# Introduction

## Overview

The Otorio Risk Assessment Monitoring & Management platform, RAM2, is an industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. The RAM2 offers a comprehensive, centralized, simplified, and automated industrial cyber risk management solution.

RAM2 easily integrates a variety of production floor data sources (e.g. OT, IT, security logs and network data) and provides actionable views of factory 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 day-to-day tasks.

In RAM2 you can perform the following tasks

* Create a logical hierarchical structure for the factory, with shops, cells & assets
* physical assets assign them to shops and cells the factory
* updated
* Calculate the Risk Level for each asset, cell, and shop, based on the vulnerabilities discovered in the assets, and the impact levels
* if vulnerabilities are found
* Easily view KPI and detailed information about the risk levels of the factory and its components

## Main Features

### Factory Management

RAM2 manages security for assets (such as shop-floor machines) in a single factory.

The factory is divided hierarchically into the following entities:

**Factory** – a single business or industrial unit, but can be distributed over several geographical locations

**Shop** –an element of a factory, in which specific activities are performed

**Cell** – a production unit in a shop

**Asset** – a single machine or device in a cell

In RAM2, you first define the shops in the factory. After this, you define production cells, and assign them to shops.

RAM2 receives information about assets in the factory from Asset Collectors. Using this, it builds a list of assets. This list is updated regularly, based on updated information from the Asset Collectors. The information includes details about the device type, and the firmware/software installed on it.

Newly discovered assets are not assigned to cells. This you do, manually, in RAM2.

RAM2 calculates a Risk Level for each asset, based on the information it receives about the assets from Asset Collectors, and using an internal threat intel database of known vulnerabilities. It then calculates the Risk Level for cells and shops, based on the Risk Levels of the component assets.

RAM2 also has views to show the security and risk status of the factory, shops, cells, and assets, as well as alerts that are generated when security issues are found in the course of a scan.

### Risk Assessment

* Calculate risk for assets per vuln
* Calculate risk for cell & shop per assets.
* Internal algorithm

### Alerts

RAM2 generates alerts for security issues discovered in assets in the course of a scan. The alert indicates the severity of the issue, and details for it (such as the specific vulnerability for the issue). There are filterable views to see alerts for shops, cells and assets, or for specific risk levels or vulnerabilities.

You can acknowledge an alert for a specific asset.

### Manage Vulnerabilities-

RAM2 assesses the risk level for an asset using a list of vulnerabilities compiled by the Otorio threat intelligence research team, and based on published open source vulnerabilities, industrial best practices, etc.

You can view the list of vulnerabilities, and filter views and alerts according to specific vulnerabilities. You can also disable specific vulnerabilities, in which case, asset scans will not report or show on issues relating to them.

## Key Indicators

The top of the Dashboard shows key indicators for the factory.



Figure 5 Key Factory Indicators

These are:

* The number of shops
* The number of cells in the factory
* The total number of assets in the factory

# The

the shops factory, as well as key summary information for the factory as whole

The left side shows a list of the shops in the factory.

Select one of the shops, to see information for it.

* t
* the number of production cells in the shop
* t
* t

a pie-chart distribution of s

pie-chart

There are four different Risk Levels: Critical, High, Medium, and Low.

in the pie-chartThis is shown on the right.

t

A shop marked with a red dot indicates there are alerts for one or more assets in the shop.



in the shop,

generated for assets in the shop,

In this view, there is no overall Risk Level

Click , on the right, to open the list of Unassigned Assets. There, you can view details for the assets, and assign them to production cells.

## Navigation from the Dashboard

At the top of every page, including the Dashboard, is the top-level menu-bar.



Use these menus to navigate to different pages in RAM2, to perform the actions discussed in later sections.

Dashboard – navigate to the Dashboard

Investigate –navigate to the Alerts page

Factory –navigate to the Shops, Production Cells, and Assets pages

More – navigate to the Configuration, and Troubleshooting pages

You can also click  to return to the Dashboard from any other page.

## Login to RAM2

Connect to RAM2 from a browser, with the URL for your RAM2 server.

Enter your username and password.

Once you are logged, the Dasbhoard view will open.

### First steps

The first time you are logging into RAM2, there are no shops or cells. If assets have been discovered, there will be a list of Unassigned Assets.

Your first steps at this point will be to create shops, and cells, and, after this, to assign assets to cells. These steps are described in the next section.

# Factory Management

In RAM2 you can define shops and production cells for your factory.

RAM2 creates a list of assets automatically, based on information received from Asset Collectors in the factory.

In RAM2, you can assign cells to shops, and then assets to cells.

## Shops

Shops are the highest-level entity in a factory.

### Shop view

Select Shops from the Factory menu to see the shops you have defined for the factory.

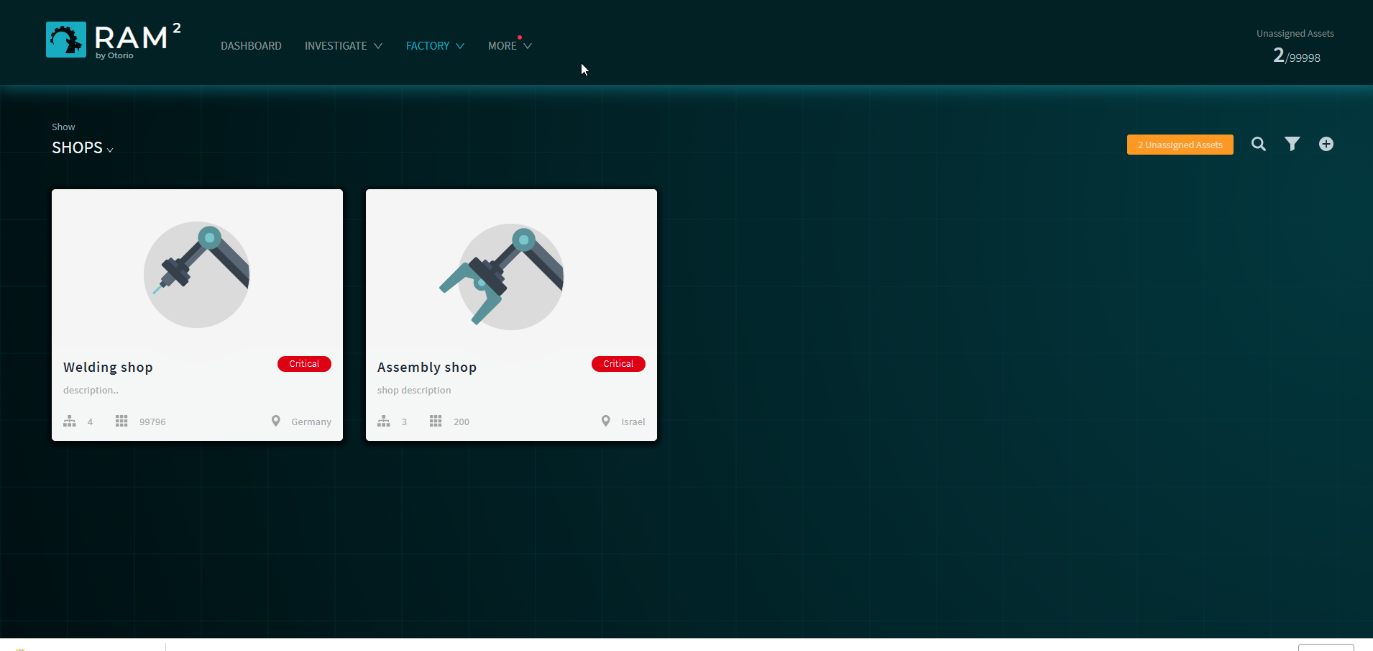


Figure 8 Shops

Each image in this view represents a shop, and shows the following information for it:

* the overall shop Risk Level
* the number of cells
* the number of assets
* the geographic location of the shop

### Create shop

Add or modify shops in the factory, in the Shops page.

To add a new shop:

1. Select Shops from the top-level Factory menu. A list of all shops in the factory is shown.
2. Click .
3. In the Create New Shop panel, enter the following:
4. **Shop name & description** – the name for the shop in RAM2, and a description of it; this is free text
5. **Location** – the geographic location of the shop
6. **Image** – (optional) upload an image for the shop.

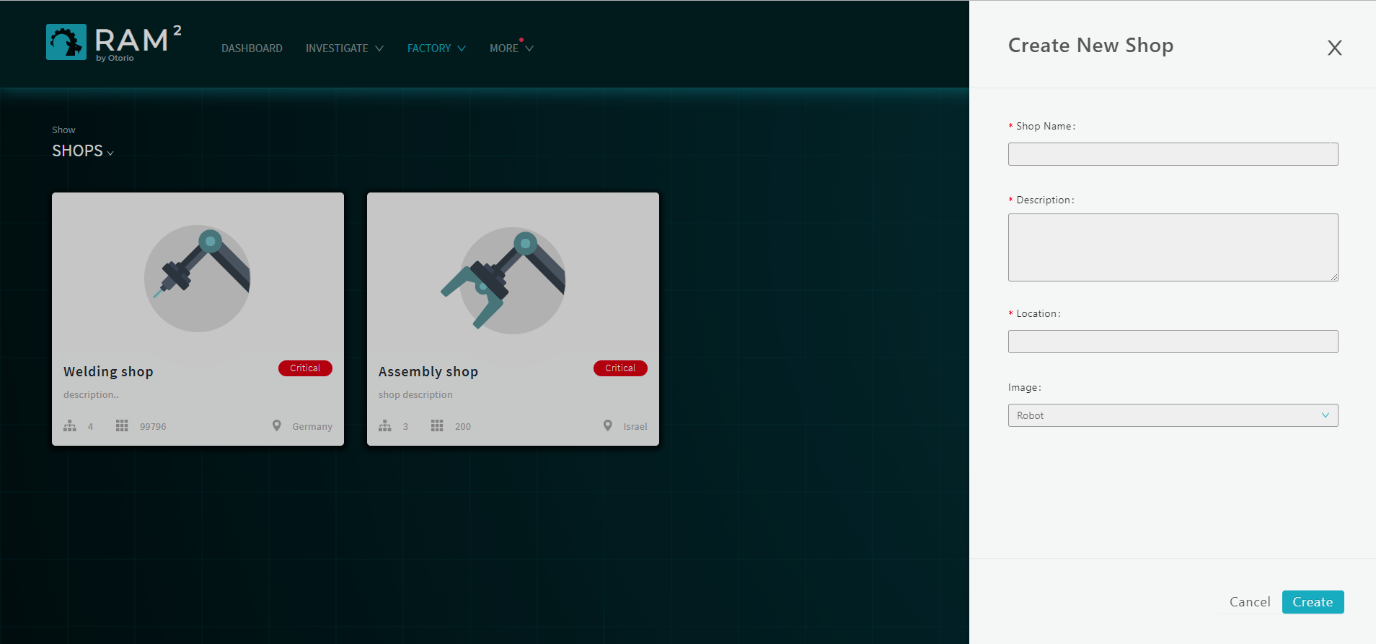


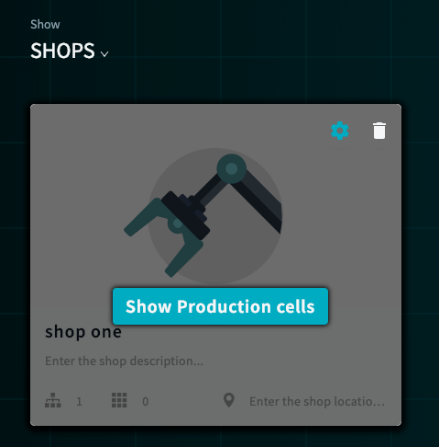
Figure 13 Create new shop

1. Click Create.

The new shop will appear on the page.

To modify details for a shop:

1. In the Shops page, hover over the image of the shop to be modified.



1. Click .

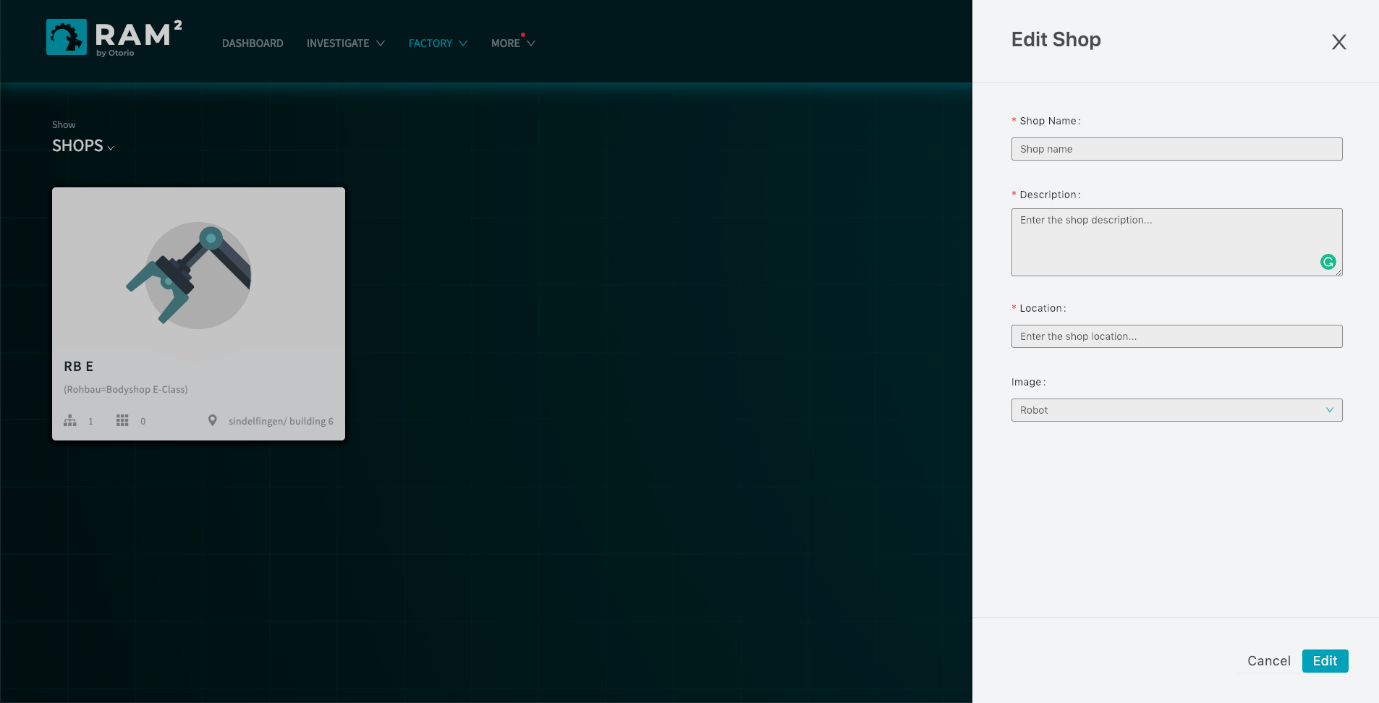


Figure 14 Edit shop

1. In the Edit Shop panel, make changes to the shop details, as necessary, and then click Edit.

### Create production cells for a shop

### Actions/Navigation from Shop view

* Cells
* Unassigned assets

### Filter or Search the views

You can filter or search the Dashboard views in RAM2 to select specific items of interest.

Click  to select the filter for the view. The options vary according to the view, but the filter panel on the right is common.

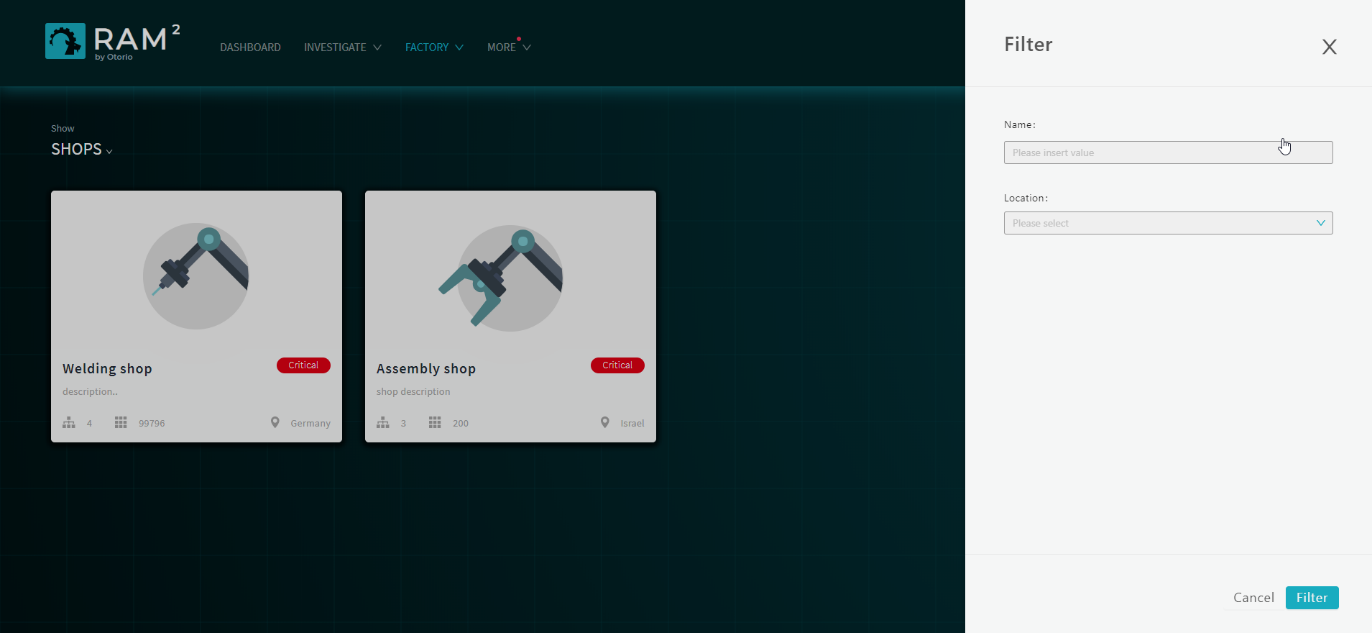


Figure 12 -– Filter

## Cells

Production Cells are entities within shops. A cell can be assigned to a single shop.

### Cells view

Click on a shop to show the production cells in it. Alternatively, select Cells from the top-level Factory menu, to show all the cells in the factory.

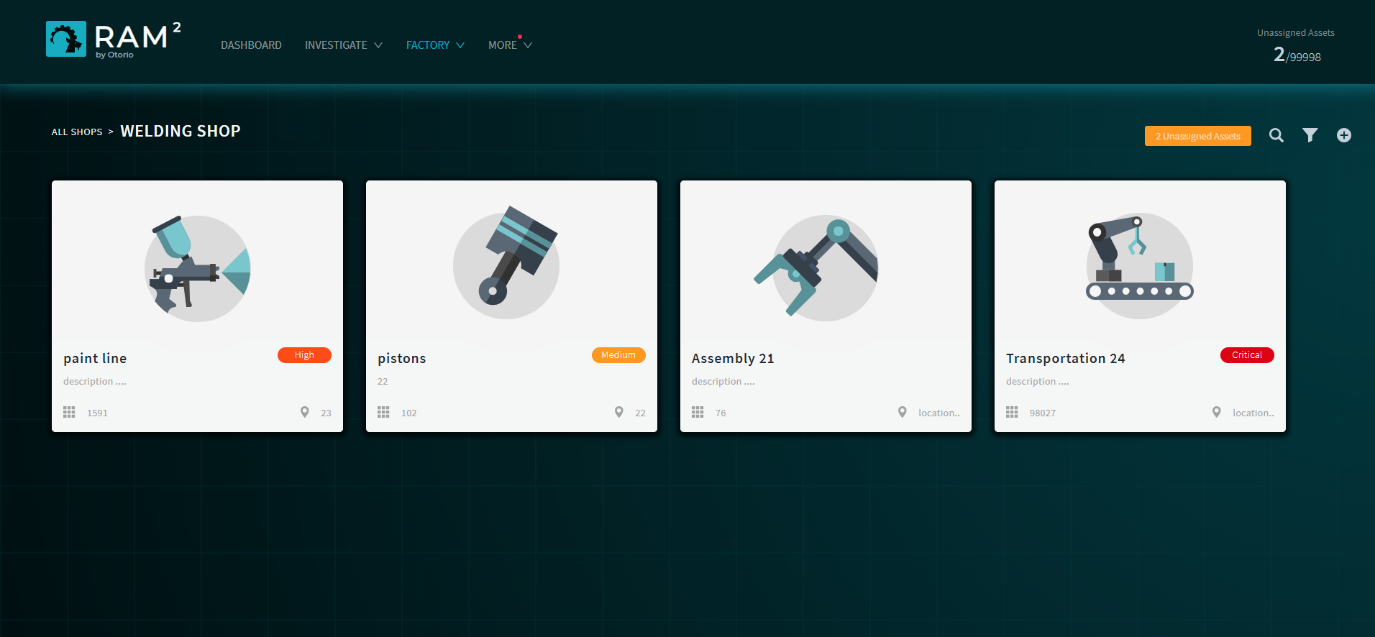


Figure 9 Shop cells

Each image in this view represents a production cell, and shows this information:

* the overall Risk Level for the cell
* the number of assets
* the location of the cell

### Create Cells

Add or modify cells in the Production Cells page. Select Production Cells from the top-level Factory menu. When you create the cell, you assign it to a shop. Alternatively, you can add a cell from the Shops page for a specific shop, in which case the cell, once created, is assigned to this shop.

To create a cell:

1. Select Production Cells from the top-level Factory menu. A list of all cells in the factory is shown.
2. Click .
3. In the Create New Production cell panel, enter the following:
4. **Cell name & description** - the name for the cell in RAM2, and a description of it; this is free text
5. **Location** - the geographic location of the cell
6. **Shop** – the shop with which the cell will be associated (from a list)
7. **Image** – upload an image for the cell

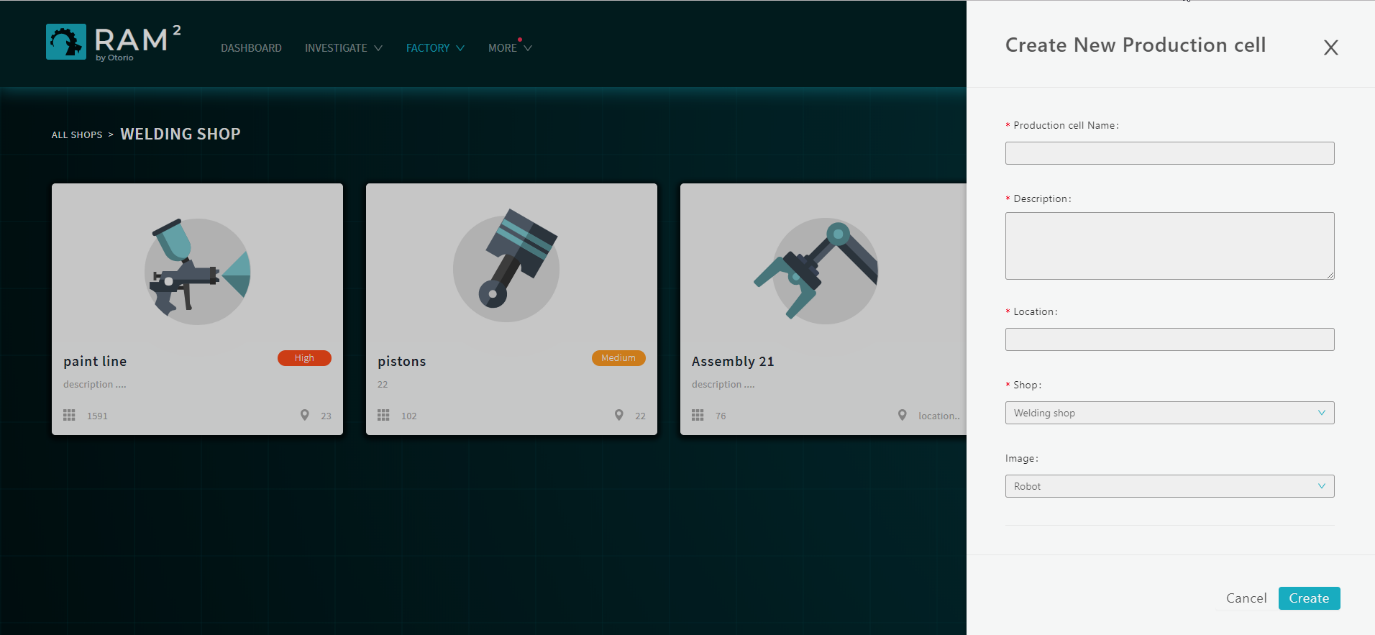


Figure 15 Create production cell

1. Click Create.

The cell will appear on the Production Cells page, and also as one of the cells in the Shops page to which it was assigned.

To create a cell in a shop:

1. In the Shops page, select the shop to which the cell will be added. The current cells for this shop will be shown.
2. Click .
3. In the Create New Production cell panel, enter the following
4. Cell name & description - the name for the cell in RAM2, and a description for it
5. Location - the geographic location of the cell
6. Image – upload an image for the cell
7. Click Create.

The cell will appear in the page for the cell.

### Modify cells

### Assign cells to shops

### Change assignment to shop

When you create a cell, it is assigned to a shop. You can change the shop to which it is assigned by editing the cell details.

To change the Shop for a Cell:

1. Select the Shops page for the shop containing the cell.
2. Hover over the cell to be moved, and click .
3. In the Edit Production Cell panel, select the new Shop from the list.
4. Click Edit.

### Actions/Navigation from the Cell view

* assets

factory

Assets are individual shop-floor machines. They are discovered automatically (for example, using the MSB). You can assign them to production cells once they are discovered, or move them to different cells.

Once discovered, RAM2 assesses a Risk Level for them.

Once they are assigned to a cell, their Risk Level contributes to the overall Risk Level of their assigned cell and shop.

factory

### Assign assets to cells

You can assign an asset to a cell from the Assets page. Select Assets from the top-level Factory menu. This will show a list of all the assets in the factory (assigned and unassigned). Filter or search for the assets to assign to a cell. For example, to assign newly discovered unassigned assets, filter for Unassigned assets.

To assign a single asset to a cell:

1. Hover over the asset in the list.

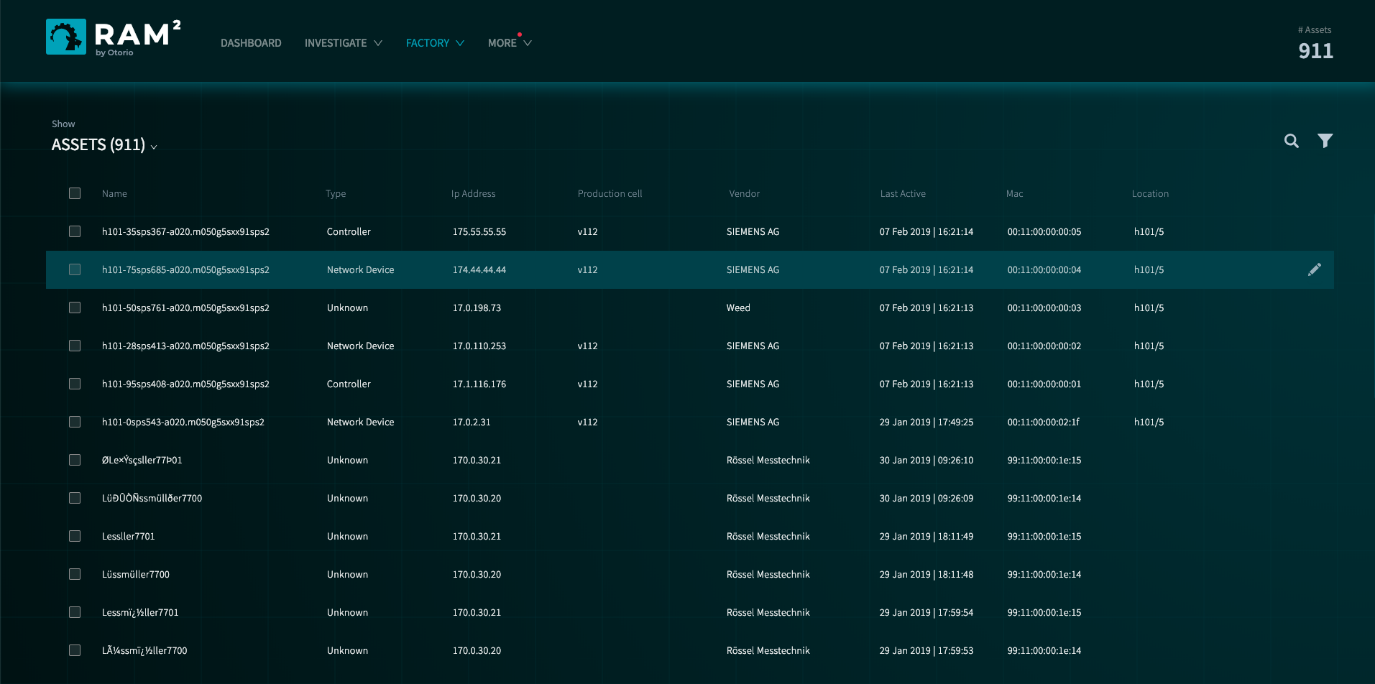


Figure 16 Select an asset to assign

1. Click  (on the right side).

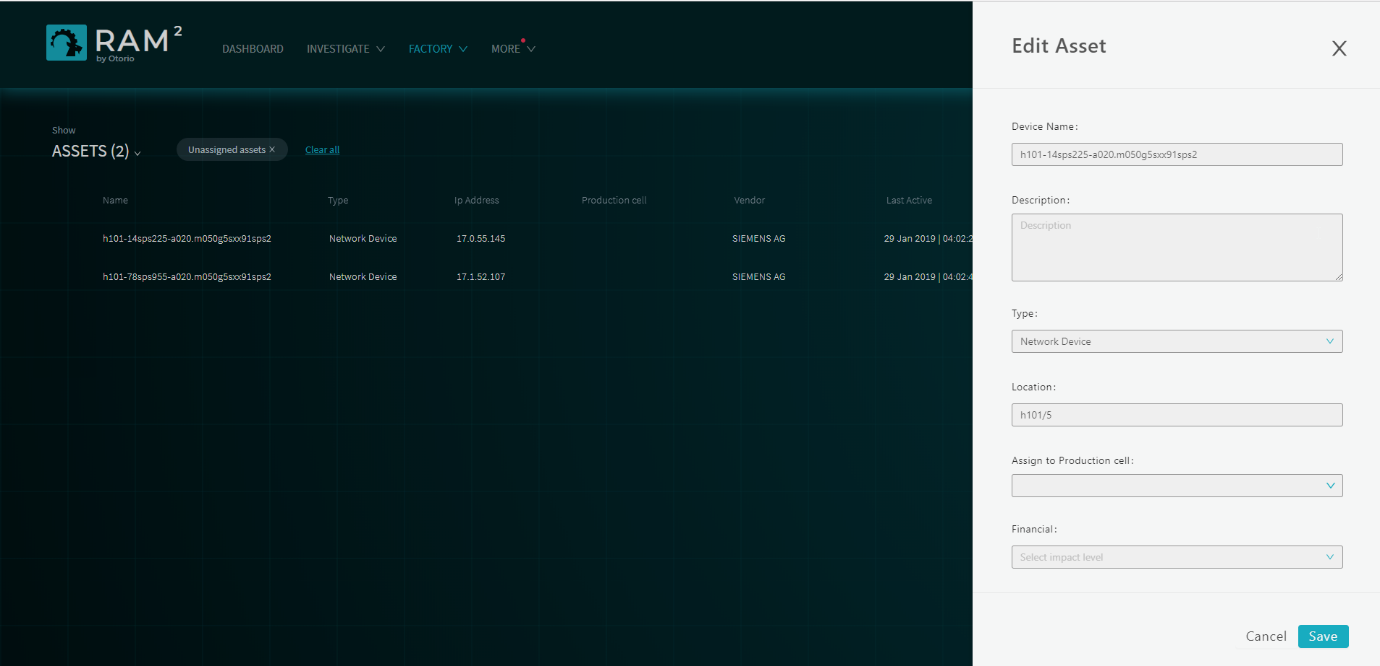


Figure 17 Assign an asset to a cell

1. In the Edit Asset panel, select the production cell from the list.
2. Click Save.

### Bulk assign assets to cells

To asset a number of assets at once:

1. Select the assets in the list, and then .

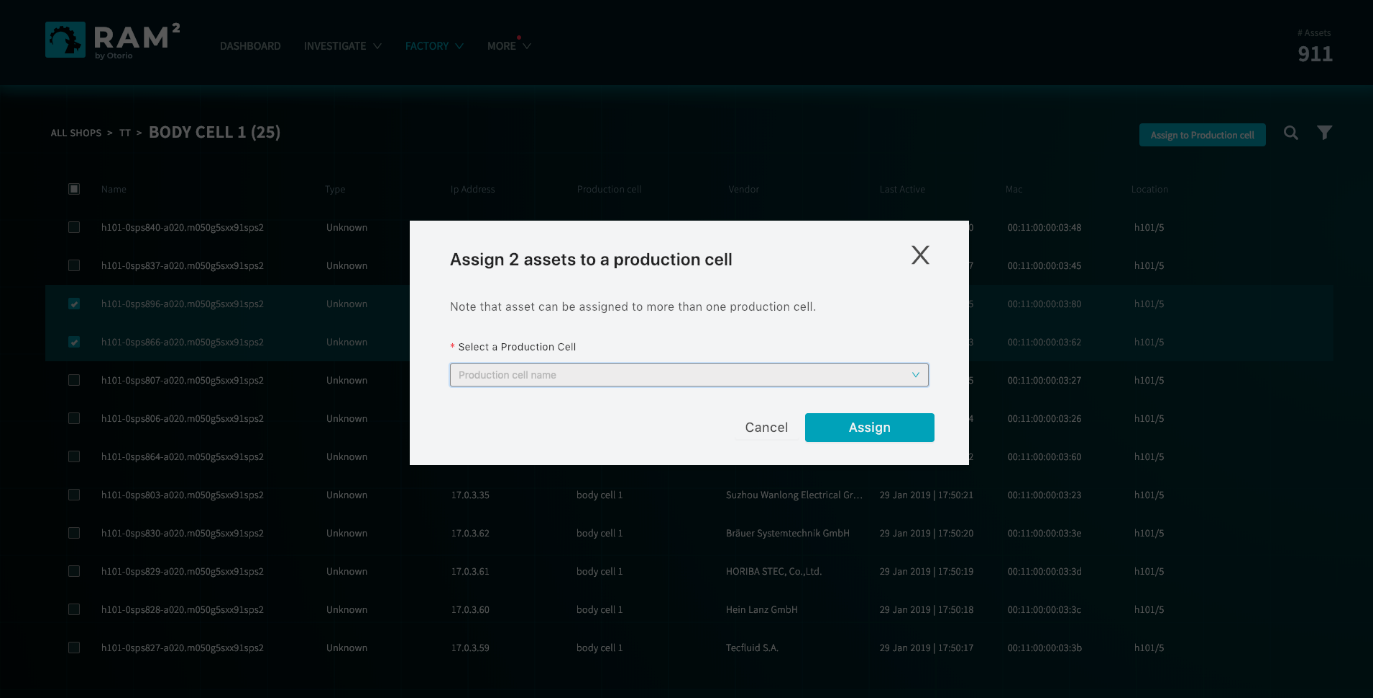


Figure 18 Assign multiple assets to a cell

1. Select the production cell from the list.
2. Click Assign.

# Alerts

RAM2 generates alerts when security issues are discovered in assets after they are scanned. These alerts are shown in the Alerts view.

You can perform the following actions on alerts, from the Alerts page.

* View details for the alert, and the asset affected.
* View the distribution of alerts according to alert type or production cell.
* Acknowledge the issue in the alert
* Disable specific vulnerabilities from generating alerts.

## View alert details

## View alert distribution

## Acknowledge alerts

You can acknowledge an alert for a specific asset. The Alerts page will indicate the alert is acknowledged in the Acknowledged column. Once an alert is acknowledged, future alerts of this type for this asset will not be shown. This can help to declutter the display.

To acknowledge an alert:

1. On the Alerts page, select the alert.
2. Click  opposite the alert
3. Enter an explanation why the alert is being acknowledged. This text will be saved with the alert, and visible to others (for example, in reports).

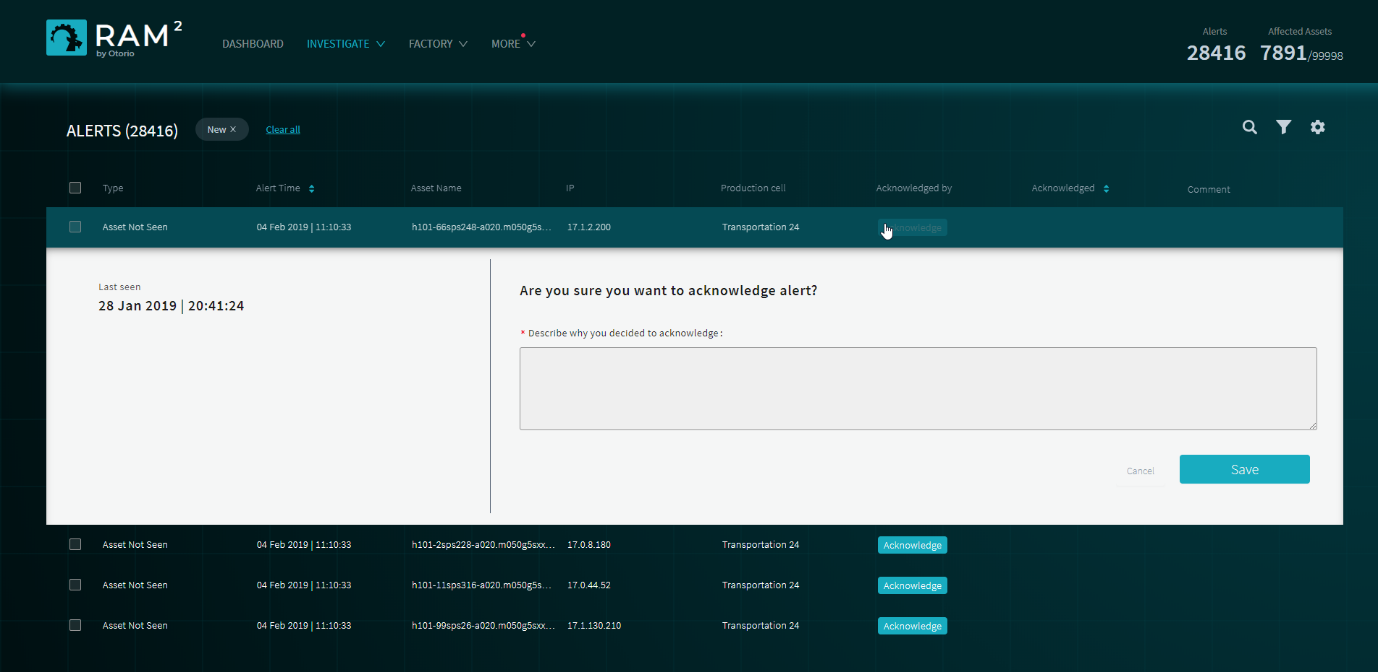


Figure 19 Acknowledge an alert

1. Click Save.

To acknowledge a number of alerts:

1. On the Alerts page, select the alerts to acknowledge
2. Click  at the top of the page.
3. Enter an explanation why the alerts are being acknowledged.
4. Click Save.

Acknowledged alerts will show the name of the user who acknowledged them, on the Alerts page.

## Disable vulnerabilities

You can manage the list of vulnerabilities that the RAM2 maintains, and select which ones will generate alerts, and which will be ignores. This applies to all assets.

When you disable a vulnerability, all alerts issued for that vulnerability (that appear in the Alerts page) are acknowledged.

To disable a vulnerability:

1. In the Alerts page, click .
2. In the Vulnerability alerts management panel, disable alerts for which you do not want to receive alerts.

You can enable a disabled vulnerability in the same way. Once a vulnerability is enabled, alerts for it will be issued.

## Examples

### View alerts by Asset, Cell or Shop

### View by Vulnerability (CVE)

### View details (KPI)

### Acknowledge an alert

### Investigate alerts

### Disable a vulnerability

# Users

You must login to RAM2 with a username and password.

Admin users of RAM2 can create users within RAM2.

## User types

* Admin & regular

## Add users

# Configuration

You can configure the RAM2 server settings in the System Settings page. Select this from the top-level More menu.

## Network config

To configure the RAM network settings:

1. Select System Settings from the top-level More menu
2. Select the Network Configuration tab
3. Set these values:
4. IP - an IPv4 value, in the form 0.0.0.0
5. Subnet – the subnet mast, in the form 255.255.255.255
6. Gateway – the IP address of the gateway
7. Port – the port

## Time

To configure the RAM2 time setting:

1. In the System Settings page, select the Time Setting tab
2. Enter the system time (local time).

## Deployment mode

Turn on the deployment mode switch when RAM2 is started up. When this switch is on, RAM2 will ignore all alerts from assets as they are being discovered (in particular, alerts indicating ‘New Asset Discovered’). Once all the assets have been discovered and scanned, turn off the switch, and RAM2 will accept new alerts from assets.

## Start & Shutdown

### Startup RAM2

### Shutdown RAM2

### Export/Import settings

### Backup

### Factory Reset

# Troubleshooting

The troubleshooting page shows errors and other events that occurred in RAM2 (such as loss of connectivity to RAM2 components). It does not show alert or other event information for factory entities; this is shown in the Alerts page.