OTORIO and ServiceNow: Manage Operational Security With Efficiency

Solution Brief

ServiceNow and OTORIO unite to streamline asset management, accelerate incident resolution, and boost operational efficiency. OTORIO's RAM² integrates with ServiceNow CMDB to comprehensively discover assets and enrich data, leveraging ServiceNow's analytics for informed decision-making. This partnership provides continuous asset oversight with automated ticketing and incident resolution tailored to ensure OT security in the operational environment.

OTORIO and ServiceNow Solution Benefits:

Continuous Asset Management

Gain full visibility into your OT ecosystem

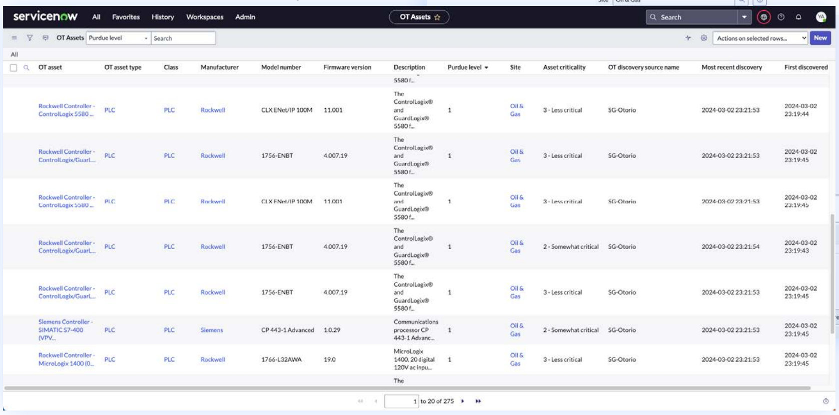
Integrate and enhance ongoing asset discovery with ServiceNow's CMDB, leveraging OTORIO's RAM² to accurately classify OT asset roles within processes and provide comprehensive oversight across OT-IT-IoT Domains.

How? RAM² collects data using OT native protocols via passive network monitoring, Safe Active querying, and offline data (such as Industrial project files, logs, PCAPs, and more). The platform integrates with industrial FWs, SCADA, DCS, IDS, Historians, and additional operational systems to enrich the inventory and identify the state of security and compliance issues. Asset inventory is continuously synchronized between RAM² and ServiceNow CMDB to provide central visibility across the customer’s OT and IT ecosystem.

- **Ensure** complete OT, IT, and IoT asset coverage in operational environments.
- **Identify** asset roles within processes down to level 0.
- **Create** a comprehensive context-based overview of the OT environment.

- Continuously monitor OT and streamline asset management.
- Gain complete visibility of OT, IT, and IoT in operational environments
- Accelerate incident resolution with seamless ticketing and mitigation guidance.
- Empower informed decisions that focus on mitigating the most critical risks first.
- Boost operational efficiency to achieve resilient business operations.

Screen 1: CMDB - asset inventory



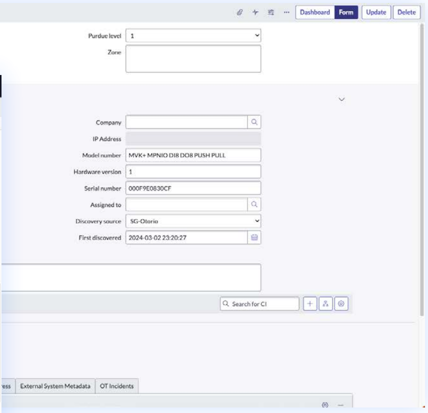
OT Assets | Purdue level | Search

All

OT asset	OT asset type	Class	Manufacturer	Model number	Firmware version	Description	Purdue level	Site	Asset criticality	OT discovery source name	Most recent discovery	First discovered
Rockwell Controller - ControlLogix 5580 ...	PLC	PLC	Rockwell	CLX ENet/IP 100M	11.001	The ControlLogix® and GuardLogix® 5580 f...	1	Oil & Gas	3 - Less critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:44
Rockwell Controller - ControlLogix/GuarL...	PLC	PLC	Rockwell	1756-ENBT	4.007.19	The ControlLogix® and GuardLogix® 5580 f...	1	Oil & Gas	3 - Less critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:45
Rockwell Controller - ControlLogix 5580 ...	PLC	PLC	Rockwell	CLX ENet/IP 100M	11.001	The ControlLogix® and GuardLogix® 5580 f...	1	Oil & Gas	3 - Less critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:45
Rockwell Controller - ControlLogix/GuarL...	PLC	PLC	Rockwell	1756-ENBT	4.007.19	The ControlLogix® and GuardLogix® 5580 f...	1	Oil & Gas	2 - Somewhat critical	SG-Otorio	2024-03-02 23:21:54	2024-03-02 23:19:43
Rockwell Controller - ControlLogix/GuarL...	PLC	PLC	Rockwell	1756-ENBT	4.007.19	The ControlLogix® and GuardLogix® 5580 f...	1	Oil & Gas	3 - Less critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:45
Siemens Controller - SIMATIC S7-400 (VPV...	PLC	PLC	Siemens	CP 443-1 Advanced	1.0.29	Communications processor CP 443-1 Advanc...	1	Oil & Gas	2 - Somewhat critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:45
Rockwell Controller - MicroLogix 1400 (0...	PLC	PLC	Rockwell	1766-L32AWA	19.0	MicroLogix 1400, 20 digital 120V ac inpu...	1	Oil & Gas	3 - Less critical	SG-Otorio	2024-03-02 23:21:53	2024-03-02 23:19:45

1 to 20 of 275

Screen2 : Individual asset page



OT Field Device
Murrelektronik IO Device - MVK (000F9E0830CF)

OT asset type	OT Field Device
Asset criticality	3 - Less critical
Site	Oil & Gas
Purdue level	1
Zone	
Company	
IP Address	
Model number	MVK+ MPNIO DI8 DO8 PUSH PULL
Hardware version	1
Serial number	000F9E0830CF
Assigned to	
Discovery source	SG-Otorio
First discovered	2024-03-02 23:20:27

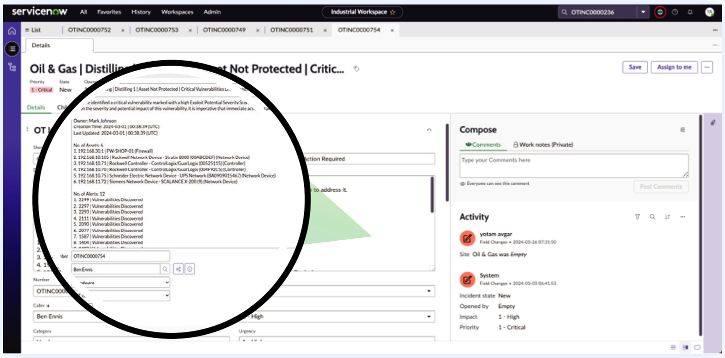
Seamless Ticketing and Incident Resolution

Proactively manage OT security incidents with step-by-step mitigation guidance

Identify security alerts, escalate and streamline OT incident resolution to ServiceNow workflows with OTORIO's RAM² incident ticket generation and step-by-step risk mitigation guidance tailored to ensure OT security in the operational environment.

How? RAM² correlates data from cross-domain sources to identify OT cyber security gaps and exposures, detect potential attacks on the operational network, and prioritize security risk by business impact. RAM² automatically opens tickets in ServiceNow and provides practical mitigation guidance for each ticket. When the ticket status is updated in ServiceNow, it syncs with the RAM² to close the loop.

- **Achieve** resilient operations with continuous OT monitoring.
- **Automate ticket generation** for asset-related issues and vulnerabilities.
- **Ensure OT security** with step-by-step mitigation guidance tailored for OT.



Oil & Gas | Distillin… …t Not Protected | Critic…

Priority: 1 - Critical State: New

…ng | Distilling 1 | Asset Not Protected | Critical Vulnerabilities D…

…identified a critical vulnerability marked with a high Exploit Potential Severity Sco… …n the severity and potential impact of this vulnerability, it is imperative that immediate act…

Owner: Mark Johnson
Creation Time: 2024-03-01 | 00:38:39 (UTC)
Last Updated: 2024-03-01 | 00:38:39 (UTC)

No. of Assets: 6
1. 192.168.30.1 | FW-SHOP-01 (Firewall)
2. 192.168.10.105 | Rockwell Network Device - Stratix 8000 (00ABCDEF) (Network Device)
3. 192.168.10.71 | Rockwell Controller - ControlLogix/GuarLogix (00525115) (Controller)
4. 192.168.10.70 | Rockwell Controller - ControlLogix/GuarLogix (004F92C5) (Controller)
5. 192.168.10.75 | Schneider Electric Network Device - UPS Network (BA0909015467) (Network Device)
6. 192.168.11.72 | Siemens Network Device - SCALANCE X-200 (9) (Network Device)

No. of Alerts: 12
1. 2299 | Vulnerabilities Discovered
2. 2297 | Vulnerabilities Discovered
3. 2293 | Vulnerabilities Discovered
4. 2111 | Vulnerabilities Discovered
5. 2090 | Vulnerabilities Discovered
6. 2077 | Vulnerabilities Discovered
7. 1587 | Vulnerabilities Discovered
8. 1404 | Vulnerabilities Discovered

Number: OTINC0000754
Caller: Ben Ennis
Impact: 1 - High

yotam avgar — Field Changes • 2024-03-26 07:31:50
Site Oil & Gas was *Empty*

System — Field Changes • 2024-03-03 06:41:53
Incident state New
Opened by Empty
Impact 1 - High
Priority 1 - Critical

Screen 3: Incident page

Efficient and Informed Decision-Making

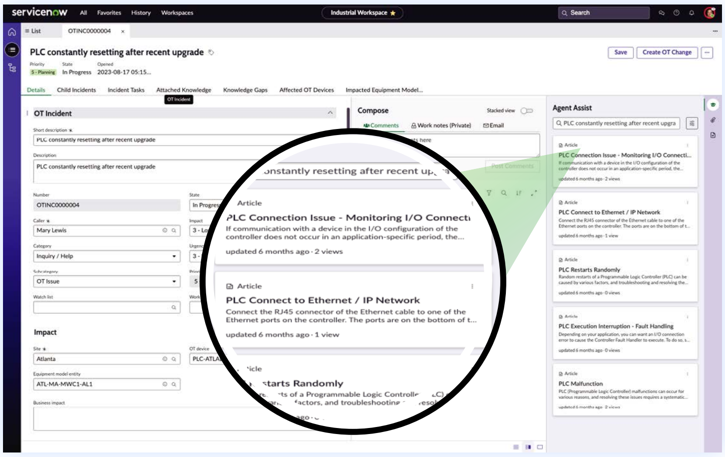
Strategically prioritize when and where you act with data-driven insights

Harness the power of ServiceNow's analytics and machine learning to anticipate trends, prioritize actions, and make precise informed decisions.

How? ServiceNow uses performance analytics to identify the trends in the asset inventory data to discover and prioritize the assets that need actions such as assignment or classification.

ServiceNow uses machine learning to recommend related knowledge articles to help expedite the incident resolution.

- **Enrich** asset inventory data with the industrial process context that helps prioritize incidents and vulnerabilities.
- **Enable** users to focus on asset-related issues by gaining insights with the help of analytics.
- **Enhance** Enhance the efficiency of incident resolution with Agent Assist by guiding users to key articles in record time.



PLC constantly resetting after recent upgrade

Priority: 5 - Planning State: In Progress Opened: 2023-08-17 05:15...

Short description: PLC constantly resetting after recent upgrade
Description: PLC constantly resetting after recent upgrade
Number: OTINC0000004
State: In Progress
Caller: Mary Lewis
Category: Inquiry / Help
Subcategory: OT Issue
Watch list:

Impact
Site: Atlanta
OT device: PLC-ATLA…
Equipment model entity: ATL-MA-MWC1-AL1
Business impact:

Agent Assist: PLC constantly resetting after recent upgra…

Article
PLC Connection Issue - Monitoring I/O Connecti…
If communication with a device in the I/O configuration of the controller does not occur in an application-specific period, the…
updated 6 months ago · 2 views

Article
PLC Connect to Ethernet / IP Network
Connect the RJ45 connector of the Ethernet cable to one of the Ethernet ports on the controller. The ports are on the bottom of t…
updated 6 months ago · 1 view

Article
PLC Restarts Randomly
Random restarts of a Programmable Logic Controller (PLC) can be caused by various factors, and troubleshooting and resolving the…
updated 6 months ago · 0 views

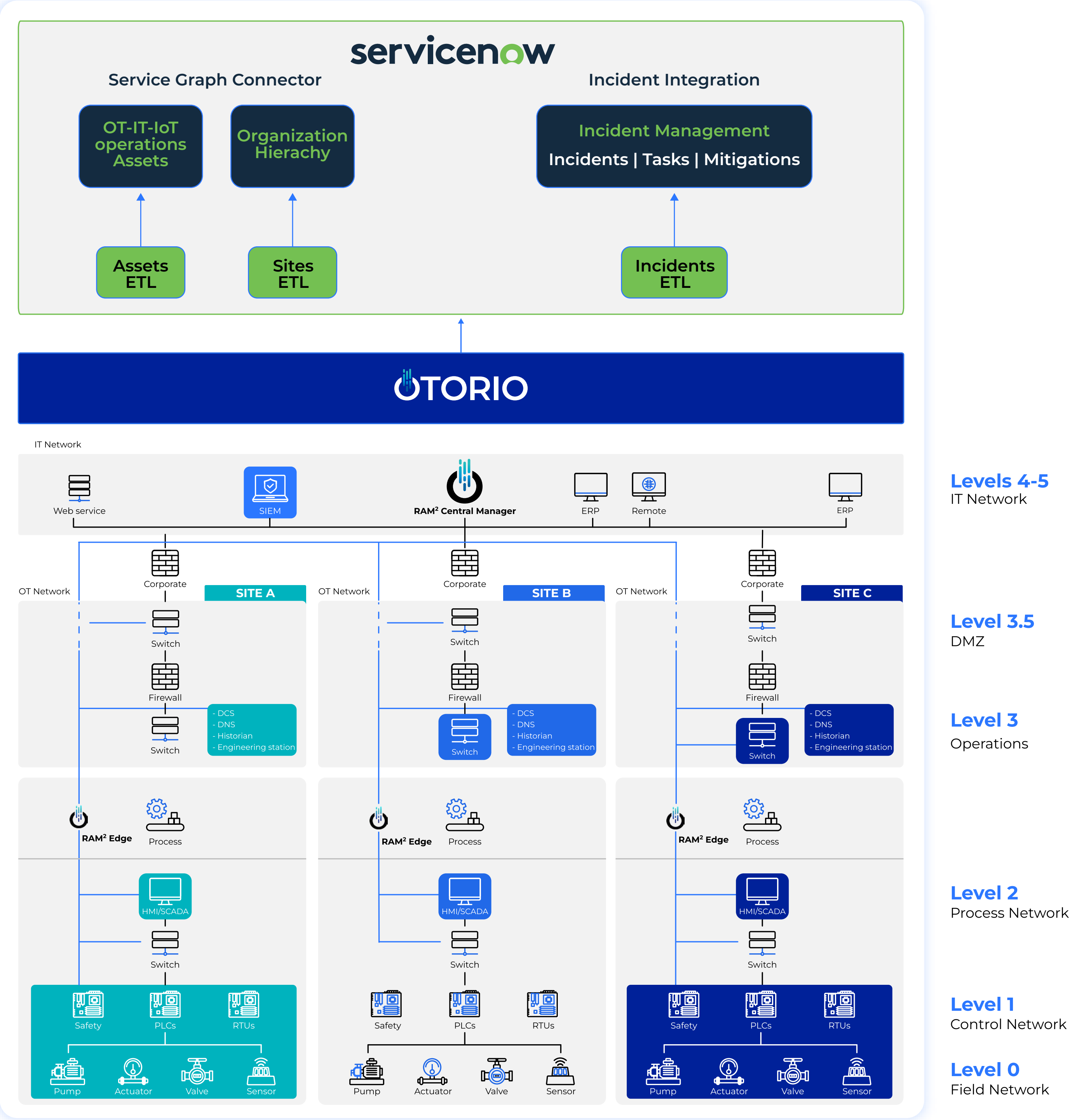
Article
PLC Execution Interruption - Fault Handling
Depending on your application, you can want an I/O connection error to cause the Controller Fault Handler to execute. To do so, s…
updated 6 months ago · 0 views

Article
PLC Malfunction
PLC (Programmable Logic Controller) malfunctions can occur for various reasons, and resolving these issues requires a systematic…
updated 6 months ago · 2 views

Screen 4: Agent Assist Screen

OT Discovery & Security - ServiceNow + OTORIO

Dedicated OT security management integrated with ServiceNow workflows



About OTORIO

OTORIO is a provider of OT security solutions, delivering a cyber risk Management platform that leverages operational context to seamlessly protect ICS-CPS environments and proactively achieve resilient, compliant business operations.

Visit OTORIO.com