Truth about running Cloud Security Assessment in 2021

A Practitioner's Story

Presented by Ashish Rajan

Website: www.ashishrajan.com
Github & Twitter : **@hashishrajan**
Cloud Security Podcast: www.cloudsecuritypodcast.tv

Documentation vs Reality

Of Cloud Security Assessment

CLOUD SECURITY PODCAST

Agenda

- Framework to pick
- Assessment Landscape
- Type of Threats in <INSERT> Cloud Provider
- Assessment Types
- Automation vs Manual Security Assessment
- Security Assessment vs CSPM vs Open Sources
- Conclusion

Disclaimer: Assumption made that you have knowledge in one or more services of any of the CLOUD SERVICE PROVIDER SERVICES as a consumer

About me

9am-5pm

- Head of Security (CISO) for a Growth Tech Company
- Prior to this - Consulting Practice for Cloud Security
- Helping migrate Enterprise into Cloud through Digital Transformation

Weekends

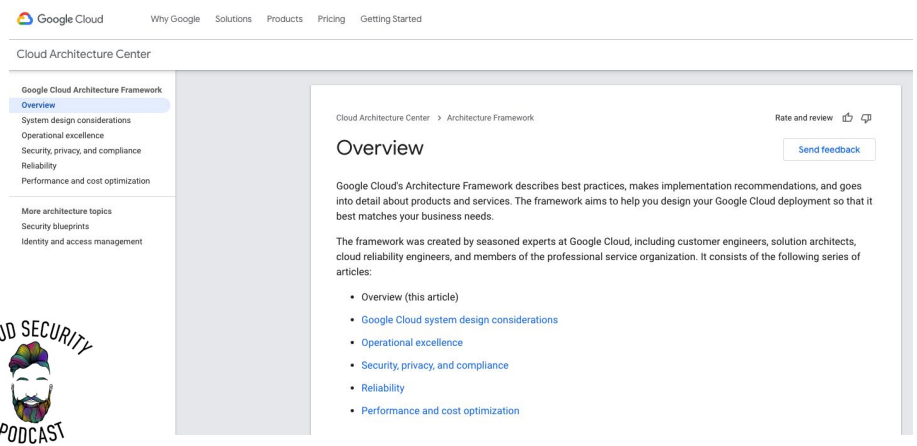
- Host of Cloud Security Podcast, weekly video podcast on Cloud Security
- CISO Advisory, Trusted Advisor, Cloud Security Auditor and Observer

Picking suitable Framework

- CyberSecurity Framework - NIST CSF, ISO 27001, GDPR, PCI, SOC2 Type 2 etc.
- Type of Organisation and size of the organisation
- Type of Data being stored and processed by the organisation
- Entire Cloud Environment vs An application hosted on Cloud Environment
- Hybrid Environment
- Custom Framework per Industry/Customer

Cloud Assessment Landscape

Documentation 🥷



Microsoft Azure Well-Architected Framework

11/20/2019 • 9 minutes to read • +9

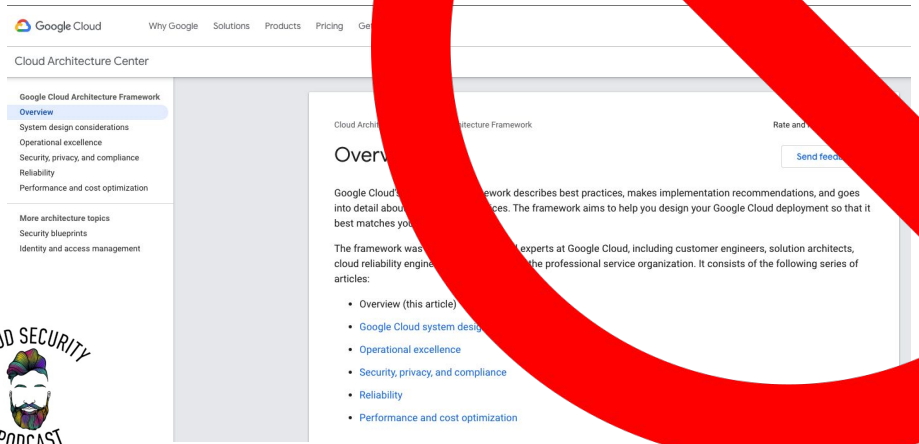
The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architecture excellence: Cost Optimization, Operational Excellence, Performance Efficiency, Reliability, and Security.

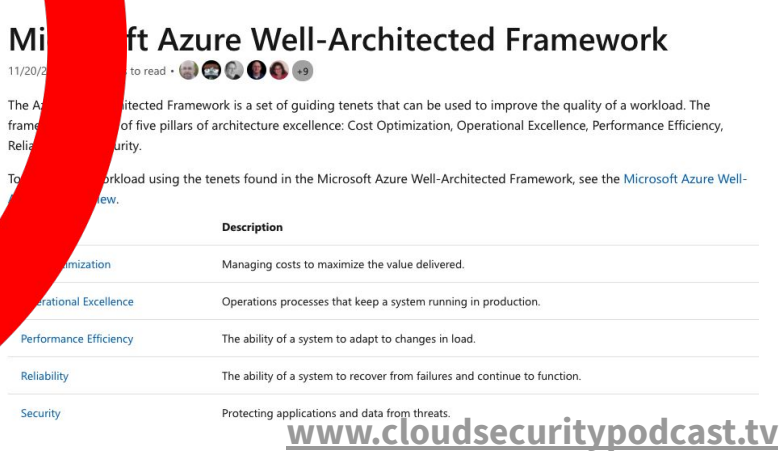
To assess your workload using the tenets found in the Microsoft Azure Well-Architected Framework, see the Microsoft Azure Well-Architected Review.

Pillar	Description
Cost Optimization	Managing costs to maximize the value delivered.
Operational Excellence	Operations processes that keep a system running in production.
Performance Efficiency	The ability of a system to adapt to changes in load.
Reliability	The ability of a system to recover from failures and continue to function.
Security	Protecting applications and data from threats.

CLOUD SECURITY PODCAST

Documentation - Not followed





TRUTH 😇: Cloud Adoption Types

- Cloud Architecture is different between Organisations
  - Migrated into Cloud recently
  - Have been in Cloud for over 1yr
    - but don’t have security tenancy accounted for in their build
    - Have been in Cloud for sometime and have Security tenancy included in the build
  - Use a Central Deployment Team to provision Cloud Tenants to Staff
  - Each Business Unit has their own version of Cloud Tenancy
  - Mix of any of the above.

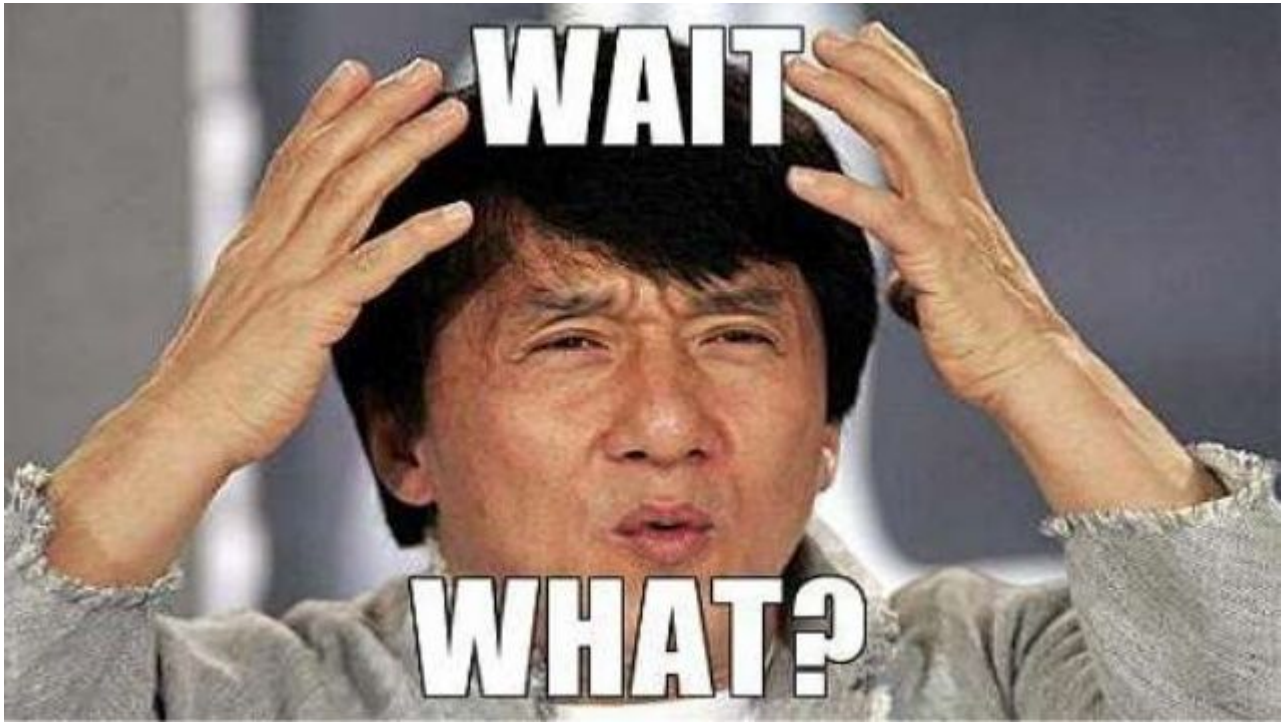
Documentation: Source Types for Assessments

- Everyone uses only 1 Cloud Service Provider
- A mature organisation will only be using Cloud Native services (possibly only from 1 Cloud Service Provider) - deploying multiple times a day
- Everything will be in Code Repository
- No RDP/SSH access to Production

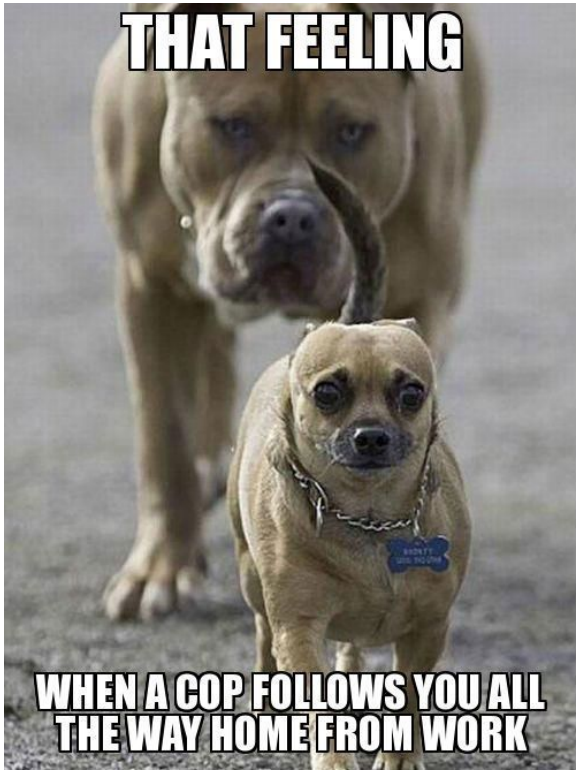
TRUTH 😇: It's a Pandora's Box

- Infrastructure Types - *Kubernetes, Containers, VMs, EC2 etc*
- Application Types - *Microservices, Monolith etc*
- Source Control - *ClickOps, Infrastructure as Code in a Git repository*, *Yaml File*
- Access Types provided : Admin Access to All Cloud Environments
- DC per Business Unit: 20+ Accounts with each one being it's own rules
- Mature organisations gives you Read Only Auditor Access customised by them for the services they use and provide secret keys with the Read only permission.
- Mature organisations using pre-defined security defaults in their accounts and provisioned User accounts

Documentation starts to show cracks



Types of REAL Threats in Cloud



Kill Chain

MITRE ATT&CK

Cloud Matrix

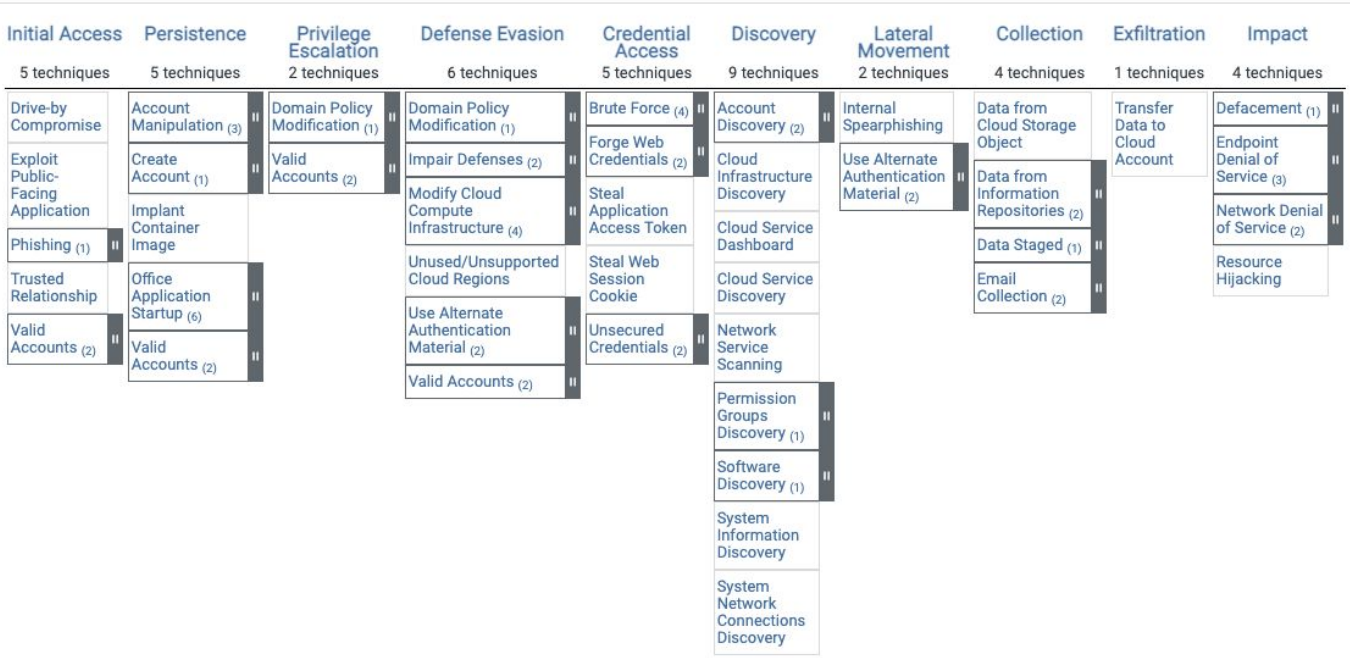
Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

View on the ATT&CK® Navigator

About the Enterprise domain

Version Permalink

layouts | show sub-techniques | hide sub-techniques | help



Last modified: 27 October 2020

TRUTH 😇: Kill Chain - Initial Access (Threat)

- Exploit Public Facing Application
- Phishing/ Valid Accounts
- Third Party Management

Types of Cloud Threats

- Exploit Public Facing Application
  - Network Security
  - Application Security
- Phishing/ Valid Accounts
  - Identity & Access Management
  - Secret Management
- Third Party Management
  - SaaS services (Shared Responsibility)
  - Managed Service Providers (Shared Responsibility)
  - CSP (Shared Responsibility)

Assessment Types

- Manual or Point in Time
  - Someone like one of my industry peers will bring their expertise to the table
- Point in Time but automated
  - Architecture Review
  - Someone like me who has developed a set of pre-defined checks in that run automatically on any given CSP
  - Manual sweep of the new services, that were not reported as in use by the Client
- Continuous
  - Cloud Access Security Broker (CASB)
  - Cloud Security Posture Manager (CSPM)

TRUTH 😇: Assessment Types

- Point in Time Continuous Assessments
  - Audit includes the context of the Application Architecture in Cloud, which is what the adversary would be exploiting not the CIS Benchmark.
  - Final Report gets added to the backlog of the Security or the Relevant Business team and actioned based on Risk level
  - There is real life Risk Awareness for the business to make an informed decision of the Risk
- Continuous Assessments (CSAB or CSPM)
  - Checks and Controls are based on customer input or services that the CSPM is currently supporting no
  - Wall of RED, where most people have been aware of everything you are about to say but it is buried deep in the wall of red between FALSE POSITIVE & IGNORE/ARCHIVED
  -

Interesting Tools (OpenSource, not CSP version)

- AWS
  - CloudMapper
  - Prowler
  - Pacu
  - CloudSpanning
- Azure
  - SkyArk (AzureStealth)
- GCP
  - - IAM Privilege Escalation
- Multi-Cloud
  - CloudCustodian
  - CloudSpolit (Developer Edition)
  - ScoutSuite
  - Cloud Security Suite
  - Forseti

Conclusion

- **Truth** - You need both Continuous and Point in time Assessments
- **Truth** - Open Source tools should only be used if you have the skill set in your team
- **Truth** - Ask your Auditor if they will understand Cloud and if they will understand your architecture instead of simply going through a checklist
- **Truth** - Run Internal assessments of your Cloud Environment before a Compliance audit by a Trusted Advisor. The auditor doesn't have to be me or someone like me but someone who wants to put the time and effort to understand and not follow a checklist.
- **Truth** - **Successful Compliance Certification NOT EQUAL SECURITY!**

Questions/Feedback

Find your Trusted Advisor to get a real picture of RISK in your Cloud Environment

Questions - www.AshishRajan.com