OTORIO

Digital Twin

OTORIO's Cyber Digital Twin

A virtual model of your operational environment for comprehensive OT security posture assessment

Overview

To achieve cyber security resilience in the operational environment, operations security practitioners must address fundamental questions like:

- What is present in my network?
- What vulnerabilities and security gaps exist, and how can I mitigate risks stemming from them?
- How well are my security controls configured?
- Which actions should I prioritize?

Even with skilled OT security personnel, protecting operational environments presents challenges for organizations that make it difficult to answer these questions. Such challenges include:

- An unclear asset inventory due to limited visibility and partial data.
- A focus on endpoint vulnerabilities without an understanding of their actual exposure to potential threats.
- The inability to get an overall OT security posture assessment.
- Ineffective mitigation actions that are not suitable for operational environments.
- Inefficiency due to a lack of impact-driven prioritization mechanisms.

Overcoming these challenges requires more than just deploying security controls in the network. Gaining better OT security awareness and an understanding of your organization's security posture depends on your ability to get a unified view of all components in the network, their interdependencies, and their relationship to operational and business goals.

OTORIO's OT security risk management platform goes beyond asset visibility and vulnerability identification. With the Cyber Digital Twin at its core, OTORIO's platform empowers you to take control of your security posture, eliminate the most critical risks, and ensure safe, efficient, and reliable operations.

What is OTORIO's Cyber Digital Twin?

OTORIO's Cyber Digital Twin (CDT) delivers an automated, logical representation of the operational network, the entities comprising it, and the characteristics of the relationship between them. It provides context to your cyber security posture along with prioritized, concise calls to action.

OTORIO's CDT is a secure, sandboxed model of your operational environment. It allows for safe (non-intrusive) breach and attack simulations (BAS) and data-driven impact analysis. CDT is used to provide a visual representation of an organization's OT network topology, and identifies segmentation gaps and attack vectors to critical assets and processes. OTORIO's CDT recommends practical steps for improving your security posture such as restricting communication or hardening of specific assets. CDT prioritizes risk mitigations according to the actual exposure of vulnerable assets and the potential impact on operations.

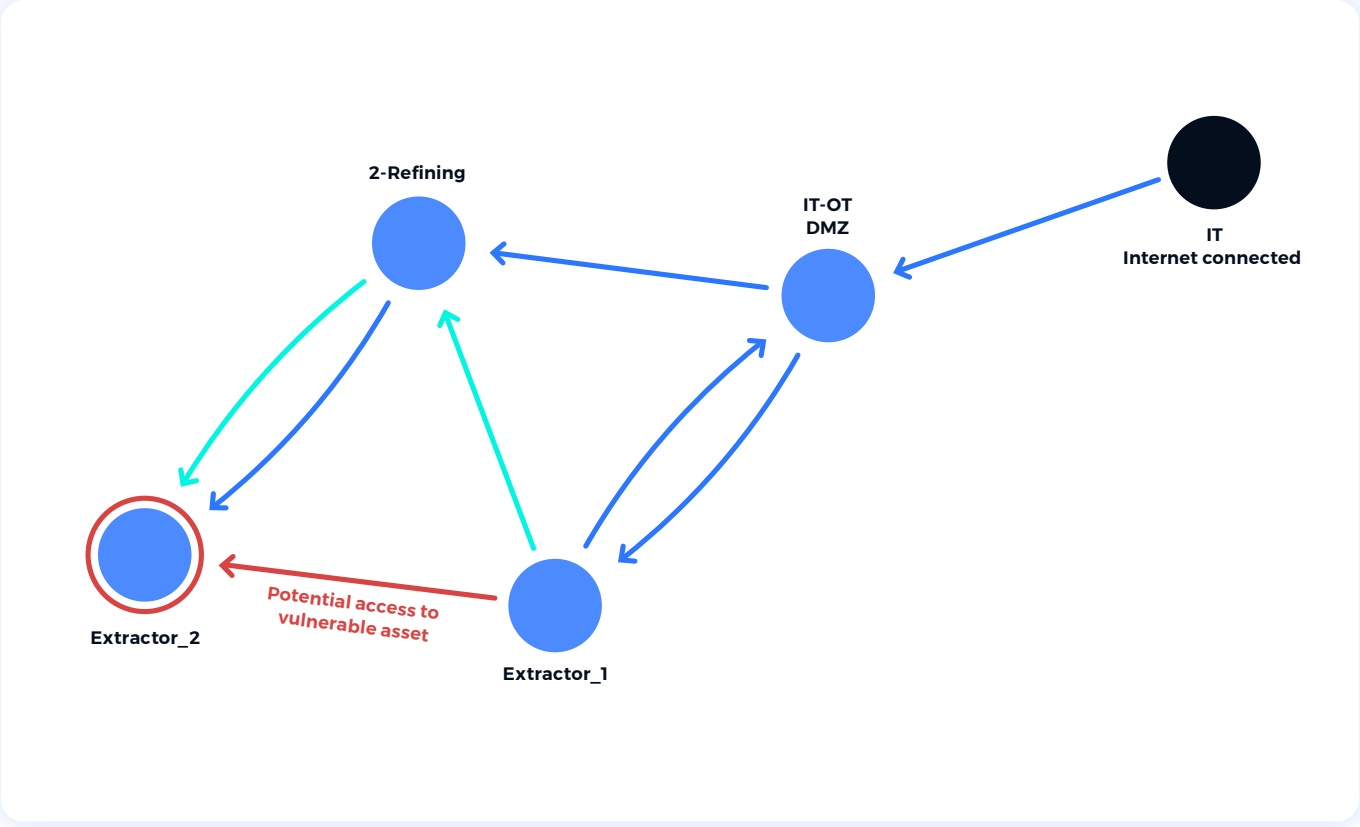


Image 1: Identifying non-restricted process communication

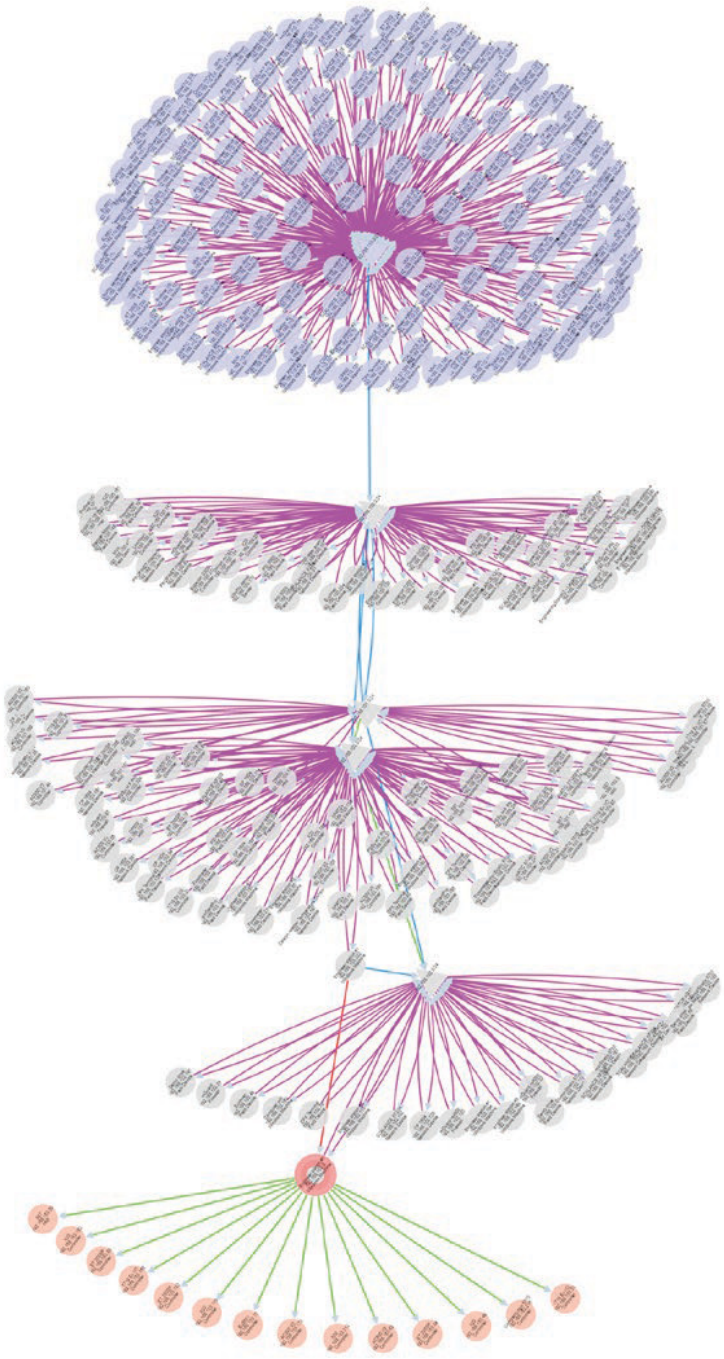


Image 2:
Full network topology with asset vulnerabilities

Benefits of OTORIO's Cyber Digital Twin

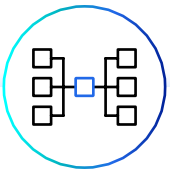
- **Eliminate blind spots from your operational environment** with the OTORIO CDT's extended visibility and unmatched integrations. Together, they provide consolidated network data analysis, a comprehensive 360° view of your operational environment, and an enhanced security posture.
- **Improve the efficiency of risk-reduction efforts** by prioritizing vulnerabilities and security gaps that can actually be exploited.
- **Proactively remove most critical risks** with clear, practical mitigation recommendations.
- **Predict the impact of potential attacks and changes in your environment, safely** using a sandboxed environment for analysis.
- **Improve the return on investment (ROI) for existing security controls** by identifying misconfigurations and necessary optimizations.
- **Get immediate value** from an automated assessment of online and offline data.
- **Minimize noise and add context** for better detection capabilities while preventing alert fatigue.

How does OTORIO's Cyber Digital Twin Work?

OTORIO CDT is based on our platform's ability to collect rich data from cross-domain sources via:

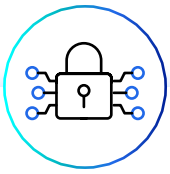
- **Passive network monitoring**
- **Integration with IT management systems**
- **Safe active querying**
- **Security controls**
  (e.g. endpoint protection and response, firewall logs and configurations, and more)
- **Operational hierarchy representation within the platform**
- **Industrial native data sources (e.g. DCS, SCADA, Historians)**
- **OTORIO's unique vulnerability database**
- **OTORIO's threat intelligence and known publications (e.g., ExploitDB)**

This data is used to construct a network topology graph based on three main CDT entities:



Assets

This includes their unique characteristics, security configurations, vulnerabilities, and operational criticality. These can be targets or entry points for a potential attack.



Network connections

These are the edges that connect assets using various protocols. Connections represent both potential accessibility in the network (e.g., based on FW configurations and open ports) and actual communication (based on traffic monitoring).

Operational processes

Provide the grouping of assets and process hierarchy according to the customer's business goals.

Once the relationships between the different entities are established, OTORIO's CDT algorithm calculates the Attack Graph, to show the potential paths among all entities.

Sample use case - Internet access to a critical asset causing a high-risk to workers' safety

In this example, the CDT predicted an attacker's path from an unmanaged asset that is exposed to direct access from the internet to a critical asset in the OT network. A series of vulnerabilities and misconfigurations could be exploited to allow an attacker to remotely execute malicious code on a CompactLogix controller. Such exploitations have the potential to cause serious physical damage to the operational system, and poses a risk to operators' on-site safety. CDT prioritizes this attack vector as critical risk and provides specific guidance for immediate and next-day mitigations. These include identifying unassigned assets, restricting insecure protocols, hardening security configurations related to the identified vulnerability and also the recommended patch for the next maintenance window.

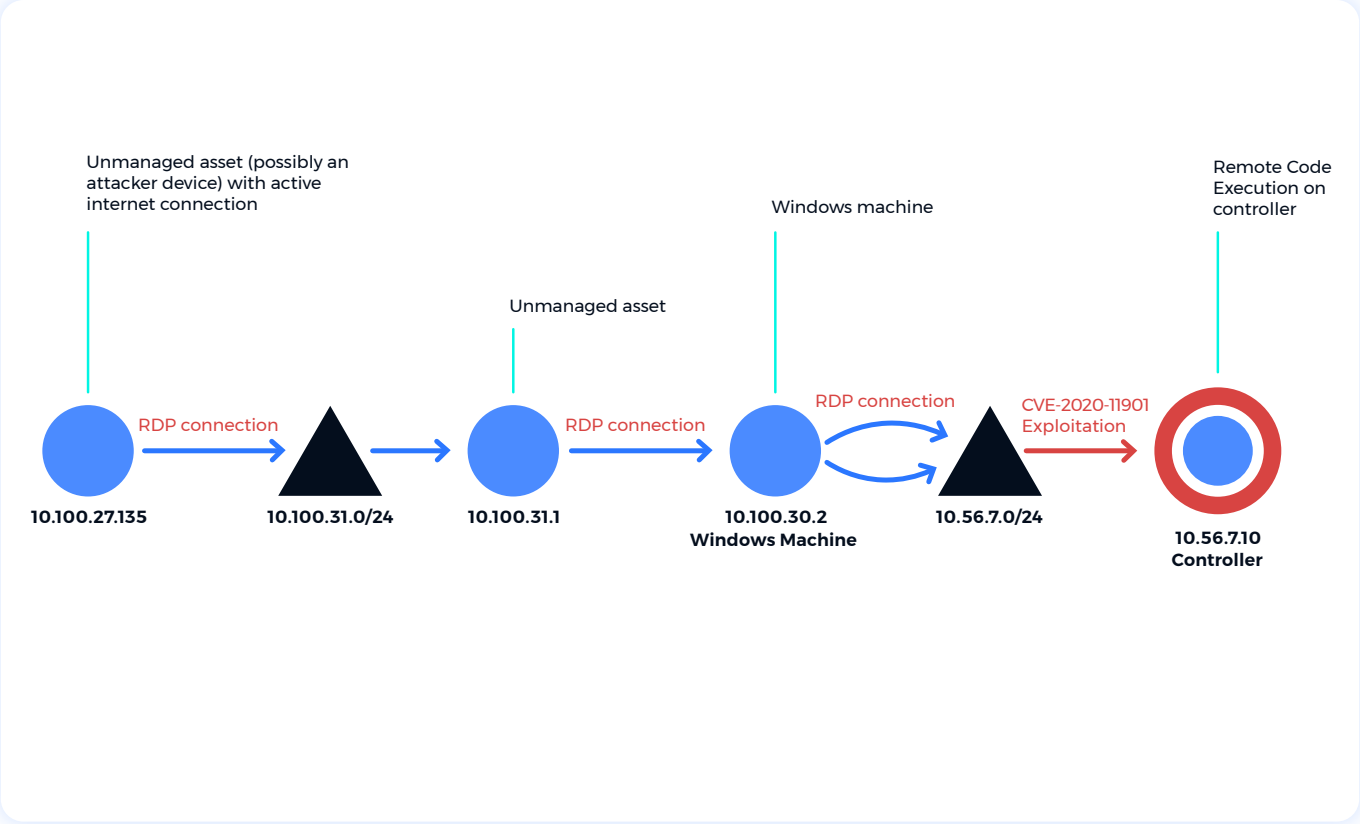


Image 3: Example of an attack vector

Deliverables: OTORIO Cyber Digital Twin

- **A visual representation of the network topology** for easy navigation between assets, their vulnerabilities, and the connections among them.
- **Analysis of inter-process communication** to review connections between different operational processes based on connection type, and identify connections that lead to vulnerable assets.
- **Identification of top assets by centrality.** This includes identifying assets that may not be critical from a business perspective, but could affect a large number of assets in the network, and therefore require more attention.
- **Examples of top attack vectors,** with full paths for review.
- **Highlighting segmentation gaps** that allow access to target assets in the network, prioritized by which assets are affected, with top firewall rules that should be considered for restriction.
- **Top vulnerabilities for mitigation,** taking into account vulnerability score, asset criticality, and the exposure level of the asset to potential attacks in the network.
- **Top assets for security hardening** due to their involvement in major attack vectors.
- **Recommendations for restricting connections between assets** as a way to block major attack vectors and reduce risk to critical processes.
- **Attack graph analysis report** with an executive summary, statistical data, detailed findings, top attack vectors, and the specific action items to mitigate critical risks.

Summary

The OTORIO Cyber Digital Twin helps improve the efficiency and effectiveness of risk reduction efforts. It does so by providing a prescriptive security posture assessment with practical mitigation steps that are prioritized according to the exposure and exploitability of vulnerabilities. This empowers OT security practitioners to proactively take action to reduce risks by understanding potential attack vectors and validating recommended changes in a safe, sandboxed environment, in the context of their existing operational processes and communication. With OTORIO CDT, you can advance your automation security efforts and ensure more cyber-resilient operations.

About OTORIO

OTORIO's industrial-native OT security platform enables industrial organizations to achieve an integrated, holistic security strategy. Together with its partners, OTORIO empowers operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

CN 120123