HELECLOUD

AWS Security Best Practices

Ivaylo Vrabchev, HeleCloud

Name - **Ivaylo Vrabchev**
Company - **HeleCloud**
Role - **AWS Consultant & Team Leader**
Skills and knowledge

- AWS
- CI/CD & Automation
- Networking
- Security

AWS Initiatives

- New Horizons Course
- AWS User Group Bulgaria
- Whitepapers & Blog posts

Internet Security Threat Report

- Crypto-jacking Attacks Explode by 8,500 Percent
- 1 in 13 Web requests lead to malware
- 92% Increase in new downloader variants
- 80% Increase in new malware on Macs
- 46% Increase in new ransomware variants
- 600% Increase in attacks against IoT devices
- Increase in mobile malware variants 54%
- 13% Overall increase in reported vulnerabilities

HELECLOUD

HELECLOUD

Public cloud security

What are your biggest operational, day-to-day headaches trying to protect cloud workloads?

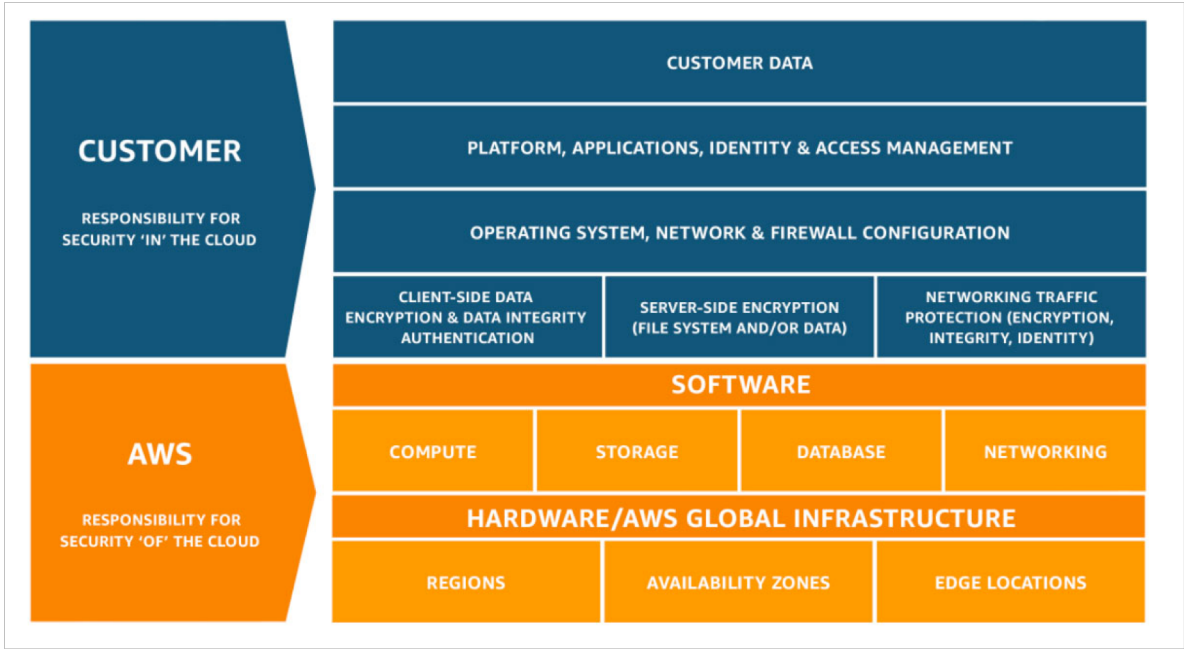
- Misconfiguration of the cloud platform – 62%
- Unauthorized access– 55%
- Insecure interfaces /APIs - 50%
- Hijacking of accounts, services or traffic – 47%

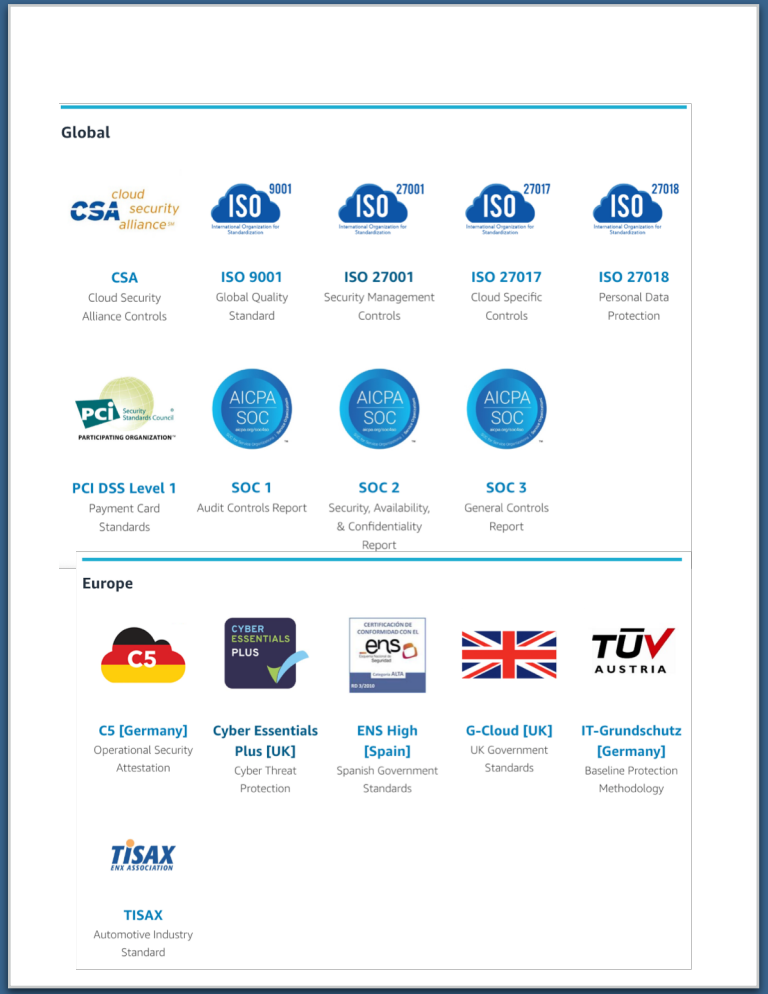
Introduction to AWS Security

Information security is of paramount importance to Amazon Web Services (AWS) customers. Security is a core functional requirement that protects mission critical information from accidental or deliberate theft, leakage, integrity compromise, and deletion.

AWS shared responsibility model

Security and Compliance is a shared responsibility between AWS and the customer. As shown in the chart, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud.





HELECLOUD

Security "of" the cloud

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

Security "in" the cloud

ACCOUNT SECURITY & COMPLIANCY

INFRASTRUCTURE & OPERATING SYSTEM

LOGGING AND MONITORING

DATA SECURITY "AT REST" AND "IN TRANSIT"

Account Security

HELECLOUD

ALTERNATIVE CONTACTS

HARDWARE MFA FOR THE ROOT ACCOUNT

STRONG PASSWORD

DO NOT USE ROOT ACCOUNT

BILLING ALARMS

AWS CLOUDTRAIL & CONFIG GLOBALLY

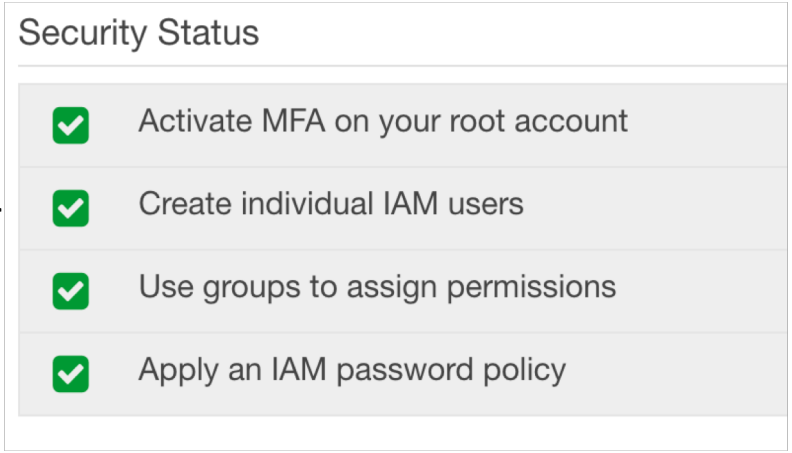
APPLY SELF COMPLIANT CONFIG RULES

SUPPORT PLAN & TRUSTED ADVISOR

AWS Identity and Access Management (IAM)

HELECLOUD

- Require at least one uppercase letter
- Require at least one lowercase letter
- Require at least one number
- Require at least one non-alphanumeric character
- Allow users to change their own password
- Enable password expiration
- Password expiration period (in days):
- Prevent password reuse
- Number of passwords to remember:
- Password expiration requires administrator reset



AWS Identity and Access Management (IAM)

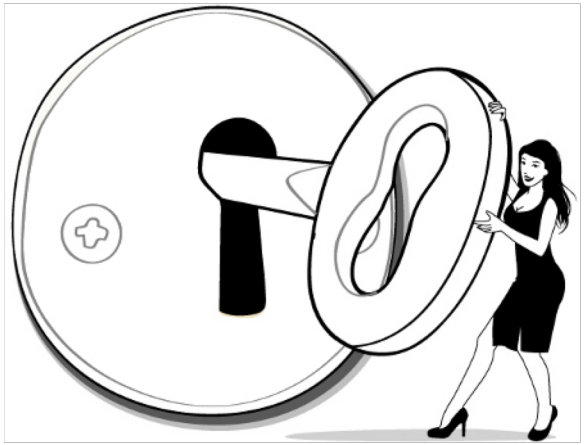
- Use central IdP AWS or External
- Grant permission only via groups or roles
- Apply least privilege model
- Enforce MFA usage for IAM users via policies

"Condition": { "Bool": {
"aws:MultiFactorAuthPresent": "true" }

AWS Identity and Access Management (IAM)

HELECLOUD

- Treat your passwords like your underwear
- Rotate passwords at least every 90 days
- Rotate access keys less than 90 days



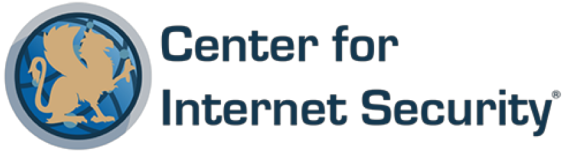
Automate least-privilege model

Aardvark

Aardvark and Repokid help us get closer to the principle of least privilege without sacrificing speed or introducing heavy process.

CIS AWS Benchmark

HELECLOUD

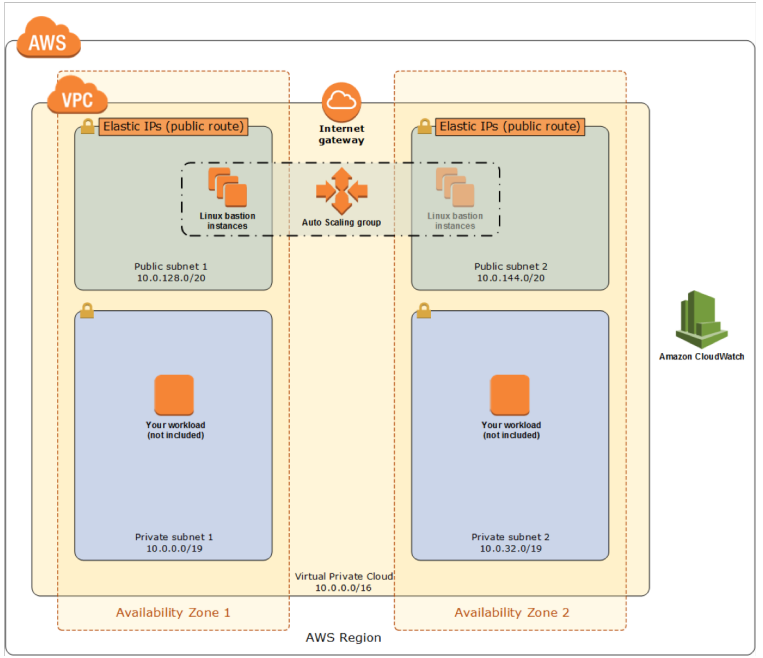


- Configure you AWS Account based on provided recommendations
- Codify all recommendation in AWS Config for compliance & historical changes
- Alert the security team if something is changed

AWS Infrastructure

HELECLOUD

- Architect your VPCs with minimum 2 private and 2 public subnets
- Expose only required resources in the public subnets
- Allow only ports used by deployed applications
- Access AWS and third-party services via VPC endpoints
- Use auditable bastion hosts or SSM to manage your instances
- Use configuration management & Infrastructure as Code (IaC) tools to codify your environment

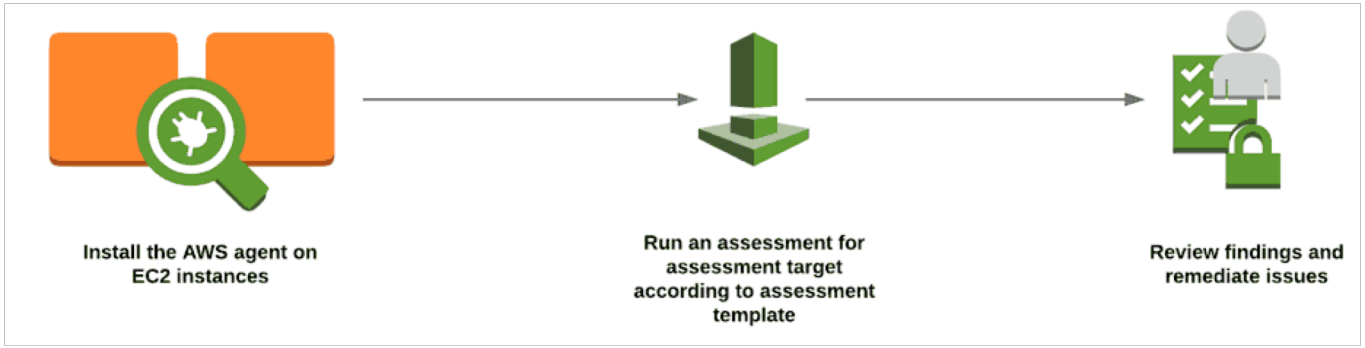


OS Hardening and Vulnerability scans

HELECLOUD

Center for Internet Security®

- Automate the process of baking AMIs
- Apply CIS recommendation for the used OS
- Introduce AWS Inspector Scans as part of the baking process and run them on a regular period of time
- Alert the security team vulnerability is detected



Anti-Virus and Integrity scans

HELECLOUD

- Install Anti-Virus software - ClamAV
- Install Integrity checks software - OSSEC
- Run periodical scans
- Automate the reactive process if malicious threat is detected - CloudWatch and Lambda

Application password management

HELECLOUD

- Grant permissions via IAM roles if possible
- Use parameter store
- Store you passwords in AWS Secrets Manager

Logging & Auditing in AWS

HELECLOUD

Configure centralized logging solution e.g. CloudWatch

Enable all infrastructure logs and store them in CloudWatch

CloudTrail

VPC Flow logs

S3 logs

CloudFront

WAF

ELB

Route53

Send OS and application logs data to CloudWatch using CW agent

Configure separate AWS account and store a copy of all CloudWatch logs into it

Enable AWS Guard Duty

Log analysis

AWS ATHENA

ELASTICSEARCH AND KIBANA (ELK)

Data security

Encrypt all your data at rest

- EBS volumes
- S3 buckets
- RDS
- SQS
- Redshift

Data & Asset Classification

- Tagging
- Naming convention

Encrypt data in transit:

- IPSec or TLS 1.2
- X.509 certificates
- SHA-256(SHA2)
- CloudHSM

HELECLOUD

Train your team

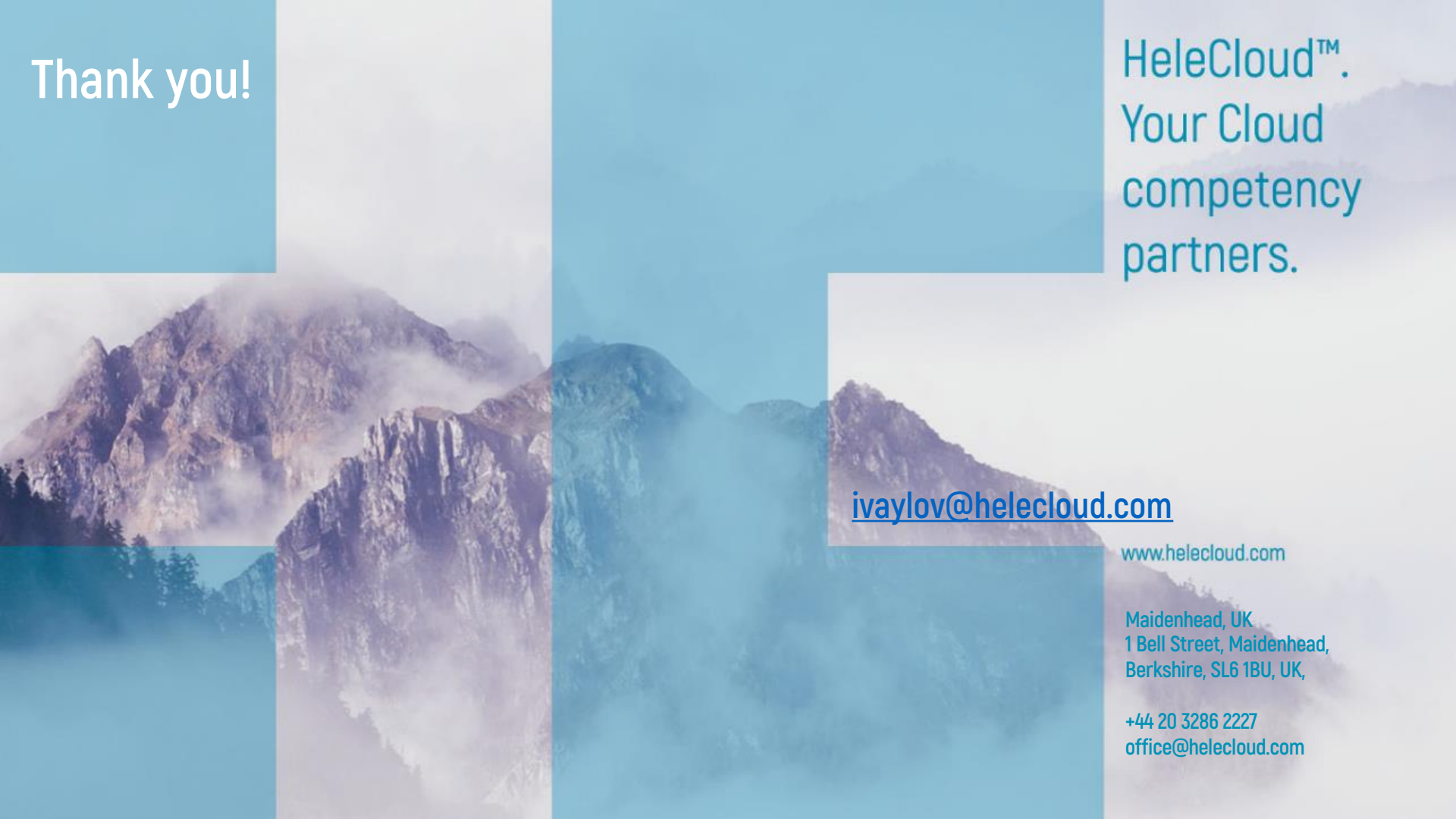
- Periodical security trainings
- Game days
- Up to date documentation

Resources

HELECLOUD

Whitepapers	https://aws.amazon.com/whitepapers/aws-security-best-practices/ https://d1.awsstatic.com/whitepapers/architecture/AWS-Security-Pillar.pdf
CIS AWS Benchmark	https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf
IAM Least privilege model	https://github.com/Netflix/repokid https://github.com/Netflix-Skunkworks/aardvark

Thank you!



HeleCloud™.
Your Cloud
competency
partners.

ivaylov@helecloud.com

www.helecloud.com

Maidenhead, UK
1 Bell Street, Maidenhead,
Berkshire, SL6 1BU, UK,

+44 20 3286 2227
office@helecloud.com