# **🔐 CompTIA Security+ SY0-701 Çalışma Rehberi**

## **📊 1. Sınavda En Sık Sorulan Konu Başlıkları (Top 10)**

|  |  |  |
| --- | --- | --- |
| **#** | **Konu Başlığı** | **Açıklama** |
| 1 | **Social Engineering Saldırıları** | Phishing, Smishing, Vishing, Impersonation |
| 2 | **Authentication & Authorization** | MFA, SSO, Role-Based Access Control |
| 3 | **Network Security** | Firewall ACL, VPN, Jump Server, Segmentation |
| 4 | **Cryptography & PKI** | Salting, Key Stretching, OCSP, FDE, Encryption at Rest |
| 5 | **Risk Management** | Risk Transfer, Risk Register, ARO, Legal Hold |
| 6 | **Security Controls** | Preventive, Detective, Compensating, Corrective |
| 7 | **Threat Actors & Attack Types** | Nation-State, Insider, Ransomware, Buffer Overflow |
| 8 | **Incident Response** | Root Cause Analysis, Chain of Custody, Threat Hunting |
| 9 | **Cloud & Virtualization** | SaaS/IaaS, Shared Responsibility Model, Isolation |
| 10 | **Security Tools & Techniques** | SIEM, DLP, IDS/IPS, Honeypot, Code Signing |

## **📌 2. Dikkat Edilmesi Gereken Anahtar Terimler ve Soru Kalıpları**

|  |  |
| --- | --- |
| **Anahtar Kelime** | **Açıklama** |
| **Salting** | Şifre hash'lerine rastgele veri ekleyerek brute-force saldırılarına karşı dayanıklılık sağlar. |
| **Smishing** | SMS üzerinden gelen phishing saldırısı. |
| **MFA (Multifactor Auth)** | Birden fazla doğrulama faktörü (şifre + parmak izi gibi). |
| **Jump Server** | Yönetim için izole edilmiş geçiş sunucusu. |
| **SIEM** | Log toplama, korelasyon ve alarm üretme aracı. |
| **Bug Bounty** | Güvenlik açıklarını bulan araştırmacılara ödül verilen program. |
| **Chain of Custody** | Dijital delilin güvenliğini sağlamak için tutulan kayıt zinciri. |
| **Geolocation Policy** | Ülkeye göre erişim engelleme. |

## **🔎 3. Konulara Göre Derinlemesine Analiz**

### **🧠 Social Engineering**

* **Saldırı Türleri:** Phishing, Vishing, Smishing, Impersonation
* **Örnek Soru:** CEO’nun adını kullanarak hediye kartı isteyen mesaj → **Smishing + Impersonation**
* **Savunma:** Güvenlik farkındalığı eğitimi, MFA

### **🔐 Authentication & Authorization**

* **Kavramlar:** SSO, MFA, RBAC, Least Privilege
* **Örnek Soru:** Tek kimlik doğrulama ile SaaS erişimi → **SSO**
* **Savunma:** MFA, Federated Identity, Role Tabanlı Yetkilendirme

### **🌐 Network Security**

* **Araçlar:** ACL, Jump Server, VPN, Bastion Host, Firewall Rules
* **Örnek Soru:** DNS sadece bir IP’den çıksın → ACL’de sadece 10.50.10.25 izinli olur
* **Savunma:** Firewall segmentasyonu, deny all varsayılan kuralı

### **🔏 Cryptography**

* **Teknikler:** Salting, Key Stretching, Full Disk Encryption (FDE), OCSP
* **Örnek Soru:** Tek yönlü dönüşüm öncesi karmaşıklaştırma → **Salting**
* **Araçlar:** TPM, Key Escrow, Code Signing

### **📋 Risk Management & Compliance**

* **Belgeler:** SLA, SOW, Risk Register, Legal Hold
* **Örnek Soru:** Siber sigorta ile riskin taşınması → **Risk Transfer**
* **Standartlar:** PCI-DSS, HIPAA, GDPR

### **🛠️ Security Controls**

* **Kontrol Türleri:** Preventive (DLP), Detective (SIEM), Corrective, Compensating
* **Örnek Soru:** SIEM haftalık log kontrolü → **Detective Control**
* **Diğer:** ACL → Preventive, Tabletop Exercise → Improvement

### **🧪 Incident Response & Forensics**

* **Aşamalar:** Preparation, Detection, Analysis, Containment, Recovery, Lessons Learned
* **Örnek Soru:** Bir saldırının kaynağını belirleme → **Analysis**
* **Araçlar:** Chain of Custody, Legal Hold, Forensic Toolkit

### **☁️ Cloud Security & Virtualization**

* **Kavramlar:** Shared Responsibility, Encryption at Rest, Segmentation
* **Örnek Soru:** IaaS ortamında veritabanı güvenliği → **Client sorumluluğundadır**
* **Önlemler:** VPN, DLP, IAM

### **🧰 Security Tools & Techniques**

* **Araçlar:** SIEM, DLP, IDS/IPS, Honeypot, Network Scanner
* **Örnek Soru:** Erişim dışı bırakmadan saldırgan davranışı tespiti → **Honeypot**
* **Koruma:** Application Allow Listing, Endpoint Protection

## **🚩 4. Kafa Karıştıran Noktalar ve İpuçları**

|  |  |  |
| --- | --- | --- |
| **Konu** | **Karışıklık** | **Açıklama** |
| **Smishing vs. Phishing** | SMS ile gelen → Smishing, E-mail ile gelen → Phishing |  |
| **Salting vs. Key Stretching** | Salting → Hash'e rastgele veri eklemek, Key Stretching → Hesaplama süresini uzatarak brute-force zorlaştırma |  |
| **DLP vs. SIEM** | DLP → Veri kaybını engeller, SIEM → Log analizi ve alarm üretir |  |
| **Red Team vs. Purple Team** | Red Team → Saldıran, Blue Team → Savunan, Purple Team → Her ikisinin birleşimi |  |
| **Compensating Control** | Öngörülemeyen zafiyetler için uygulanan geçici/alternatif güvenlik çözümü |  |

## **📚 5. Önerilen Kaynaklar**

* CompTIA resmi kaynakları (CertMaster, Study Guide)
* Professor Messer – SY0-701 videoları
* TryHackMe, HackTheBox – pratik ortamlar
* ExamTopics – Soru tipi öğrenimi (örnek PDF gibi)
* Quizlet – Kavram kartları