secunet

Cloud Security & Strategy

Cybersecurity on Board! | 23.06.2023

Agenda

01 Why Cloud computing?

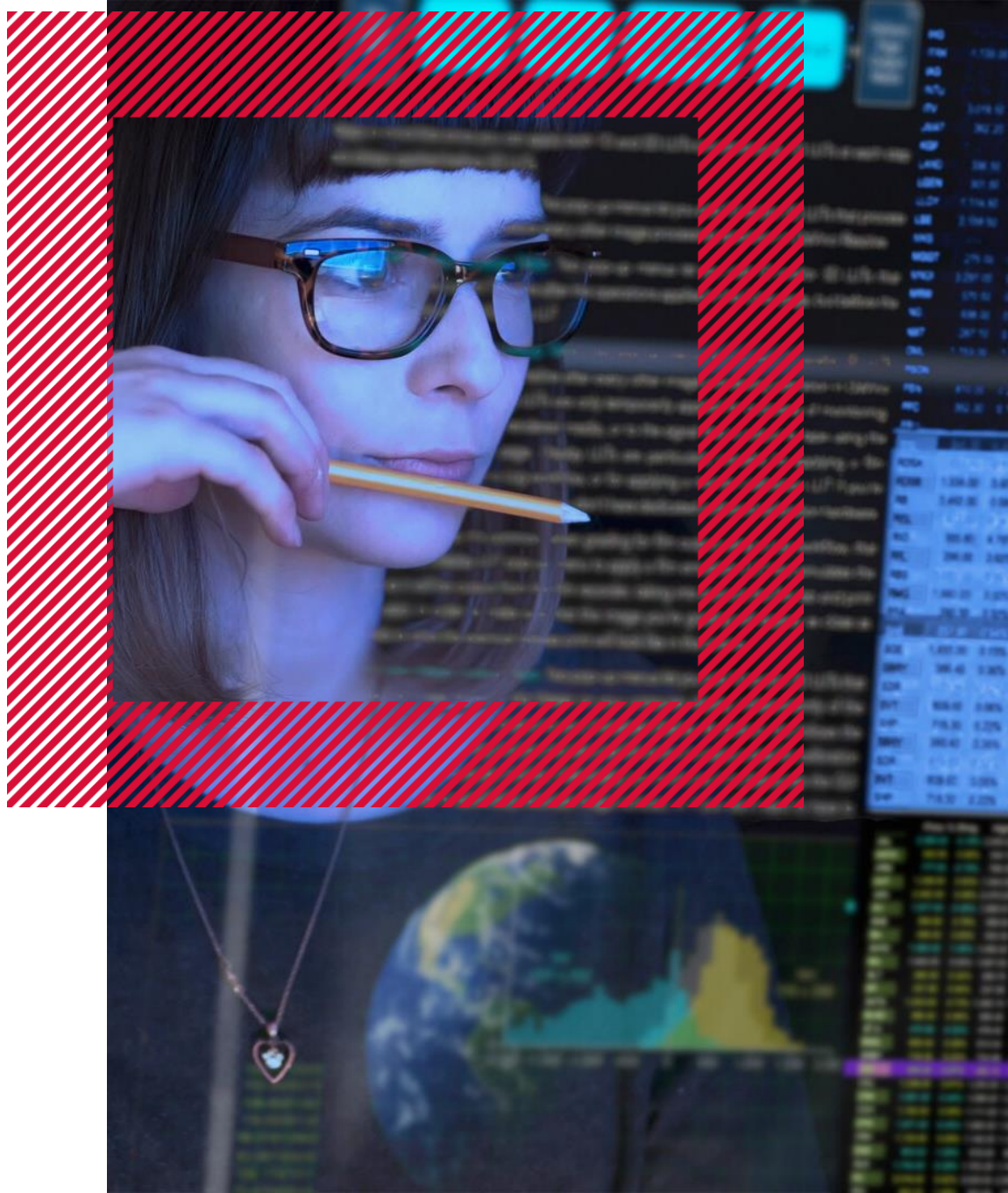
02 Key AWS security services

03 Threats & Mitigation

04 Q&A

01

Why Cloud computing?



Advantages and Opportunities

- Flexibility
- Time and location-independent collaboration
- Scalability
- Transparent monthly costs
- Automatic updates
- Availability

CLOUD COMPUTING

Deployment Models

Private Cloud

Community Cloud

Public Cloud

Hybrid Cloud

CLOUD COMPUTING

Cloud Strategy

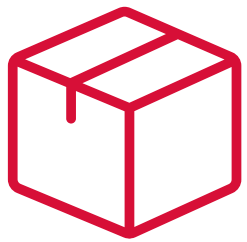
- Cloud-Only
- Cloud-First
- SaaS-First
- Private Cloud First

CLOUD
COMPUTING

02

Key AWS security services

AWS Identity and Access Management

WHO	CAN ACCESS	WHAT
		
Workforce users and workloads with IAM	Permissions with IAM policies	Resources within your AWS organization

Key AWS security services

IAM

WAF

Shield

KMS

03

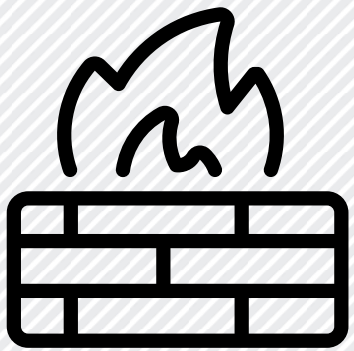
Threats & Mitigation

Threats

- Data breaches and violations
- Inadequate permission and identity management
- Insecure interfaces and APIs
- System vulnerabilities
- Account hijacking
- Malicious insiders
- Advanced Persistent Threats
- Data loss
- Insufficient auditing of the cloud service provider
- Abusive use of cloud services
- Denial of Service
- Vulnerabilities in shared resources
- Vendor Lock In / Out

Identity is the new perimeter

then



now

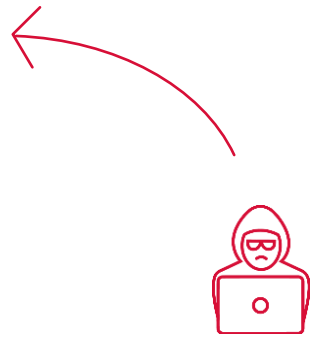
Securing the Identity Perimeter

- Implementation of strong password rules
- Use of Multi-factor Authentication (MFA)
- Allocation of permissions according to Least Privilege & Need to Know principles
- Separation of Cloud Administrators & local Administrators
- Separation of Users & Administrators

Attack vector: Theft of IAM Secrets

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

[user1]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
```



high risk

Possible solution: AWS Security Token Service (STS)


```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
aws_session_token=IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRING
EXAMPLE

[user1]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
aws_session_token=fcZib3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRING
EXAMPLE
```

Best Practices: Secrets Management

- Do not scatter
  (e.g., through Git repos, YAML / config files)
- Store and transmit encrypted
- Rotate automatically
- If possible, temporary
- Log & monitor usage
- Containers should hold them in RAM
  → not persistent
- Use PKI for TLS certificates

04

Q&A


secunet