

فهرست مطالب

۱۵.....	مقدمه ناشر
۱۶.....	سخنی از مترجم کتاب
۱۷.....	درباره مترجم
۱۸.....	مقدمه
۱۸.....	دوره آموزشی CompTIA Security+
۱۹.....	نسخه SY0-701
۲۰.....	خلاصه‌سازی کتاب
۲۰.....	فصل اول: مفاهیم امنیتی
۲۰.....	فصل دوم: شبکه‌های امن
۲۱.....	فصل سوم: تهدیدات امنیتی و حملات
۲۱.....	فصل چهارم: رمزنگاری و امنیت داده
۲۱.....	فصل پنجم: امنیت برنامه‌ها و دستگاه‌ها
۲۱.....	فصل ششم: مدیریت امنیت
۲۲.....	فصل هفتم: آموزش و آگاهی امنیتی
۲۲.....	فصل هشتم: مسائل قانونی حوزه امنیت اطلاعات

فصل اول

۲۳.....	مفاهیم امنیتی
۲۴.....	اصول و مفاهیم اصلی امنیت اطلاعات
۲۵.....	۱. محرمانگی
۲۵.....	تعریف و اهمیت محرمانگی
۲۵.....	تکنیک‌ها و ابزارهای حفظ محرمانگی
۲۵.....	۱. رمزنگاری
۲۷.....	۲. کنترل‌های دسترسی
۲۸.....	۳. سیاست‌های امنیتی و آموزش کاربران
۲۸.....	۴. مدیریت کلید

۲۸.....	۵. استفاده از شبکه‌های امن
۲۹.....	اهمیت و چالش‌های حفظ محرمانگی
۳۰.....	۲. یکپارچگی
۳۰.....	تعریف و اهمیت یکپارچگی
۳۰.....	تکنیک‌ها و ابزارهای حفظ یکپارچگی
۳۰.....	۱. الگوریتم‌های هش
۳۶.....	۲. امضاهای دیجیتال
۳۹.....	۳. کنترل نسخه و سیستم‌های مدیریت تغییرات
۴۲.....	۴. سیستم‌های تشخیص نفوذ (IDS)
۴۲.....	انواع سیستم‌های تشخیص نفوذ (IDS)
۴۳.....	تفاوت‌های اصلی بین NIDS و HIDS
۴۳.....	نحوه عملکرد سیستم‌های تشخیص نفوذ
۴۶.....	۵. کنترل دسترسی و احراز هویت قوی
۴۷.....	۳. در دسترس‌پذیری
۵۲.....	اهمیت مدل CIA در امنیت اطلاعات

فصل دوم

۵۳.....	شبکه‌های امن
۵۴.....	مبانی امنیت شبکه
۵۵.....	معرفی مفاهیم اولیه امنیت شبکه
۵۵.....	تهدیدات و آسیب‌پذیری‌های معمول شبکه
۵۶.....	تفاوت بین شبکه‌های عمومی و خصوصی و اهمیت هر کدام در امنیت
۵۷.....	تجهیزات امنیتی شبکه
۵۷.....	فایروال
۵۸.....	سیستم‌های تشخیص و پیشگیری از نفوذ (IDS/IPS)
۵۸.....	عملکرد IDS و IPS
۵۹.....	نحوه استفاده از IDS و IPS در شناسایی و جلوگیری از حملات
۵۹.....	پروکسی سرورها و VPN‌ها
۶۰.....	کاربردهای اصلی VPN

۶۱.....	تجهیزات امنیتی ابزار حیاتی.....
۶۱.....	پروتکل ها و استانداردهای امنیتی.....
۶۱.....	پروتکل های رمزنگاری شبکه.....
۶۱.....	پروتکل SSL/TLS.....
۶۲.....	پروتکل IPsec.....
۶۲.....	استانداردهای احراز هویت و کنترل دسترسی در شبکه ها.....
۶۲.....	پروتکل RADIUS.....
۶۳.....	پروتکل TACACS+.....
۶۳.....	پروتکل 802.1X.....
۶۳.....	پروتکل های امن انتقال فایل.....
۶۴.....	پروتکل SFTP.....
۶۴.....	پروتکل FTPS.....
۶۴.....	طراحی و معماری شبکه امن.....
۶۵.....	بخش بندی شبکه.....
۶۵.....	معماری شبکه Zero Trust.....
۶۶.....	ایجاد و مدیریت DMZ.....
۶۷.....	امنیت در شبکه های بی سیم.....
۶۷.....	چالش ها و تهدیدات خاص شبکه های بی سیم.....
۶۸.....	استانداردهای امنیتی برای Wi-Fi.....
۶۸.....	WEP.....
۶۹.....	WPA.....
۶۹.....	WPA2.....
۶۹.....	WPA3.....
۷۰.....	بهترین روش ها برای ایمن سازی شبکه های بی سیم.....
۷۲.....	پایش و مانیتورینگ امنیت شبکه.....
۷۲.....	ابزارهای مانیتورینگ شبکه.....
۷۲.....	Wireshark.....
۷۲.....	SolarWinds.....
۷۳.....	اهمیت پایش مداوم شبکه.....

تنظیم هشدارها و گزارش گیری ۷۴

فصل سوم

تهدیدات امنیتی و حملات ۷۵

بدافزارها و انواع آن ۷۶

ویروس ها ۷۷

کرم ها ۷۷

تروجان ها ۷۷

باج افزارها ۷۷

جاسوس افزارها ۷۸

نحوه شناسایی و مقابله با بدافزارها ۷۸

تحلیل رفتارهای بدافزارها و ابزارهای ضدبدافزار ۷۸

حملات مبتنی بر شبکه ۷۹

DDoS و DoS ۷۹

روش های مقابله ۸۰

MITM ۸۰

روش های مقابله ۸۰

شنود ۸۰

روش های مقابله ۸۰

اسکن پورت و نفوذ به شبکه ۸۱

روش های مقابله ۸۱

مهندسی اجتماعی ۸۱

فیشینگ ۸۲

ویشینگ ۸۲

اسپیرفیشینگ ۸۲

تکنیک های حملات مبتنی بر روان شناسی ۸۳

روش های پیشگیری از حملات مهندسی اجتماعی ۸۳

تهدیدات داخلی ۸۴

کارکنان ناراضی یا بی احتیاطی انسانی ۸۵

۸۵.....	حملات ناشی از دسترسی غیرمجاز داخلی
۸۵.....	استراتژی‌های مدیریت و کاهش تهدیدات داخلی
۸۶.....	حملات هدفمند و پیشرفته
۸۷.....	ویژگی‌های حملات APT و اهداف آنها
۸۷.....	مراحل اجرای حملات هدفمند
۸۸.....	ابزارها و روش‌های دفاع در برابر APT
۸۹.....	حملات روز صفر
۹۰.....	توضیح مفهوم آسیب‌پذیری‌های روز صفر
۹۰.....	مثال‌هایی از حملات روز صفر
۹۱.....	شناسایی و کاهش تأثیر آسیب‌پذیری‌های روز صفر
۹۲.....	ابزارها و تکنیک‌های تحلیل تهدیدات
۹۳.....	ابزارهای شناسایی و تحلیل حملات
۹۳.....	Snort
۹۳.....	Suricata
۹۳.....	تحلیل ترافیک شبکه و رفتارهای مشکوک
۹۴.....	روش‌های پاسخ به حوادث امنیتی

فصل چهارم

۹۵.....	رمزنگاری و امنیت داده
۹۶.....	اصول رمزنگاری، تکنیک‌های رمزنگاری متقارن و نامتقارن
۹۷.....	رمزنگاری متقارن
۹۷.....	مفاهیم کلیدی در رمزنگاری متقارن
۹۷.....	ویژگی‌ها و مزایای رمزنگاری متقارن
۹۷.....	چالش‌های رمزنگاری متقارن
۹۸.....	الگوریتم‌های رایج در رمزنگاری متقارن
۹۸.....	کاربردهای رمزنگاری متقارن
۹۸.....	یک مثال ساده از رمزنگاری متقارن
۹۹.....	رمزنگاری نامتقارن
۹۹.....	مفاهیم کلیدی در رمزنگاری نامتقارن

۹۹.....	ویژگی‌ها و مزایای رمزنگاری نامتقارن
۱۰۰.....	الگوریتم‌های رایج در رمزنگاری نامتقارن
۱۰۰.....	مثال کاربردی از رمزنگاری نامتقارن
۱۰۰.....	کاربردهای رمزنگاری نامتقارن
۱۰۱.....	چالش‌ها و محدودیت‌ها
۱۰۲.....	الگوریتم‌های رمزنگاری متداول و کاربردهای آنها
۱۰۲.....	AES
۱۰۲.....	RSA
۱۰۲.....	ECC
۱۰۲.....	DES
۱۰۳.....	3DES
۱۰۳.....	SHA
۱۰۳.....	Twofish و Blowfish
۱۰۳.....	Diffie-Hellman Key Exchange
۱۰۴.....	کاربردهای کلی الگوریتم‌های رمزنگاری
۱۰۴.....	الگوریتم‌های رمزنگاری: نحوه کار، کاربردها و ویژگی‌ها
۱۰۵.....	کنترل‌های حفاظت از داده در حالات انتقال و سکون
۱۰۶.....	راهکارهای جلوگیری از نشت داده‌ها

فصل پنجم

۱۰۸.....	امنیت برنامه‌ها و دستگاه‌ها
۱۰۹.....	امنیت نرم‌افزار و اصول برنامه‌نویسی امن
۱۱۱.....	آسیب‌پذیری‌های نرم‌افزاری و حملات به اپلیکیشن‌ها
۱۱۱.....	تزریق SQL
۱۱۲.....	روش‌های پیشگیری
۱۱۲.....	حملات XSS
۱۱۲.....	روش‌های پیشگیری
۱۱۳.....	حملات CSRF
۱۱۳.....	روش‌های پیشگیری

۱۱۳	امنیت دستگاه‌های همراه و IoT
۱۱۴	امنیت دستگاه‌های همراه
۱۱۵	امنیت IoT
۱۱۵	شناسایی تهدیدات خاص در دستگاه‌های همراه و IoT
۱۱۶	روش‌های مقابله با تهدیدات دستگاه‌های همراه و IoT
۱۱۶	پیاده‌سازی کنترل‌های امنیتی بر روی دستگاه‌ها و نرم‌افزارها
۱۱۶	رمزنگاری برای حفاظت از داده‌ها
۱۱۷	MFA
۱۱۷	پیکربندی امن دستگاه‌ها و نرم‌افزارها
۱۱۸	مدیریت به‌روزرسانی‌ها

فصل ششم

۱۱۹	مدیریت امنیت
۱۲۱	ISMS
۱۲۱	تعریف ISMS و اهداف آن
۱۲۲	اهداف اصلی ISMS
۱۲۲	استاندارد ISO/IEC 27001
۱۲۲	اجزای کلیدی ISMS
۱۲۳	مراحل پیاده‌سازی ISMS
۱۲۴	مثال‌های عملی استفاده از ISMS
۱۲۴	مزایای ISMS
۱۲۵	مدیریت دسترسی و احراز هویت
۱۲۵	احراز هویت
۱۲۶	MFA
۱۲۶	روش‌های بیومتریک
۱۲۶	احراز هویت مبتنی بر توکن
۱۲۷	مدیریت دسترسی
۱۲۷	کنترل دسترسی مبتنی بر نقش (RBAC)
۱۲۷	کنترل دسترسی مبتنی بر ویژگی (ABAC)

۱۲۷	مدیریت دسترسی پویا
۱۲۷	IAM
۱۲۸	ویژگی‌های کلیدی IAM
۱۲۹	مثال‌هایی از استفاده IAM
۱۲۹	فوائد پیاده‌سازی IAM
۱۳۰	پیاده‌سازی ابزارهای مدیریتی
۱۳۰	فایروال
۱۳۱	نحوه کارکرد فایروال‌ها
۱۳۱	برندهای معروف فایروال‌ها
۱۳۲	جایگاه فایروال‌ها در شبکه
۱۳۲	نحوه کار با فایروال‌ها
۱۳۳	IDS/IPS
۱۳۳	IDS
۱۳۳	IPS
۱۳۴	کارکردهای IDS/IPS
۱۳۴	SIEM
۱۳۴	نحوه عملکرد SIEM
۱۳۶	ویژگی‌های کلیدی SIEM
۱۳۶	کاربردهای SIEM
۱۳۶	مزایای استفاده از SIEM
۱۳۷	چالش‌های استفاده از SIEM
۱۳۷	برندهای معروف SIEM
۱۳۸	برنامه‌های مدیریت و پاسخ به حوادث امنیتی
۱۳۸	تعریف حادثه امنیتی
۱۳۸	اهداف برنامه‌های مدیریت و پاسخ به حوادث
۱۳۸	مراحل برنامه‌های مدیریت و پاسخ به حوادث امنیتی
۱۳۹	نقش ابزارها در مدیریت و پاسخ به حوادث
۱۴۰	ساختار تیم مدیریت حوادث امنیتی
۱۴۰	مثال عملی از یک برنامه مدیریت حوادث

مزایای برنامه‌های مدیریت و پاسخ به حوادث ۱۴۱

فصل هشتم

آموزش و آگاهی امنیتی ۱۴۲

- اهمیت آگاهی‌بخشی امنیتی به کارمندان و آموزش‌های مربوط به تهدیدات ۱۴۴
- چرا آگاهی‌بخشی امنیتی اهمیت دارد؟ ۱۴۴
- مهم‌ترین تهدیداتی که کارمندان باید آموزش ببینند ۱۴۵
- مزایای آموزش‌های امنیتی به کارمندان ۱۴۵
- چگونه آگاهی‌بخشی امنیتی به‌طور مؤثر انجام شود؟ ۱۴۶
- چالش‌های آگاهی‌بخشی امنیتی ۱۴۶
- مقاومت کارکنان در برابر آموزش امنیتی ۱۴۶
- دلایل مقاومت ۱۴۷
- راهکارها ۱۴۷
۱. تغییرات سریع تهدیدات سایبری ۱۴۷
۲. محدودیت منابع (مالی و انسانی) ۱۴۷
۳. عدم درک اهمیت امنیت توسط کارکنان ۱۴۸
۴. پیچیدگی محتوا و روش آموزش ۱۴۸
۵. نبود ارزیابی مناسب اثربخشی آموزش‌ها ۱۴۹
- ایجاد انگیزه برای رعایت مسائل امنیتی ۱۴۹
- مشکلات انگیزشی ۱۴۹
- راهکارها ۱۵۰
- ایجاد برنامه آموزشی امنیتی ۱۵۰
۱. شناسایی نیازها و اهداف آموزشی ۱۵۰
- مثال ۱۵۰
۲. تقسیم‌بندی مخاطبان ۱۵۱
- مثال ۱۵۱
۳. طراحی محتوای آموزشی ۱۵۱
- روش‌های ارائه محتوا ۱۵۱
- مثال ۱۵۲

۴. انتخاب روش‌های آموزش	۱۵۲
مثال	۱۵۲
۵. برگزاری آموزش‌ها	۱۵۲
۶. ارزیابی اثربخشی آموزش‌ها	۱۵۲
روش‌های ارزیابی	۱۵۲
مثال	۱۵۳
۷. به‌روزرسانی مداوم برنامه‌ها	۱۵۳
راهکارها	۱۵۳
۸. ایجاد فرهنگ امنیتی در سازمان	۱۵۳
روش‌های ایجاد فرهنگ امنیتی	۱۵۳
مدیریت سیاست‌ها و رویه‌های امنیتی برای پیشگیری از حملات داخلی و انسانی	۱۵۴
اهمیت سیاست‌ها و رویه‌های امنیتی	۱۵۴
حملات داخلی و انسانی	۱۵۴
تهدیدات داخلی	۱۵۴
تهدیدات انسانی خارجی	۱۵۵
طراحی و اجرای سیاست‌های امنیتی	۱۵۵
۱. تحلیل نیازها و ریسک‌ها	۱۵۵
۲. تعریف سیاست‌های دسترسی و استفاده از اطلاعات	۱۵۵
۳. آموزش و آگاهی کارکنان	۱۵۵
۴. تعریف رویه‌های گزارش‌دهی	۱۵۵
۵. پیاده‌سازی ابزارهای مدیریتی	۱۵۶
مثال‌هایی از سیاست‌های امنیتی برای پیشگیری از تهدیدات داخلی و انسانی	۱۵۶
پیشگیری از تهدیدات داخلی و انسانی	۱۵۶
نحوه ایجاد انگیزه برای رعایت مسائل امنیتی در محیط کار	۱۵۷
نحوه ایجاد انگیزه در رعایت مسائل امنیتی	۱۵۷
اهمیت ایجاد انگیزه برای رعایت مسائل امنیتی	۱۵۸
چالش‌های ایجاد انگیزه در کارکنان	۱۵۸
راهکارهای ایجاد انگیزه برای رعایت مسائل امنیتی	۱۵۹
۱. آموزش و آگاهی‌بخشی با روش‌های جذاب و تعاملی	۱۵۹

۱۵۹	۲. ایجاد فرهنگ امنیتی در سازمان
۱۵۹	۳. پاداش‌دهی و تقدیر از رفتارهای امنیتی مثبت
۱۶۰	۴. ساده‌سازی سیاست‌ها و رویه‌های امنیتی
۱۶۰	۵. ارتباط دادن امنیت به موفقیت سازمانی
۱۶۰	۶. استفاده از ابزارهای تعاملی و تکنولوژی
۱۶۱	۷. تشویق رفتارهای امنیتی از طریق رقابت سالم
۱۶۱	۸. ارائه بازخورد مداوم

فصل هشتم

۱۶۲	مسائل قانونی حوزه امنیت اطلاعات
۱۶۳	آشنایی با قوانین و مقررات بین‌المللی و محلی مرتبط با امنیت اطلاعات
۱۶۴	چگونه استاندارد GDPR اجرا می‌شود؟
۱۶۴	اهداف اصلی GDPR
۱۶۴	ویژگی‌ها و الزامات کلیدی GDPR
۱۶۵	چرا GDPR مهم است؟
۱۶۵	مزایای GDPR
۱۶۵	پیاده‌سازی CCPA
۱۶۶	پیاده‌سازی LGPD
۱۶۶	استانداردها و چهارچوب‌های امنیتی مانند ISO 27001 و NIST
۱۶۷	ISO/IEC 27001: استاندارد سیستم مدیریت امنیت اطلاعات
۱۶۷	هدف و اهمیت ISO 27001
۱۶۷	ساختار استاندارد ISO 27001
۱۶۷	بخش‌های اصلی استاندارد
۱۶۸	فرآیند پیاده‌سازی ISO 27001
۱۶۹	الزامات پیوست A در ISO 27001
۱۶۹	مزایای ISO 27001
۱۶۹	گواهینامه ISO 27001
۱۷۰	استانداردها و چهارچوب‌های امنیتی NIST
۱۷۰	اهمیت NIST در امنیت اطلاعات

۱۷۰	چهارچوب‌ها و استانداردهای اصلی NIST
۱۷۲	چگونه NIST در سازمان‌ها اجرا می‌شود؟
۱۷۲	مزایای استفاده از استانداردهای NIST
۱۷۳	مدیریت انطباق سازمان با مقررات و الزامات قانونی
۱۷۳	فرآیند مدیریت انطباق
۱۷۳	۱. شناسایی الزامات قانونی
۱۷۳	۲. ارزیابی وضعیت فعلی سازمان
۱۷۳	۳. تدوین سیاست‌ها و فرآیندهای انطباق
۱۷۴	۴. پیاده‌سازی اقدامات کنترلی
۱۷۴	۵. انتصاب یک مسئول انطباق (Compliance Officer)
۱۷۴	۶. نظارت و ارزیابی مداوم
۱۷۴	مزایای مدیریت انطباق
۱۷۵	چالش‌های مدیریت انطباق
۱۷۵	اصول حاکمیت امنیت اطلاعات و ممیزی‌های امنیتی
۱۷۵	اصول حاکمیت امنیت اطلاعات
۱۷۶	ممیزی‌های امنیتی
۱۷۶	انواع ممیزی‌های امنیتی
۱۷۶	مراحل یک ممیزی امنیتی
۱۷۷	نمونه یک ممیزی امنیتی: بررسی انطباق با ISO 27001