# 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

Entity hierarchy:

Plant

Shops

Cells

assets

### Asset Management

Add shops to plant

Associate cells to shops

Associate assets to cells

### Alerts

### 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

What this view is used for

What is shown

The Dashboard view is the first view seen 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

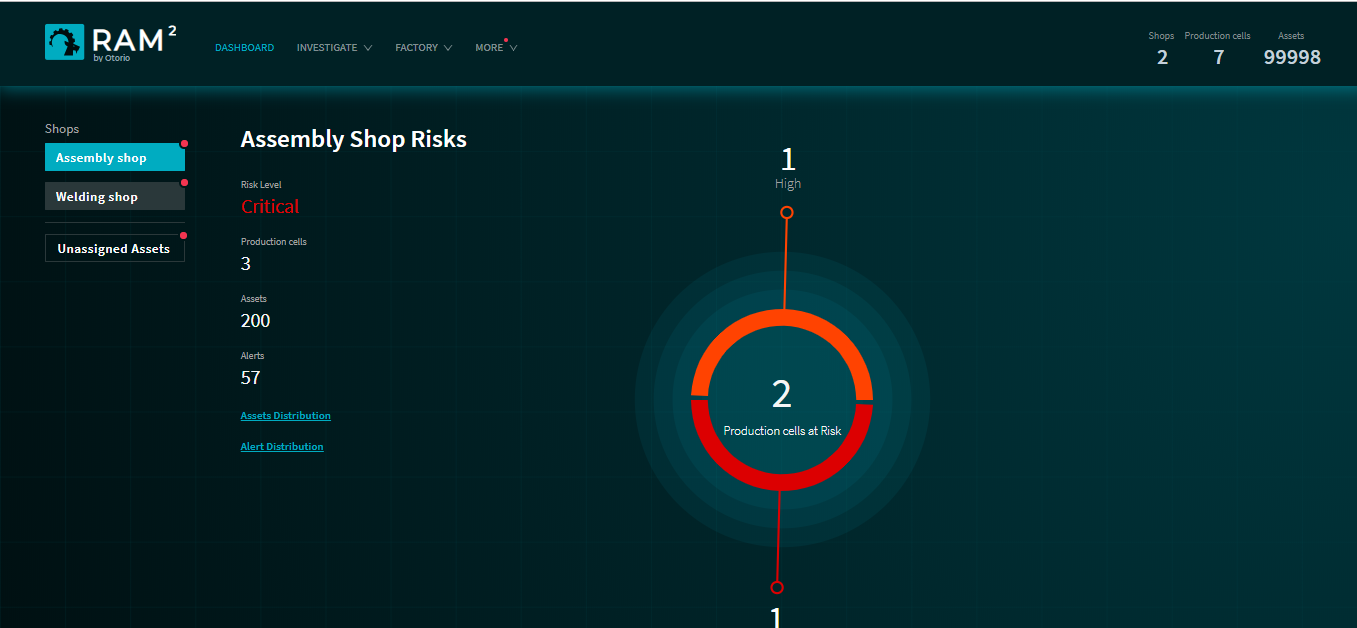


Figure Dashboard view

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.

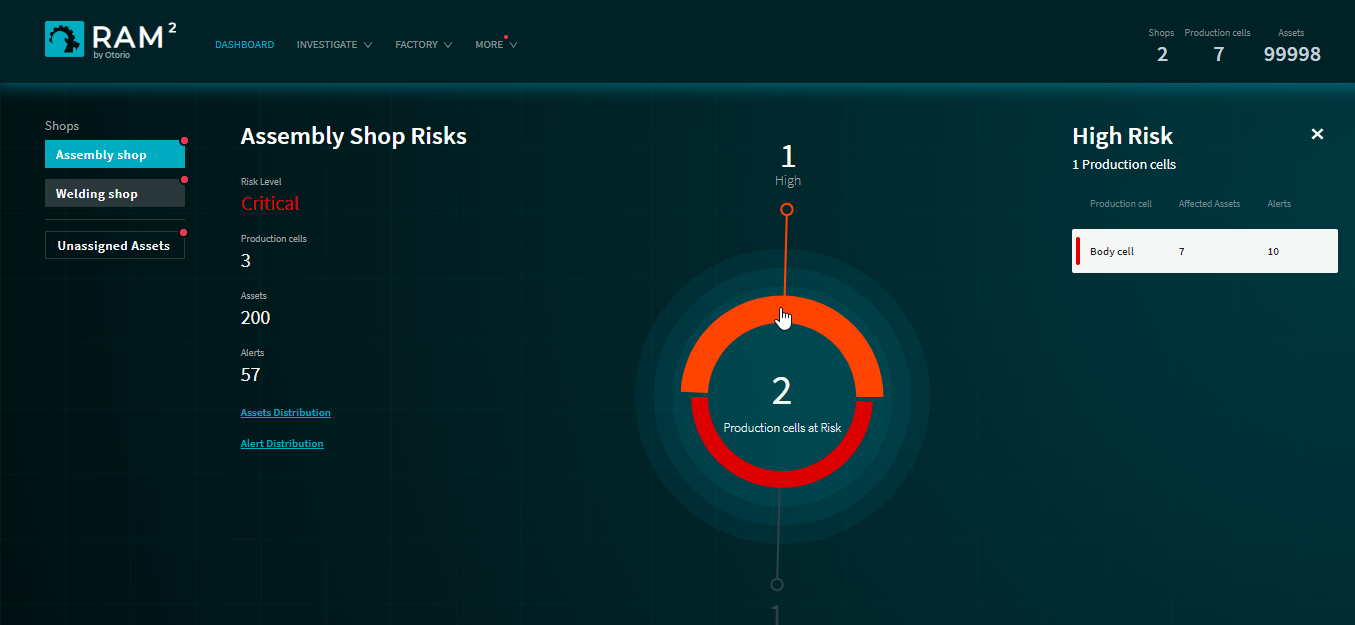


Figure At-risk production cell details

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

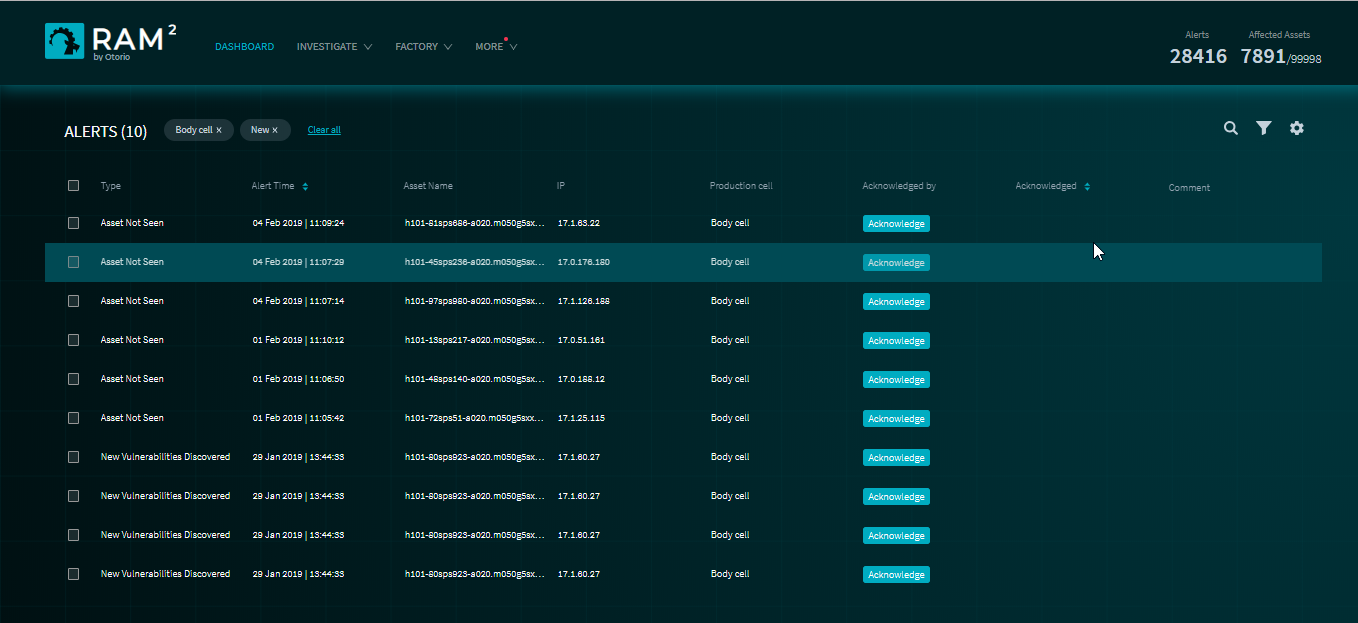


Figure Alerts for Production Cell

### 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.

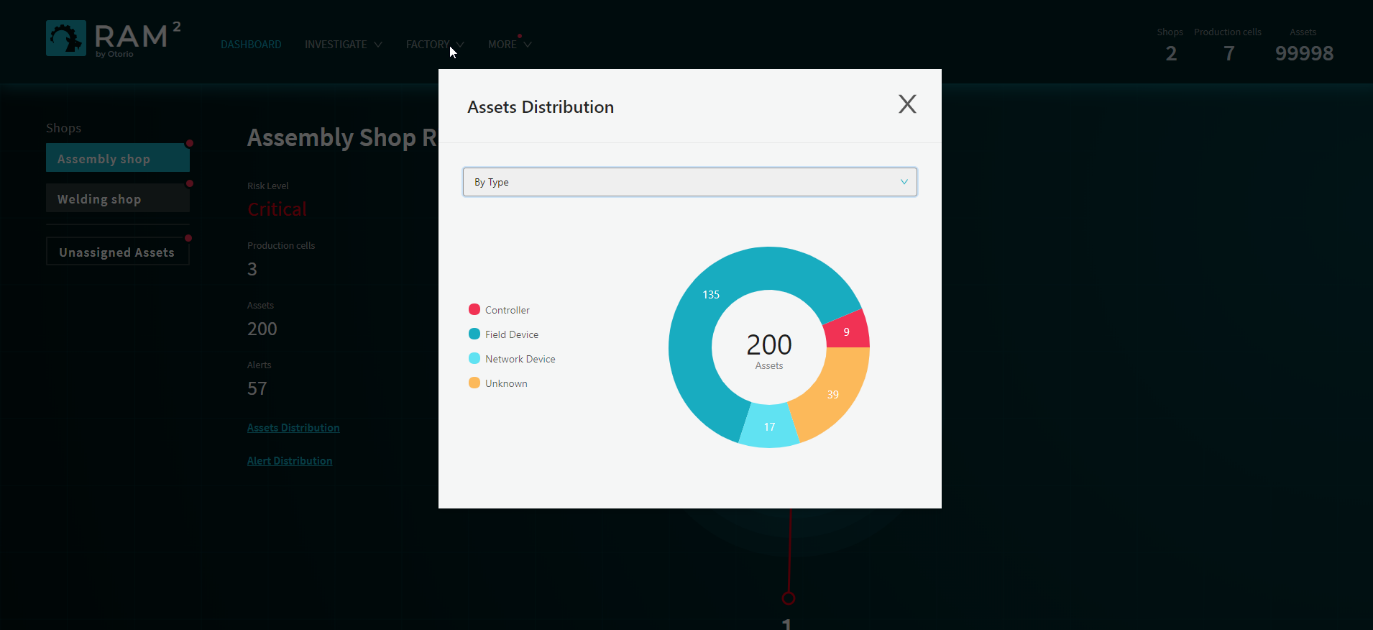


Figure Asset Distribution by Asset Type

### 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.

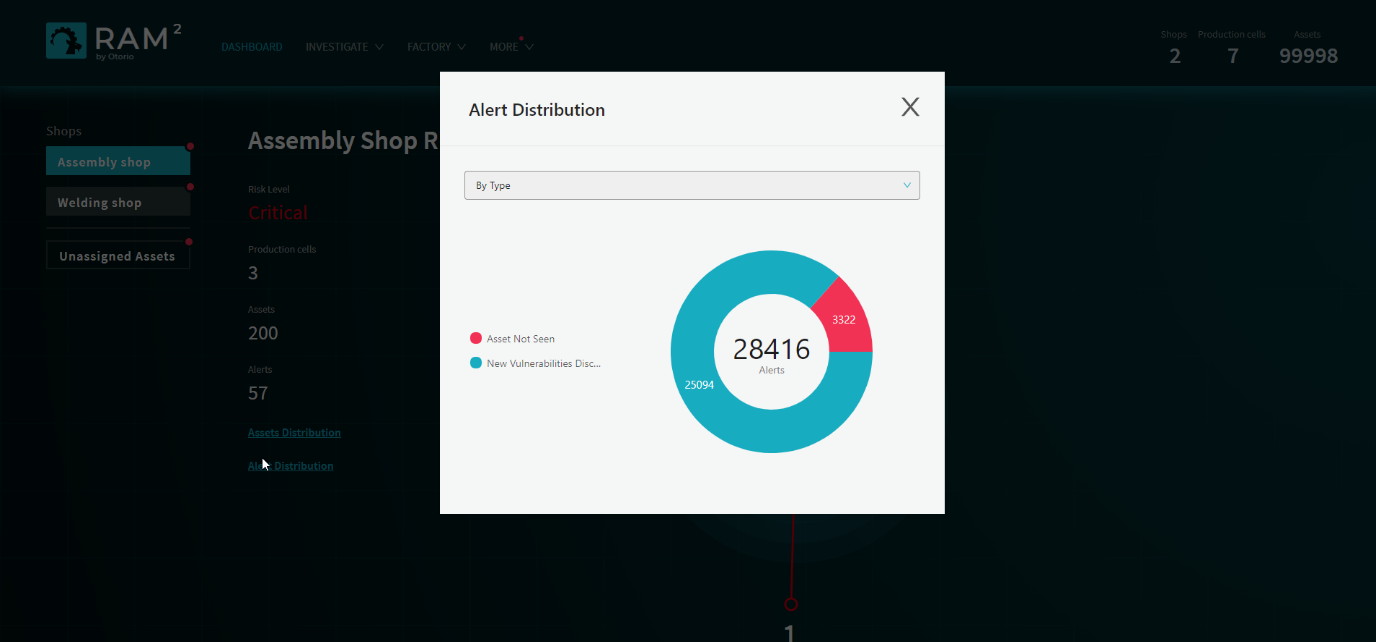


Figure Alert Distribution by Alert Type

### 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)

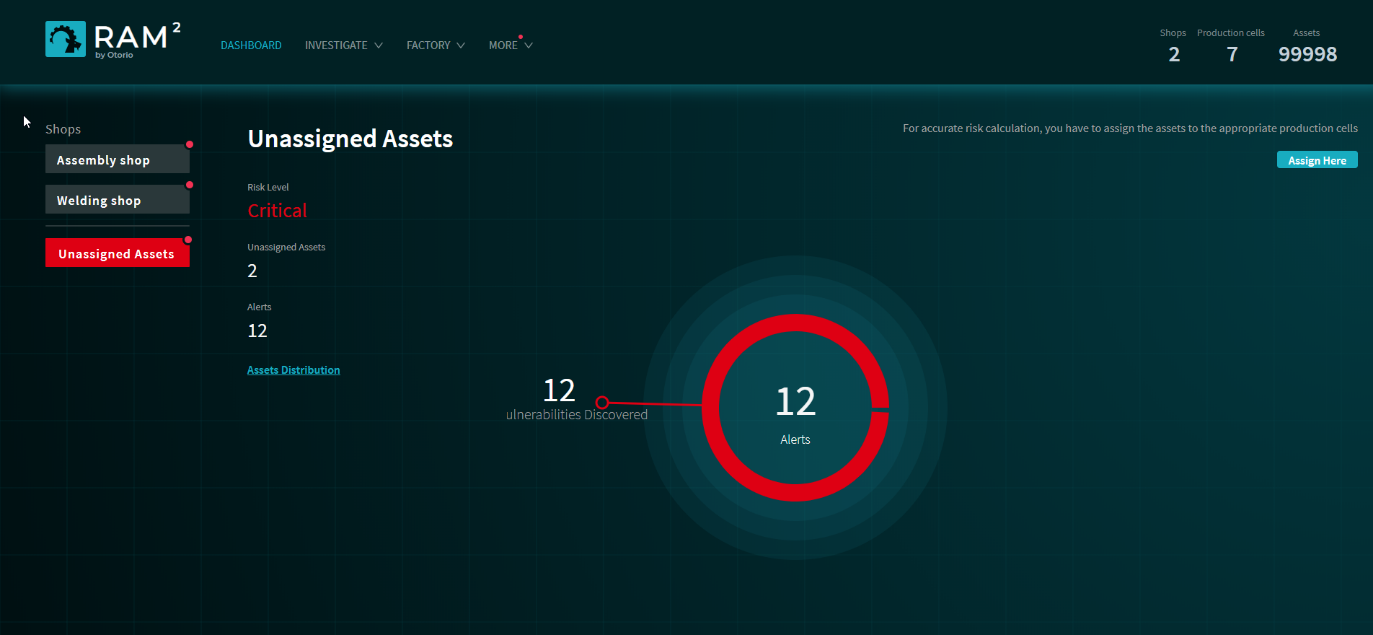


Figure Unassigned Assets

## 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