



مؤسسه فرهنگی هنری
دیباگران تهران

به نام خدا

برگزیده

CompTIA

Security + SYO-701

ترجمه و تالیف:

سجاد دلیری



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: برگزیده CompTIA Security + SYO-701

◀ تالیف و ترجمه: سجاد دلیری

◀ ناشر: مؤسسه فرهنگی هنری دیباگران تهران

◀ ویراستار: پروین عبدی

◀ صفحه آرایی: نازنین نصیری

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۴۰۳

◀ چاپ و صحافی: صدف

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۲۵۰۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۹۰۸-۲

◀ نشانی واحد فروش: تهران-خیابان انقلاب-

خ شهدای زاندارمری-بین خ فخررازی و ۱۲ فروردین-

پلاک ۸۸ طبقه دوم-واحد ۴ تلفن ها: ۶۶۴۸۳۷۶۳-۶۶۴۸۳۷۶۲

◀ فروشگاههای اینترنتی دیباگران تهران:

WWW.MFTBOOK.IR

www.dibagaran-tehran.com

سرشناسه: هیورمن، لوئیس Heuermann, Lewis
عنوان و نام پدیدآور: برگزیده CompTIA Security+ SYO-701
/ترجمه و تالیف: سجاد دلیری؛
ویراستار: پروین عبدی.
مشخصات نشر: تهران: دیباگران تهران: ۱۴۰۳
مشخصات ظاهری: ۱۷۸ ص: مصور، جدول
شابک: ۹۷۸-۶۲۲-۲۱۸-۹۰۸-۲
وضعیت فهرست نویسی: فیبا
یادداشت: کتاب حاضر ترجمه بخشهایی از کتاب COMPTIA Security+ syo-701 cert guide است.
موضوع: شبکه های کامپیوتری-تدابیر ایمنی-آزمون ها-راهنمای مطالعه
computer networks-security measures-examinations-study guides: موضوع
موضوع: تکنسین های کامپیوتر-گواهی و گواهی نامه ها-راهنمای مطالعه
computer technicians-certifications-study guides: موضوع
موضوع: داده پردازی-کارمندان-گواهی و گواهی نامه ها-راهنمای مطالعه
electronic data processing personnel-certification-study guides: موضوع
شناسه افزوده: دلیری، سجاد، ۱۳۵۸- مترجم
رده بندی کنگره: ۵۱۰۵/۵۹ TK
رده بندی دیویی: ۰۰۵/۸۰۷۶
شماره کتابشناسی ملی: ۹۹۳۰۰۰۰

نشانی تلگرام: @mftbook نشانی اینستاگرام دیبا dibagaran_publishing

هر کتاب دیباگران، یک فرصت جدید علمی و شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

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 دسترس پذیری
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	پروتکل‌ها و استانداردهای امنیتی
۶۱	پروتکل‌های رمزنگاری شبکه
۶۱	پروتکل SSL/TLS
۶۲	پروتکل IPsec
۶۲	استانداردهای احراز هویت و کنترل دسترسی در شبکه‌ها
۶۲	پروتکل RADIUS
۶۳	پروتکل TACACS+
۶۳	پروتکل 802.1X
۶۳	پروتکل‌های امن انتقال فایل
۶۴	پروتکل SFTP
۶۴	پروتکل FTPS
۶۴	طراحی و معماری شبکه امن
۶۵	بخش‌بندی شبکه
۶۵	معماری شبکه Zero Trust
۶۶	ایجاد و مدیریت DMZ
۶۷	امنیت در شبکه‌های بی‌سیم
۶۷	چالش‌ها و تهدیدات خاص شبکه‌های بی‌سیم
۶۸	استانداردهای امنیتی برای Wi-Fi
۶۸	WEP
۶۹	WPA
۶۹	WPA2
۶۹	WPA3
۷۰	بهترین روش‌ها برای ایمن‌سازی شبکه‌های بی‌سیم
۷۲	پایش و مانیتورینگ امنیت شبکه
۷۲	ابزارهای مانیتورینگ شبکه
۷۲	Wireshark
۷۲	SolarWinds
۷۳	اهمیت پایش مداوم شبکه

تنظیم هشدارها و گزارش‌گیری ۷۴

فصل سوم

تهدیدات امنیتی و حملات ۷۵

بدافزارها و انواع آن ۷۶

ویروس‌ها ۷۷

کرم‌ها ۷۷

تروجان‌ها ۷۷

باچ‌افزارها ۷۷

جاسوس‌افزارها ۷۸

نحوه شناسایی و مقابله با بدافزارها ۷۸

تحلیل رفتارهای بدافزارها و ابزارهای ضدبدافزار ۷۸

حملات مبتنی بر شبکه ۷۹

DDoS و DoS ۷۹

روش‌های مقابله ۸۰

MITM ۸۰

روش‌های مقابله ۸۰

شنود ۸۰

روش‌های مقابله ۸۰

اسکن پورت و نفوذ به شبکه ۸۱

روش‌های مقابله ۸۱

مهندسی اجتماعی ۸۱

فیشینگ ۸۲

ویشینگ ۸۲

اسپیرفیشینگ ۸۲

تکنیک‌های حملات مبتنی بر روان‌شناسی ۸۳

روش‌های پیشگیری از حملات مهندسی اجتماعی ۸۳

تهدیدات داخلی ۸۴

کارکنان ناراضی یا بی‌احتیاطی 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	پیاپی‌سازی 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	فواید 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

۱۴۱ مزایای برنامه‌های مدیریت و پاسخ به حوادث

فصل هفتم

آموزش و آگاهی امنیتی ۱۴۲

۱۴۴ اهمیت آگاهی‌بخشی امنیتی به کارمندان و آموزش‌های مربوط به تهدیدات

۱۴۴ چرا آگاهی‌بخشی امنیتی اهمیت دارد؟

۱۴۵ مهم‌ترین تهدیداتی که کارمندان باید آموزش ببینند

۱۴۵ مزایای آموزش‌های امنیتی به کارمندان

۱۴۶ چگونه آگاهی‌بخشی امنیتی به‌طور مؤثر انجام شود؟

۱۴۶ چالش‌های آگاهی‌بخشی امنیتی

۱۴۶ مقاومت کارکنان در برابر آموزش امنیتی

۱۴۷ دلایل مقاومت

۱۴۷ راهکارها

۱۴۷ ۱. تغییرات سریع تهدیدات سایبری

۱۴۷ ۲. محدودیت منابع (مالی و انسانی)

۱۴۸ ۳. عدم درک اهمیت امنیت توسط کارکنان

۱۴۸ ۴. پیچیدگی محتوا و روش آموزش

۱۴۹ ۵. نبود ارزیابی مناسب اثربخشی آموزش‌ها

۱۴۹ ایجاد انگیزه برای رعایت مسائل امنیتی

۱۴۹ مشکلات انگیزشی

۱۵۰ راهکارها

۱۵۰ ایجاد برنامه آموزشی امنیتی

۱۵۰ ۱. شناسایی نیازها و اهداف آموزشی

۱۵۰ مثال

۱۵۱ ۲. تقسیم‌بندی مخاطبان

۱۵۱ مثال

۱۵۱ ۳. طراحی محتوای آموزشی

۱۵۱ روش‌های ارائه محتوا

۱۵۲ مثال

۱۵۲	۴. انتخاب روش‌های آموزش
۱۵۲	مثال
۱۵۲	۵. برگزاری آموزش‌ها
۱۵۲	۶. ارزیابی اثربخشی آموزش‌ها
۱۵۲	روش‌های ارزیابی
۱۵۳	مثال
۱۵۳	۷. به‌روزرسانی مداوم برنامه‌ها
۱۵۳	راهکارها
۱۵۳	۸. ایجاد فرهنگ امنیتی در سازمان
۱۵۳	روش‌های ایجاد فرهنگ امنیتی
۱۵۴	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
۱۵۵	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
۱۵۶	۵. پیاده‌سازی ابزارهای مدیریتی
۱۵۶	مثال‌هایی از سیاست‌های امنیتی برای پیشگیری از تهدیدات داخلی و انسانی
۱۵۶	پیشگیری از تهدیدات داخلی و انسانی
۱۵۷	نحوه ایجاد انگیزه برای رعایت مسائل امنیتی در محیط کار
۱۵۷	نحوه ایجاد انگیزه در رعایت مسائل امنیتی
۱۵۸	اهمیت ایجاد انگیزه برای رعایت مسائل امنیتی
۱۵۸	چالش‌های ایجاد انگیزه در کارکنان
۱۵۹	راهکارهای ایجاد انگیزه برای رعایت مسائل امنیتی
۱۵۹	۱. آموزش و آگاهی‌بخشی با روش‌های جذاب و تعاملی

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

مسائل قانونی حوزه امنیت اطلاعات ۱۶۲

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

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که بتواند
خواسته‌های به‌روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید تألیف "جناب آقای سجاد دلیری" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
dibagaran@mftplus.com

سخنی از مترجم کتاب

در دنیای دیجیتالی امروز، امنیت اطلاعات دیگر یک انتخاب نیست؛ بلکه یک نیاز ضروری و حیاتی است. هدف من از تدریس و اشتراک تجربه‌های چندین ساله‌ام در حوزه امنیت سایبری، انتقال دانش و آگاهی به کسانی است که می‌خواهند در این مسیر گام بردارند و به محافظان آینده دنیای دیجیتال تبدیل شوند. امیدوارم مطالب این دوره؛ نه تنها به شما در کسب مهارت‌های عملی کمک کند، بلکه درک عمیق‌تری از اهمیت و مسئولیت‌های امنیت اطلاعات، به شما ببخشد. با تلاش و پشتکار، شما نیز می‌توانید در این مسیر به یک متخصص شایسته و قابل اعتماد تبدیل شوید.

از همه همکارانم که در حوزه مقدس دفاع سایبری یا هر حوزه امنیت فناوری اطلاعات به کار ارزشمند آموزش یا مهندسی و راهبری سامانه‌های امنیتی و غیرامنیتی مشغول هستند؛ خالصانه تقاضا دارم در صورتی که کمی، کاستی و یا اشتباهی را که احتمالاً از روی ناآگاهی یا غیرتعمدانه در این مکتوب گنجانده‌ام و از دید تیزبین آن بزرگواران مشهود است، از طریق ایمیل daliri583@gmail.com به اطلاع برسانند؛ تا علاوه بر بهره‌وری اینجانب از راهنمود ایشان از جهت دقت در نگارش‌های متعاقب، موجب تصحیح این کتاب نیز در نسخ بعدی گردند.

”آموزش امنیت سایبری نه تنها به عنوان حرفه من، بلکه به عنوان رسالتی برای ایجاد دنیای دیجیتال امن‌تر، برایم ارزشمند است. باور دارم که هرچه بیشتر متخصصان آینده در این حوزه آموزش ببینند، شانس مقابله با تهدیدات پیچیده و حفاظت از دارایی‌های دیجیتال افزایش می‌یابد.“

باتشکر - سجاد دلیری - آذرماه ۱۴۰۳ - تهران - ایران

درباره مترجم

سجاد دلیری، با بیش از دو دهه تجربه در حوزه امنیت سایبری و فناوری اطلاعات، یکی از متخصصان مجرب ایران در این زمینه است. او علاوه بر تدریس و فعالیتهای آموزشی، به عنوان کارشناس ارشد امنیت اطلاعات در **بانک کشاورزی** فعالیت می کند و در حال تکمیل مقطع دکتری خود در رشته مهندسی کامپیوتر با تمرکز بر تحقیق در زمینه امنیت بلاک چین است.

ایشان عضو هیأت علمی وابسته **دانشگاه آزاد اسلامی** بوده و در واحد تهران جنوب این دانشگاه دروس طراحی الگوریتم، شبکه های کامپیوتری و... را تدریس کرده است. همچنین دوره های متعددی از جمله CCNA، Network+ و Security+ را در **مجتمع فنی تهران** (مؤسسه ای با سابقه درخشان آموزشی) ارائه می دهد.

سجاد دلیری دارای مدارک بین المللی معتبری همچون EC-Council SOC و Microsoft Azure است و تخصص او در حوزه هایی چون امنیت شبکه، مدیریت ریسک، و مقابله با تهدیدات سایبری، او را به یکی از پیشگامان این حوزه در ایران تبدیل کرده است. علاوه بر تدریس، او سابقه چاپ چندین مقاله در ژورنال های معتبر را نیز دارد که نشان از تعهد وی به پژوهش و توسعه دانش در حوزه امنیت و شبکه وی دارد.

در این کتاب، او با تکیه بر دانش و تجربیات گسترده خود در محیط های عملی و آکادمیک، تلاش می کند تا مطالب را به گونه ای ارائه دهد که خوانندگان بتوانند علاوه بر کسب دانش نظری، مهارت های عملی مورد نیاز برای مقابله با چالش های دنیای واقعی امنیت سایبری را نیز به دست آورند. تعهد وی به آموزش و پرورش نسل جدید متخصصان امنیت اطلاعات، این کتاب را به منبعی ارزشمند برای علاقه مندان به ورود به دنیای امنیت و شبکه تبدیل کرده است.

مقدمه

امنیت اطلاعات در دنیای دیجیتال امروز، یکی از مهم‌ترین و حساس‌ترین حوزه‌های مدیریت سازمانی به‌شمار می‌آید. رشد سریع فناوری‌ها و انتقال حجم عظیمی از داده‌ها در فضای دیجیتال، سازمان‌ها را در معرض انواع تهدیدات و حملات سایبری قرار داده است. این تهدیدات که به سرعت و در سطح جهانی گسترش می‌یابند، می‌توانند به افشای اطلاعات، تغییرات غیرمجاز در داده‌ها، دسترسی‌های غیرمجاز و حتی از دسترس خارج کردن منابع و سیستم‌ها منجر شوند. از این رو، امنیت اطلاعات به یکی از ارکان اصلی و بنیادی حفظ دارایی‌های سازمانی و حفاظت از حریم خصوصی تبدیل شده است.

هدف امنیت اطلاعات، ایجاد یک چهارچوب حفاظتی است که سازمان‌ها را در برابر تهدیدات سایبری و نقاط ضعف سیستم‌ها مقاوم سازد و در عین حال دسترسی امن و مطمئن کاربران مجاز به منابع را تضمین کند. برای دستیابی به این هدف، امنیت اطلاعات از اصول، مفاهیم و تکنیک‌های متنوعی بهره می‌برد که شامل محرمانگی^۱، یکپارچگی^۲، در دسترس‌پذیری^۳، کنترل‌های امنیتی، مدیریت ریسک و مقابله با تهدیدات است. در این مجموعه، به بررسی جامع این مفاهیم و شیوه‌های اجرایی و عملیاتی در حوزه امنیت اطلاعات خواهیم پرداخت تا درک عمیق‌تری از این حوزه و نیازمندی‌های آن به دست آوریم.



دوره آموزشی + CompTIA Security+

دوره +CompTIA Security برای اولین بار در اوایل دهه ۲۰۰۰ میلادی معرفی شد و به‌عنوان یک گواهینامه پایه برای ورود به دنیای امنیت اطلاعات طراحی شد. CompTIA، سازمان غیرانتفاعی بین‌المللی که به توسعه مدارک فناوری اطلاعات می‌پردازد، این دوره را به منظور ایجاد استاندارد در زمینه امنیت سایبری و آموزش متخصصان امنیتی راه‌اندازی کرد. اولین نسخه این گواهینامه، بر اصول پایه‌ای امنیت اطلاعات تمرکز داشت و موضوعاتی مانند شناسایی تهدیدات، اصول شبکه‌های امن و کنترل دسترسی را پوشش می‌داد.

با گذشت زمان و پیشرفت فناوری و افزایش پیچیدگی حملات سایبری، CompTIA نیز محتوای دوره Security+ را به‌روزرسانی و تکامل بخشید تا با چالش‌ها و نیازهای امنیتی جدید هماهنگ شود. نسخه‌های جدید این دوره، موضوعات بیشتری از جمله امنیت شبکه‌های ابری، اصول امنیت مجازی‌سازی، تحلیل رفتارهای مشکوک، و مدیریت حوادث را به آموزش‌های پایه اضافه کردند. این به‌روزرسانی‌ها نشان از تلاش CompTIA برای حفظ تطابق گواهینامه Security+ با تحولات دنیای سایبری و الزامات صنعتی دارد.

دوره Security+ به مرور به یکی از پرطرفدارترین گواهینامه‌های امنیت سایبری تبدیل شد و سازمان‌ها و شرکت‌های بسیاری این گواهینامه را به‌عنوان معیاری برای استخدام نیروهای امنیتی پذیرفتند. این گواهینامه در

1- Confidentiality
2- Integrity
3- Availability

حوزه‌های دولتی، مالی و فناوری، به‌عنوان یک استاندارد معتبر شناخته می‌شود. هم‌اکنون، دوره Security+ یکی از اصلی‌ترین و معتبرترین دوره‌های امنیت اطلاعات در سطح جهانی محسوب می‌شود که با جدیدترین نسخه آن، SY0-701، تلاش می‌شود تا نیازهای روز بازار کار در زمینه امنیت سایبری و محافظت از داده‌ها به‌خوبی پاسخ داده شود.

این گواهینامه نه‌تنها به متخصصان امنیت امکان می‌دهد تا دانش پایه‌ای و مهارت‌های عملی خود را افزایش دهند، بلکه آنها را برای مدارک پیشرفته‌تر و تخصصی‌تر آماده می‌سازد. با گذر از چندین نسخه و به‌روزرسانی‌های متعدد، CompTIA Security+ همچنان جایگاه خود را به‌عنوان یک استاندارد مطمئن در حوزه امنیت سایبری حفظ کرده و به مسیر حرفه‌ای بسیاری از متخصصان امنیت کمک کرده است.



نسخه SY0-701

کتاب “CompTIA Security+ SY0-701 Cert Guide” توسط تیمی از متخصصان برجسته امنیت اطلاعات، با راهبری لوئیس هیورمن^۱، تألیف شده است. این نویسندگان، با تجربه گسترده در حوزه امنیت سایبری، تلاش کرده‌اند تا با ارائه محتوایی جامع و به‌روز، دانشجویان و متخصصان را برای موفقیت در آزمون Security+ آماده کنند. آنها در مقدمه کتاب بر اهمیت درک عمیق مفاهیم امنیتی و به‌کارگیری آنها در محیط‌های واقعی تأکید کرده‌اند و هدف خود را تسهیل یادگیری و تقویت مهارت‌های عملی خوانندگان بیان نموده‌اند.

نسخه جدید کتاب CompTIA Security+ با کد SY0-701، به‌روزرسانی‌های مهمی را در حوزه امنیت سایبری معرفی کرده است. این نسخه با تمرکز بر روندها و تکنیک‌های نوین، به‌ویژه در زمینه تهدیدات جاری، اتوماسیون، مدل‌های امنیتی Zero Trust^۲، اینترنت اشیا^۳ (IoT) و مدیریت ریسک، طراحی شده است. یکی از تغییرات کلیدی در SY0-701، به‌روزرسانی ۲۰ درصد از اهداف آزمون است که شامل تأکید بر روندهای فعلی در تهدیدات، حملات، آسیب‌پذیری‌ها، اتوماسیون، Zero Trust، ریسک، IoT، فناوری عملیاتی (OT)^۳ و محیط‌های ابری می‌شود. این تغییرات به منظور تطابق با نیازهای روزافزون صنعت و اطمینان از مهارت‌های مورد نیاز متخصصان امنیت سایبری صورت گرفته است.

علاوه بر این، نسخه SY0-701 بر تکنیک‌های امنیتی در محیط‌های ترکیبی، شامل فضاهای ابری و داخلی، تأکید دارد. این به‌روزرسانی‌ها به متخصصان امنیتی کمک می‌کند تا با چالش‌های امنیتی در محیط‌های مدرن و پیچیده آشنا شوند و مهارت‌های لازم برای مقابله با آنها را کسب کنند. با این تغییرات، گواهینامه CompTIA Security+ همچنان به‌عنوان یکی از معتبرترین مدارک در حوزه امنیت سایبری شناخته می‌شود و به متخصصان کمک می‌کند تا با دانش و مهارت‌های به‌روز، در مسیر حرفه‌ای خود پیشرفت کنند.

1- Lewis Heuermann

2- Internet of Things

3- Operation Technology



خلاصه سازی کتاب

برای بهبود دسترسی به محتوای دوره **CompTIA Security+** و افزایش درک مطالب برای فراگیران، تصمیم گرفته شده که به جای ساختار اصلی ۲۴ فصل آن، محتوا به ۸ فصل کلی تر و جامع تر تقسیم شود. این رویکرد کمک می کند تا دانشجویان بتوانند در مدت زمان کوتاه تری مطالب را فرا بگیرند و تمرکز بیشتری بر مفاهیم اصلی و ضروری امنیت اطلاعات داشته باشند. با این ساختار جدید، از هم پوشانی مفاهیم در فصل های متعدد کاسته می شود و مسیر آموزشی روشن تری در اختیار یادگیرندگان قرار می گیرد.

در این تقسیم بندی، مطالب به گونه ای سازماندهی شده اند که هر فصل یک حوزه اساسی و مشخص از امنیت اطلاعات را پوشش دهد. به عنوان مثال، در فصلی با موضوع **مفاهیم امنیتی**، مباحث پایه ای و اصول کلیدی امنیت اطلاعات به صورت یکجا ارائه می شوند، در حالی که در ساختار ۲۴ فصلی ممکن است این اصول در فصل های مختلف پخش شده باشند. این نوع سازماندهی، یکپارچگی در یادگیری را افزایش می دهد و به دانشجویان اجازه می دهد تا مطالب مرتبط را به صورت منسجم و منطقی دنبال کنند.

علاوه بر این، فشرده سازی مطالب در ۸ فصل، امکان تمرکز بیشتر بر مباحث کلیدی مانند **مدیریت ریسک**، **تهدیدات و حملات امنیتی**، و **رمزنگاری و امنیت داده ها** را فراهم می کند. با این روش، دانشجویان نه تنها اطلاعات لازم برای موفقیت در آزمون Security+ را به دست می آورند، بلکه آمادگی بیشتری برای مقابله با چالش های امنیتی در محیط های عملی خواهند داشت. در مجموع، این ساختار بهینه سازی شده به فراگیران کمک می کند تا به صورت مؤثرتر و با درک عمیق تر از امنیت سایبری، به مفاهیم مورد نیاز مسلط شوند و آمادگی خود را برای فعالیت در حوزه امنیت اطلاعات به بهترین شکل افزایش دهند.

خلاصه کردن مطالب کتاب **CompTIA Security+ SY0-701** در هشت فصل پیشنهاد شده به این شکل خواهد بود:

فصل اول: مفاهیم امنیتی

- اصول و مفاهیم اصلی امنیت اطلاعات شامل مثلث امنیت (محرمانگی، یکپارچگی، دسترسی).
- انواع مختلف کنترل های امنیتی (پیشگیرانه، تشخیصی، اصلاحی).
- مفاهیم پایه ای مدیریت ریسک و ارزیابی ریسک های امنیتی.
- انواع تهدیدات امنیتی و آسیب پذیری ها.

فصل دوم: شبکه های امن

- طراحی و پیاده سازی شبکه های امن شامل مدل های امنیتی مختلف شبکه.
- ابزارها و تکنیک های امنیت شبکه مانند فایروال، VPN و NAC.
- اصول لایه بندی امنیت شبکه و نقش Zero Trust در امنیت شبکه.
- مفاهیم نظارت و تجزیه و تحلیل داده های شبکه برای شناسایی تهدیدات.

فصل سوم: تهدیدات امنیتی و حملات

- انواع مختلف حملات مانند حملات مهندسی اجتماعی، فیشینگ، بدافزار و حملات محرومیت از خدمت‌رسانی (DoS).^۱
- تکنیک‌های کاهش تهدیدات و شناسایی رفتارهای مخرب.
- آشنایی با تست نفوذ و جمع‌آوری اطلاعات برای شناسایی آسیب‌پذیری‌ها.
- شناسایی و مقابله با تهدیدات داخلی^۲ و سوءاستفاده از آسیب‌پذیری‌ها.

فصل چهارم: رمزنگاری و امنیت داده

- اصول رمزنگاری، تکنیک‌های رمزنگاری متقارن و نامتقارن.
- الگوریتم‌های رمزنگاری متداول و کاربردهای آنها.
- کنترل‌های حفاظت از داده، مانند رمزنگاری داده در انتقال و در حالت سکون.
- راهکارهای جلوگیری از نشت داده‌ها (DLP)^۳ و محافظت از اطلاعات حساس.

فصل پنجم: امنیت برنامه‌ها و دستگاه‌ها

- امنیت نرم‌افزار و اصول برنامه‌نویسی امن.
- مفاهیم مرتبط با آسیب‌پذیری‌های نرم‌افزاری و حملات به اپلیکیشن‌ها.
- امنیت دستگاه‌های همراه و IoT، شناسایی تهدیدات خاص آنها.
- پیاده‌سازی کنترل‌های امنیتی بر روی دستگاه‌ها و نرم‌افزارها.

فصل ششم: مدیریت امنیت

۱. اصول مدیریت آسیب‌پذیری و استفاده از سیستم مدیریت اطلاعات (ISMS).^۴
۲. مدیریت دسترسی و احراز هویت شامل MFA^۵ و مدیریت هویت و دسترسی (IAM).^۶
۳. پیاده‌سازی ابزارهای مدیریتی برای کنترل و نظارت بر امنیت.
۴. برنامه‌های مدیریت و پاسخ به حوادث امنیتی.

1- Denial of Service
2- insider threats
3- Data Loss Prevention
4- Information Security Management System
5- Multi Factor Authentication
6- Information and Access Management

فصل هفتم: آموزش و آگاهی امنیتی

- اهمیت آگاهی بخشی امنیتی به کارمندان و آموزش های مربوط به تهدیدات.
- چالش های آگاهی بخشی
- ایجاد برنامه های آموزشی و فرهنگ سازی امنیتی در سازمان.
- مدیریت سیاست ها و رویه های امنیتی برای پیشگیری از حملات داخلی و انسانی.
- نحوه ایجاد انگیزه برای رعایت مسائل امنیتی در محیط کار.

فصل هشتم: مسائل قانونی حوزه امنیت اطلاعات

- آشنایی با قوانین و مقررات بین المللی و محلی مرتبط با امنیت اطلاعات.
- استانداردها و چهارچوب های امنیتی مانند ISO 27001 و NIST.
- مدیریت انطباق سازمان با مقررات و الزامات قانونی.
- اصول حاکمیت امنیت اطلاعات و ممیزی های امنیتی.

با این ساختار، مطالب کتاب به صورت جامع و مختصر پوشش داده می شود و به عنوان مرجع کاملی برای آمادگی در آزمون Security+ و درک عمیق تر از امنیت اطلاعات می تواند مورد استفاده قرار گیرد.