

## فهرست

|                                                               |    |
|---------------------------------------------------------------|----|
| بخش ۱؛ مبانی و مفاهیم کلیدی SOAR .....                        | ۱۵ |
| فصل ۱؛ مقدمه‌ای بر SOAR .....                                 | ۱۵ |
| ۱-۱- (SOAR) چیست؟ تعریف، اهداف و چشم‌انداز.....               | ۱۶ |
| ۱-۲- ارکان اصلی SOAR: هماهنگ‌سازی، خودکارسازی و پاسخ‌دهی..... | ۱۶ |
| ۱-۳- اهمیت حیاتی SOAR در امنیت سایبری مدرن.....               | ۱۸ |
| فصل دوم؛ درک عمیق هماهنگ‌سازی امنیتی.....                     | ۲۱ |
| ۱-۲- تعریف و مفاهیم کلیدی و اصول هماهنگ‌سازی.....             | ۲۲ |
| ۲-۲- چرا به هماهنگی امنیتی نیاز داریم؟.....                   | ۲۳ |
| ۳-۲- تفاوت هماهنگ‌سازی امنیتی و خودکارسازی امنیتی.....        | ۲۵ |
| فصل سوم؛ کاوش در خودکارسازی امنیتی.....                       | ۲۹ |
| ۱-۳- مبانی و اصول خودکارسازی امنیتی.....                      | ۳۰ |
| ۲-۳- مزایا و دستاوردهای خودکارسازی در عملیات امنیت.....       | ۳۱ |
| ۳-۳- ابزارها و پلتفرم‌های کلیدی برای خودکارسازی امنیتی.....   | ۳۳ |
| فصل ۴؛ بررسی مفهوم پاسخ‌دهی (RESPONSE) در چارچوب SOAR.....    | ۳۷ |
| ۱-۴- مفهوم و جایگاه پاسخ در اکوسیستم SOAR.....                | ۳۷ |
| ۲-۴- نقش حیاتی فرآیندهای پاسخ‌دهی در SOAR.....                | ۳۹ |
| ۳-۴- استراتژی‌ها و چارچوب‌های مؤثر برای پاسخ به رخدادها.....  | ۴۱ |
| بخش ۲؛ اجزاء، استراتژی و برنامه‌ریزی SOAR.....                | ۴۵ |
| فصل ۵؛ اجزای کلیدی یک پلتفرم SOAR کارآمد .....                | ۴۷ |
| ۱-۵- مدیریت Case.....                                         | ۴۸ |
| ۲-۵- گردش کار خودکار.....                                     | ۴۹ |
| ۱-۲-۵- درک خودکارسازی جریان‌های کاری در SOAR.....             | ۴۹ |
| ۲-۲-۵- نقش پلی‌بوک‌های پاسخ‌دهی در خودکارسازی گردش کار.....   | ۵۰ |

- ۵۰.....SOAR در گردش کار در ۳-۲-۵ مزایای خودکارسازی
- ۵۱.....Threat Intelligence یکپارچه سازی در ۳-۵
- ۵۱.....SOAR در Threat Intelligence درک در ۱-۳-۵
- ۵۲.....SOAR در Threat Intelligence اهمیت در ۲-۳-۵
- ۵۳.....ایزارهای همکاری و ارتباط تیمی در ۴-۵
- ۵۳.....SOAR در همکاری در ۱-۴-۵ درک
- ۵۴.....SOAR در همکاری در ۲-۴-۵ اهمیت
- ۵۹..... فصل ۶؛ طراحی و تدوین استراتژی SOAR سازمانی
- ۶۰.....ارزیابی و درک نیازهای امنیتی خاص سازمان شما در ۱-۶
- ۶۰.....محیط ریسک در ۱-۱-۶
- ۶۱.....توانمندی های فناورانه در ۲-۱-۶
- ۶۱.....مشارکت ذی نفعان در ۳-۱-۶
- ۶۲.....تعریف اهداف و مقاصد شفاف برای پیاده سازی SOAR در ۲-۶
- ۶۲.....اهداف راهبردی در ۱-۲-۶
- ۶۲.....اهداف عملیاتی در ۲-۲-۶
- ۶۳.....اهداف قابل سنجش در ۳-۲-۶
- ۶۳.....اولویت بندی اهداف در ۴-۲-۶
- ۶۴.....انتخاب ابزارها و پلتفرم SOAR مناسب در ۳-۶
- ۶۴.....درک گزینه های موجود در ۱-۳-۶
- ۶۴.....ارزیابی ویژگی ها در ۲-۳-۶
- ۶۵.....در نظر گرفتن پشتیبانی ارائه دهنده در ۳-۳-۶
- ۶۵.....ملاحظات مربوط به هزینه در ۴-۳-۶
- ۶۳.....بخش ۳؛ طراحی، ساخت و پیاده سازی پلی بوک های SOAR
- ۶۷..... فصل ۷؛ مقدمه ای بر پلی بوک های SOAR

|          |                                                                 |
|----------|-----------------------------------------------------------------|
| ۶۷.....  | ۱-۷- پلی بوک SOAR چیست؟ تعریف و کارکرد.....                     |
| ۶۷.....  | ۲-۷- اهمیت و مزایای استفاده از پلی بوکها در عملیات امنیت.....   |
| ۶۸.....  | ۳-۷- انواع متداول پلی بوکها و کاربردهای آنها.....               |
| ۷۳.....  | <b>فصل ۸: طراحی پلی بوکهای SOAR مؤثر و کارا.....</b>            |
| ۷۴.....  | ۱-۸- شناسایی انواع رخدادها برای توسعه پلی بوک.....              |
| ۷۵.....  | ۲-۸- تعریف دقیق دامنه و اهداف هر پلی بوک.....                   |
| ۷۶.....  | ۳-۸- شناسایی محرکها (Triggers) و ورودیهای پلی بوک.....          |
| ۷۸.....  | ۴-۸- تعیین اقدامات، گردش کارها و نقاط تصمیم گیری.....           |
| ۷۹.....  | ۵-۸- تعریف نقشها و مسئولیتها در اجرای پلی بوکها.....            |
| ۸۰.....  | ۶-۸- آزمون اولیه و اصلاح طرح پلی بوک.....                       |
| ۸۱.....  | ۷-۸- مستندسازی پلی بوکها برای شفافیت و نگهداری.....             |
| ۸۲.....  | نمونه End-to-End طراحی پلی بوک.....                             |
| ۸۷.....  | <b>فصل ۹: پیاده سازی راهحل های SOAR و پلی بوکها.....</b>        |
| ۸۷.....  | ۱-۹- گامهای کلیدی برای پیاده سازی پلتفرم SOAR.....              |
| ۹۰.....  | ۲-۹- پیکربندی پلتفرم SOAR برای اجرای پلی بوکها.....             |
| ۹۲.....  | ۳-۹- یکپارچه سازی SOAR با سایر فناوریهای امنیتی موجود.....      |
| ۹۴.....  | ۴-۹- آزمون و اعتبارسنجی پلی بوکهای پیاده سازی شده.....          |
| ۹۵.....  | ۵-۹- اصلاح و بهینه سازی عملکرد پلی بوکها.....                   |
| ۹۷.....  | ۶-۹- اجتناب از دامهای رایج در پیاده سازی.....                   |
| ۹۹.....  | ۷-۹- مطالعات موردی از پیاده سازی موفق SOAR.....                 |
| ۹۹.....  | ۱-۷-۹- مطالعه موردی اول: یک مؤسسه مالی بزرگ.....                |
| ۱۰۰..... | ۲-۷-۹- مطالعه موردی دوم: یک ارائه دهنده خدمات درمانی متوسط..... |
| ۱۰۰..... | ۳-۷-۹- مطالعه موردی سوم: یک شرکت تجارت الکترونیک.....           |
| ۱۰۳..... | <b>بخش ۴: عملیات، نگهداری و بهینه سازی SOAR.....</b>            |



## فصل ۱۰؛ نگهداری و بهروزرسانی اکوسیستم SOAR شما ..... ۱۰۵

- ۱-۱۰-۱ اهمیت نگهداری منظم و پیشگیرانه پلتفرم SOAR ..... ۱۰۵
- ۱-۱۰-۱-۱ انجام نگهداری مؤثر برای SOAR ..... ۱۰۶
- ۱-۱۰-۲ نگهداری و بهروزرسانی پلی‌بوک‌های SOAR ..... ۱۰۷
- ۱-۱۰-۲-۱ بازبینی و بهروزرسانی منظم محرک‌ها و اقدامات پلی‌بوک ..... ۱۰۸
- ۱-۱۰-۲-۲ نظارت بر عملکرد پلی‌بوک و شاخص‌های کلیدی عملکرد (KPLs) ..... ۱۰۹
- ۱-۱۰-۳-۲ اصلاح و بهبود جریان‌های کاری برای افزایش کارایی ..... ۱۱۰
- ۱-۱۰-۴-۲ انجام آزمون‌ها و تمرین‌های دوره‌ای برای پلی‌بوک‌ها ..... ۱۱۰
- ۱-۱۰-۵-۲ مستندسازی تغییرات و مدیریت نسخه ..... ۱۱۱
- ۱-۱۰-۶-۲ آموزش اعضای تیم امنیتی ..... ۱۱۲
- ۱-۱۰-۳-۱ تکامل استراتژی SOAR همگام با چشم‌انداز تهدیدات ..... ۱۱۳
- ۱-۱۰-۱-۳ درک چشم‌انداز تهدید ..... ۱۱۳
- ۱-۱۰-۲-۳ به‌روز ماندن با Threat Intelligence ..... ۱۱۴
- ۱-۱۰-۳-۳ سازگار کردن پلی‌بوک‌های خودکارسازی ..... ۱۱۴
- ۱-۱۰-۴-۳ بازنگری در اولویت‌بندی ریسک (Risk Prioritization) ..... ۱۱۴
- ۱-۱۰-۵-۳ آموزش و آگاهی‌رسانی منظم ..... ۱۱۵
- ۱-۱۰-۶-۳ بازبینی رخدادها و درس‌آموخته‌ها ..... ۱۱۵
- ۱-۱۰-۴-۱ استراتژی‌های بلندمدت SOAR و بهبود مستمر ..... ۱۱۵
- ۱-۱۰-۴-۱ برنامه‌ریزی راهبردی و تعیین اهداف ..... ۱۱۶
- ۱-۱۰-۲-۴ یادگیری و بهبود مستمر ..... ۱۱۶
- ۱-۱۰-۳-۴ ساخت تیمی توانمند ..... ۱۱۶
- ۱-۱۰-۴-۴ سرمایه‌گذاری در فناوری ..... ۱۱۶
- ۱-۱۰-۵-۴ بازبینی و حسابرسی منظم ..... ۱۱۷
- ۱-۱۰-۶-۴ مدیریت ریسک ..... ۱۱۷

|                                                                             |     |
|-----------------------------------------------------------------------------|-----|
| فصل ۱۱؛ آموزش، آگاهی بخشی و حاکمیت SOAR.....                                | ۱۱۹ |
| ۱-۱۱- آموزش و آگاهی بخشی برای کاربران و ذینفعان SOAR.....                   | ۱۱۹ |
| ۲-۱۱- گزارش دهی، تحلیل داده ها و اندازه گیری عملکرد.....                    | ۱۲۰ |
| ۳-۱۱- حصول اطمینان از انطباق و قابلیت حسابرسی با SOAR.....                  | ۱۲۱ |
| بخش ۵؛ مباحث پیشرفته و چشم انداز آینده.....                                 | ۱۲۵ |
| فصل ۱۲؛ مثال های کاربردی از پلی بوک های SOAR.....                           | ۱۲۷ |
| ۱-۱۲- پلی بوک پاسخ به آلودگی بدافزار (Malware Infection Playbook).....      | ۱۲۷ |
| ۲-۱۲- پلی بوک مقابله با حملات فیشینگ (Phishing Attack Playbook).....        | ۱۲۹ |
| ۳-۱۲- پلی بوک شناسایی و مدیریت تهدیدات داخلی (Insider Threat Playbook)..... | ۱۳۰ |
| ۴-۱۲- پلی بوک پاسخ به نفوذ شبکه (Network Intrusion Playbook).....           | ۱۳۲ |
| ۵-۱۲- پلی بوک مدیریت نقض داده ها (Data Breach Playbook).....                | ۱۳۴ |
| فصل ۱۳؛ بهترین شیوه ها برای به حداکثر رساندن اثربخشی SOAR.....              | ۱۳۷ |
| ۱-۱۳- همسوسازی SOAR با نیازهای خاص سازمانی.....                             | ۱۳۸ |
| ۲-۱۳- تقویت همکاری بین تیم های امنیت و فناوری.....                          | ۱۳۹ |
| ۳-۱۳- شروع با پلی بوک های ساده و توسعه تدریجی.....                          | ۱۳۹ |
| ۴-۱۳- مستندسازی دقیق همه چیز.....                                           | ۱۴۰ |
| ۵-۱۳- آزمون و اعتبارسنجی دقیق و منظم.....                                   | ۱۴۱ |
| ۶-۱۳- اصلاح و بهینه سازی مستمر.....                                         | ۱۴۲ |
| ۷-۱۳- الویت دهی به آموزش و آگاهی بخشی.....                                  | ۱۴۳ |
| ۸-۱۳- بهره گیری از گزارش ها و تحلیل ها برای کسب بینش.....                   | ۱۴۴ |
| فصل ۱۴؛ آینده SOAR و روندهای نوظهور.....                                    | ۱۴۷ |
| ۱-۱۴- روندهای نوظهور در هماهنگ سازی و خودکارسازی امنیتی.....                | ۱۴۸ |
| ۱-۱-۱۴- ادغام با فناوری های نوظهور.....                                     | ۱۴۸ |
| ۲-۱۴- نقش هوش مصنوعی (AI) و یادگیری ماشین (ML) در تقویت SOAR.....           | ۱۵۰ |

- ۱۴-۲-۱- بهبود شناسایی تهدیدات..... ۱۵۰
- ۱۴-۲-۲- پاسخ‌دهی Intelligent..... ۱۵۱
- ۱۴-۲-۳- پاسخ‌دهی هوشمندانه..... ۱۵۱
- ۱۴-۲-۴- قابلیت‌های پیش‌بینی‌کننده..... ۱۵۱
- ۱۴-۲-۵- خودکارسازی وظایف روتین..... ۱۵۱
- ۱۴-۲-۶- چالش‌ها و ملاحظات..... ۱۵۲
- ۱۴-۳- آماده‌سازی سازمان برای تحولات آینده SOAR..... ۱۵۲
- ۱۴-۳-۱- به‌روز ماندن..... ۱۵۳
- ۱۴-۳-۲- سرمایه‌گذاری در فناوری..... ۱۵۳
- ۱۴-۳-۳- آموزش و توسعه..... ۱۵۳
- ۱۴-۳-۴- انطباق با چشم‌انداز در حال تحول تهدیدات..... ۱۵۳
- ۱۴-۳-۵- شکار پیش‌دستانه تهدیدات..... ۱۵۴
- ۱۴-۳-۶- حریم خصوصی و انطباق قانونی..... ۱۵۴
- بخش ۶؛ نتیجه‌گیری..... ۱۵۷**
- فصل ۱۵؛ جمع‌بندی و مسیر پیش رو..... ۱۵۹**
- ۱۵-۱- بازبینی نکات کلیدی، مفاهیم و شیوه‌های عملی..... ۱۵۹
- ۱۵-۲- مسیر پیش‌رو با SOAR: چالش‌ها و فرصت‌ها..... ۱۶۱
- ۱۵-۲-۱- یادگیری مستمر..... ۱۶۱
- ۱۵-۲-۲- سرمایه‌گذاری در نوآوری..... ۱۶۱
- ۱۵-۲-۳- ایجاد روابط همکاری..... ۱۶۲
- ۱۵-۲-۴- تقویت فرهنگ امنیت سایبری..... ۱۶۲
- ۱۵-۲-۵- ممیزی‌ها و بازبینی‌های منظم..... ۱۶۲
- ۱۵-۲-۶- برنامه‌ریزی برای تاب‌آوری..... ۱۶۲
- ۱۵-۲-۷- تعامل با جامعه امنیت سایبری..... ۱۶۲
- ۱۵-۳- سخن پایانی و تشویق به اقدام..... ۱۶۳