Wednesday, June 26, 2024

11:00 AM - 11:20 AM

DataBee from Comcast Technology Solutions- From Golden Shackles to Golden Age: Breaking the Dependency on Security Vendor-Specific Configurations

Jill Cagliostro

Director of Product Management

Comcast

Abstract:

Once a security tool is fully deployed in the network and environment, it becomes near impossible to change out vendors without significant operational impact. The impact is more than just replacing the existing solution, it's also updating all upstream and downstream integration points, such as custom detection content or log parsers. This leads potentially gaps in coverage due to limitations in the tooling deployed and the tools desired. Not to mention, those golden shackles really hurt the wallet, or security budget. We'll cover the principles, practices, patterns, and other opportunities that help DISA unshackle the golden handcuffs to get the full potential out of your IT investment by beginning your journey to a vendor agnostic approach to security. Leverage Zeek offerings via BluVector and standardizing to open-source detection formats like Sigma detections into your existing security tooling and operations. Learn how to leverage the metadata of Sigma Detections such as MITRE ATT&CK tags to chain together patterns of events. We'll cover an example of automating threat hunting activities to reduce the noise by chaining together Sigma Detections with Zeek logs in BluVector to look for evasive malware and modeling Advanced Persistent Threats.

By the end of the talk, we'll understand a roadmap for how we can transform into open architecture that's vendor agnostic, enabling the offboarding of redundant systems with ease. Enter the Golden Age of security operations by optimizing for your use cases, not which vendor was there first.