STEALING THE SILVER LINING FROM YOUR CLOUD

Anant Shrivastava : Technical Director

NotSoSecure part of
claranet cyber security

NotSoSecure part of claranet cyber security

We hack

Web Application Security Assessment

Infrastructure Security Assessment

Mobile Application Security Assessment

Source Code Review

IoT Security Assessment

Red Team Exercises

For **private/corporate training** please contact us at:
training@notsosecure.com

We teach

Beginner Friendly

Hacking 101

Basic Infrastructure Hacking

Basic Web Hacking

Advanced/Specialist Offensive Courses

Advanced Infrastructure Hacking

Advanced Web Hacking

Hacking and Securing Cloud

Specialist Defensive Courses

Application Security for Developers

DevSecOps

About Myself

- Director NotSoSecure Global Services
- Sysadmin / Development / Security : all shades of IT
- Project Owner: HackingArchivesofIndia, AndroidTamer, CodeVigilant
- Contributor : null, G4H and many more
- @anantshri on social platforms

NotSoSecure part of claranet cyber security

Agenda

- Setting the Stage
  - Everyone wants cloud
  - Organizations in cloud
  - Cloud Migration
- Understanding the environment
  - Cloud Responsibility matrix
  - Cloud Security Tooling
- Stealing the silver lining
  - ATT&CK Framework
  - Example Scenarios

NotSoSecure part of claranet cyber security

Everyone Wants Cloud

- Cloud Computing is the “In” thing.
- Besides the usuals of why cloud makes sense.
- 2020 has made it pretty clear remote working is here to stay.
- Data Centers & concepts of physical network boundaries are aging

NotSoSecure part of claranet cyber security

Orgs In the Cloud

- Born in Cloud Now (Fully cloud Native : no self datacenter footprint)
  - Mostly Startups
  - SaaS Service providers
  - Cloud service aggregator or consumers
- Migrating from existing
  - **Rehost** (Lift and Shift)
  - **Refactor** (modernize application for cloud but still stick largely to IaaS)
  - **Rearchitect** (monolith to microservices, containers / orchestration)
  - **Rebuild** (rewrite app as cloud native apps)
  - **Replace** (leveraging other SaaS options)

NotSoSecure part of claranet cyber security

Cloud Migration : Security Concerns

- Cloud is a paradigm shift from conventional environments
- Conventional wisdom and controls just won't work
- Cloud Security concerns
  - Misconfigurations are the biggest concerns
  - Access control failures (Insecure API's / Interfaces)
  - Unauthorized access due to credential leakage
  - Unintended Data Exposure to public
  - Data Loss and data sovereignty is next in line (GDPR and similar)

Ref: https://notsosecure.com/security-architecture-review-of-a-cloud-native-environment/

NotSoSecure part of claranet cyber security

Responsibility Matrix

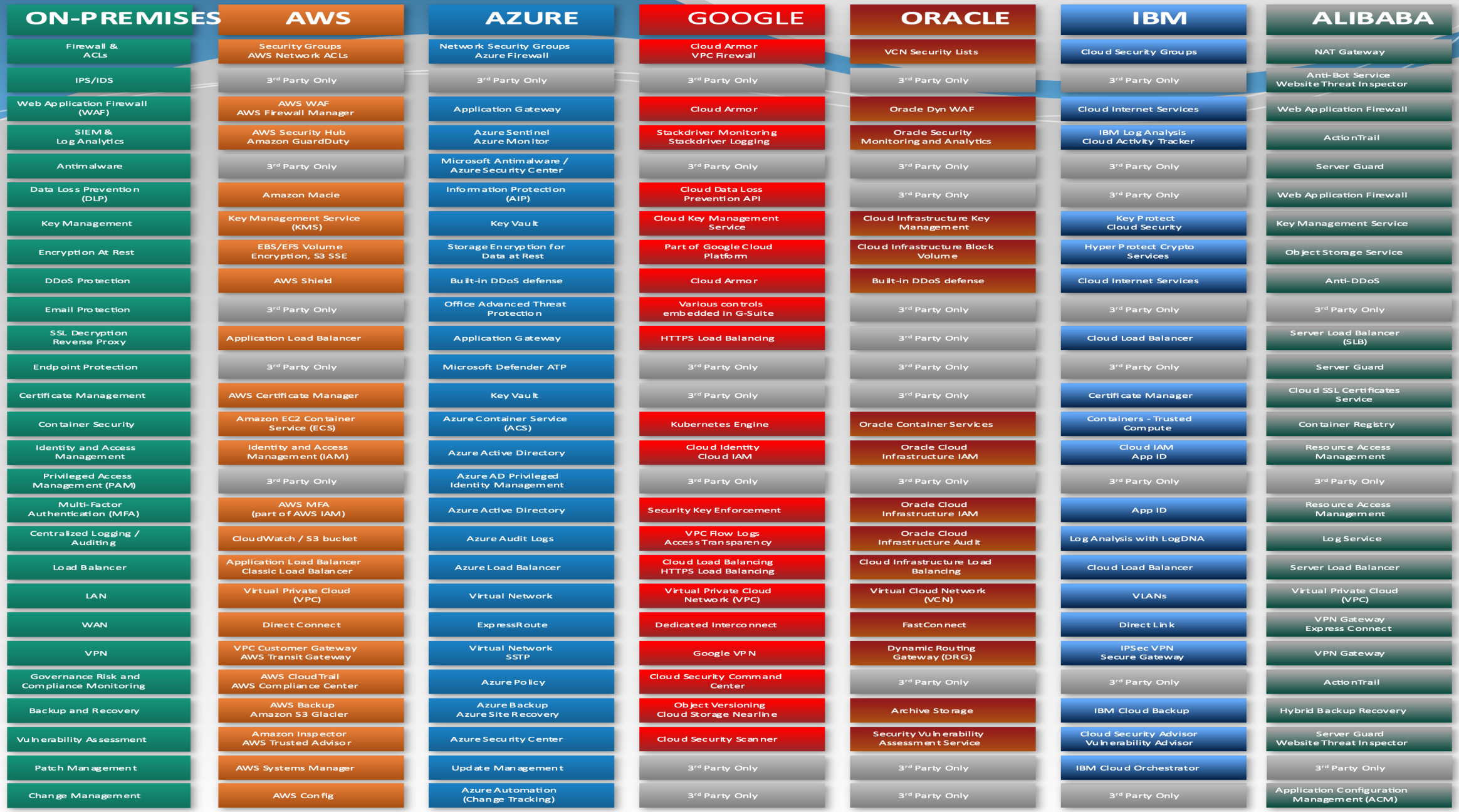
Responsibilities	On-prem	IaaS	CaaS	PaaS	FaaS	SaaS
All Things Client Side	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Data (Transit and Cloud)	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Identity & Access Management	Tenant	Tenant	Tenant	Tenant	Tenant	Tenant
Functional Logic	Tenant	Tenant	Tenant	Tenant	Tenant	Provider
Applications	Tenant	Tenant	Tenant	Tenant	Provider	Provider
Runtime	Tenant	Tenant	Tenant	Provider	Provider	Provider
Middleware	Tenant	Tenant	Provider	Provider	Provider	Provider
OS	Tenant	Tenant	Provider	Provider	Provider	Provider
Virtualization	Tenant	Provider	Provider	Provider	Provider	Provider
Load Balancing	Tenant	Provider	Provider	Provider	Provider	Provider
Networking	Tenant	Provider	Provider	Provider	Provider	Provider
Servers	Tenant	Provider	Provider	Provider	Provider	Provider
Physical Security	Tenant	Provider	Provider	Provider	Provider	Provider

NotSoSecure part of claranet cyber security

Security Tooling in Cloud

- Most vendors provide basic set of tools
- 3rd parties are still needed for some tools
- Native tool offerings
  - Tightly coupled with Cloud providers and hence larger visibility
  - Mostly internals are hidden, and only limited stuff is exposed
  - Limitation in terms of flexibility on modifying the outputs
- 3rd Party offering
  - Especially useful if you are in multi cloud / hybrid environment
  - Limited to the stuff exposed to 3rd party
  - Allows more flexibility in terms of output modification

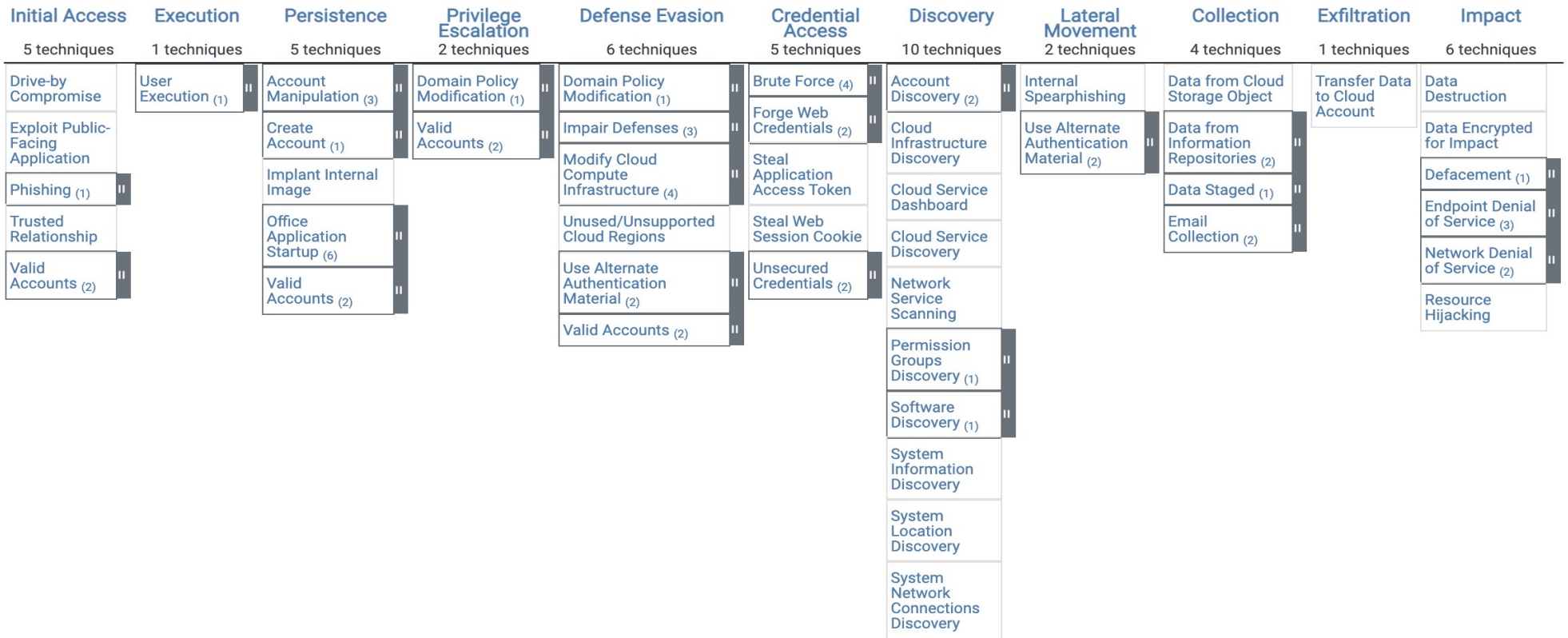
NotSoSecure part of claranet cyber security



Mapping of On-Premises Security Controls vs Major Cloud Providers Version 4.5 Apr 2019 © Adrian Grigorof, Marius Mocanu

Attacking the Cloud

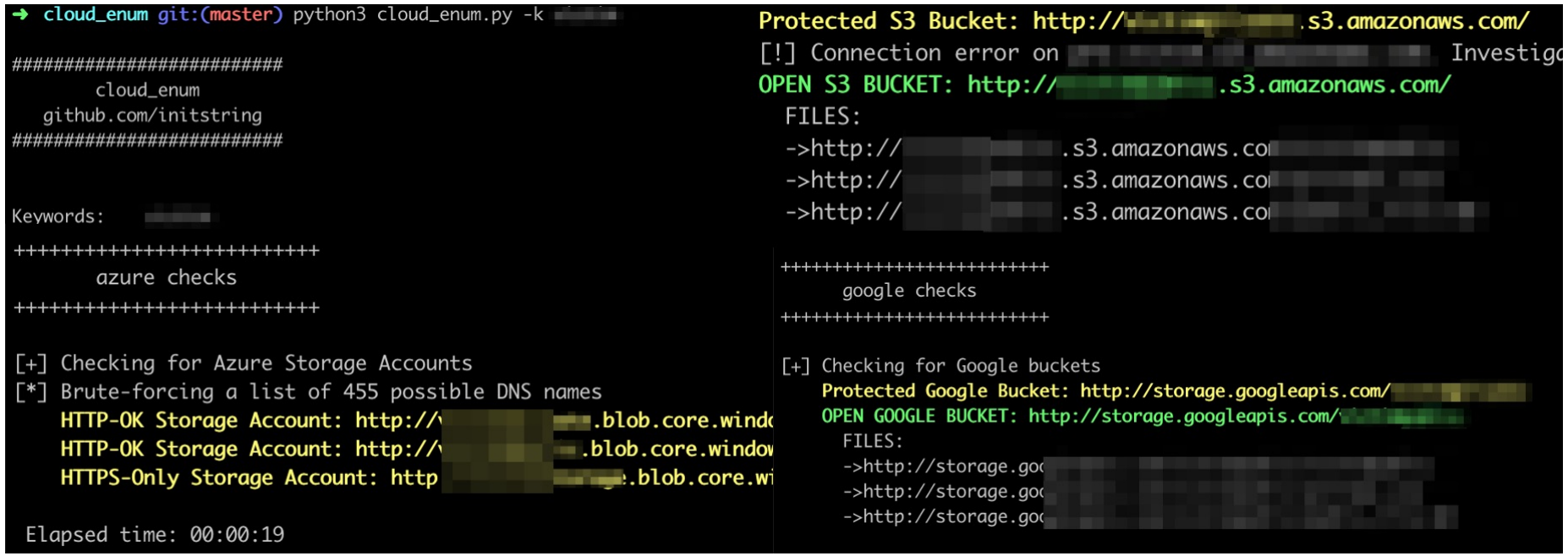
- MITRE does a good job



Last modified: 27 April 2021

NotSoSecure part of claranet cyber security

Enumeration



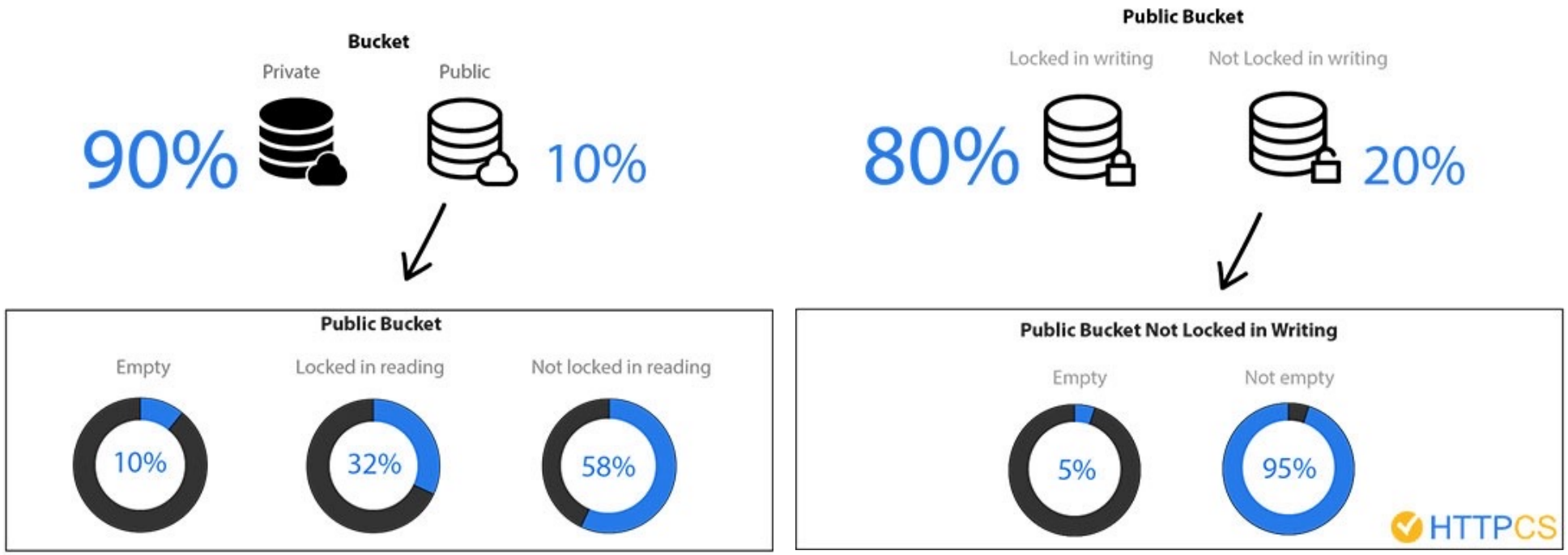
NotSoSecure part of claranet cyber security

Storage Accounts

- Lynchpin of cloud existance
- Storage attacks
  - Enumeration
  - Attack
  - Exploit and post exploit

NotSoSecure part of claranet cyber security

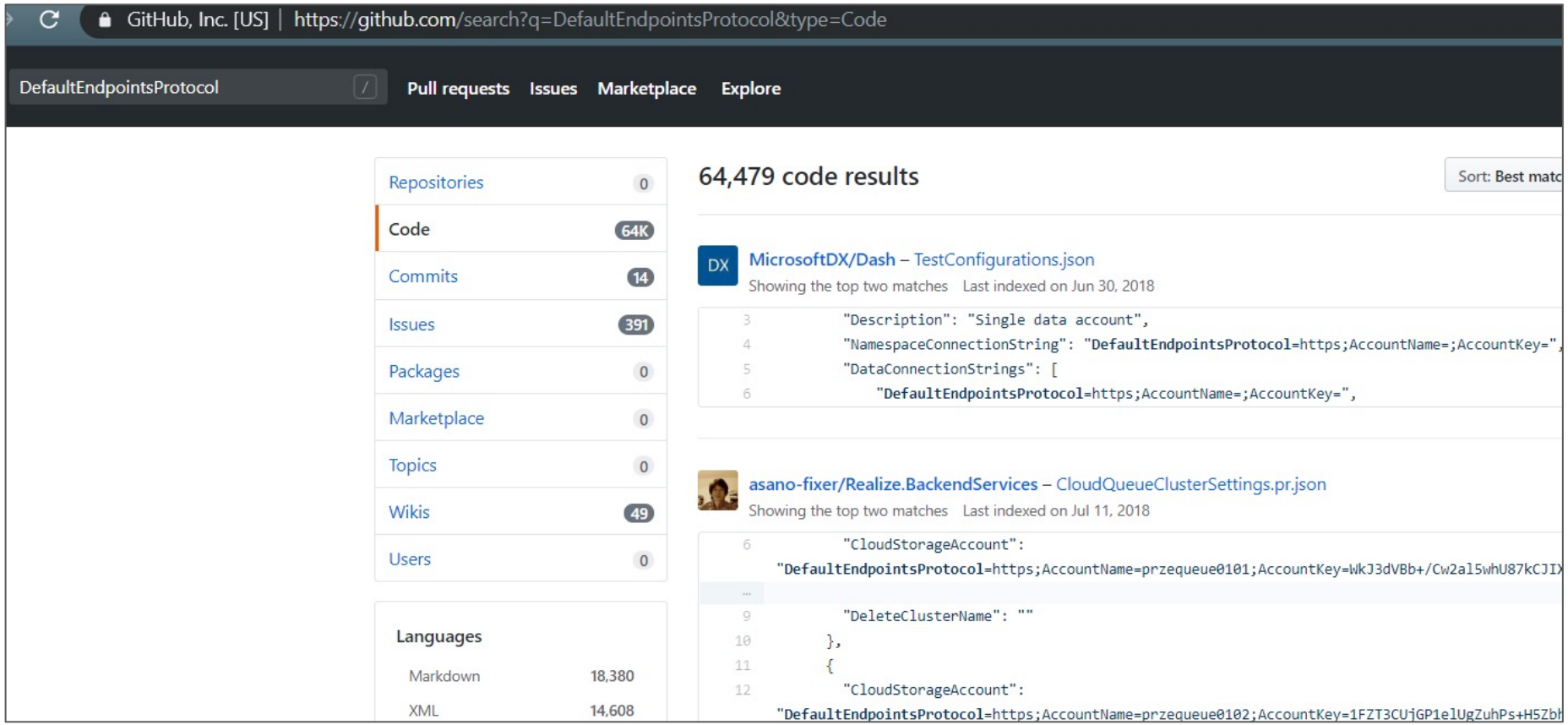
AWS S3



https://www.bleepingcomputer.com/news/security/2-percent-of-amazon-s3-public-buckets-arent-write-protected-exposed-to-ransom-attacks/
https://blog.httpcs.com/etude-dimpact-configuration-aws-buckets-amazon-s3/

NotSoSecure part of claranet cyber security

Azure blob



NotSoSecure part of claranet cyber security

Case Study

Azure Attacks: Azure Storage

Starting point: Overly Privileged Azure Storage SAS URL is exposed

Exploitation Process:

- Obtain an Azure Storage SAS URL
- Load the URL in Azure Storage explorer or similar
- Identify various assets available in the storage
- Access the source code of the Azure function
- Plant a backdoor, next invocation gets the backdoor running
- Hide the backdoor

Reference:
https://www.notsosecure.com/identifying-exploiting-leaked-azure-storage-keys/

Case Study

PaaS: Elastic Beanstalk: Attack Case Study

- Starting point: SSRF on an application hosted in AWS Elastic Beanstalk

Exploitation Process:

1. Obtained Metadata details (account id, region, security-credentials)
2. No direct access to read S3 bucket list
3. Enumerated bucket name using the account id and region
4. Access source code of the application via AWS S3 CLI
5. CI/CD in place hence a backdoor pushed to S3 bucket will result in shell deployed on the official website
6. Summitroute did extra research & identified more such naming patterns

Reference:
https://www.notsosecure.com/exploiting-ssrf-in-aws-elastic-beanstalk/
https://summitroute.com/blog/2019/02/10/aws_resource_naming_patterns/
https://gist.github.com/0xdabbad00/645837c1fcd043876d13a56819188227

Authentication Services: AWS IAM

- Cloud shadow admins are the accounts which have permissions that attackers could abuse to escalate privileges and take hold of the entire environment

- These accounts are typically overlooked as they are not a member of privileged group (Ex. Domain Admin)

NotSoSecure part of claranet cyber security

Case Study

AWS Policies

- AWS has multiple policies which are basically mapped to user roles to grant/restrict the access
- “AmazonElasticTranscoderFullAccess” policy has “iam:PutRolePolicy” permissions.
- “iam:PutRolePolicy” permission allows us to attach an inline policy to role.
- AWS has fixed this by rolling out new policy “AmazonElasticTranscoder_FullAccess”

Reference:
https://medium.com/ymedialabs-innovation/an-aws-managed-policy-that-allowed-granting-root-admin-access-to-any-role-51b409ea7ff0

Case Study

AWS Cognito

- Cognito supports two types of credentials Unauthenticated and Authenticated
- Unauthenticated credentials related research was performed by Andres Riancho (BlackHat 2019)
- We extended the research around authenticated Credentials and found ways to leverage hidden signup features

Reference:
https://andresriancho.com/internet-scale-analysis-of-aws-cognito-security/
https://www.notsosecure.com/hacking-aws-cognito-misconfigurations/

Thank You

Contact / Feedback : anant@notsosecure.com

We are running multiple training programs @ BlackHat USA 2021

https://notsosecure.com/blackhat-2021/

NotSoSecure part of claranet cyber security