AFCEA Greater Augusta Chapter Course:
Zero Trust as the Operational Backbone of CMMC

Presented by Derek Kernus and Noël Vestal
Aethon Security

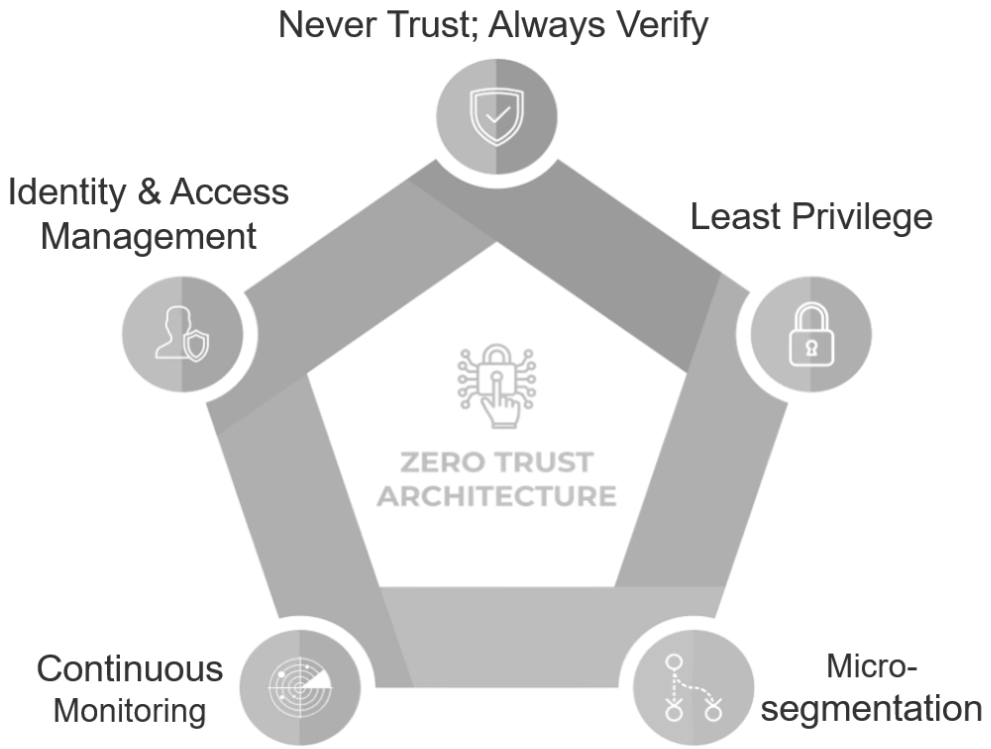
AETHON SECURITY

AGENDA

- Zero Trust Architecture (ZTA) overview
  - Why traditional security models fall short
  - Identity as the new control plane - Identity-Centric-Security (ICS)
- High level CMMC overview
- How ZTA supports CMMC
  - Using ZTA as the backbone for CMMC
  - Turning compliance into resilience
  - Continuous Monitoring CMMC requirements and ZTA
- How to get started with ZTA and CMMC
  - High level ZTA and CMMC implementation plan
  - Common pitfalls to avoid when implementing ZTA and CMMC
- Questions?

AETHON SECURITY

Zero Trust Architecture Overview



- No default trust
- Least privilege access
- Assume breach mentality
- Continuous verification
- Resource-centric security

AETHON SECURITY

Why Traditional Security Models Fall Short

AETHON SECURITY

ZTA and Identity-Centric-Security (ICS)

- **Identity-Centric Security (ICS)** makes identity the primary control point for cybersecurity
- **ICS supports ZTA** by aligning with the principle of “never trust, always verify”
- **In an ICS model, access is dynamic rather than static**, permissions can be adjusted in real time based on context, behavior, and risk

AETHON SECURITY

CMMC Overview

The Cybersecurity Maturity Model Certification (CMMC) is a verification program consisting of 3 levels put in place by the government to validate the compliance with contract regulations requiring cybersecurity protections be in place.

AETHON SECURITY

How ZTA Supports CMMC

- **It shifts CMMC from "compliance checklist" to continuous protection**
  Instead of treating access, monitoring, authentication, and data protection as one-time assessment activities, ZTA turns them into continuous controls that are enforced, measured, and improved over time.
- **It enforces least privilege (a CMMC requirement) and reduces blast radius**
  Zero Trust assumes that no user, device, application, or network segment should be automatically trusted. Access is granted based on identity, device health, role, location, sensitivity of the data, and business need.
- **It strengthens protection of CUI across cloud, hybrid, and third-party environments**
  Many contractors do not operate in a simple on-premises environment anymore. CUI may exist in Microsoft 365, GCC High, GCC, cloud platforms, endpoints, file shares, collaboration tools, backups, and service provider environments.

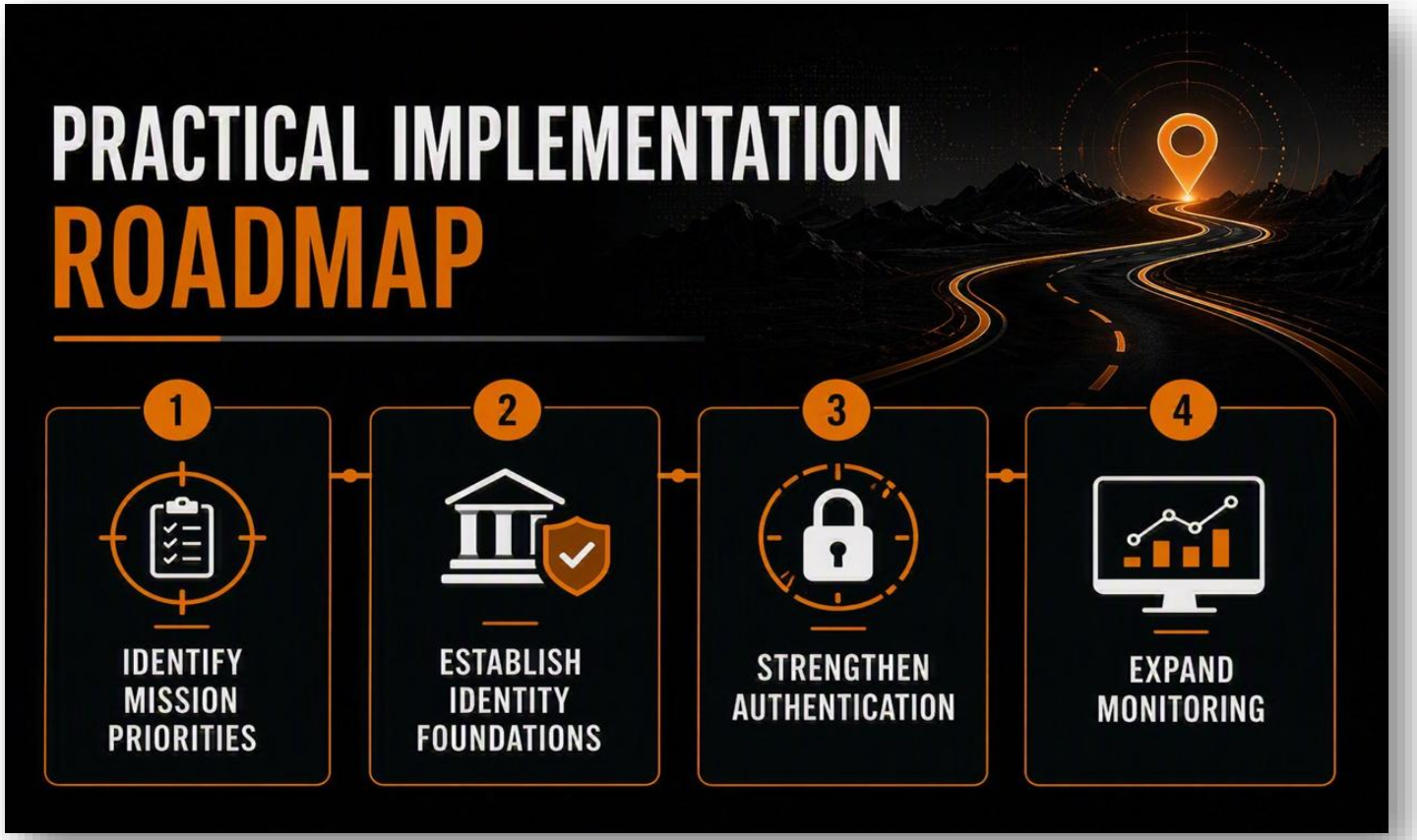
AETHON SECURITY

How ZTA Supports CMMC

- **It creates adaptability against evolving threats and future requirements**
  CMMC is a point-in-time certification, but cybersecurity risk changes constantly. Zero Trust creates resilience by giving the organization a security model that can adapt as threats and requirements evolve. Instead of relying on static perimeter defenses, ZTA supports ongoing risk-based decisions, automated enforcement, and continuous improvement.

AETHON SECURITY

How to Get Started With ZTA and CMMC



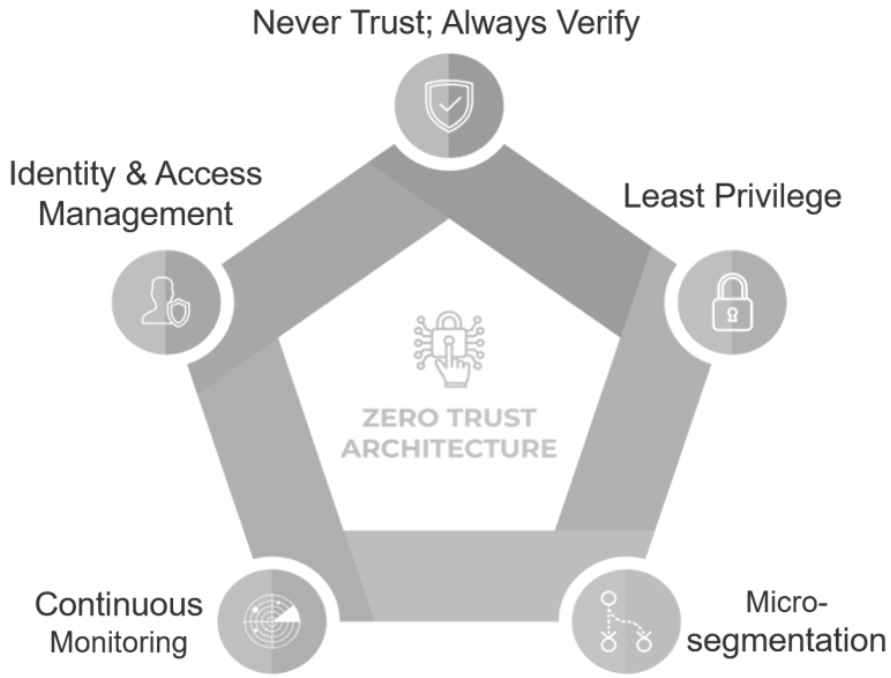
AETHON SECURITY

Common Challenges When Implementing ZTA

AETHON SECURITY

Recap and Action Items

- ZTA creates identity focused security: identity = access
- ZTA works with CMMC to create a more resilient security posture
- ZTA is built for hybrid environments and works across platforms
- ZTA creates adaptability against evolving threats and future requirements, making continuous monitoring for CMMC more effective



AETHON SECURITY

Questions?

AETHON SECURITY