Pearson | VUE

# Cloud Security

Vladan Pulec | Pearson VUE

November 4, 2020

# PEARSON VUE DELIVERS

**16** MILLION EXAMS EACH YEAR

IN MORE THAN **20,000**

TEST CENTERS IN

**180** COUNTRIES. THAT IS ONE TEST

DELIVERED GLOBALLY EVERY

**2.2** SECONDS

# Respected certifications

## Aligned to the military





U.S. Department of Defense
DEFENSE SECURITY SERVICE
















AMT
American Medical Technologists
Certifying Excellence in Allied Health



NCEES
advancing licensure for
engineers and surveyors

# Why?

- Cloud has different security challenges compared to the on-premise hosting
- Cloud adoption is accelerating
- On average, it takes 279 days to detect and contain a breach
- Cloud migration complexity is one of the top 5 most contributing factors to the cost of a data breach
- Chances of experiencing a data breach are going up
- Average of a cost per stolen record: $150

# Essential Characteristics

On-Demand Self-Service

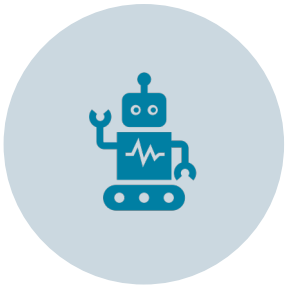
Broad Network Access

Resource Pooling

Rapid Elasticity

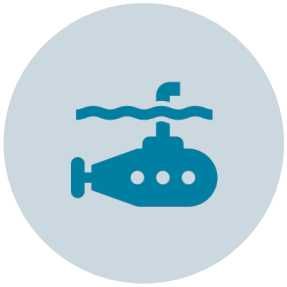
Built-In Security Tools

# Key Factors to Better Security



Security Automation (machine learning, analytics, automated response)

Real-Time Monitoring and Response (SEIM/SOAR) using Centralized Log Collection “and Analytics



Defense in Depth

Zero Trust

# Challenges

- Identity and credential management
- Misconfiguration and Vulnerabilities
- Insecure APIs
- Data Security
- Change control
- Weak control plane
- Advanced persistent threats

# Identity and Credential Management

## Threats

- Insider threat
- Data misuse

## Mitigations

- JML (Joiner-Mover-Leaver) process
- 2-Factor Authentication (2FA)
- User Behavior Analytics
- Secure credential storage (key values) and perform key rotation
- Centralized log collection (cloud-native or centralized solution to cover hybrid deployments)
- Security Information Event Management (SEIM) and Security Orchestration, Automation Response (SOAR)

# Misconfiguration & Vulnerabilities

## Threats

- System exposure/compromise

## Mitigations

- Cloud-native configuration/compliance monitoring and alerting
- Rules preventing misconfiguration
- Host and Network Scanning (internal and perimeter)

# Insecure APIs

## Threats

- Weak access control
- Susceptible to DDoS

## Mitigations

- DevSecOps & penetration testing
- Utilize API Management/Gateway
- Cloud-native DDoS

# Data Security

## Threats

- Data exfiltration and leakage
- Insider threat or mistake
- No visibility into what is stored in the cloud
- Cloud provider exploit

## Mitigations

- Enforce encryption at rest and in-transit
- Data masking, data retention, backups
- Use modern encryption and ciphers
- Use bring-your-own encryption keys
- Asset tagging practice
- IPS/IDS – network and host
- Data Loss Protection (DLP)
- Zero Trust
- Monitoring for Indicators of Compromise (SEIM)

# Change control

## Threats

- Unauthorized deployments

## Mitigations

- Devops with auditable deployments
- Separation of duty
- CI/CD service accounts with the most restrictive permissions possible

# Weak control plane

## Threats

- Data loss
- Shadow IT

## Mitigations

- Least privilege model
- 2-factor authentication
- Logging
- Defense in Depth
- Zero Trust
- SOAR/SEIM
- Automated scanning to detect shadow IT

# Advanced Persistent Threats

## Threats

- Malware
- Ransomware
- Unrestricted lateral movement

## Mitigations

- Utilize cloud-native protections
- Zero trust architecture - (MFA, micro-segmentation, context-based access, etc)

# Sources

IBM: Cost of a Data Breach Report 2019

Varonis: 107 Must-Know Data Breach Statistics for 2020

ForcePoint: Cyber Edu

NIST: Zero Trust Architecture


# Vladan Pulec

Enterprise Architect - Security & AI

Vladan.Pulec@Pearson.com