



مؤسسه فرهنگی هنری  
دیبگران تهران

**به نام خدا**



مؤسسه فرهنگی هنری  
دیبگران تهران

**معرفی نسل جدید**

**مراکز عملیات امنیت**

**Next Generation SOC**

مؤلف

**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: معرفی نسل جدید مراکز عملیات امنیت Next Generation SOC

◀ مولف: رضا آدینه

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرای: فرناوش عبدالهی

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۸

◀ چاپ و صحافی: درج عقیق

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۴۰۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۲۱۸-۲

◀ نشانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

◀ فروشگاههای اینترنتی دیباگران تهران :

[WWW.MFTBOOK.IR](http://WWW.MFTBOOK.IR)

[www.dibbook.ir](http://www.dibbook.ir)

[www.dibagaran-tehran.com](http://www.dibagaran-tehran.com)

◀ نشانی تلگرام: @mftbook      نشانی اینستاگرام دیبا [dibagaran\\_publishing](https://www.instagram.com/dibagaran_publishing)

هر کتاب دیباگران، یک فرصت جدید شغلی.

هر گوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتها و اپ دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

سرشناسه: آدینه، رضا، ۱۳۶۷-  
عنوان و نام پدیدآور: معرفی نسل جدید مراکز عملیات  
امنیت Next generation SOC / مولف: رضا آدینه.  
مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۸  
مشخصات ظاهری: ۱۱۲ص: مصور،  
شابک: ۹۷۸-۶۲۲-۲۱۸-۲۱۸-۲  
وضعیت فهرست نویسی: فیبا  
موضوع: زیر ساخت مجازی-تدابیر ایمنی  
موضوع: Cyberinfrastructure=security measures  
موضوع: سامانه های امنیتی  
موضوع: security systems  
موضوع: شبکه های کامپیوتری  
موضوع: computer networks-security measures  
رده بندی کنگره: QA ۷۶/۹  
رده بندی دیویی: ۰۰۵/۸  
شماره کتابشناسی ملی: ۵۹۴۱۶۴۸

# فهرست مطالب

## بخش اول : تعریف نسل جدید مرکز عملیات امنیت ..... ۷

- ❖ فصل ۱ : ظهور نسل جدیدی از پاسخدهی به حوادث امنیت سایبری ..... ۸
- ویژگی های اصلی یک مرکز عملیات امنیت نسل جدید ..... ۱۰
- آنچه در این فصل می خوانیم ..... ۱۰
- مرکز عملیات امنیت (SOC) چیست؟ ..... ۱۱
- دلایل ایجاد یک مرکز عملیات امنیت (SOC) ..... ۱۱
- حوزه های عملکرد مرکز عملیات امنیت (SOC) ..... ۱۲
- تجهیزات مرکز عملیات امنیت (SOC) ..... ۱۳
- چالش های ایجاد و پیاده سازی یک مرکز عملیات امنیتی ..... ۱۴
- SECOPS چیست؟ ..... ۱۵
- فرآیندهای مرکز عملیات امنیت (SOC) ..... ۳۱
- اندازه گیری مرکز عملیات امنیت (SOC) ..... ۳۴
- آینده مرکز عملیات امنیت (SOC) ..... ۳۶

## بخش دوم : معرفی مولفه های اصلی نسل جدید SOC ..... ۳۷

- ❖ فصل ۱ : پلتفرم SOAR ، تمام آنچه باید در مورد هماهنگ سازی، خودکار سازی و واکنش امنیتی بدانید؛ ..... ۳۸
- داده های زیاد و منابع کم ..... ۳۸
- ❖ فصل ۲ : پلتفرم SOAR چیست؟ ..... ۴۲
- تجزیه و تحلیل هوشیاری ..... ۴۴
- هوشیاری عملیات را هوشمندتر می کند: آغاز یک حلقه بازخورد میان هوشیاری و عملیات ..... ۴۴
- SOAR در عمل ..... ۴۵
- ❖ فصل ۳ : هماهنگ سازی مبتنی بر هوشیاری ..... ۴۶
- ❖ فصل ۴ : کاهش زمان واکنش و بازیابی توسط SOAR ..... ۴۹
- SOAR در عمل: ارسال و بازیابی ایمیل سرقت هویت ..... ۵۰
- ❖ فصل ۵ : دستیابی به SOAR هوشمندتر ..... ۵۱
- ❖ فصل ۶ : ترکیب هوشیاری، اتوماسیون، هماهنگ سازی و واکنش در یک پلتفرم ..... ۵۳
- انعطاف پذیری و توسعه پذیری به عنوان اصل مرکزی ..... ۵۳
- استفاده از تجزیه و تحلیل برای درک عملکرد پلت فرم و تیم ..... ۵۴

۵۷	قابلیت‌هایی برای بهبود و اثربخشی
۵۹	مرور یک نمونه پلتفرم SOAR
۶۰	❖ فصل ۷: چک‌لیستی برای یک راه‌حل SOAR کامل
<b>بخش سوم: پلت‌فرم‌های هوشیاری پیرامون تهدیدات و هر آنچه که باید در این باره بدانید</b>	
۶۳	❖ فصل ۱: اهمیت هوشیاری پیرامون تهدیدات
۶۴	دشمن خود را بشناسید.
۶۷	رویکرد جامع
۶۷	رویکرد متمرکز
۶۹	❖ فصل ۲: هوشیاری پیرامون تهدیدات چیست؟
۶۹	منابع تهدید داخلی و خارجی
۷۰	هوشیاری پیرامون تهدیدات عملکردی
۷۶	❖ فصل ۳: پلت‌فرم‌های هوشیاری پیرامون تهدیدات: نرم‌افزارهای شرکتی مهم جدید ...
۷۸	ظرفیت سازمانی پایین هوشیاری پیرامون تهدیدات
۷۹	ظرفیت سازمانی متوسط هوشیاری پیرامون تهدیدات
۸۱	ظرفیت سازمانی بالای هوشیاری پیرامون تهدیدات
۸۲	قابلیت‌های مورد انتظار از پلت‌فرم هوشیاری پیرامون تهدیدات
۸۴	یک پلتفرم هوشیاری پیرامون تهدیدات باید چه ویژگی‌هایی داشته باشد
۸۷	خودکارسازی فرآیند پلتفرم هوشیاری پیرامون تهدیدات
۹۳	❖ فصل ۴: در حمایت از به اشتراک‌گذاری: یک پلتفرم هوشیاری پیرامون تهدیدات باید به توانمند شدن انجمن‌ها، ISAC و ISAO کمک کند.
۹۶	شروع به اشتراک‌گذاری
۹۸	❖ فصل ۵: خلاصه‌ای از مزایا و نکات کلیدی پیرامون هوشیاری پیرامون تهدیدات
۱۰۱	❖ پیوست‌ها: مدل الماس برای تجزیه و تحلیل تهاجم
۱۰۲	مدل الماس چیست؟
۱۰۴	چک‌لیست پیرامون هوشیاری پیرامون تهدیدات
<b>بخش چهارم: آینده نگری</b>	
۱۱۱	جمع بندی
۱۱۲	منابع و مراجع

# خط مشی کیفیت انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌های است که بتواند خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد. هر کتاب دیباگران تهران، یک فرصت جدید شغلی

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 "جناب آقای 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](mailto: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](mailto:bookmarket@mft.info)

### نسل جدید مراکز عملیات امنیت؛

نسل جدید مراکز عملیات امنیت از سال ۲۰۱۲ تا کنون شناخته می شود. همانطور که می دانید مرکز عملیات امنیت همان قابلیت است که در سازمان با استفاده از متخصصان، فرایند ها و فناوری ها اقدام به پایش امنیت سایبری کرده و به شناسایی ریسک ها و تهدیدات سازمانی می پردازد.

اما با پیشرفته تر شدن تهدیدات و پیچیده تر شدن آن ها عامل زمان در شناسایی و پاسخدهی به حوادث نقش پر رنگ تری پیدا کرده است. لذا پارادایم جدیدی از مرکز عملیات امنیت به وجود آمده که ویژگی های متفاوتی را ارائه می دهد. تمام تلاش سازمان ها برای کنترل ریسک بوده است و با در نظر داشتن حملات پیشرفته، همچنین نرخ رشد حملات سایبری در کمیت و کیفیت، راهکارهای سنتی به تنهایی کفایت لازم برخوردار نیستند.

همچنین بنابه انواع تهدیدات مدرن و نحوه ی حملات آن ها نقاط شناسایی تهدیدات در ساختارهای شبکه تغییر کرده است.

در این کتاب تلاش شده است ضمن مرور این ویژگی ها، وضعیت کلی یک مرکز عملیات امنیت نسل جدید را برای استفاده شما عزیزان فراهم آورد.

هدف این کتاب تنها مروری بر مفاهیم و ویژگی های جدیدی است که یک مرکز عملیات امنیت می بایست داشته باشد.