🟦 1. General Security Concepts (12%)

🔹 Security Controls

Types (easy memory trick: "P D M D O D C C T")

Type	Meaning	Example	Problem	Solution
Preventive	Stops attacks	MFA, firewall	Weak passwords	Enforce password policy
Detective	Finds attacks	IDS, SIEM alerts	Unknown intrusion	Configure SIEM rules
Corrective	Fixes damage	Backups, patches	Ransomware hit	Restore + patch
Deterrent	Discourages attackers	CCTV, warning banners	Insider curiosity	Monitoring warning
Directive	Tells what to do	Policies, SOPs	Confusion in steps	Provide clearer SOP
Technical	Tech-based	Encryption	Data stolen	Encrypt endpoints
Operational	Day-to-day actions	Log reviews	Missed alert	Daily log checklist
Managerial	Governance	Risk assessments	No risk visibility	Regular audits
Compensating	Backup control when main fails	Guards instead of MFA	Legacy system no MFA	Add CCTV + logging
Physical	Tangible protection	Locks, gates	Tailgating	Install turnstiles

---

🔹 CIA + AAA + Zero Trust

CIA

- **Confidentiality** – Only authorized access
  Problem: Data leak → *Solution:* Encryption + ACL
- **Integrity** – No unauthorized modification
  Problem: Tampered logs → *Solution:* Hashing, checksums
- **Availability** – Systems stay online
  Problem: DDoS → *Solution:* Load balancers, redundancy

AAA

- **Authentication** – Who are you? (Password, MFA)
- **Authorization** – What can you do? (RBAC)
- **Accounting** – What did you do? (Logs)

Zero Trust

"**Never trust, always verify**."
Example: MFA everywhere, micro segmentation.

Deception/Disruption

- **Honeypots** to trap attackers
- **Honeytokens** fake credentials to track intruders

🔹 Change Management

Business Processes → Technical impact → Documentation → Version control

Example:

- Problem: Admin pushes config → outage
- Solution: Change request → Approval → Test → Deploy → Document

---

🔹 Crypto Basics

Term	Meaning	Example
PKI	Certificates	HTTPS
Encryption	Protect info	AES-256
Hashing	One-way	SHA-256
Digital signature	Integrity + Non-repudiation	Signed emails
Obfuscation	Hide logic	Encoding JS
Blockchain	Immutable ledger	Cryptocurrency

Problem: Password stolen
Solution: Hash + salt + MFA

🟥 2. Threats, Vulnerabilities, Mitigations (22%)

🔹 Threat Actors

Actor	Motivation	Example
Nation-state	Espionage	APT29
Hacktivists	Political message	Anonymous
Insider	Sabotage/data theft	Angry employee
Organized crime	Money	Ransomware gangs
Script kiddies	Fun/no skill	Running Metasploit
Shadow IT	Unapproved systems	Hidden servers

Problem: Insider using USB drive
Solution: DLP + disable USB ports

🔹 Threat Vectors

- Message-based → Phishing
- Social engineering → Vishing, smishing
- File-based → Malicious PDF
- Network → Open ports
- Supply chain → Compromised vendor

Solution: Training + hardening + patching

🔹 Vulnerabilities

- Software flaws → buffer overflow
- Cloud misconfig → open S3 bucket
- Mobile → unpatched OS
- Web → XSS, SQLi
- Hardware → side-channel attacks
- Supply chain → tampered firmware

🔹 Malicious Activity

Examples + Solutions:

- **Password attacks** → brute-force → *MFA, lockouts*
- **Network attacks** → MITM → *TLS, ARP inspection*
- **Physical attacks** → tailgating → *badge readers*
- **Cryptographic attacks** → downgrade attacks → *force TLS 1.3*

🔹 Mitigation Techniques

- **Segmentation** → block lateral movement
- **Hardening** → disable unused services
- **Access control** → RBAC, ACL
- **Patch management** → monthly updates
- **Isolation** → sandbox suspicious files

🟩 3. Security Architecture (18%)

🔹 Architecture Models

Model	Example	Problem	Solution
On-prem	Local servers	Hardware failure	HA servers
Cloud	AWS/Azure	Misconfig	IAM policies
Virtualization	Hypervisors	VM escape	Patch hypervisor
IoT	Sensors	Weak passwords	Change defaults
ICS	Power plants	0 patch tolerance	Network isolation
IaC	Terraform	Bad code changes	Code reviews

🔹 Enterprise Infrastructure

- Secure communication → VPN, TLS
- Secure access → ACL, MFA
- Control selection → based on risk

🔹 Data Protection

- Data at rest → AES
- Data in motion → TLS
- Data types → PII, PHI, PCI
- Data classification → Public, Internal, Confidential

🔹 Resilience

- High availability → Failover clusters
- Backup types → Full, incremental, differential
- Site considerations → Hot, warm, cold site
- Continuity → DRP, BCP
- Testing → Tabletop, simulations

🟧 4. Security Operations (28%)

🔹 Computing

- Secure baseline → CIS benchmarks
- Hardening → Disable SMBv1, remove bloatware
- Sandboxing → Analyze malware safely
- Wireless security → WPA3, disable WPS

🔹 Asset Management

- Keep inventory of hardware/software
- Decommission properly → wipe/sanitize
- Track data assets → classification

Example:

- Problem: Rogue device found

- Solution: NAC block + asset inventory check

🔹 **Vulnerability Management**

1. Identify → Scan
2. Analyze → CVE/CVSS
3. Remediate → Patch
4. Validate → Rescan
5. Report → to management

🔹 **Alerting & Monitoring**

Tools:

- SIEM (Splunk)
- EDR/XDR
- IDS/IPS
- Firewall logs

Problem: Alert fatigue
Solution: Tuning + baselines

🔹 **Identity & Access**

- Provisioning → create users
- De-provisioning → remove users fast
- MFA
- SSO
- PAM → password vaulting

🔹 **Automation & Orchestration**

- Scripts → reduce human error
- SOAR → auto-response
- Benefits → speed, consistency

🔹 **Incident Response**

Steps:

1. **Preparation**
2. **Detection**
3. **Containment**
4. **Eradication**
5. **Recovery**
6. **Lessons learned**

Example:

- Ransomware → isolate → restore → root cause analysis

🔹 **Data Sources**

- Logs: system, firewall, DNS, EDR
- PCAPs
- Threat intel feeds

🟧 **5. Security Program Management (20%)**

🔹 **Security Governance**

- Policies → high-level

- Standards → mandatory
- Procedures → step-by-step
- Guidelines → optional

🔹 **Risk Management**

- Identify → asset list
- Assess → likelihood × impact
- Mitigate → controls
- Accept → low risks
- Transfer → insurance
- Avoid → stop activity
- BIA → what happens if system dies?

Example:

- RTO/RPO → recovery objectives

🔹 **Third-Party Risk**

- Vendor assessment
- SLA, MSA
- Continuous monitoring
- Supply chain security

🔹 **Compliance**

- GDPR, HIPAA, PCI-DSS
- Fines if violated

- Audits check compliance

🔹 **Audits & Assessments**

- Internal audit
- External audit
- Pen testing

🔹 **Security Awareness**

- Phishing simulations
- User training
- Learning suspicious behaviour
- Reporting channels