Emergin
g

TECHNET
EMERGENCE

AFCEA

March 11-12, 2024 • Hyatt Regency, Reston, Virginia

March 12, 2024
Reston, Virginia

https://event.afcea.org/TNE24JOIN

Cyber –
IOT

Cyber - IOT

Emerging
Cyber
IOT

Meet your Panel

Introductions

Gurdip Singh
Divisional Dean, George Mason University
AFCEA Technology Committee

Moderator

Bryan Ward
SAIC Enterprise Solution Architect,
National Intelligence and space group
AFCEA Technology Committee

Logan Harr
Principal Director for Integrated Sensing and Cyber, OUSD R&E

Bob Flores
Founder and CTO, Applicology
Former CTO, CIA

Ken Bible
CISO, DHS

Bob Gourley
Founder and CTO, OODA
AFCEA Technology committee

Cyber - IOT

Emerging

Cyber
IOT

Today’s Mission

Cybersecurity of IoT solutions in DoD and Intelligence

Our Flight Plan

✓Panel Introductions

- Topic introductions (IoT, current and future IoT cyber issues)
- Prepared questions for Panel
- Open questions for Panel

AIxCC

AI CYBER CHALLENGE

AICyberChallenge.com

Zero Trust

In the Past . . .

Assets were protected by implementing a perimeter around the network.

Everyone (and everything) inside the perimeter was trusted;
Everyone (and everything) outside the perimeter was not.

So, a lot of emphasis (read: $$$$) was place on perimeter security.

But, when the perimeter was breached, the attacker could then act as a trusted entity.

And then . . .

Mobile and Cloud dissolved the perimeter.

In fact, the network and perimeter were now software-defined.

So, protection mechanisms had to change.

Thus begat the concept of Zero Trust.

Zero Trust is NOT . . .

A product.

A tool.

A single technology solution.

Something you can touch.

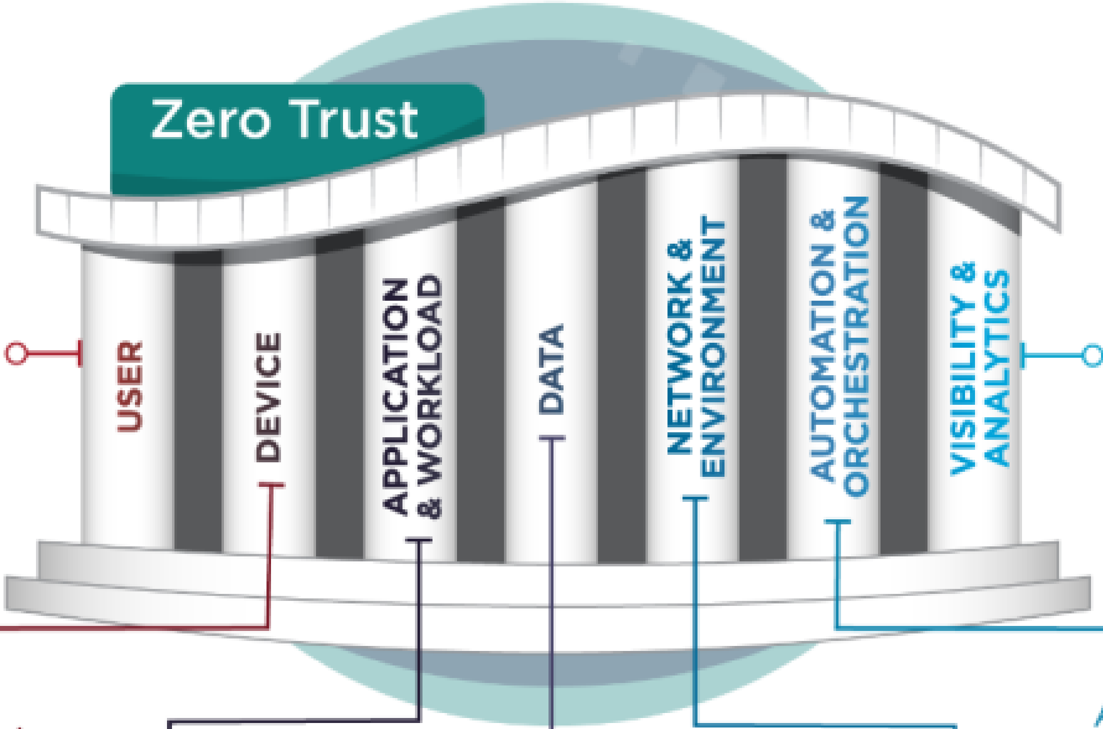
Zero Trust IS . . .

A concept. A framework.

NIST: the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources.

A collection of methodologies that drives these key principles:

- Trust nothing. Verify everything.
- Authentication of Identity (humans and not) *always* precedes connectivity, and then is continuously re-verified.
- All identities follow a least-privilege access model.
- Applications (and their environments) remain invisible until Identity is verified.
- Encryption is enabled end-to-end.
- Micro-segmentation of the network.
- Continuous analytics.



Continually authenticate, assess, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Understand the health and status of devices to inform risk decisions. Real time inspection, assessment and patching informs every access request.

Secure everything from applications to hypervisors, to include the protection of containers and virtual machines.

Data transparency and visibility is enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automate security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Segment, isolate and control (physically and logically) the network envrionment with granular policy and access controls.

Source: NSA

Emergin g

Horizon

Special

Bryan Ward and Gurdip Singh

https://event.afcea.org/**TNE24JOIN**