SAND2018-11699C

# Applying a Threat Model to Cloud Computing

*PRESENTED BY*

Han Lin

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

# First, why are we using cloud?

Innovation:

- Better linked to emerging technologies (e g ,devices)
- Shift focus from asset ownership to service management
- Tap into private sector innovation

Agility:

- More responsive to urgent agency needs
- Purchase "as-a-service" from trusted cloud providers
- Near-instantaneous increases and reductions in capacity

Efficiency:

- Improved asset utilization (server utilization > 60-70%)
- Improved productivity in application development, application management, network, and end-user

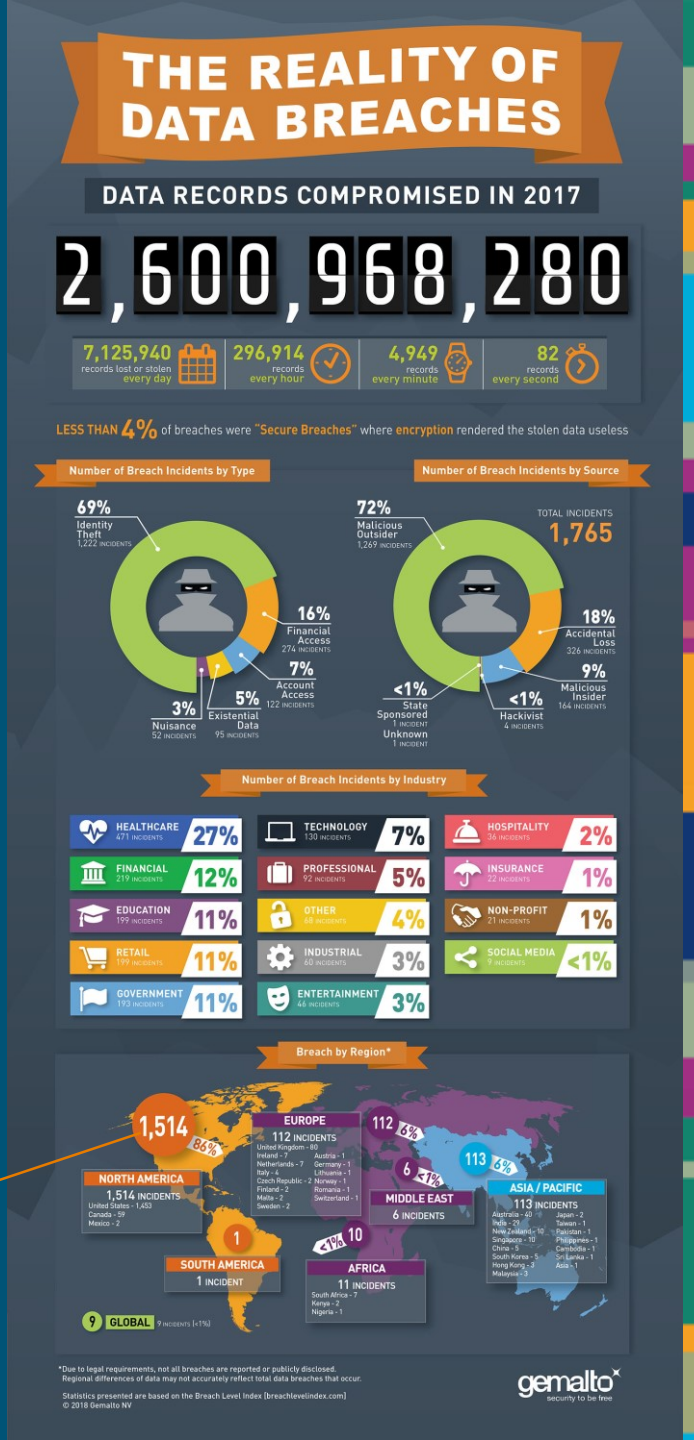
… But not what this talk is about. This talk is about applying a threat model to some of cloud-specific operation characteristics.

# 2017 was named “The Year of the Breach”

“Another misconfigured Amazon S3 bucket exposes 48M records
News roundup: A misconfigured Amazon S3 bucket led to the exposure of 48 million records collected by a private data analytics firm.”[1]

[1] Bacon, M., TechTarget – Security, April 20, 2018

| | | | | | |
|---|---|---|---|---|---|
| Deep Root Analytics/ Republican National Committee | 198,000,000 | 06/13/17 | Identity Theft | Accidental Loss | United States |
| U.S Department of the Interior, U.S. Office of Personnel Management | 22,000,000 | 04/01/15 | Identity Theft | State Sponsored | United States |
| United State Voters | 191,337,174 | 12/28/15 | Identity Theft | Accidental Loss | United States |



# Why is security different in the cloud?

- Cloud's resources are owned and managed by Cloud Service Providers (CSPs) and tenants (i.e., customers)
- Thus security is managed by CSPs and tenants
  - Shared security responsibility model
- Differences Between On-Prem and Cloud:
- Difficulties arise with:
  - Ephemerality
  - Attribution
  - Geo-political boundaries
  - Data governance
  - Shared responsibilities
  - …

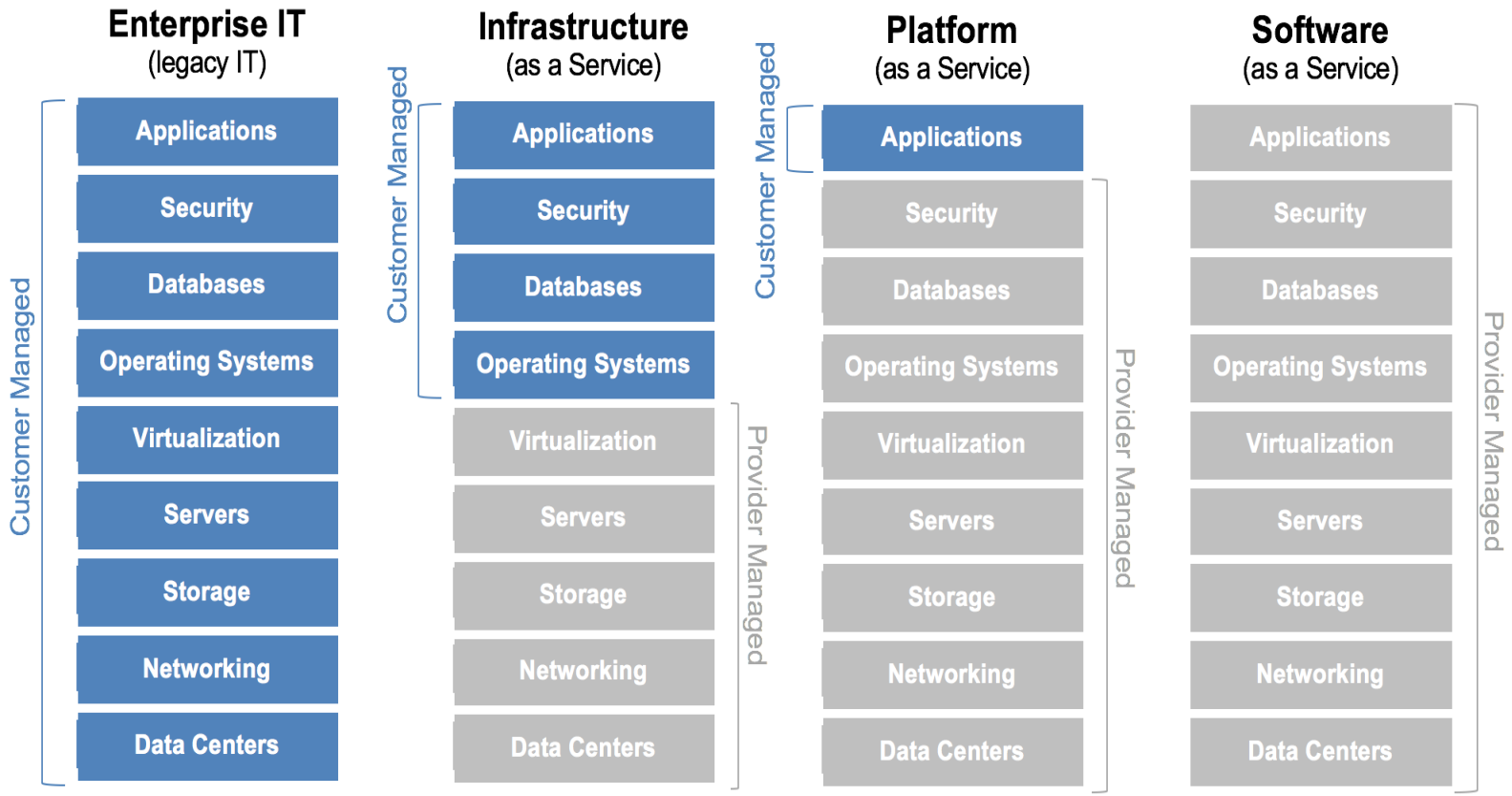
To the CSP: Cloud Security is an after thought

# Some Cloud-Specific Security Challenges

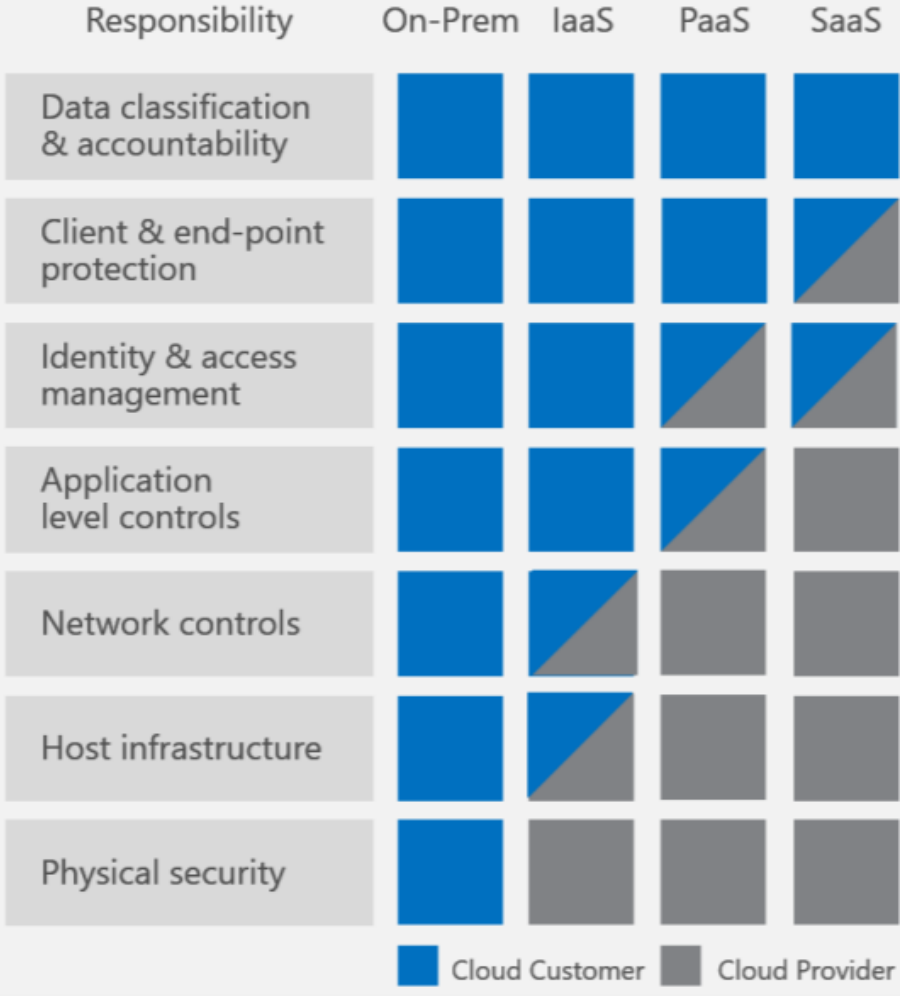
Challenges revolve around:

- Shared Responsibility Model for Cloud Security
  - Both CSP and tenant have specific areas of security responsibility
- Cloud Computing Offers Less Visibility and Control
  - Depending on cloud model being used; SaaS, PaaS, or IaaS
- Application Programming Interfaces (API) Calls
- On-Demand Self Service Simplifies Unauthorized Use
- Multi-tenancy increases the attack surface
- Secure Data Transmission to/from Cloud
- Secure Data Storage and Data Loss in Cloud
- Key Management for Cloud Cryptography
- Identity and Access Management (IAM)
- Logging and Visibility
- Forensics & Incident Response

# Cloud Shared Security Responsibility Model – (View 1 of 2)



# Cloud Shared Security Responsibility Model – (View 2 of 2)




Service models determine the level of responsibility that either the tenant or cloud service provider has.

# Shared Security Responsibility Models

## SaaS - Tenant has least control over security implementations

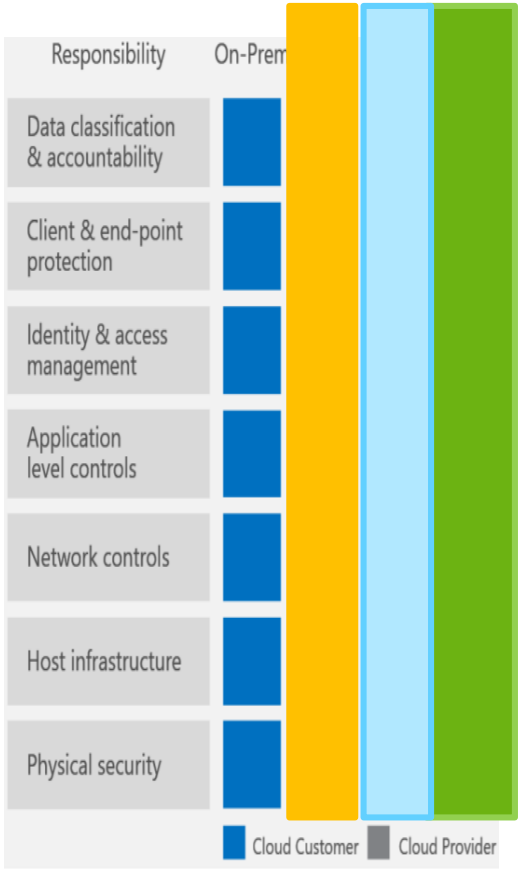
- Access control
  - Strong password policies
  - Multifactor authentication
  - Identity federation
  - Role granularity & privileged user access control

## PaaS - Includes the SaaS security concerns plus

- Operating system (OS) image configuration and patching
- Application configuration and libraries
- User and user role security
- Access authentication and authorization

## IaaS - Includes the SaaS and PaaS security concerns plus:

- OS and above
  - Hardening, Image integrity, Access roles and privileges
- Network access controls (e.g., network security groups)
- Network monitoring
- Network function virtualization



# CSP and Tenant Each Own & Manage Resources

Challenges resulting from shared resource ownership & management

- Shared Responsibility Model for Cloud Security
  - Both CSP and tenant have specific areas of security responsibility.
  - Cloud location being remote, the tenant cannot be expected to handle all security roles and responsibilities.
    - Example: Physical security, SW patches
  - Additionally, the cloud compute resources are shared among multiple tenants.
    - Example: Prevent data from exposure to adjacent tenants
- Cloud Computing Offers Less Visibility and Control
  - Depending on cloud model being used; SaaS, PaaS, or IaaS.
    - Example: Tenant never has access to full network visibility (possibly expose adjacent tenant data).

# Application Programming Interfaces (API) Calls

Application programming interfaces (APIs) are provided by CSPs to manage and interact with (i.e., enable, create, retrieve, update, or delete access) the cloud service's resources.

Cloud APIs introduce three security risks:

- Unauthorized changes (integrity),
- Information leakage (confidentiality), and
- Interference with legitimate activity (denial of service).

Security risks associated with public cloud APIs are further increased because these APIs are typically accessible from the Internet.

# On-Demand Self Service Simplifies Unauthorized Use

CSP has mechanisms in place that make this process very easy and streamlined. This on-demand capability is a feature in cloud.

- Unless prohibited, users can provision and de-provision cloud resources without the consent and guidance of an organization's IT decisionmakers.
- Cloud resources should be provisioned, these resources may not be secured correctly, and are subject to abuse.
- "Shadow IT" becomes more challenging to identify and mitigate.

Thus many threats identified using the threat model are further increased by this cloud feature.

# Multi-tenancy increases the attack surface

Cloud applications or functions run in a multitenancy environment; i.e., multiple tenants may be sharing the same cloud compute):

- CSP solely responsible for maintaining data segregation.
- Cloud software and other components must have been developed with a strong emphasis on security.

Note recent discovery of the Spectre and Meltdown vulnerabilities create additional threats that can lead to compromise of the integrity and confidentiality of tenant data.

# Data Integrity & Confidentiality

## Secure Data Transmission to/from Cloud

- Tenant must consider securing data in transit to and from the cloud, along with data storage in the cloud.

## Secure Data Storage and Data Loss in Cloud

- Data stored in the cloud can be susceptible to compromise. Most CSPs offer forms of data encryption while data is at rest in cloud storage.

## Key Management for Cloud Cryptography

- When using cryptography to secure data either being sent to or stored in the cloud, keys are handled by both, CSP and tenant.

# Identity and Access Management (IAM)

## IAM challenges

- Authentication
- Authorization
  - Use policy to determine access with Users, Roles, Groups
  - Role-Based Access Control (RBAC)
- Federated identities
  - Extend authoritative repositories (i.e., Active Directory) to cloud and/or use token service
- Single sign-on (SSO)
- Auditing and user activity monitoring
  - Log info needed for audits

# Logging and Visibility

## Lack of Visibility

- East/West traffic and North/South traffic.
- Ephemeral VMs (instances)
  - An instance may last 30 seconds – did we log data, did we store? Capture image?
- Traffic not logged:
  - Traffic generated by instances when they contact the cloud DNS server. If you use your own DNS server, then all traffic to that DNS server is logged.
  - DHCP traffic

## Vulnerability scans

- Virtual Machines (VMs) are being spun up and down frequently, making it more difficult for a scheduled scan to cover all assets.

## Log archival considerations:

- Retention: How long does CSP retain logs?
  - How log does the customer require?
  - Customer may have to write logs to customer managed data store

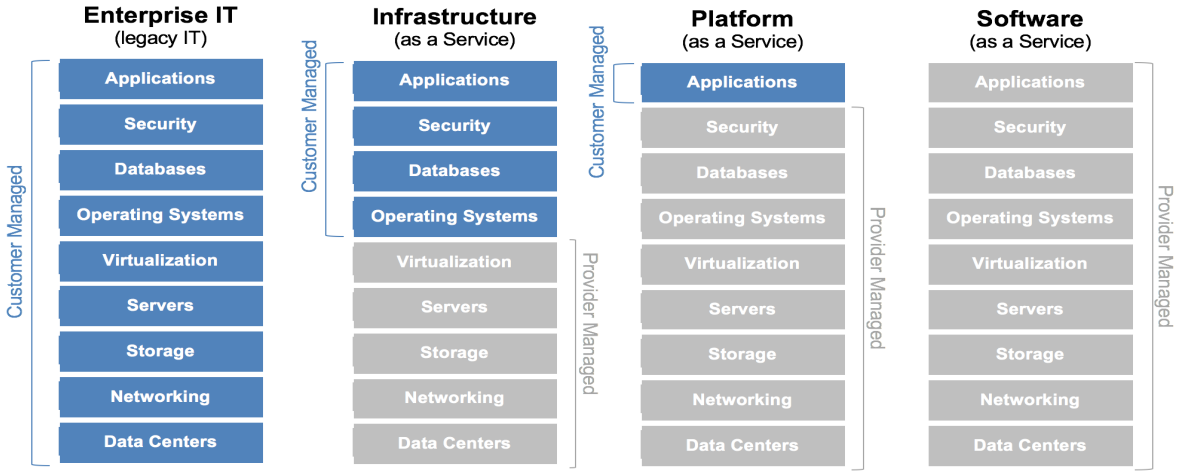
# Threat Surface: Is the cloud a new attack surface?

Yes!

- But, the cloud has some of the same issues as on-prem
  - Example: Azure 0-day Cross-Site Scripting (XSS) in August, 2016

- New threats are introduced
  - Example: Red Hat instances in Azure in February, 2017
    - Exposed Admin API keys in config file
    - Allowed access to any VM within customer account

Attack surface is CSP's resources plus tenant's resources with Less Visibility



# STRIDE-LM Threat Model

STRIDE-LM as a threat classification model, it is an acronym for:

**Spoofing - Tampering - Repudiation - Information Disclosure - Denial of Service - Escalation of Privilege - Lateral Movement**

Used as part of a threat modeling exercise to determine:

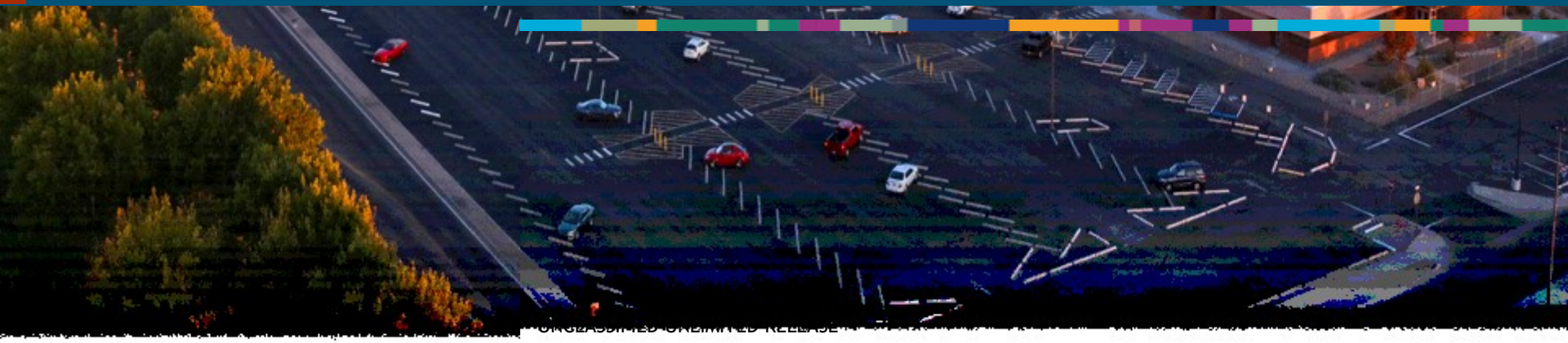
- "What can go wrong in this application or feature we are creating?"
- Brainstorm potential threats to the cloud by creating abuse scenarios.
- See cloud application through the eyes of the attacker.
- A general model of what attackers do to break cloud computing security.

# STRIDE-LM application Example - Spoofing

## Apply STRIDE-LM: Spoofing

| Spoofing: |
| --- |
| ***Threat:*** Unauthorized Identity and Access Management (IAM) change – the change may provide escalation of privilege for a malicious user or enable an unauthorized escalation to admin for a malicious user.<br>***Example mitigation:*** Securing and monitoring user account credentials and access to cloud IAM resources. |
| ***Threat:*** Unauthorized changes to admin roles and access rights that provides increased privileges for malicious purposes. This threat may also include changes to how admin activities are logged to hide malicious activity.<br>***Example mitigation:*** Monitoring your admin activities provides critical insight into who is changing your Cloud environment and how it is changed. Also, monitor all admin activities with the administrative audit log. |
| ***Threat:*** User and admin access compromise from compromised user credentials (e.g., brute force login attempts).<br>***Example mitigation:*** Monitor user login activities to look for signs of compromised user credentials. |
| ***Threat:*** Users attempting to log into the cloud environment from non-jump hosts are not authorized.<br>***Example mitigation:*** Cloud Security teams use jump host logins to limit and control the number of ingress points into cloud environment. Limit access into cloud only through jump host. |

# Thank you



# Extra

# STRIDE-LM application Example – Tampering with Data & Repudiation

| Tampering with data: |
| --- |
| ***Threat:*** Unauthorized disabling cloud logging services or unauthorized deleting or overwriting cloud logging data.<br>***Example mitigation:*** Protect logging data. |
| ***Threat:*** Tampering with or modifying data collected and used for Incident Response (IR).<br>***Example mitigation:*** Audit actions on noting personnel who dismiss alerts, when the alert was dismissed, and what annotations are made. |

| Repudiation: |
| --- |
| ***Threat:*** Unauthorized user claims to have not accessed account.<br>***Example mitigation:*** Cloud monitoring and logging. |

# STRIDE-LM application Example – Information Disclosure

| Information disclosure: |
| --- |
| ***Threat:*** Unauthorized file transfers to/from production from/to cloud environments.<br>***Example mitigation:*** Use strong encryption on your stored data and secure communication links with protocols that provide message encryption. Also configuring firewalls for your virtual private network that control incoming and outgoing traffic with security groups and ACLs. |
| ***Threat:*** Unauthorized cloud outbound connection. Cloud outbound connections are difficult to control because, for example, software package repositories (e.g., Ubuntu) are hosted at various IP addresses around the world. This threat includes malware command and control evasion.<br>***Example Mitigation:*** Collect a baseline of outbound connections in production cloud environments that represents normal behavior. Any deviations from normal outbound connections should be reviewed. |
| ***Threat:*** Outbound/inbound network connections to/from known malicious IP addresses.<br>***Example mitigation:*** Monitor outbound connections to addresses that are known to host or distribute malware or involved with botnet activity. |
| ***Threat:*** Unauthorized viewing and manually editing critical files.<br>***Example mitigation:*** Identify data ownership and limit access per role (e.g., create, modify/delete, read, archive/restore) for sensitive files. Also, configuring firewalls for your virtual private networks that control incoming and outgoing traffic with security groups and ACLs. |
| ***Threat:*** Unauthorized Network access to data stores (e.g., AWS S3 buckets).<br>***Example mitigation:*** Use authentication and authorization for limiting access to data stores. |
| ***Threat:*** Unauthorized network ACL changes to access data stores or network security groups (NSG).<br>***Example mitigation:*** Changes should be alerted and logged. |
| ***Threat:*** Operating with high-risk cloud configurations. Examples include, database not encrypted, database access open to the public, default Security Group applied, production data store set as public.<br>***Example mitigation:*** Monitor for any of the previously mentioned insecure settings. |
| ***Threat:*** Insecure or incomplete data deletion from cloud storage may result in unauthorized data exfiltration.<br>***Example mitigation:*** Check cloud provider deletion policy. |

# STRIDE-LM application Example – Denial of Service, Elevation of Privilege, & Lateral Movement

| Denial of service: |
| --- |
| ***Threat:*** *Denial-of-service attack (DoS) against cloud infrastructure.*<br>***Example mitigation:*** *Block IP addresses; whitelisting* |
| ***Threat:*** *Terminate cloud compute instance.*<br>***Example mitigation:*** *Limit access to trusted individuals.* |

| Elevation of privilege: |
| --- |
| ***Threat:*** User privilege escalation. Privilege escalations in cloud environment may provide early indications of a breach by insider threats.<br>***Example mitigation:*** Follow the principle of least privilege and use least privileged service accounts to run processes and access resources. |

| Lateral Movement: |
| --- |
| ***Threat:*** Unauthorized attempts to scan adjacent host or attempted access of adjacent host. Or unauthorized network security group changes.<br>***Example mitigation:*** Use flow logs of cloud virtual networks to examine cloud network traffic. Network traffic examination in the cloud is limited to examining traffic sourced or destined from/to a host in the tenant cloud subscription. |