

# Indice generale

## **Introduzione .....xvii**

L'esame Security+.....	xvii
Sostenere l'esame.....	xix
Dopo l'esame Security+ .....	xx
Argomenti trattati nel libro .....	xx
Elementi di questa Guida.....	xxiii
Esame SY0-701 – Obiettivi dell'esame.....	xxiii
Mappa degli obiettivi dell'esame di certificazione SY0-701 .....	xxiv
Test di valutazione .....	xxv
Risposte al test di valutazione.....	xxix
Gli autori.....	xxxii
L'editor tecnico.....	xxxii
Il redattore tecnico.....	xxxiii
Ringraziamenti.....	xxxiii

## **Capitolo 1 Il professionista della sicurezza, oggi ..... 1**

Gli obiettivi della sicurezza informatica .....	1
I rischi delle violazioni dei dati.....	3
La triade DAD.....	3
L'impatto della violazione .....	4
Analisi dei gap .....	7
Categorie dei controlli di sicurezza .....	7
Tipi di controlli di sicurezza.....	8
La protezione dei dati .....	9
Crittografia dei dati .....	10
Prevenzione della perdita dei dati.....	10
Minimizzazione dei dati.....	11
Restrizioni di accesso .....	12
Segmentazione e isolamento .....	12
Riepilogo .....	13
Concetti essenziali per l'esame .....	13
Domande di ripasso .....	14

<b>Capitolo 2</b>	<b>Panorama delle minacce alla sicurezza informatica .....</b>	<b>19</b>
	Le varie minacce alla sicurezza informatica .....	19
	Classificazione delle minacce alla sicurezza informatica .....	20
	Soggetti delle minacce .....	21
	Motivazioni degli hacker .....	27
	Vettori di minaccia e superfici d'attacco .....	28
	Dati e intelligence sulle minacce .....	30
	Intelligence open source .....	31
	Intelligence proprietaria e closed source .....	33
	Valutazione dell'intelligence sulle minacce .....	34
	Gestione e scambio degli indicatori di minacce .....	36
	Organizzazioni per la condivisione delle informazioni .....	37
	Condurre le proprie ricerche .....	38
	Riepilogo .....	38
	Concetti essenziali per l'esame .....	38
	Domande di ripasso .....	39
<b>Capitolo 3</b>	<b>Codice malevolo.....</b>	<b>45</b>
	Malware.....	45
	Ransomware .....	46
	Troian .....	47
	Worm.....	49
	Spyware.....	50
	Bloatware .....	51
	Virus .....	52
	Keylogger .....	54
	Bombe logiche .....	54
	Rootkit .....	55
	Riepilogo .....	56
	Concetti essenziali per l'esame .....	57
	Domande di ripasso .....	58
<b>Capitolo 4</b>	<b>Ingegneria sociale e attacchi alle password .....</b>	<b>63</b>
	Ingegneria sociale e vettori umani.....	63
	Tecniche di ingegneria sociale.....	65
	Attacchi alle password .....	69
	Riepilogo .....	72
	Concetti essenziali per l'esame .....	72
	Domande di ripasso .....	72
<b>Capitolo 5</b>	<b>Valutazione e test della sicurezza .....</b>	<b>77</b>
	Gestione delle vulnerabilità .....	77
	Identificazione degli obiettivi di scansione.....	78
	Determinazione della frequenza delle scansioni .....	78

Configurazione delle scansioni delle vulnerabilità.....	81
Manutenzione dello scanner .....	85
Strumenti per la scansione delle vulnerabilità .....	88
Revisione e interpretazione dei report delle scansioni .....	89
Conferma dei risultati della scansione .....	98
Classificazione delle vulnerabilità.....	99
Gestione delle patch .....	100
Piattaforme legacy .....	100
Configurazioni deboli.....	102
Messaggi d'errore .....	102
Protocolli non sicuri.....	103
Crittografia debole .....	104
Penetration test.....	105
Adottare la mentalità da hacker .....	105
Le motivazioni dei penetration test .....	107
Vantaggi del penetration test .....	107
Tipi di penetration test .....	108
Regole d'ingaggio .....	110
Riconoscimento.....	111
Conduzione del test.....	112
Pulizia .....	113
Audit e valutazioni.....	113
Test della sicurezza .....	113
Valutazioni della sicurezza .....	115
Audit della sicurezza .....	115
Ciclo di vita delle vulnerabilità.....	117
Identificazione delle vulnerabilità.....	117
Analisi delle vulnerabilità .....	118
Risposta e riparazione delle vulnerabilità.....	118
Convalida delle riparazioni.....	119
Reporting .....	119
Riepilogo .....	119
Concetti essenziali per l'esame .....	120
Domande di ripasso .....	121

## **Capitolo 6 Sicurezza delle applicazioni.....127**

Best practice di software assurance.....	127
Il ciclo di vita dello sviluppo di software .....	128
Le fasi dello sviluppo di software .....	129
DevSecOps e DevOps .....	130
Progettazione e programmazione per la sicurezza .....	132
Pratiche sicure di programmazione.....	132
Sicurezza delle API .....	133
Test della sicurezza del software .....	133
Analisi e test del codice.....	134
Vulnerabilità alle iniezioni di codice .....	135

Attacchi SQL Injection.....	135
Attacchi a iniezione di codice .....	139
Attacchi a iniezione di comandi.....	139
Sfruttamento delle vulnerabilità di autenticazione.....	140
Autenticazione tramite password.....	141
Attacchi alle sessioni .....	142
Sfruttamento delle vulnerabilità delle autorizzazioni.....	145
Riferimenti diretti e non sicuri a un oggetto.....	145
Attraversamento delle directory.....	146
Inclusione di file .....	147
Escalation dei privilegi.....	148
Sfruttamento delle vulnerabilità delle applicazioni web.....	148
XSS (Cross-Site Scripting) .....	148
Request Forgery.....	151
Controlli di sicurezza delle applicazioni.....	152
Convalida dell'input.....	152
Firewall per applicazioni web .....	154
Query con parametri.....	154
Sandboxing.....	154
Sicurezza del codice.....	156
Pratiche sicure di programmazione.....	158
Commenti nel codice sorgente .....	158
Gestione degli errori.....	158
Credenziali hardcoded .....	159
Monitoraggio dei pacchetti.....	160
Gestione della memoria .....	160
Condizioni di competizione .....	161
API non protette .....	162
Automazione e orchestrazione .....	163
Casi d'uso dell'automazione e dello scripting .....	163
Vantaggi dell'automazione e dello scripting.....	164
Altre considerazioni.....	164
Riepilogo .....	165
Concetti essenziali per l'esame .....	165
Domande di ripasso .....	166

## **Capitolo 7 Crittografia e PKI.....171**

Una panoramica sulla crittografia .....	172
La crittografia storica .....	172
Obiettivi della crittografia .....	177
Riservatezza .....	178
Integrità .....	180
Autenticazione .....	181
Non ripudiabilità.....	181
Concetti di crittografia.....	181
Chiavi di crittografia.....	182

Cifrature .....	183
Crittografia moderna .....	183
Segretezza crittografica .....	184
Algoritmi a chiave simmetrica.....	185
Algoritmi a chiave asimmetrica .....	186
Algoritmi di hashing.....	189
Crittografia simmetrica .....	189
Standard di crittografia dei dati .....	189
AES (Advanced Encryption Standard).....	189
Gestione delle chiavi simmetriche.....	190
Crittografia asimmetrica.....	192
RSA.....	193
Curva ellittica .....	194
Funzioni hash .....	194
SHA.....	195
MD5.....	196
Firme digitali.....	196
HMAC.....	197
Infrastruttura a chiave pubblica.....	198
Certificati .....	199
Autorità di certificazione .....	200
Generazione e distruzione di certificati .....	201
Formati dei certificati .....	204
Gestione delle chiavi asimmetriche .....	204
Attacchi crittografici .....	205
Forza bruta.....	205
Analisi della frequenza .....	206
Testo in chiaro noto.....	206
Testo in chiaro scelto .....	206
Attacco a chiavi correlate.....	206
Attacco a compleanno .....	206
Attacco a downgrade .....	207
Hashing, salting e allungamento delle chiavi .....	208
Sfruttamento di chiavi deboli.....	208
Sfruttamento dell'errore umano .....	208
Problemi emergenti nella crittografia.....	209
Tor e il Dark Web .....	209
Blockchain .....	209
Crittografia leggera.....	210
Crittografia omomorfa.....	211
Computer quantistici .....	211
Riepilogo .....	211
Concetti essenziali per l'esame .....	211
Domande di ripasso .....	212

**Capitolo 8 Gestione delle identità e degli accessi .....217**

Identità .....	218
Autenticazione e autorizzazione .....	219
Tecnologie di autenticazione e autorizzazione .....	219
Metodi di autenticazione .....	225
Le password .....	225
Autenticazione a più fattori .....	229
Password monouso .....	230
Fattori biometrici .....	232
Account.....	233
Tipi di account.....	234
Creazione e revoca degli account.....	234
Schemi di controllo degli accessi .....	236
Permessi di accesso al file system .....	238
Riepilogo .....	239
Concetti essenziali per l'esame .....	240
Domande di ripasso .....	241

**Capitolo 9 Resilienza e sicurezza fisica.....245**

Resilienza e recupero nelle architetture di sicurezza.....	246
Considerazioni sull'architettura e la sicurezza .....	248
Resilienza dello spazio di memorizzazione.....	249
Controlli di risposta e recupero .....	255
Pianificazione della capacità per la resilienza e il recupero.....	258
Test dei controlli e dei progetti di resilienza e recupero.....	259
Controlli di sicurezza fisica.....	260
Sicurezza del sito .....	260
Rilevamento di attacchi fisici .....	266
Riepilogo .....	266
Concetti essenziali per l'esame .....	267
Domande di ripasso .....	268

**Capitolo 10 Sicurezza del cloud e della virtualizzazione .....273**

Il cloud.....	273
I vantaggi del cloud .....	274
I ruoli nel cloud .....	276
Modelli di servizi cloud .....	277
Modelli di distribuzione cloud.....	280
Cloud privato.....	280
Modello a responsabilità condivisa .....	282
Standard e linee guida per il cloud .....	284
Virtualizzazione .....	286
Hypervisor .....	287
I componenti dell'infrastruttura cloud .....	287

Risorse di elaborazione del cloud.....	288
Risorse di archiviazione del cloud.....	290
Networking nel cloud .....	292
Problemi relativi alla sicurezza nel cloud.....	296
Disponibilità.....	296
Sovranità dei dati .....	297
Sicurezza della virtualizzazione.....	297
Sicurezza delle applicazioni .....	298
Governance e audit dei fornitori terzi .....	299
Rafforzare l'infrastruttura cloud.....	299
CASB (Cloud Access Security Broker).....	299
Policy sull'uso delle risorse.....	300
Gestione dei segreti .....	301
Riepilogo .....	301
Concetti essenziali per l'esame .....	302
Domande di ripasso .....	303

## **Capitolo 11 Sicurezza degli endpoint.....307**

Vulnerabilità del sistema operativo.....	308
Vulnerabilità hardware.....	309
Protezione degli endpoint.....	310
Preservare l'integrità del boot .....	310
Strumenti per la sicurezza degli endpoint.....	313
Tecniche di rafforzamento.....	319
Rafforzamento .....	319
Rafforzamento del servizio .....	319
Rafforzamento della rete.....	321
Password di default .....	321
Rimozione di software non necessario .....	321
Rafforzamento del sistema operativo .....	322
Criteri di gruppo e protezione avanzata di Windows .....	323
Rafforzamento di Linux: SELinux.....	324
Configurazione, standard e schemi .....	325
Crittografia.....	327
Protezione dei sistemi embedded e specializzati.....	327
Sistemi embedded.....	328
SCADA e ICS .....	330
Protezione dell'Internet of Things.....	331
Considerazioni sulle comunicazioni .....	333
Vincoli di sicurezza dei sistemi embedded.....	333
Gestione delle risorse.....	334
Smantellamento .....	335
Conservazione.....	337
Riepilogo .....	337
Concetti essenziali per l'esame .....	338
Domande di ripasso .....	339

**Capitolo 12 Sicurezza della rete.....345**

Progettare reti sicure .....	346
Considerazioni sull'infrastruttura.....	348
Concetti di progettazione della rete.....	349
Segmentazione della rete.....	352
Zero Trust .....	353
Controllo degli accessi alla rete .....	355
Sicurezza delle porte e protezioni a livello di porta.....	356
Reti private virtuali e accesso remoto .....	359
Dispositivi di rete e strumenti di sicurezza.....	360
Tecnologie di inganno e contrasto .....	368
Sicurezza, servizi e gestione della rete.....	369
Protocolli sicuri .....	374
Utilizzo di protocolli sicuri .....	375
Protocolli sicuri .....	376
Attacchi alla rete .....	379
Attacchi on-path.....	379
Attacchi al DNS .....	381
Attacchi a riproduzione delle credenziali.....	383
Codice malevolo.....	383
Attacchi Distributed Denial of Service .....	384
Riepilogo .....	386
Concetti essenziali per l'esame .....	387
Domande di ripasso .....	389

**Capitolo 13 Sicurezza wireless e mobile .....393**

Costruire reti wireless sicure.....	394
Metodi di connessione.....	394
Modelli di rete wireless.....	399
Attacchi contro reti e dispositivi wireless.....	400
Progettare una rete.....	403
Sicurezza del controller e dell'access point.....	406
Standard sulla sicurezza Wi-Fi .....	406
Autenticazione wireless.....	407
Gestione dei dispositivi mobili sicuri.....	409
Metodi di distribuzione dei dispositivi mobili.....	409
Rafforzamento dei dispositivi mobili.....	411
Gestione dei dispositivi mobili .....	412
Riepilogo .....	415
Concetti essenziali per l'esame .....	416
Domande di ripasso .....	417

**Capitolo 14 Monitoraggio e risposta agli incidenti.....423**

Risposta agli incidenti.....	424
Il processo di risposta agli incidenti .....	424



Formazione .....	429
Caccia alle minacce.....	429
Gli attacchi e gli incidenti .....	431
Dati e strumenti di risposta agli incidenti .....	432
Monitoraggio delle risorse di elaborazione .....	433
Sistemi SIEM .....	433
Aggregazione, correlazione e analisi dei file log .....	437
Regole .....	437
Benchmark e logging.....	445
Reporting e archiviazione.....	445
Mitigazione e ripristino .....	445
SOAR (Security Orchestration, Automation and Response)...	446
Tecniche di contenimento, mitigazione e recupero .....	446
Analisi delle cause profonde .....	449
Riepilogo .....	449
Concetti essenziali per l'esame .....	450
Domande di ripasso .....	452
<b>Capitolo 15 Analisi forense digitale.....</b>	<b>457</b>
Concetti di analisi forense digitale .....	458
Conservazione legale ed e-Discovery .....	458
Conduzione dell'analisi forense digitale .....	460
Acquisizione di dati forensi .....	460
Strumenti di acquisizione.....	465
Convalida dell'integrità dei dati forensi .....	468
Recupero dei dati.....	470
Suite forensi e un caso di studio .....	471
Reporting.....	474
Analisi forense digitale e intelligence .....	475
Riepilogo .....	476
Concetti essenziali per l'esame .....	476
Domande di ripasso .....	477
<b>Capitolo 16 Governance e conformità della sicurezza .....</b>	<b>483</b>
Governance della sicurezza.....	483
Governance aziendale .....	484
Programmi di governance, rischio e conformità .....	485
Governance della sicurezza delle informazioni.....	485
Tipi di strutture di governance.....	486
Comprensione dei documenti delle policy .....	487
Policy .....	487
Standard .....	489
Procedure .....	492
Linee guida.....	493
Eccezioni e controlli compensativi .....	494
Monitoraggio e revisione.....	495

Gestione delle modifiche .....	496
Processi e controlli di gestione delle modifiche.....	497
Controllo della versione.....	499
Documentazione .....	500
Gestione del personale .....	500
Privilegi minimi .....	500
Separazione dei compiti.....	500
Rotazione del lavoro e ferie obbligatorie .....	501
Ordine sulla scrivania.....	501
Onboarding e offboarding.....	501
Accordi di non divulgazione .....	501
Social media .....	502
Gestione dei rischi relativi a terze parti.....	502
Scelta del fornitore .....	502
Valutazione del fornitore.....	502
Accordi con i fornitori .....	503
Monitoraggio dei fornitori .....	504
Chiusura dei rapporti con i fornitori.....	505
Rispettare le leggi e i regolamenti .....	505
Requisiti comuni di conformità.....	506
Reporting di conformità .....	506
Conseguenze della non conformità.....	507
Monitoraggio della conformità .....	508
Adozione di framework standard.....	508
Il NIST Cybersecurity Framework .....	509
Il NIST Risk Management Framework.....	512
Norme ISO.....	513
Benchmark e guide alla sicurezza della configurazione.....	514
Sensibilizzazione e formazione sulla sicurezza .....	514
Formazione degli utenti.....	515
Attività continue di sensibilizzazione .....	517
Riepilogo .....	519
Concetti essenziali per l'esame .....	519
Domande di ripasso .....	520

## **Capitolo 17 Gestione dei rischi e privacy .....525**

Analisi dei rischi .....	525
Identificazione dei rischi.....	527
Valutazione dei rischi.....	527
Analisi dei rischi .....	529
Gestione dei rischi .....	532
Mitigazione dei rischi .....	533
Prevenzione dei rischi.....	534
Trasferimento dei rischi .....	534
Accettazione dei rischi.....	535
Monitoraggio dei rischi .....	536

---

Registro dei rischi .....	537
Reporting dei rischi .....	539
Pianificazione del recupero dai disastri.....	539
Tipi di disastri .....	540
Analisi dell'impatto sull'azienda.....	540
Privacy .....	541
Inventario dei dati .....	541
Classificazione delle informazioni .....	542
Ruoli e responsabilità dei dati .....	543
Ciclo di vita delle informazioni.....	544
Tecnologie per il miglioramento della privacy .....	546
Notifica di violazione della privacy e dei dati .....	546
Riepilogo .....	547
Concetti essenziali per l'esame .....	547
Domande di ripasso .....	548
<b>Appendice Risposte alle domande di ripasso.....</b>	<b>553</b>
<b>Indice analitico.....</b>	<b>593</b>