RAM^2 Product Overview

Introduction

This document provides an overview of the main features of the RAM^2 (Risk Assessment, Monitoring & management), and describes how to configure and use it.

It is intended to help users who are unfamiliar with RAM^2 gain a quick understanding of how it works, how to configure it for the first time, and how to use it. RAM^2 has many options and features, some of which are outside the scope of this overview.

Note also that some features described here may not be implemented in your plant as they may require sensors for continuous monitoring.

About RAM^2

The Otorio Risk Assessment Monitoring & Management platform, RAM^2, an unparalleled industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. The RAM^2 offers an industry-first, comprehensive, centralized, simplified, and automated industrial cyber risk management solution.

RAM^2 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.

RAM^2 enables continuous cyber risk management by presenting an on-going, focused compliance status, and a comprehensive operational OT-IT converged asset view.

Dashboard

The Dashboard shows the overall status of the shop floors in terms of assets, risk levels, and alerts.

The Dashboard shows an interactive pie chart showing the risk level of each shop, and its production cells, in the factory. If there are no risks, the Dashboard will indicate this as well. Production cells cards are displayed, from where you can easily navigate to alert screens, to deal with the prioritization of the shop floor threats.

Assets that have not yet been assigned to cells are shown in the "Unassigned assets" tab, and can be filtered according to alert type only.

The risk level for an asset is calculated using a proprietary algorithm developed by Otorio, which considers the severities of vulnerabilities, as well as the number and types of alerts and assets in the network.

RAM^2 Version 1.0 Features

Risk Dashboard

- **Comprehensive risk overview**, prioritized by threat intelligence algorithms and operational impacts.
- **Automated risk management**, based on monitored changes, and behavioral deviations from internal

policies, and segment breaches.

Factory management

- **Manage the shop floor** - create operational layers to group data with similar operational characteristics.
- **Manage operational impacts** - define and manage impacts of assets or cells on the operational layers, that can be used as an aid in risk prioritization.

Asset management

- **Automatically accumulate** asset attributes, behavior, and security posture, based on multiple data sources.
- **Business intelligence** – insightful and actionable analysis of assets distribution by assets types, operational context, and security posture.

Alert management

- **Alerts on critical changes**, and behavioral deviations of assets from multiple data sources (network data, AV data, patch management, etc).
- **Business intelligence** – insightful and actionable analysis of assets distribution by assets types, operational context, and security posture.
- **Disable alert** – the ability to disable/enable alerts for selected CVEs, in order to reduce the false alarms and known CVEs which are not interesting to the customer.

Vulnerabilities management

- **Identify security vulnerabilities in assets in the environment** - RAM^2 continuously tracks vulnerabilities within the shop floor, using a list of vulnerabilities compiled and updated by the Otorio threat intelligence research team. Currently thousands of relevant ICS vulnerabilities are listed.

Factory Management

The first step in managing assets in the factory is to group them into operational layers, for better mapping and visualization in later steps. You create “cards” (groups) for shops and production cells in their respective tabs in the Factory section. You can manage basic attributes and operational impacts for each card.

The card shows the risk level for the shop or cell. The risk level is calculated using a proprietry algorithm developed by Otorio, which considers the severities of vulnerabilities, as well as the number and types of alerts, assets in the network, and managed operational impacts on production cells or assets.

Assets can be grouped and assigned to cells, and cells assigned to shops.

Assets are configured and managed in the Assets tab under the Factory section.

Assets Management

Assets and their attributes are automatically collected from external collectors (such as the MSB). Details such as IP and MAC addresses, types, vendor, firmware and hardware versions, family, and more, are collected and displayed for each asset.

The following customized characteristics and attributions are assigned to assets:

- Device Name
- Description
- Type (controller, engineering stations, HMIs, servers, controllers, I/Os, other ICS devices and networking equipment)
- Location
- Production Cell
- Impact Levels (based on several factors: financial, safety productivity, operational, reputation, and regulator)

The asset inventory is synchronized with the Otorio Threat Intelligence Module, which provides knowledge about known and unknown vulnerabilities that are discovered in assets.

The assets can be filtered based on various categories and characteristics.

Investigate - Alerts

The Alerts section shows alerts that have been generated by the system.

RAM^2 generates the following types of alerts:

- **New Asset Discovered**
- **Asset not seen** (in a configurable interval)
- **New Vulnerability Discovered** (known and unknown vulnerability on an asset based on the Otorio Threat Intelligence Module*)
- **Segment breach** (network policy deviations)
- **Firmware Version Changed**
- **IP Address Changed**
- **State Changed**

After you remedy risks and handle alerts, you can acknowledge them in RAM^2. They won't be displayed again for the asset in which they were discovered. Future versions of RAM^2 will also suggest mitigation recommendations, based on the alerts. As with the asset management, the alerts can also be filtered, based on various categories and characteristics.

Disable alerts for specific CVEs

You can disable specific alerts. Disabled alerts won't be shown in the Alerts view. Use this feature to reduce the number of alerts by disabling alerts for specific CVEs. You can re-enable an alert later on, after which they will be shown.

*the Otorio Threat Intelligence Module, integrated into RAM^2, is constantly updated and managed by Otorio’s researchers. The current version contains more than 1,000 relevant ICS vulnerabilities.

Appliance Settings

Configuration

This section is used to configure the RAM^2 appliance.

- Device details
- Network Configuration
- Set Time
- System actions: **Deployment Mode, Download diagnostic, Restart, Shutdown**