Securing a Heterogeneous Distributed Data Mesh in DDIL Environments

Darren Pulsipher
Chief Solution Architect for Public Sector
Intel

As the edge becomes more capable, developers are looking at how to exploit all of the power at the edge for AI inference, data compression, and data analytics in a distributed manner. Deploying microservices and data transformations on edge requires new ways to securely deploy microservices on heterogeneous devices in a large edge ecosystem. Additional cybersecurity vulnerabilities arise when the data transformation microservices consume and publish information from data streams distributed over the mesh.

Specifically, there is a need to protect the data mesh from bad actors from eavesdropping on data streams, injecting information into data streams, taking data transformation microservices, and manipulating data transformation micro-services.

This session will expose the attack vectors inherent in data meshes, the obstacles to overcome in heterogenous DDIL environments, and the potential for undetectable snooping and spoofing attacks. Then the session will focus on defending against these cyberattacks, using a holistic systems architectural approach to securing the data streams, data mesh, transformational algorithms, and AI models.