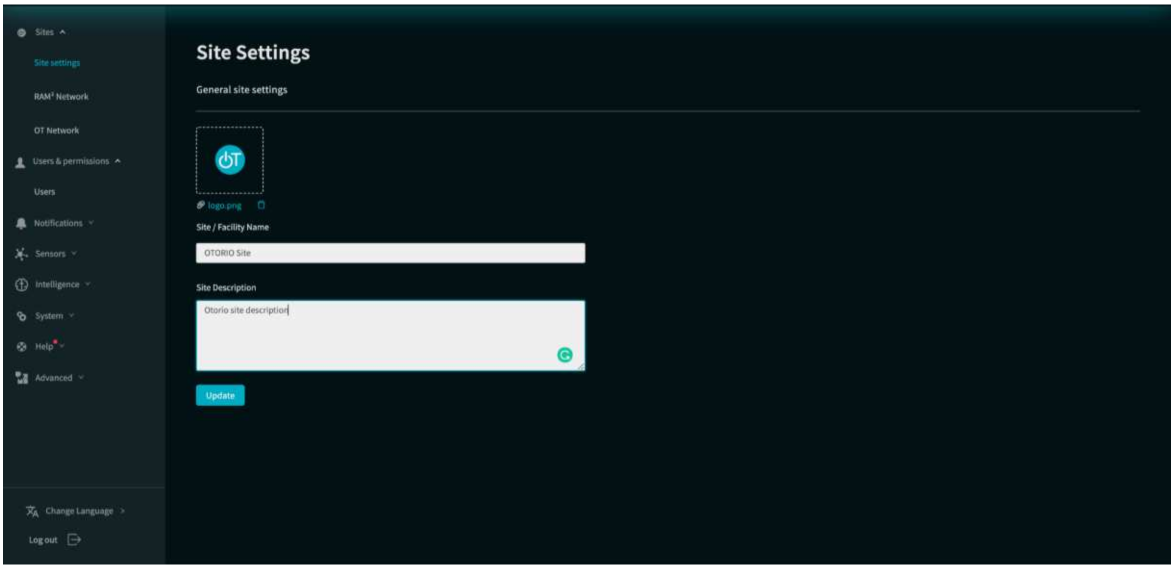
Configure the Central Management site settings by navigating to the More*/Settings/Site*

12.1 Site Settings

Configure company logo - presented at the login screen.

Configure Site name - presented in the dashboard

Configure Site description - presented in the dashboard



Site Settings

General site settings

logo.png

Site / Facility Name: OTORIO Site

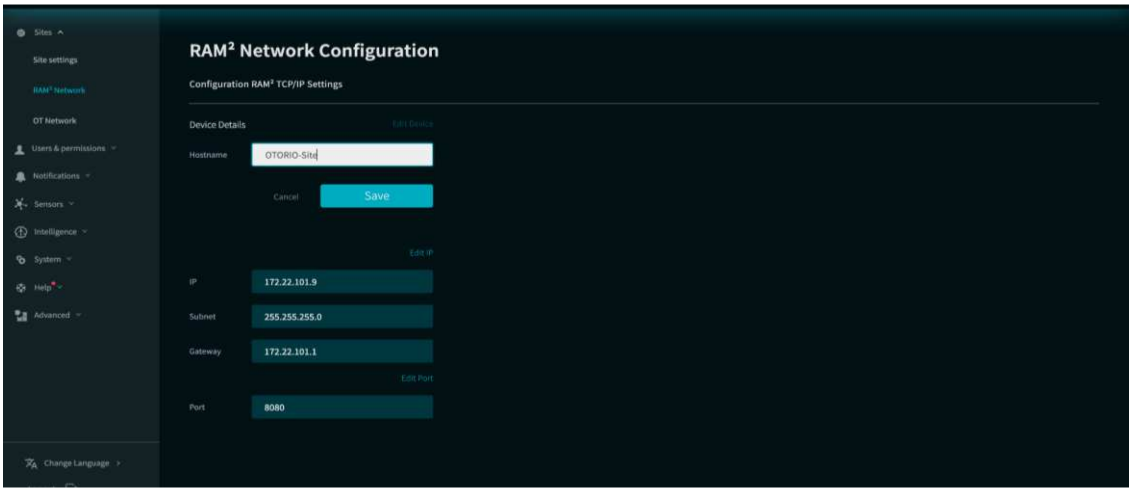
Site Description: Otorio site description

Figure 57

12.2 Network configuration

To configure the network settings:

In the *Network settings* page.



RAM² Network Configuration

Configuration RAM² TCP/IP Settings

Device Details

Hostname: OTORIO-Site

IP: 172.22.101.9

Subnet: 255.255.255.0

Gateway: 172.22.101.1

Port: 8080

Figure 58 Network configuration

Set these values:

a. Hostname - server hostname

b. IP - an IPv4 value, in the form 0.0.0.0

c. Subnet – the subnet mask, in the form 255.255.255.255

d. Gateway – the IP address of the gateway

e. Port – the port

12.3 OT Network Configuration

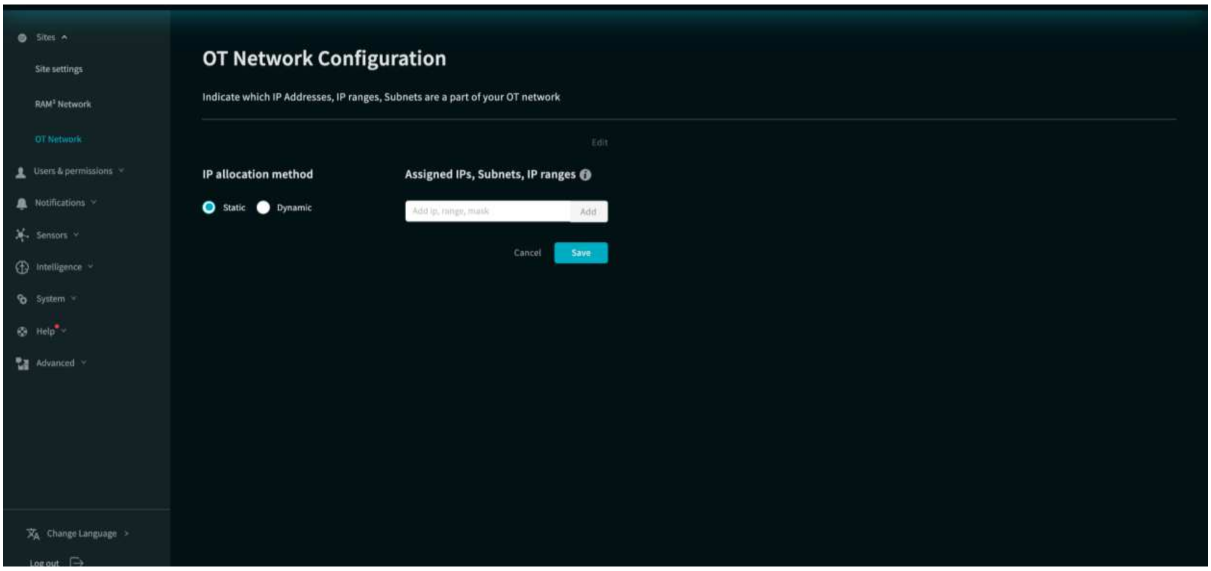
By default, the product monitors all Assets and Alerts that are provided from the various integration plugins.

To limit the monitoring to assets from specific parts of the network and alerts that relate to it:

1. In the *Configurations* page, select the *Site Configuration* tab.
2. Add all IP, IP ranges, subnet mask to be monitored in the following format:
    a. Mask 10.0.0.1/24 → Scan all IP in range 10.0.0.0 - 10.0.0.254

    b. Range 10.0.0.1 - 10.0.1.23 → meaning we need to scan all IP in range 10.0.0.1 - 10.0.0.255 + 10.0.1.0 - 10.0.1.23

    c. Single IP 10.0.0.1 → meaning we need to scan only 10.0.0.1 IP



OT Network Configuration

Indicate which IP Addresses, IP ranges, Subnets are a part of your OT network

IP allocation method

● Static ○ Dynamic

Assigned IPs, Subnets, IP ranges

Add ip, range, mask

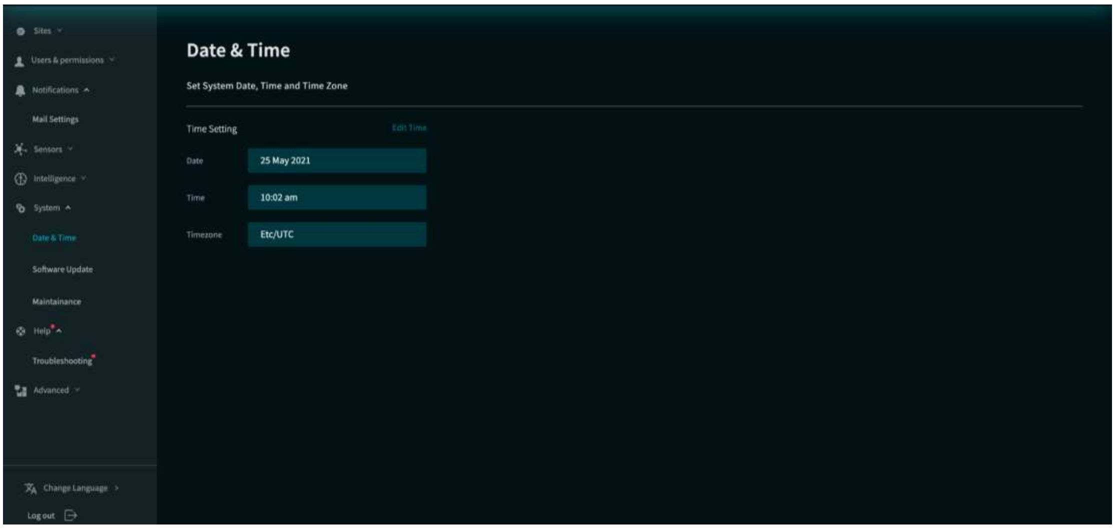
Figure 59 OT Network configuration

13. System Settings

13.1 Time

To configure the time setting:

1. Select *Date & Time Setting* page.



Date & Time

Set System Date, Time and Time Zone

Time Setting

Date: 25 May 2021

Time: 10:02 am

Timezone: Etc/UTC

Figure 60 Set time

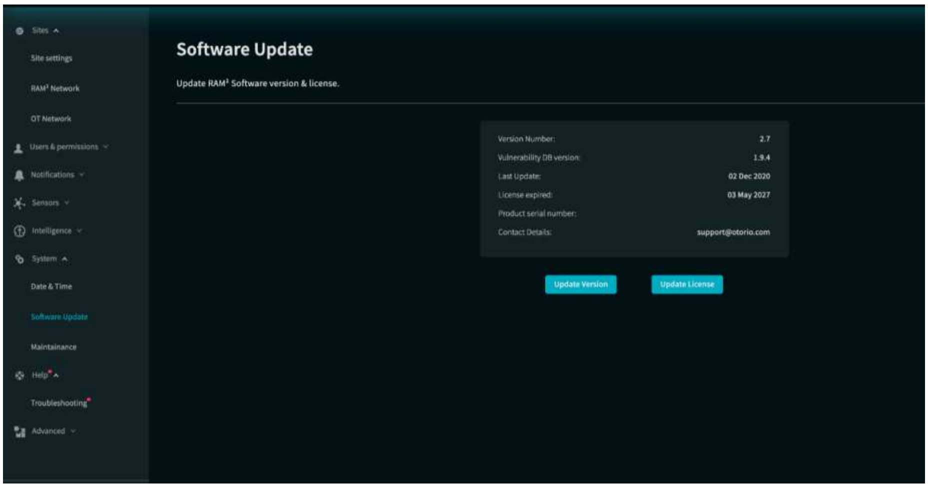
2. Edit the system time, date, time-zone.

14. License Updating

14.1 Product Licensing

The Software Updates section also includes software license information. The page shows the license expiration date. When a license requires updating, download the license update file from the Otorio web portal.

Click the Update License button on the screen, click update file and upload your license file. The panel on the screen will update with your new license expiration date.



Software Update

Update RAM³ Software version & license.

Version Number: 2.7
Vulnerability DB version: 1.9.4
Last Update: 02 Dec 2020
License expired: 03 May 2027
Product serial number:
Contact Details: support@otorio.com

Figure 61 License update screen

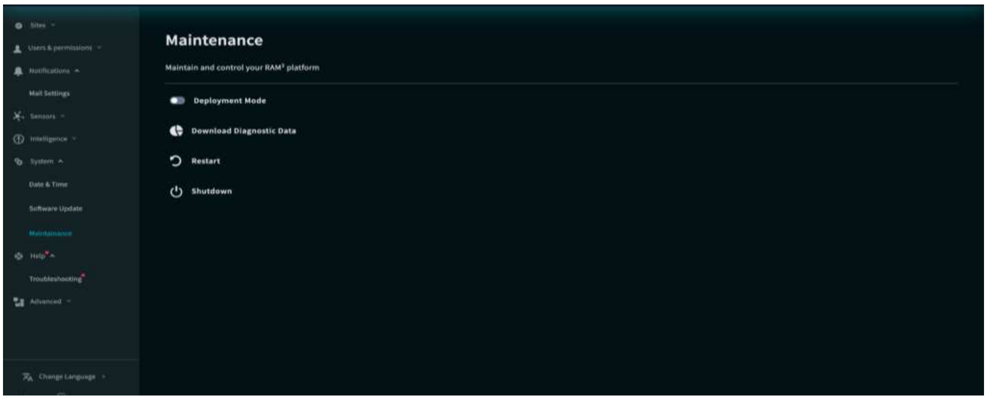
14.2 Maintenance

14.2.1 Deployment mode

The central management can be set to ignore all alerts from assets. Use this option when the product is first started after deployment, to ignore alerts from assets as they are discovered (in particular, alerts indicating ‘New Asset Discovered’). Once the central management is running, and all assets have been discovered, alerts should be re-enabled.

This control is the Deployment Mode. Set the deployment mode in the *System Settings* page.

In the *Configurations* page, select the *System* tab.



Maintenance

Maintain and control your RAM³ platform

Figure 62 System settings

14.3 Download Diagnostics Data

In case when technical support is required, click to Download Diagnostics Data and share the file with Otorio for troubleshooting.

14.4 Start & Shutdown

Restart or shut down the product from the *Systems* tab of the *Configurations* page.

Click ↻ Restart to restart or ⏻ Shutdown to shut it down.

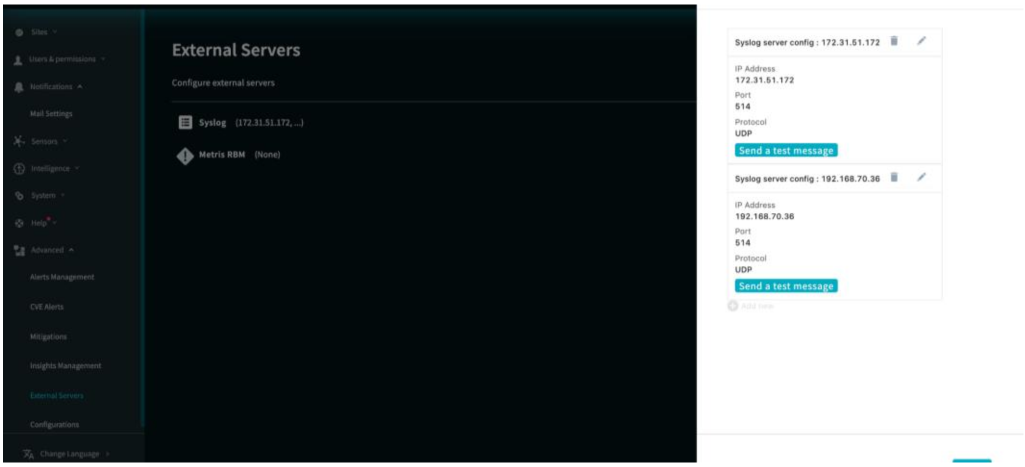
15. External Servers integrations

Configure integration with external consumers in the external *servers* page. Using the top navigation bar, click More > Settings>Advanced/External Servers to reach the page.

15.1 Central Management - Syslog configuration

Use the settings in the central management to send logs to the local Syslog server by adding the connection information in this screen.

You may add more than one Syslog server as a consumer of the system's logs.



External Servers

Configure external servers

Syslog (172.31.51.172, ...)

Metris RBM (None)

Syslog server config : 172.31.51.172

IP Address
172.31.51.172

Port
514

Protocol
UDP

Syslog server config : 192.168.70.36

IP Address
192.168.70.36

Port
514

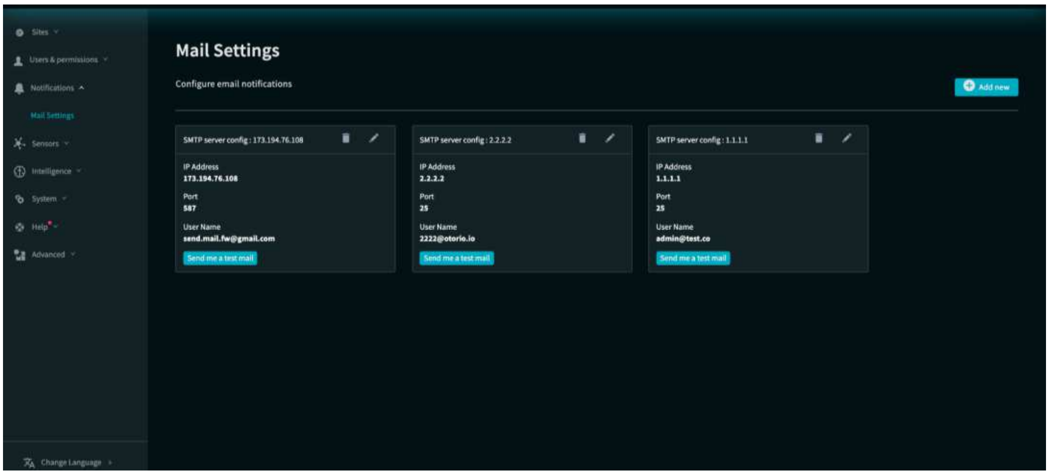
Protocol
UDP

Figure 63

15.2 Central Management - SMTP configuration

Configure the system to send email notifications by setting the SMTP server connection information.

You may add more than one SMTP server as a relay of the email notifications.



Mail Settings

Configure email notifications

SMTP server config : 173.194.76.108

IP Address
173.194.76.108

Port
587

User Name
send.mail.fw@gmail.com

SMTP server config : 2.2.2.2

IP Address
2.2.2.2

Port
25

User Name
2222@otorio.io

SMTP server config : 1.1.1.1

IP Address
1.1.1.1

Port
25

User Name
admin@test.co

Figure 64

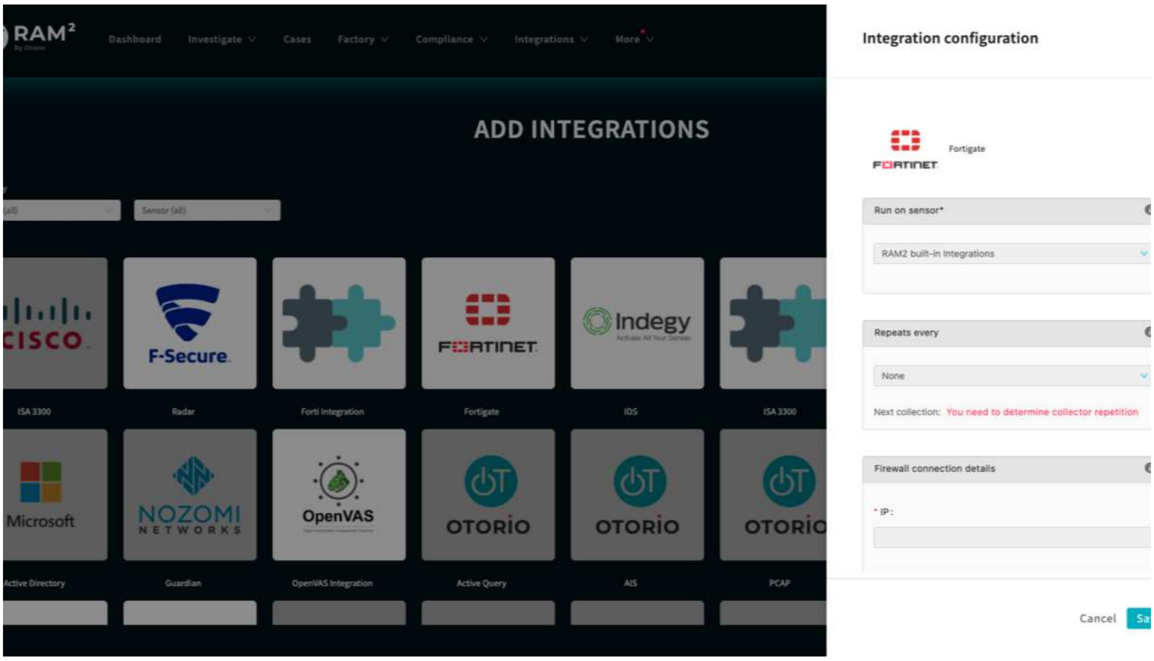
16. Integrations Plugins

The solution integrates with a variety of production floor data sources. The integrations page lists all supported data sources, sorted by vendor and product name. The list may be filtered by the data source family (firewall, EDR, IDS, Industrial Systems and more). Each of the data sources may be used for one or more purposes:

- **Asset Collection** – Collect information on the different assets that are seen or managed by the data source. This information is presented in the Site section as described above.
- **FW Rules collection** – FW configuration is the baseline for the network communication, with it the solution evaluates network activity and setup.
- **Events collection** – Most of the security and industrial systems report on suspicious events. The solution collects the important events from each data source either by Syslog or API.

The integration capabilities are dependent on the specific data source capabilities and available support.

16.1 Add Integration



Integration configuration

FORTINET Fortigate

Run on sensor*: RAM2 built-in Integrations

Repeats every: None

Next collection: You need to determine collector repetition

Firewall connection details

* IP:

Figure 65

A new data source is added by clicking on the relevant plugin icon. A matching configuration panel is opened to input the required parameters. It is possible to add several instances of the same plugin type by repeating the add function.

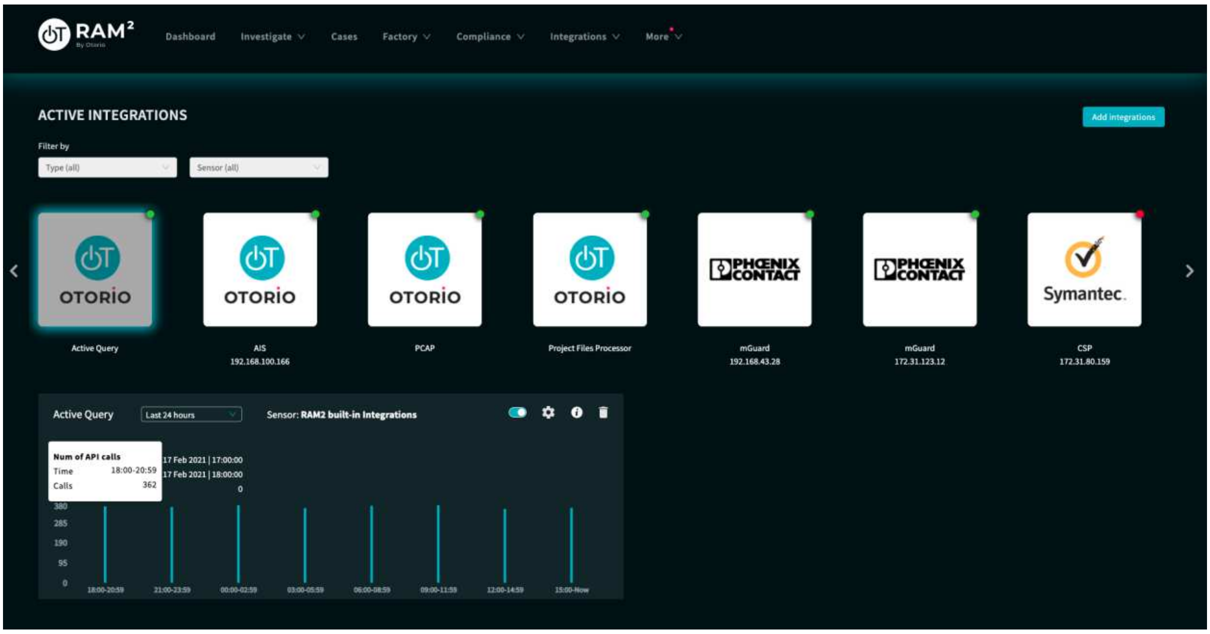
“Repeats every” section sets the frequency of assets and FW rules collection, if applicable.

“Connection details” requires one or more of the following parameters on the data source’s management: IP, port, domain, credentials with a certain permission. Also choose to collect FW Rules or security events via Syslog.

To save the settings, click on the save button, the data is saved and verified and the “Active Integrations” page is opened.

16.2 Active Integrations

On the Active Integrations page you can review the plugin’s health, by choosing the specific instance to be reviewed.



ACTIVE INTEGRATIONS

Filter by

Type (all) | Sensor (all)

Active Query

AIS 192.168.100.166

PCAP

Project Files Processor

mGuard 192.168.43.28

mGuard 172.31.123.12

CSP 172.31.80.159

Active Query | Last 24 hours | Sensor: RAM2 built-in Integrations

Num of API calls
Time 18:00-20:59
Calls 362

17 Feb 2021 | 17:00:00
17 Feb 2021 | 18:00:00
0

Figure 66

A red dot on the right-top of the tile indicates a validity check failure, meaning one or more of the parameters in plugin configuration was incorrect or the connection with the data source failed for network issues. You can review the specific issue on the troubleshooting page or click on the settings wheel to review and change the settings.

When the data source passes the validity checks, and a green dot appears on the tile’s corner, it is possible to enable the collection by the Activation Toggle. Turn-off the activation toggle will stop the data collection, while all the settings are saved.

If you wish to cancel the data source for any reason, you can choose to delete it and the setup parameters. Note that the information collected from this data source will remain in the system.

Information on the collected data appears on the graphs at the bottom of the page.

Graphs may be presented for the last 24 hours / 7 days or 30 days by using the combo box.

The API Calls graph appears when there is a data collection via API (asset or FW collection, and security events in some cases). API collection occurs according to the configured frequency, and you can see the last time the collection completed successfully, and when the next collection is scheduled. Number of alerts stands for the events that were reported by the data source. The Y axis of the graph stands for the number of successful API calls per time unit. In steady state, this number is stable and is a specific pre plugin.

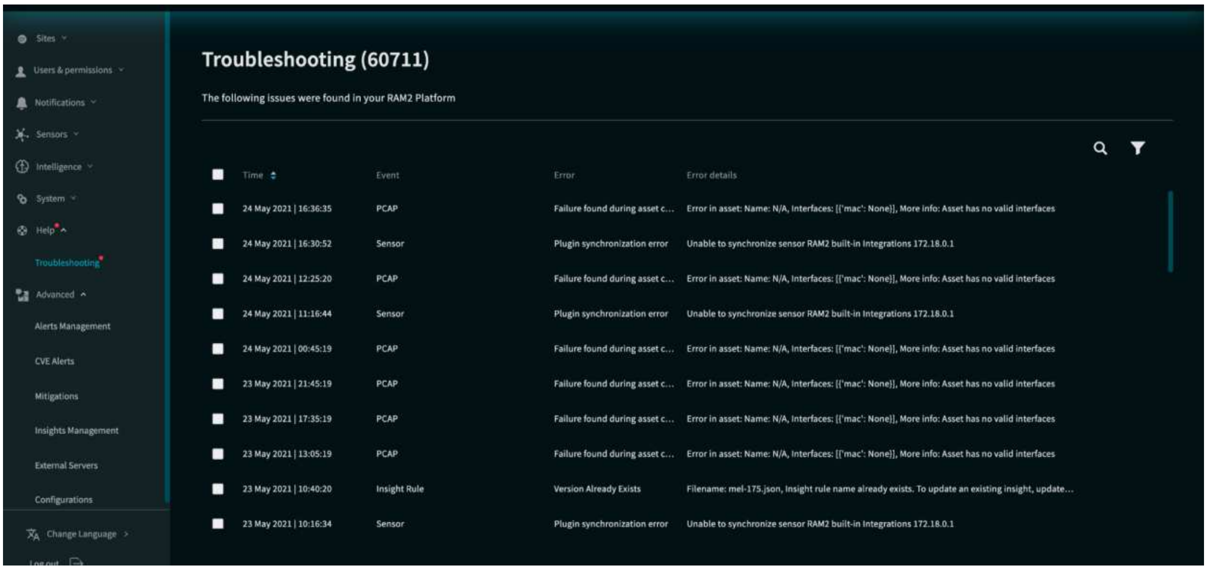
The Syslog Messages graph appears when events collection via syslog is applicable. Syslog collection is a continuous process and the level of alerts (represented by the y axis) is dependent on valid communication and the data source logic. On the Last Collection field, you may see when the data source was activated for the last time.

In order to add more data sources, click on the “Add Integration” button on the right-top corner.

17. Troubleshooting

The troubleshooting page shows errors and other events that occurred in the system (such as loss of connectivity to a specific data source). It does not show alert or other event information for site entities; this is shown in the Alerts page.

Select *More/Settings/Help/Troubleshooting*



Troubleshooting (60711)

The following issues were found in your RAM2 Platform

□	Time	Event	Error	Error details
□	24 May 2021 | 16:36:35	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	24 May 2021 | 16:30:52	Sensor	Plugin synchronization error	Unable to synchronize sensor RAM2 built-in Integrations 172.18.0.1
□	24 May 2021 | 12:25:20	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	24 May 2021 | 11:16:44	Sensor	Plugin synchronization error	Unable to synchronize sensor RAM2 built-in Integrations 172.18.0.1
□	24 May 2021 | 00:45:19	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	23 May 2021 | 21:45:19	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	23 May 2021 | 17:35:19	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	23 May 2021 | 13:05:19	PCAP	Failure found during asset c...	Error in asset: Name: N/A, Interfaces: [{'mac': None}], More info: Asset has no valid interfaces
□	23 May 2021 | 10:40:20	Insight Rule	Version Already Exists	Filename: mel-175.json, Insight rule name already exists. To update an existing insight, update...
□	23 May 2021 | 10:16:34	Sensor	Plugin synchronization error	Unable to synchronize sensor RAM2 built-in Integrations 172.18.0.1

Figure 67 Troubleshooting

Users can filter the list for specific errors or events.

Click Delete all to remove all entries in the list.

18. Appendix

18.1 Alert categories and types

Alerts describes preparedness and security issue under the following categories:

Asset Inventory - Keep track of the equipment and inventory status. Alert types: New asset discovery, changes in asset state, asset compliance and more.

Host Security - Monitor devices with a remote connecting to the network that creates a potential entry point for security threats Alert types: Malware detected, EDR status, Host policy violation and more.

Network Security - Monitor network activities and identify or prevent unauthorized access, misuse, modification, or denial of the network and network-accessible resources. Alert types: Suspicious authentication, potential attack on security appliances, network segmentation and more.

User Privileges and Behavior - Keep track of suspicious user access to various resources and user behavior anomaly.

Vulnerability Management and Threat Intelligence - Identify, classify, prioritize, and mitigate ICS vulnerabilities on your assets.

Remote Connection Activities - Monitor remote access to your network that are potentially involved in malicious activity.

Additional alert categories, types and subtypes may be defined in the system by the OTORIO team, to allow new integration plugins to report alerts of the new types.

18.2 Data source types

EDR - EDR covers a single host security status and monitoring, connecting it to the solution provides information on Windows endpoints and servers so the user is able to see the related vulnerabilities for each device, monitor EDR coverage and be informed on malware activity and various suspicious actions on the that are considered a malicious activity indicators.

Firewall - Firewalls covers the network aspect of the site, connecting it to RAM^2 covers Windows & Linux endpoints/servers and HMI devices, as well as the FW management itself, allowing monitoring of network activities, network segmentation, network attacks and network policy violations that are performed by a device in the network or towards it.

IDS / IPS - IDS connection to RAM^2 provides a vast asset inventory - I/O devices, Controllers, HMIs and Windows/Linux endpoints and servers, allowing RAM^2 to monitor asset state (PLC stop / start), network attacks and network policy violation.

Industrial Systems - Industrial systems connection to RAM^2 mainly supports asset inventory for HMI, Controllers and I/O devices and the ability to monitor asset configuration (change in IP / firmware)

Vulnerability / patch management - Vulnerability / patch management systems assists with Windows and Linux endpoints and servers discovery and monitoring and IT vulnerabilities coverage for it.

User Management / AIM - Active Directory connection to RAM^2 provides information on misconfigured users and groups and allows policy enforcement on it.

Secure Remote Access - Secure Remote access systems provide RAM^2 with the ability to monitor network policy violations that are performed over the network.

19. Bibliography

(1) SEAFTY4RAILS Project, Deliverable D1.4

(2) RAM2 user manual, Otorio 2022

SAFETY4RAILS

Partners:

Fraunhofer EMI

uic

Metro de Madrid

EGO Genel Müdürlüğü

RFI RETE FERROVIARIA ITALIANA GRUPPO FERROVIE DELLO STATO ITALIANE

LEONARDO

ceis avisa partners

STAM MASTERING EXCELLENCE

TCDD

IC information company

RMIT UNIVERSITY

University of Reading

etra I+D

DEMOKRITOS NATIONAL CENTRE FOR SCIENTIFIC RESEARCH

RINA

WINGS ICT SOLUTIONS

Newcastle University

EOS EUROPEAN ORGANISATION FOR SECURITY

IN Innova Integra

LAUREA AMMATTIKORKEAKOULU University of Applied Sciences

CyberServices MADE IN EUROPE

FGC Ferrocarrils de la Generalitat de Catalunya

erarGE

MTRS

INTRACOM TELECOM

UNIVERSITAS Miguel Hernández

TREE TECHNOLOGY

Elbit Systems™ C⁴I and Cyber

ProRail

Comune di Milano

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.