IDENTITY & ACCESS MANAGEMENT – A ZERO TRUST JOURNEY

April 29, 2025

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

CYBER HAWAII

ABOUT CYBERHAWAII

CyberHawaii is an information sharing and analysis non-profit organization committed to developing and enhancing Hawaii’s cybersecurity capabilities

- CyberHawaii is committed to a whole community approach that will help to:
  - Mitigate cyber risks for all community members
  - Develop educational and workforce pathways for students
  - Augment cyber services being delivered by government agencies, commercial entities, research organizations and Community Based Organizations
  - Inform local decision makers about cyber security risks and solutions
- Founded 2016
- Part of CyberUSA network
- Supported by corporate memberships and grants

CYBER HAWAII

CYBERHAWAII MEMBERS & STRATEGIC PARTNERS

Growth

HAWAI'I PACIFIC HEALTH

HAWAII STATE FEDERAL CREDIT UNION

KAMEHAMEHA SCHOOLS 1887 IMUA

SERVCO

UNIVERSITY OF HAWAI'I

First Hawaiian Bank

Hawaiian Electric

Hawaiian Telcom

Matson

UHA HEALTH INSURANCE

Sustaining

DRFORTRESS

TECHMANA

HAWAI'I COMMUNITY FOUNDATION

DELTA DENTAL HDS Hawaii Dental Service

hmsa

referentia

Strategic Partners

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Office of Homeland Security State of Hawaii

UNIVERSITY OF HAWAI'I

NAVAL CRIMINAL INVESTIGATIVE SERVICE

U.S. COAST GUARD 14TH DISTRICT

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security Investigations

UNITED STATES SECRET SERVICE

UNITED STATES ARMY

DEPARTMENT OF EDUCATION STATE OF HAWAII

STATE OF HAWAII 1959

INFRAGARD

HAWAII DEFENSE ALLIANCE

DBEDT

Kaimana Hila

And Others

CYBER HAWAII

IDENTITY & ACCESS MANAGEMENT – A ZERO TRUST JOURNEY

2025 CyberHawaii/CISA Fortify Cybersecurity Education Series

ADMINISTRATIVE

- Enter questions into chat box
- Presentation being recorded & will be posted by CyberHawaii website
- The presenter has agreed that you can contact them after his presentation if you have questions or would like more information
- Please remain on mute during the presentation until designated Q&A sessions

CYBER HAWAII

PRESENTERS

Giovanni Williams
Cybersecurity Advisor
Cybersecurity & Infrastructure Security Agency (CISA)

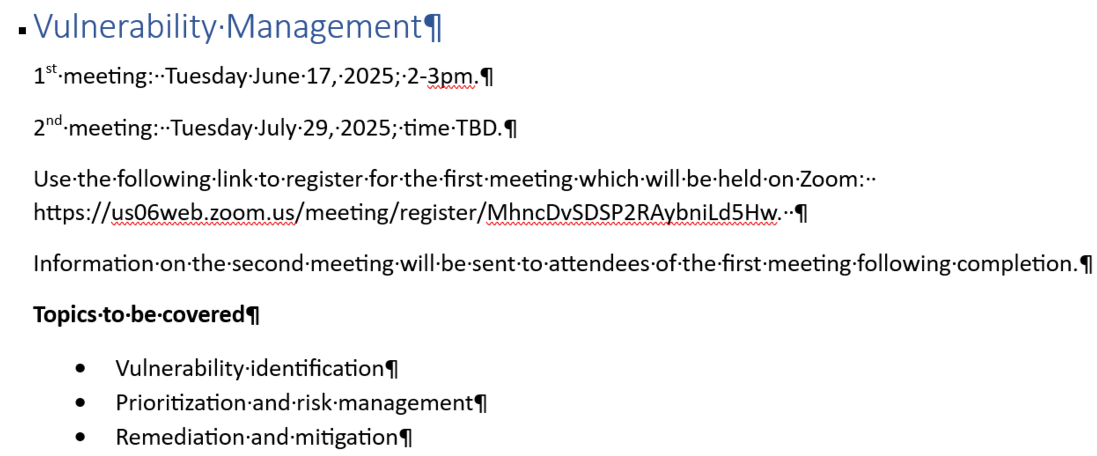
Giovanni.Williams@mail.cisa.dhs.gov

MAHALO - SI YU'US MA'ÅSE – THANK YOU

Next session: Identity & Access Management – A Zero Trust Journey Part 2

- Tuesday May 28, 2025, 2pm Hawaii time
- In person attendance @ CyberHawaii in Manoa Innovation Center
- Remote attendance via Zoom
- Participatory discussion
- Email invitation to be sent

Upcoming Series



- Vulnerability·Management¶

1st·meeting:··Tuesday·June·17,·2025;·2-3pm.¶

2nd·meeting:··Tuesday·July·29,·2025;·time·TBD.¶

Use·the·following·link·to·register·for·the·first·meeting·which·will·be·held·on·Zoom:·· https://us06web.zoom.us/meeting/register/MhncDvSDSP2RAybniLd5Hw.··¶

Information·on·the·second·meeting·will·be·sent·to·attendees·of·the·first·meeting·following·completion.¶

Topics·to·be·covered¶

- Vulnerability·identification¶
- Prioritization·and·risk·management¶
- Remediation·and·mitigation¶

DEFINITION

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.

ZTA is an enterprise’s cybersecurity plan that uses zero trust concepts and encompasses component relationships, workflow planning, and access policies.

Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan.

Source: NIST SP 800-207: Zero Trust Architecture 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

KEY CONCEPTS

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

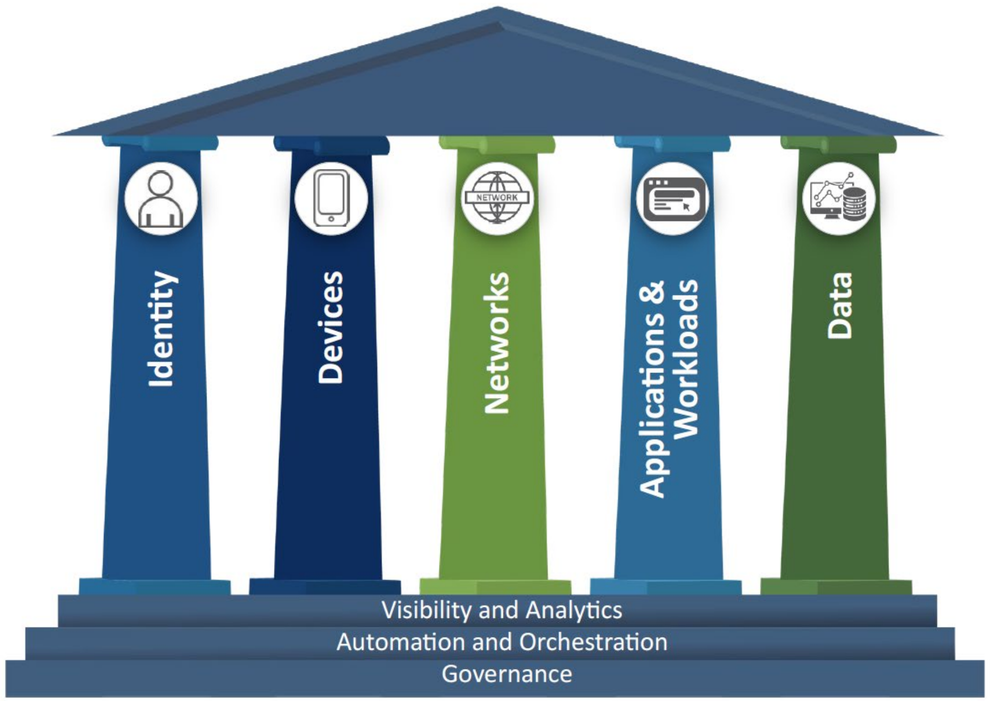


Figure 1: Zero Trust Maturity Model Pillars[8]

CHALLENGES

- Most organizations operate on “implicit” rather than “explicit” trust
    - Cultural change
- Senior leadership not involved
- Expensive to modernize legacy systems