Security Architecture

CompTIA Security+ certification exam, SY0-801 (V8)

19% of the exam · 4 exam objectives · SY0-801

Security Architecture (19% of the exam) covers how architecture models change security, how to arrange infrastructure and access to protect it, how to protect data in every state and role, and how resilience and recovery keep services running.

You should be able to: A company can accept losing 30 minutes of data and being down for 15 minutes. Which value is the RPO, which is the RTO, and what kind of recovery site does a 15 minute RTO call for?

Every exam objective: the key point and the trap

3.1 Compare and contrast security implications of different architecture models.

Cloud deployment models: public (any customer), private (one organization), community (a group with shared needs) and hybrid (a mix). Multicloud means using more than one provider; serverless leaves servers to the provider while the customer still secures code, data and permissions.

Trap: Treating multicloud and hybrid as the same thing. Hybrid mixes deployment models (such as private and public); multicloud uses more than one provider.

3.2 Given a scenario, manage the security architecture to best protect the infrastructure.

Infrastructure considerations: device placement follows security zones (for example a screened subnet for public servers), keep the attack surface small, and use diversity so one flaw does not affect every layer.

Trap: Choosing a control because the device or user is 'inside the network'. Zero Trust gives no trust for location, and a screened subnet is for public facing systems, not internal ones.

3.3 Summarize concepts and strategies used to protect data.

Data types: structured data fits a fixed schema (tables); unstructured data does not (email, documents, images). Data states: at rest (stored), in transit (moving), in use (being processed).

Trap: Mixing up hashing and encryption. Hashing cannot be reversed; encryption can be with the key. Also mixing owner and custodian: the owner decides, the custodian carries out.

3.4 Explain the importance of resilience and recovery in security architecture.

Sites: hot (ready with current data, fastest, costliest), warm (equipment ready, data to load), cold (space and power only, slowest). Environmental factors such as location and climate matter in choosing them.

Trap: Swapping RTO and RPO. RTO is about time down; RPO is about data lost, measured back from the failure.

Key terms

IaC: Infrastructure as Code

OT: Operational Technology

VPN: Virtual Private Network

SSE: Security Service Edge

gMSA: Group Managed Service Account

UPS: Uninterruptible Power Supply

RTO: Recovery Time Objective

RPO: Recovery Point Objective

MTTR: Mean Time to Repair

MTBF: Mean Time Between Failures

ExamDragon, examdragon.com/secplus. Independent exam preparation, not affiliated with or endorsed by CompTIA; written in our own words to the SY0-801 exam objectives. CompTIA and Security+ are trademarks of CompTIA, Inc.