



مؤسسه فرهنگی هنری
دیارگران تهران

به نام خدا



مؤسسه فرهنگی هنری
دیارگران تهران

هوشمندسازی امنیت

و مقابله با تهدیدات پیشرفته

مؤلف

مهندس رضا آدینه



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: هوشمندسازی امنیت و مقابله با تهدیدات پیشرفته

سرشناسه: آدینه، رضا، ۱۳۶۷-
عنوان و نام پدیدآور: هوشمندسازی امنیت و مقابله با تهدیدات پیشرفته / مولف: رضا آدینه.
مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۸
مشخصات ظاهری: ۲۳۴ص: مصور،
شابک: ۹-۱۴۹-۲۱۸-۶۲۲-۹۷۸
وضعیت فهرست نویسی: فیبا
موضوع: جاسوسی مجازی cyber intelligence
موضوع: تروریسم رایانه ای - پیشگیری
موضوع: cyberterrorism-prevention
موضوع: جنگ سایبری (military sceince) cyberspace operation
موضوع: شبکه های کامپیوتری - تدابیر ایمنی
موضوع: computer networks-security measures
موضوع: کامپیوترها - ایمنی اطلاعات - تدابیر ایمنی
موضوع: computer security-security measures
موضوع: جرایم کامپیوتری - پیشگیری
موضوع: computer crimes-prevention
موضوع: امنیت ملی - نوآوری
موضوع: national security-technological innovations
رده بندی کنگره: HV ۶۷۷۳
رده بندی دیویی: ۳۶۴/۱۸
شماره کتابشناسی ملی: ۵۷۴۶۴۴۵

مؤلف: مهندس رضا آدینه
ناشر: موسسه فرهنگی هنری دیباگران تهران
صفحه آرای: فرنوش عبدالمهی
طراح جلد: داریوش فرسای
نوبت چاپ: اول
تاریخ نشر: ۱۳۹۸
چاپ و صحافی: درج عقیق
تیراژ: ۱۰۰۰ جلد
قیمت: ۹۹۰۰۰۰ ریال
شابک: ۹-۱۴۹-۲۱۸-۶۲۲-۹۷۸
نشانی واحد فروش: تهران، میدان انقلاب،
خ کارگر جنوبی، روبروی پاساژ مهستان،
پلاک ۱۲۵۱
تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶
فروشگاههای اینترنتی دیباگران تهران :
WWW.MFTBOOK.IR
www.dibagaran-tehran.com
www.mftdibagaran.ir
نشانی تلگرام: @mftbook

فهرست مطالب

فصل ۱: چالش‌ها و آمارها پیرامون تهدیدات و پاسخدهی به حوادث.....۱۶

- ۱-۱- مقدمه ۱۷
- ۲-۱- چالش‌های رایج امنیت سایبری ۱۸
- ۳-۱- اقدامات عمومی سازمان‌ها در مواجهه با چالشهای مطرح شده ۲۰
- ۴-۱- مروری بر آمارهای ارائه شده در زمینه مدیریت پاسخدهی به حوادث ۲۱
- ۱-۴-۱- تحقیقات انجام شده توسط SCO MAGAZINE ۲۲
- ۲-۴-۱- تحقیقات انجام شده ی SANS ۲۲
- ۳-۴-۱- تحقیقات انجام شده توسط گارتنر ۲۲
- ۴-۴-۱- تحقیقات انجام شده توسط VERIZON ۲۲

فصل ۲: راهکار اصلی مقابله با تهدیدات، مرکز عملیات امنیت و هوشمندسازی امنیت ۲۳

- ۱-۲- راهکار اصلی مقابله با تهدیدات ۲۴
- ۱-۱-۲- ظهور نسل جدیدی از پاسخدهی به حوادث امنیت سایبری و مروری بر نسل های مراکز عملیات امنیت سایبری ۲۴
- ۲-۱-۲- مرور تاریخچه نسل های مختلف مرکز عملیات امنیت ۲۵
- ۳-۱-۲- خلاصه ی اجرایی پیرامون مرکز عملیات امنیت ۲۶
- ۴-۱-۲- نام گذاری و انتخاب نام مرکز عملیات امنیت ۲۷
- ۵-۱-۲- نسل اول مرکز عملیات امنیت: ۱۹۷۵ الی ۱۹۹۵ ۲۷
- ۶-۱-۲- نسل دوم مرکز عملیات امنیت: ۱۹۹۶ الی ۲۰۰۱ ۲۸
- ۷-۱-۲- نسل سوم مرکز عملیات امنیت: سال های ۲۰۰۲ الی ۲۰۰۶ ۲۹
- ۸-۱-۲- نسل چهارم مرکز عملیات امنیت: سال ۲۰۰۷ الی ۲۰۱۲ ۳۱

- ۳۲ ۹-۱-۲- نسل پنجم مرکز عملیات امنیت: از سال ۲۰۱۳ تا کنون
- ۳۴ ۱۰-۱-۲- روند تکامل مقابله با نقض امنیت
- ۳۴ ۱۱-۱-۲- جمع بندی این فصل
- ۳۵ ۲-۲- مروری بر مفاهیم کاربردی تحلیل
- ۳۵ ۱-۲-۲- داده کاوی چیست؟
- ۳۷ ۲-۲-۲- BIG DATA چیست؟
- ۳۸ ۳-۲-۲- معرفی هوشمندی و هوش امنیتی
- ۵۰ ۱-۳-۲-۲- معرفی انواع هوشمندی در برابر تهدیدات
- ۵۱ ۲-۳-۲-۲- انواع مختلف THREAT INTELLIGENCE
- ۵۲ ۳-۲- مقایسه‌ی هوش امنیتی با هوش تجاری
- ۵۲ ۴-۲- هدف از پیاده سازی هوش امنیت در سازمان
- ۵۴ ۵-۲- مقایسه اجمالی هوش امنیتی با روش‌های سنتی امنیت سایبری
- ۵۶ ۶-۲- مدیریت ریسک

فصل ۳: مدلسازی تهدیدات، مولف های هوش امنیت، مدل های حملات در روش های

اشتراک گذاری اطلاعات تهدیدات.....۶۱

- ۶۲ ۱-۳-۱- مروری بر اجزای راهکار هوشمند سازی امنیتی
- ۶۳ ۱-۱-۳- مولفه‌ی اول هوش امنیت، مدل سازی دارایی‌ها
- ۶۳ ۲-۱-۳- مولفه‌ی دوم هوش امنیت، مدل سازی تهدیدات
- ۶۸ ۳-۱-۳- مدل سطح بلوغ شناسایی استیلیونز
- ۷۱ ۴-۱-۳- عناصر مدل سازی مفهومی تهدید
- ۷۲ ۵-۱-۳- یک مدل مفهومی برای طبقه‌بندی تهدید
- ۷۳ ۶-۱-۳- استخراج ویژگی مفهومی
- ۷۴ ۷-۱-۳- طرح‌های فعلی برای نمایش تهدید سایبری
- ۷۵ ۸-۱-۳- مثال‌هایی برای کاربردهای مدل‌های مفهومی تهدید سایبری
- ۷۷ ۱-۸-۱-۳- مروری بر مفهوم مدل سازی تهدیدات برنامه های کاربردی
- ۷۸ ۲-۸-۱-۳- رویکرد مهاجم - محور
- ۷۸ ۳-۸-۱-۳- رویکرد نرم افزار - محور
- ۷۸ ۴-۸-۱-۳- رویکرد دارایی - محور
- ۷۹ ۹-۱-۳- سیر تکاملی مدل سازی تهدید
- ۷۹ ۱۰-۱-۳- مراحل تولید مدل تهدید

۸۰ ۱۱-۱-۳- مرحله‌ی اول؛ تجزیه‌ی نرم افزار
۸۰ ۱۲-۱-۳- مرحله‌ی دوم؛ مروری بر روش‌های شناسایی و رتبه‌بندی تهدیدات
۸۱ ۱۳-۱-۳- مرحله‌ی سوم؛ تعیین اقدامات متقابل و کاهش اثرات تهدیدات
۸۱ ۱۴-۱-۳- تجزیه‌ی نرم‌افزار
۸۲ ۱۵-۱-۳- اطلاعات مدل تهدید
۸۲ ۱۶-۱-۳- وابستگی‌های خارجی
۸۲ ۱۷-۱-۳- نقاط ورودی
۸۳ ۱۸-۱-۳- دارایی‌های برنامه
۸۳ ۱۹-۱-۳- سطوح اعتماد
۸۴ ۲۰-۱-۳- نمودار جریان داده‌ها
۸۵ ۲۱-۱-۳- نمادها
۸۵ ۲۲-۱-۳- شناسایی و رتبه‌بندی تهدیدات
۸۶ ۲۳-۱-۳- طبقه‌بندی تهدیدات
۸۶ ۲۴-۱-۳- STRIDE
۸۶ ۲۵-۱-۳- کنترل‌های امنیتی
۸۷ ۲۶-۱-۳- تجزیه و تحلیل تهدیدات
۸۹ ۲۷-۱-۳- نمودار موارد کاربرد و موارد سوءاستفاده در مکانیزم تصدیق اصالت
۸۹ ۲۸-۱-۳- رتبه‌بندی تهدیدات
۹۰ ۲۹-۱-۳- شناسایی اقدامات متقابل
۹۲ ۳۰-۱-۳- استراتژی کاهش تاثیرات تهدید
۹۳ ۳۱-۱-۳- پیش‌پردازش داده‌ها
۹۳ ۳۲-۱-۳- نرمال کردن داده‌ها
۹۳ ۳۳-۱-۳- مولفه‌ی سوم هوش امنیت، تشخیص تهدیدات
۹۸ ۳۴-۱-۳- مولفه‌ی چهارم هوش امنیت، مدیریت وصله و مدیریت آسیب‌پذیری
۹۹ ۳۵-۱-۳- مولفه‌ی پنجم هوش امنیت، سامانه مدیریت رخدادها و حوادث امنیت
۱۰۲ ۳۶-۱-۳- مولفه‌ی ششم هوش امنیت، فریب تهدیدات؛
THREAT ۳۷-۱-۳- مولفه‌ی هفتم هوش امنیت، هوشیاری از تهدیدات یا هوشمندی پیرامون تهدیدات (THREAT
۱۰۲ INTELLIGENCE)
۱۱۳ ۳۸-۱-۳- آماده‌سازی هوشیاری محیط عملیاتی سایبری
۱۱۴ ۳۹-۱-۳- سطوح هوشیاری
۱۱۵ ۴۰-۱-۳- شکاف‌های شناسایی شده در پشتیبانی هوشیاری پیرامون تهدیدات سایبری از واکنش به
۱۱۶ ۱-۴۰-۱-۳- شکاف‌های سطح تاکتیکی

- ۱۱۷-۱-۳-۲-۴۰- شکاف‌های سطح عملیاتی؛
- ۱۱۷-۱-۳-۳-۴۰- شکاف‌های سطح استراتژیک؛
- ۱۱۸-۱-۳-۴۱- فرصت‌های هوشیاری پیرامون تهدیدات برای پشتیبانی از واکنش به تهدیدات
- ۱۱۸-۱-۳-۱-۴۱- سطح تاکتیکی
- ۱۱۸-۱-۳-۲-۴۱- آماده‌سازی
- ۱۲۱-۱-۳-۳-۴۱- شناسایی و تجزیه و تحلیل
- ۱۲۳-۱-۳-۴-۴۱- مهار، ریشه‌کن کردن و بازیابی
- ۱۲۴-۱-۳-۵-۴۱- فعالیت پس از رویداد
- ۱۲۴-۱-۳-۶-۴۱- سطح عملیاتی
- ۱۲۵-۱-۳-۷-۴۱- آماده‌سازی
- ۱۲۶-۱-۳-۸-۴۱- شناسایی و تجزیه و تحلیل
- ۱۲۷-۱-۳-۹-۴۱- مهار، ریشه‌کن کردن و بازیابی
- ۱۲۷-۱-۳-۱۰-۴۱- فعالیت پس از رویداد
- ۱۲۸-۱-۳-۱۱-۴۱- سطح استراتژیک
- ۱۲۸-۱-۳-۱۲-۴۱- آماده‌سازی
- ۱۳۱-۱-۳-۱۳-۴۱- شناسایی و تجزیه و تحلیل
- ۱۳۱-۱-۳-۱۴-۴۱- نگهداری، ریشه‌کن کردن و بازیابی
- ۱۳۲-۱-۳-۱۵-۴۱- فعالیت‌های پس از رویداد؛
- ۱۳۲-۱-۳-۱۶-۴۱- روش‌های اشتراک‌گذاری اطلاعات تهدیدات
- ۱۳۳-۱-۳-۴۲- استانداردسازی اطلاعات هوشیاری پیرامون تهدیدات با استفاده از روش شرح اطلاعات تهدید ساختاریافته (STIX)
- ۱۳۸-۱-۳-۴۳- رویکردهای فعلی
- ۱۳۹-۱-۳-۴۴- تاریخچه
- ۱۴۰-۱-۳-۴۵- STIX چیست؟
- ۱۴۱-۱-۳-۴۶- کاربردها
- ۱۴۱-۱-۳-۴۶-۱- (UC1) مورد کاربرد اول، آنالیز تهدیدات سایبری؛
- ۱۴۲-۱-۳-۴۶-۲- (UC2) مورد کاربرد دوم، مشخص کردن الگوهای شاخص برای تهدیدات سایبری؛
- ۱۴۲-۱-۳-۴۶-۳- (UC3) مدیریت واکنش به تهدیدات سایبری
- ۱۴۳-۱-۳-۴۶-۴- (UC3.1) جلوگیری از تهدیدات سایبری
- ۱۴۳-۱-۳-۴۶-۵- (UC3.2) تشخیص تهدیدات سایبری
- ۱۴۴-۱-۳-۴۶-۶- (UC3.3) پاسخ به رویداد
- ۱۴۴-۱-۳-۴۶-۷- اصول راهبردی
- ۱۴۴-۱-۳-۴۶-۸- صراحت

۱۴۴ یکپارچه سازی به جای کپی کردن
۱۴۵ انعطاف پذیری
۱۴۵ توسعه پذیری
۱۴۵ خودکار بودن
۱۴۶ خوانایی
۱۴۶ معماری
۱۴۷ ساختار STIX
۱۴۷ مشاهدات
۱۴۷ شاخص های تهدیدات سایبری
۱۴۸ رویدادها
۱۴۹ تاکتیک ها، فنون و رویه ها (TTP)
۱۵۰ کمپین ها
۱۵۰ عواملان تهدید
۱۵۱ اهداف بهره وری
۱۵۲ اقدامات (COA)
۱۵۳ نشانه گذاری داده
۱۵۴ پیاده سازی
۱۵۴ استفاده
۱۵۵ نتیجه گیری و اقدامات آتی
۱۵۸ تبادل خودکار امن اطلاعات شاخص (TAXII)
۱۵۸ مرور اجمالی
۱۵۸ پیشینه
۱۵۹ اهداف و انگیزه ها
۱۶۰ یک چارچوب تبادل
۱۶۰ گستره
۱۶۰ مدل HUB AND SPOKE (قطب و اقمار)؛
۱۶۱ مدل منبع-مشترک
۱۶۱ مدل PEER-TO-PEER (یک به یک)
۱۶۲ مشخصات و مستندات پروتکل TAXII
۱۶۴ سلسله مراتب مشخصات TAXII
۱۶۴ فواید
۱۶۵ وضعیت کنونی
۱۶۶ گام های آینده

۱۶۶ OSINT مفهوم	۱-۱۲-۲-۳
۱۶۸ OSINT منابع	۲-۱۲-۲-۳
۱۶۹ بهترین منابع اطلاعاتی خود را شناسایی کنید؛	۱۳-۲-۳
۱۶۹ ابزارهای مدیریت اطلاعات	۱۴-۲-۳
۱۷۰ مرور برخی از راهکارهای هوشیاری پیرامون تهدیدات؛	۱۵-۲-۳
۱۷۱ COLLECTIVE INTELLIGENCE FRAMEWORK	۱-۱۵-۲-۳
۱۷۲ COLLABORATIVE RESEARCH INTO THREATS	۲-۱۵-۲-۳
۱۷۳ MALWARE INFORMATION SHARING PLATFORM	۳-۱۵-۲-۳
۱۷۷ MALWARE COMMUNICATIONS ANALYZER (MALCOM)	۴-۱۵-۲-۳
	THE MANTIS CYBER THREAT INTELLIGENCE MANAGEMENT	۵-۱۵-۲-۳
۱۷۸ FRAMEWORK	
۱۷۹ چگونگی انتخاب راهکار هوشمندی پیرامون تهدیدات	۱۶-۲-۳
	MISP چیست و چرا سازمان ها به چنین راهکارهایی در مرکز عملیات امنیت نیازمند	۱-۱۶-۲-۳
۱۸۰ هستند ؟	
۱۸۰ بررسی ها و تحقیقات انجام شده	۲-۱۶-۲-۳
۱۸۱ مدل بلوغ هوشیاری از تهدیدات سایبری	۳-۱۶-۲-۳
۱۸۲ حوزه اول: هماهنگی با کسب و کار و چستی تهدیدات	۴-۱۶-۲-۳
۱۸۲ حوزه دوم: توانایی درک کردن	۵-۱۶-۲-۳
۱۸۳ حوزه سوم: توانایی کنترل یا اقدام بر روی موارد درک شده	۶-۱۶-۲-۳
۱۸۶ استفاده از مدل بلوغ هوشیاری پیرامون تهدیدات؛	۷-۱۶-۲-۳
۱۹۲ PYRAMID OF PAIN مفهوم	۸-۱۶-۲-۳
۱۹۵ HASHES اولین لایه ی هرم،	۹-۱۶-۲-۳
۱۹۶ دومین لایه ی هرم، آدرس های شبکه (IP ADDRESSES)	۱۰-۱۶-۲-۳
۱۹۷ سومین لایه ی هرم، نام دامنه ها (DOMAIN NAME)	۱۱-۱۶-۲-۳
۱۹۷ چهارمین لایه ی هرم، NETWORK & HOST ARTIFACTS	۱۲-۱۶-۲-۳
۱۹۹ پنجمین لایه ی هرم، TOOLS	۱۳-۱۶-۲-۳
۲۰۰ ششمین لایه ی هرم، TOOLS, TECHNIQUES & PROCEDURES	۱۴-۱۶-۲-۳
۲۰۳ مولفه ی هشتم هوش امنیتی، مفهوم شکار تهدیدات (THREAT HUNTING)	۱۵-۱۶-۲-۳
۲۰۵ چرا اقدام به شکار تهدیدات کنیم ؟	۱۷-۱۶-۲-۳
۲۰۶ چرا شکار تهدیدات عملیات با ارزشی است؟	۱۸-۱۶-۲-۳
۲۰۷ پیش نیازهای شکار تهدیدات	۱۹-۱۶-۲-۳
۲۰۹ مفهوم مدل بلوغ مرکز عملیات امنیت	۲۰-۱۶-۲-۳
۲۱۰ پیش نیازهای شکار تهدیدات (ادامه)	۲۱-۱۶-۲-۳

- ۲۱۲.....متدولوژی ۱۷-۲-۳
- ۲۱۶.....چگونه فرضیه سازی کنیم؟ ۱۸-۲-۳
- ۲۱۹.....فرضیه حاصل از هوشیاری ۱۹-۲-۳
- ۲۲۲.....آگاهی وضعیتی ۲۰-۲-۳
- ۲۲۴.....تخصص در دامنه ۲۱-۲-۳
- ۲۲۵.....بهترین رویکردها ۲۲-۲-۳
- ۲۲۶.....بلوغ فرضیه ۲۳-۲-۳
- ۲۲۷.....آیا ابزارهای شما توانایی لازم را می دهند؟ ۲۴-۲-۳
- ۲۲۸.....وقتی صحبت از شکار تهدیدات به میان می آید، تحلیلگر امنیتی دقیقاً باید دنبال چه موارد احتمالی باشد؟ ۲۵-۲-۳
- ۲۲۹.....سازمان‌ها در چه بازه‌های زمانی اقدام به شکار تهدیدات می کنند؟ ۲۶-۲-۳
- ۲۳۰.....شاخص‌ها و نشانه‌ها ۲۷-۲-۳
- ۲۳۰.....بررسی مفاهیم IOC ها و IOA ها ۱-۲۷-۲-۳
- ۲۳۳.....چگونه از شاخص‌ها برای حفظ امنیت و ارتقای امنیت استفاده نماییم؟ ۲-۲۷-۲-۳
- ۲۳۵.....انواع IOCها ۳-۲۷-۲-۳
- ۲۳۶.....برخی کاربردهای شاخص‌ها برای شکار تهدیدات ۴-۲۷-۲-۳
- ۲۴۲.....چگونگی جست‌وجوی INDICATORها برای شناسایی و شکار تهدیدات؛ ۵-۲۷-۲-۳
- ۲۴۳.....تشخیص فعالیت PSEXEC با استفاده از BRO ۶-۲۷-۲-۳
- ۲۴۳.....مروری کلی بر معماری منطقی سیستم شکار تهدیدات ۲۸-۲-۳
- ۲۴۴.....مروری بر پلتفرم‌های تجاری و پیشرفته شکار تهدیدات؛ ۲۹-۲-۳
- ۲۴۵.....مروری بر کاربردی‌ترین ابزارهای متن باز شکار تهدیدات؛ ۳۰-۲-۳
- ۲۴۵.....HELK-۱-۳۰-۲-۳
- ۲۴۶.....SOF-ELK-۲-۳۰-۲-۳
- ۲۴۶.....مدل بلوغ شکار تهدیدات ۳۱-۲-۳
- ۲۴۹.....مدل بلوغ ارائه شده شرکت SQRRL ۳۲-۲-۳
- ۲۵۱.....مطالعه‌ی آماری وضعیت شکار تهدیدات ۳۳-۲-۳
- ۲۵۲.....چرخه شکار تهدیدات ارائه شده توسط شرکت SQRRL ۳۴-۲-۳
- ۲۵۵.....چه مواردی شکار تهدیدات نمی‌باشند ۳۵-۲-۳
- ۲۵۵.....معرفی ۱۰ نکته جهت شکار تهدیدات موثر ۳۶-۲-۳
- ۲۵۶.....اندازه گیری موفقیت شکار تهدیدات ۳۷-۲-۳
- ۳۸-۲-۳.....مولفه‌ی نهم هوش امنیتی، راهبری، خودکارسازی و مدیریت حوادث امنیت سایبری (SECURITY AUTOMATION & ORCHESTRATION) ۲۵۶.....
- ۲۵۸.....چگونه به سازمان‌ها کمک می کند با تهدیدات امنیتی مقابله کنند؟ ۱-۳۸-۲-۳

۲۶۲	۱-۴- چکیده مفهوم هوش امنیتی
۲۶۵	۲-۴- مسیر پیاده سازی راهکار TI تا رسیدن به TH
	۱-۲-۴- شش روش برای استفاده از زنجیره مرگ سایبری به وسیله یک پلتفرم هوشیاری پیرامون
۲۷۲	تهدیدات
۲۷۲	۱-۱-۲-۴- اولویت بندی هشدارهای سنسورها
۲۷۳	۲-۱-۲-۴- اولویت بندی پیشرفت نفوذ
۲۷۴	۳-۱-۲-۴- اندازه گیری تاثیر گذاری
۲۷۴	۴-۱-۲-۴- اندازه گیری مقاومت
۲۷۵	۵-۱-۲-۴- اندازه گیری تمامیت تحلیلی
۲۷۵	۶-۱-۲-۴- شناسایی و ردگیری کمپین ها
۲۷۶	۲-۲-۴- استراتژی کلی و کلان
	۳-۲-۴- نقش PEOPLE, PROCESS, TECHNOLOGY در بهره برداری از CTI برای
۲۷۷	اجرای شکار تهدیدات
۲۷۹	۴-۲-۴- شکارچی تهدیدات به چه کسی گفته می شود؟
۲۷۹	۱-۴-۲-۴- استایل شخصی
۲۷۹	۲-۴-۲-۴- مهارت های مورد نیاز
۲۷۹	۳-۴-۲-۴- ذهن خلاق و تحلیلگر
۲۸۰	۴-۴-۲-۴- تحلیل لاگ
۲۸۰	۵-۴-۲-۴- جرم شناسی و تحلیل عمیق در سطح شبکه
۲۸۰	۶-۴-۲-۴- تسلط بر ساختار شبکه
۲۸۰	۷-۴-۲-۴- تسلط بر چرخه عمر نفوذگران
۲۸۱	۸-۴-۲-۴- ابزارها
۲۸۱	۹-۴-۲-۴- تسلط بر ساختار سیستم عامل
۲۸۱	۱۰-۴-۲-۴- تسلط بر روش های نفوذ
۲۸۲	۵-۲-۴- فرایندها
۲۸۵	۶-۲-۴- جایگاه این راهکار در ساختار سازمانی
۲۸۶	۷-۲-۴- فناوری ها و ابزارها
۲۸۶	۸-۲-۴- جمع آوری داده ها
۲۸۸	۹-۲-۴- نگهداری داده ها
۲۸۸	۱۰-۲-۴- مدل دیاموند

۲۹۰.....	۱۱-۲-۴- فهمیدن مدل تحلیل نفوذ دیاموند در شکار تهدیدات و پاسخدهی به حوادث؛
۲۹۳.....	۱۲-۲-۴- قوانین و هشدارها (RULES & ALERTING)
۲۹۴.....	۱۳-۲-۴- METRICS
۲۹۵.....	۱۴-۲-۴- استفاده‌ی موثر از CTI
۳۰۱.....	۱۵-۲-۴- معرفی پلتفرم PALISADE
۳۰۱.....	۱۶-۲-۴- چرخه عمر واکنش به رویداد
۳۰۲.....	۱۷-۲-۴- چرخه هوشیاری
۳۰۳.....	۱۸-۲-۴- مفهوم مقابله با جاسوسی
۳۰۵.....	۱۹-۲-۴- پیاده سازی موثر راهکارهای DECEPTION برای شکار تهدیدات موثر
۳۰۷.....	۲۰-۲-۴- مفهوم TRADECRAFT
۳۰۸.....	۲۱-۲-۴- ایجاد یک " پایگاه دانش
۳۰۸.....	۲۲-۲-۴- مدیریت دارایی
۳۰۹.....	۲۳-۲-۴- سطوح حملات
۳۱۱.....	۲۴-۲-۴- بردارهای حملات
۳۱۲.....	۲۵-۲-۴- حوزه‌ها/دامنه‌ها
۳۱۲.....	۲۶-۲-۴- مدیریت هوشمندانه لاگ‌ها
۳۱۳.....	۲۷-۲-۴- مدیریت هویت و کنترل دسترسی
۳۱۳.....	۲۸-۲-۴- ایجاد خط مبنا

فصل ۵: هوشیاری از تهدیدات برای شکار تهدیدات..... ۳۱۵

۳۱۷.....	۱-۵- سخن پایانی
۳۲۱.....	ضمیمه ۱
۳۲۳.....	مراجع

خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی است که بتواند خواسته‌هایی به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.

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 دانشگاهی، علوم پایه و به ویژه علوم کامپیوتر و انفورماتیک گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و 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 روشن می‌نماید.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری جمعی از اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران، محققان و نیز پرسنل ورزیده و ماهر در زمینه امور نشر درصدد هستند تا با تلاش‌های مستمر خود برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهند.

کتابی که در دست دارید با همت "مهندس رضا آدینه" و تلاش جمعی از همکاران انتشارات میسر گشته که شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

کارشناسی و نظارت بر محتوا: زهره قزلباش

در خاتمه ضمن سپاسگزاری از شما دانش‌پژوه گرامی درخواست می‌نماید با مراجعه به آدرس dibagaran.mft.info (ارتباط با مشتری) فرم نظرسنجی را برای کتابی که در دست دارید تکمیل و ارسال نموده، انتشارات دیباگران تهران را که جلب رضایت و وفاداری مشتریان را هدف خود می‌داند، یاری فرمایید.

امیدواریم همواره بهتر از گذشته خدمات و محصولات خود را تقدیم حضورتان نماییم.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران
bookmarket@mft.info

مقدمه مولف

طبق بررسی ها و تجارب حاصله سال ها فعالیت در حوزه امنیت اطلاعات سایبری تصمیم به تالیف کتابی دانشی و کاربردی و به روز برای تمامی علاقه‌مندان به این حوزه گرفتم . با در نظر داشتن این مسله که راهکارهای سنتی صرفا مبتنی بر پایش امروزه کارایی چندانی برای مقابله با تهدیدات پیشرفته ندارند؛ و ظهور نسل جدید راهکارهای امنیتی، جای خالی کتابی برای مفاهیم کاربردی و نوین احساس می شد. به همین خاطر این نوشتار بر همین اساس و با هدف تعریف مدلی کاربردی و مفهومی مبتنی بر هوشمند سازی و بهره برداری از مفاهیم نوین تالیف شده است.

برای تالیف این کتاب از منابع معتبر بسیاری استفاده شده است که همگی از بروزترین منابع در دسترس بوده اند. در ادامه لازم به ذکر است که در صورت وجود هرگونه نقطه نظر پیرامون کتاب پیش رو می توانید با آدرس ایمیل اینجانب در تماس باشید.

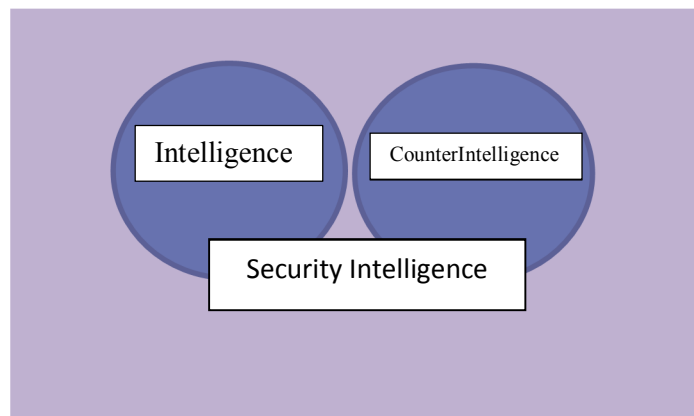
REZA_ADINEH@LIVE.COM

در این قسمت از تمامی دوستان و عزیزانی که در تالیف این کتاب اینجانب را یاری کردند تقدیر و تشکر می کنم.

پیشگفتار

در دنیای امروزی تهدیدات بسیاری برای سازمان‌ها وجود دارند. سازمان‌ها برای مقابله با تهدیدات نیازمند اطلاعات و داده‌های مفید جهت تشخیص نشانه‌های آنها می‌باشند. برای مقابله با تهدیدات که به سرعت در حال رشد و پیچیده‌تر شدن می‌باشند نیاز به راهکارهای مناسب جهت پیشگیری، تشخیص و پاسخ در بازه زمانی موثری می‌باشد تا کسب‌وکار سازمان‌ها دچار اختلال و آسیب نگردد. لذا سازمان‌ها می‌بایست در برنامه‌های امنیت سایبری خود از مفهومی به نام **Security Intelligence** به اختصار **SI** بهره‌مند شوند. **SI** شامل مجموعه اطلاعاتی می‌باشد که در راستای محافظت سازمان در برابر تهدیدات داخلی و بیرونی مورد استفاده قرار می‌گیرد. در **SI** تمامی فرایندها، سیاست‌ها و ابزار لازم جهت جمع‌آوری و تحلیل اطلاعات پیرامون تهدیدات در نظر گرفته می‌شود. در این نوشتار به معرفی مفاهیم و مضامین، بهره‌برداری از این مفاهیم، بررسی راهکارهای مناسب در راستای نیل به اهداف مذکور جهت مقابله و شناسایی این قبیل تهدیدات پرداخته می‌شود. و در نهایت مدلی برای شکار تهدیدات سایبری بر همین اساس ارائه می‌دهد.

هدف اصلی این نوشتار علاوه بر معرفی مفاهیم و مضامین کاربردی و مروری بر بهترین ابزارها برای محقق کردن راهکارهای ذکر شده، معرفی نظریه‌ای جدید بر مبنای بهره‌برداری موثر از مفهوم "هوشمندی پیرامون تهدیدات" **Threat Intelligence** برای اجرای (شکار تهدیدات) **Threat Hunting** می‌باشد.



دیدگاه اصلی بر محور مفهوم هوشمند سازی امنیت سایبری و بکار گرفتن این راهکار در سازمان می‌باشد. دو مولفه‌ی اصلی هوشمندی پیرامون تهدیدات و شکار تهدیدات از محورهای اساسی این نوشتار می‌باشد. بطور کل مفهوم هوشمندسازی امنیت متشکل از دو قسمت اساسی می‌باشد، یکی تحت عنوان **Intelligence** و دیگری تحت عنوان **CounterIntelligence** می‌باشند. تمرکز این

نوشتار بر استفاده از راهکارهای هوشمندی پیرامون تهدیدات در راستای پیشبرد فرایندهای شکار تهدیدات می‌باشد. که تلاش شده است تا تمامی جوانب موضوع مورد بررسی قرار گرفته و راهکاری مناسب و کاربردی ارائه گردد. محوریت این نوشتار بر اساس تعریف، کاربرد و معرفی راهکارهای برگزیده این مضامین می‌باشد. در تمام نوشتار مفاهیم زیادی مطرح شده که سعی بر چکیده نویسی این مضامین شده است. لذا می‌بایست ابتدا به تعریف مفهوم هوشمند سازی امنیتی پرداخت و ضمن معرفی الزامات و مولفه های تشکیل دهنده آن، مولفه های کلیدی و چگونگی پیاده سازی این مجموعه مرور گردد.