# Introduction

## Overview

The Otorio Risk Assessment Monitoring & Management platform, RAM2 an unparalleled industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. The RAM2 offers an industry-first, 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, 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.

## Main Features

### Factory Management

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

The factory is divided hierarchically into the following entities.

**Plant** – this is a factory, possibly distributed over several geographical locations, but related logically as one business or industrial unit.

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

**Cells** – a unit in a shop

**Assets** – a single machine or device in a cell. An asset can belong to only one cell.

RAM2 scans assets in cells to assess their security and risk level, and then assesses an overall risk level for the cell, and then the shop, based on the risk levels of the component assets.

### Asset Management

RAM2 discovers assets in the plant automatically (if they are connected to the plant network and discoverable). Discovered assets are initially unassigned to any cell or shop.

In RAM2, you can define shops and cells for the plant, and then assign cells to shops, and assets to cells.

RAM2 scans assets, once they are discovered, whether or not they are assigned to a cell.

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

You can perform the following actions

Add shops to plant – define new shops, which are automatically included in the plant

Associate cells to shops – define new cells, and associate them with a shop, or move existing cells from one shop to another

Associate assets to cells – associate assets to a cell, or move assets from one cell to another

### 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.

### Vulnerabilities

## What RAM2 does

### Discover & map assets in plant network

### Continuously collect information about assets (MSB)

* Device, FW, IP,

### Correlate asset info with vulnerability information to generate an asset risk assessment & score

* CVEs
* Otorio Threat Intel Research Team

### Generate Shop-level risk level, based on cell & asset risk assessments

* Otorio proprietary algorithm

### Generate alerts about assets

# Views

## Dashboard View

The Dashboard view is the first view you see when the RAM2 application starts. It shows summary information for each shop in your plant. You can select from the list of shops on the left. For each shop it shows:

* The overall Risk Level for the shop
* The number of production cells in the shop
* The number of assets in the shop (assigned to cells)
* The number of alerts that have been logged for the shop

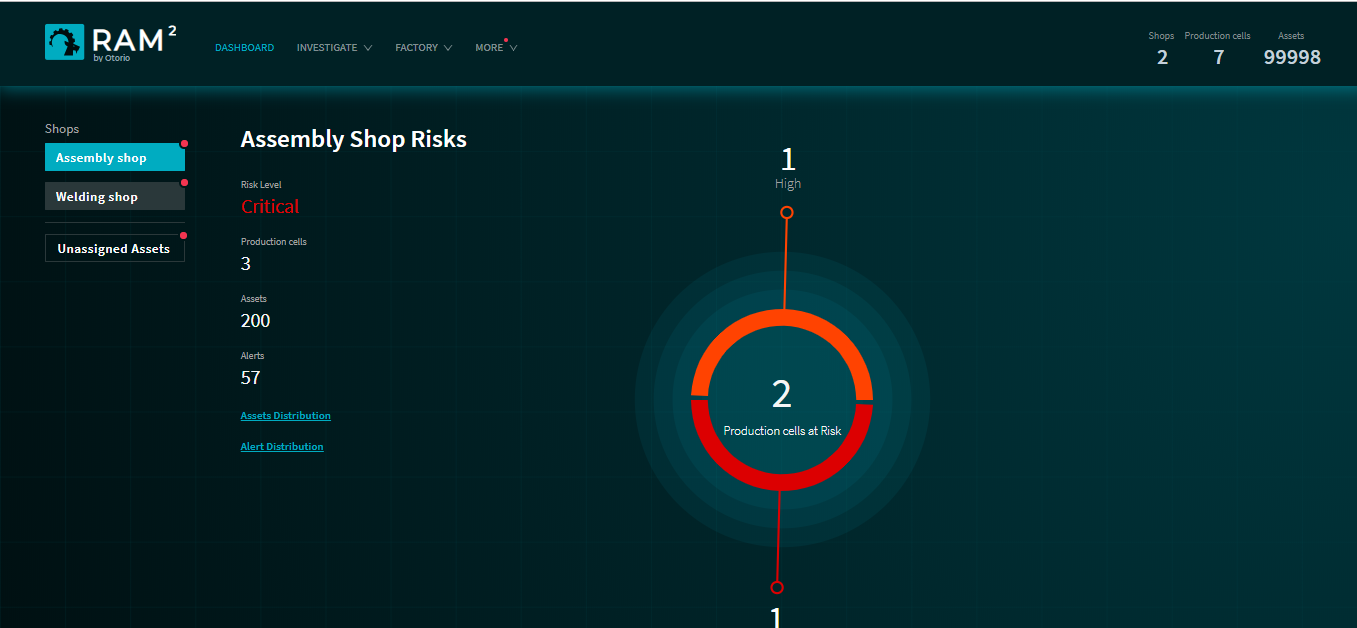


Figure 1 Dashboard view

Click on  or the *Dashboard* link to return to the Dashboard from any other RAM2 view.

The center of the Dashboard shows graphically the Risk Level distribution of the production cells in the shop. This is color-coded by Risk Level. In the example above, there is one cell at Risk Level ‘High’, and one at ‘Critical’ (and the third not at risk).

Click on one of the Risk Level, to show more detail. In the example below the cell at High Risk has 7 assets affected by risk, with 10 alerts generated.

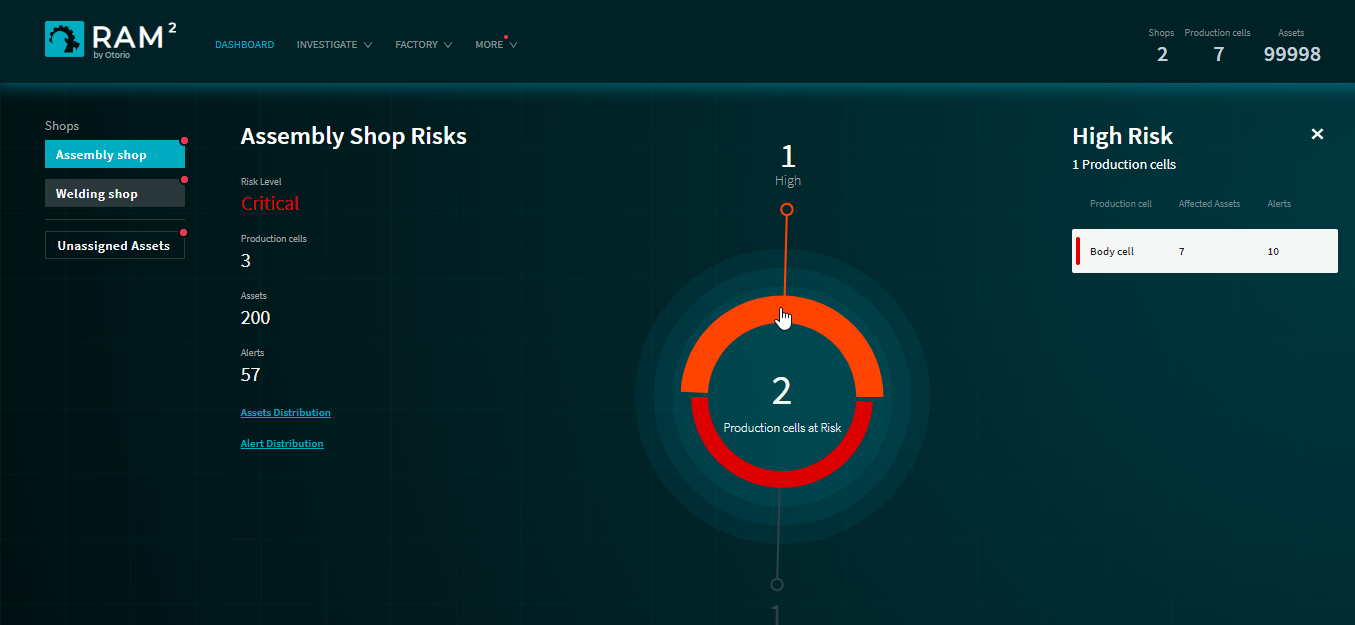


Figure 2 At-risk production cell details

Click on the detail (at the right) to open a list of the alerts for the cell.

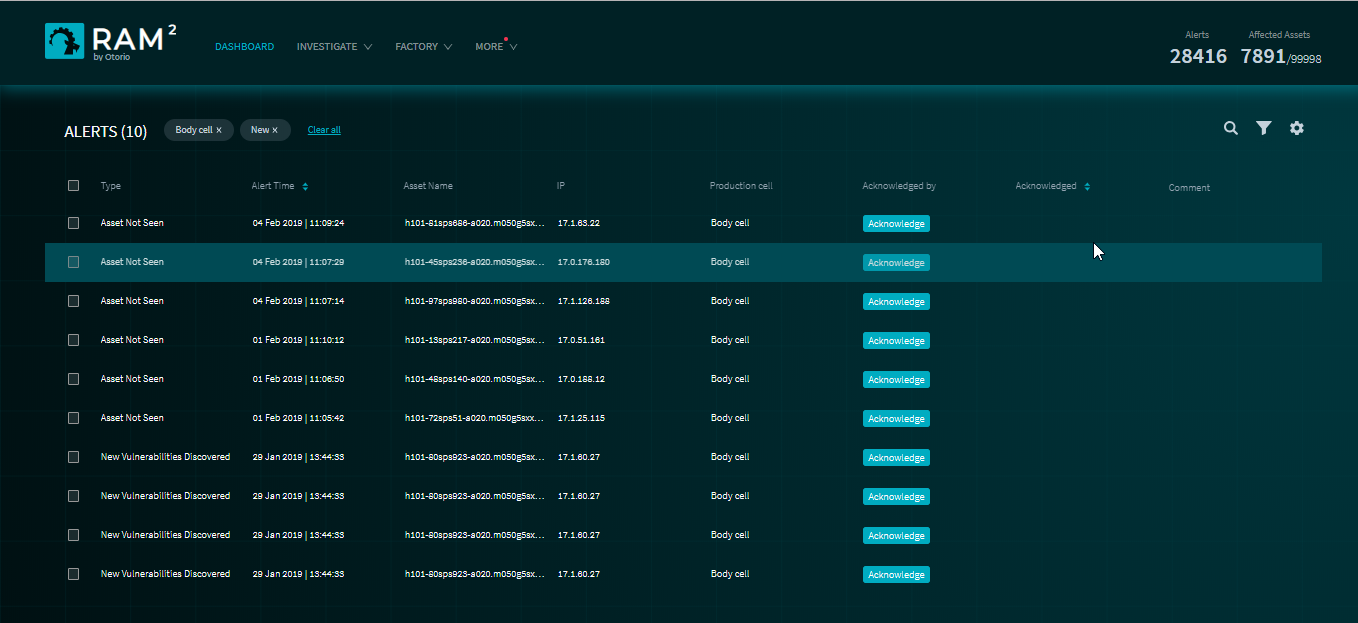


Figure 3 Alerts for Production Cell

### Shop information

### Asset Distribution

From the Dashboard, you can see a distribution of assets according to asset type or production cell.

Click on the *Assets Distribution* link on the Dashboard, and select the distribution type.

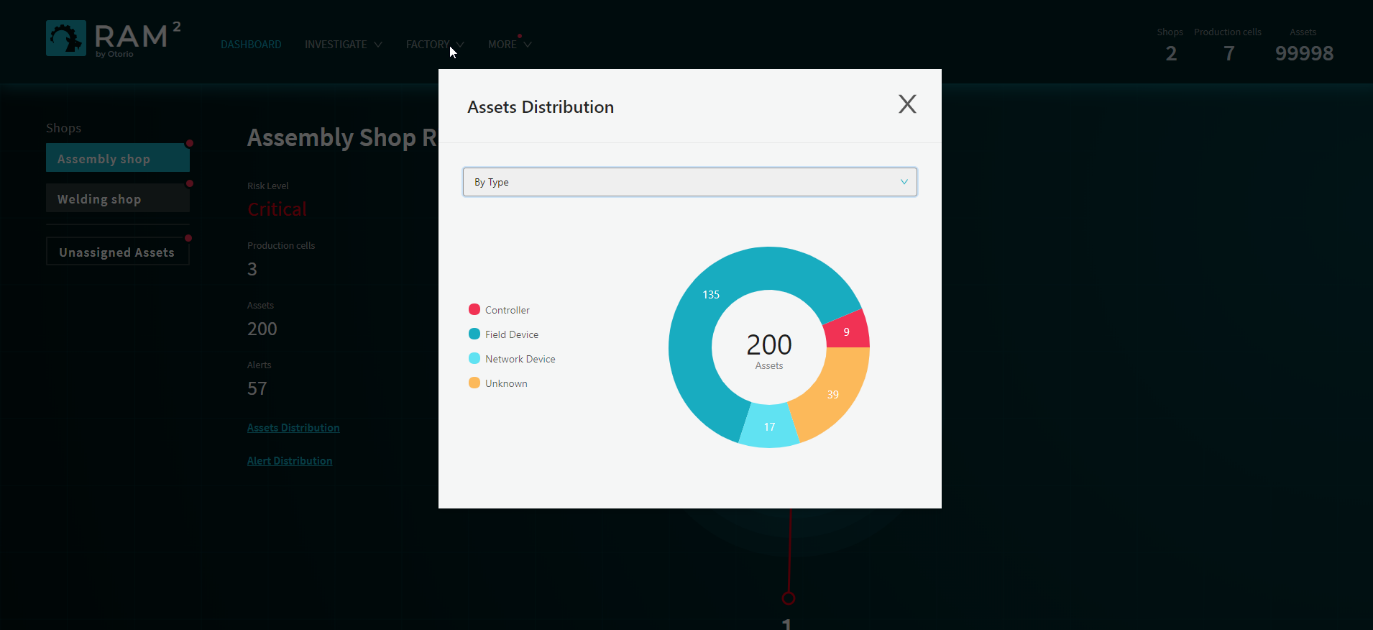


Figure 4 Asset Distribution by Asset Type

### Alert Distribution

From the Dashboard, you can also see a distribution of alerts according to alert type or production cell.

Click on the *Alert Distribution* link on the Dashboard, and select the distribution type.

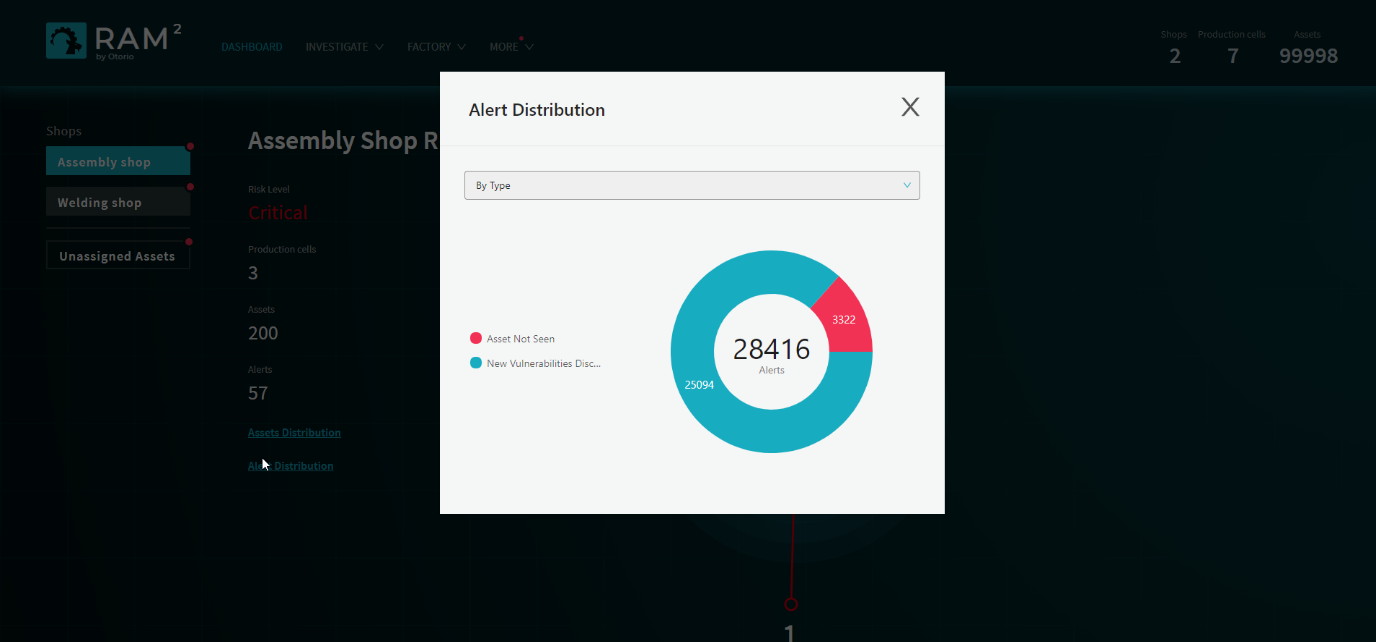


Figure 5 Alert Distribution by Alert Type

### Unassigned Assets

You can see a list of unassigned assets (assets that are not assigned to any production cell) from the Dashboard. Click on *Unassigned Assets* in the list of shops, on the left. This view is similar to the Shops view, including an overall Risk Level (based on all the unassigned cells taken together)

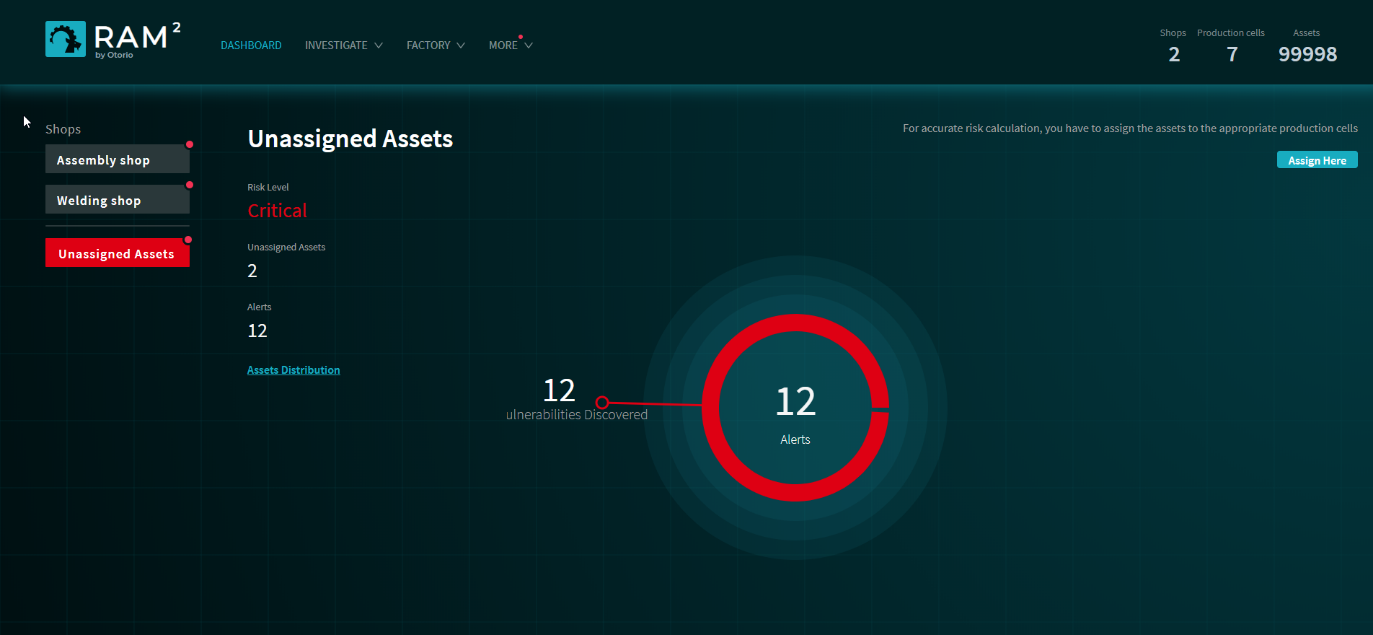


Figure 6 Unassigned Assets

## Assets

## Alerts

## Filters

# Factory management

## Shops

### Shop attributes

Location, risk level

### Create Shops

## Cells

### Cell attributes

Location, risk level,

### Create Cells

### Assign Cells to Shop

## Examples

### Create a Shop & Cells

# Assets

## Discover assets

## Asset types

## Asset attributes

Vendor, model, IP, Cell, location, IP, type,

### BI

Impact level

Risk level

## Assign assets

### Assign Assets to Cells

### Change cell assignment

### Unassigned assets

## Search Assets

Search by: Asset info, operational status, risk status, location

Filter Assets:

## Examples

### View a filtered group of assets

### Assign an asset to a cell

# Alerts

## Alert types

New asset discovered

Asset not seen

New vulnerability discovered

Segment breach

FW version changed

IP address changed

State changed

## View/Filter alerts

## Acknowledge alerts

## Disable alerts (manage CVE policy)

## Examples

### View alerts by Asset, Cell or Shop

### View by Vulnerability (CVE)

### View details (KPI)

### Acknowledge an alert

### Investigate alerts

### Disable a vulnerability

# Users

## User types

## Add users

# Configuration

## Network config

## Time

### Set time

## Deployment mode

### What is the Deployment Mode?

## Start & Shutdown

### Startup RAM2

### Shutdown RAM2

## Diagnostics

# Troubleshooting