مؤسسه فرهنگی هنری
دیباگران تهران

به نام خدا

برگزیده

CompTIA

Security + SYO-701

ترجمه و تالیف:

سجاد دلیری

مؤسسه فرهنگی هنری دیباگران تهران

عنوان کتاب: برگزیده CompTIA Security + SYO-701

تالیف و ترجمه : سجاد دلیری

ناشر: موسسه فرهنگی هنری دیباگران تهران

ویراستار: پروین عبدی

صفحه آرایی: نازنین نصیری

طراح جلد: داریوش فرسایی

نوبت چاپ: اول

تاریخ نشر: ۱۴۰۳

چاپ و صحافی: صدف

تیراژ: ۱۰۰ جلد

قیمت: ۲۵۰۰۰۰۰ ریال

شابک: ۲-۹۰۸-۲۱۸-۶۲۲-۹۷۸

نشانی واحد فروش: تهران-خیابان انقلاب-خ شهدای ژاندارمری-بین خ فخررازی و ۱۲ فروردین-پلاک ۸۸ طبقه دوم-واحد۴ تلفن ها: ۶۶۴۸۳۷۶۳-۶۶۴۸۳۷۶۲

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagarantehran.com

نشانی تلگرام: @mftbook نشانی اینستاگرام دیبا dibagaran_publishing

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: ۲-۹۰۸-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

یادداشت:کتاب حاضر ترجمه بخشهایی از کتاب COMPTIA Security+ syo-701 cert guide است.

موضوع:شبکه های کامپیوتری-تدابیر ایمنی-آزمون ها-راهنمای مطالعه

موضوع:computer networks-security measures-examinations-study guides

موضوع:تکنسین های کامپیوتر-گواهی و گواهی نامه ها-راهنمای مطالعه

موضوع:computer technecians-certifications-study guides

موضوع:داده پردازی-کارمندان-گواهی و گواهی نامه ها-راهنمای مطالعه

موضوع:electronic data processing personnel-certification-study guides

شناسه افزوده: دلیری،سجاد،۱۳۵۸-مترجم

رده بندی کنگره:۵۱۰۵/۵۹ TK

رده بندی دیویی:۰۰۵/۸۰۷۶

شماره کتابشناسی ملی:۹۹۳۰۰۰۰

فهرست مطالب

فصل اول

فصل دوم

فصل سوم

فصل چهارم

فصل پنجم

فصل ششم

فصل هفتم

فصل هشتم

مقدمه ناشر

خط مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب هایی با کیفیت عالی است که بتواند خواسته های به روز 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.

گستردگی علوم وسرعت 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 زمینه های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُربار، 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 منتشرگشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

با نظرات خود مشوق و راهنمای ما باشید

با ارائه نظرات و پیشنهادات وخواسته های خود،به ما کمک کنید تا بهتر و دقیق تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم.برای رساندن پیام هایتان به ما از رسانه های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره های 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؛ نه‌تنها 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 اطلاعم برسانند؛ تا علاوه‌بر بهره‌وری اینجانب از راهنمود ایشان از جهت دقت در نگارش‌های متعاقب، موجب تصحیح این کتاب نیز در نسخ بعدی گردند.

"آموزش امنیت سایبری نه‌تنها به‌عنوان حرفه من، بلکه به‌عنوان 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 ـ سجاد دلیری ـ آذرماه ۱۴۰۳ ـ تهران ـ 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 علاوه‌بر تدریس و فعالیت‌های آموزشی، به‌عنوان کارشناس ارشد امنیت اطلاعات در **بانک کشاورزی** فعالیت می‌کند و در حال تکمیل مقطع دکتری خود در رشته مهندسی کامپیوتر با تمرکز بر تحقیق در زمینه امنیت بلاک‌چین است.

ایشان عضو هیأت‌علمی وابسته **دانشگاه آزاد اسلامی** بوده و در واحد تهران جنوب این دانشگاه دروس طراحی الگوریتم، شبکه‌های کامپیوتری و... را تدریس کرده است. همچنین دوره‌های متعددی ازجمله Network+، CCNA و Security+ را در **مجتمع فنی تهران** (مؤسسه‌ای با سابقه درخشان آموزشی) ارائه می‌دهد.

سجاد دلیری دارای مدارک بین‌المللی معتبری همچون EC-Council SOC و Microsoft Azure است و تخصص او در حوزه‌هایی چون امنیت شبکه، مدیریت ریسک، و مقابله با تهدیدات سایبری، او را به یکی از پیشگامان این حوزه در ایران تبدیل کرده است. علاوه‌بر تدریس، او سابقه چاپ چندین مقاله در ژورنال‌های 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 محیط‌های عملی و آکادمیک، تلاش می‌کند تا مطالب را به‌گونه‌ای ارائه دهد که خوانندگان بتوانند علاوه‌بر کسب دانش نظری، مهارت‌های عملی مورد نیاز برای مقابله با چالش‌های دنیای واقعی امنیت سایبری را نیز به دست آورند. تعهد وی به آموزش‌وپرورش نسل جدید متخصصان امنیت اطلاعات، این کتاب را به منبعی ارزشمند برای علاقه‌مندان 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 به‌سرعت 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. ازاین‌رو، 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[1]، یکپارچگی[2]، در دسترس‌پذیری[3]، 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 به‌دست آوریم.

دوره آموزشی CompTIA Security+

دوره CompTIA Security+ برای اولین‌بار 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 استانداردی 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 ازجمله 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 لویس هیورمن[1]، 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 امنیتیZero Trust ، اینترنت اشیا[2] (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)[3] 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.

علاوه‌بر 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

خلاصه‌سازی کتاب

برای بهبود دسترسی به محتوای دوره **CompTIA Security+** و افزایش درک مطالب برای فراگیران، تصمیم گرفته شده که به‌جای ساختار اصلی ۲۴ فصل آن، محتوا به ۸ فصل کلی‌تر و جامع‌تر تقسیم شود. این رویکرد کمک می‌کند تا دانشجویان بتوانند در مدت زمان کوتاه‌تری مطالب را فرا بگیرند و تمرکز بیشتری بر مفاهیم اصلی و ضروری امنیت اطلاعات داشته باشند. با این ساختار جدید، از هم‌پوشانی مفاهیم در فصل‌های متعدد کاسته می‌شود و مسیر آموزشی روشن‌تری در اختیار یادگیرندگان قرار می‌گیرد.

در این تقسیم‌بندی، مطالب به‌گونه‌ای سازماندهی شده‌اند که هر فصل یک حوزه اساسی و مشخص از امنیت اطلاعات را پوشش دهد. به‌عنوان مثال، در فصلی با موضوع **مفاهیم امنیتی**، مباحث پایه‌ای و اصول کلیدی امنیت اطلاعات به‌صورت یکجا ارائه می‌شوند، در حالی که در ساختار ۲۴ فصلی ممکن است این اصول در فصل‌های مختلف پخش شده باشند. این نوع سازماندهی، یکپارچگی در یادگیری را افزایش می‌دهد و به دانشجویان اجازه می‌دهد تا مطالب مرتبط را به‌صورت منسجم و منطقی دنبال کنند.

علاوه‌بر این، فشرده‌سازی مطالب در ۸ فصل، امکان تمرکز بیشتر بر مباحث کلیدی مانند **مدیریت ریسک**، **تهدیدات و حملات امنیتی**، و **رمزنگاری و امنیت داده‌ها** را فراهم می‌کند. با این روش، دانشجویان نه‌تنها اطلاعات لازم برای موفقیت در آزمون Security+ را به‌دست می‌آورند، بلکه آمادگی بیشتری برای مقابله با چالش‌های امنیتی در محیط‌های عملی خواهند داشت. در مجموع، این ساختار بهینه‌سازی شده به فراگیران کمک می‌کند تا به‌صورت مؤثرتر و با درک عمیق‌تر 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 کنترل‌های امنیتی (پیشگیرانه، تشخیصی، اصلاحی).
- مفاهیم پایه‌ای مدیریت ریسک و ارزیابی ریسک‌های امنیتی.
- انواع تهدیدات امنیتی و آسیب‌پذیری‌ها.

فصل دوم: شبکه‌های امن

- طراحی و پیاده‌سازی شبکه‌های امن شامل مدل‌های امنیتی مختلف شبکه.
- ابزارها و تکنیک‌های امنیت شبکه مانند فایروال، VPN و NAC.
- اصول لایه‌بندی امنیت شبکه و نقش Zero Trust در امنیت شبکه.
- مفاهیم نظارت و تجزیه‌وتحلیل داده‌های 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)[1].
- تکنیک‌های کاهش تهدیدات و شناسایی رفتارهای مخرب.
- آشنایی با تست نفوذ و جمع‌آوری اطلاعات برای شناسایی آسیب‌پذیری‌ها.
- شناسایی و مقابله با تهدیدات داخلی[2] 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)[3] 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 امنیت اطلاعات (ISMS)[4].
۲. مدیریت دسترسی و احراز هویت شامل MFA[5] و مدیریت هویت و دسترسی (IAM)[6].
۳. پیاده‌سازی ابزارهای مدیریتی برای کنترل و نظارت بر امنیت.
۴. برنامه‌های مدیریت و پاسخ به حوادث امنیتی.

1- Danial 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 آگاهی‌بخشی امنیتی به کارمندان و آموزش‌های مربوط به تهدیدات.
- چالش‌های آگاهی بخشی
- ایجاد برنامه‌های آموزشی و فرهنگ‌سازی امنیتی در سازمان.
- مدیریت سیاست‌ها و رویه‌های 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 بین‌المللی و محلی مرتبط با امنیت اطلاعات.
- استانداردها و چهارچوب‌های امنیتی مانند ISO 27001 و NIST.
- مدیریت انطباق سازمان با مقررات و الزامات قانونی.
- اصول حاکمیت امنیت اطلاعات و ممیزی‌های امنیتی.

با این ساختار، مطالب کتاب به‌صورت جامع و مختصر پوشش داده می‌شود و به‌عنوان مرجع کاملی برای آمادگی در آزمون Security+ و درک عمیق‌تر از امنیت اطلاعات می‌تواند مورد استفاده قرار گیرد.