COMPTIA SECURITY+ SY0-701 · WEEK 16

Final Review, Exam Strategy, and the Project Briefing



Objectives 1.0 to 5.0 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Review the key concepts and common exam traps in each of the five SY0-701 domains.
2. Plan remaining study time in proportion to the domain weights and your own weak spots.
3. Apply a time plan for performance-based and multiple-choice questions on exam day.
4. Use keywords such as BEST, FIRST, and MOST to choose between plausible answers.
5. Translate technical findings into business risk, cost, and decisions for leaders.
6. Prepare and deliver a 10-minute briefing on the Lakeside Family Clinic project.

AGENDA

3 min	How to use the final review
8 min	Domain 1: General security concepts
12 min	Domain 2: Threats, vulnerabilities, mitigations
10 min	Domain 3: Security architecture
15 min	Domain 4: Security operations
11 min	Domain 5: Program management and oversight
12 min	Exercise: mixed scenarios
8 min	Exam-day strategy
9 min	Briefing non-technical leaders
2 min	Wrap-up

Study in proportion to the exam weights

12%	22%	18%	28%	20%
1.0 General concepts	2.0 Threats, mitigations	3.0 Security architecture	4.0 Security operations	5.0 Program management

Domains 4 and 2 are half the exam. On a 90-question exam, 28% is about 25 operations questions.

Domain 1 traps: controls, zero trust, crypto

Trap	Remember
Deterrent vs preventive	Deterrent discourages; preventive actually stops
Hashing vs encryption	Hashing is one-way; encryption is reversible
Signing vs encrypting	Sign: your private key. Encrypt: their public key
Zero trust planes	Control plane decides; data plane enforces
Backout plan	How to undo a change that fails
Salting	Random value so equal passwords hash differently

Domain 2 traps: actors, attacks, indicators

Trap	Remember
Spraying vs brute force	Spraying tries one password on many accounts
Impossible travel	Logins too far apart in too little time
Race condition	TOC/TOU: state changes between check and use
XSS vs request forgery	XSS runs script; forgery sends requests as user
Vishing, smishing	Voice call phishing and SMS text phishing
Unpatchable system	Segment, isolate, and monitor it

Domain 3: design for failure, protect the data

Resilience and design

- Fail-closed blocks traffic when a device fails
- Inline IPS can block; a tap or monitor only sees
- Hot site ready now; warm partial; cold space only
- Load balancing shares load; clustering fails over
- Replication copies mistakes too; it is not a backup

Data protection

- States: at rest, in transit, in use
- Tokenization swaps data for a token in a vault
- Masking hides part of a value, such as ****1234
- Sovereignty: data follows the laws where it lives
- Cloud responsibility matrix splits the duties

Domain 4 is the biggest: know these cold

Topic	Remember
SPF, DKIM, DMARC	Allowed senders, a signature, then the policy
SAML vs OAuth	SAML handles sign-in; OAuth delegates access
False positive	Flags something harmless; tune the rule
MAC, DAC, RBAC, ABAC	Labels, owner's choice, job role, attributes
IR order	Contain before eradicating; RAM before disk
Sanitize vs destroy	Wipe to reuse; destroy when media is retired

Domain 5: governance, risk, and compliance

Topic	Remember
Policy vs standard	Policy: broad intent. Standard: specific rule
SLE and ALE	SLE = value x EF; ALE = SLE x ARO
Transfer	Insurance moves cost, not accountability
Controller vs processor	Controller decides; processor follows orders
MOU vs MOA	MOU: shared intent. MOA: specific duties
Unknown environment	Testers start with no information

One scenario from every domain



12

MINUTES · SMALL GROUPS

Answer each scenario, name its domain, and say which word in the question decided your answer.

1. A login banner warns that use is monitored. Control type?
2. 400 accounts, one failed login each, same password. Attack?
3. A firewall must block all traffic if it fails. Failure mode?
4. Which log shows who logged on to a Windows server last night?
5. A vendor offers its SOC 2 Type II report as proof. Audit type?
6. Asset $40,000, EF 50%, ARO 2. What is the ALE?
7. The EHR must be back within 4 hours. RTO or RPO?
8. Which record lists the servers allowed to send a domain's email?
9. Ransomware is confirmed on one PC. What happens first?
10. One legacy device cannot be encrypted. What is the response?

Plan your 90 minutes before you sit down

1
Survey
See whether PBQs open the exam; flag long ones

2
Answer MCQs
Work multiple choice at about a minute each

3
Flag and move
Stuck after a minute? Best guess, flag, go on

4
Return to PBQs
Spend the banked time on flagged simulations

5
Review flags
Change an answer only for a clear reason

6
Answer all
A blank scores zero; never leave one empty

Speak in risk, cost, and decisions

Technical report says

- CVSS 9.8 flaw on the VPN appliance
- No MFA on remote desktop; 4625 bursts in logs
- Flat network with no segmentation
- Deploy EDR with 24x7 managed monitoring

Leadership briefing says

- A known flaw lets outsiders into our network
- A stolen password alone opens patient records
- One infected PC can reach every system we run
- Tools that spot and stop attacks, about $8,000 a year

REVIEW

Five questions: write your answers first

1. Which two domains together make up half of the SY0-701 exam?
2. To send a confidential message to Dana, which key encrypts it?
3. What is the difference between hot, warm, and cold sites?
4. What should you do when a long PBQ appears at the start of the exam?
5. How should the finding "no MFA on remote access" be stated to clinic leaders?

TAKEAWAYS

Four things to take with you

01

Study by weight and weakness

Domains 4 and 2 are half the exam; your weakest domain comes next.

02

Read for the keyword

BEST, FIRST, and MOST decide between plausible answers.

03

Bank time for PBQs

Flag long ones, answer the rest, return, and never leave a blank.

04

Brief in business terms

Lead with the bottom line, the cost, and the decision you need.

NEXT Lab 16: Final briefing to Lakeside Family Clinic leadership