ATARC Zero Trust Working Group – Phase 2 Integrated Lab(s)

Introduction

As participants engage in the ATARC Zero Trust Integration Lab (ZTIL) it is paramount they understand the lab's intent: Demonstrating fully integrated Zero Trust solutions. The lab is not a platform for demonstrating niche solutions and then linking those solutions to isolated areas of Zero Trust. This lab is meant to support proofs of concept for integrated solution sets, possibly incorporating multiple vendors' products, implementing Zero Trust solutions in a simulated production environment.

Participants should look to DoD's Zero Trust Reference Architecture[1] and CISA's Zero Trust Maturity Model[2] as the key references for their integrated solutions. Participants need not look to address *all* Zero Trust pillars and capabilities to the fullest level of maturity but should address a broad cross-section. Similarly, participants need not look to demonstrate the highest level of Zero Trust maturity but show how their solution set can evolve to support full maturity. Use cases provide additional reference points. Again, the ZTIL is not a platform for demonstrating how a single product fits within the context of the provided use cases but how an integrated solution set addresses the use cases in toto.

Participants' must submit the following:

- How their integrated solution addresses the Zero Trust pillars and capabilities as defined in Reference 1 (a template for providing this information can be found on ATARC's Huddle site at ZTCapabilities (huddle.com));
- The maturity level their integrated solution achieves as defined in Reference 2; and
- At a high level, how the integrated solution addresses the provided use cases.

These submissions will be screened in advance to ensure ZTIL resources are not expended inappropriately and to avoid wasting possible participants' time.

Integrated solutions should address the full scope of the provided scenarios, perhaps not at the highest maturity level but touch all aspects of the scenarios. If vendors have solutions that address only limited aspects of the scenarios, they should seek to partner with other vendors or and integrator so a total solution will be proven in the ZTIL. To assist vendors' connection with other solutions aimed at complimenting their offering(s) in developing a total, integrated solution, information on many relevant offerings can be found through ATARC's Zero Trust Huddle site.

---

[1] https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

[2] https://www.cisa.gov/zero-trust-maturity-model

Background

The government recognizes the complexity of a full Zero Trust Architecture (ZTA). The government further recognizes no single vendor will address all aspects of a ZTA. When addressing the scenarios provided below, clearly state the following:

- The individual products and vendors represented in your integrated solution and the role/function of each;
- Identify any existing, operational deployments of your solution in either a government setting or private industry, providing specifics on the operational setting (size of agency, etc.); and
- Anticipated technical exchange format (demonstration and Q&A between government and vendor[s] technical SMEs).

For each scenario, it is important to describe how you establish a dynamic risk evaluation and how you would dynamically ingest this risk information, specifically detailing how determined risk would be put into action.

Unless otherwise stated, assume an unclassified (or CUI) setting (simulated) when addressing the scenarios.

For each scenario, solutions must address all aspects of Zero Trust, addressing the following guidance:

- Identity & Access Management (IAM) tool that provides authentication services to the user, using OAuth 2.0 token-based access standards;
- Integrates Identity Management Source (e.g. HR ID system, Global Directory Service);
- The IAM should retrieve user credentials via strong authentication, such as a PKI or FIDO2-based hard token for Multi-Factor Authentication (e.g. PIV, Yubikey, etc.);
- Ability for the IAM to challenge user for step-up credentials in the case of elevating to administrator privileges;
- Ability to continuously authenticate users based on changes in defined policies using Continuous Access Evaluation Protocol; and.
- Ability to provide authentication policy on a per application basis (i.e. user can have administrator access to one application, while not to another).

Device Pillar:

- Device Management tool integrated with the IAM in the previous section; and
- Ability for the IAM to query the device on compliance with various policies (e.g. is EDR running, compliance baseline applied, OS patched, etc.).

Network Pillar:

- Ability to micro-segment the application environment on a per flow basis.

Application Pillar:

- Ability to secure API calls within and in between systems; and
- Ability to protect the application's environment.

Visibility and analytics:

- Ability to ingest telemetry logs and correlate to find suspicious events (eventually leveraging AI/ML to do at scale); and
- Ability to baseline and monitor user behavior and identity suspicious events (i.e. UEBA).

SOAR:

- Ability to automate user onboarding, off-boarding, privilege access management via policies; and
- Ability to block malicious activities via automated alerts and integration of the security toolsets.

Governance:

- Ability to identity attributes (e.g. device compliance, data tags, credentials, etc.) to build a "confidence score" that will determine whether the user should be authenticated to the application or denied access; and
- Ability to provide conditional access or context-aware policy decision points for access to the application.

Scenario 1

An agency employee is working remotely, using personally owned devices, must regularly access a public cloud based, agency application. The employee routinely accesses the system as a standard user but occasionally switches to administrator mode to perform systems maintenance. The user's physical location changes frequently with personal travel. At times, that travel takes the user to countries designated as a high threat due to state-sponsored cyber activity. Beyond standard user and administrator activity, there is a specific instance when the user is using administrator privileges to troubleshoot an issue and accesses another system. Further into the troubleshooting process, the user attempts to access a third system but does not have administrator privileges.

Scenario 2

An agency employee and/or contractor, working on from an agency satellite office and using government furnished equipment, is accessing Internet sites. The sites vary between sites supporting job related research and his/her personal bank. Limited personal use is acceptable per agency policy.

Scenario 3

A contracted employee provides ongoing improvements to an agency system as part of a development team and provides administrator and routine maintenance to the operational system. Development is performed from the contracted employee's corporate offices using devices provides by his/her company. Development is performed on a separate network,

isolated from the production network. Both operate within a data center located at the agency's facilities. When appropriate, the contracted employee moves systems from the development environment into production.

Scenario 4
Use the conditions described in Scenario 3 but both the development and production systems are cloud-based.

Scenario 5

A public user accesses an agency's citizen facing system that houses sensitive/PII information. The user has to be verified (i.e. Identity proofing) and have an account on the system for access. The user will be entering data into the system but also occasionally checking the status of their request in the system (e.g. TSA PreCheck)

Scenario 6
An agency system interfaces with another agency's system (e.g. accessing fingerprint information as part of a background investigation process). Both systems are public cloud-based. Describe both normal, ongoing operations and an incident when the agency is informed the other agency's system is experiencing an active exploit.

Scenario 7
Use Scenario 5 but both systems are located on-premise in the agencies' data centers.

Scenario 8
Use Scenario 5 but the primary system is located on-premise in the agencies' data centers and the secondary, accessed system is in a public cloud.

Scenario 9
Use Scenario 5 but the primary system is housed in a public cloud and the secondary, accessed system is located on-premise in the agency's data center.

Scenario 10
Use Scenarios 5 through 8 above but address from the perspective the primary agency system is being accessed to gain fingerprint data (PII or High Categorized) by another agency's system.

Scenario 11
The remote users (e.g. telework, off-site) of an agency's cloud-based HVA system are having connectivity issues that are inconsistently kicking them off their session. Outline any tools you provide for administrators' troubleshooting.

Scenario 12

The ICAM administrator has reported a user's credentials were compromised. Describe any tools/methods you provide to validate unauthorized access to systems under the ZTA umbrella has not occurred, either on-premise or cloud-based.

Scenario 13

An agency has decided to perform penetration exercises against their HVA systems operating under the ZTA umbrella, both on-premise and cloud-based. Describe the tools/methods you provide or support to accommodate these penetration exercises.

Additional Scenarios Considerations:

- Using any of the appropriate above scenarios, show an occurrence or event which after granted authentication and access to a resource where a factor changes the risk/confidence score to increase resulting in the need to take an action (i.e. downgrade of privileges or rejecting of access)
- Workload to Workload - within On-Premises Data Center
- Workload to Workload – On-premises Data Center to/from Public Cloud
- Monitoring Capabilities – On-Premises, Cloud and Hybrid, Continuous Monitoring and Evaluation
- Privilege Access to Critical Infrastructure
- IoT
- Migration from On-Premises to Cloud
- Cloud to Cloud Integration
- Public/Non-employee or Customer Facing Services
- Threats
    - Insider
    - Ransomware Prevention, Detection and Response
    - Phishing
    - Etc. (identified by participant[s])

Archtecture and Deployment of Solution

Federal agencies face myriad physical challenges and configurations. Some small agencies are located in a single, CONUS location. Others are dispersed globally, including locations with poor in-country infrastructure. Accordingly, it is important to understand the solutions being presented in the lab, how they may be deployed in different environments. The below use cases describe multiple possibilities an agency may have in regards to how they are organized geographically and physically. It is important to understand how the deployed solution may accommodate each. Where possible, simulate the use case(s) in your lab demonstration. When that is not possible, detail how your product would address the outlined conditions.

- **Use Case 1 – Central HQ Operations**

This use case involves a large, CONUS headquarters location. The following assumptions should be applied to this use case:

- Robust, reliable connectivity is available from multiple sources.
- Users operate using government furnished equipment on a network with a clearly definable perimeter.
- Users access data and applications located both on-premise and in the cloud.

- **Use Case 2 – Satellite office with highly reliable, robust connectivity**

  The following assumptions should be applied to this use case:

  - Satellite office location may be CONUS or OCONUS.
  - Staff size ranges from a dozen to several hundred.
  - Robust, reliable connectivity is available from multiple sources.
    - Users operate using government furnished equipment on a network with a clearly definable perimeter.
  - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

- **Use Case 3 - Bandwidth challenged satellite office and little to no local IT support staff**

  The following assumptions should be applied to this use case:

  - Satellite office location may be CONUS or OCONUS.
  - Staff size ranges from 10 to several dozen.
  - Connectivity options are limited and sometimes/often prove unreliable.
    - Users operate using government furnished equipment on a network with a clearly definable perimeter.
  - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

- **Use Case 4 - A remote user accessing corporate applications and data using a government-issued device**

  The following assumptions should be applied to this use case:

  - The user may be operating out of a CONUS or OCONUS location.
  - Device could be a PC/Mac, tablet, or smart phone.
  - In the case of a smart phone, the device is managed using an agency controlled and issued mobile device management solution.
  - Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.

- **Use Case 5 - A remote user accessing corporate applications and data using a personal device**

  The following assumptions should be applied to this use case:

  - The user may be operating out of a CONUS or OCONUS location.
  - Device could be a PC/Mac, tablet, or smart phone.

- The device is privately, personally owned and not controlled or managed by the government agency.
- Users access data and applications located both on-premise, HQ-based on-premise, and in the cloud.
- In the case of cloud access, the access is direct between the device and the cloud. The traffic does not traverse a government owned/managed network. (Non-VPN)