# 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

### Asset Management

### 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

### Risk Level per Shop

## 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