A GATHID LABS SERIES: EPISODE 3

Bridging Operational Technology and Information Technology

Identity Within the Six Key Principles of OT Cybersecurity

As industrial environments experience an increasing convergence between operational technology (OT) and information technology (IT), maintaining a secure and efficient identity governance strategy becomes critical. Gathid's innovative approach—combining digital twins, daily identity and access data snapshots, and knowledge graph technology—offers businesses the tools they need to streamline identity governance across complex, disconnected systems.

In this post, we'll explore how Gathid's platform aligns with the Six Key Principles of OT cybersecurity, as outlined by international cybersecurity agencies like the Australian Signals Directorate (ASD) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA). These principles provide essential guidelines for securing OT environments, and Gathid's patented technologies help organizations ensure compliance, security, and visibility across both OT and IT landscapes.

1. Safety is Paramount

Safety risks span across physical, OT, and digital environments. For industrial companies, a breach in any one of these areas could result in operational disruptions or even physical harm. Gathid's daily identity models offer in-depth visibility into who has access to critical OT and IT systems, as well as physical facilities. By regularly identifying access discrepancies that could compromise safety, Gathid helps organizations enforce security policies proactively.

Whether it's controlling access to a factory floor or an industrial control system, Gathid's platform ensures that businesses have a clear, comprehensive view of their entire access environment. This directly supports the principle of maintaining safety across all systems.

2. Knowledge of the Business is Crucial

Understanding the full business context is essential when managing access to OT systems and physical assets. Gathid's identity graph provides a unified view of all access rights. With this holistic view, decision-makers can ensure that identity and access decisions are made in the context of overall business priorities.

This feature supports the principle of ensuring business decisions are informed by complete, up-to-date data—allowing companies to manage access without compromising productivity or operational integrity.

3. OT Data is Extremely Valuable and Needs to be Protected

OT systems underpin essential services like energy, water, and healthcare, making them prime targets for cyberattacks. Protecting the sensitive data within these environments is crucial to maintaining public safety and avoiding disruptions to critical services.

Gathid's digital twin technology captures daily snapshots of access to OT systems, allowing organizations to regularly review and address any anomalies in access permissions, with context to other related (although technically disconnected) systems. This proactive approach helps businesses safeguard their OT data and ensure that security policies are enforced across both physical and digital systems, aligning with the principle of protecting valuable OT data against cyber threats.

4. Segment and Segregate OT from All Other Networks

Segmentation and segregation are fundamental security principles for keeping OT systems isolated from external networks and preventing unauthorized access. Gathid's platform helps businesses visualize the relationships between identities, access rights, and systems across OT, IT, and physical environments. This visualization allows system administrators to identify areas where segmentation is necessary and enforce appropriate access controls.

By highlighting the interconnections between users and systems, Gathid enables organizations to maintain the secure segmentation of their OT networks from other areas, ensuring compliance with this key cybersecurity principle.

5. The Supply Chain Must Be Secure

Industrial businesses often rely on complex supply chains, which can introduce significant security risks if third-party access to OT systems isn't properly governed. Gathid's Identity Graph helps businesses monitor and visualize all third-party access to OT and IT systems, providing a clear overview of how external vendors, contractors, or suppliers could interact with critical infrastructure.

By ensuring that only authorized third parties have access to specific assets, Gathid reduces the risk of supply chain-related vulnerabilities. This aligns with the principle of securing the supply chain by ensuring that third-party access is governed, reviewed, and minimized wherever possible.

6. People Are Essential for OT Cybersecurity

The human element remains critical in managing OT and IT security. Gathid provides security teams, administrators, and OT engineers with the tools needed to manage access across complex, diverse systems. Daily snapshots of identity data allow these teams to monitor for unauthorized access or misconfigured permissions, ensuring they can respond quickly to any access-related anomalies.

By keeping everyone—from IT administrators to OT security personnel—aligned with up-to-date identity and access data, Gathid supports collaboration across departments. This helps ensure that human insight and action remain central to the organization's security efforts, reinforcing the principle that people are essential to maintaining OT cybersecurity.

A Unified Approach to OT and IT Security

By aligning with the Six Key Principles of OT Cyber Security, Gathid's platform offers industrial organizations a robust solution for managing identities across the converging landscapes of OT and IT. Whether it's ensuring safety, protecting valuable data, or securing the supply chain, Gathid provides the tools needed to maintain a strong, holistic identity governance strategy.

As the convergence of OT and IT continues to evolve, businesses will need advanced solutions to address the growing complexity of identity management. Gathid's low-touch, high-value solution simplifies these challenges, offering the visibility, insight, and security needed to navigate this shifting landscape.

What's Next?

In the final post of our series, we'll examine real-world case studies that showcase how Gathid's platform has been successfully deployed to address identity governance challenges in industrial environments. Stay tuned for insights into how businesses are using digital twins and knowledge graphs to secure their OT and IT systems!

Schedule a Demo | Learn More | Read Online