



OG CYBER



SECURE CLOUD ARCHITECTURE

OGC-Team Expertise for Cool Delivery





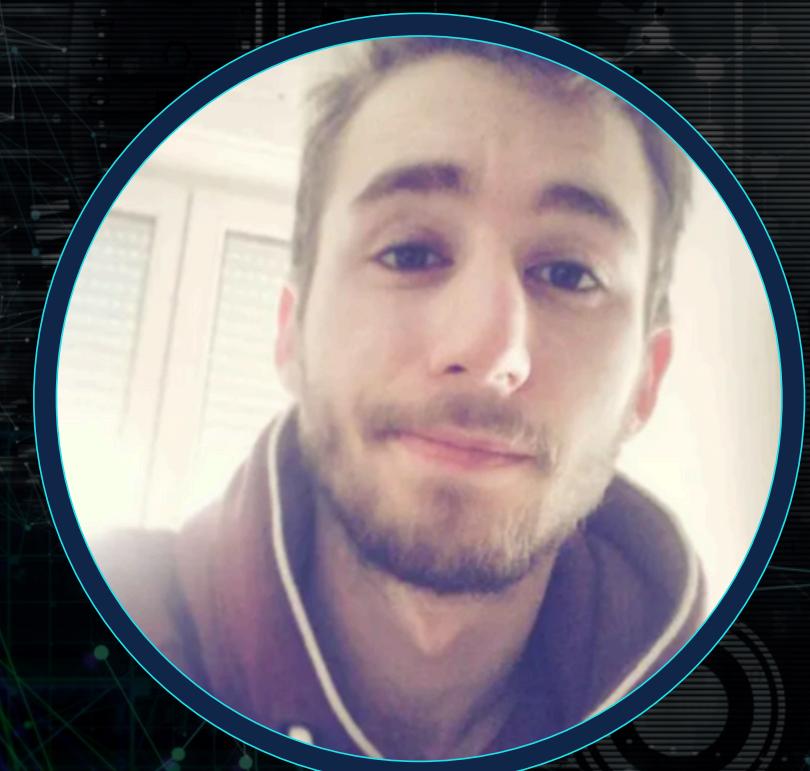
OG CYBER



TEAM



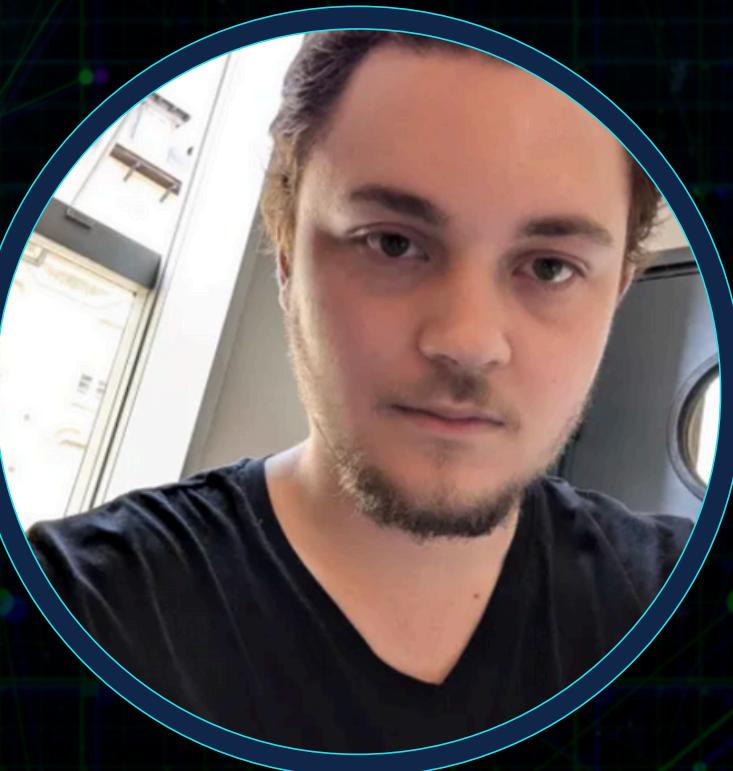
Bilal
Benlahcene



Silviu Zaino



Raphael
de Monchy

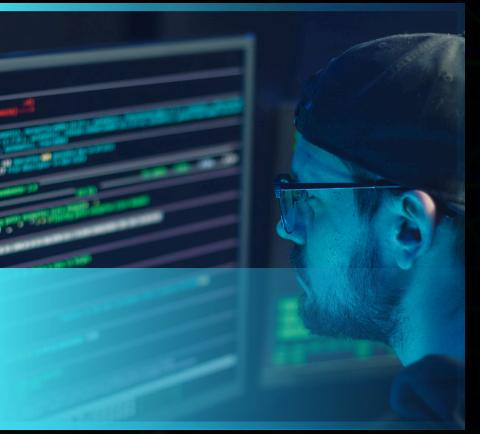


Louis
Outrey



SUMMARY

- 1 Introduction & Context
- 2 Fundamentals recap
- 3 Cloud Security Risks & Challenges
- 4 Proposed Secure Cloud Architecture
- 5 Tools & Best Practices
- 6 Conclusion





OUR MISSION



OGC-Team

ON-PREM
→ CLOUD (AWS)
 → 



Cool
Delivery

- OG-Team was assigned to **secure** and **modernize** Cool Delivery's infrastructure.
- We designed a **scalable**, **secure** **AWS-based** architecture.



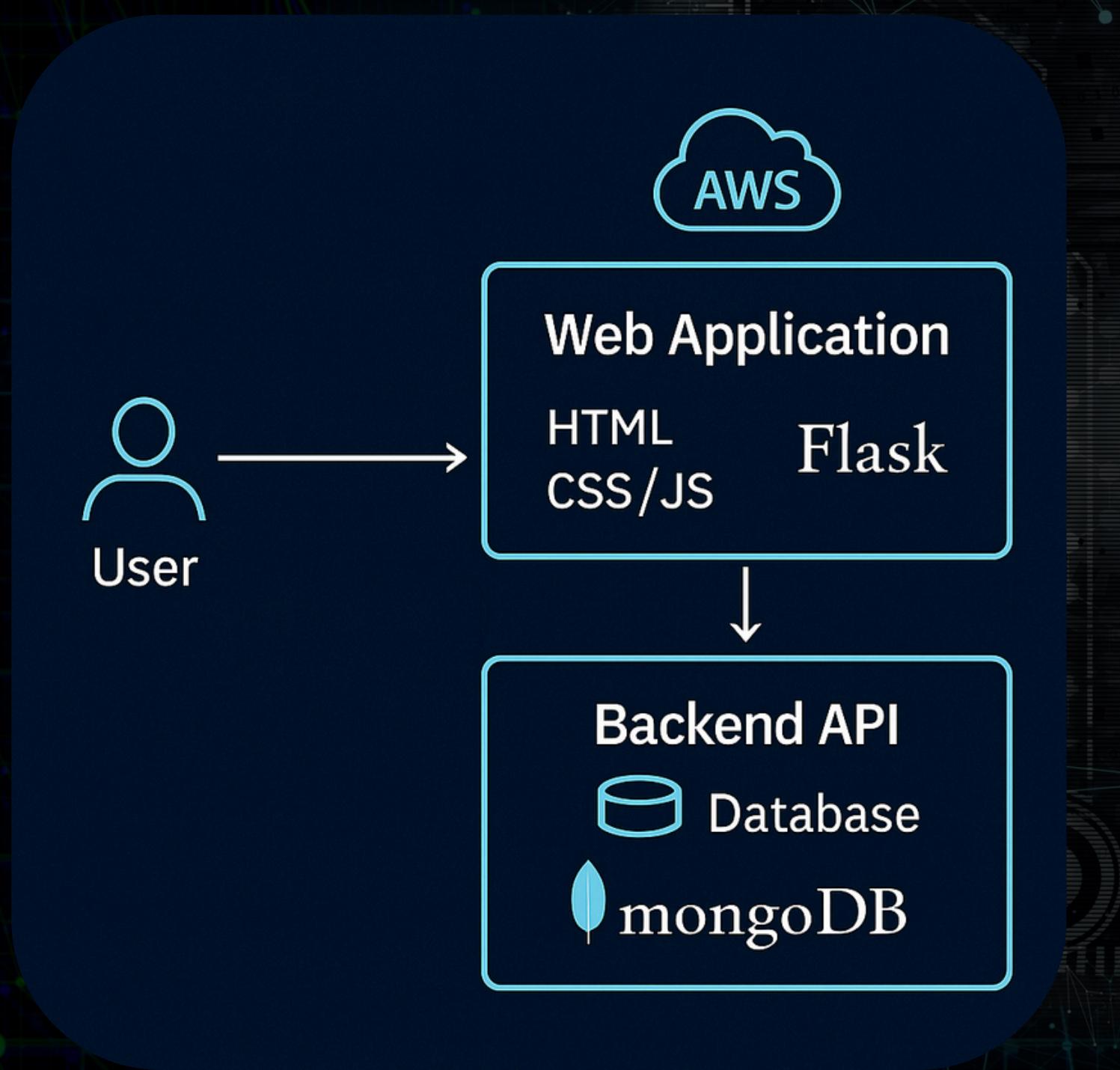
WHY MOVE TO THE CLOUD ?

On-Prem	AWS
Hardware	Virtualized
Fixed cost	Pay-per-use
Manual ops	Automation

- Scalability
- Flexibility
- Cost efficiency



PROJECT SCOPE



- 3 Environments
- Full stack: Front(s3), api(Flask), db (mongodb)
- Goal: secure & scalable setup



FUNDAMENTALS RECAP



Cloud



Security



Architecture

- Cloud: **shared** computing resources
- Security = protection
- Architecture = **structured** design



STRIDE THREAT MODEL SUMMARY



Spoofing



Tampering



Repudiation



Information Disclosure



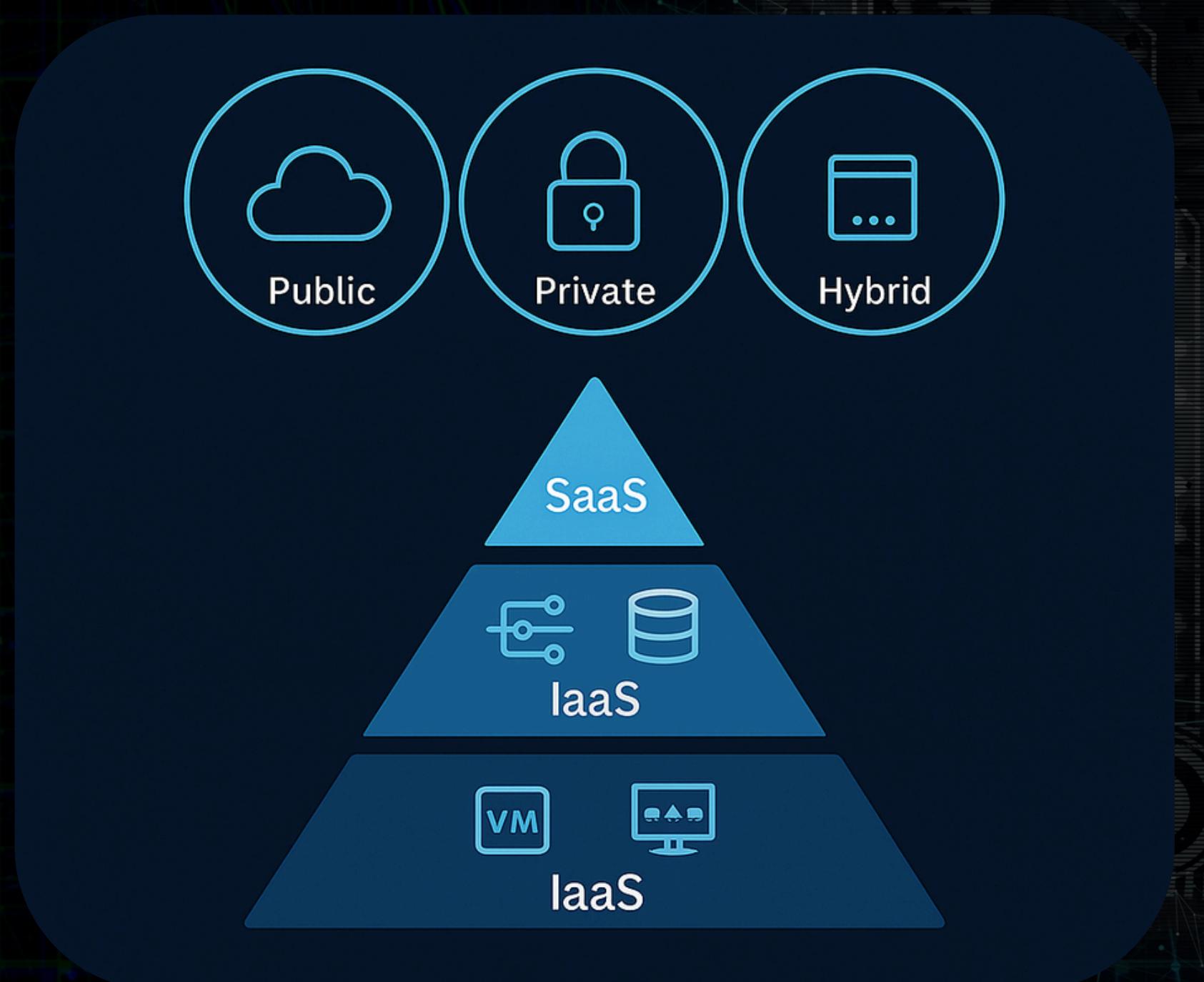
Denial
of Service



- MFA blocks spoofing
- IAM least privilege prevents privilege escalation
- Cloudtrail logs actions



CLOUD TYPE



- Cloud types: public, private, hybrid
- IaaS: infra / vm
- PaaS: platform / db / app hosting
- SaaS: ready-to-use apps



CLOUD SECURITY THREATS



Spoofing



Injection



Misconfiguration



DDoS



Vulnerability
Exploitation

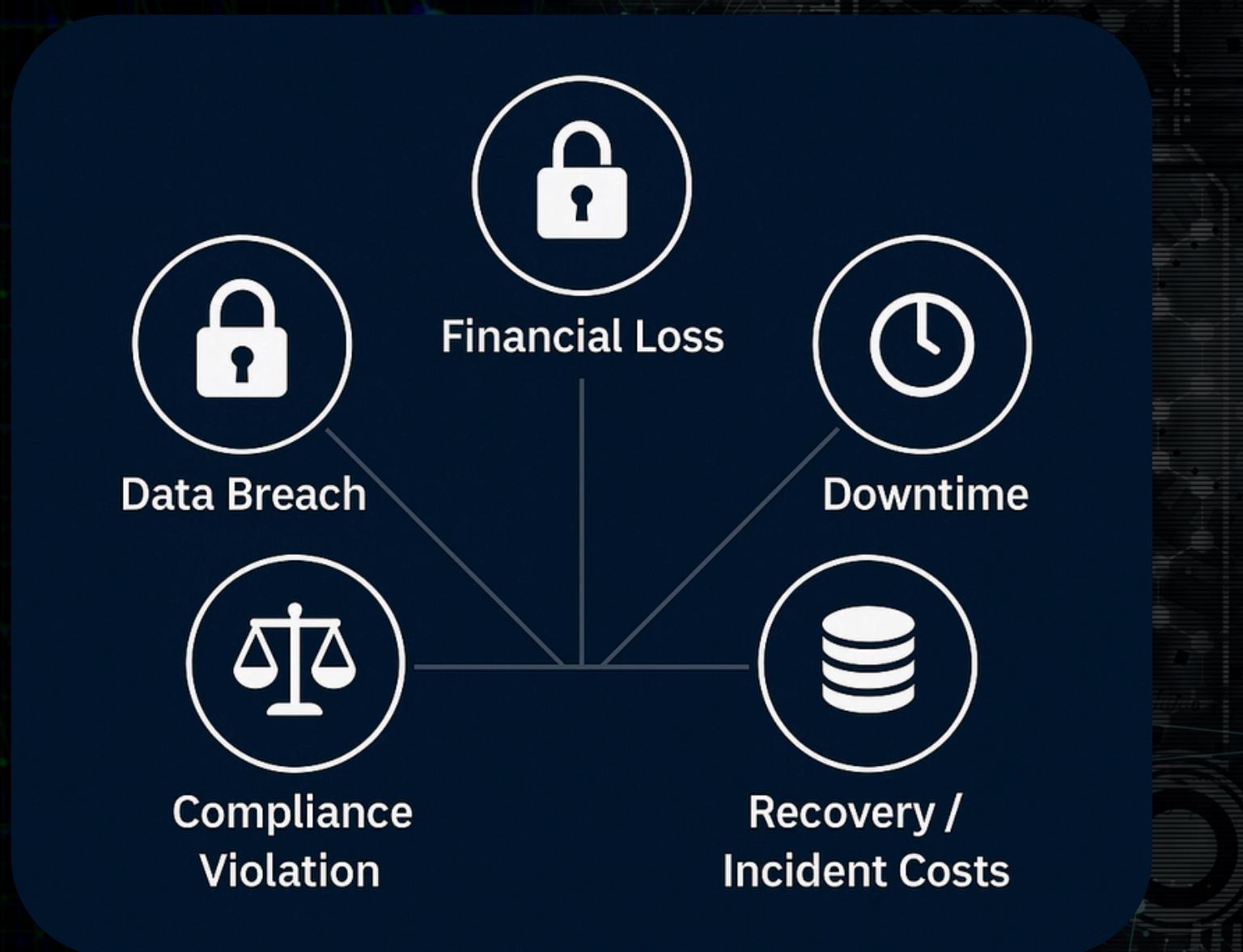


Insider
Threats

- Top attack vectors in cloud environments
- Often enabled by human error or poor configuration
- Threat modeling is key to mitigation



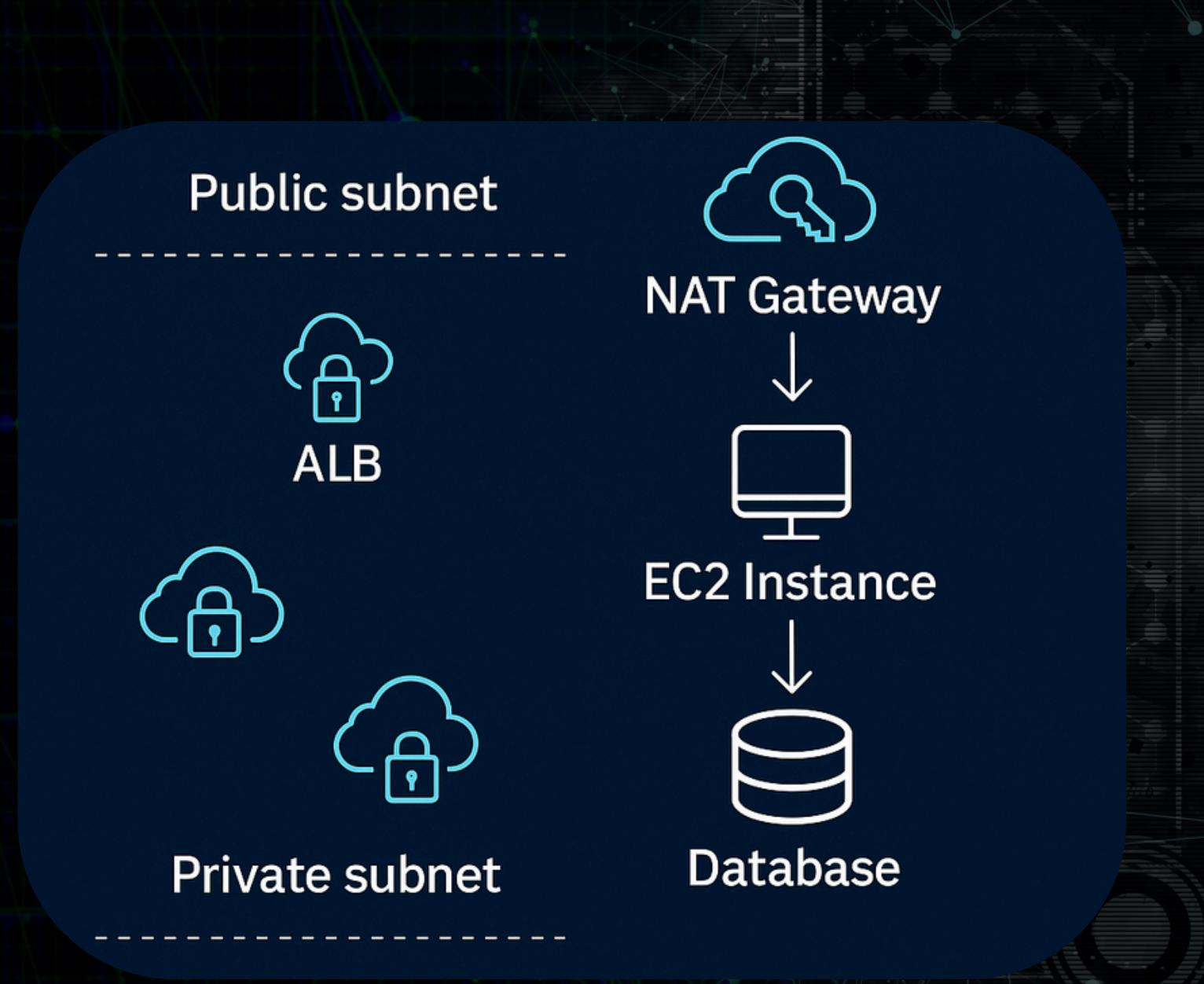
CLOUD SECURITY THREATS



- Breaches = Legal, Financial & Trust Damage
- Misconfigurations = Most common entry point
- Cloud incidents = Higher recovery time and costs



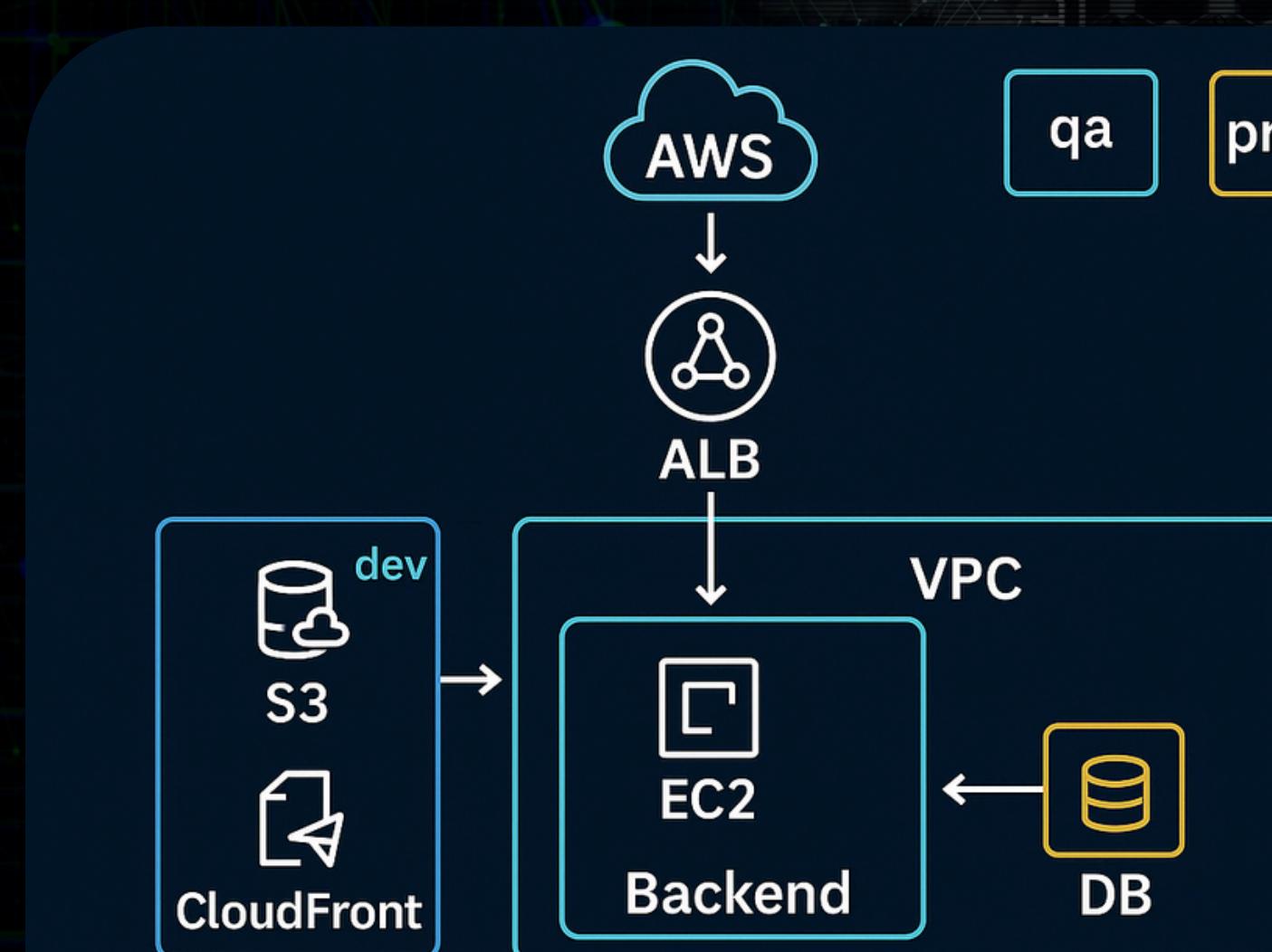
NETWORK SEGMENTATION & SECURITY



- Public : loader balancer, s3 (statique)
- Private: ec2 (backend)
- Secured: logs & monitoring



OVERVIEW ARCHITECTURE



Resources
You are using the following Amazon EC2 resources in the Europe (Ireland) Region:

Instances (running)	1	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	1
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	2	Snapshots	0	Volumes	1

Backend ec2

sg-04dbe013cd1563208 - launch-wizard-1

Details

Security group name	Security group ID	Description	VPC ID
launch-wizard-1	sg-04dbe013cd1563208	launch-wizard-1 created 2025-04-23T18:57:16.522Z	vpc-028489f8c8aa672e6
Owner	Inbound rules count	Outbound rules count	
639649899092	3 Permission entries	1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

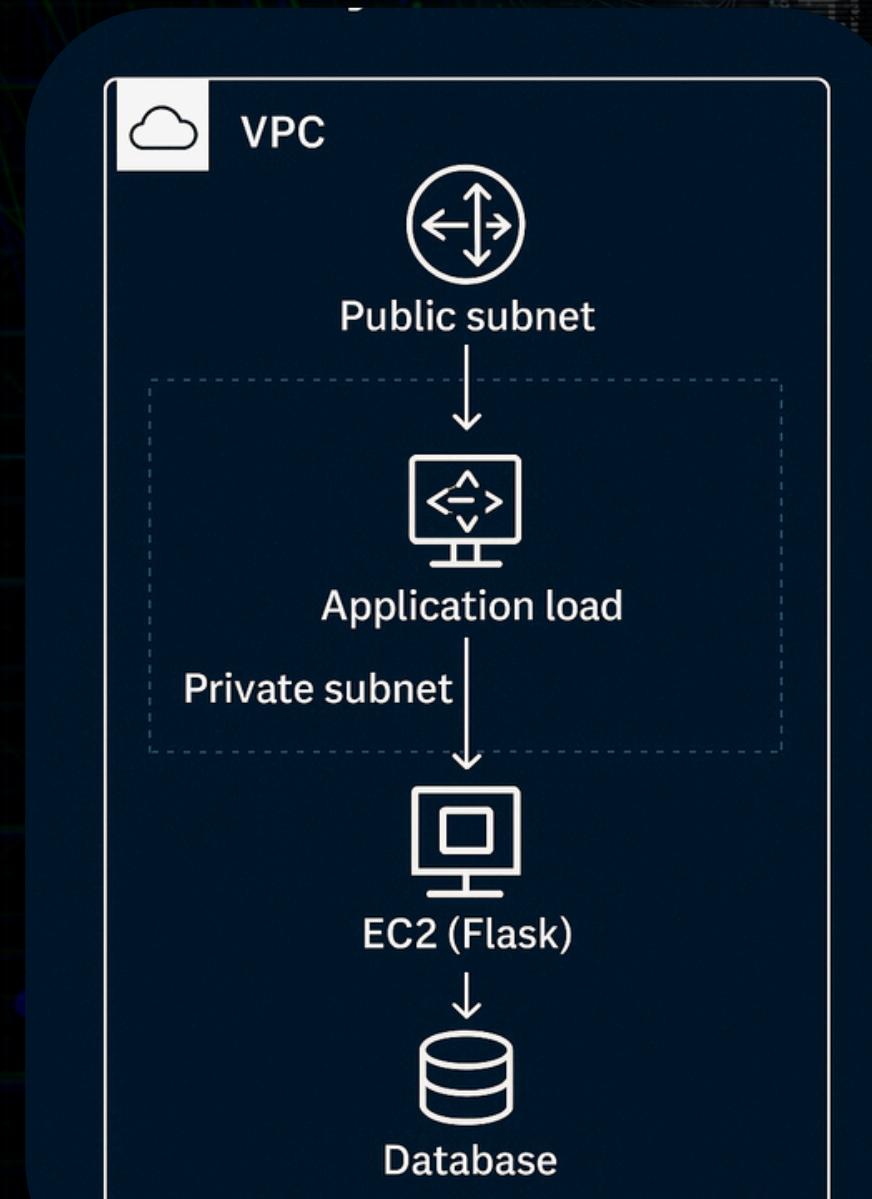
Inbound rules (3)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
-	sgr-04ab0beab4fcfc12e	IPv4	SSH	TCP	22	0.0.0.0/0	-
-	sgr-0555f132d6bbb03cc	IPv4	HTTPS	TCP	443	0.0.0.0/0	-
-	sgr-0dff83561555c665a	IPv4	HTTP	TCP	80	0.0.0.0/0	-

Frontend s3



NETWORK AND SEGMENTATION



Details Info

VPC ID vpc-028489f8c8aa672e6	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0bf15984c266f42dd	Main route table rtb-07cf9c2ff5c0ddc26
Main network ACL acl-0e2d36b21146e4300	Default VPC Yes	IPv4 CIDR 172.31.0.0/16	IPv6 pool -
IPv6 CIDR -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 639649899092

Subnets (3)
Subnets within this VPC

- eu-west-1a
 - subnet-0cb65fcbe9a81dd22
- eu-west-1b
 - subnet-0e7f6a260e215dcc
- eu-west-1c
 - subnet-03b1803ca77b41636

Route tables (1)
Route network traffic to resources

- rtb-07cf9c2ff5c0ddc26

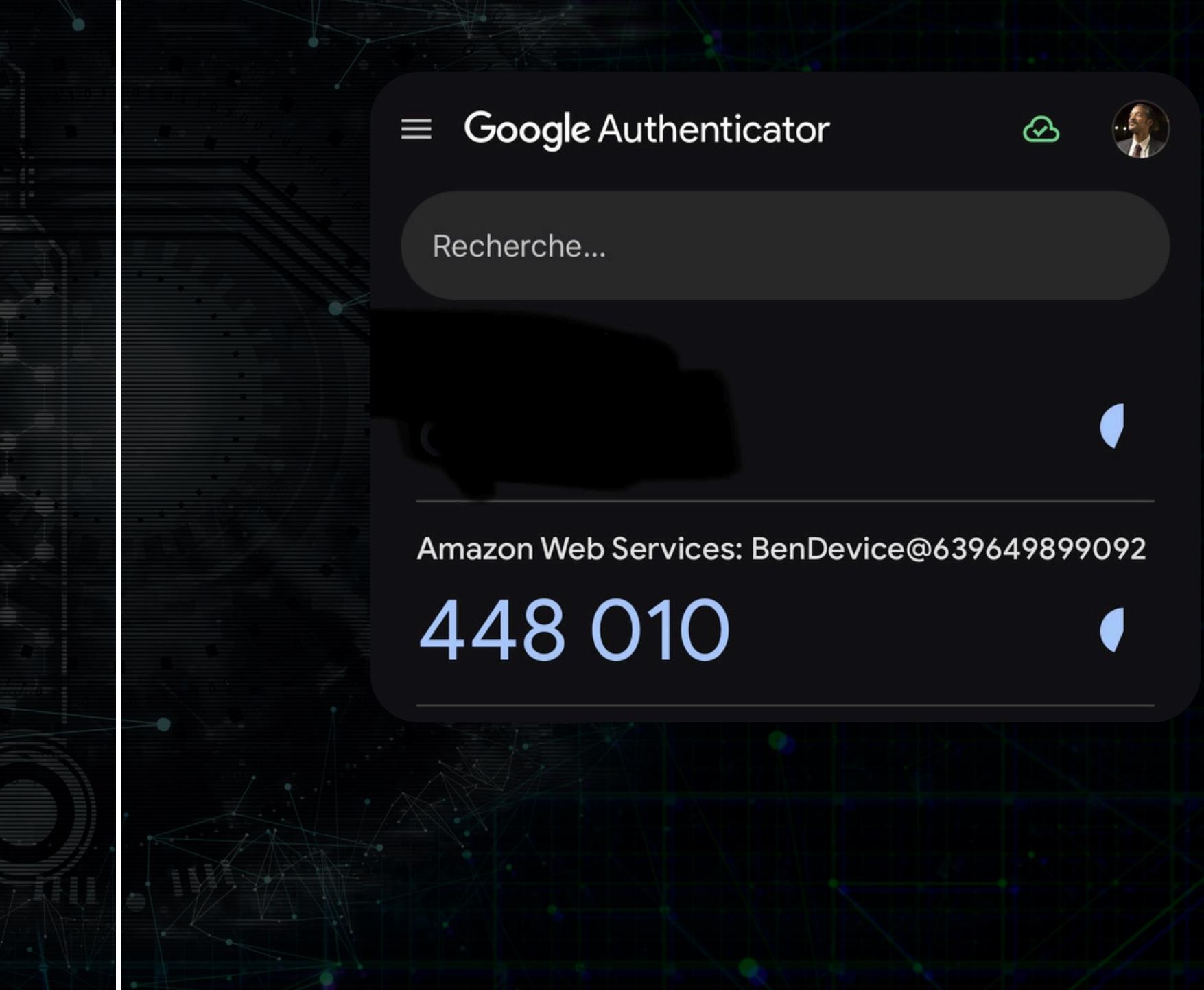
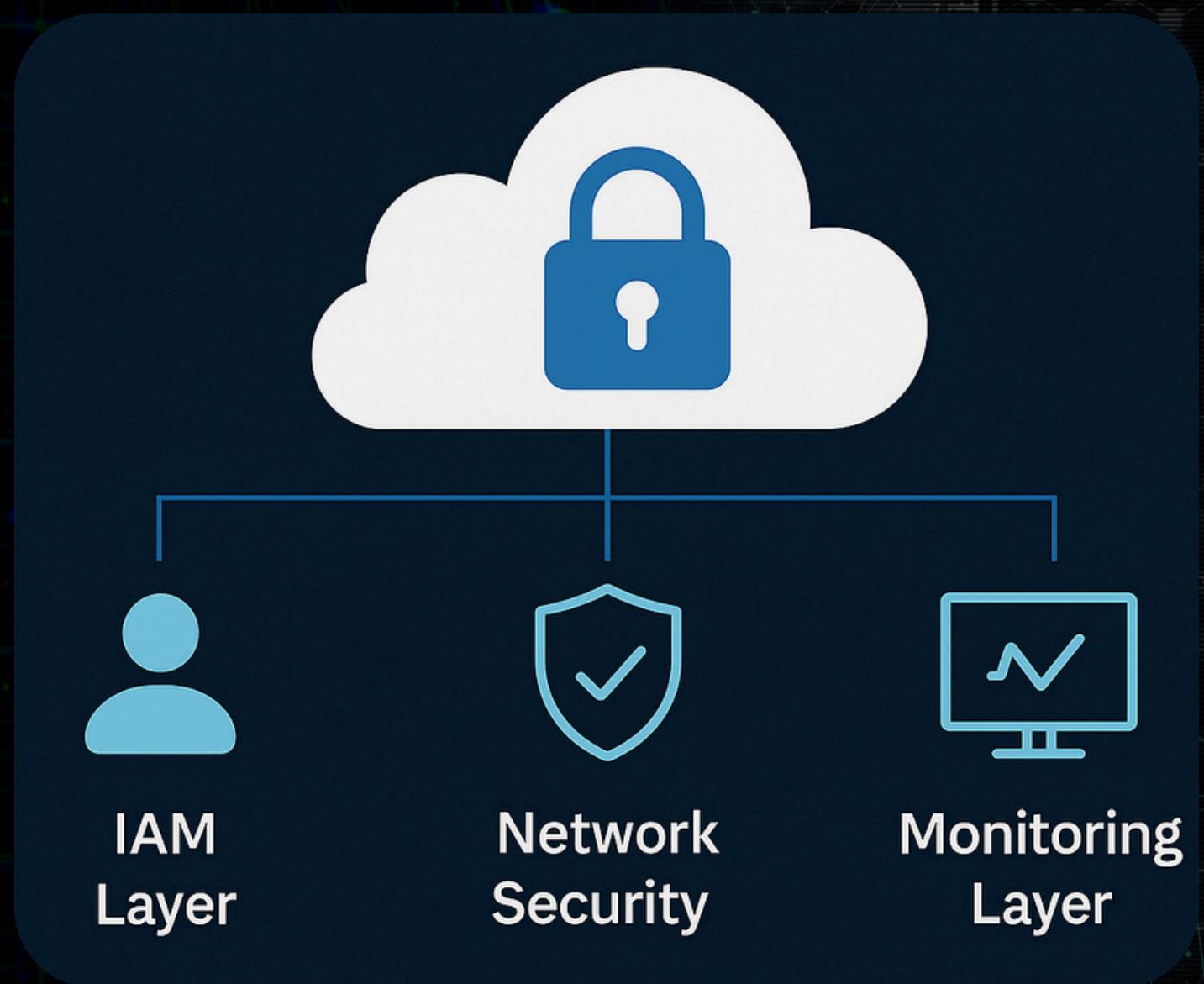
Network connections (1)
Connections to other networks

- igw-09c4122d402f266bb

Subnets (vpc)

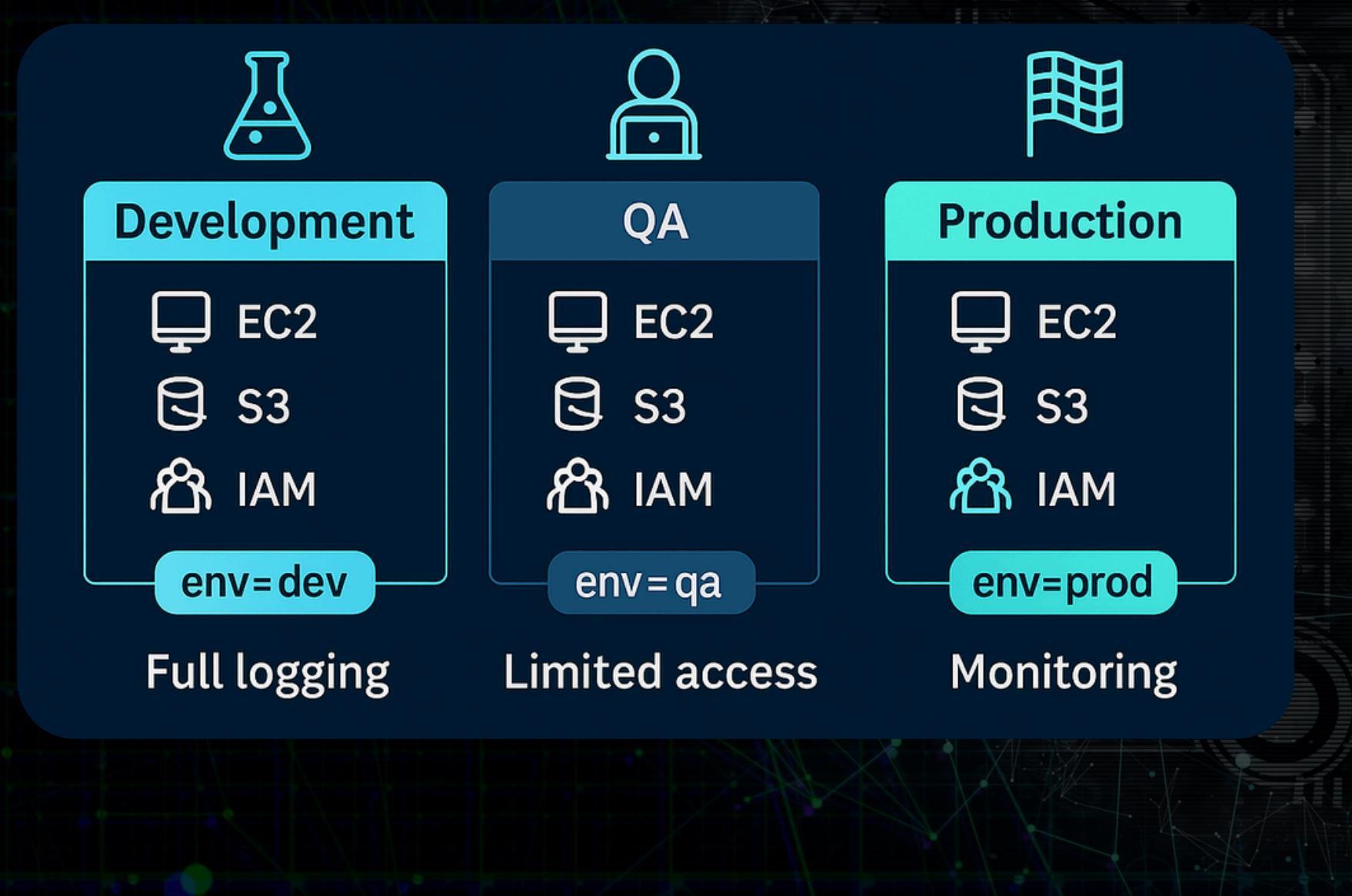


IAM & SECURITY





SEPARATION DEV / QA / PROD



```
[ec2-user@ip-172-31-44-223 ~]$ sudo systemctl enable auditd
[ec2-user@ip-172-31-44-223 ~]$ sudo systemctl start auditd
[ec2-user@ip-172-31-44-223 ~]$ sudo systemctl status auditd
● auditd.service - Security Auditing Service
  Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
  Active: active (running) since Mit 2025-04-23 18:44:03 UTC; 17h ago
    Docs: man:auditd(8)
          https://github.com/linux-audit/audit-documentation
   Main PID: 2609 (auditd)
     CGroup: /system.slice/auditd.service
             └─2609 /sbin/auditd

Apr 23 18:44:03 localhost augenrules[2613]: backlog_wait_time 15000
Apr 23 18:44:03 localhost augenrules[2613]: enabled 1
Apr 23 18:44:03 localhost augenrules[2613]: failure 1
Apr 23 18:44:03 localhost augenrules[2613]: pid 2609
Apr 23 18:44:03 localhost augenrules[2613]: rate_limit 0
Apr 23 18:44:03 localhost augenrules[2613]: backlog_limit 8192
Apr 23 18:44:03 localhost augenrules[2613]: lost 0
Apr 23 18:44:03 localhost augenrules[2613]: backlog 1
Apr 23 18:44:03 localhost augenrules[2613]: backlog_wait_time 15000
Apr 23 18:44:03 localhost systemd[1]: Started Security Auditing Service.
[ec2-user@ip-172-31-44-223 ~]$
```

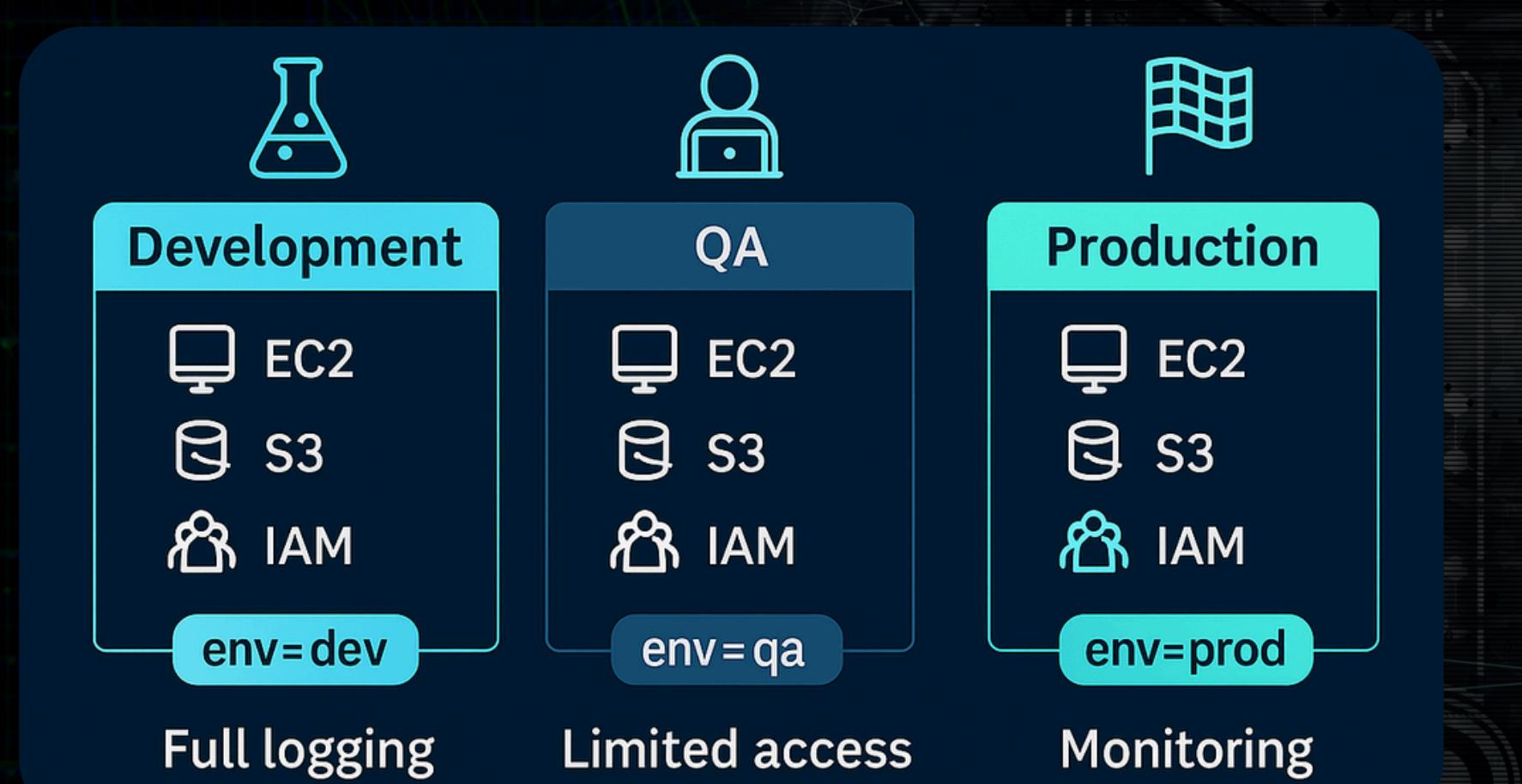
```
[ec2-user@ip-172-31-44-223 ~]$ sudo lsof -i -P -n | grep LISTEN
rpcbind 2645 rpc 8u IPv4 15942 0t0 TCP *:111 (LISTEN)
rpcbind 2645 rpc 11u IPv6 15945 0t0 TCP *:111 (LISTEN)
master 3092 root 13u IPv4 18079 0t0 TCP 127.0.0.1:25 (LISTEN)
sshd 3522 root 3u IPv4 77621 0t0 TCP *:22 (LISTEN)
sshd 3522 root 4u IPv6 77630 0t0 TCP *:22 (LISTEN)
[ec2-user@ip-172-31-44-223 ~]$ sudo systemctl list-units --type=service --state=running
UNIT                                     LOAD  ACTIVE SUB   DESCRIPTION
acpid.service                            loaded  active running ACPI Event Daemon
amazon-ssm-agent.service                loaded  active running amazon-ssm-agent
atd.service                               loaded  active running Job spooling tools
audited.service                          loaded  active running Security Auditing Service
chronyd.service                         loaded  active running NTP client/server
crond.service                           loaded  active running Command Scheduler
dbus.service                             loaded  active running D-Bus System Message Bus
fail2ban.service                         loaded  active running Fail2Ban Service
firewalld.service                       loaded  active running firewalld - dynamic firewall daemon
getty@tty1.service                      loaded  active running Getty on tty1
gssproxy.service                        loaded  active running GSSAPI Proxy Daemon
libstoragemgmt.service                 loaded  active running libstoragemgmt plug-in server daemon
lvm2-lvmetad.service                   loaded  active running LVM2 metadata daemon
network.service                         loaded  active running LSB: Bring up/down networking
postfix.service                         loaded  active running Postfix Mail Transport Agent
rngd.service                            loaded  active running Hardware RNG Entropy Gatherer Daemon
rpcbind.service                         loaded  active running RPC bind service
rsyslog.service                         loaded  active running System Logging Service
serial-getty@ttyS0.service              loaded  active running Serial Getty on ttys0
sshd.service                            loaded  active running OpenSSH server daemon
systemd-journald.service               loaded  active running Journal Service
systemd-logind.service                 loaded  active running Login Service
systemd-udevd.service                  loaded  active running udev Kernel Device Manager

LOAD  = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB   = The low-level unit activation state, values depend on unit type.
```

23 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.



MONITORING & ALERTING



Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about

S3 static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint.

<http://cool-delivery-frontend.s3-website-eu-west-1.amazonaws.com>

Console sign-in

Console sign-in link

<https://639649899092.signin.aws.amazon.com/console>

Console password

Updated 12 minutes ago (2025-04-24 12:49 GMT+2)

Last console sign-in

Never



AWS TOOLS & SERVICES USED



EC2
Compute
backend



Frontend
static hosting



CDN / cache



ALB
Secure routing
(HTTPS)



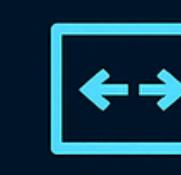
IAM
Access
control



CloudWatch
Logs /
monitoring



Auditing



VPC
Network
segmentation

- Each service was selected and integrated according to its role on our architecture
- This ensures performance, security, and maintainability across all environments and workloads



BEST PRACTICES APPLIED

- Least Privilege IAM
- MFA enabled for all users
- Subnet isolation:
public / private
- Centralized logging
(CloudWatch)
- Full audit trail
(CloudTrail)
- Environment tagging enforced
- Public access disabled by default

- Our architecture implements key aws best practices to ensure a secure, scalable, and auditable environment
- Resources are isolated by design, access is tightly controlled and every action is monitored and traceable



CONCLUSION

