A GATHID LABS SERIES: EPISODE 2

Bridging Operational Technology and Information Technology

The Role of Digital Twins and Knowledge Graphs in Identity Governance

In the first post of our series, we discussed the convergence of operational technology (OT) and information technology (IT) in industrial businesses. As these two domains increasingly overlap, managing identity and access across both physical and digital systems becomes more complex.

In this post we'll explore how two innovative technologies, digital twins and knowledge graphs, can help to enable and secure identity governance practices.

What is a Digital Twin?

A digital twin is a virtual representation of an organization's entire identity and access ecosystem, spanning both OT and IT systems. Populated with data from across the enterprise, this dynamic model represents the constantly evolving identity landscape .

Unlike static records, digital twins are powered by contextual data that enables monitoring and predictive analytics. This means that changes in identity, access rights, or system roles are automatically detected and flagged for action. By providing connected visibility, digital twins can help organizations to mitigate risks and address potential security threats earlier than before.

How Digital Twins Support Identity Governance

In the industrial sector, where OT and IT systems often operate in silos, achieving comprehensive identity governance is challenging. Digital twins help bridge this gap by offering a unified view of all identities and access privileges, enabling organizations to govern identities more effectively across their entire landscape. This is particularly useful for hybrid and multi-cloud environments.

For example, a digital twin can provide administrators with insights into who has access to critical OT assets, such as programmable logic controllers (PLCs) or supervisory control and data acquisition (SCADA) systems, while simultaneously showing their access to IT resources like cloud servers and data centers. This unified view simplifies the identification of inconsistencies, inappropriate access, and potential conflicts between roles.

Introducing Knowledge Graphs for Identity Relationships

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 map the connections between users, roles, permissions, and systems. By aggregating data from various sources, it creates a model of related information, revealing how users interact with both OT and IT environments.

For instance, employees in an industrial organization may have different levels of access to factory machinery (OT) and cloud-based analytics tools (IT). A knowledge graph visualizes these access privileges, making it easier to enforce consistent governance policies and identify security risks.

The Power of Combining Digital Twins and Knowledge Graphs

When combined, digital twins and knowledge graphs offer a powerful foundation for identity governance. While digital twins provide a real-time reflection of the identity landscape, knowledge graphs organize the contextual data and properties of those identities. Together, these technologies enable industrial businesses to view their identity and access environment in unprecedented detail.

Here's why this combination is so effective:

- **Dynamic Modelling**: As new identities, roles, permissions, and access changes occur, gaining insight and understanding impacts of the changes allow verification that identity data remains appropriate.

- **Contextual Monitoring**: Organizations can be notified of changes in access across both OT and IT environments and understand the broader context behind these changes. This insight allows them to proactively identify potential risks and take informed actions.

- **Versatile Analytics**: These technologies offer the flexibility to model data and gain a macro or micro view of identities and access patterns. Enabling dynamic role mining, automated compliance checks, or access reviews by department or asset type, digital twins and knowledge graphs provide the analytical tools necessary for robust, secure, identity governance, even covering air-gapped applications.

A Holistic View of Identity Governance

Industrial organizations require the ability to achieve a holistic view of Identity and Access Management (IAM) and Identity Governance and Administration (IGA). This unified approach closes the gap between OT and IT, ensuring that identity governance is consistent, secure, and scalable across both physical and digital systems.

By leveraging these advanced technologies, businesses can streamline identity governance processes, reduce security risks, and meet industry regulations. As the convergence of OT and IT accelerates, the need for a comprehensive view of identity management will only become more critical.

What's Next?

In the next post in our series, we'll delve deeper into the principles of OT cybersecurity and explore how identity governance plays a critical role in protecting industrial operations. Stay tuned to learn how to safeguard your critical systems with cutting-edge technologies like digital twins and knowledge graphs!

Schedule a Demo | Learn More | Read Online