DIYAKO
Secure Bow

SOC Survey

SANS

2025

یافته‌های کلیدی

۴۳٪ از پاسخ‌دهندگان می‌گویند تسلط بر SIEM مهم‌ترین مهارت فنی موردنظر آن‌ها در زمان جذب نیرو است.

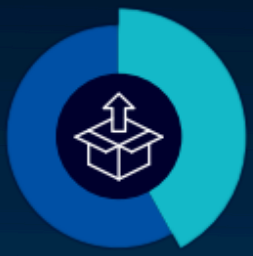
۴۲٪ از مراکز عملیات امنیتی (SOC) تمام داده‌های ورودی را مستقیماً وارد سیستم مدیریت اطلاعات و رویدادهای امنیتی (SIEM) می‌کنند، آن‌هم اغلب بدون داشتن برنامه‌ای برای بازیابی یا مدیریت آن‌ها.

۸۵٪ از پاسخ‌دهندگان می‌گویند هشدارهای امنیتی مربوط به Endpointها، اصلی‌ترین عامل آغاز واکنش آن‌هاست.

۷۹٪ از مراکز عملیات امنیتی (SOC) به‌صورت ۲۴ ساعته و در تمام ایام هفته فعال هستند.

۶۹٪ از مراکز عملیات امنیتی (SOC) همچنان برای گزارش‌دهی شاخص‌ها (Metrics) به فرآیندهای کاملا دستی یا غالبا دستی متکی هستند.

۶۹٪ از مراکز عملیات امنیتی (SOC) از داده‌های هوش تهدیدات سایبری (CTI) عمدتاً برای پاسخ‌گویی به رخدادها استفاده می‌کنند.



۴۲٪ از مراکز عملیات امنیتی (SOC) ابزارهای هوش مصنوعی و یادگیری ماشین (AI/ML) را به‌صورت پیش‌فرض و بدون هیچ‌گونه سفارشی سازی استفاده می‌کنند.

پویایی نیروی انسانی و استخدام

۴۲٪

از کارکنان مرکز عملیات امنیتی (SOC) از بودجه SOC اطلاع ندارند که نشان‌دهنده‌ی فاصله و عدم هماهنگی بین تیم‌های فنی و تجاری است.

۶۲٪

از متخصصان مراکز عملیات امنیتی (SOC) معتقدند که سازمانشان به اندازه کافی برای حفظ استعدادهای برتر تلاش نمی‌کند.

۷۳٪

از سازمان‌ها گاهی به اعضای تیم مرکز عملیات امنیتی (SOC) اجازه دورکاری می‌دهند.

۳ تا ۵ سال

رایج‌ترین مدت زمان حضور کارکنان در مراکز عملیات امنیتی (SOC) است.

۲ تا ۱۰ نفر

رایج‌ترین اندازه برای یک مرکز عملیات امنیتی (SOC) با نیروی کامل است.

خلاصه اجرایی

در نه سال گذشته، مؤسسه SANS هر سال یک نظرسنجی صنعتی برگزار کرده تا درک بهتری از نحوه ساخت، تجهیز و مدیریت مراکز عملیات امنیتی (SOC) به دست آورد و همچنین چالش‌های اصلی تحلیل‌گران SOC و فرصت‌های بهبود در صنعت را شناسایی کند. هدف از نظرسنجی امسال این بود که بینشی در مورد عملکرد SOCها در مقایسه با یکدیگر ارائه دهد، اولویت‌های بهبود در سال پیش رو را مشخص کند و شناخت بهتری از فناوری‌های مؤثر و کم‌اثر در سراسر صنعت امنیت به‌دست آورد.

گزارش امسال به بررسی داده‌ها و بینش‌هایی می‌پردازد که شامل مقایسه ساختار SOCها، روندهای برون‌سپاری، ملاحظات فناوری، حوزه‌های قابل بهبود و روش‌های پیاده‌سازی فناوری‌های مختلف است.
اگرچه هوش مصنوعی آخرین روند فناورانه محسوب می‌شود، اما نکته قابل توجه این است که در طول نه سال اجرای این نظرسنجی، قابلیت‌ها، سطح نیروی انسانی، خدمات برون‌سپاری‌شده و چالش‌های مرتبط با عملیات امنیتی، عمدتاً بدون تغییر باقی مانده‌اند.

عملیات امنیتی مسیری بلندمدت و تدریجی است که برای رسیدن به نتایج مؤثر، نیازمند صبر، پشتکار و تعهد مستمر است.

دموگرافی پاسخ دهندگان

بیشتر پاسخ‌دهندگان در ایالات متحده مستقر بودند و شرکت‌کنندگانی از ۵۷ کشور مختلف نیز در نظرسنجی حضور داشتند. صنایع اصلی شامل ترکیب معمولی از بخش‌های بانکداری و امور مالی (۱۶٪)، امنیت سایبری (۱۴٪)، فناوری (۱۴٪) و دولت (۱۴٪) بودند. همچنین، اندازه سازمان‌ها نیز تنوع بالایی داشت. شکل ۱ جزئیات دموگرافی پاسخ‌دهندگان نظرسنجی را نشان می‌دهد.

شکل ۱. مشخصات جمعیتی پاسخ‌دهندگان نظرسنجی

تعریف مرکز عملیات امنیتی (SOC)

مرکز عملیات امنیتی (SOC) مدرن در سال ۲۰۲۵ حول چند عنصر بنیادین ساخته شده است که نحوه عملکرد آن، نقاط قوتش و سازگاری‌اش با تهدیدات در حال تحول را تعیین می‌کنند. این عناصر شامل توانمندی‌های اصلی، مدل عملیاتی (داخلی یا برون‌سپاری شده)، معماری داده‌ها و استراتژی نیروی انسانی هستند. بر اساس داده‌های نظرسنجی جاری، یک SOC عملیاتی معمولی دارای چهار ویژگی زیر است:

- **توانمندی‌ها:** وظایف اصلی مرکز عملیات امنیتی (SOC) و کارهای روزمره‌ای که انجام می‌دهد.
- **عملکرد داخلی در مقابل برون‌سپاری:** وظایفی که به‌صورت داخلی انجام می‌شود در مقابل آن‌هایی که به طرف‌های ثالث واگذار شده‌اند.
- **معماری:** ساختار جمع‌آوری، ذخیره‌سازی و دسترسی به داده‌ها و محل انجام این فرآیندها.
- **نیروی انسانی و ساعات کاری:** جزئیاتی درباره اندازه تیم، نقش‌ها، مهارت‌های مورد انتظار و اینکه SOC به‌صورت ۲۴ ساعت می باشد یا در ساعات محدود فعالیت می‌کند.

علاوه بر این، بر اساس داده‌ها، یک مرکز عملیات امنیتی (SOC) پایه می‌تواند به شرح زیر تعریف شود:

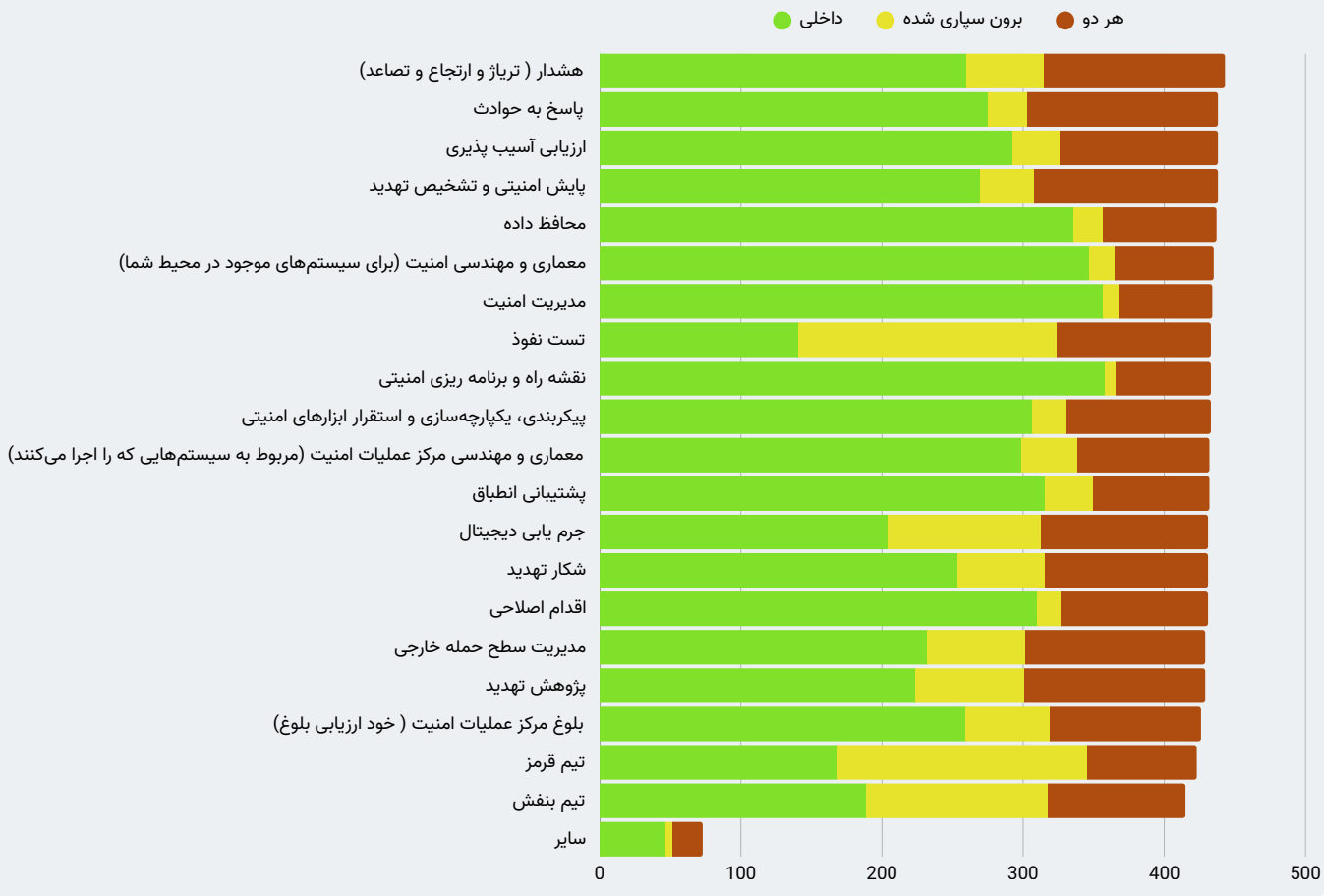
- اولویت اصلی آن دسته‌بندی هشدارها، شناسایی تهدیدات و پاسخ به رخدادها به عنوان وظایف کلیدی است، در حالی که هوش تهدید، مدیریت آسیب‌پذیری‌ها و شکار تهدید به عنوان وظایف پشتیبانی عمل می‌کنند.
- تیمی متشکل از ۱۰ نفر تمام‌وقت (یا معادل تمام‌وقت) دارد که میانگین مدت زمان حضور کارکنان بین سه تا پنج سال است.
- بیشتر فعالیت‌های نظارت، شناسایی و پاسخ به رخدادها به صورت داخلی انجام می‌شود، در حالی که تست نفوذ، بررسی‌های دیجیتال قانونی، بخشی از اطلاعات تهدید و سایر وظایف نیازمند تخصص یا مهارت بالاتر به برون‌سپاری واگذار شده‌اند.
- معماری متمرکزی دارد، با رشد پذیرش رایانش ابری، هرچند همچنان از نظر حجم استفاده عقب‌تر از پذیرش ابری در بخش فناوری اطلاعات است.
- در اکثر موارد به‌صورت ۲۴ ساعته و هفت روز هفته فعال است، اگرچه برخی هنوز به پوشش چرخشی یا افزایش واکنش «بر حسب نیاز» متکی هستند.
- گزارش‌دهی شاخص‌ها به‌صورت دستی انجام می‌شود، اگرچه نزدیک به نیمی از پاسخ‌دهندگان این روش را وقت‌گیر می‌دانند. اتوماسیون هنوز محدود است.
- به شدت به ابزار EDR به عنوان قابل اعتمادترین و بالغ‌ترین ابزار متکی است، در حالی که هوش مصنوعی و یادگیری ماشین (AI/ML) در پایین‌ترین رتبه رضایت قرار دارند.
- بیش از همیشه داده ذخیره می‌کند و اغلب همه داده‌ها را بدون برنامه مشخصی برای مدیریت یا تحلیل، مستقیماً به SIEM یا syslog ارسال می‌کند که منجر به مشکلات دیدپذیری و مدیریت اطلاعات می‌شود.

توانمندی‌ها و برون‌سپاری

انتظارات از وظایف مرکز عملیات امنیتی (SOC) گسترده و جامع است. پاسخ‌های نظرسنجی به‌وضوح نشان می‌دهد که عدم پوشش مسئولیت‌های اصلی، چه به‌صورت داخلی و چه از طریق برون‌سپاری، منجر به ناکارآمدی SOC در شناسایی و پاسخ‌گویی به تهدیدات خواهد شد.

اگرچه در تقسیم فعالیت‌ها بین تیم‌های داخلی و تامین کنندگان خارجی مانند MSSPها تنوع وجود دارد، اما انتظارات اصلی از عملکرد SOC به طور سالانه تا حد زیادی ثابت مانده است. سه فعالیت برتر گزارش‌شده عبارت‌اند از برنامه‌ریزی و نقشه راه امنیتی (۸۰٪)، مدیریت امنیت (۸۰٪) و معماری و مهندسی امنیت (۷۸٪).

چه فعالیت‌هایی در مرکز عملیات امنیتی (SOC) شما انجام می‌شود؟
کدام فعالیت‌ها به‌طور کامل یا جزئی به سرویس دهندگان خارجی واگذار شده‌اند، چه از طریق ارائه‌دهنده خدمات مدیریت امنیت (MSSP) و چه به دلیل میزبانی ابری؟



شکل ۲. تعداد پاسخ‌ها درباره فعالیت‌های عملیاتی مرکز عملیات امنیت (SOC) مرتبط با برون‌سپاری

مقایسه توانمندی‌های داخلی و برون‌سپاری‌شده در SOC

عملکردهای اصلی مرکز عملیات امنیتی (SOC) مانند معماری، نظارت و تطابق معمولاً به‌صورت داخلی انجام می‌شوند. احتمالاً دلیل این موضوع نیاز این حوزه‌ها به درک عمیق از سیستم‌های داخلی، اولویت‌های کسب‌وکار و زمینه سازمانی است. این فعالیت‌ها همچنین مستلزم هماهنگی نزدیک با ذی‌نفعان حقوقی و مدیریتی هستند، که اجرای آن‌ها را در صورت انجام داخلی، مؤثرتر می‌سازد.

سوالی که از شرکت کنندگان پرسیده شد به همراه نتایج آن.
کدام‌یک از گزینه‌های زیر بهترین توصیف را از قابلیت پاسخ‌گویی به رخداد در مرکز عملیات امنیتی (SOC) شما ارائه می‌دهد؟

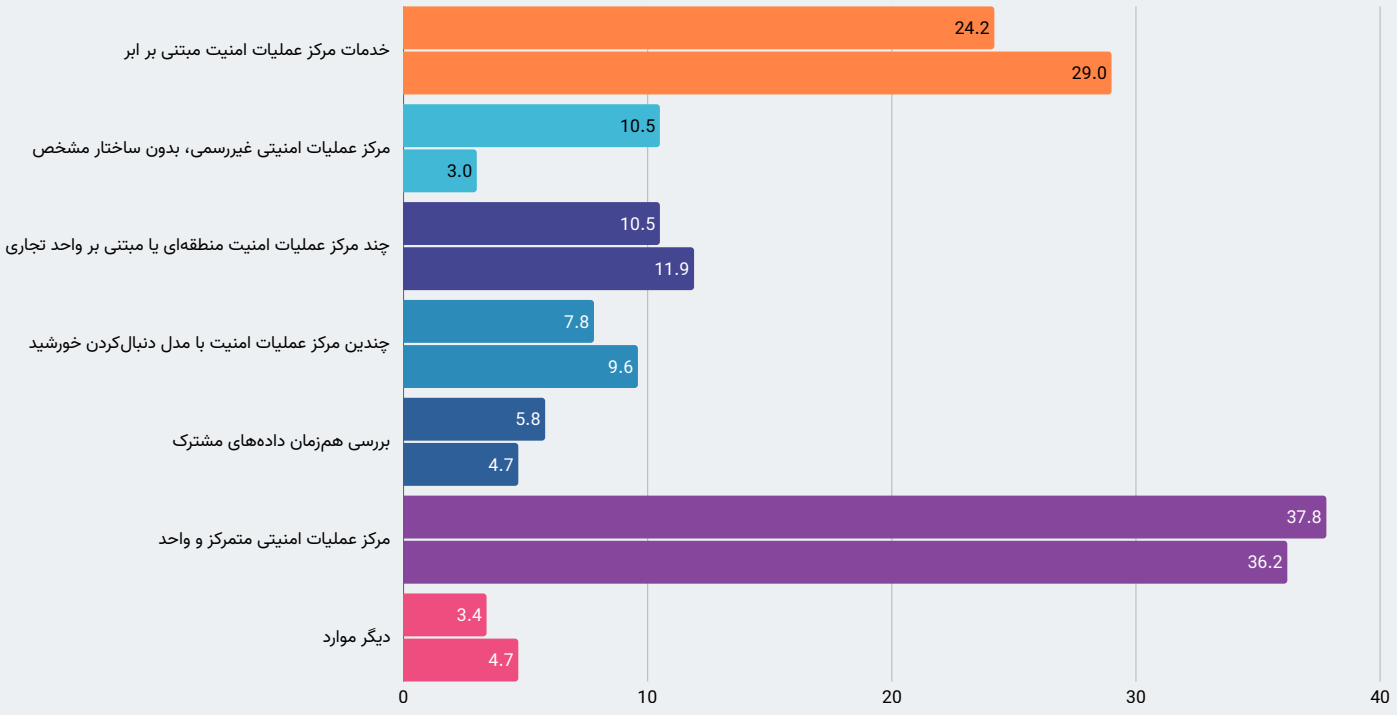
پاسخ‌گویی به رخداد، بخشی کاملاً یکپارچه از قابلیت داخلی SOC ما است.	50.9%
ما از پاسخ‌دهندگان داخلی برای مدیریت رخدادها استفاده می‌کنیم که این وظیفه را به‌صورت موردی و در صورت نیاز انجام می‌دهند.	47.9%
ما از پاسخ‌دهندگان داخلی استفاده می‌کنیم که با ارائه‌دهنده خدمات خارجی SOC ما همکاری دارند.	17.2%
ما از پاسخ‌دهندگان به رخداد استفاده می‌کنیم که توسط ارائه‌دهنده خدمات خارجی SOC ما تأمین می‌شوند.	16.9%
پاسخ‌گویی به رخدادها توسط یک ارائه‌دهنده خدمات انجام می‌شود که جزئی از همکاری ما در حوزه خدمات SOC نیست.	16.0%
ما از پاسخ‌دهندگان داخلی اختصاصی برای مدیریت رخدادها استفاده می‌کنیم، اما آن‌ها از SOC جدا هستند و برنامه‌ای برای یکپارچه‌سازی با SOC وجود ندارد.	14.8%
ما از پاسخ‌دهندگان داخلی استفاده می‌کنیم که در تلاش برای یکپارچه‌سازی آن‌ها با SOC داخلی خود هستیم، اما هنوز این کار انجام نشده است.	12.7%
موارد دیگر	2.4%

شکل ۳. قابلیت‌های واکنش به حوادث (Incident Response)

معماری

بیشتر پاسخ‌دهندگان (۳۸٪) اعلام کرده‌اند که یک مرکز عملیات امنیتی (SOC) متمرکز و واحد را اداره می‌کنند که این معماری در حال حاضر رایج‌ترین مدل است. استقرار SOC مبتنی بر ابر در رتبه دوم با ۲۴٪ قرار دارد، اما پاسخ‌دهندگان نشان داده‌اند که تغییرات برنامه‌ریزی‌شده باعث افزایش این رقم به ۲۹٪ در ۱۲ ماه آینده خواهد شد که بیانگر علاقه فزاینده به عملیات امنیتی بومی ابر است.

سوال زیر از شرکت کنندگان پرسیده شده و نتایج آن نیز آورده شده است.
زیرساخت (معماری) مرکز عملیات امنیتی (SOC) شما در حال حاضر چگونه استقرار یافته و یا احتمالاً در ۱۲ ماه آینده چگونه تغییر خواهد کرد؟



شکل ۴. معماری مرکز عملیات امنیت (SOC)، وضعیت فعلی و برنامه‌ریزی‌شده

با وجود تبلیغات گسترده پیرامون مرکز عملیات امنیتی (SOC) مبتنی بر ابر، معماری‌های متمرکز و درون‌سازمانی همچنان مدل غالب محسوب می‌شوند. فاصله بین اهداف اعلام‌شده برای مهاجرت به فضای ابری و پیاده‌سازی‌های واقعی، واقعیتی را نشان می‌دهد: مهاجرت به ابر، به‌ویژه در حوزه عملیات امنیتی، هنوز در مرحله گذار قرار دارد.
اگرچه SOCهای متمرکز و یکپارچه همچنان پیشتاز هستند، داده‌های سال‌به‌سال هنوز نشانه‌ای از یک تغییر معماری قاطع به‌سوی فضای ابری ارائه نمی‌دهند.
با تشدید بی‌ثباتی‌های سیاسی جهانی تا سال‌های ۲۰۲۵ و ۲۰۲۶، انتظار می‌رود که بررسی‌ها و حساسیت‌ها نسبت به جریان‌های بین‌المللی داده افزایش یابد. درگیری‌های ژئوپلیتیکی، باعث تمرکز بیشتر نهادهای نظارتی و سازمان‌ها بر روی محل ذخیره‌سازی داده، افراد دارای دسترسی نهادهای نظارت‌کننده بر داده‌ها شده است.

SOCها باید آمادگی پاسخ‌گویی به سؤالات دشوار در خصوص دیدپذیری فرامرزی، نظارت توسط اشخاص ثالث و محل اقامت داده‌ها را داشته باشند. این موارد صرفاً مسائل فنی نیستند، بلکه نگرانی‌های حقوقی و راهبردی نیز محسوب می‌شوند. رهبران امنیتی باید انتظار مشارکت عمیق‌تر از سوی واحدهای حقوقی، تطابق مقررات (Compliance) و ذی‌نفعان کسب‌وکار را داشته باشند، چرا که این موضوعات در حال تبدیل شدن به اولویت‌های اصلی در دستور کار سازمان‌ها هستند.

چالش های SOC مدرن

امروزه مراکز عملیات امنیتی (SOC) برای کسب نتایجی سریع‌تر، هوشمندانه‌تر و پیش‌گیرانه‌تر (Proactive) در امنیت سایبری تحت فشار هستند، اما چندین شکاف حیاتی مانع دستیابی به این هدف شده‌است. ابزارهای هوش مصنوعی و یادگیری ماشین (AI/ML) با سرعت زیادی در حال رشد هستند، اما در صورتی که بدون یکپارچگی هدفمند و نظارت کافی استفاده شوند، اغلب باعث هدر رفت بودجه، افزایش ریسک و ناکامی در ارائه پشتیبانی مؤثر می‌شوند. هم‌زمان، هوش تهدید (با وجود فراوانی) اغلب به‌دلیل استفاده ناهماهنگ و نبود تحلیل عینی، به‌درستی به‌کار گرفته نمی‌شود و تیم‌ها را در وضعیت واکنشی (Reactive) نگه می‌دارد. همچنین، با اینکه رهگیری ارتباط TLS منبع مستقیم اطلاعات نیست(به علت رمزنگاری)، به یکی از نقاط بحث‌برانگیز در موضوع دیدپذیری (Visibility) تبدیل شده و نگرانی‌هایی درباره حریم خصوصی، عملکرد و اعتماد ایجاد کرده است. این مسائل در مجموع نشان‌دهنده نیازی عمیق‌تر به هم‌راستایی راهبردی و اتخاذ رویکردهای عملیاتی هوشمندتر در سطح SOC هستند.

کارکنان مراکز عملیات امنیتی (SOC) به‌طور گسترده از ابزارهای هوش مصنوعی و یادگیری ماشین (AI/ML) استفاده می‌کنند، اما این استفاده بدون یکپارچگی هدفمند و نظارت مناسب صورت می‌گیرد. این ابزارها در اصل ارزشمند هستند، اما ممکن است منجر به هدررفت بودجه، افزایش ریسک و عدم ارائه پشتیبانی مؤثر برای عملیات SOC شوند. اگرچه میزان رضایت از این فناوری‌ها پایین است، گزارش‌ها نشان می‌دهد که میزان استفاده از آن‌ها همچنان بالاست.

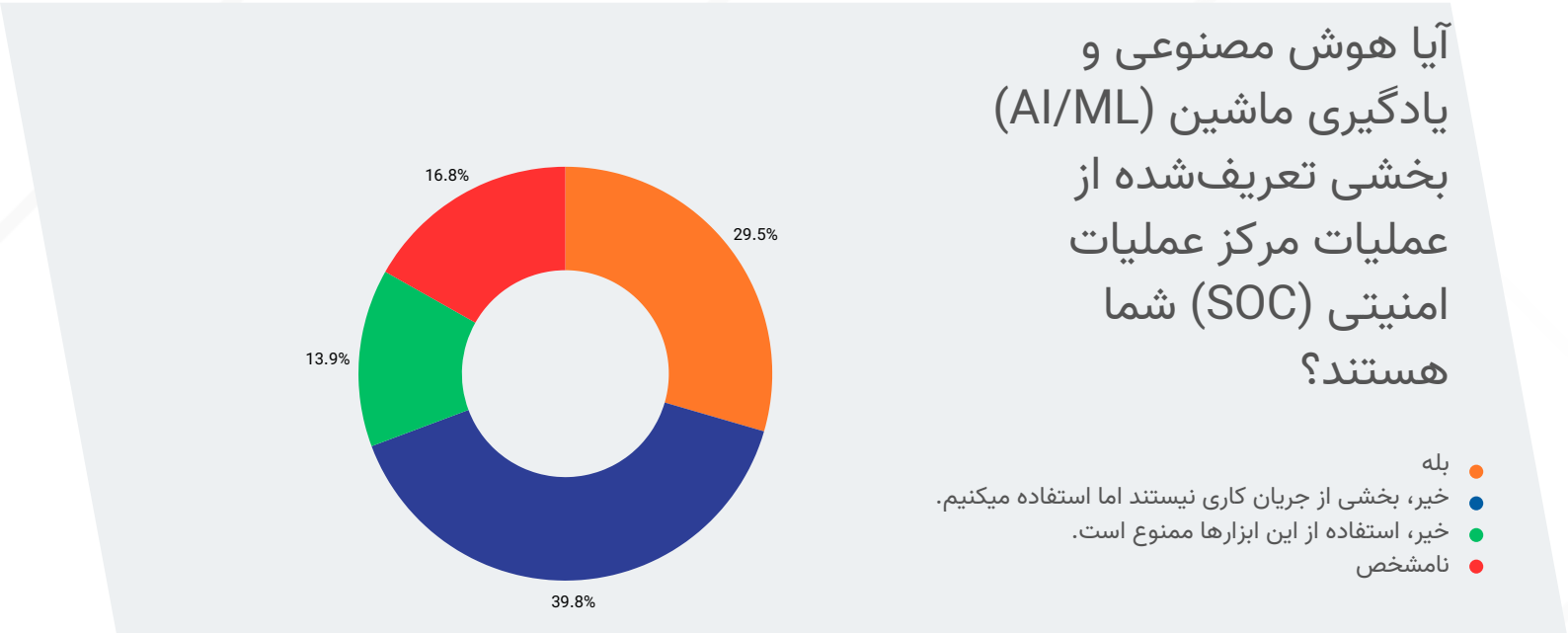
هوش مصنوعی و یادگیری ماشین

با توجه به تأثیر قابل‌توجه ابزارهای هوش مصنوعی (AI) و یادگیری ماشین (ML) بر مراکز عملیات امنیتی (SOC) در سال‌های اخیر، آشنایی بیشتر با تأثیر این دو حوزه همچنان اهمیت زیادی خواهد داشت. جالب است که داده‌ها نشان می‌دهد اکثریت (۴۰٪) از این ابزارها استفاده می‌کنند، اما این ابزارها بخشی از عملیات تعریف‌شده SOC نیستند (به شکل ۵ مراجعه کنید).

احتمالاً یک SOC با دو وظیفه داخلی روبروست که باید به آن‌ها رسیدگی کند:

۱. اولویت داخلی SOC : تغییر از استفاده فردی و ناهماهنگ از ابزارهای هوش مصنوعی و یادگیری ماشین (AI/ML) به یک پیاده‌سازی استاندارد و مورد تأیید تیم؛ به‌گونه‌ای که نقاط قوت این ابزارها به حداکثر برسد و در عین حال ریسک‌ها به حداقل کاهش یابد.

۲. اولویت خارجی SOC : حفظ نظارت بر داده‌هایی که از سازمان به پلتفرم‌های AI/ML و سامانه‌های فناوری اطلاعات غیرمجاز (Shadow IT) منتقل می‌شوند. هرچند ممکن است بسیاری از این داده‌ها کم‌ریسک به نظر برسند، اما ضروری است ابزارهای پیشگیری از نشت اطلاعات (DLP) host-base به‌عنوان بخشی از استقرار استاندارد در نظر گرفته شوند تا دیدپذیری(Visibility) و کنترل حفظ شود.



شکل 5. هوش مصنوعی و یادگیری ماشین در عملیات مرکز امنیت (SOC)

آقای Seth Misner (نویسنده دو دوره LDR414 و SEC511)

نظرسنجی SOC در سال ۲۰۲۵ یک تضاد نگران‌کننده را برجسته می‌کند؛ مراکز عملیات امنیتی با دشواری در جذب و نگه‌داشت تحلیل‌گران ماهر مواجه‌اند، در حالی که هوش مصنوعی (AI)، یادگیری ماشین (ML) و خودکارسازی، بیشترین برنامه‌ریزی برای توسعه را به خود اختصاص داده‌اند، با اینکه کمترین میزان ارزش واقعی را ارائه داده‌اند. هوش مصنوعی باید به‌عنوان مکملی برای تحلیل‌گران عمل کند، نه جایگزین آن‌ها. نگرانی من این است که مدیران ممکن است به AI به چشم یک راه میان‌بُر برای پر کردن خلأ نیروی انسانی نگاه کنند، به‌جای آن‌که در استعداد انسانی و یکپارچگی هدفمند AI سرمایه‌گذاری کنند؛ چیزی که برای بهبود واقعی و اساسی عملکرد SOC ضروری است.

تیم‌های امنیت سایبری ممکن است مستقیماً مسئول ریسک‌های ناشی از خطاهای هوش مصنوعی یا خروجی‌های نادرست نباشند، اما مرکز عملیات امنیتی (SOC) می‌تواند نقش کلیدی در کاهش تأثیرات تجاری آن‌ها ایفا کند. تیم‌های **حکمرانی، ریسک و انطباق (GRC)** به پشتیبانی فنی نیاز دارند تا بتوانند نحوه استفاده از ابزارهای هوش مصنوعی و سیستم‌ها یا داده‌هایی که این ابزارها با آن‌ها تعامل دارند را پایش کنند.

هوش تهدید (Threat Intelligence)

فعالیت‌های مرتبط با هوش تهدید (Threat Intelligence) بخش قابل‌توجهی از عملیات SOC را تشکیل می‌دهند (۷۳٪) و استفاده اصلی از آن‌ها در پاسخ به حوادث است (۶۹٪). شکل ۶ روش‌های مختلف استفاده از داده‌ها و هوش تهدید سایبری (CTI) را نشان می‌دهد. معمولاً اطلاعات CTI از طریق ایمیل یا اسناد (۵۶٪) و یا گزارش‌ها (۵۵٪) منتشر می‌شود.

از آنجا که هوش تهدید عمدتاً مبتنی بر تحلیل هست، از پاسخ‌دهندگان درباره روش‌های تحلیلی که بیشترین استفاده را دارند سؤال شد. رایج‌ترین پاسخ (۷۲٪) این بود که تحلیل‌گران بر اساس تجربه و شهود خود عمل می‌کنند. هرچند تخصص نقش مهمی دارد، اما دلایل محکمی وجود دارد برای اینکه روش‌های تحلیلی ساختارمندتری (مانند روش‌های مفهومی یا استقرایی) در فرایند تحلیل گنجانده شوند تا انسجام بیشتری ایجاد شود و سوگیری کاهش یابد.

علاوه بر این، اکثر اطلاعات از منابع خارجی به دست می‌آید، که این موضوع نشان‌دهنده‌ی نیاز فزاینده به تولید هوش تهدید از منابع داخلی سازمان است، نه فقط تکیه بر فیدهای خارجی. بهره‌گیری از داده‌های داخلی می‌تواند ارزیابی ریسک، شکار تهدید و توانمندی‌های واکنش را تقویت کند.

مؤثرترین روش برای ایجاد هوش تهدید داخلی، همکاری و اشتراک‌گذاری اطلاعات است. با این حال، تیم‌های هوش تهدید مستقر در SOC ممکن است از حمایت سازمانی کافی برای این همکاری برخوردار نباشند. در چنین مواردی، همکاری غیررسمی با همتایان می‌تواند راه‌حلی عملی و قابل قبول باشد.

اطلاعات و داده‌های CTI (اطلاعات تهدید سایبری) در سازمان شما چگونه مورد استفاده قرار می‌گیرند؟ همه گزینه‌های مرتبط را انتخاب کنید.

شکل ۶. شمارش پاسخ‌ها درباره استفاده از داده‌های CTI در درون سازمان

پاسخ به حادثه واکنشی(Reactive) است، نه پیش‌دستانه(Proactive).

توانایی پاسخ به حادثه در SOC عمدتاً به دو صورت توصیف شده است: یا کاملاً به‌عنوان بخشی از SOC داخلی یکپارچه است (۵۱٪) یا از طریق پاسخ‌دهندگان داخلی حادثه که به‌صورت موردی و در صورت نیاز عمل می‌کنند (۴۸٪). داده‌ها همچنین نشان می‌دهند که آغاز پاسخ به حادثه عمدتاً توسط هشدارهای امنیتی داخلی تحریک می‌شود (۸۵٪). وقتی درباره میزان رضایت از قابلیت‌های پاسخ به حادثه پرسیده شد، پاسخ‌دهندگان بیشترین رضایت را از ابزارهای تشخیص و پاسخ (EDR) و مهار مهاجمین داشتند و کمترین رضایت را از فناوری‌های فریب (Deception Technologies) ابراز کردند که این روند از سال ۲۰۲۲ به‌صورت پیوسته ادامه دارد. تنها ابزارهای هوش مصنوعی و یادگیری ماشین (AI/ML) در سال‌های اخیر رتبه بدتری داشته‌اند.

وقتی درباره شکار تهدید پرسیده شد، وضعیت مشابهی مشاهده شد. اکثر تیم‌ها شکار تهدید نیمه‌خودکار با استفاده از ابزارهای ارائه‌شده توسط تامین کننده را توصیف کردند (۴۸٪). اگرچه این از نظر فنی نوعی شکار محسوب می‌شود، اما اغلب به تحلیل‌های مبتنی بر گذشته محدود می‌شود و شکار واقعی مبتنی بر تکنیک نیست. این تفاوت اهمیت دارد چون شکار مؤثر نیازمند تحلیل‌گران ماهر است که همچنان کمبود آن وجود دارد. کمبود نیروی ماهر بزرگ‌ترین مانع ذکرشده برای عدم انجام شکار پیشرفته‌تر توسط تیم‌هاست (۱۶٪). جزئیات بیشتر در بخش بعدی ارائه شده است.

اجرای Windows Defender با Signatureهای به‌روز شده و اسکن فایل‌ها، شکار تهدید نیست؛ این تشخیص پایه‌ای است. اگرچه قابلیت‌های جستجوی تاریخی به دلیل پیشرفت ابزارهای ارائه‌شده توسط تامین کننده در حال بهبود است، اما SOCها باید دیگر این کار را «شکار» ننامند. هنوز ارزش واقعی در انجام شکار به روش سخت و سنتی وجود دارد. شکار واقعی تهدید مبتنی بر روش‌های اثبات‌شده، تحلیل فرضیه‌محور و آشنایی عمیق با رفتار مهاجم است. هشدارها برای شناسایی تهدیدات شناخته شده طراحی شده‌اند، اما مهاجمین پیچیده همیشه باعث فعال شدن آن‌ها نمی‌شوند. آن‌ها به صورت پنهانی و زیر آستانه تشخیص فعالیت می‌کنند و اگر فعالانه شکار نکنید، آن‌ها را پیدا نخواهید کرد.

اجرای اسکن Windows Defender شکار تهدید نیست، بلکه تشخیص پایه‌ای است. شکار واقعی تهدید شامل تحلیل فرضیه‌محور و دانش عمیق رفتار مهاجم برای کشف تهدیدات مخفی است که از هشدارها فرار می‌کنند.

نیروی انسانی SOC و نگهداشت آن

با وجود روند رو به رشد «بازگشت به دفتر کار» (RTO) در ایالات متحده، ۷۳٪ از پاسخ‌دهندگان اعلام کردند که کارکنان SOC می‌توانند از خانه کار کنند. با این حال، پاسخ‌ها نشان می‌دهند که این اجازه به نقش و مجموعه مهارت‌های خاص هر فرد بستگی دارد. به‌طور خلاصه، اگرچه بیشتر مراکز SOC از نظر اصولی با کار از راه دور موافق‌اند، اما هر عضوی از تیم این انعطاف‌پذیری را دریافت نمی‌کند حتی زمانی که فناوری لازم نیز فراهم است.

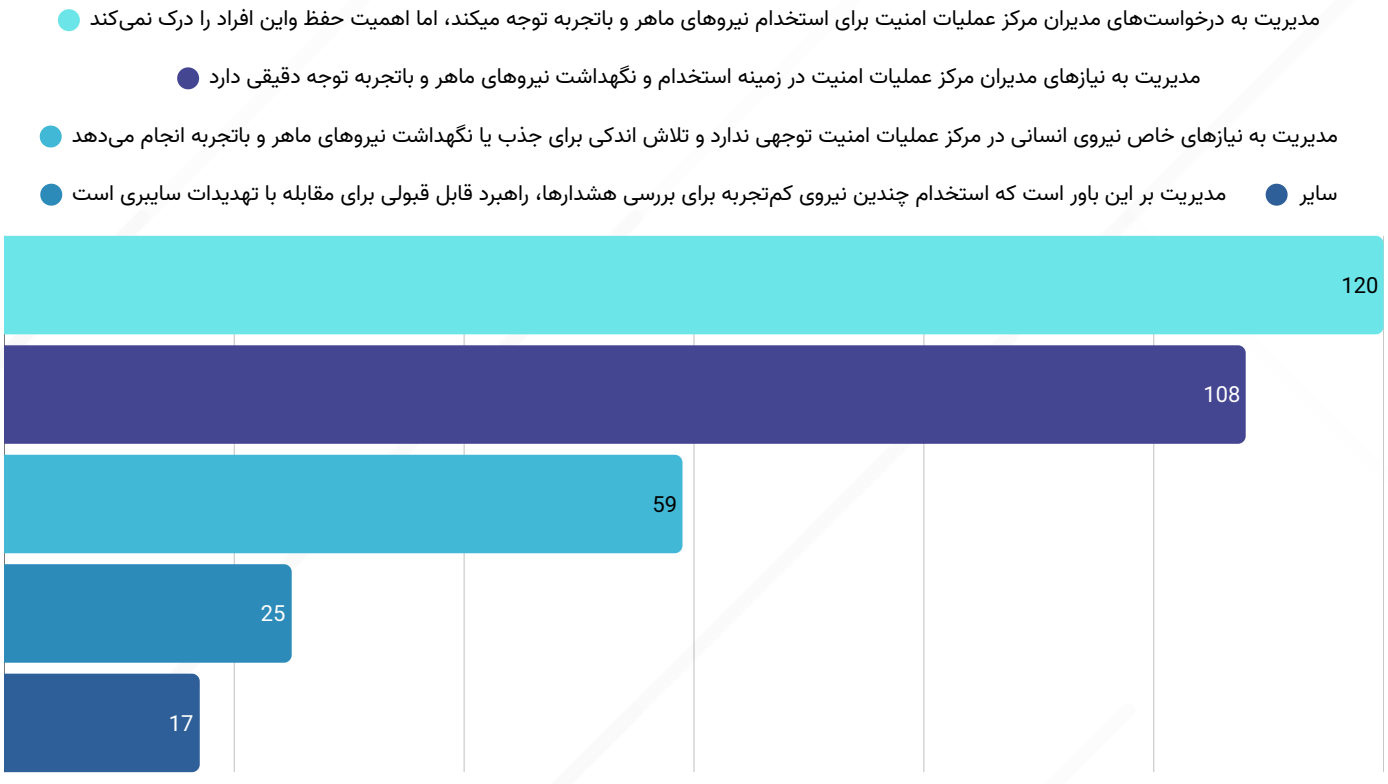
تیم‌های SOC به‌طور دائمی با کمبود کارکنان ماهر مواجه‌اند. این یک چالش مستمر است و رهبران SOC می‌گویند سازمان‌هایشان اقدامات کافی برای حفظ بهترین نیروهایی که در اختیار دارند، انجام نمی‌دهند. نگهداشت کارکنان فقط یک موضوع منابع انسانی نیست؛ بلکه نشان‌دهنده اولویت‌های رهبری است. حفظ بهره‌وری و اثربخشی بالای SOC دشوار خواهد بود اگر نرخ ترک شغل بالا باشد. اگر می‌خواهید تیم‌تان بماند، باید نشان دهید که به‌طور جدی به عوامل رضایت شغلی اهمیت می‌دهید.

در حالی که کمبود نیروی متخصص همچنان به عنوان مهم‌ترین چالش مراکز SOC مطرح می‌شود، ۶۲٪ از پاسخ‌دهندگان به‌طور آشکار اعلام کرده‌اند که به توانایی یا اراده سازمان خود برای رسیدگی مؤثر به این مشکل از طریق برنامه‌های واقعی نگهداشت نیروی انسانی اعتماد ندارند (شکل ۷). این شکاف نشان‌دهنده یک مشکل عمیق‌تر است: شاید استراتژی‌هایی برای نگهداشت نیرو وجود داشته باشد، اما برای کسانی که قرار است از آن بهره‌مند شوند، قابل رؤیت یا معتبر نیستند. بهبود شفافیت در مورد این برنامه‌ها و اجرای واقعی آن‌ها (نه صرفاً شعارهای تبلیغاتی) می‌تواند در بازسازی اعتماد و حفظ استعدادها نقش مؤثری داشته باشد.

جالب است که با وجود این بی‌اعتمادی، پاسخ‌دهندگان معمولاً بین سه تا پنج سال در محیط SOC باقی می‌مانند (۳۱٪) و تنها درصد بسیار کمی بیش از ده سال در این حوزه می‌مانند (۴٪).

یکی از رایج‌ترین سوالاتی که رهبران مراکز عملیات امنیت (SOC) با آن مواجه‌اند این است: برای اداره یک SOC به چند نفر نیروی انسانی نیاز است؟
رایج‌ترین پاسخ عدد ۱۰ نفر (به‌صورت معادل تمام‌وقت یا FTE) است، این نقطه شروع خوبی برای برنامه‌ریزی محسوب می‌شود. این تعداد امکان پوشش مناسب برای عملکردهای کلیدی مانند پایش، پاسخ به حوادث، هوش تهدید (Threat Intelligence) و مهندسی را فراهم می‌کند.
البته در شرکت‌های بزرگ چندملیتی، تیم‌های SOC می‌توانند به‌راحتی به صدها نفر گسترش یابند. اما برای بیشتر سازمان‌هایی که به‌دنبال حفظ یک توانمندی داخلی قوی هستند، عدد ۱۰ نفر عددی منطقی برای برنامه‌ریزی است.

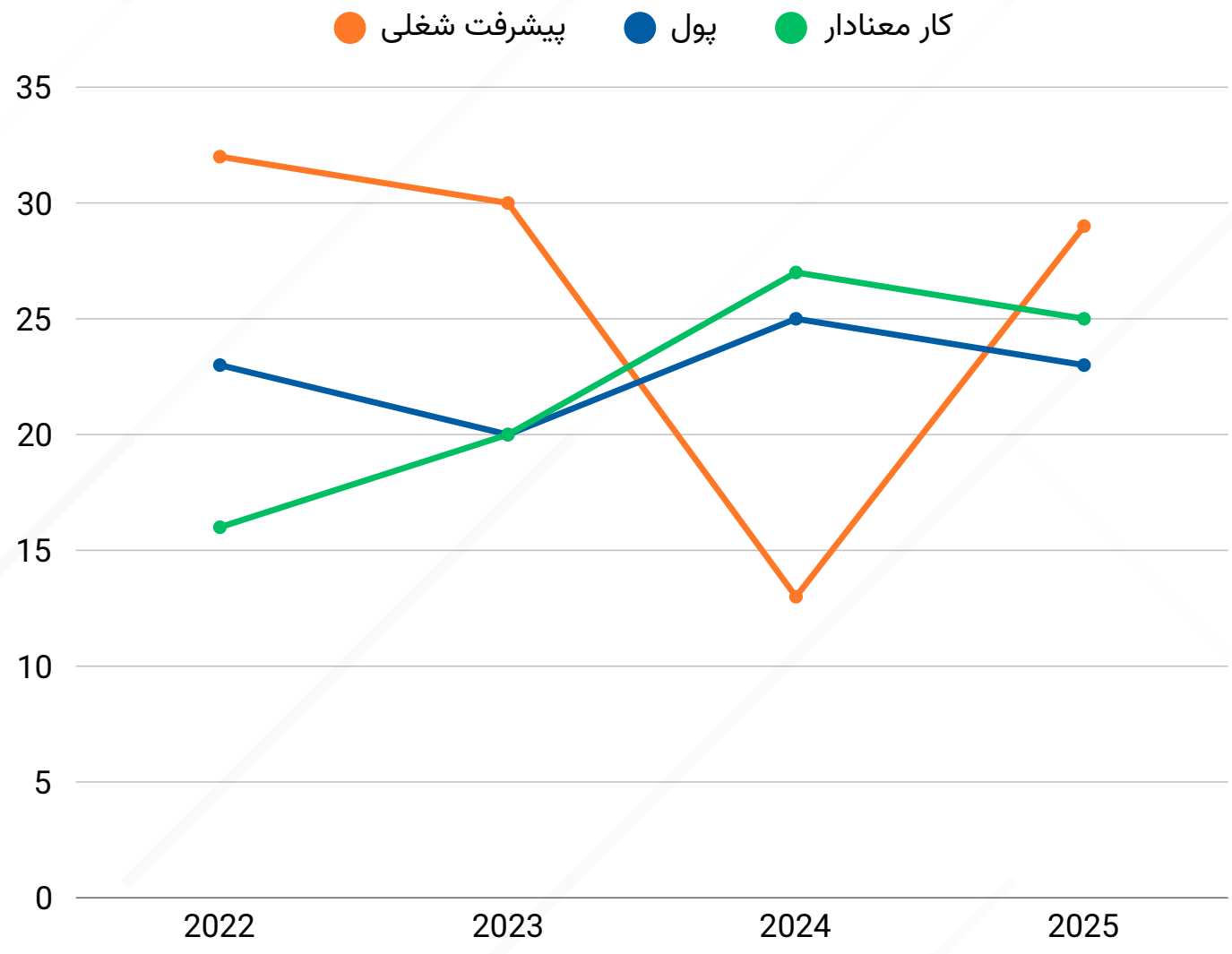
در محیط کاری شما، چگونه به سرمایه انسانی رسیدگی می‌شود؟
بهترین گزینه را انتخاب کنید.



شکل ۷. تعداد پاسخ‌ها درباره تلاش‌های مربوط به نگهداشت نیروی انسانی

مقایسه‌های سال‌به‌سال نشان می‌دهد که حقوق و مزایا و کار جذاب به‌طور فزاینده‌ای به عنوان راهبردهای مؤثر برای نگهداشت نیروی انسانی شناخته می‌شوند. اگرچه فرصت‌های پیشرفت شغلی در سال ۲۰۲۴ از اهمیت کمتری برخوردار بودند، اما به نظر می‌رسد در سال ۲۰۲۵ به‌طور چشمگیری دوباره مورد توجه قرار گرفته‌اند (شکل ۸).

موثرترین روشی که تاکنون برای حفظ کارکنان SOC یافته‌اید چیست؟

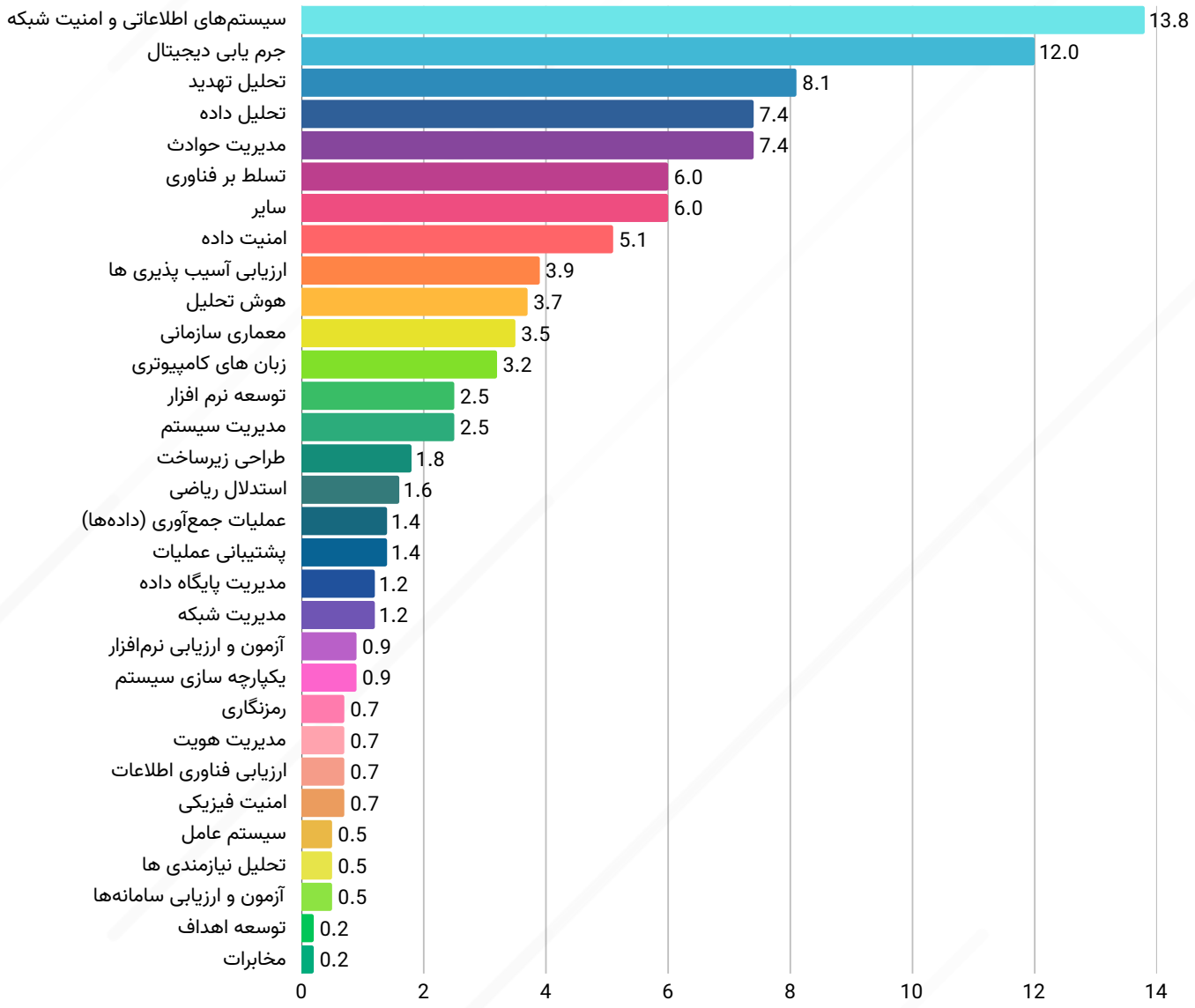


شکل ۸. روش‌های مؤثر برای نگهداشت کارکنان

آنچه رهبران SOC در یک کارمند به‌دنبال آن هستند، چیست؟

وقتی از پاسخ‌دهندگان پرسیده شد که بزرگ‌ترین کمبود مهارت فنی هنگام استخدام نیروهای فنی چیست (یعنی کدام مهارت بیشتر از سایرین کمبود دارد)، آن‌ها امنیت سیستم‌های اطلاعاتی و شبکه (۱۴٪) و جرم یابی دیجیتال (Digital Forensics) با ۱۲٪ را به‌عنوان مهم‌ترین موارد معرفی کردند. پس از آن، مجموعه گسترده‌ای از سایر مهارت‌ها قرار دارند که در شکل ۹ مشخص شده‌اند.
برای مهارت‌های غیر فنی، مدیریت ریسک با ۱۴٪ در صدر قرار گرفت.

مهم‌ترین کمبود مهارت فنی هنگام استخدام نیرو برای نقش‌های فنی چیست؟



شکل ۹. کمبود مهارت‌ها

آقای Joshua Wright (نویسنده دوره SEC504)

نتایج نظرسنجی نشان می‌دهد که ۶۲٪ از متخصصان SOC معتقدند سازمان‌شان اقدامات کافی برای حفظ نیروهای برتر انجام نمی‌دهد. یک SOC عالی با ابزار ساخته نمی‌شود، بلکه با فرهنگی شکل می‌گیرد که تحلیلگرانی را که کار خارق‌العاده انجام می‌دهند، به رسمیت می‌شناسد و پاداش می‌دهد.

وقتی تحلیلگران احساس کنند با مأموریت سازمان ارتباط دارند و درک کنند که نقش آن‌ها بخش مهمی از این مأموریت است، انرژی، خلاقیت و ابتکار لازم برای موفقیت را به همراه می‌آورند.

مدیران باید تحلیلگران با استعدادی را که الگوی موفقیت در سطوح مختلف توانایی فنی هستند، شناسایی کرده و به آن‌ها قدرت دهند تا به رهبرانی تبدیل شوند که دیگران بتوانند از آن‌ها پیروی کنند.

چه چیزی در فناوری SOC داغ است و چه چیزی نیست؟

اگر رهبری شرکت آمادگی اختصاص کامل منابع لازم برای اثربخش‌کردن یک ابزار را نداشته باشد، بهتر است اصلاً آن ابزار را به‌کار نگیرد.

یک فناوری جدید و جذاب که به نظر می‌رسد راه‌حل فوق‌العاده‌ای باشد، نیازمند بودجه، آموزش، زمان و یکپارچه‌سازی با جریان کاری است.

راهکارهای شناسایی و پاسخ به تهدید در نقطه پایانی یا گسترده (EDR/XDR) بار دیگر در صدر فهرست رضایت‌مندی قرار گرفته‌اند و تنها فناوری‌ای هستند که در سال جاری امتیازی بالاتر از ۳ از ۴ کسب کرده‌اند (در مقایسه بین فناوری‌های مورد استفاده و سطح رضایت). این ابزار، بیشترین میزان استقرار و بیشترین سطح اعتماد را در میان ابزارهای SOC دارد.

رضایت بالا از EDR/XDR به دلیل استقرار کامل، اثربخشی در آغاز فرآیندهای پاسخ به حادثه و پشتیبانی از طریق آموزش و منابع مناسب به‌دست آمده است.

در مقابل، ابزارهای مبتنی بر هوش مصنوعی و یادگیری ماشین (AI/ML) همچنان عملکرد ضعیفی دارند. از میان سه فناوری AI/ML ارزیابی‌شده، دو مورد در پایین‌ترین رده‌ها قرار گرفتند؛ از جمله ابزارهای تولید زبان طبیعی (Generative Language Tools) که تنها امتیاز ۲ از ۴ را کسب کردند.

عملکرد ضعیف این ابزارها ناشی از جدید بودن آن‌هاست؛ اغلب بدون مالکیت مشخص، مجوز رسمی، بودجه کافی برای پیاده‌سازی، یا برنامه‌ای برای ادغام در عملیات روزمره معرفی می‌شوند.

به‌طور کلی، ابزارهای تثبیت‌شده همچنان بالاترین امتیازات را به خود اختصاص می‌دهند. EDR همچنان برترین فناوری ارزیابی‌شده باقی مانده است، چرا که از نظر قابلیت اطمینان و بلوغ فناوری، مورد اعتماد است. این ابزارها، در SOC بسیار پرکار هستند: به‌خوبی شناخته‌شده، گسترده مستقرشده و آزمون پس‌داده در طول زمان.

در مقابل، فناوری‌های جدیدتر مانند AI/ML و فریب (Deception) همچنان در برآورده کردن انتظارات دچار چالش هستند. رضایت‌مندی از آن‌ها پایین باقی مانده است، که نشان می‌دهد با وجود علاقه بالا، عملکرد واقعی و یکپارچگی این ابزارها با محیط‌های عملیاتی هنوز به سطح مطلوب نرسیده است.

البته احتمال زیادی وجود دارد که این وضعیت در آینده تغییر کند و فروشندگان فناوری‌های AI/ML نباید ناامید شوند. در سال ۲۰۱۷، «کشف دارایی و موجودی‌گیری» پایین‌ترین رتبه را داشت، اما اکنون در میانه جدول قرار گرفته است.

پیشرفت برای هوش مصنوعی محتمل است.

نتیجه‌گیری: روندهای امیدوارکننده، اما هنوز کارهایی باقی مانده است

نظرسنجی SOC سال ۲۰۲۵ تأیید می‌کند که SOC به‌طور امیدوارکننده‌ای در مسیر روندهای تثبیت‌شده در حال پیشرفت است، اما در برخی حوزه‌ها این روند بسیار کند است. قابلیت‌های اصلی قوی باقی مانده‌اند، اما تعادل همچنان به سمت کارهای واکنشی متمایل است. فناوری‌های هوش مصنوعی و یادگیری ماشین (AI/ML) همچنان عملکرد قابل‌توجهی ندارند. شکار تهدیدها به دلیل کمبود نیروی انسانی محدود شده است و رضایت از ابزارها، همان‌طور که همیشه بوده، به استقرار کامل و ادغام دقیق آن‌ها بستگی دارد.

نظرسنجی SOC سال ۲۰۲۵ تصویری آشنا را نشان می‌دهد: توانمندی قابل‌قبول، برخی روندهای امیدوارکننده، اما حرکت محدود رو به جلو و نارضایتی مستمر کارکنان.

واضح است که پیشرفت نیازمند هدفمندی است در جذب نیرو، آموزش، معماری و استفاده از ابزارها.

جمع‌آوری داده‌ها کار آسانی است، اما استفاده هوشمندانه از آن‌ها بخش دشوار ماجراست.

تیم‌های SOC می‌دانند به چه چیزی نیاز دارند ابزارهای کارآمد، کارکنانی که باقی بمانند و زمان کافی برای انجام کارهای فراتر از واکنش به هشدارها. اما بودجه، نرخ ترک خدمت و تغییر اولویت‌ها همچنان مانع اصلی هستند. شاخص‌ها ردیابی می‌شوند، اما هنوز به صورت دستی. پذیرش خدمات ابری نوسان دارد. ابزارهای AI/ML بیش از حد تبلیغ شده‌اند و کمتر از حد انتظار عمل می‌کنند.

در همین حال، تعداد رو به افزایشی از سازمان‌ها به راهبرد «همه چیز را در SIEM ذخیره کن» روی آورده‌اند؛ رویکردی که امروز توجیه‌پذیر است اما پرداخت هزینه آن در آینده دشوار خواهد بود. این یک استراتژی دیده‌بانی است که خطر فروپاشی تحت بار سنگین خود را دارد.

ابزارها به تنهایی این مشکلات را حل نمی‌کنند، بلکه انسان‌ها این کار را انجام می‌دهند. در حالی که پیشرفت‌هایی در حال وقوع است، این پیشرفت‌ها نابرابر بوده و اغلب سال‌هاست که توسط همان مسائل ساختاری محدود شده‌اند.

خلاصه اینکه SOCها درجا نزده‌اند، اما خیلی هم سریع حرکت نمی‌کنند.

دستاوردهای واقعی از طریق وضوح هدف، هماهنگی و تصمیم به توقف نامیدن فرآیندهای واکنشی گذشته به عنوان «شکار تهدید» حاصل خواهد شد.

پنج دلیل برای خوش‌بینی نسبت به آینده مرکز عملیات امنیت (SOC)

پوشش گسترده ۲۴ ساعته و ۷ روز هفته	۷۹٪ از مراکز عملیات امنیت (SOC) اکنون به‌صورت شبانه‌روزی فعالیت می‌کنند، که نشان‌دهنده بلوغ SOC و تعهد به پایش مداوم است. این امر همچنین از سوی ذی‌نفعان کسب‌وکار که به جدیت تهدیدات سایبری جهانی واقف‌اند، مورد حمایت قرار می‌گیرد.
افزایش استفاده از فضای ابری	اگرچه ساختار متمرکز (Centralized SOC) همچنان رایج‌ترین معماری است، اما گزارش شده که برنامه‌هایی برای مهاجرت سیستم‌های SOC به منابع ابری در حال اجراست.
افزایش گزارش‌های مربوط به شناسایی پیشگیرانه	هرچند هنوز در اقلیت هستند، اما تعداد بیشتری از تیم‌ها گزارش می‌دهند که از جستجوهای SIEM و شکار تهدیدها استفاده می‌کنند، نه فقط از هشدارهای خودکار.
شفافیت بیشتر در استفاده از AI/ML	سازمان‌ها به‌تدریج و بسیار آهسته شروع به یکپارچه‌سازی هدفمند ابزارهای هوش مصنوعی و یادگیری ماشین در جریان‌های کاری کرده‌اند، که نشان می‌دهد با داشتن برنامه مشخص، این کار امکان‌پذیر است.
پیشرفت شغلی در صدر عوامل نگهداشت نیرو	کارکنان مایل به ماندن در سازمان هستند، اما فقط زمانی که آینده‌ای برای خود ببینند. و این یک فراخوان جدی برای اقدام از سوی رهبران سازمان است.

تحلیل مدیریتی دیاکو با تجربه از سال 1389 در طراحی، پیاده‌سازی، راهبری، ممیزی و بلوغ مراکز عملیات امنیت سایبری و پاسخ‌دهی به حملات سایبری

برای بهبود بلوغ (Maturity) و ارتقاء عملکرد SOC، ابزارها و فعالیت‌های عملی زیادی پیشنهاد می‌شود. بر اساس نتایج SANS SOC Survey 2025 و سایر مباحث مرتبط، مراحل پیشنهادی، خلأها، چالش‌ها، تحقیقات و تجارب از سال ۱۳۸۹ در بزرگترین پروژه های مراکز عملیات امنیت و پاسخگو به حملات سایبری و نقشه مسیر (roadmap) را این‌گونه جمع‌بندی کرده‌ایم:

مراحل طراحی و ارتقاء بلوغ SOC

1.ارزیابی وضعیت فعلی

- بررسی فرآیندها، ابزارها، تیم، معماری و مدل‌های عملیاتی.
- شناسایی نسخ ابزار، پراکندگی داده، نحوه گزارش‌گیری و معیارهای عملکرد.
- استفاده از مدل‌هایی مانند SOC-CMM برای ارزیابی سطح بلوغ.

2.تعریف اهداف و نقشه راه (Roadmap)

- تدوین چشم‌انداز: دستیابی به SOC هوشمند، خودکار و پژوهش‌محور.
- تعیین شاخص‌های کلیدی: سرعت تشخیص، پوشش تهدیدات، دقت تشخیص، نرخ هشدارهای کاذب، مهارت تیم، اتوماسیون فرآیندها.
- تثبیت ارتباط با اهداف کسب‌وکار (کاهش ریسک، انطباق، کارایی) و جلب حمایت مدیریت ارشد.

3.بهبود قابلیت‌ها

- **فناوری و اتوماسیون:**
  - کاهش «alert fatigue» با بهره‌گیری از AI/ML برای تراياج خودکار و اولویت‌بندی هشدارها.
  - اتوماسیون متداول مانند SOAR، گردش کار، گزارش‌گیری و به‌روزرسانی قوانین.
- **نیروی انسانی و مهارت:**
  - مهارت‌های کلیدی مورد نیاز: تهدیدشناسی، threat modeling، مهندسی داده، detection-as-code و SDLC امنیتی.
  - برنامه آموزش، منتورینگ و توسعه مسیر شغلی، برای ماندگاری استعداد تیم.

- **فرهنگ و ارتباطات:**
  - بهبود مشارکت بین تیم‌ها (Data Engineering، Hunting، CTI و IR).
  - معرفی CTI داخلی یا ترکیبی و تعریف واضح خواسته‌های اطلاعاتی (INT-requirements).

4.اندازه‌گیری و بازبینی تفاوت‌ها

- پیاده‌سازی KPIs قابل اندازه‌گیری: نرخ false positives (حدود ۷۰٪)، پوشش تهدید، سرعت تشخیص و ...
- اندازه‌گیری تاثیر CTI (CTI effectiveness) و پروژه‌های hunting طبق CTI-CMM یا CU-GIRH.
- گزارش‌گیری هوشمند، خودکار و به‌روز به مدیریت برای اصلاح جهت‌گیری‌ها.

خلأها و چالش‌های کلیدی

- کمبود نیروی انسانی متخصص و نرخ چرخش بالا: ۶۲٪ تیم‌ها کافی به حفظ استعدادها توجه نمی‌کنند.
- فقدان داده‌ی باکیفیت و دسترسی ناقص به منابع: ۵۲٪ telemetry مهندسان DE به‌دلیل مشکلات داده نمی‌توانند عملکرد بهینه داشته باشند.
- اطلاعات محدود درباره بودجه و گزارش‌گیری دستی: ۴۲٪ تیم‌ها از بودجه بی‌خبرند؛ ۶۹٪ هنوز گزارش‌گیری را دستی مدیریت می‌کنند.
- مشکل اثبات ارزش و تاثیر CTI و DE برای مدیران ارشد: نیمی از تیم‌ها هنوز اثربخشی را گزارش نمی‌کنند یا نمی‌دانند.

راه‌کارهای پیشنهادی

ارتقاء مدل بلوغ SOC:

- استفاده از SOC-CMM برای خطوط پایه، سنجش بهبود و رشد مستمر.

توسعه نیروی انسانی:

- مهارت‌هایی مانند تهدیدمدل‌سازی و مهندسی داده را اولویت آموزش دهید.
- ادغام CTI، DE و SOC برای ایجاد تیم‌های تلفیقی با دامنه سنگین مهارتی.

برنامه اتوماسیون و AI:

- مکانیزم‌های ترایاج هوشمند، تولید قوانین، اعتبارسنجی detectionها، گزارش‌سازی، و Runbook خودکار.
- شروع تدریجی با AI و استفاده مؤثر بدون وابستگی به وعده‌های بیش از حد تبلیغاتی.

ابزارها و معیارها:

- KPIهای مدون برای مدیریت بهتر چرخه تشخیص، عملکرد CTI، پوشش تهدید و کاهش false positives.
- ساخت داشبورد خودکار برای شفافیت و تصمیم‌گیری سریع.

نقشه راه پیشنهادی 12 ماهه

فاز اقدامات اصلی

1. ارزیابی (ماه ۱–۲) تحلیل SOC فعلی، مشخص کردن gaps، مدل بلوغ اولیه.
2. طراحی هدف (ما ۲–۴) تعریف ارزش‌پیشنهادی، KPIs، نقشه راه اولویت‌ها.
3. اجرا (ما ۴–۸) بهبود داده‌ها و دسترسی، اتوماسیون اولیه، ارتقاء SOPها.
4. تقویت مهارت‌ها و فرهنگ (ما ۶–۱۰) آموزش و توسعه تیم، اجرای Purple-teaming، بهبود هماهنگی CTI/DE.
5. اندازه‌گیری و بازخورد (ما ۸–۱۲) گزارش پیشرفت، بهینه‌سازی roadmap، تثبیت فرهنگ بهبود مستمر.

جمع‌بندی

- فناوری کافی نیست: بلوغ واقعی SOC در تعامل ابزار، فرآیند، داده و نیروی انسانی شکل می‌گیرد.
- تمرکز بر اتوماسیون هوشمند و مهارت‌های حیاتی تضمین می‌کند SOC نه فقط واکنشی، بلکه پیش‌بینی‌کننده و اثربخش باشد.
- معیارهای درست و بازخورد هدفمند حلقه یادگیری دائمی را فعال کرده و ارزش را برای ذی‌نفعان اثبات می‌کنند.

در نهایت، نقشه راه مشخص، ساده، شفاف، ماژولار، مدیریت پذیر مبتنی بر مدیریت ریسک فنی، سیستمی و فرآیندی در تعامل مهندسی شده جهت رصد هرچه تمامتر مخاطرات و تهدیدات همراه با پیشبینی وخودکار سازی و نظارت ۳۶۰ همراه با مانور های سفارشی سازی شده با تکیه بر دانش(استاندارد و ابزار و کنترل های امنیتی تکمیل کننده هستند نه پایه وحیاتی).