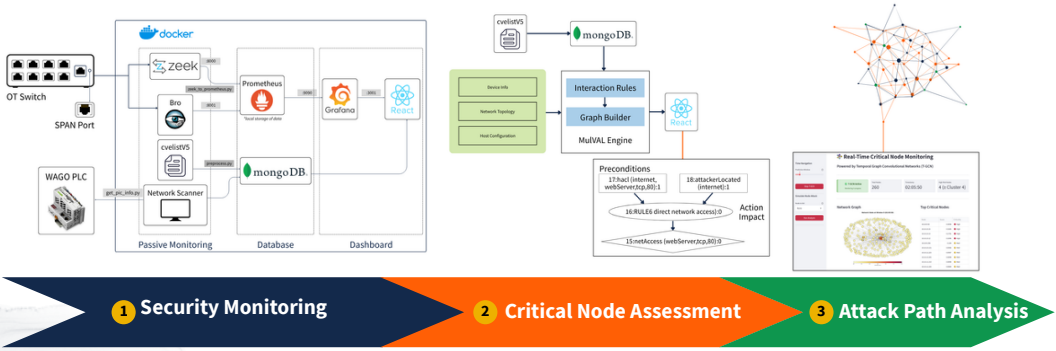
THRUST 4: EVALUATION

SECURITY MONITORING PLATFORM

Many industrial systems are still relying on outdated protocols and security mechanisms. To further complicate the issue, the rapid growth of IoT devices is often deployed with limited security considerations. This results in systems being susceptible to attacks and operational inefficiencies. A flexible and customizable network monitoring platform is required to understand how weaknesses can propagate across complex networks and effectively respond to threats as well as adapting to the diverse requirements of critical infrastructures.



The core of the monitoring platform is an end-to-end monitoring pipeline that transforms raw network traffic into actionable security insights. It is designed to give operators a clear and intuitive understanding of complex systems. The monitoring platform is connected to SPAN ports and uses Zeek, Prometheus, and Grafana pipeline to monitor and visualize network traffic for vulnerabilities and anomalies. The security monitoring tool is integrated with a Graph Convolutional Network (GCN) model to process network traffic and categorize assets according to their criticality levels. This enables operators to prioritize defense strategies on the most vital assets, optimizing the limited resources available.

After identifying critical assets, the attack graph tool models potential attack paths across interconnected systems, capturing how vulnerabilities can be exploited in sequence. By visualizing how threat propagates, the system enables operators to prioritize mitigation strategies at the most critical points of failure.

Related publication: Tan, H. C., Kalbarczyk, Z., & Nicol, D. M. (2025). A Scalable Framework for Security Monitoring and Vulnerability Assessment in Smart Cities.