Wednesday, February 15, 2023
11:40 AM – 12:00 Noon
Security-Centric Warfare: Getting Past the NO! – Leveraging Security to Enable Joint & Coalition Information Sharing

Russ Smith
Technical Director, Strategic Response Group
ZScaler

Abstract:
This presentation describes the core elements necessary to achieve a zero trust architecture, and how those core elements enable joint and coalition data sharing. Military forces have always been challenged to share information with coalition partners. Ever since coalition countries joined together, arguably dating back to European Coalition Wars of the 18th century, the inability to share information greatly hinders military effectiveness. Modern warfare requires the rapid exchange of critical battlefield intelligence and operational information, especially with joint and coalition partners.

The Department of Defense is rapidly embracing a Zero Trust Architecture (ZTA) for its data protection benefits in today's cyber domain. Additionally, of the many benefits in migrating to a ZTA, one key benefit is removing the challenge of creating a purpose-built network specifically for the duration of the contingency. Installing, Operating and Maintaining a coalition network is a slow process that is often late to need for a "fight tonight" scenario. The concept of a Mission Partner Environment (MPE) that is readily available and can support the rapid onboarding of coalition partners in a dynamic joint and coalition battlespace is needed to address today's threat.

As coalition partners undertake digital transformation journeys to increase efficiency, improve agility, and achieve a military or competitive advantage, security practitioners must keep pace. In addition, for those countries critical to the success of coalition objectives but perhaps not as far down the digital transformation journey, there must be a way to on-board those forces into the joint and coalition data sharing environment.

A successful zero trust architecture supporting coalition operations is described in this presentation through seven elements broken down into three critical activities to protect users and data:

- Verify the identity and context (who is connecting, what is the access context, and where is the connection going).
- Control the content and access (assess risk, prevent compromise, and prevent data loss).
- Enforce policy to either grant access, conditionally grant access, or deny access.

This presentation concludes by thoroughly describing the critical steps necessary to bring coalition partners into the MPE to ensure identity is verified and information is available.

- Leverage an Information Technology Service Management (ITSM) platform for automated account provisioning to create authenticated coalition force personas.
- Make the authenticated persona available as a Master User Record (MUR) to a Zero Trust platform to apply zero trust policies.

- Enforce application and data access available through policies established for individual coalition partners.
- Monitor and terminate the session once data exchange is complete.