ATARC

ATARC Zero Trust Lab Phase 3 - Multicloud Track Draft Use Cases

Scenario 1

A public user regularly accesses Internet facing websites located in AWS and Azure that houses sensitive information (CUI, PII, and PHI). Outline tools that prevent the downloading and uploading of malware, distributed denial of service (DDoS) attacks, Ransomware attacks, SQL Injections, cross site scripting attacks, and data exfiltration.

Scenario 2

A privileged administrator implements and maintains an artificial intelligence (AI) solution without the knowledge of an organization's IT and Cybersecurity groups. The privileged administrator authenticates via the organization's phishing resistant Multi-Factor Authentication (MFA) solution and their actions are tracked via Privileged Access Management (PAM). The AI solution operates from AWS and gathers information from AWS and other cloud environments in the organization including Azure and GCP. The solution is does not have an Authority to Operate (ATO). Outline tools that detect the user of unauthorized technologies.

Scenario 3

A contractor works from their own personal device. The contractor accesses an organization's resources without being on the organization's domain. The contractor's identity is federated with the organization's identity provider (IdP). The contractor has privileged access to systems hosted in Azure and AWS. Describe how systems in Azure and AWS only permit access for person and non-person identities that are allowed.

Use Case 1 – A public user accessing Internet facing web servers hosted in AWS and Azure

The following assumptions should be applied to this use case:

- The user may originate from any geographic location
- The user has no association with the organization
- Device may be a PC/MAC, tablet, or phone

Use Case 2 – A remote user copying data between AWS and Azure

The following assumptions should be applied to this use case:

- The user may be operating out of a CONUS or OCONUS location
- Device is a laptop that is owned and centrally managed by the organization.

Use Case 3 – A privileged administrator implementing capabilities without the knowledge of the organization's IT and Cybersecurity groups in both AWS and Azure

The following assumptions should be applied to this use case:

- The user is authenticating via phishing resistant Multi-Factor Authentication (MFA) solution
- Privileged Access Management (PAM) is tracking this user's actions
- The user could be using Government Furnished Equipment (GFE) or may be using Bring Your Own Device (BYOD)