Wednesday, May 7, 2025
12:20 pm – 12:40 pm
Advanced Cyber Deception – The Future of Cyber Defense

Sreenivas Gukal, Ph.D.
Chief Product Officer
Acalvio Technologies

Abstract:
In 2024, Google announced the first zero day detected by AI. Amazon cyber chief CJ Moses said that AWS saw a billion cyber threats a day driven by AI. University researchers published papers on how Generative AI can come up with AI agents to create exploits based on just CVE descriptions. We are in the new age of AI-driven attacks and the attacks will only get worse.

Advanced Cyber Deception (ACD) is ideal for active cyber defense against both N-day and zero-day attacks. Deception is the only security technology that allows introducing new entities into the network to create enticing false opportunities for the attacks to target, at every step of the attack progression. ACD has progressed far beyond honeypots of the old – deceptive entities now include any type of endpoint in the network, applications, document and data repositories. Deception also extends to identities, in identity repositories such as Active Directory or Cloud IAM directories, and on endpoint credential caches, cloud services such as secrets managers, Kubernetes clusters etc. With AI integrated into every aspect of deception technology, ACD is easy to use and very effective in high-fidelity early threat detection.

Automated Moving Target Defense (AMTD) based on cyber deception is the paradigm shifting technology to address AI-driven attacks. Join this session to learn about the advances in deception technology to address evolving threats.

1. Layered deception – multiple independent layers of deception that change to address different threat scenarios to provide a very effective moving target defense.

2. Just in time deception that is automatically deployed as response actions to confirm low priority alerts by other security solutions.

3. Dynamic deception that keeps changing the network neighborhood.

4. Identity deception that is pervasive – endpoints have many credential stores that attackers can steal from for lateral movement and privilege escalation. NSA and five eyes intelligence agencies recently published a paper on the attacks against Active Directory and how deception is the only effective way.

5. Perception-changing deception – living off the land, and increasingly living off the cloud, attacks leverage native legitimate tools and cloud services. By deploying deception in these tools and services, attacker perception can be changed without actually changing the network.