Cloud Threat Assessment Report

Executive Summary

This report identifies and evaluates key security threats associated with a newly deployed virtual machine (VM) instance on a public cloud platform (AWS). In line with the shared responsibility model, the cloud provider (AWS) is responsible for securing the infrastructure, while the organization is accountable for securing data, identity, applications, and configurations. The threats outlined are based on practical exploration of the cloud environment, security scanning using AWS Security Hub, and references to industry sources such as the Cloud Security Alliance (CSA) Top Threats report.

Threat Analysis

Threat Name	Description	Potential Impact	Recommended Countermeasures
Misconfigured Security Groups	Overly permissive or public settings.	Data breaches or service compromise.	Use AWS Config/Security Hub, audit r
Insecure APIs	Poorly secured APIs open to abuse.	Data manipulation or compromise.	Enforce OAuth2, monitor and restrict a
Weak IAM	Improper roles or use of root account.	Privilege escalation, insider threats.	Apply RBAC, disable root access, use
Account Hijacking	Credential theft via phishing.	Unauthorized access, data loss.	Use MFA, monitor logins, train staff.
Insufficient Logging	Lack of audit trails and alerts.	Undetected breaches.	Enable CloudTrail, SIEM integration.

Validation Using AWS Security Tools

Environment Setup:

- AWS Free Tier EC2 instance
- Apache installed
- Open ports initially

Findings:

- Security Group misconfig (0.0.0.0/0)
- Root access without MFA
- Logging initially off
- EBS unencrypted
- No backup plan

Cloud Threat Assessment Report

Recommendations

1. Restrict network access to known IPs.
2. Enforce IAM best practices (RBAC, MFA).
3. Enable CloudTrail and SIEM logging.
4. Secure API access with gateways and authentication.
5. Automate compliance with AWS Config.

Conclusion

The threats identified are common in public cloud environments. Following the outlined countermeasures will reduce the attack surface and enhance cloud security maturity.