RAM^2 Product Overview

Welcome

This document describes how to configure and use the Otorio RAM^2 (Risk Assessment, Monitoring & Management) appliance. 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.

About OTORIO

OTORIO is a service provider focused on the full life-cycle of industrial cyber risk solutions. It was founded as a joint venture between experienced Israeli defense professionals and a leading Austrian plant engineering group, combining the best of both domains. OTORIO offers comprehensive cybersecurity solutions and services for established industries.

Our know-how is based on years of deep domain expertise in cyber security engineering, and hands-on hacking of mission critical operational systems. The collaboration with Andritz AG brings more than 160 years of industrial engineering and operational technology know-how for leading industrial customers, in a variety of verticals.

In today's ever-changing technology landscape, security does more than protect existing systems; it enables businesses to maximize production and exploit opportunities. OTORIO assists businesses in driving their operational environment forward in an optimized and secured way.

Guided by strong professional integrity and competence, we offer a comprehensive solution based on a unique formulation of military grade innovative technology and professional services, designed and operated by highly trained cyber security “special forces”. OTORIO’s leading experts are engaged at different touch points throughout the entire security process (requirements, specification, development, and deployment).

About this overview

This document aims to provide a basic understanding of how to configure and use RAM^2 (Risk Assessment, Monitoring & management). This manual serves as a user guide to help users who are unfamiliar with the RAM^2 gain a brief understanding of how the product works, how to configure it for the first time, and how to use it. Note that RAM^2 has many options and features, that are not all covered in this manual.

RAM^2 Version 1.0 Features

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

- Extract asset attributes: query MSB, as data collector, with values updated every 24 hours.
-

Business intelligence: provide views of assets, distributed according to type and process.

Alert management

- Issue alerts on critical changes in assets: new asset discovery or asset disappearance; changes in asset in state, firmware version and IP; new vulnerability discovery.
- Business intelligence: provide views of assets, distributed according to type and process.

Vulnerabilities management

- Identify security vulnerabilities in assets in the environment: using a list of vulnerabilities compiled and updated by Otorio researchers. Currently more than 1,000 relevant ICS vulnerabilities are listed.

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.

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 with sync to the Otorio Threat Intelligence Module*)
- 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