STACKTITAN

TACTICAL ASSESSMENT CATALOG

CLOUD SECURITY

Cloud computing provides convenience for the world's ever connected personal and professional lifestyles. Further, the prolific Internet of Things (IoT) continues to communicate and process data within abstract cloud computing (as a service) infrastructures. As the complexity of these cloud environments continue to increase, so does the need to ensure adequate security controls are efficient to defend against attacks. Stacktitan provides a variety of cloud services, such as DevOp/CICD, infrastructure security, and active adversarial assessments.

INFRASTRUCTURE SECURITY REVIEW

DOCUMENT COLLECTION AND NETWORK REVIEW

The initial engagement commonly begins with a collaborative knowledge transfer necessary to understand important operational processes, deployed infrastructure, user access, and security controls. The full disclosure of details and subsequent information obtained through review is then used to establish further tactical assessments within the environment.

SEGMENTATION REVIEW

Establishing adequate logical segmentation within the specific cloud environment should be considered a critical tenant to an in-depth attack and containment mitigation strategy. Logical access controls such as access control rulesets and filters will be reviewed to ensure adequacy and documentation are aligned with intended use cases. Examples of environments that are often subject to such reviews are testing, staging, dev-op, and production environments.

LOGICAL NETWORKING REVIEW

Virtual cloud environments, similar to on premise hosted resources; introduce a variety of networking capabilities. Some of the possibilities are network-to-network, network-to-Internet, dev-op network, and corporate backhaul networks. Each of these access deployments introduces their own risk if not secured correctly.

INFRASTRUCTURE SECURITY REVIEW

IDENTITY AND ACCESS MANAGEMENT (IAM) REVIEW

Configured user account roles and their respective permissions need to align with effective security principles, such as least privilege. The implementation of such principles will help to ensure that user accounts and groups have appropriate authentication and authorization. In addition, this review will help to illuminate issues associated with provisioning and decommissioning user accounts in order to prevent superfluous access.

TRUST PROVIDER REVIEW

Cloud hosted resources and their respective applications often require integration of a trust provider resource. This requirement may be introduced as a result of a proprietary applications or integration with third party products, such as a Single-Sign-On (SSO) solution. Further, technologies like SAML and OIDC may be leveraged throughout the implementations. Additional areas of concerns may be encryption security while performing authentication. This review phase will help to identify areas of improvement.

COMPUTE INSTANCE REVIEW

This review identifies the number of stale compute instances within the hosted cloud environment. This is often a result of administrator / dev-op turnover along with increased resources within the environment.

INFRASTRUCTURE SECURITY REVIEW

IDENTITY AND ACCESS MANAGEMENT (IAM) REVIEW

Configured user account roles and their respective permissions need to align with effective security principles, such as least privilege. The implementation of such principles will help to ensure that user accounts and groups have appropriate authentication and authorization. In addition, this review will help to illuminate issues associated with provisioning and decommissioning user accounts in order to prevent superfluous access.

TRUST PROVIDER REVIEW

Cloud hosted resources and their respective applications often require integration of a trust provider resource. This requirement may be introduced as a result of a proprietary applications or integration with third party products, such as a Single-Sign-On (SSO) solution. Further, technologies like SAML and OIDC may be leveraged throughout the implementations. Additional areas of concerns may be encryption security while performing authentication. This review phase will help to identify areas of improvement.

COMPUTE INSTANCE REVIEW

This review identifies the number of stale compute instances within the hosted cloud environment. This is often a result of administrator / dev-op turnover along with increased resources within the environment.

APPLICATION SECURITY ASSESSMENT

DATA STORE REVIEW

Data store and database access and exposure must be secured as these resources almost contain business critical information. This review will inspect access control lists and permissions associated with data access. Further, data will be reviewed to ensure sensitive data is encrypted as necessary. A data content review will be performed to identify content that may be unintentionally exposed to the public and/or other sources that should not have access.

SECURITY ASSESSMENT

VULNERABILITY ASSESSMENT

Reference the Vulnerability Assessment STAC document provided under separate cover.

PENETRATION ASSESSMENT

Reference the Penetration Assessment STAC document provided under separate cover.

APPLICATION SECURITY ASSESSMENT

Reference the Application Security Assessment STAC document provided under separate cover.