Introduction to DOD Zero Trust

Student Guide

August 2024

Center for Development of Security Excellence

Contents

Lesson 1: Course Introduction

Introduction

Course Welcome

Welcome to the Introduction to the Department of Defense, or DOD, Zero Trust course. This course provides DOD and industry professionals, like you, an overview on the role of Zero Trust Architecture, or ZTA, in protecting DOD technology infrastructure and information.

Course Objectives

By the end of the course, you will be able to explain the role of ZTA in protecting DOD technology infrastructure and information. Here are the course objectives:

- Explain the philosophy behind Zero Trust
- Identify the policies and guidance associated with the DOD ZTA
- Describe the pillars and capabilities of the DOD ZTA
- Explain the tenets for successful adoption of Zero Trust

Lesson 2: Overview of the DOD ZTA

Introduction

Lesson Overview

Welcome to the *Overview of the Department of Defense Zero Trust Architecture, or DOD ZTA*, lesson. This lesson will introduce you to the Zero Trust concept and the policies and guidance behind it.

Take a moment to review the lesson objectives.

- Explain the philosophy behind Zero Trust
- Identify the policies and guidance associated with the DOD Zero Trust Architecture (ZTA)

DOD ZTA

What is Zero Trust?

Zero Trust is a security model, set of system design principles, and coordinated cybersecurity and system management strategy. It is based on an acknowledgement that threats exist both inside and outside traditional network boundaries. Zero Trust focuses on users, assets, and resources. This represents a shift from the “castle-and-moat” approach to cybersecurity where the user is trusted once inside the network or “castle.”

Zero Trust assumes that a breach is inevitable or has already occurred, and therefore aims to contain damage and protect data in real time. Zero Trust represents a major cultural shift in the DOD’s approach to cybersecurity.

Policies and Guidance

Several policies and guidance direct the implementation of DOD ZTA.

First, Executive Order, or EO, 14028, “Improving the Nation’s Cybersecurity,” requires Federal agencies to modernize cybersecurity practices. Next, the Office of Management and Budget Memorandum, OMB M-22-09, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” establishes a Federal ZTA. In addition, the National Institute for Standards and Technology Special Publication, or NIST SP, 800-207, “Zero Trust Architecture,” outlines migration steps, standards, and guidance for transitioning to a ZTA. Finally, the DOD Zero Trust Strategy defines the DOD’s approach to shift to a ZTA.

EO 14028

Improving the Nation’s Cybersecurity, May 2021
Directs the Federal agencies to modernize their cybersecurity approaches to identify, deter, protect against, detect, and respond to cyber threats and threat actors.

OMB M-22-09

Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 2022
Sets forth a Federal ZTA, setting goals for the Federal government where:

- Employees access necessary resources for their jobs through enterprise-managed accounts that protect against phishing attacks.
- Devices used are consistently tracked and monitored, taking device security posture into account when granting access.
- Systems are isolated with network traffic encrypted.
- Enterprise applications are tested internally and externally and are securely available via the Internet.
- Security and data teams collaborate to develop data categories and security rules to automatically detect and block unauthorized access.

NIST SP 800-207

Zero Trust Architecture, August 2020
Outlines migration steps, standards, and guidance for transitioning to a ZTA.

DOD Zero Trust Strategy

Improving the Nation's Cybersecurity, October 2022
Defines the DOD's approach to shift to a ZTA in alignment with the Executive-level guidance and DOD strategies, including:

- National Security Strategy
- National Defense Strategy
- DOD Cyber Strategy
- DOD Digital Modernization Strategy

Review Activities

Knowledge Check 1

Which of the following is a philosophy of Zero Trust?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Security breaches are preventable with a tailored security model.
- ○ Network data cannot be trusted without validation.
- ○ Once a user is verified, they are trusted inside the network.
- ○ Users both inside and outside the network must be verified.

Knowledge Check 2

Which document sets the goals for a Federal ZTA?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

Knowledge Check 3

Which document defines how the DOD will shift to a ZTA?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

Knowledge Check 4

Which document requires Federal agencies to modernize their cybersecurity approaches?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

Knowledge Check 5

Which document provides migration steps, standards, and guidance for transitioning to a ZTA?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

Conclusion

Lesson Summary

You have completed the *Overview of the DOD ZTA* lesson.

Lesson 3: Pillars and Capabilities

Introduction

Lesson Overview

Welcome to the *Pillars and Capabilities* lesson. This lesson will focus on the pillars and capabilities upon which the Department of Defense Zero Trust Architecture, or DOD ZTA, is built. Take a moment to review the lesson objective.

- Describe the pillars and capabilities of the DOD ZTA

Pillars

Overview

The foundation for the DOD ZTA, is based on seven DOD Zero Trust Pillars and their enablers to ensure standardization of execution. The pillars are:

- User
- Devices
- Applications & workloads
- Data
- Network & environment
- Automation & orchestration
- Visibility & analytics

Each DOD Zero Trust Capability aligns to one of the seven DOD Zero Trust Pillars. The capabilities range from target to advanced levels, where Target Level Zero Trust is the minimum set of Zero Trust capability outcomes and activities necessary to secure and manage risk.

Execution enablers are cross-cutting, non-technical capabilities and activities that address culture, governance, and elements of:

- Doctrine
- Organization
- Training
- Material
- Leadership and education
- Personnel
- Facilities
- Policy

The design, development, deployment, and operations of Zero Trust capabilities must account for changes and/or additions to how DOD Components execute Zero Trust across

the execution enablers. The ZT Capability baseline timelines provide the projected roadmap for achieving the ZT Target Level by the end of fiscal year, or FY, 2027.

Activities

The Zero Trust Capabilities further break down into 152 activities, 91 target, and 61 advanced activities. You may refer to the DOD Zero Trust Strategy, Appendix B, for all 152 activities.
Within each pillar are capabilities that may contain one or more target and/or advanced activities. This lesson will focus on each pillar and its capabilities. When fully developed and mature, Zero Trust overlays will result in slight modifications to the Risk Management Framework, or RMF, process. RMF security controls will be associated with Zero Trust pillars, capabilities, and activities.

Pillar 1: User

The User pillar focuses on user management to protect and secure network interactions. Under the User Pillar, the organization authenticates, assesses, and monitors user activity patterns on an ongoing basis. It then uses these patterns to govern user access and privileges. For example, you might implement identity capabilities such as multi-factor authentication, or, MFA, or Privileged Access Management, or PAM, for privileged functions to secure, limit, and enforce access to data, applications, assets, and services, or DAAS.

The user pillar capabilities and activities break down into target and advanced target levels:

- 1.1 User inventory (target level)
- 1.2 Conditional user access (target and advanced level)
- 1.3 Multi-factor authentication (target and advanced level)
- 1.4 Privileged access management (target and advanced level)
- 1.5 Identity federation & user credentialing (target and advanced level)
- 1.6 Behavioral, contextual identification, and biometrics (target and advanced level)
- 1.7 Least privileged access (target level)
- 1.8 Continuous authentication (target and advanced level)
- 1.9 Integrated identity, credential, and access management (ICAM) platform (target and advanced level)

Pillar 2: Devices

The next pillar, Devices, focuses on the devices authorized to access enterprise resources. Understanding the health and status of authorized devices helps make informed risk decisions. Real time inspections, assessments, and patching inform every access request. For example, implement solutions to monitor and manage devices, such as mobile device managers, comply to connect programs, or trusted platform modules, or TPM.

The device pillar capabilities and activities break down into target and advanced target levels as follows:

- 2.1 Device inventory (target and advanced level)

- 2.2 Device detection and compliance (target and advanced level)
- 2.3 Device authorization with real-time inspection (target and advanced level)
- 2.4 Remote access (target and advanced level)
- 2.5 Partially and fully automated asset, vulnerability, and patch management (target level)
- 2.6 Unified endpoint management (UEM) and mobile device management (MDM) (target level)
- 2.7 Endpoint & extended detection & response (EDR & XDR) (target and advanced level)

Pillar 3: Applications & Workloads

The Applications & Workloads pillar focuses on securing information technology, or IT, resources against breaches, unauthorized access, or tampering. This includes:

- Tasks on systems or services on-premises
- Applications or services running in a cloud environment
- Containers and virtual machines

Some examples of the Application & Workload pillar include implementing application delivery methods, such as proxy technologies, to enable additional protections to decision and enforcement points, and vetting source code and common libraries through development, security, and operations, or DevSecOps, practices to secure applications from their inception.

The applications and workloads pillar capabilities and activities break down into target and advanced target levels as follows:

- 3.1 Application Inventory (target level)
- 3.2 Secure Software Development and Integration (target and advanced level)
- 3.3 Software Risk Management (target level)
- 3.4 Resource Authorization and Integration (target and advanced level)
- 3.5 Continuous Monitoring and Ongoing Authorizations (advanced level)

Pillar 4: Data

The fourth pillar, Data, focuses on data management. It categorizes the organization's DAAS based on mission criticality and enables and secures data transparency and visibility using:

- Enterprise infrastructure
- Applications
- Standards
- Robust end-to-end encryption

- Data tagging

Examples for the data pillar includes the implementation of solutions such as:

- Data Rights Management (DRM)
- Data Loss Prevention (DLP)
- Software Defined Environments
- Granular data-tagging

The data pillar capabilities and activities break down into target and advanced target levels as follows:

- 4.1 Data Catalog Risk Assessment (target level)
- 4.2 DOD Enterprise Data Governance (target level)
- 4.3 Data Labeling and Tagging (target and advanced level)
- 4.4 Data Monitoring and Sensing (target and advanced level)
- 4.5 Data Encryption and Rights Management (target and advanced level)
- 4.6 Data Loss Prevention (DLP) (target and advanced level)
- 4.7 Data Access Control (target and advanced level)

Pillar 5: Network & Environment

The Network & Environment pillar focuses on:

- Segmenting, isolating, and physically and logically controlling the network environment
- Using granular access and policy restrictions

An example of this process would be implementing micro-segmentation to provide greater protections and controls over DAAS:

- Privileged access
- Internal and external data flows
- Lateral movement

The network & environment pillar capabilities and activities break down into target and advanced target levels:

- 5.1 Data Flow Mapping (target level)
- 5.2 Software Defined Networking (SDN) (target and advanced level)
- 5.3 Macro Segmentation (target level)
- 5.4 Micro Segmentation (target and advanced level)

Pillar 6: Automation & Orchestration

The sixth pillar, Automation and Orchestration, focuses on automating security responses enabled by artificial intelligence, or AI. This is based on defined processes and security

policies. A suitable example of Automation and Orchestration would include: blocking actions or forced remediation that is based on intelligent decisions.

The automation & orchestration pillar capabilities and activities break down into target and advanced target levels:

- 6.1 Policy Decision Point (PDP) and Policy Orchestration (target and advanced level)
- 6.2 Critical Process Automation (target and advanced level)
- 6.3 Machine Learning (ML) (target level)
- 6.4 Artificial Intelligence (advanced level)
- 6.5 Security Orchestration, Automation, and Response (SOAR) (target and advanced level)
- 6.6 Application Programming Interface (API) Standardization (target level)
- 6.7 Security Operations Center (SOC) and Incident Response (IR) (target and advanced level)

Pillar 7: Visibility & Analytics

The last pillar, Visibility and Analytics, focuses on analyzing events, activities, and behaviors. From these we can derive context and apply artificial intelligence/machine learning, or AI/ML, while achieving a highly personalized model that improves detection in reaction time and in making real-time access decisions. For example, based on what's learned, the organization can make changes to security policy and identify alert triggers that require a response.
The visibility & analytics pillar capabilities and activities break down into target and advanced target levels:

- 7.1 Log All Traffic (Network, Data, Apps, Users) (target level)
- 7.2 Security Information and Event Management (SIEM) (target and advanced level)
- 7.3 Common Security and Risk Analytics (target level)
- 7.4 User and Entity Behavior Analytics (target and advanced level)
- 7.5 Threat Intelligence Integration (target level)
- 7.6 Automatic Dynamic Policies (advanced level)

Review Activities

Knowledge Check 1

Which pillar focuses on the devices authorized to access enterprise resources?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads

- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 2

Which pillar implements micro-segmentation to provide greater protections and controls over DAAS?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 3

Which pillar focuses on automating security responses enabled by AI?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 4

Which pillar contains the concept that user activity must be authenticated, assessed, and monitored on an ongoing basis?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 5

Which pillar focuses on securing IT resources against breaches, unauthorized access, or tampering?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 6

Which pillar states that, based on what's learned, policy changes are made and alert triggers are identified?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Knowledge Check 7

Which pillar focuses on data management?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

Conclusion

Lesson Summary

You have completed the *Pillars and Capabilities* lesson.

Lesson 4: Tenets for Successful Adoption

Introduction

Lesson Overview

Welcome to the *Tenets for Successful Adoption* lesson. This lesson will focus on the tenets required to successfully adopt the DOD ZTA. Take a moment to review the lesson objective.

- Explain the tenets for successful adoption of Zero Trust

Seven Tenets Defined

Seven Tenets

NIST SP 800-207 defines seven tenets for the successful adoption of ZTA.

- **Tenet 1:** All data sources and computing services are considered resources.
- **Tenet 2:** All communication is secured regardless of network location.
- **Tenet 3:** Access to individual enterprise resources is granted on a per-session basis.
- **Tenet 4:** Access to resources is determined by dynamic policy, including the observable state of client identity, application/service, and the requesting assets, and may include other behavioral and environmental attributes.
- **Tenet 5:** The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- **Tenet 6:** All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- **Tenet 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.

Tenets

Tenet 1: All Resources

Tenet 1 states that *all* data sources and computing services are considered resources. A network may comprise many types of devices that must all be considered as resources, including devices that share data, such as:

- Aggregators and storage
- Software as a service or SaaS
- Actuators

- Personally owned devices that access enterprise resources

Tenet 2: Secure Communication

Tenet 2 states that all communication must be secured regardless of network location. Network location has no bearing on trust. Access requests from within a network must meet the same security requirements as requests and communication from non-enterprise networks. Communication should:

- Be conducted as securely as possible
- Protect confidentiality and integrity
- Provide authentication

Tenet 3: Per-session Access

Tenet 3 states that access to individual enterprise resources must be granted on a per-session basis. Enterprise resource access is granted after trust in the requestor has been evaluated, with the least privileges needed to complete the task (that is, “sometime recently”) while not directly before initiating a session or performing a transaction, and authentication and authorization to one resource will not automatically grant access to a different resource.

Tenet 4: Dynamic Access

Tenet 4 states that access to resources must be determined by dynamic policy. A dynamic policy includes:

- Observable state of client identity, the application and/or service, and the requesting asset
- Behavioral attributes:
  - Automated subject analytics
  - Device analytics
  - Measured deviations
- Environmental attributes, such as requestor network’s:
  - Location
  - Time
  - Reported active attacks

An organization protects resources by defining:

- What resources they have
- A list of the members that can be authenticated
  - For Zero Trust, identity can be the user account and any associated attributes assigned by the enterprise
- What access those members need

Tenet 5: Posture Monitoring Pillar 6: Automation & Orchestration

According to tenet 5, the enterprise must monitor and measure the integrity and security posture of all owned and associated assets. Posture monitoring ensures that:

- The security posture of an asset will be evaluated every time it is requested.
- Devices and applications are continuously monitored using diagnostics and mitigation.
- Patches and/or fixes are applied as needed.
- Trusted assets will be treated differently than assets that are discovered to be subverted, have known vulnerabilities, or are not managed by the enterprise.

Tenet 6: Authentication and Authorization

Tenet 6 states that access is only allowed after dynamic authentication and authorization and that this must be strictly enforced. Authentication and authorization is a constant cycle of:

- Obtaining access
- Scanning and assessing threats
- Adapting and continually reevaluating trust in ongoing communication

An enterprise implementing Zero Trust would be expected to have the following systems in place:

- Identity, Credential, and Access Management (ICAM)
- Asset management systems
- Multifactor authentication (MFA)

Tenet 7: Current State Monitoring

According to Tenet 7, the enterprise collects as much information as possible about the:

- Current state of assets
- Network infrastructure
- Communications

The enterprise then uses this information to improve its security posture. This includes data related to:

- Network traffic
- The enterprise’s asset security posture
- Access requests

This data can also be used to provide context for access requests from subjects.

Review Activities

Knowledge Check 1

Out of the seven tenets covered in this lesson, which one states that network location has no bearing on trust?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Tenet 1: All Resources
- ○ Tenet 3: Per-session Access
- ○ Tenet 6: Authentication and Authorization
- ○ Tenet 2: Secure Communications

Knowledge Check 2

According to Tenet 2: Secure Communications, which of the following is not true?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ A network may comprise many types of devices that must all be considered as resources.
- ○ Access requests from within the organization do not need to meet the same security requirements as external requests.
- ○ Security posture of an asset will be evaluated every time it is requested.
- ○ None of the above.

Knowledge Check 3

Tenet 7: Current State Monitoring states that the enterprise collects as much information as possible about the current state of assets to improve its security posture. Which of the following does that include?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ The enterprise environmental attributes.
- ○ The security posture of an asset will be evaluated every time it is requested.
- ○ The enterprise's asset security posture, network traffic, and access requests.
- ○ Devices and applications should be continuously monitored using diagnostics and mitigation.

Knowledge Check 4

According to Tenet 3: Per-session Access, which of the following is true?
Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Patches and/or fixes should be applied as needed.
- ○ Authentication and authorization to one resource will not automatically grant access to a different resource.
- ○ Data can also be used to provide context for access requests from subjects.
- ○ The security posture of an asset will be evaluated every time it is requested.

Conclusion

Lesson Summary

You have completed the *Tenets for Successful Adoption* lesson.

Lesson 5: Course Conclusion

Conclusion

Course Summary

This course introduced you to DOD Zero Trust and provided you with an overview of the role of Zero Trust Architecture in protecting DOD technology infrastructure and information. Understanding the concepts, definitions, and general information provided in this course is vital to support the DOD ZTA.

Lesson Summary

Congratulations. You have completed the *Introduction to DOD Zero Trust* course.
You should now be able to perform all of the listed activities.

- Explain the philosophy behind Zero Trust
- Identify the policies and guidance associated with the DOD ZTA
- Describe the pillars and capabilities of the DOD ZTA
- Explain the tenets for successful adoption of Zero Trust

To receive course credit, you **must** take the *Introduction to DOD Zero Trust* examination. Please use the STEPP system from the Center for Development of Security Excellence to access the online exam.

Appendix A: Answer Key

Lesson 2 Review Activities

Knowledge Check 1

Which of the following is a philosophy of Zero Trust?

- ○ Security breaches are preventable with a tailored security model.
- ○ Network data cannot be trusted without validation.
- ○ Once a user is verified, they are trusted inside the network.
- ⦿ Users both inside and outside the network must be verified. (correct)

***Feedback**: Zero Trust acknowledges that threats exist both inside and outside traditional network boundaries—never trust, always verify.*

Knowledge Check 2

Which document sets the goals for a Federal ZTA?

- ○ EO 14028, Improving the Nation's Cybersecurity
- ⦿ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (correct)
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

***Feedback**: OMB M-22-09 sets the goals for a Federal ZTA.*

Knowledge Check 3

Which document defines how the DOD will shift to a ZTA?

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ⦿ DOD Zero Trust Strategy (correct)

***Feedback**: The DOD Zero Trust Strategy defines the DOD's approach to shift to a ZTA.*

Knowledge Check 4

Which document requires Federal agencies to modernize their cybersecurity approaches?

- ⦿ EO 14028, Improving the Nation's Cybersecurity (correct)
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ○ NIST SP 800-207, Zero Trust Architecture
- ○ DOD Zero Trust Strategy

***Feedback**: EO 14028 requires Federal agencies to modernize their cybersecurity approaches.*

Knowledge Check 5

Which document provides migration steps, standards, and guidance for transitioning to a ZTA?

- ○ EO 14028, Improving the Nation's Cybersecurity
- ○ OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- ◉ NIST SP 800-207, Zero Trust Architecture (correct)
- ○ DOD Zero Trust Strategy

***Feedback**: NIST SP 800-207 outlines migration steps, standards, and guidance for transitioning to a ZTA.*

Lesson 3 Review Activities

Knowledge Check 1

Which pillar focuses on the devices authorized to access enterprise resources?

- ○ Pillar 1: User
- ◉ Pillar 2: Devices (correct)
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 2: Devices focuses on the devices authorized to access enterprise resources.*

Knowledge Check 2

Which pillar implements micro-segmentation to provide greater protections and controls over DAAS?

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ◉ Pillar 5: Network & Environment (correct)
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 5: Network & Environment implements micro-segmentation to provide greater protections and controls over DAAS.*

Knowledge Check 3

Which pillar focuses on automating security responses enabled by AI?

- ○ Pillar 1: User
- ○ Pillar 2: Devices

- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ◉ Pillar 6: Automation & Orchestration (correct)
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 6: Automation & Orchestration focuses on automating security responses enabled by AI.*

Knowledge Check 4

Which pillar contains the concept that user activity must be authenticated, assessed, and monitored on an ongoing basis?

- ◉ Pillar 1: User (correct)
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 1: User contains the concept user activity must be authenticated, assessed, and monitored on an ongoing basis.*

Knowledge Check 5

Which pillar focuses on securing IT resources against breaches, unauthorized access, or tampering?

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ◉ Pillar 3: Applications & Workloads (correct)
- ○ Pillar 4: Data
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 3: Applications and Workloads focuses on securing IT resources against breaches, unauthorized access, or tampering.*

Knowledge Check 6

Which pillar states that, based on what's learned, policy changes are made and alert triggers are identified?

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ○ Pillar 4: Data

- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ⦿ Pillar 7: Visibility & Analytics (correct)

***Feedback**: Pillar 7: Visibility & Analytics states that based on what's learned, policy changes are made and alert triggers are identified.*

Knowledge Check 7

Which pillar focuses on data management?

- ○ Pillar 1: User
- ○ Pillar 2: Devices
- ○ Pillar 3: Applications & Workloads
- ⦿ Pillar 4: Data (correct)
- ○ Pillar 5: Network & Environment
- ○ Pillar 6: Automation & Orchestration
- ○ Pillar 7: Visibility & Analytics

***Feedback**: Pillar 4: Data focuses on data management.*

Lesson 4 Review Activities

Knowledge Check 1

Out of the seven tenets covered in this lesson, which one states that network location has no bearing on trust?

- ○ Tenet 1: All Resources
- ○ Tenet 3: Per-session Access
- ○ Tenet 6: Authentication and Authorization
- ⦿ Tenet 2: Secure Communications (correct)

***Feedback:** Tenet 2: Secure Communications states that network location has no bearing on trust.*

Knowledge Check 2

According to Tenet 2: Secure Communications, which of the following is not true?

- ○ A network may comprise many types of devices that must all be considered as resources.
- ⦿ Access requests from within the organization do not need to meet the same security requirements as external requests. (correct)
- ○ Security posture of an asset will be evaluated every time it is requested
- ○ None of the above.

***Feedback**: According to Tenet 2, access requests from within the organization do not need to meet the same security requirements as external requests.*

Knowledge Check 3

Tenet 7: Current State Monitoring states that the enterprise collects as much information as possible about the current state of assets to improve its security posture. Which of the following does that include?

- ○ The enterprise environmental attributes.
- ○ The security posture of an asset will be evaluated every time it is requested.
- ⦿ The enterprise's asset security posture, network traffic, and access requests. (correct)
- ○ Devices and applications should be continuously monitored using diagnostics and mitigation.

***Feedback**: According to Tenet 7, the enterprise must collect as much information as possible about data related to asset security posture, network traffic, and access requests.*

Knowledge Check 4

According to Tenet 3: Per-session Access, which of the following is true?

- ○ Patches and/or fixes should be applied as needed.
- ⦿ Authentication and authorization to one resource will not automatically grant access to a different resource. (correct)
- ○ Data can also be used to provide context for access requests from subjects.
- ○ The security posture of an asset will be evaluated every time it is requested.

***Feedback**: According to Tenet 3: Per-session Access, authentication and authorization to one resource will not automatically grant access to a different resource.*