Thursday, August 18, 2022
12:00 NOON – 12:20 PM
Rethinking Sensor Collection Strategies Through Security At Scale Principles

Mike Saxton
Director, Threat Hunt and DFIR
Booz Allen Hamilton

Abstract:
Organization's data needs are not slowing down. In fact, 71% of organizations today feel that their data is growing at a concerning rate. Federal organizations are facing the challenge of defending enterprises at the multi-million endpoint scale and traditional approaches to security fall apart at the size of Government. This requires new methods for collecting and detecting threats at the petabyte to exabyte scale. Organizations, such as the Army, are not immune to this challenge, but rather more susceptible as the needs of the networks must always match the needs of the Warfighter. Multi-cloud environments, microservices, and observability, logging, and tracing will only add to the Army's need for a broader strategy to providing a Common Operating Picture for Situational Understanding. As more data is moved to the cloud, especially multiple cloud environments, careful consideration should be given to how data is used and transported.

Centralized platforms provide a tremendous opportunity for long-term searches, yet operational teams struggle to gather timely and necessary information due to the volume of data stored. To meet the needs of both operational Security Operations Teams and Commander's requiring real-time information, while also meeting the needs of having long-term storage, moving to a Federated Data Model provides a new approach to gathering real-time data, while offering the speed necessary for results in real time. A federal data model exists where data is stored in the individual locations where the data is created, while only bringing back information necessary for the questions being asked. Also called, cross-cluster searching, this approach lets organizations leave data where it's at, orchestrate a search that is spread across all the locations and return results. The data can still be shipped to a central location; however this approach allows operations analysts to access the data when they need it which out shipping delays. In addition to cross-cluster searching, new capabilities exist to analyze, detect, and alert on data enroute to a central platform in real-time.

Following an approach, we refer to as Bringing the Detection to the Data, Not Data to the Detection, teams can have access to real-time information while data is streaming vice waiting for data in a central platform to decompress, index, and be available for searching. This streaming detection capability can provide situational understanding at the time the event is happening as detection is abstracted from the remainder of the shipping and storage process. Finally, this federated process allows for multi-enclave searching by only needing to transport the question or query to the other enclaves, rather than attempting to move