WE STAND WITH
UKRAINE

Common security pitfalls in AWS for highly regulated industries

WE STAND WITH UKRAINE

% whoami
Daniel Rankov

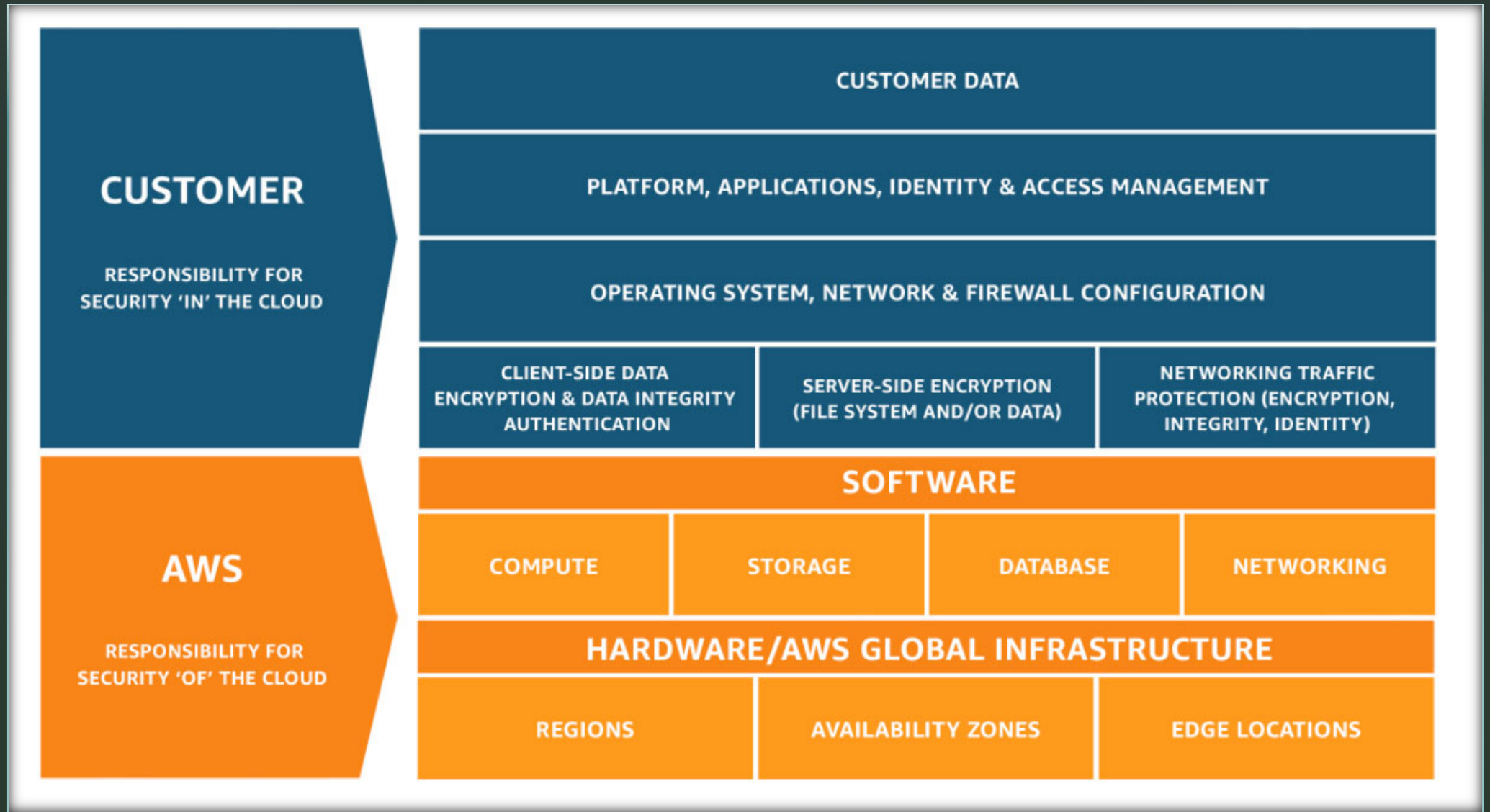
- Cloud & DevOps Consultant
- Multiple certifications on AWS, including Solution Architect and DevOps professional levels
- Leading Cloud & DevOps teams in multicloud environments
- Corporate AWS and DevOps training
- AWS Bulgaria User Group Co-Organizer
- AWS Community Hero

Regulated industries

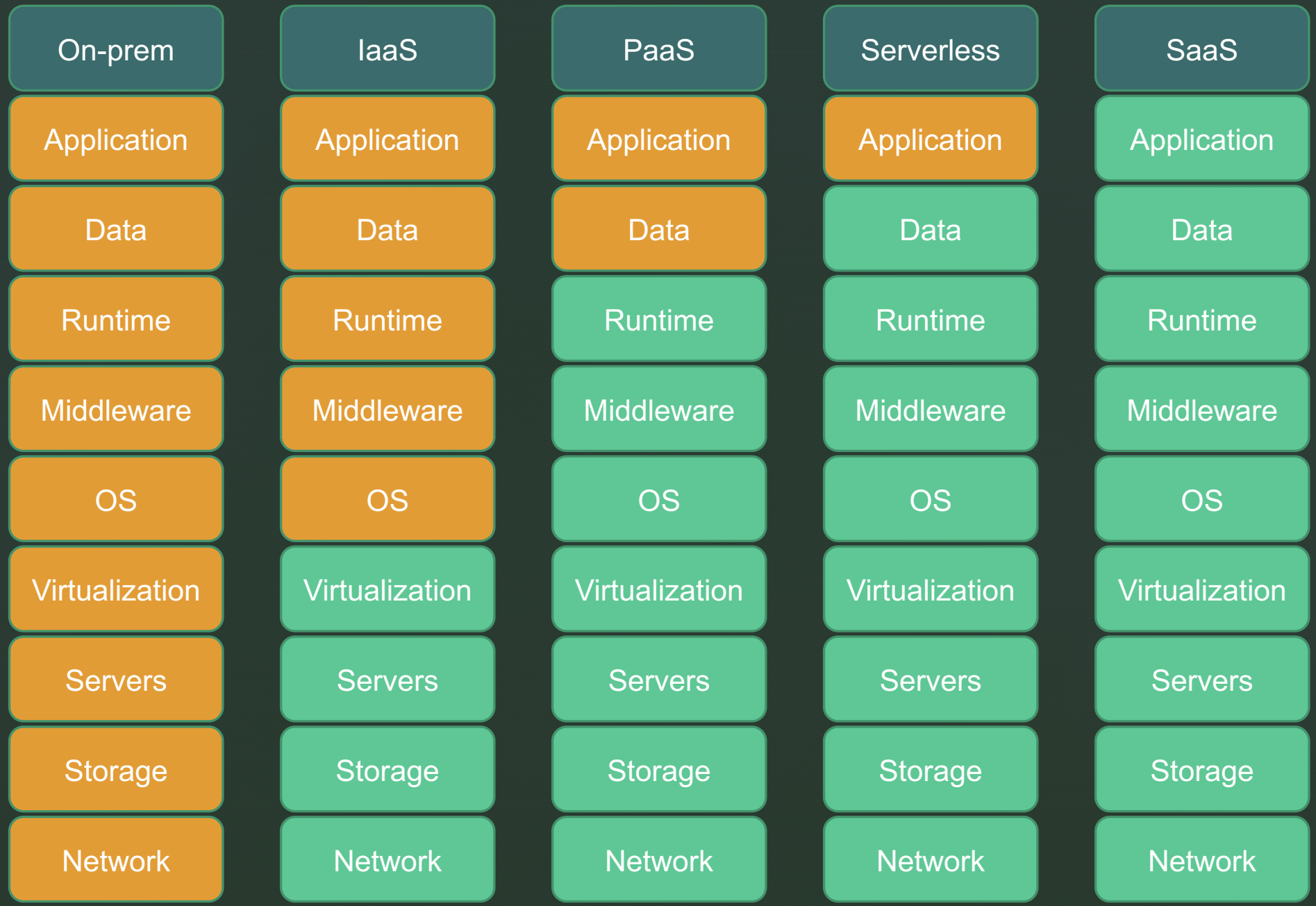
- Healthcare
- Banking
- Insurance
- Telecommunications
- Energy
- Agriculture
- Defence

WE STAND WITH
UKRAINE

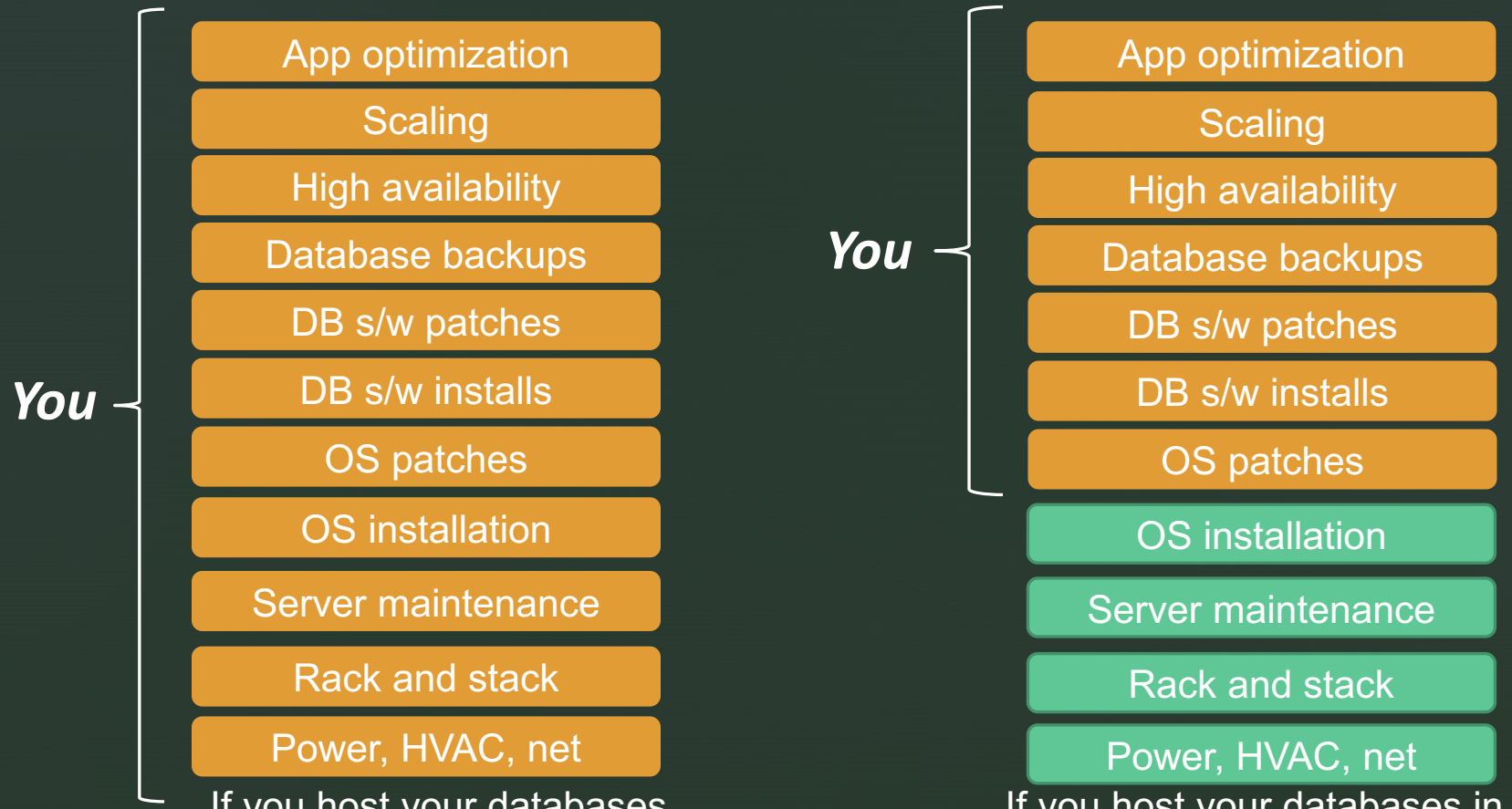
AWS Shared Responsibility Model



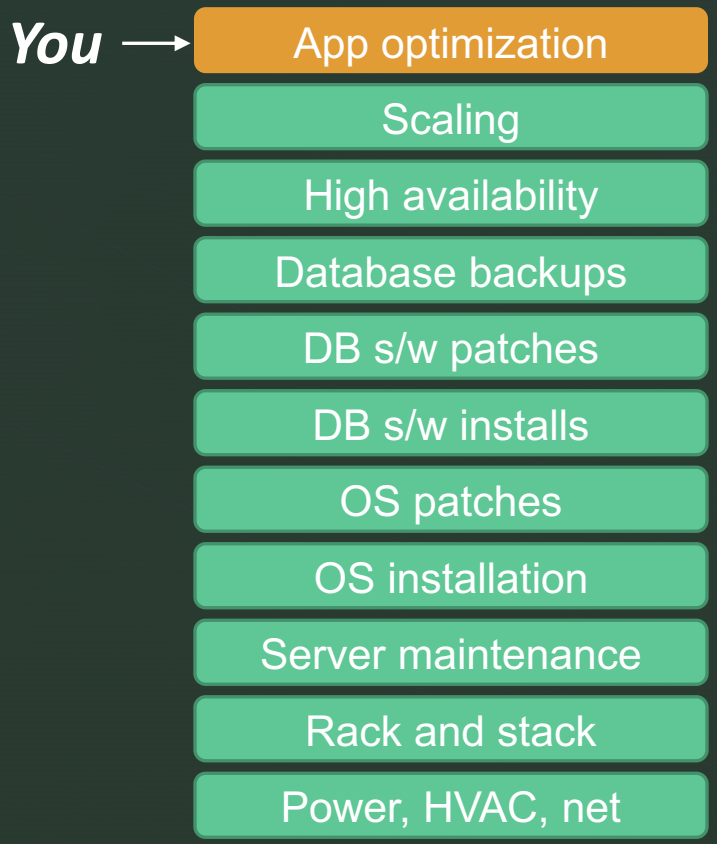
WE STAND WITH UKRAINE



Managed service – Relational database

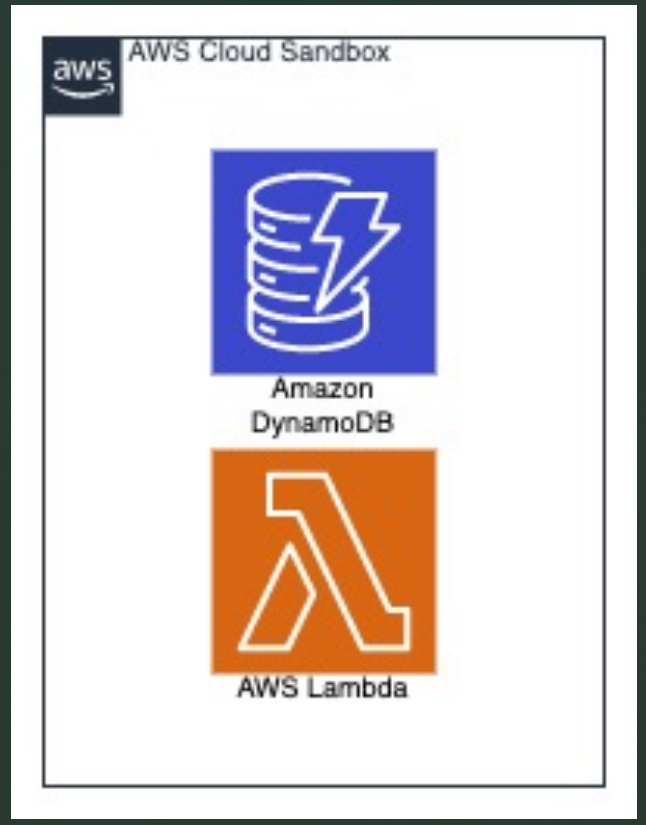


Managed service – Relational database

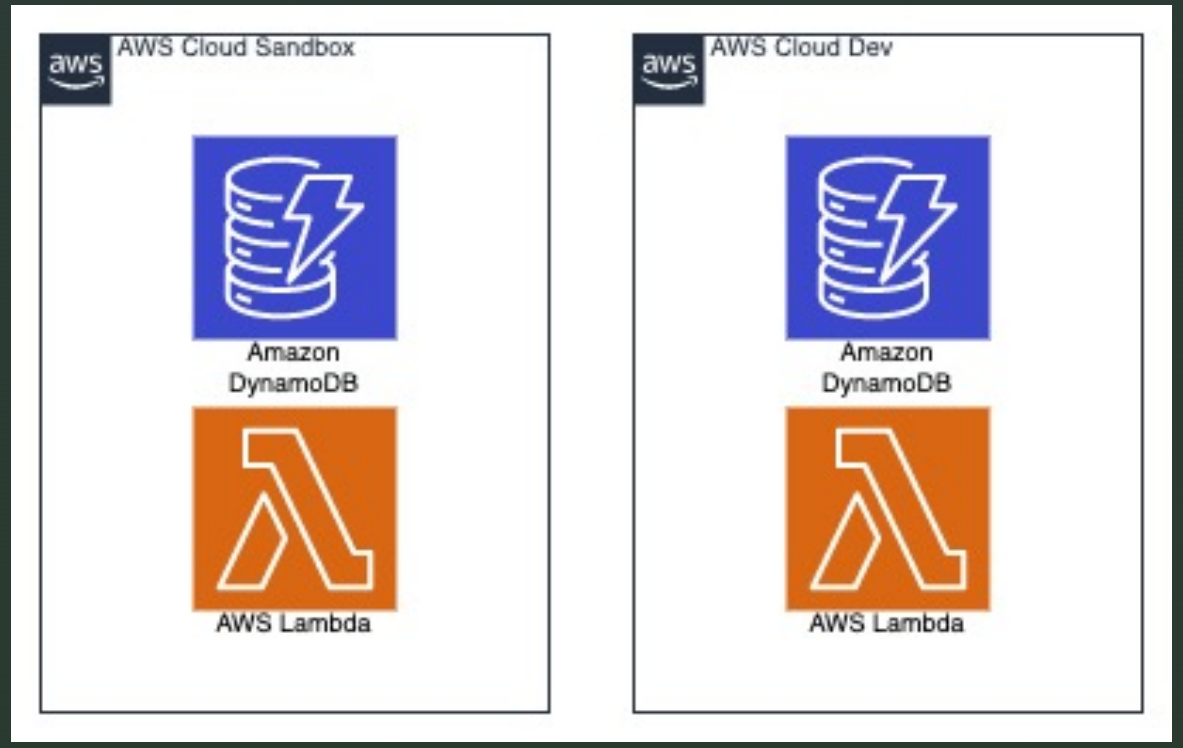


If you host your databases in
a managed database service

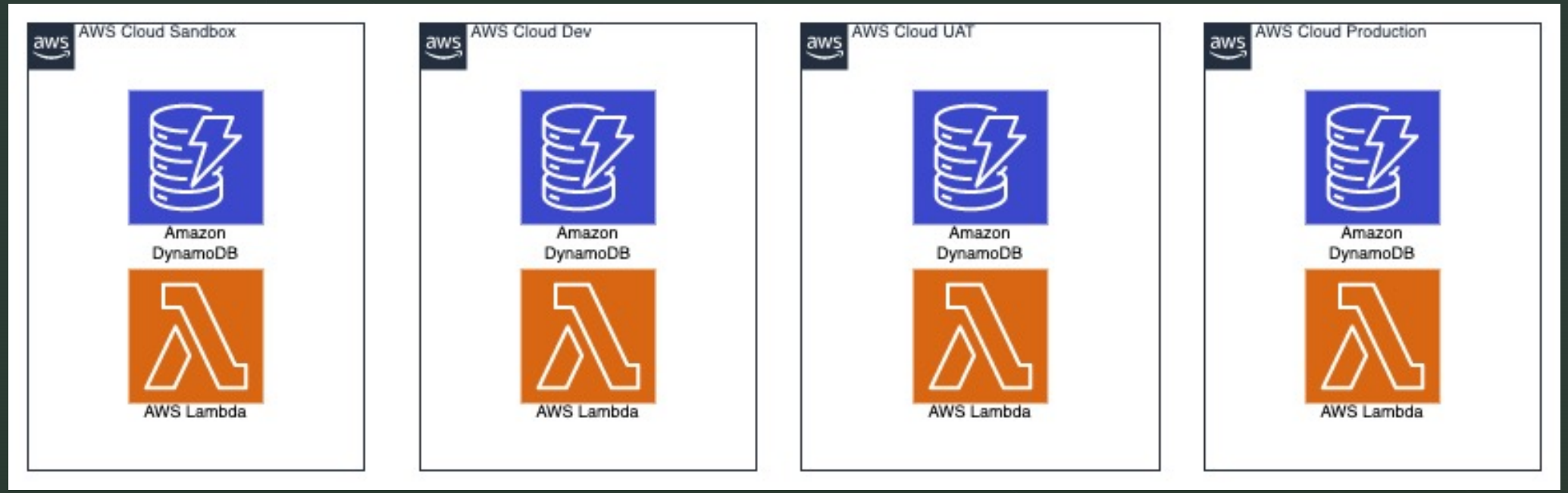
AWS account structure



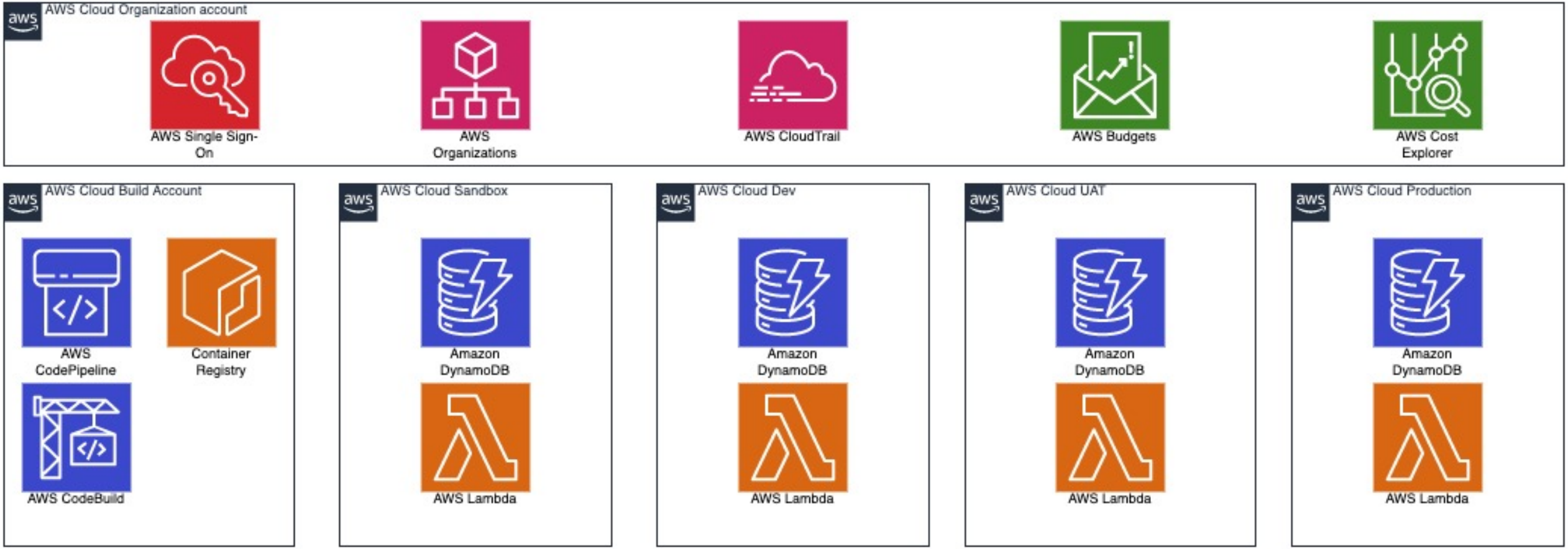
AWS account structure



AWS account structure



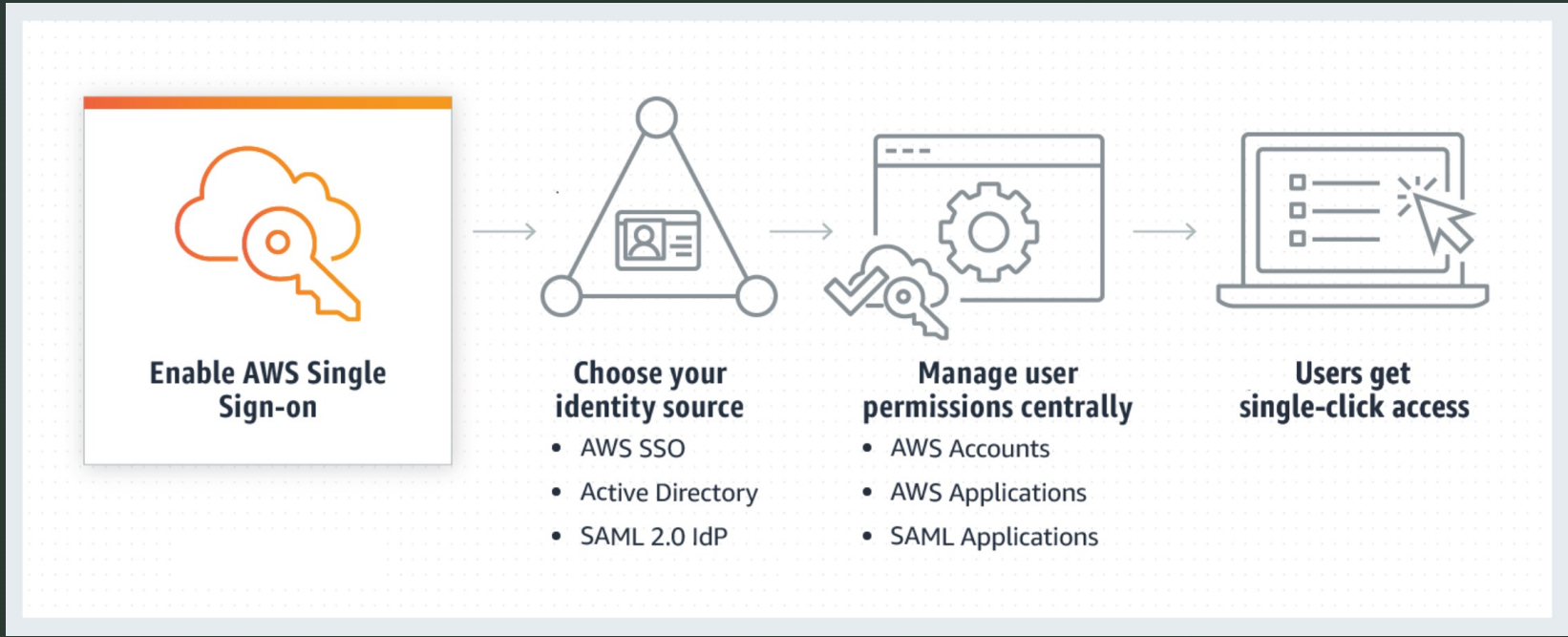
AWS account structure



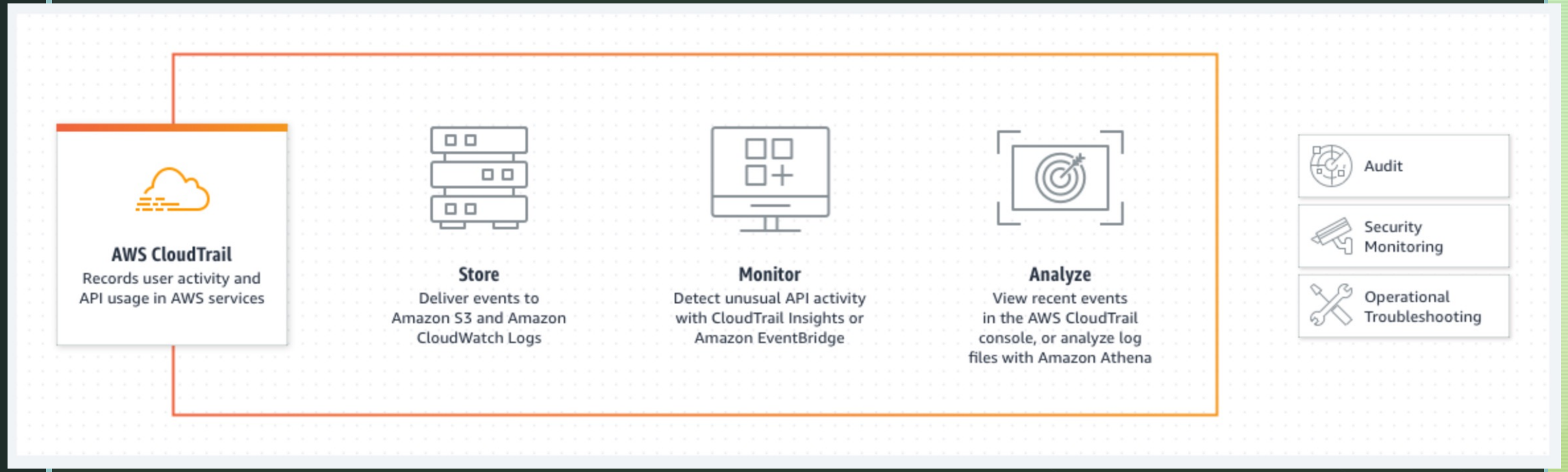
AWS service control policies (SCPs)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyDynamoDB",
            "Effect": "Deny",
            "Action": "dynamodb:*",
            "Resource": "*"
        }
    ]
}
```

AWS Single Sign-On



AWS CloudTrail



IAM Access Analyzer

WE STAND WITH
UKRAINE

AWS SecurityHub

AWS Foundational Security Best Practices v1.0.0

Overview

Last updated 2 hours ago

Security score

86%

119 of 139 controls passed

100 of 620 checks failed

16% failed

Enabled	Failed	Unknown	No data	Passed	Disabled
139	20	0	0	119	14

Enabled controls (139)

statuses and check counts updated 2 hours ago

Disable | Download

Filter enabled controls

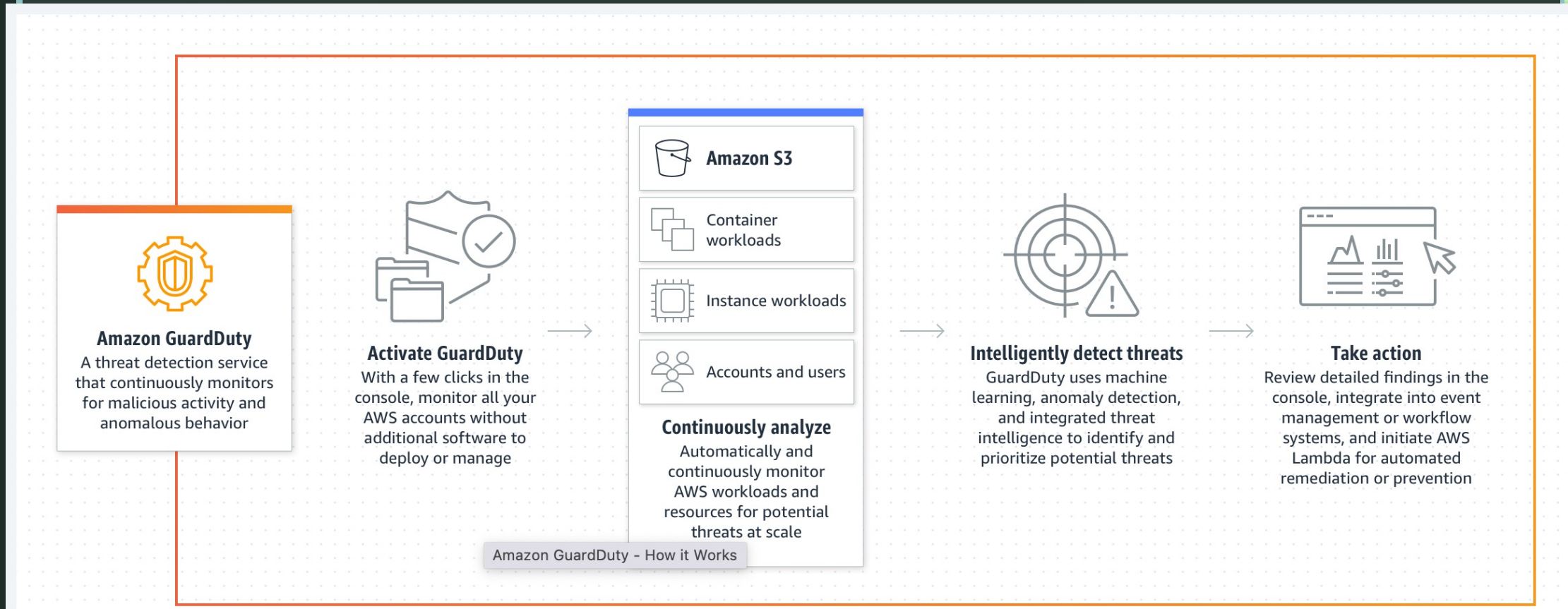
Compliance Status	Severity	ID	Title	Failed checks
Failed	Critical	EC2.19	Security groups should not allow unrestricted access to ports with high risk	1 of 20

AWS Config Conformance Packs

- Operational Best Practices for FedRAMP(Moderate)
- Operational Best Practices for FFIEC
- Operational Best Practices for HIPAA Security
- Operational Best Practices for K-ISMS
- Operational Best Practices for Load Balancing
- Operational Best Practices for Logging
- Operational Best Practices for Management and Governance Services
- Operational Best Practices for MAS Notice 655
- Operational Best Practices for MAS TRMG
- Operational Best Practices for Monitoring
- Operational Best Practices for NBC TRMG
- Operational Best Practices for NERC CIP
- Operational Best Practices for NCSC Cloud Security Principles
- Operational Best Practices for NCSC Cyber Assesment Framework
- Operational Best Practices for Networking and Content Delivery Services
- Operational Best Practices for NIST 800-53 rev 4
- Operational Best Practices for NIST 800-53 rev 5

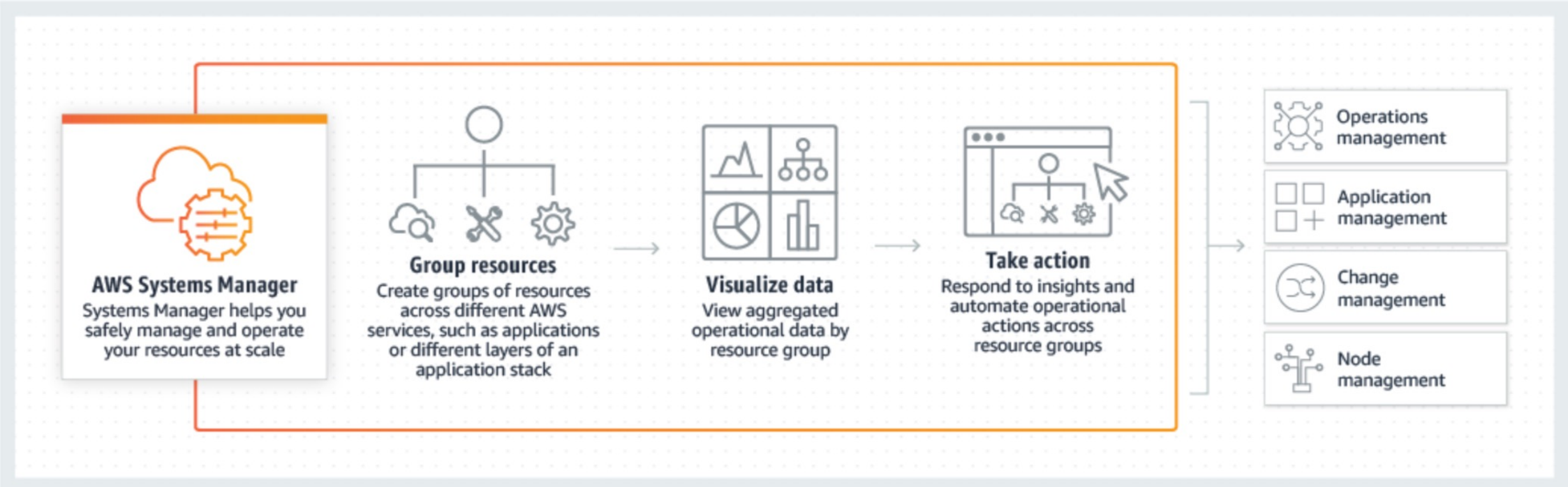
WE STAND WITH
UKRAINE

Amazon GuardDuty



WE STAND WITH
UKRAINE

AWS Systems Manager



Create Infrastructure - manual

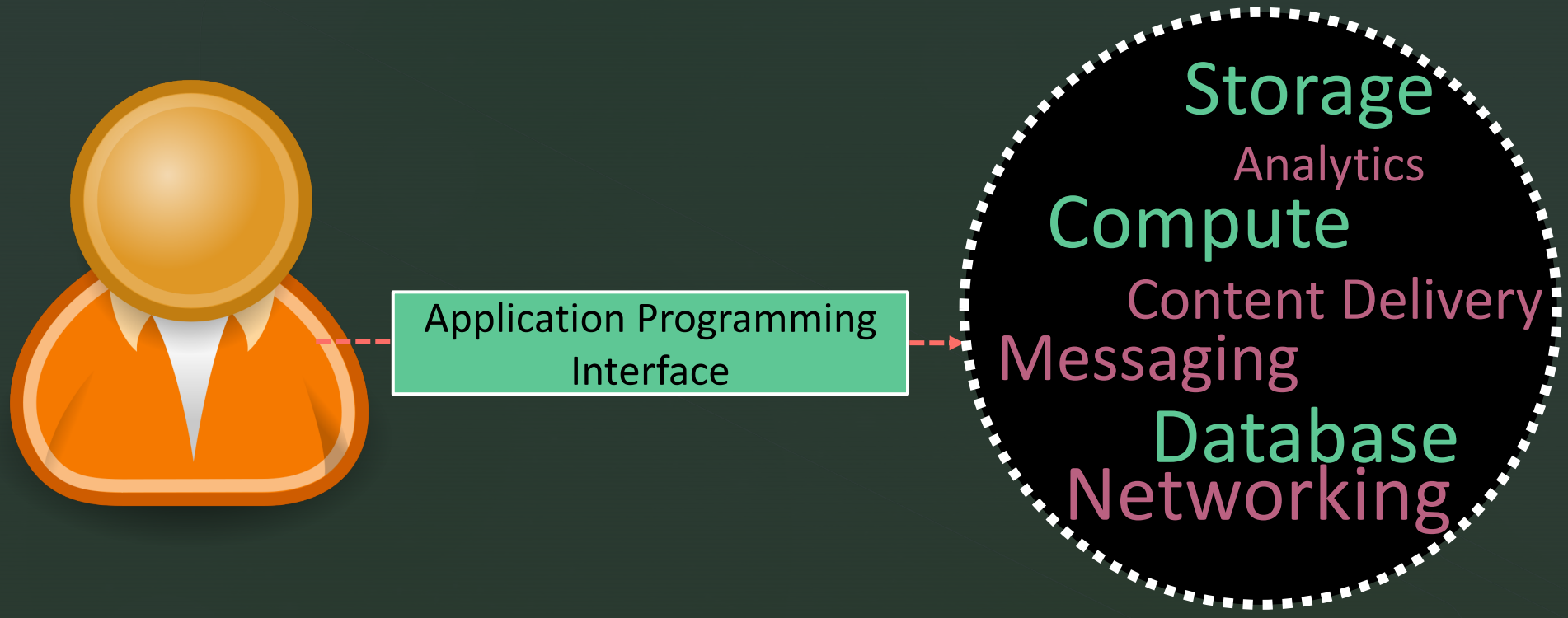
Storage
Analytics
Compute
Content Delivery
Messaging
Database
Networking

Create Infrastructure - API

Application Programming Interface

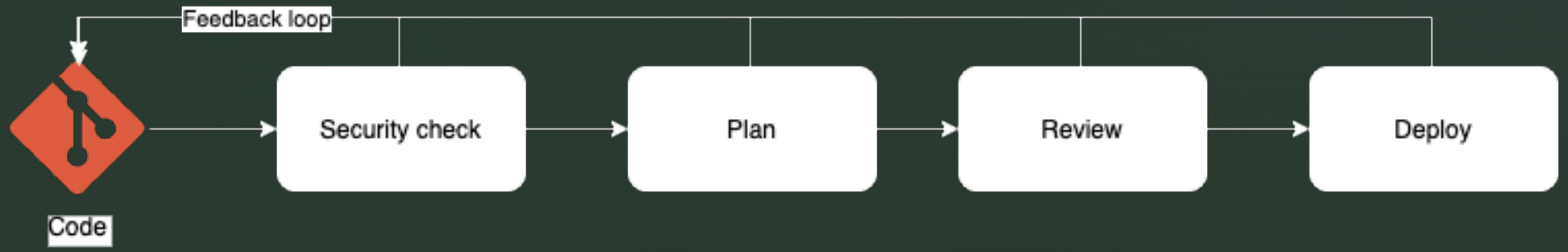
Storage
Analytics
Compute
Content Delivery
Messaging
Database
Networking

Create Infrastructure – Infrastructure as Code (IaC)



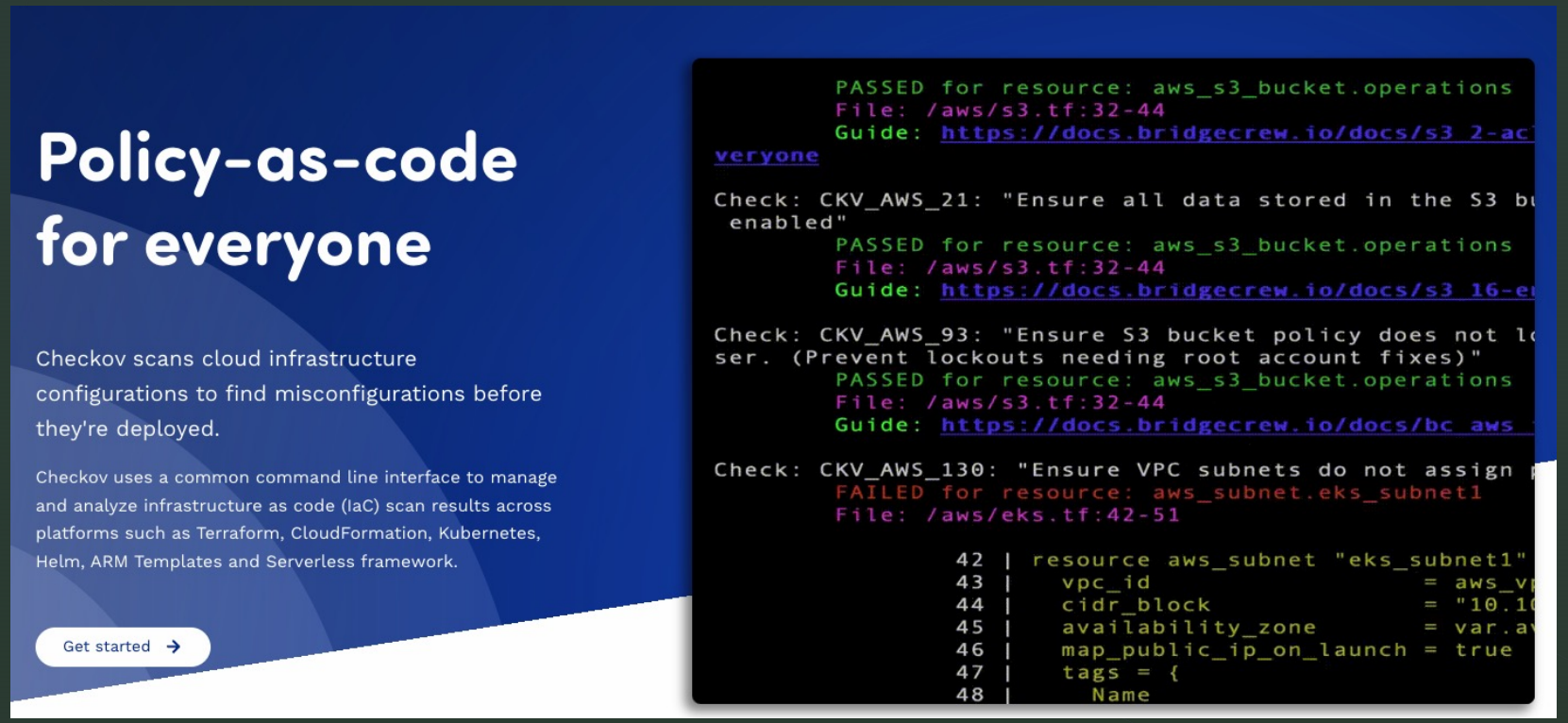
Infrastructure as code (IaC) benefits

- Secure
- Auditable and Traceable
- Repeatable and Consistent
- Documented
- Part of the CI/CD Process
- Cost-Efficient



WE STAND WITH
UKRAINE

Shift security left - Checkov



Security control matrix

HIPAA Regulatory Citation (45 C.F.R. § xxx.xxx)	Name	HIPAA Regulation Text	HIPAA Rule Category	AWS Commentary
§164.308(a)(5)(ii)(A)	Security Awareness and Training — Security Reminders	Periodic security updates.	Security Rule	The customer is responsible for implementing security reminders as a part of the customer's security awareness training procedures. As one illustrative example, the customer may, during a quarterly meeting, remind workforce members with access to ePHI to lock their workstations when away.
§164.308(a)(5)(ii)(B)	Security Awareness, Training, and Tools — Protection from Malicious Software	Procedures for guarding against, detecting, and reporting malicious software.	Security Rule	The customer is responsible for training its workforce members on procedures for guarding against malicious software. There are AWS partners that can help guard against, detecting, and reporting malicious software: https://aws.amazon.com/security/partner-solutions/#infrastructure
§164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools — Log-in Monitoring	Procedures for monitoring log-in attempts and reporting discrepancies.	Security Rule	The customer is responsible for training appropriate workforce members on how to monitor log-in attempts and identify discrepancies. As one illustrative example, the customer should train appropriate workforce members on how to use AWS CloudTrail to identify suspicious attempts to access AWS.
§164.308(a)(5)(ii)(D)	Security Awareness, Training, and Tools — Password Management	Procedures for creating, changing, and safeguarding passwords.	Security Rule	The customer, at its discretion, may choose to provide AWS user accounts and privileges to workforce members within the customer's AWS infrastructure. The customer is responsible for configuring the password policies to be enforced, and is responsible for all aspects of developing and managing mechanisms and procedures for creating, changing, and safeguarding passwords within its operating systems and applications. For more information, refer to: http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html http://docs.aws.amazon.com/IAM/latest/UserGuide/access.html http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.htm

WE STAND WITH UKRAINE

Data residency and soveregnity

WE STAND WITH UKRAINE

Reference architectures

Security, identity, and compliance

Learn how to meet your security and compliance goals using AWS infrastructure and services.

Identity and access management
Manage access to AWS services and resources.

Detection
Learn how to detect suspicious activity in your AWS account.

Infrastructure protection
Monitor and control your network infrastructure.

Data protection
Operate the security services that protect your data.

Compliance
Implement compliance controls with AWS.

Incident response
Learn how to automate incident response and recovery.

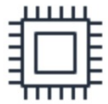
Analytics and big data

Build secure, reliable, cost-effective data-processing architectures.

Data lakes
Best practices for setting up and managing data lakes.

Data analytics
Analyze your data at scale on AWS.

Data management
Store and manage your data in the cloud.



Compute and HPC

Learn how to develop, deploy, run, and scale your applications.

Core compute
Deploying secure, reliable compute capacity.

High performance computing
Best practices for high performance computing.

EC2 Spot and Fleet
Guidance for running EC2 Spot instances and Spot Fleet.

Containers

Learn the most secure, reliable, and scalable way to

DevOps practices
Leverage containers to enable DevOps workflows.

Observability
Enable visibility and anomaly detection.

Container security
Best practices for securing your containers.

WE STAND WITH UKRAINE

AWS Compliance program

WE STAND WITH

UKRAINE

Customers in Regulated Industries

For security and compliance, customers choose AWS. To see more examples of customer success stories, visit our **Testimonials webpage**.

Nasdaq

"AWS allowed us to store information in a cost effective manner while alleviating the burden of supporting the necessary infrastructure since AWS takes care of that. It really is a win-win for us and our customers."

PHILIPS — Healthcare

robinhood — Financial Services

Berkeley UNIVERSITY OF CALIFORNIA — Education

CITY OF CHICAGO INCORPORATED 4TH MARCH 1837 — Government

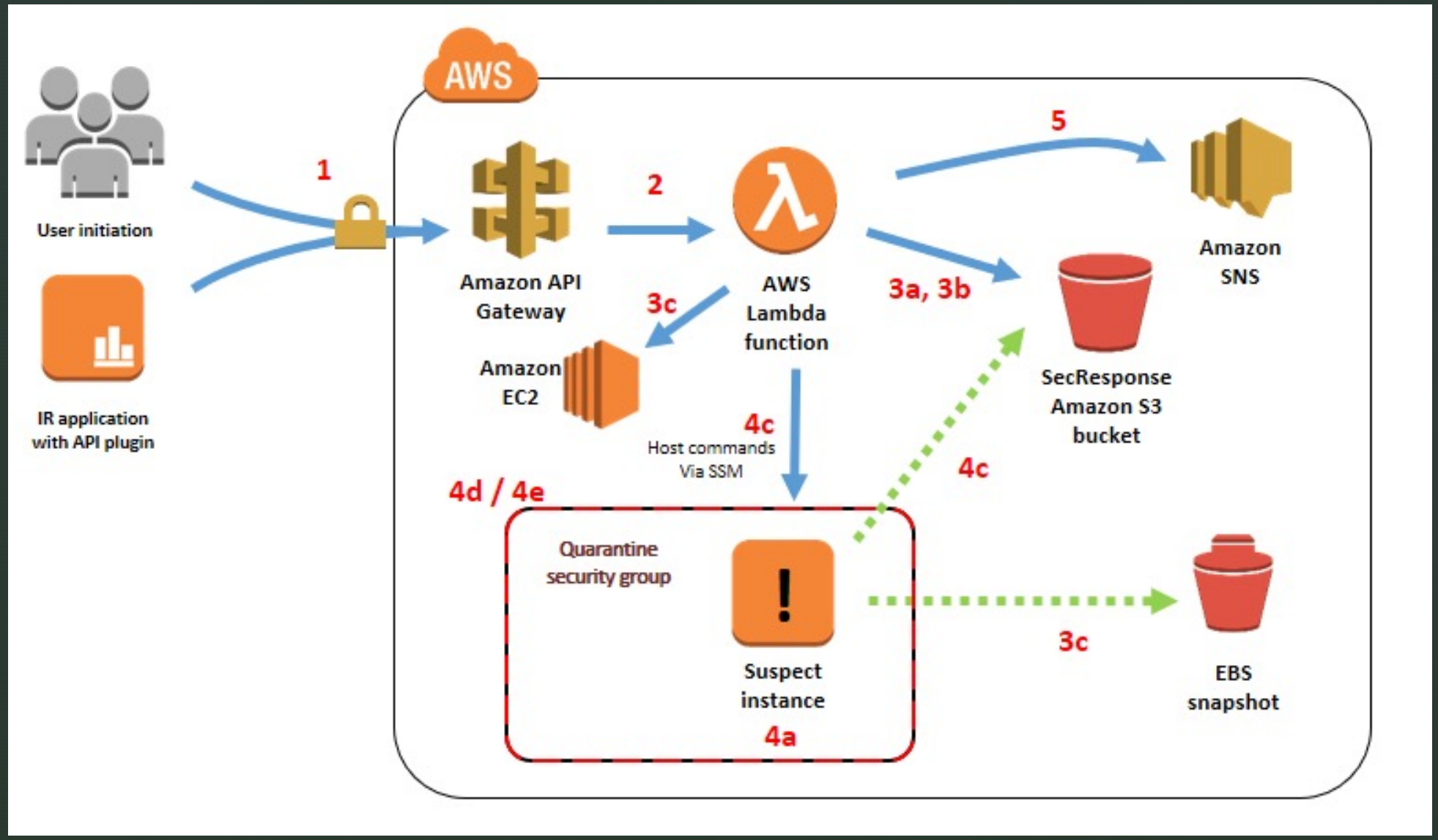
HESS — Energy

WE STAND WITH
UKRAINE

People

- Break the wall
- Work together
- We all want the same thing

Automated incident response

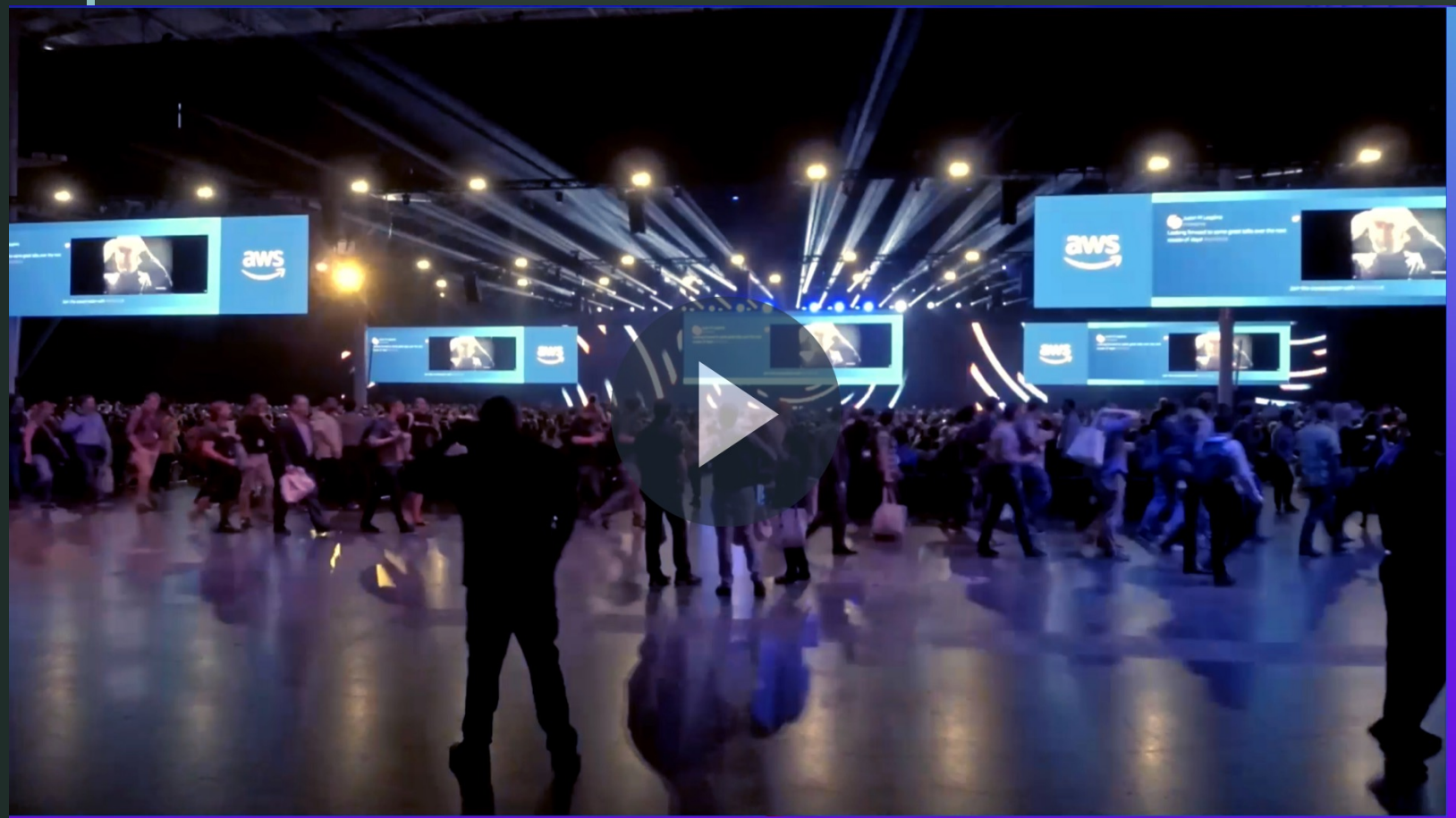


Recap

- Know AWS Shared Responsibility Model
- Use multi-account strategy
- Use managed services
- Enable Security Hub
- Use Infrastructure as Code (IaC)
- Work together

AWS re:Inforce

- https://reinforce.awsevents.com



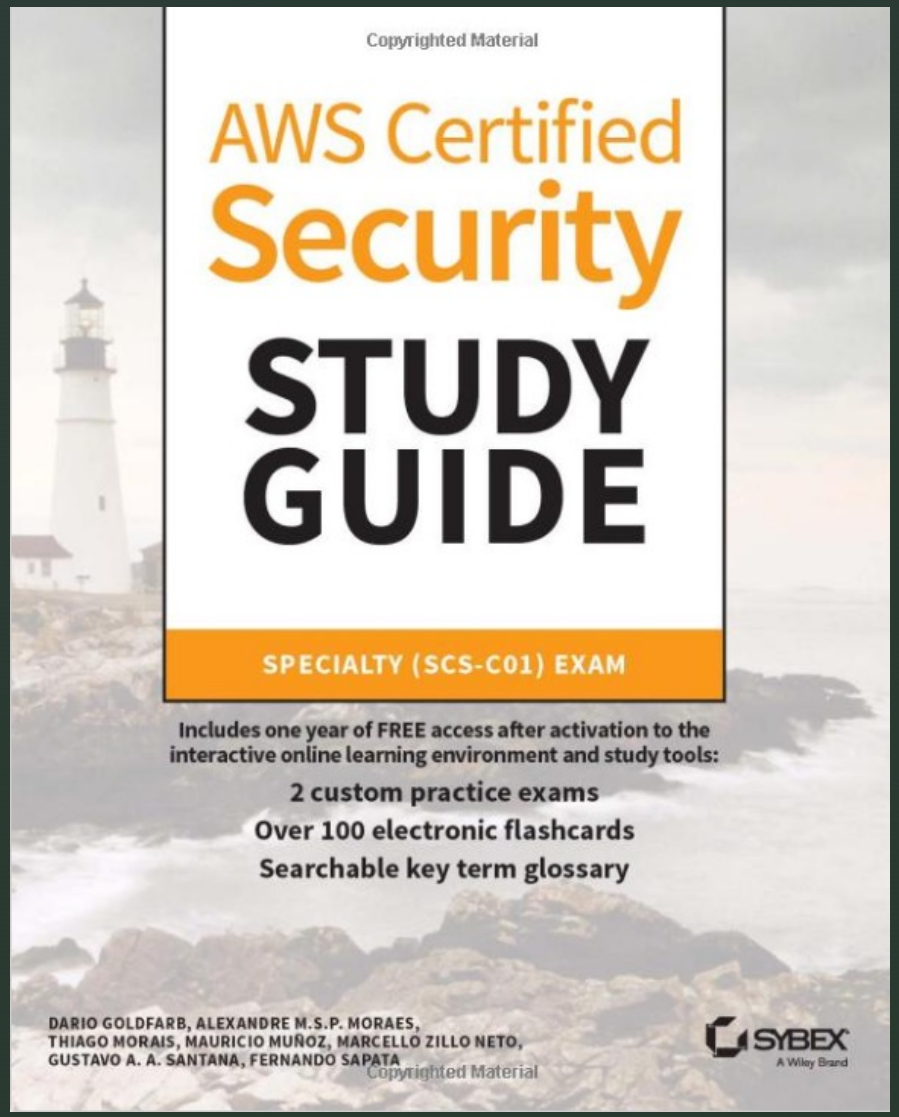
RE:INFORCE 2022

Because security is the **top priority**

Join us in summer 2022 for two days to reinforce your AWS security posture. Discover how AWS is innovating in the world of cloud security, and then hone your technical skills in expert-led interactive sessions. You'll hear the latest from industry-leading speakers in security, compliance, identity, and privacy and meet fellow security professionals at our fun events. Stay tuned for more updates and information about attending re:Inforce 2022.

WE STAND WITH
UKRAINE

Resources



WE STAND WITH
UKRAINE

Resources

- Infrastructure as Code
  - https://www.terraform.io/
  - https://aws.amazon.com/cdk/
  - https://aws.amazon.com/cloudformation/
- AWS Security resources
  - https://aws.amazon.com/security/
  - https://aws.amazon.com/compliance/
  - https://aws.amazon.com/blogs/security/
  - https://aws.amazon.com/podcasts/aws-podcast/
  - https://aws.amazon.com/certification/certified-security-specialty/

WE STAND WITH
UKRAINE

Resources

- AWS Security
  - https://aws.amazon.com/blogs/security/how-to-automate-incident-response-in-aws-cloud-for-ec2-instances/
  - https://aws.amazon.com/blogs/security/use-iam-access-analyzer-to-generate-iam-policies-based-on-access-activity-found-in-your-organization-trail/
  - https://reinforce.awsevents.com
- AWS Bulgaria User Group
  - https://www.meetup.com/AWS-Bulgaria/

WE STAND WITH
UKRAINE

Thank you

https://www.linkedin.com/in/danielrankov/

https://twitter.com/DanielRankov