Assignment – 4

Name: Ishan Aakash Patel

Student ID: 146151238

Course: Threat Intelligence (CYT-245)

List top 10 threats relevant to cloud computing

Threat	Source	Explanation	Applicable to	Preventive Controls	Detective Controls	Corrective Controls
Data Breaches	CSA	Unauthorized access to confidential data through hacking, malware, or insider threats.	IaaS, PaaS, SaaS	Strong encryption, multi-factor authentication (MFA)	Security audits, access log monitoring, IDS	Incident response plan, regular updates and patches
Data Loss	NIST	Accidental or malicious deletion, corruption, or loss of data.	IaaS, PaaS, SaaS	Regular data backups, redundant storage solutions	Data integrity checks, backup process monitoring	Data recovery procedures, use of recovery tools
Account Hijacking	OWASP	Unauthorized access to cloud accounts via phishing, credential stuffing, or weak passwords.	IaaS, PaaS, SaaS	Strong password policies, MFA, user education on phishing	Account activity monitoring, anomaly detection systems	Account lockdown, password resets, forensic analysis
Insecure Interfaces and APIs	OWASP	Security issues like unauthorized access, data leakage, and service disruptions through insecure interfaces and APIs.	IaaS, PaaS, SaaS	Secure coding practices, API gateways with robust authentication and authorization	Security testing of APIs, API usage monitoring	Patch and update vulnerable APIs, revise security policies
Denial of Service (DoS)	ISO	Attacks that make cloud services unavailable by overwhelming them with traffic.	IaaS, PaaS, SaaS	Rate limiting, anti-DDoS services and solutions	Traffic pattern monitoring, IDS deployment	Mitigation strategies, service recovery procedures

Threat	Source	Explanation	Applicable to	Preventive Controls	Detective Controls	Corrective Controls
Malicious Insiders	ISACA	Individuals with authorized access who misuse their access to harm the organization.	IaaS, PaaS, SaaS	Background checks, least privilege access, enforce access controls	Insider activity monitoring, SIEM tools	Access revocation, investigations, legal actions
Abuse and Nefarious Use of Cloud Services	CSA	Use of cloud resources for malicious purposes like hosting malware or launching attacks.	IaaS, PaaS, SaaS	Strict usage policies, automated abuse detection tools	Cloud usage audits, unusual activity detection tools	Suspension of abusive activities, policy and monitoring review
Insufficient Due Diligence	NIST	Failure to fully understand and address cloud security risks.	IaaS, PaaS, SaaS	Comprehensive risk assessments, security training and awareness programs	Security policy reviews, continuous security posture assessment	Update and enhance security measures, implement corrective actions
Shared Technology Vulnerabilities	CSA	Vulnerabilities from multi-tenant architectures where resources are shared among multiple users.	IaaS, PaaS, SaaS	Robust isolation mechanisms, regular updates and patches	Monitoring tenant interactions, security testing and vulnerability assessments	Apply patches and updates, revise architecture for better isolation
Advanced Persistent Threats (APTs)	MITRE	Prolonged and targeted cyberattacks aimed at stealing data or disrupting operations.	IaaS, PaaS, SaaS	Multi-layered security measures, threat intelligence, advanced endpoint protection	Continuous monitoring, SIEM tools, threat detection systems	Incident response strategies, forensic analysis, system remediation