Thursday, February 14, 2019
10:30 AM – 10:50 AM

## Steps to Security Validation - How to Measure, Manage, and Continuously Validate Your Cybersecurity

**Maj Gen Earl Matthews, USAF (Ret.)**
Senior Vice President, Strategy
Verodin

Abstract: Organizations have been managing security based on assumptions, hopes and prayers for decades. We assume our technology will detect and block that attack or leak, we hope our incident response techniques will be efficient and effective when under assault, and we pray that our security teams are well trained and practiced when everything goes wrong. But in many cases, we don't have a way to evaluate our security effectiveness let alone have any empirical evidence to back up our assumptions. In short, assumption-based security sucks.

Assumption-based security results in many negative outcomes.

- Security tool overload and shelf-ware is being predicated on a tradition of purchasing too many security buzzwords, evaluating solutions incorrectly, purchasing the wrong solutions, not tuning what we have, not retiring antiquated solutions and burning through time, money and other resources.
- Defensive regression is resulting in perhaps a once effective set of security controls no longer operating as desired because of configuration mistakes, loss of expertise and even malice.
- Poor business decision making is occurring because most of us don't know if our security spend is making us more secure, if we are investing in the right areas or if we can even communicate the state of our security effectiveness to stakeholders.

Enough is enough. We need to move beyond assumptions. We need to "know." We need to assess the efficacy of our security technology, talent and techniques. This presentation will focus on moving from assumption based security to continuous security validation and as it relates to security effectiveness.