Deloitte.

Emerging technologies 5x5 series: Insights and actions

Cyber digital twin: Building blocks of a secure Industry 4.0 metaverse

Cyber physical systems are integral parts of the operations of day-to-day life, business, infrastructure, and care of the physical world. Operating cybersecurity digital twins allows an organization to analyze and secure these systems with minimal impact to critical processes and infrastructure. A cyber digital twin is a high-fidelity virtual representation of a physical component, asset, system process, or environment. It provides a real-time automated platform that can be leveraged to simulate a 3D environment to visualize automated system responses and is used to identify and mitigate potential risks to help reduce unnecessary expense and exposures.

5 things you should know	*5 actions you can take*
Cyber risk isn't just about information technology security. It ripples through many aspects of an organization's operations—from the critical assets used to the products developed and manufactured. Assessing the cyber posture of critical assets is often a challenge since it can cause business impacts and unplanned downtime.	1 **Non-invasive cyber posture assessment:** Cyber digital twins bring novel capabilities that create replicas of critical industrial processes and assets. The replicas can facilitate cyber posture assessments that are non-invasive. Non-invasive assessments can help identify security weaknesses and provide guidance on mitigating active threats and attack scenarios.
Cyber attacks on critical infrastructures are on the rise, and organizations are catalyzing their efforts to train personnel on incident response. But the critical industrial systems and testbeds can be expensive. And recreating cyber scenarios on physical systems could potentially cause actual damage to the physical asset, which may decrease the reusability of the systems and increases the cost of the training.	2 **Incident response training:** Cyber digital twins facilitate hands-on training using virtual testbeds that closely replicate the physical processes. The training provides better understanding of how the system may behave in case of cyber scenarios and provides playbooks that can be leveraged during a cyber incident.
With the increase in interconnectivity, the industry is seeing **an influx of novel solutions** that automate, secure, or catalyze the existing workflows. For critical industrial processes, it is difficult to test integrations and dataflows. Minor changes in the tech stack could require a significant budget to test and modify the integrations.	3 **Tool rationalization:** The virtualization capabilities of the cyber digital twin can replicate critical dataflows and integrations at a much lower cost. Organizations can reuse the virtualized model to test a diverse set of integrations and can help optimize their tech stack.
The scale and criticality of industrial systems make **the identification of vulnerabilities and crown jewel assets a major industrial challenge.** The mitigation efforts are confined within the planned maintenance windows, and the security teams need to focus their efforts on the relevant assets.	4 **Managed vulnerability rationalization and business impact analysis:** The cyber digital twins help the security team identify mission-critical assets and provide insights on active attack paths that could lead to a major business impact. This analysis can be periodically repeated to provide daily insights, which can help the security team manage active attack surfaces.
Cyber risk isn't just about data centers. It extends into the cloud, across third-party networks, through edge devices, and to connected devices. High connectivity creates a dynamic tech stack, and organizations are constantly looking to enrich their capabilities through new technologies.	5 **Technology prototyping:** Using the cyber digital twin, organizations can investigate the impact of security updates, tools, and new technology integrations. The cyber digital twin can act as a prototyping environment, allowing a full investigation of integrations, disruptions, and implementation deployments.

Want to see this live? Come see us at the Cyber IoT Studio or *The Smart Factory @ Wichita!*

Connect with us:

WENDY FRANK
Principal | Cyber IoT Leader
Deloitte & Touche LLP
wfrank@deloitte.com

RAMSEY HAJJ
Principal | Cyber IoT
Deloitte & Touche LLP
rhajj@deloitte.com

ANNE ROBBINS
Senior Manager | Cyber IoT
Deloitte & Touche LLP
anrobbins@deloitte.com

RISHABH (GEORGE) DAS, PhD
Advisory Specialist Master | Cyber & Strategic Risk
Deloitte & Touche LLP
rishadas@deloitte.com