A GATHID LABS SERIES: EPISODE 1

Bridging Operational Technology and Information Technology

Identity Governance Solutions for Industrial Companies

As industrial companies embrace digital transformation, they increasingly straddle two worlds: the traditional domain of operational technology (OT), consisting of physical machines and equipment, and the digital realm of information technology (IT), which includes cloud services, third-party applications, on-premises servers, etc. While these two areas were once distinct, advancements in technology such as smart devices, artificial intelligence, and compliance are now compelling their convergence into a unified industrial landscape.

The Benefits and Challenges of IT/OT Convergence

The convergence of OT and IT offers immense benefits, such as increased operational efficiency, preventative security insights, and predictive maintenance capabilities. However, it also introduces a significant challenge - governing identities and their access across both physical and digital systems. Managing user identities across these two distinctly separate environments is complex, especially when it comes to ensuring security and compliance.

One of the key issues is that OT and IT systems are often air-gapped, and contain unrelated identities and complex, disparate data structures and physical infrastructure. Many industrial businesses are left dealing with multiple siloed sources of identity data, which leads to security vulnerabilities and inconsistent access governance, that may result in "toxic role combinations", where users have excessive or inappropriate access to critical systems, posing a security risk.

Limited Visibility and Governance Gaps

In many industrial organizations, OT and IT are managed by separate teams with different expertise, processes, and priorities. OT teams, for instance, often focus on safety and operational reliability, while IT Security teams prioritize cybersecurity and data protection. This separation creates challenges when it comes to aligning identity and access management (IAM) across both environments.

Identity governance in OT is often managed by physical security personnel and operational engineers who are often not integrated into broader IT governance processes. As a result, Chief Information Security Officers (CISOs) and Chief Information Officers (CIOs) frequently lack simple visibility into who has access across the entire organization. Without this visibility, it becomes difficult to ensure that all access is properly monitored and managed, leaving critical systems exposed to potential threats.

Addressing the Challenge with Advanced Technologies

So how can industrial companies bridge the gap between OT and IT identity governance? The answer lies in advanced technologies such as digital twins and knowledge graphs. These tools provide a way to unify identity and access data across both physical and digital systems, offering organizations a comprehensive view of their identity landscape.

- **Digital Twins**: A digital twin is a virtual model designed to accurately reflect a physical object, process, or system. Digital twins can model an organization's entire identity and access environment, including OT and IT systems. It can update dynamically based on data from across the enterprise, offering insights into related user access, role changes, and potential vulnerabilities.

- **Knowledge Graphs**: A knowledge graph is a data structure that models relationships between entities (such as people, places, and concepts) using nodes and edges to represent entities and their connections. It facilitates advanced data integration and analysis, commonly used in areas like semantic search, recommendation systems, and AI, to enhance decision-making and information discovery.

  Knowledge graphs can be used to help visualize complex relationships between user identities, roles, permissions, and system resources. By consolidating data from various sources, knowledge graphs provide a structured model of interconnected information, enabling organizations to easily identify and address access risks.

Looking Ahead

As OT and IT systems continue to converge, it's clear that a proactive approach to identity governance is critical. Leveraging digital twins and knowledge graphs can help industrial companies gain more comprehensive visibility into their identity and access ecosystem, ensuring that they improve and maintain the security and efficiency of their operations. In upcoming posts, we'll explore the role of these technologies in more detail and examine how businesses can take action to secure their identity landscape.

Stay tuned as we dive deeper into the solutions that will help industrial organizations navigate the complexities of IT/OT convergence.

Schedule a Demo | Learn More | Read Online