Introduzione

Se vi state preparando a sostenere l'esame Security+, vorrete senza dubbio trovare quante più informazioni possibili sulla sicurezza, informatica e fisica. Più informazioni avrete a disposizione e più esperienza acquisirete, meglio sarà quando tenterete l'esame. Questa guida è stata scritta proprio con questo scopo. L'obiettivo è stato fornirvi informazioni sufficienti per prepararvi al test, ma non così tante da sovraccaricarvi di informazioni che esulano dall'ambito dell'esame.

Questo libro presenta il materiale a un livello tecnico intermedio. L'esperienza e la conoscenza dei concetti della sicurezza, dei sistemi operativi e dei sistemi applicativi vi aiuteranno a comprendere appieno le sfide che dovrete affrontare come professionisti della sicurezza.

Alla fine di ogni capitolo abbiamo incluso delle domande di ripasso, per darvi un assaggio di quel che vuol dire sostenere l'esame. Se lavorate già nel campo della sicurezza, vi consigliamo di rispondere prima a queste domande per valutare il vostro livello di competenza. Potrete utilizzare il libro, quindi, principalmente per colmare le lacune delle vostre attuali conoscenze. Questa guida vi aiuterà pertanto ad affinare le vostre conoscenze di base prima di affrontare l'esame.

Se riuscirete a rispondere correttamente al 90% o più delle domande di ripasso di un determinato capitolo, potrete tranquillamente passare al capitolo successivo. Se invece non riuscite a rispondere correttamente a quel livello di domande, rileggete il capitolo e riprovate a rispondere alle domande. Il vostro punteggio dovrebbe migliorare.

NOTA

Non limitatevi a studiare le domande e le risposte! Le domande dell'esame vero e proprio saranno differenti dalle domande pratiche presentate in questo libro. L'esame è concepito per mettere alla prova le vostre conoscenze su un concetto o un obiettivo, quindi utilizzate questo libro per apprendere gli obiettivi che stanno dietro quelle domande.

L'esame Security+

L'esame Security+ è concepito come una certificazione neutrale rispetto al fornitore per i professionisti della sicurezza informatica e per coloro che desiderano entrare nel

campo. CompTIA consiglia di dotarsi di questa certificazione coloro che lavorano o aspirano a lavorare in ruoli come i seguenti:

- amministratore di sistema;
- amministratore della sicurezza;
- tecnico di supporto IT di II livello;
- responsabile del supporto informatico;
- analista della sicurezza informatica;
- analista.

L'esame tratta principalmente cinque ambiti:

1. concetti generali della sicurezza;
2. minacce, vulnerabilità e mitigazioni;
3. architettura della sicurezza;
4. attività della sicurezza;
5. gestione e supervisione del programma di sicurezza.

Queste cinque aree comprendono una serie di argomenti, dalla progettazione del firewall alla risposta agli incidenti e all'analisi forense, concentrandosi soprattutto sull'apprendimento basato su scenari. Ecco perché CompTIA consiglia a coloro che tentano l'esame di possedere CompTIA Network+ e due anni di esperienza di lavoro in un ruolo di amministratore della sicurezza/dei sistemi, sebbene molti superino l'esame anche prima di essere assunti per il loro primo ruolo nel campo della sicurezza informatica.
CompTIA descrive l'esame Security+ come una verifica del possesso delle conoscenze e competenze necessarie per:

- valutare il livello di sicurezza degli ambienti aziendali;
- consigliare e implementare adeguate soluzioni di sicurezza;
- monitorare e proteggere ambienti ibridi;
- operare con la consapevolezza delle normative e delle policy applicabili;
- identificare, analizzare e rispondere a eventi e incidenti relativi alla sicurezza.

L'esame Security+ è condotto in un formato che CompTIA chiama "valutazione basata sulle prestazioni". Ciò significa che l'esame combina domande standard a scelta multipla con altri formati di domande interattive. L'esame può includere diversi tipi di domande, per esempio a scelta multipla, a schema libero, a risposta multipla, drag-and-drop e problemi basati su immagini.
L'esame negli Stati Uniti costa 392 dollari, ma presenta costi più o meno equivalenti in altre località in tutto il mondo. Potete trovare maggiori dettagli sull'esame Security+ e su come sostenerlo su:

`www.comptia.org/certifications/security`

Avrete 90 minuti per sostenere l'esame e in quell'arco di tempo vi verrà chiesto di rispondere a un massimo di 90 domande. Il vostro esame verrà valutato su una scala che va da 100 a 900, con un punteggio minimo di 750.

Dovete anche sapere che CompTIA è noto per includere nei suoi esami anche domande più vaghe. Potreste trovare una domanda per la quale due delle quattro risposte possibili sembrerebbero corrette, ma potrete sceglierne solo una. Utilizzate le vostre conoscenze, la logica e l'intuito per scegliere la risposta migliore e poi andate avanti. A volte, le domande sono formulate sintatticamente in modi che farebbero rabbrividire: un errore di battitura, un verbo sbagliato. Non fatevi distrarre da questi dettagli; rispondete alla domanda e passate alla successiva.

NOTA

CompTIA esegue spesso il cosiddetto *item seeding*, ovvero include negli esami anche domande che non danno punteggio. Lo fa per raccogliere dati psicometrici, che vengono poi utilizzati per lo sviluppo di nuove versioni dell'esame. Prima di sostenere l'esame, vi verrà comunicato che questo potrebbe includere domande senza punteggio. Pertanto, se vi imbattete in una domanda che non sembra riguardare nessuno degli obiettivi dell'esame (o proprio sembra avulsa dall'esame), è probabile che si tratti proprio di una di queste domande. Tuttavia, non potete mai sapere veramente se una domanda è valida o meno, quindi fate sempre del vostro meglio per rispondere a ogni domanda.

Sostenere l'esame

Una volta che vi sentite preparati per sostenere l'esame, potete visitare il sito web CompTIA per acquistare il voucher per l'esame:

`https://store.comptia.org`

Attualmente, CompTIA offre due opzioni per sostenere l'esame: un esame in presenza, da svolgersi presso un centro di test, e un esame a casa, da sostenere sul proprio computer.

Esami in presenza

CompTIA collabora con i centri di test di PearsonVUE, quindi il vostro passo successivo sarà individuare un centro di test vicino a voi. Negli Stati Uniti, potete farlo in base al vostro indirizzo o codice postale, mentre per i partecipanti al test non statunitensi sarà più facile inserire la città e il Paese. Potete cercare un centro test vicino a voi sul sito web PearsonVUE, dove dovrete care clic su "Find a test center".

`https://www.pearsonvue.com/comptia`

Ora che sapete dove desiderate sostenere l'esame, dovrete creare un account CompTIA e programmare l'esame tramite PearsonVUE.
Il giorno del test, portate con voi due documenti di identità e assicuratevi di presentarvi con sufficiente anticipo prima dell'inizio dell'esame. Ricordate che non potrete portare con voi appunti, dispositivi elettronici (inclusi smartphone e orologi) o altri materiali.

Esami a domicilio

Nel 2020 CompTIA ha iniziato a offrire la supervisione degli esami online in risposta alla pandemia di coronavirus. Al momento della stampa di questo libro, l'opzione di test a domicilio è ancora disponibile e sembra probabile che continui. I candidati che utilizzano questo approccio possono sostenere l'esame da casa o dall'ufficio e saranno controllati tramite webcam da un supervisore remoto.
A causa della rapida evoluzione dell'esperienza dei test a domicilio, i candidati che desiderano sfruttare questa possibilità dovrebbero aggiornarsi sul sito web CompTIA con gli ultimi dettagli.

Dopo l'esame Security+

Una volta sostenuto l'esame vi verrà comunicato immediatamente il punteggio ottenuto, così saprete subito se avete superato il test. Vi consigliamo di conservare il report sul punteggio e i dati di registrazione all'esame nell'indirizzo e-mail utilizzato per registrarvi.

Conservare la certificazione

Come molte altre certificazioni CompTIA, anche Security+ deve essere rinnovata periodicamente. Per rinnovarla potete superare la versione più recente dell'esame, ottenere una certificazione CompTIA di settore di livello superiore, completare un corso CompTIA Certmaster CE o completare delle attività di formazione continua sufficienti per guadagnare un numero di CEU (*Continuing Education Unit*) sufficienti.
CompTIA fornisce informazioni sui rinnovi tramite il proprio sito web all'indirizzo:

```
https://www.comptia.org/continuing-education
```

Quando vi iscriverete per rinnovare la certificazione, vi verrà chiesto di accettare il codice etico del programma CE, di pagare la quota di rinnovo e di inviare i materiali richiesti per il metodo di rinnovo prescelto.
Un elenco completo delle certificazioni di settore che potete utilizzare per acquisire CEU utili ai fini del rinnovo del Security+ è disponibile al seguente indirizzo:

```
https://www.comptia.org/continuing-education/choose/renew-with-a-single-activity/earn-non-comptia-it-industry-certifications
```

Argomenti trattati nel libro

Questo libro copre tutto ciò che dovete sapere per conoscere i compiti e le responsabilità di base di un amministratore della sicurezza e anche per superare l'esame Security+.

- Il *Capitolo 1* costituisce un'introduzione al campo della sicurezza informatica. Imparerete a conoscere il ruolo fondamentale svolto dai professionisti della sicurezza informatica nel proteggere la riservatezza, l'integrità e la disponibilità dei dati della propria azienda. Scoprirete anche i tipi di rischi che le aziende devono affrontare e l'uso dei controlli di sicurezza gestionali, operativi e tecnici per ridurre tali rischi.

- Il *Capitolo 2* approfondisce il panorama delle minacce alla sicurezza informatica, aiutandovi a comprendere i diversi tipi di soggetti che rappresentano minacce nell'ambiente odierno e i vettori che sfruttano per indebolire i controlli di sicurezza. Imparerete anche a utilizzare le fonti di intelligence sulle minacce, per migliorare il programma di sicurezza della vostra azienda e mitigare i problemi relativi alla sicurezza che derivano da diversi tipi di vulnerabilità.
- Il *Capitolo 3* esplora l'ampia gamma di software dannosi che potreste incontrare. In questo capitolo vengono trattati i worm, i virus, i trojan, il ransomware e vari altri tipi di malware. Conoscerete non solo i numerosi strumenti utilizzati dagli hacker, ma scoprirete anche come capire che è in atto una violazione ed esempi reali dell'impatto del malware sulle aziende.
- Il *Capitolo 4* approfondisce il lato umano della sicurezza delle informazioni. Esplorerete le tecniche di ingegneria sociale impiegate, che vanno dal phishing all'impersonificazione, nonché le tecniche di disinformazione. Successivamente, approfondirete gli attacchi tramite password, come gli attacchi a forza bruta e a spraying di password.
- Il *Capitolo 5* esplora i diversi tipi di valutazioni della sicurezza e le procedure di test che potete utilizzare per valutare l'efficacia del programma di sicurezza. Imparerete a conoscere le diverse tecniche di valutazione utilizzate dai professionisti della sicurezza informatica e la corretta conduzione dei penetration test in un'ampia varietà di contesti. Imparerete anche a sviluppare un programma di valutazione che soddisfi i requisiti di sicurezza della vostra azienda.
- Il *Capitolo 6* tratta i problemi relativi alla sicurezza riguardanti il codice delle applicazioni e gli indicatori relativi agli attacchi alle applicazioni. Imparerete a utilizzare i concetti di sviluppo, distribuzione e automazione sicuri delle applicazioni e scoprirete come aiutare la vostra azienda a sviluppare e distribuire codice resistente alle minacce.
- Il *Capitolo 7* spiega il ruolo fondamentale svolto dalla crittografia nei programmi di sicurezza, facilitando la comunicazione sicura e l'archiviazione protetta dei dati. Conoscerete i concetti crittografici di base e imparerete a utilizzarli per proteggere i dati presenti nel vostro ambiente. Scoprirete anche quali sono gli attacchi più comuni ai sistemi di crittografia, che potrebbero essere utilizzati per indebolire i vostri controlli.
- Il *Capitolo 8* spiega l'uso dell'identità come forma di sicurezza per le aziende. Imparerete a conoscere i componenti di un'identità, come funzionano l'autenticazione e l'autorizzazione, quali tecnologie vengono implementate per abilitarle e come i modelli di Single Sign-On, federazione e autenticazione interagiscono con l'infrastruttura di autenticazione e autorizzazione. Imparerete anche il funzionamento dell'autenticazione a più fattori e biometrica, come metodi per fornire un'autenticazione più sicura. Anche gli account, gli schemi di controllo dell'accesso e le autorizzazioni hanno un loro specifico ruolo ed esplorerete anche ciascuno di questi argomenti.
- Il *Capitolo 9* illustra i concetti della sicurezza fisica. Senza sicurezza fisica, un'azienda non può pensare di avere un ambiente veramente sicuro. In questo capitolo imparerete a costruire un'infrastruttura resiliente e resistente ai disastri, utilizzando il backup e la ridondanza. Esplorerete i fattori di cui le aziende devono tenere conto quando progettano l'architettura della sicurezza e imparerete a conoscere un'ampia gamma di controlli di sicurezza fisici per garantire che strutture e sistemi rimangano protetti da disastri, attacchi e altre minacce fisiche. Nel frattempo, approfondirete la resilienza e come può essere attuata nell'architettura della vostra azienda.

- Il *Capitolo 10* esplora la sicurezza nel campo del cloud computing e della virtualizzazione. Molte aziende ora distribuiscono le loro applicazioni critiche nel cloud e utilizzano ambienti cloud per elaborare dati riservati. Scoprirete come le aziende utilizzano i servizi cloud a loro disposizione e come creano architetture cloud per soddisfare le loro esigenze. Imparerete anche a gestire il rischio relativo alla sicurezza informatica dei servizi cloud, utilizzando una combinazione di controlli tradizionali e specifici per il cloud.
- Il *Capitolo 11* presenta una panoramica dei numerosi tipi di endpoint che potrebbe essere necessario proteggere. Esplorerete la sicurezza delle workstation e dei dispositivi mobili, e imparerete a proteggere i sistemi embedded, i sistemi di controllo industriale e i dispositivi Internet of Things. Anche gli endpoint necessitano di certe soluzioni di sicurezza, come la crittografia e processi di boot sicuri. Successivamente, parleremo di rafforzamento, di tecniche di mitigazione e di cicli di vita della sicurezza, incluso lo smaltimento dei sistemi, dei supporti e di altri componenti della vostra infrastruttura tecnologica.
- Il *Capitolo 12* tratta la sicurezza della rete, dall'architettura e dalla progettazione agli attacchi e alle difese. Esplorerete le tecniche e le minacce più comuni degli attacchi alla rete e scoprirete i protocolli, le tecnologie, i concetti di progettazione e le tecniche di implementazione di reti sicure, per contrastare o evitare tali minacce. Inoltre, imparerete a conoscere il ruolo del Zero Trust nella progettazione di reti sicure.
- Il *Capitolo 13* esplora il mondo della sicurezza wireless e mobile. Scoprirete come funziona una varietà sempre crescente di tecnologie wireless, dal GPS al Bluetooth fino al Wi-Fi. Conoscerete alcuni attacchi wireless comunemente impiegati e scoprirete come progettare e costruire un ambiente wireless sicuro. Imparerete anche le tecnologie e gli schemi costruttivi utilizzati per rendere sicuri e proteggere i dispositivi wireless, come la gestione dei dispositivi mobili e i metodi di distribuzione dei dispositivi.
- Il *Capitolo 14* spiega che cosa fare quando le cose vanno storte. Gli incidenti sono una realtà quotidiana per i professionisti della sicurezza e imparerete a conoscere le policy, le procedure e le tecniche di risposta agli incidenti. Imparerete anche dove e come ottenere le informazioni necessarie per i processi di risposta, quali strumenti vengono comunemente utilizzati e quali tecniche di mitigazione possono essere impiegate per controllare gli attacchi e recuperare i sistemi dopo gli attacchi.
- Il *Capitolo 15* esplora le tecniche e gli strumenti forensi digitali. Imparerete a trovare le prove come parte delle indagini, gli strumenti e i processi forensi e come utilizzarli per determinare che cosa è andato storto. Conoscerete anche i processi legali e probatori necessari per condurre le indagini forensi quando sono coinvolte le forze dell'ordine o un consulente legale.
- Il *Capitolo 16* approfondisce il mondo delle policy, degli standard e della conformità, elementi fondamentali alla base di qualsiasi programma di sicurezza informatica. Imparerete a scrivere e applicare policy riguardanti il personale, la sua formazione, i dati, le credenziali e altre questioni. Imparerete anche l'importanza di comprendere le normative, le leggi e gli standard che governano il mondo in cui opera l'azienda e a gestire la conformità a tali requisiti.

- Il *Capitolo 17* descrive i concetti di gestione dei rischi e della privacy, che sono cruciali per il lavoro dei professionisti della sicurezza informatica. Imparerete a conoscere il processo di gestione dei rischi, inclusa la loro identificazione, valutazione e gestione. Imparerete anche le conseguenze delle violazioni della privacy e i controlli che potete mettere in atto per proteggere la privacy delle informazioni di identificazione personale.

Elementi di questa Guida

Questa Guida utilizza alcuni elementi comuni per aiutarvi nella preparazione.

- Le *Note sull'esame* sono presenti in ogni capitolo per avvisarvi di informazioni importanti relative agli obiettivi dell'esame.
- La sezione *Riepilogo* di ciascun capitolo riassume brevemente i contenuti del capitolo, consentendovi di comprendere facilmente gli argomenti trattati.
- I *Concetti essenziali per l'esame* si concentrano sugli argomenti principali specifici dell'esame e sulle conoscenze critiche che dovete dimostrare nel test. Questa parte del capitolo si concentra sugli obiettivi dell'esame, forniti da CompTIA.
- Le *Domande di ripasso*, alla fine di ogni capitolo, vi aiuteranno a valutare le vostre conoscenze e a scoprire se siete pronti a sostenere l'esame in base alle vostre conoscenze degli argomenti del capitolo.

Esame SY0-701 – Obiettivi dell'esame

CompTIA fa il possibile per garantire che i suoi programmi di certificazione riflettano accuratamente le best practice del settore IT. Lo fa istituendo dei comitati relativi a ciascuno dei suoi programmi di esame. Ciascun comitato è composto da un gruppo di professionisti IT, fornitori di servizi di formazione e editori, che sono responsabili di stabilire il livello di competenza di base per superare l'esame e di determinare il livello appropriato del pubblico cui l'esame si rivolge.
Una volta determinati questi fattori, CompTIA condivide queste informazioni con un gruppo di esperti in materia (SME) selezionati manualmente. Queste persone sono i veri "motori" intellettuali dietro il programma di certificazione. Essi esaminano i risultati forniti dai comitati, li perfezionano e li modellano negli obiettivi che troverete di seguito. CompTIA chiama questo processo JTA (*Job-Task Analysis*).
Infine, CompTIA conduce un sondaggio per garantire che gli obiettivi e i pesi loro attribuiti riflettano realmente i requisiti professionali. Solo allora gli esperti in materia possono mettersi al lavoro scrivendo le centinaia di domande necessarie per l'esame. Anche così, in molti casi occorre tornare a eseguire ulteriori perfezionamenti prima che l'esame sia pronto per essere pubblicato nel suo stato finale. Potete essere certi che i contenuti che state per studiare vi serviranno per molto tempo, dopo aver sostenuto l'esame.
CompTIA pubblica anche i pesi relativi a ciascuno degli obiettivi dell'esame. La Tabella I.1 elenca i cinque ambiti degli obiettivi Security+ e la misura in cui si trovano rappresentati nell'esame.

Tabella I.1

Dominio	Percentuale dell'esame
1.0 Concetti generali della sicurezza	12%
2.0 Minacce, vulnerabilità e mitigazioni	22%
3.0 Architettura della sicurezza	18%
4.0 Attività della sicurezza	28%
5.0 Gestione e supervisione del programma di sicurezza	20%

Mappa degli obiettivi dell'esame di certificazione SY0-701

Obiettivo	Capitoli
1.0 Concetti generali della sicurezza	
1.1 Confrontare e contrapporre i vari tipi di controlli di sicurezza.	1
1.2 Riassumere i concetti fondamentali della sicurezza.	1, 8, 9, 12
1.3 Spiegare l'importanza dei processi di gestione delle modifiche e il loro impatto sulla sicurezza.	16
1.4 Spiegare l'importanza di utilizzare soluzioni crittografiche appropriate.	1, 7, 11
2.0 Minacce, vulnerabilità e mitigazioni	
2.1 Confrontare e contrapporre i soggetti e le motivazioni comuni delle minacce.	2
2.2 Spiegare i vettori di minaccia più comuni e le superfici d'attacco.	2, 4
2.3 Descrivere i vari tipi di vulnerabilità.	2, 6, 7, 10, 11, 13
2.4 Dato uno scenario, analizzare gli indicatori di un'attività dannosa.	3, 4, 6, 9, 12, 13, 14
2.5 Spiegare lo scopo delle tecniche di mitigazione utilizzate per proteggere l'azienda.	8, 11, 12, 14, 16
3.0 Architettura della sicurezza	
3.1 Confrontare e contrapporre le implicazioni sulla sicurezza dei diversi modelli di architettura.	9, 10, 11, 12
3.2 Dato uno scenario, applicare i principi della sicurezza per proteggere l'infrastruttura aziendale.	12
3.3 Confrontare e contrapporre i concetti e le strategie di protezione dei dati.	1, 10, 13, 17
3.4 Spiegare l'importanza della resilienza e del ripristino nell'architettura della sicurezza.	9, 17
4.0 Attività della sicurezza	
4.1 Dato uno scenario, applicare tecniche di sicurezza comuni alle risorse di elaborazione.	6, 10, 11, 12, 13
4.2 Spiegare le implicazioni sulla sicurezza di una corretta gestione dell'hardware, del software e delle risorse dei dati.	11
4.3 Spiegare le varie attività associate alla gestione delle vulnerabilità.	2, 5, 6
4.4 Spiegare i concetti e gli strumenti di allerta e monitoraggio della sicurezza.	5, 11, 12, 14
4.5 Dato uno scenario, modificare le caratteristiche dell'azienda per migliorare la sicurezza.	11, 12
4.6 Dato uno scenario, implementare e manutenere la gestione dell'identità e degli accessi.	8
4.7 Spiegare l'importanza dell'automazione e dell'orchestrazione relativamente alla sicurezza delle attività.	6

4.8 Spiegare le attività appropriate di risposta agli incidenti.	14, 15
4.9 Dato uno scenario, utilizzare le fonti di dati per supportare un'indagine.	14
5.0 Gestione e supervisione del programma di sicurezza	
5.1 Riassumere gli elementi di un'efficace governance della sicurezza.	16, 17
5.2 Spiegare gli elementi del processo di gestione dei rischi.	17
5.3 Spiegare i processi associati alla valutazione e gestione dei rischi relativi a terze parti.	16
5.4 Riassumere gli elementi di un'efficace conformità alla sicurezza.	16
5.5 Spiegare le tipologie e gli scopi degli audit e delle valutazioni.	5
5.6 Dato uno scenario, implementare pratiche di consapevolezza della sicurezza.	16

NOTA

Gli obiettivi dell'esame sono soggetti a modifiche in qualsiasi momento, senza preavviso e a discrezione di CompTIA. Visitate il sito web di CompTIA (`https://www.comptia.org`) per ottenere l'elenco aggiornato degli obiettivi dell'esame.

Test di valutazione

1. L'azienda per cui lavora Chris ha disabilitato gli aggiornamenti automatici. Qual è il motivo più comune per disabilitare gli aggiornamenti automatici per i sistemi aziendali?
   A. Per evitare interruzioni dei processi operativi per i dipendenti.
   B. Per prevenire violazioni della sicurezza dovute a patch e aggiornamenti dannosi.
   C. Per evitare problemi con patch e aggiornamenti problematici.
   D. Tutte le risposte precedenti.

2. Quale dei seguenti elementi è meno volatile secondo l'ordine forense di volatilità?
   A. La tabella di routing del sistema.
   B. I file log.
   C. I file temporanei.
   D. I registri della CPU.

3. Ed vuole indurre un utente a connettersi al suo Access Point Evil Twin. Che tipo di attacco dovrebbe condurre per aumentare le possibilità che l'utente si connetta?
   A. Un attacco a dissociazione.
   B. Un attacco denial-of-service all'applicazione.
   C. Un attacco puramente testuale.
   D. Un attacco denial-of-service alla rete.

4. Quale termine viene utilizzato per descrivere le indagini sui siti wireless che mostrano la potenza relativa degli Access Point su un diagramma dell'edificio o della struttura?
   A. Signal Survey.
   B. db map.

C. AP topology.
D. Heatmap.

5. Quale dispositivo hardware viene utilizzato per creare la base di attendibilità hardware per desktop e laptop?
   A. La memoria di sistema.
   B. Un HSM.
   C. La CPU.
   D. Il TPM.

6. Angela desidera impedire agli utenti della sua azienda di modificare ripetutamente la propria password dopo che è stata modificata, in modo che non possano riutilizzare la password corrente. Quali due impostazioni di sicurezza della password deve implementare per far sì che ciò accada?
   A. Impostare una cronologia delle password e un'età minima per la password.
   B. Impostare una cronologia delle password e un certo livello minimo di complessità.
   C. Impostare un'età minima e massima per le password.
   D. Impostare un certo livello minimo di complessità delle password e un'età massima.

7. Chris desidera creare un sito di backup che sia completamente pronto a subentrare in tutte le attività della sua azienda in qualsiasi momento. Che tipo di sito dovrebbe creare?
   A. Un cold site.
   B. Un sito clone.
   C. Un hot site.
   D. Un ready site.

8. Quale dei seguenti non è un vincolo comune dei sistemi embedded e specializzati?
   A. Potenza di calcolo.
   B. Impostazioni del firewall particolarmente complesse.
   C. Mancanza di connettività di rete.
   D. Impossibilità di applicare patch.

9. Gary sta esaminando i log SSH del suo sistema e vede i login dell'utente "Gary" con password come `password1`, `password2`, … `PassworD`. Che tipo di attacco ha scoperto Gary?
   A. Un attacco a dizionario.
   B. Un attacco rainbow table.
   C. Un attacco pass-the-hash.
   D. Un attacco a spraying di password.

10. Kathleen vuole predisporre un sistema che consenta l'accesso a una zona ad alta sicurezza da una zona a bassa sicurezza. Che tipo di soluzione dovrebbe configurare?
    A. VDI.
    B. Un container.
    C. Una sottorete schermata.
    D. Un jump server.

11. L'azienda di Derek teme che un dipendente scontento pubblichi informazioni riservate relative all'azienda. Da che tipo di minaccia si deve proteggere Derek?
    A. Shoulder surfing.
    B. Ingegneria sociale.
    C. Minacce interne.
    D. Phishing.

12. Jeff è preoccupato per gli effetti che un attacco ransomware potrebbe avere sulla sua azienda e sta progettando uno schema di backup che consentirebbe all'azienda di ripristinare rapidamente i dati dopo tale attacco. Che tipo di controllo sta implementando Jeff?
    A. Correttivo.
    B. Preventivo.
    C. Investigativo.
    D. Di deterrenza.

13. Samantha sta indagando su un incidente della sicurezza informatica in cui un utente interno ha utilizzato il proprio computer per partecipare a un attacco denial-of-service contro una terza parte. Che tipo di policy è stata molto probabilmente violata?
    A. BPA.
    B. SLA.
    C. AUP.
    D. MOU.

14. Jean ha recentemente completato il processo di test di accettazione e sta preparando il suo codice per la distribuzione. Quale ambiente dovrebbe ospitare il suo codice prima che venga rilasciato per l'uso?
    A. Test.
    B. Produzione.
    C. Sviluppo.
    D. Staging.

15. Rob ha creato un documento che descrive come il personale può utilizzare i dispositivi di proprietà dell'azienda, incluso se e quando è consentito il loro uso personale. Che tipo di policy ha creato Rob?
    A. Una policy di gestione delle modifiche.
    B. Una policy di utilizzi accettabili.
    C. Una policy di controllo degli accessi.
    D. Un playbook.

16. Oren ha ottenuto un certificato per il suo dominio che copre `*.acmewidgets.net`. Quale dei seguenti domini non sarebbe coperto da questo certificato?
    A. `www.acmewidgets.net`.
    B. `acmewidgets.net`.
    C. `test.mail.acmewidgets.net`.
    D. `mobile.acmewidgets.net`.

17. Richard sta inviando un messaggio a Grace e vorrebbe applicargli una firma digitale prima di inviarlo. Quale chiave deve utilizzare per creare la firma digitale?
    A. La propria chiave privata.
    B. La propria chiave pubblica.
    C. La chiave privata di Grace
    D. La chiave pubblica di Grace

18. Stephanie sta esaminando un database delle transazioni dei clienti e si imbatte nella tabella dei dati seguente. Quale tecnica di minimizzazione dei dati è stata probabilmente utilizzata per oscurare le informazioni della carta di credito in questa tabella?

Numero ordine	Importo	Data	Numero carta di credito
1023	$25.684	10/7/2023	c4ca4238a0b923820dcc509a6f75849b
1024	$65.561	12/6/2023	c81e728d9d4c2f636f067f89cc14862c
1025	$44.015	11/7/2023	eccbc87e4b5ce2fe28308fd9f2a7baf3
1026	$89.553	7/6/2023	a87ff679a2f3e71d9181a67b7542122c
1027	$50.316	10/16/2023	e4da3b7fbbce2345d7772b0674a318d5
1028	$39.200	5/3/2023	b53b3a3d6ab90ce0268229151c9bde11
1029	$67.897	3/1/2023	6364d3f0f495b6ab9dcf8d3b5c6e0b01
1030	$98.141	1/21/2023	5821bb96cd2066d808a7b64b5b58b394
1031	$13.851	10/29/2023	89d948e603f12c523728803d61347951
1032	$60.475	3/13/2023	b02ac13e3fadb4ecf1874b34087eb096
1033	$67.207	9/15/2023	1ed3c76c640836c99be028b261311643
1034	$2.525	10/9/2023	e53a0a2978c28872a4505bdb51db06dc
1035	$66.399	3/5/2023	4903e02b3b0ae4b6b824a0a4c187e5c5
1036	$37.676	11/4/2023	8fd7e6c0a7120aa9778b5fb08a1fa8ee

    A. Distruzione.
    B. Mascheramento.
    C. Hashing.
    D. Tokenizzazione.

19. Andrew sta collaborando con il suo team finanziario per acquistare una polizza assicurativa sulla sicurezza informatica per coprire l'impatto finanziario di una violazione dei dati. Che tipo di strategia di gestione dei rischi sta utilizzando?
    A. Prevenzione del rischio.
    B. Trasferimento del rischio.
    C. Accettazione del rischio.
    D. Mitigazione dei rischi.

20. Shelly sta scrivendo un documento che descrive i passaggi che i team di risposta agli incidenti seguiranno al primo avviso di un potenziale incidente. Che tipo di documento sta creando?
    A. Linee guida.
    B. Uno standard.

C. Una procedura.
D. Una policy.

Risposte al test di valutazione

1. **C.** Il motivo più comune per disattivare l'applicazione automatica delle patch è evitare problemi con patch e aggiornamenti problematici o imperfetti. Nella maggior parte degli ambienti, la necessità di applicare regolarmente le patch è accettata e gestita senza causare interruzioni significative. Tale preoccupazione sarebbe diversa se i sistemi sottoposti a patch facessero parte di un processo industriale o di un ambiente di produzione in fabbrica. Le patch dannose provenienti da fonti legittime come un repository di aggiornamenti automatici sono eccezionalmente rare e non rappresentano una preoccupazione comune o una motivazione forte per questo tipo di comportamento. Per ulteriori informazioni, vedere il Capitolo 11.
2. **B.** I file log, insieme a qualsiasi file archiviato su disco senza l'intenzione di essere sovrascritto frequentemente, sono gli elementi meno volatili fra quelli elencati. L'ordine dalle risposte alle più volatili prevede i registri della CPU, la tabella di routing del sistema, i file temporanei e i file log. Per ulteriori informazioni, vedere il Capitolo 15.
3. **A.** Se Ed riesce a dissociare il suo obiettivo dall'Access Point cui è attualmente connesso, può utilizzare una potenza di trasmissione più elevata o un Access Point più vicino per apparire più in cima nell'elenco degli Access Point. Se riesce a ingannare l'utente o il sistema inducendolo a connettersi al suo Access Point, può poi condurre attacchi on-path o tentare altri exploit. È improbabile che degli attacchi denial-of-service causino l'associazione di un sistema a un altro Access Point e un attacco di puro testo è un tipo di attacco crittografico e non è utile per questo tipo di tentativo. Per ulteriori informazioni, vedere il Capitolo 12.
4. **D.** Le indagini sul sito che mostrano la potenza relativa su una mappa o un diagramma sono chiamate heatmap. Possono aiutare a mostrare dove gli Access Point forniscono un segnale forte e dove più Access Point potrebbero essere in competizione tra loro a causa della sovrapposizione dei canali o di altri problemi. Possono anche aiutare a identificare le zone morte dove il segnale non arriva. Per fare ciò occorre condurre Signal Survey, db map e AP topology. Per ulteriori informazioni, vedere il Capitolo 13.
5. **D.** Una base di attendibilità hardware fornisce un elemento univoco che significa che una scheda o un dispositivo non può essere replicato. Per fornire la base di attendibilità hardware viene comunemente utilizzato un TPM (*Trusted Platform Module*). La CPU e la memoria di sistema non sono univoche per i comuni desktop e laptop e un HSM (*Hardware Security Module*) viene utilizzato per creare, gestire e archiviare certificati crittografici nonché per eseguire e scaricare operazioni crittografiche. Per ulteriori informazioni, vedere il Capitolo 11.
6. **A.** Angela deve conservare una cronologia delle password e impostare un'età minima per la password, in modo che gli utenti non possano semplicemente reimpostare una vecchia password finché non l'avranno cambiata abbastanza volte da oltrepassare la cronologia. Per ulteriori informazioni, vedere il Capitolo 8.

7. **C.** Gli hot site sono sempre pronti a subentrare nelle attività in tempo reale. I cold site in genere sono semplicemente sistemi già pronti con l'infrastruttura di base necessaria per creare un sito. I siti clone e i ready site non sono termini utilizzati nel settore. Per ulteriori informazioni, vedere il Capitolo 9.
8. **B.** I sistemi embedded e specializzati tendono ad avere CPU a basso consumo, meno memoria, meno spazio di archiviazione e spesso potrebbero non essere in grado di gestire attività a uso intensivo della CPU, come gli algoritmi crittografici o gli strumenti di sicurezza built-in. Pertanto, la presenza di un firewall è relativamente improbabile, soprattutto se non è integrata la connettività di rete o se si prevede che il dispositivo operi su una rete sicura. Per ulteriori informazioni, vedere il Capitolo 11.
9. **A.** Un attacco con dizionario utilizzerà una serie di password probabili, insieme a loro varianti comuni per tentare di violare un account. Gli accessi ripetuti per un singolo ID utente con iterazioni di varie password sono probabilmente un attacco a dizionario. Una rainbow table viene utilizzata per abbinare una password con hash alla password che è stata sottoposta ad hashing con quel valore. Un attacco pass-the-hash fornisce un codice hash di autenticazione catturato per provare a operare come un utente autorizzato. Un attacco a spraying di password utilizza una password nota (spesso derivante da una violazione) per tentare di accedere ad altri siti differenti. Per ulteriori informazioni, vedere il Capitolo 4.
10. **D.** I jump server sono sistemi utilizzati per fornire una presenza e un percorso di accesso fra zone di sicurezza differente. VDI è un'infrastruttura desktop virtuale e viene utilizzata per fornire sistemi virtuali controllati per la produttività e la presentazione delle applicazioni, tra le altre cose. Un container è un modo per fornire a un'applicazione un ambiente scalabile e prevedibile senza disporre di un sistema virtuale sottostante completo; una sottorete schermata è una zona protetta esposta a un'area o una popolazione avente un livello di affidabilità inferiore. Per ulteriori informazioni, vedere il Capitolo 12.
11. **C.** L'azienda di Derek è preoccupata per le minacce interne o per le minacce create dai dipendenti e da altri elementi dell'azienda o che godono in qualche modo della fiducia dell'azienda. L'ingegneria sociale prevede di ingannare qualcuno per consentire a un estraneo di raggiungere i suoi obiettivi. Il phishing tenta di acquisire informazioni personali attraverso l'ingegneria sociale e altre tecniche, mentre lo Shoulder Surfing è una tecnica in cui un malintenzionato osserva alle spalle qualcuno per acquisire informazioni come password o numeri di carta di credito. Per ulteriori informazioni, vedere il Capitolo 2.
12. **A.** I controlli correttivi risolvono i problemi relativi alla sicurezza che si sono già verificati. Il ripristino dai backup dopo un attacco ransomware è un esempio di controllo correttivo. I controlli preventivi tentano di fermare futuri problemi. I controlli di rilevamento si concentrano sul rilevamento di problemi ed eventi, mentre i controlli di deterrenza tentano di scoraggiare azioni ostili. Per ulteriori informazioni, vedere il Capitolo 1.
13. **C.** Questa attività rappresenta quasi certamente una violazione della policy aziendale di utilizzo accettabile (AUP), che dovrebbe contenere disposizioni che descrivano l'uso appropriato delle reti e delle risorse IT appartenenti all'azienda. BPA non è

un termine comune, in questo contesto. Gli accordi sul livello di servizio (SLA) determinano un livello di servizio minimo concordato e i MOU, o memorandum d'intesa, vengono utilizzati per documentare gli accordi tra le aziende. Vedere il Capitolo 16 per ulteriori informazioni.

14. **D.** L'ambiente di staging è un ambiente di transizione per il codice che ha superato con successo i test ed è in attesa di essere distribuito in produzione. È qui che dovrebbe risiedere il codice prima di essere rilasciato per l'uso. L'ambiente di sviluppo è il luogo in cui gli sviluppatori lavorano sul codice prima di prepararlo per la distribuzione. L'ambiente di test è il luogo in cui è possibile sottoporre a test il software o i sistemi senza influire sull'ambiente di produzione. L'ambiente di produzione è il sistema live. Il software, le patch e altre modifiche che sono state sottoposte a test e approvate passano alla produzione. Per ulteriori informazioni, vedere il Capitolo 6.
15. **B.** Le policy di utilizzi accettabili definiscono il modo in cui possono e devono essere utilizzati i sistemi, i dispositivi e i servizi dell'azienda. Le policy di gestione delle modifiche determinano il modo in cui un'azienda gestisce le modifiche e il controllo delle modifiche. La documentazione del controllo degli accessi viene generalmente gestita come standard e i playbook descrivono come eseguire determinati compiti o processi.
16. **C.** I certificati jolly proteggono il dominio elencato e tutti i sottodomini di primo livello. `test.mail.acmewidgets.net` è un sottodominio di secondo livello di `acmewidgets.net` e non sarebbe coperto da questo certificato. Per ulteriori informazioni, vedere il Capitolo 7.
17. **A.** Il mittente di un messaggio può firmare digitalmente il messaggio crittografando un digest del messaggio con la propria chiave privata. Per ulteriori informazioni, vedere il Capitolo 7.
18. **C.** Questi dati assomigliano molto a dati con hash, poiché i campi hanno tutti la stessa lunghezza e sembrano contenere dati privi di significato ma univoci. Se il campo fosse tokenizzato, sarebbe più probabile trovare un numero sequenziale o un altro identificatore riconoscibile. Se il campo fosse mascherato, conterrebbe asterischi o altri caratteri segnaposto. Per ulteriori informazioni, vedere il Capitolo 1.
19. **B.** L'acquisto di un'assicurazione è l'esempio più comune di trasferimento del rischio, ovvero il trasferimento della responsabilità a terzi. L'evitamento implica sforzi per prevenire che il rischio si verifichi, l'accettazione è semplicemente accettare formalmente che il rischio possa verificarsi; i tentativi di mitigazione servono per limitare l'impatto del rischio. Per ulteriori informazioni, vedere il Capitolo 17.
20. **C.** Le procedure forniscono una serie di istruzioni dettagliate a "lista di controllo" che guidano il modo in cui i dipendenti dovrebbero reagire in una determinata circostanza. Le procedure guidano comunemente le prime fasi della risposta agli incidenti. Gli standard definiscono il modo in cui come dovrebbero essere implementate le policy. Le linee guida sono puramente volontarie, mentre le policy impongono un obbligo. Per ulteriori informazioni, vedere il Capitolo 16.

Gli autori

Mike Chapple, Ph.D., Security+, CySA+, *CISSP*, è autore del best-seller *CISSP (ISC)² Certified Information Systems Security Professional Study Guide* (Sybex, 2021) e *CISSP (ISC)² Official Practice Tests* (Sybex, 2021). È un professionista della sicurezza informatica che vanta vent'anni di esperienza nell'istruzione superiore, nel settore privato e governativo. Mike attualmente è professore nel dipartimento *IT, Analytics, and Operations* presso il Mendoza College of Business dell'Università di Notre Dame (Indiana), dove tiene corsi universitari e di laurea su argomenti come la sicurezza informatica, la gestione dei dati e l'analisi aziendale.
Prima di tornare alla Notre Dame, Mike è stato vicepresidente esecutivo e responsabile delle informazioni del Brand Institute, una società di consulenza marketing con sede a Miami. Ha anche trascorso quattro anni nel gruppo di ricerca sulla sicurezza informatica presso la National Security Agency e ha prestato servizio come ufficiale dell'intelligence in servizio attivo per l'aeronautica americana.
Mike è editor tecnico di "Information Security Magazine" e ha scritto più di 25 libri. Ha conseguito sia la laurea che il dottorato alla Notre Dame in computer science e ingegneria. Ha inoltre conseguito un master in computer science presso l'Università dell'Idaho e un master in business administration presso l'Auburn University. Possiede, inoltre, le certificazioni CySA+ (*Cybersecurity Analyst+*), Security+, CISM (*Certified Information Security Manager*), CCSP (*Certified Cloud Security Professional*) e CISSP (*Certified Information Systems Security Professional*).
Per ulteriori informazioni su Mike e sui suoi materiali di certificazione IT consultate il suo sito web, `https://www.certmike.com`.

David Seidl, *CySA+, CISSP, Pentest+,* è vicepresidente per il settore Information Technology e CIO presso l'Università di Miami, dove guida un pluripremiato team di professionisti IT. Nella sua carriera ha ricoperto diversi ruoli tecnici e di sicurezza delle informazioni, tra cui il ruolo di direttore senior per i servizi tecnologici del campus presso l'Università di Notre Dame, dove ha co-diretto il passaggio della Notre Dame al cloud e ha supervisionato le sue attività nel cloud, l'implementazione dell'ERP, dei database, la gestione delle identità e vari altri servizi e tecnologie. Ha ricoperto anche il ruolo di direttore della sicurezza informatica alla Notre Dame e ha guidato il programma di sicurezza informatica dell'università. Ha tenuto corsi universitari sulla sicurezza delle informazioni e sulle reti come istruttore per il Mendoza College of Business di Notre Dame. È un autore di best-seller, specializzato in certificazione della sicurezza informatica e guerra informatica e ha scritto oltre 20 libri sull'argomento.
David ha conseguito una laurea in tecnologie della comunicazione e un master in sicurezza delle informazioni presso la Eastern Michigan University ed è dotato delle certificazioni CISSP, CySA+, Pentest+, GPEN e GCIH.

L'editor tecnico

Chris Crayton, MCSE, CISSP, CASP+, CySA+, A+, N+, S+, è un consulente tecnico, formatore, autore e capo editor tecnico. Ha lavorato come istruttore nel campo delle tecnologie informatiche e di rete, direttore della sicurezza delle informazioni, ammi-

nistratore di rete, tecnico di rete e specialista di PC. Ha lavorato come editor tecnico e collaboratore per numerosi titoli tecnici per molte grandi case editrici. È stato anche insignito di numerosi premi professionali e didattici.

Il redattore tecnico

Shahla Pirnia è una redattrice tecnica freelance e correttrice di bozze specializzata nei temi della sicurezza informatica e della certificazione. Attualmente ricopre il ruolo di editor tecnico per `CertMike.com`, dove lavora su progetti tra cui libri, corsi video e prove pratiche.
Ha conseguito le lauree in Computer and Information Science e Psicologia presso il Global Campus dell'Università del Maryland, insieme a una laurea AA in Information Systems presso il Montgomery College, Maryland. Le certificazioni IT di Shahla includono CompTIA Security+, Network+, A+ e ISC2 CC.

Ringraziamenti

Libri come questo coinvolgono il lavoro di molte persone e, come autori, abbiamo apprezzato molto il duro lavoro e la dedizione dimostrati dal team di Wiley. Vorremmo ringraziare in particolare il senior acquisitions editor Kenyon Brown. Abbiamo collaborato con lui per molteplici progetti e apprezziamo costantemente il suo lavoro.
Sentiamo un grosso debito di gratitudine nei confronti di Runzhi "Tom" Song, assistente di ricerca di Mike a Notre Dame. Il supporto di Tom con i materiali didattici che accompagnano questo libro è stato inestimabile.
Abbiamo molto apprezzato anche il lavoro del team di editing e produzione di questo libro, inclusa Lily Miller, la nostra project editor, che ha portato al progetto i suoi anni di esperienza e il suo grande talento; Chris Crayton, il nostro editor tecnico, e Shahla Pirnia, il nostro redattore tecnico, ci hanno fornito utili consigli e garantito feedback preziosi un po' in tutto il libro; Saravanan Dakshinamurthy, il nostro production editor, ci ha guidato attraverso l'impaginazione, la formattazione e la pulizia finale, per mettere insieme un grande libro. Vorremmo anche ringraziare i numerosi contributori che hanno lavorato dietro le quinte, compresi i team grafici, di produzione e tecnici, che hanno trasformato il libro e i materiali di accompagnamento in un prodotto finito.
La nostra agente, Carole Jelen di Waterside Productions, continua a fornirci meravigliose opportunità, consigli e assistenza nel corso di tutta la nostra carriera di scrittori.
Infine, vorremmo ringraziare le nostre famiglie e le persone che amiamo, per il loro sostegno a tarda sera, nei fine settimana e nelle lunghe ore impegnate a scrivere, correggere e mandare in stampa questo libro.