In the Cloud: Cloud Security Hygiene in Higher Education

Session Outcomes:

1. Learn how to secure your multi-cloud environments
2. Understand how to avoid common pitfalls for cloud security posture management
3. Find out how to establish governance and monitor configuration drift for your cloud environments
The Problem: Cloud Security is a Black Box

Cloud Security Is a Black Box

- Multi-Cloud Security Requires Zero Trust
- SaaS Applications are not 100% Secure by Default
- Secure By Design can be achieved using cloud reference architectures
- Cross-Cloud Security Posture Management is Needed
- Unified Threat Detection and Security Monitoring
Cloud Security Hygiene 1: Zero Trust is Not Optional

Zero Trust Is Not Optional

- Evolving Threat Landscape
  - Solorigate*
  - HAFNIUM
  - Nobellium
  - Advanced Ransomware
  - Siloscape
- Modern Defense In Depth
  - Risk-Based Security
  - Integrated Security Architecture
Cloud Security Hygiene:
Know Your Cloud Admin Estate

- Cloud-Only Accounts
  - Break-Glass Accounts
  - Global / Super / Tenant Admin
- Hybrid / Synced Identity
  - Just-In-Time for Multi-role admins
  - Domain Admin
- Service Principals / API Keys
- Leverage SSO to Reduce Identity/Credential sprawl
Cloud Security Hygiene: Know Your Cloud Security Posture

- Multi-Cloud Visibility
  - Compute
  - Storage
  - Containers
- Current Configuration vs. Baseline Recommendations
- Continuous Monitoring, Remediation, & Threat Management
Cloud Security Hygiene: Know The Data In The Cloud

Know the Data in the Cloud

- Data Types & Categories
  - PII
  - HIPAA
  - HCRI
  - CUI
- Locations
  - Blobs / Buckets
  - SQL / NoSQL / MySQL
- Broaden the Scope
  - Backups / Code Repositories
  - Compliance
  - Oversight
Cloud Security Hygiene: Security Monitoring Should Include Cloud

- IaaS / PaaS / SaaS
  - End-User Activity
  - Administrator Activity
  - Data Exfiltration Activity
  - Identity / Credential Theft Activity
  - Threat Actor Activity
  - Platform Configuration Activity
  - .................
Conclusion

- Develop a Zero Trust architecture to protect your cloud estate
- Know the identity perimeter and leverage cloud security posture management to create a cloud security baseline
- Monitor Your High Value Cloud Assets and Cloud Admin Activity with a SIEM

Questions?

NOTE: This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the Creative Commons Attribution 4.0 International (CC BY 4.0), which grants usage to the general public, with appropriate credit to the author.