

GSAW 2017 Tutorial H:

How to Build a Zero-Trust Architecture

Length: Half day

Overview:

This tutorial will give overview of building a zero trust architecture based on industry standards and best practices. It will discuss the importance of zero trust in today's threat environment and then it will discuss why it is important in ground systems based on current threats.

The tutorial will be presented in two parts.

First half (2 hours):

- Building extremely secure network architectures: Zero Trust Architecture
- Zero Trust Definition
- How to build Zero Trust Architecture and the functional pieces that are required (using a real case study)
- Policy Approval using a SECOPS
- Using what is currently in place – NOT a “fork lift” change
- Correct implementation of People, Process and Technology
- Managing a Zero Trust Architecture

Second Half (2 hours):

- Discuss threats to ground systems
- Outline the standard architecture for a ground systems
- Discuss lessons learned / trends from cyber assessments on NASA's ground systems
- Discuss the principles discussed in part one of presentation and how to apply
- Focus on migrating from existing trusted to zero-trust
- Discuss building from ground up a zero trust in ground systems

Instructors: Barry Lyons IV, SGT, Inc. and Brandon Bailey, NASA IV&V

Biographies:

Barry Lyons IV: 24+ years of extensive, leading edge Cyber/ Information Assurance (IA) security expertise and systems engineering experience focusing on the architecture, design, implementation, certification and accreditation, management and operations of mission critical enterprise systems, airborne solutions, cross domain information sharing solutions, and comprehensive “Need to Know/Need to Share” On Demand Information Delivery solutions. Highly skilled in all critical disciplines and activities required for management and oversight of enterprise network and application systems. Extensive experience in large scale enterprise applications and leading edge software solutions designed specifically to meet mission critical needs. Dynamic, fun speaker.

Brandon Bailey has over 10 years of experience in the test and evaluation field with specialization in cybersecurity. Brandon has experience testing in both the intelligence and civil space arena. Recently Brandon's work at National Aeronautics and Space Administration (NASA)'s Independent Verification and Validation Program involved building and managing a software testing and research laboratory as

well as leading the information assurance and cybersecurity activities as they relate to NASA's space and ground missions. These efforts resulted in improving the security for the mission segments within NASA's enterprise which includes: vulnerability assessments, infusing secure coding principles, counteracting the threat landscape by infusing security analyses in the standard IV&V workflow and working within the CCSDS security working group to develop international security standards.

Description of Intended Students and Prerequisites:

Very basic understanding of network architectures.

What can Attendees Expect to Learn:

What a Zero-Trust architecture is and how to deploy and manage it.