آذر ۱۴۰۱

نقش در حال تکامل NDR

استفاده از هوش مصنوعی برای پشتیبانی از راهبردهای XDR

ترجمه شده توسط شرکت مهندسی امن ارتباط سینداد

اهداف تحقیق

پتانسیل در اختلالات جدی کسب‌وکار باعث شده که تشخیص سریع و دقیق تهدیدات، امری حیاتی شده که مانع از اتلاف داده، نقض سازگاری و اتلاف درآمد می‌شود. حتی هنگامی‌که منابع و کاربران محدوده پیشین خود را ترک کنند، شبکه باید نقش کلیدی در تشخیص تهدیدات بازی کند تا مانع از بروز اختلالات در کسب‌وکار شود. به‌طور مشخص، ابزارهای مبتنی بر شبکه، دید منسجم و جامعی در محیط‌های ناهمگون فراهم کرده و خارج از محدوده‌ای است که حمله‌کننده بتواند آن را تغییر دهد. با این‌حال، تعداد ابزارهای موجود برای تشخیص حمله و پاسخ به آن، باعث شده کاربران در خصوص اولویت‌بندی دچار عدم قطعیت شوند.

به‌منظور کسب بینش در خصوص این روندها، ESG موارد زیر را در ۳۷۶ شرکت بررسی کرده است. این مطالعه تلاش می‌کند به موارد زیردست یابد:

بینشی در خصوص چالش‌هایی کسب کند که تیم‌های امنیتی در خصوص کشف و پاسخ به تهدیدهای فعلی با آن مواجه هستند.

بررسی کند که امروزه چگونه از ابزارهای NDR استفاده می‌شود و اینکه آیا برای طرح‌ها و راهبردهای XDR گسترده‌تر مناسب هستند یا خیر.

قابلیت‌های کلیدی که سازمان از ابزارهای NDR نیاز دارد و موارد کاربردی که سعی در رسیدگی به آن دارند را ارزیابی می‌کنند.

درک اینکه چرا تیم‌های امنیتی NDR را در اولویت قرار داده و فهم مزایای این ابزار

یافته های کلیدی

سازمان‌ها با چالش‌های بسیاری در خصوص تشخیص تهدید و پاسخ به آن مواجه هستند.

تهدیدهای رمزنگاری‌شده، مسئله مهمی بوده و می‌تواند منجر به بروز مشکلاتی در زنجیره حمله شود.

تیم‌های امنیتی بنا به دلایل گوناگونی،NDR را در اولویت قرار می‌دهند.

بسیاری از سازمان‌ها از NDR به عنوان خط اول دفاع استفاده می‌کنند؛ زیرا استفاده از آن آسان بوده و محدوده وسیعی را پوشش می‌دهند.

موارد کاربرد گوناگون نیازمند طیفی از قابلیت‌ها است.

محدوده وسیعی از پوشش و قابلیت‌های تحقیقی، مهم‌ترین بخش است.

هوش مصنوعی قوی، بخش جدایی‌ناپذیر NDR شده است.

کاربران انتظار دارند که AI تشخیص تهدید و کارآمدی عملیاتی را بهبود بخشد.

NDR به عنوان یک مؤلفه کلیدی برای راهبردهای XDR نمایان شد.

افراد بسیاری، NDR را به‌عنوان اساس و بنیاد XDR می‌دانند و تمرکز ابری، حیاتی است.

تیم‌های امنیتی از مزایای امنیتی و کسب‌وکاری NDR بهره می‌برند.

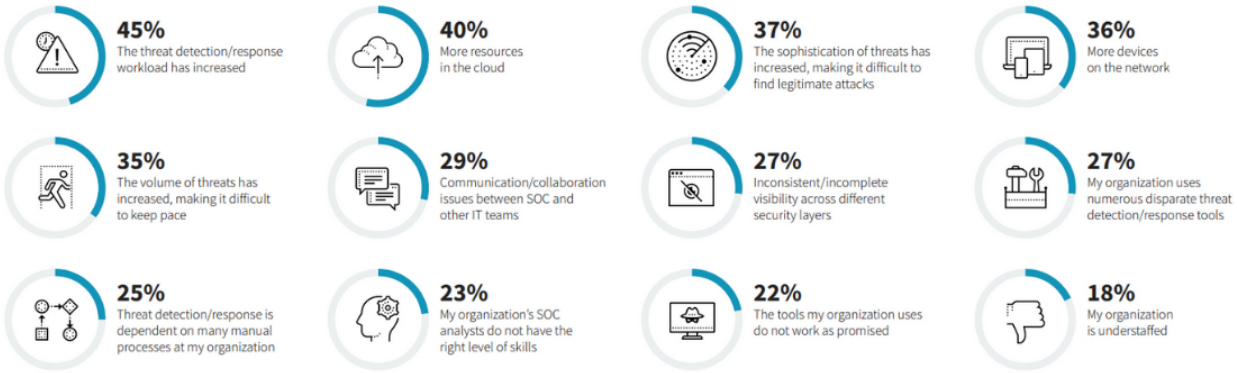
افراد بسیاری به مزایای زیر اشاره کرده‌اند: نواقص کمتر، هزینه کمتر و انتقال ابری سریع‌تر

سازمان‌ها با چالش‌های بسیاری در خصوص تشخیص تهدید و پاسخ به آن مواجه هستند.

پیچیدگی، تهدیدها و بارکاری SOC، مسائل کلیدی هستند.

برای بسیاری از تیم‌های امنیتی، تشخیص تهدید و پاسخ به آن (TDR) بنا به دلایل گوناگونی، دشوارتر شده است. تقریباً نیمی از سازمان‌ها (۴۵ درصد) به افزایش بارکاری تشخیص تهدید و پاسخ به آن اشاره‌کرده‌اند. علت این امر در بسیاری موارد، نتیجه این است که باید از محیط‌های توزیع‌شده‌تر و پویاتری در برابر دشمنان همیشگی، محافظت کنند.پیچیدگی محیطی نقش مهمی دارد؛ به‌گونه‌ای که ۴۰ درصد سازمان‌ها افزایش منابع مبتنی برابر و ۳۶ درصد آن‌ها افزایش تعداد دستگاه‌های موجود در شبکه را به‌عنوان چالش‌های اصلی اعلام کردند.دورنمای تهدید نیز جز مسائل مهمی است که به ذهن می‌آید؛ به‌گونه‌ای که ۳۷ درصد سازمان‌ها به تهدیدات پیچیده و دقیق و ۳۵ درصد آنها به حجم حملات به‌عنوان چالش‌های موجود اشاره‌کرده‌اند.

چالش‌های تشخیص تهدید و پاسخ به آن



۴۵ درصد: بارکاری تشخیص / پاسخ به تهدید افزایش‌یافته است.

۴۰ درصد: منابع بیشتر در ابر

۳۷ درصد: پیچیدگی و جزئیات تهدیدها بیشتر شده و درنتیجه یافتن تهدیدهای مشروع را دشوار می‌کند.

۳۶ درصد: تعداد دستگاه‌های موجود در شبکه افزایش‌یافته است.

۳۵ درصد: حجم تهدیدها بیشتر شده است، درنتیجه همگام شدن و هم سرعت شدن با تهدیدات دشوارتر شده است.

۲۹ درصد: مسائل ارتباطی / همکاری میان SOC و دیگر تیم‌های IT

۲۷ درصد: دید غیرمنسجم / ناکامل نسبت به لایه‌های امنیتی گوناگون

۲۷ درصد: سازمان من از ابزارهای تشخیص / پاسخ به تهدید متفاوتی استفاده می‌کند.

۲۵ درصد: تشخیص / پاسخ به تهدید وابسته به فرآیندهای دستی بسیاری در سازمان است.

۲۳ درصد: تحلیلگران SOC سازمان، سطح مهارتی مناسبی ندارند.

۲۲ درصد: ابزارهایی که در سازمان استفاده می‌شود، کارکرد مطلوبی ندارند.

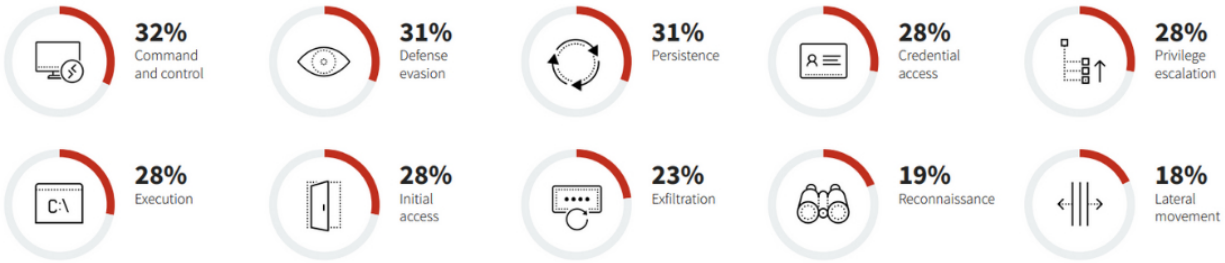
۱۸ درصد: تعداد کارکنان سازمان کم است.

مسائل در کل زنجیره حمله، پراکنده هستند.

بسیاری از تیم‌های امنیتی در تشخیص و متوقف کردن تهدیدهایی که سازمان آن‌ها را هدف قرار داده، مشکل‌دارند.

درنتیجه وجود چنین چالش‌هایی، بسیاری از تیم‌های امنیتی در تشخیص و متوقف کردن تهدیدهایی که سازمان آن‌ها را هدف قرار داده، دشواری دارند. علاوه براین، مسائل در اغلب قسمت‌های چهارچوب MITER ATT&CK وجود دارد. تقریباً یک‌سوم سازمان‌های موردبررسی اشاره کردند که در شناسایی و مسدود کردن ارتباطات فرمانی و کنترلی مشکل‌دارند. همچنین بسیاری از سازمان‌ها به مسائلی در طول گام‌های گریز و تداوم اشاره کردند. ۲۸ درصد از سازمان‌ها به مشکلات زیر اشاره کردند: تشخیص دسترسی به اعتبار، افزایش امتیاز، اجرا و دسترسی اولیه. عملیات اکتشافی و تحرک جانبی، مشکلات کم‌اهمیت‌تری بوده و به ترتیب ۱۹ و ۱۸ درصد از سازمان‌ها به آن اشاره کردند.

حوزه‌هایی که دارای بیشترین دشواری در چهارچوب MITER ATT&CK هستند



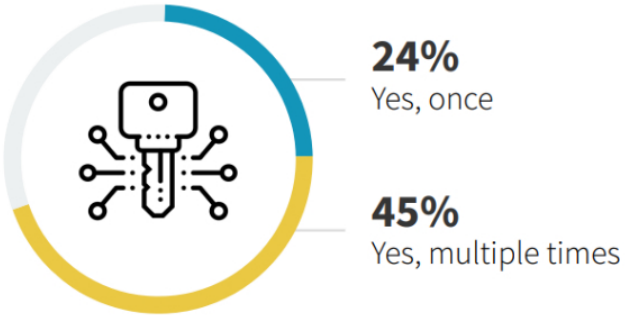
۳۲ درصد: فرمان و کنترل
۳۱ درصد: گریز دفاعی
۳۱ درصد: تداوم persistant
۲۸ درصد: افزایش امتیاز privildge escalation
۲۸ درصد: اجرا
۲۸ درصد: دسترسی اولیه
۲۳ درصد: سرقت اطلاعات رایانه‌ای
۱۹ درصد: عملیات اکتشافی
۱۸ درصد: تحرک جانبی

حمله‌کنندگان مکرراً و در طول مراحل گوناگون از رمزنگاری استفاده می‌کنند.

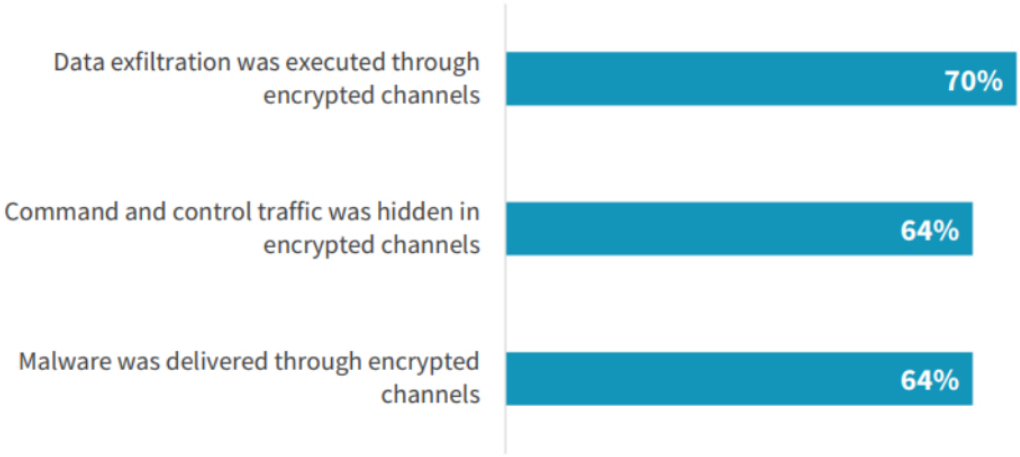
استفاده از رمزنگاری برای گمراه کردن حملات، یکی از دلایلی است که منجر به دشوار شدن تشخیص حمله در طول زمان شده است. درواقع، ۲۴ درصد سازمان‌ها درگیر حمله‌ای می‌شوند که فقط یک‌بار از رمزنگاری استفاده کرده است، درحالی‌که تقریباً نیمی از آن‌ها (۴۵ درصد) چندین حمله را تجربه کرده‌اند که از این رویکرد استفاده می‌کند. علاوه براین، از رمزنگاری چندین بار در مراحل گوناگون حمله استفاده می‌شود. بیش از ۳/۲ سازمان‌ها (۷۰ درصد) درگیر حمله‌ای با رویکرد رمزنگاری‌شده‌اند که داده‌ها از طریق کانال‌های رمزنگاری‌شده، سرقت شده است. ۶۴ درصد از سازمان‌ها اعلام کردند که ارتباطات فرمان و کنترل رمزنگاری‌شده و / یا بدافزار در طول تحویل، کدگذاری شده است.علت اصلی این موضوع، احتمالاً نبود دید و بینایی است؛ به‌گونه‌ای که ۳۴ درصد سازمان‌ها گزارش کردندکه نسبت به ترافیک رمزنگاری شده در محیط خود، دید دارند.

فقط ۳۴ درصد سازمان‌ها نسبت به‌کل ترافیک رمزنگاری شده خود، دید دارند.

آیا سازمان شما تاکنون قربانی حمله‌ای شده که از ترافیک رمزنگاری‌شده برای جلوگیری از تشخیص حمله استفاده کند؟



حمله‌کنندگان چگونه از رمزنگاری استفاده می‌کنند؟



داده‌ها از طریق کانال‌های رمزنگاری‌شده، سرقت می‌شوند.
ترافیک فرمان و کنترل در کانال‌های رمزنگاری‌شده، پنهان می‌شود.
بدافزار از طریق کانال‌های رمزنگاری‌شده، تحویل داده می‌شود.

تیم‌های امنیتی بنا به دلایل گوناگونی NDR را در اولویت قرار می‌دهند.

از NDR اغلب به‌عنوان اولین خط دفاع استفاده می‌شود.

در هنگام انتخاب ابزارهای تشخیص حمله و پاسخ به آن، تیم‌های امنیتی گزینه‌های مختلفی پیشرو دارند. امنیت اطلاعات و مدیریت رخداد (SIEM) و تشخیص و پاسخ نقطه انتهایی (EDR) عناصر اصلی در SOC هستند. و در طول ۱۸ ماه گذشته، علاقه به تشخیص و پاسخ تعمیم‌یافته (XDR) شدیداً افزایش‌یافته است. باوجود تمامی گزینه‌ها، ۴۶ درصد سازمان‌ها اعلام کردند که مؤثرترین ابزار برای تشخیص تهدید و پاسخ به آن، NDR است. درنتیجه، بسیاری از آن‌ها، NDR را در اولویت قرار می‌دهند. به‌طور مشخص، ۴۲ درصد سازمان‌ها اعلام کردند که تمایل دارند از NDR به‌عنوان اولین خط دفاع برای تشخیص حمله استفاده کنند. ۳۳ درصد آن‌ها از NDR در کنار ابزارهای دیگر نظیر SIEM، EDR و XDR به‌عنوان اولین خط دفاع استفاده می‌کنند.

۴۶ درصد سازمان‌ها، فناوری تشخیص و پاسخ شبکه را به‌عنوان مؤثرترین ابزار تشخیص حمله و پاسخ به آن اعلام کردند.

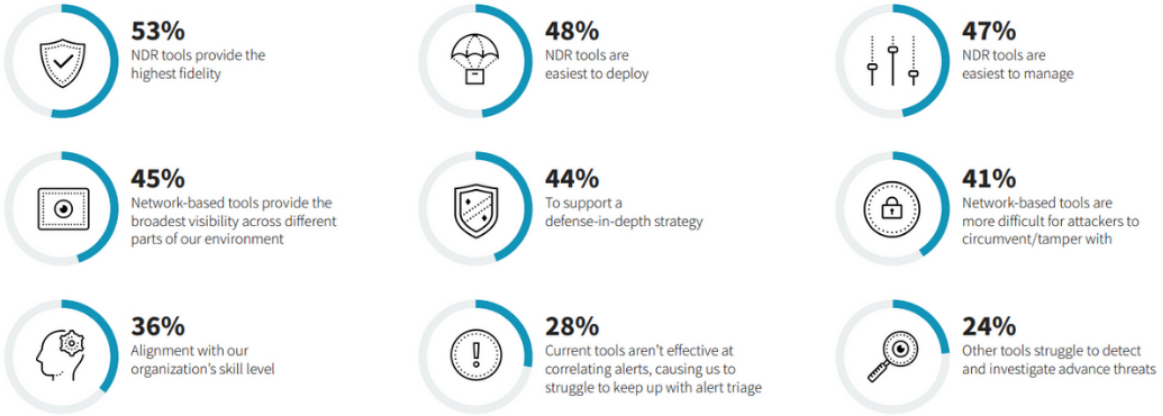
سازمان‌ها چگونه از NDR برای تشخیص تهدید و پاسخ به آن استفاده می‌کنند؟

۴۲ درصد: سازمان تمایل (یا انتظار) دارد از ابزارهای NDR به‌عنوان اولین خط دفاع برای تشخیص حمله استفاده کند.
۱۳ درصد: سازمان تمایل (یا انتظار) دارد از EDR به‌عنوان اولین خط دفاع برای تشخیص حمله استفاده کند.
۷ درصد: سازمان تمایل (یا انتظار) دارد از XDR به‌عنوان اولین خط دفاع برای تشخیص حمله استفاده کند.
۵ درصد: سازمان تمایل (یا انتظار) دارد از SIEM به‌عنوان اولین خط دفاع برای تشخیص حمله استفاده کند.
۳۳ درصد: سازمان از ابزارهای NDR و دیگر ابزارها (نظیر EDR، SIEM و XDR) باهم به‌عنوان خط اول دفاع برای تشخیص حمله استفاده می‌کند.

از NDR به دلیل صحت بالا، آسانی استفاده و گستردگی پوشش استفاده می‌شود.

دلایلی که ممکن است یک سازمان بر اساس آن، ابزارهای NDR را برای استفاده انتخاب کند، بسیار متنوع است. مثبت کاذب و منفی کاذب، اثر قابل‌توجهی روی تیم‌های امنیتی داشته و اثربخشی بالا را به امری ضروری تبدیل کرده است. درنتیجه، بیش از نیمی از سازمان‌ها (۵۳ درصد) از NDR استفاده می‌کنند، زیرا احساس می‌کنند این ابزار، دارای بالاترین میزان صداقت و صحت است. همچنین به‌سادگی استقرار (۴۸ درصد) و سادگی مدیریت (۴۷ درصد) نیز اشاره‌شده و می‌تواند به سازمان‌هایی که دچار مشکل شکاف مهارت‌های امنیت سایبری هستند، کمک کند تا به کارآمدی بهتری دست یابند. درنهایت، ۴۵ درصد سازمان‌ها اعلام کردند که دیدی که NDR ارائه می‌کند، بخش‌های گوناگونی از محیط را پوشش داده و یکی از دلایل استفاده آن‌ها از NDR است. باوجود حمله‌کنندگانی که از دید مجزا شده (جزیره‌ای) استفاده می‌کنند، بسیاری از سازمان‌هایی که دارای منابع ابری و منابع محلی هستند، دستیابی به دید سازگارتر، یک اولویت است.

دلایل اصلی استفاده از NDR



۵۳ درصد: ابزارهای NDR صداقت و صحت بالاتری تأمین می‌کنند.

۴۸ درصد: ابزارهای NDR ساده‌ترین پیاده‌سازی و استقرار را دارند.

۴۵ درصد: ابزارهای مبتنی بر شبکه، دید گسترده‌ای در سراسر بخش‌های گوناگون محیط ما فراهم می‌کنند.

۴۴ درصد: از یک راهبرد دفاع در عمق پشتیبانی می‌کنند.

۳۶ درصد: متناسب با سطح مهارتی سازمان ما، تنظیم می‌شوند.

۲۸ درصد: ابزارهای فعلی در هماهنگی هشدارها کارآمد نیستند؛ درنتیجه باعث می‌شوند ما با اولویت‌بندی هشدارها درگیر باشیم.

موارد کاربرد گوناگون، نیازمند طیفی از قابلیت‌ها هستند.

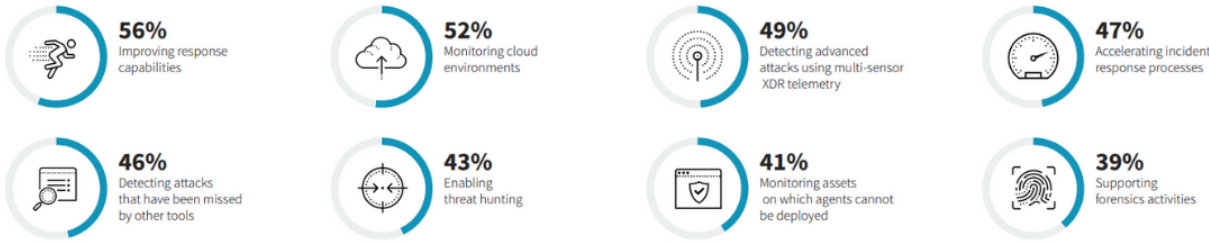
NDR از مجموعه گوناگونی از موارد کاربرد، پشتیبانی می‌کند.

تیم‌های امنیتی برای پشتیبانی از موارد کاربرد گوناگون، از NDR استفاده می‌کنند. در بالای فهرست، ۵۶ درصد سازمان‌های شرکت‌کننده در بررسی، تلاش می‌کنند تا قابلیت‌های پاسخ سازمان خود را بهبود بخشند. در ادامه، ۴۷ درصد سازمان‌ها از NDR استفاده می‌کنند تا فرآیندهای پاسخ به حادثه خود را تسریع کنند. تکامل تحلیل سنتی ترافیک شبکه (NTA) به سمت NDR بر حوزه‌های زیر متمرکز است: ساده‌سازی جریان‌های کار و یکپارچه‌سازی به‌منظور حصول اطمینان از اینکه، وقتی یک حمله شناسایی می‌شود، بتواند به‌صورت مؤثر و سریعی به آن رسیدگی کند. بیش از نیمی از سازمان‌ها (۵۲ درصد) از NDR برای نظارت بر محیط‌های ابری استفاده می‌کنند. همچنین نقطه پیشین را از منظر نیاز به سازگاری میان محیط‌های داخلی و خارجی، اعتبارسنجی می‌کنند. در همین راستا، ۴۱ درصد سازمان‌ها برای نظارت بر دارایی‌هایی که آژانس‌ها نمی‌توانند روی آن‌ها مستقر شوند، از NDR استفاده می‌کنند.

این موضوع به محیط‌های ابری و دستگاه‌های IoT اشاره می‌کند؛ هر دو گزینه می‌توانند از مزایای مدل‌های توسعه بدون آژانس بهره ببرند.

در بالای فهرست، ۵۶ درصد سازمان‌های شرکت‌کننده در بررسی، تلاش می‌کنند تا قابلیت‌های پاسخ سازمان خود را بهبود بخشند.

موارد کاربردی که NDR پشتیبانی می‌کند.



۵۶ درصد: بهبود قابلیت‌های پاسخ

۵۲ درصد: نظارت بر محیط‌های ابری

۴۹ درصد: تشخیص حملات پیشرفته با استفاده از تلمتری XDR چند حسگری

۴۷ درصد: تسریع فرآیندهای پاسخ به حادثه

۴۶ درصد: تشخیص حملاتی که ابزارهای دیگر قادر به تشخیص آن‌ها نیستند.

۴۳ درصد: قابلیت جستجوی حمله

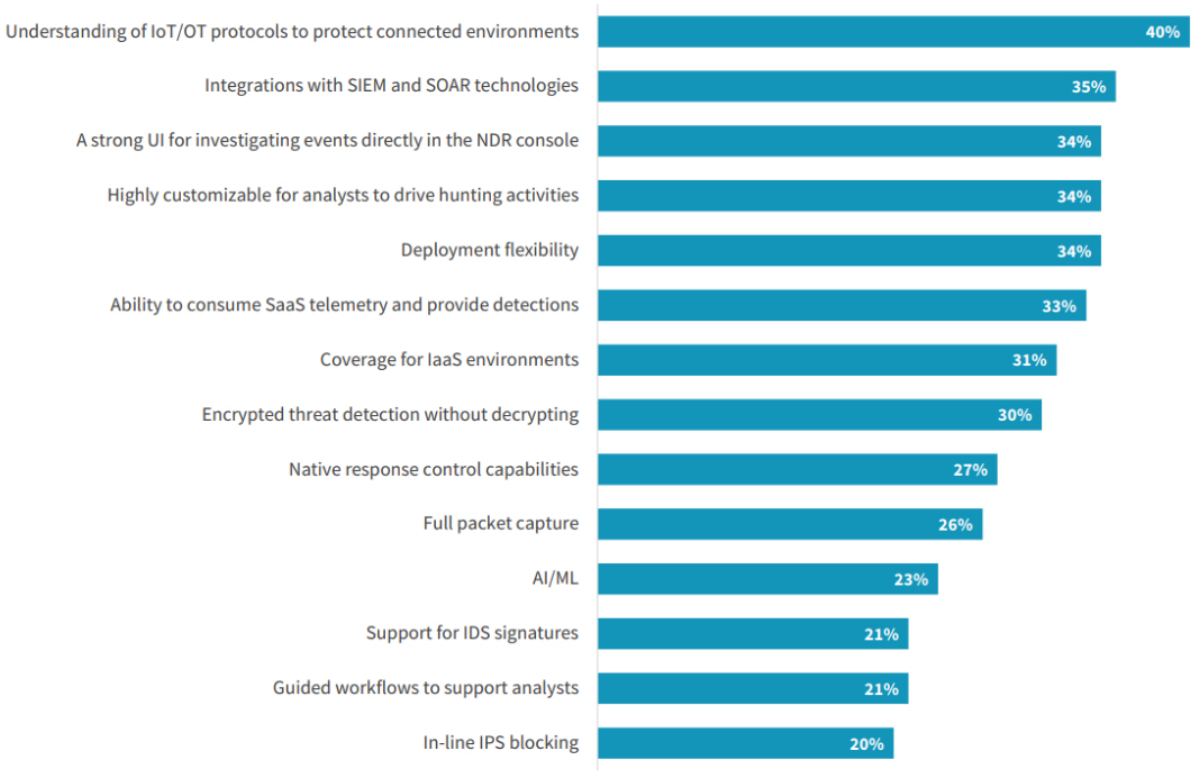
۴۱ درصد: نظارت بر دارایی‌هایی که agent ها نمی‌توانند روی آن‌ها مستقر شوند.

۳۹ درصد: پشتیبانی از فعالیت‌های کشف حقایق

قابلیت‌های پوشش و تحقیق درواقع مهم‌ترین موارد هستند.

پشتیبانی از موارد کاربردی که تا این حد گوناگون و متنوع هستند، به قابلیت‌هایی نیاز دارد.برای آنکه بتوان بخش‌های گوناگون محیط را به‌صورت سازگاری مدیریت کرد، درک پروتکل‌های IoT / OT (۴۰ درصد)، انعطاف‌پذیری استقرار (۳۴ درصد) و پوشش محیط‌های IaaS (۳۱) حائز اهمیت هستند.علاوه براین، قابلیت استفاده از دورسنجی SaaS (۳۳ درصد) نیز یک ویژگی جدیدتر بوده که می‌تواند به تکامل پوشش NDR کمک کند.در خصوص بررسی حوادث، تحلیلگران امنیتی معمولاً ترجیح می‌دهند ابتدا نحوه کار کردن آن‌ها را دریابند. بعضی از تحلیلگران ترجیح می‌دهند در مراحل اولیه فرآیند به SIEM تبدیل شوند؛ به‌گونه‌ای که ۳۵ درصد سازمان‌ها به نیاز به ادغام با ابزارهای SIEM و SOAR اشاره کردند. در مقابل، سازمان‌های دیگر ممکن است زمان بیشتری را در کنسول NDR صرف کنند. علت این امر ممکن است انجام تحلیل‌های اولیه بیشتر باشد، یا اینکه سازمان آن‌ها از یک SIEM استفاده نمی‌کند. درنتیجه، ۳۴ درصد سازمان‌ها به نیاز به استفاده از یک UI قوی برای بررسی مستقیم رویدادها اشاره کردند. درنهایت، ۳۰ درصد اعلام کردند که برای تشخیص حملات رمزنگاری‌شده، نیازی به رمزگشایی ندارند و تهدیدات ناشی از این نوع حملات اشاره کردند.

مهم‌ترین ویژگی‌های NDR



۴۰ درصد: درک پروتکل‌های IoT / OT برای حفاظت از محیط‌های متصل
۳۵ درصد: بررسی فناوری‌های SIEM و SOAR
۳۴ درصد: یک UI قوی برای بررسی مستقیم رخدادها در کنسول NDR
۳۴ درصد: سفارشی‌سازی بالا برای تحلیل به‌منظور جستجوی فعالیت‌ها
۳۴ درصد: انعطاف‌پذیری استقرار
۳۳ درصد: قابلیت مصرف دورسنجی SaaS و تشخیص
۳۱ درصد: پوشش محیط‌های IaaS
۳۰ درصد: تشخیص حمله رمزنگاری‌شده بدون رمزگشایی
۲۷ درصد: قابلیت‌های کنترل پاسخ محلی
۲۶ درصد: ضبط کامل بسته
۲۳ درصد: AI / ML
۲۱ درصد: پشتیبانی از امضاهای IDS
۲۱ درصد: جریان‌های کاری راهنما برای پشتیبانی از تحلیل
۲۰ درصد: مسدود کردن IPS درون برنامه‌ای

AI قوی بخش جدایی‌ناپذیر NDR شده است.

در طول چند سال گذشته، فروشندگان NDR قابلیت‌های هوش مصنوعی و یادگیری ماشین را به ابزارهای خود اضافه کرده‌اند. کاربران نیاز به پشتیبانی AI/ML را ذکر کرده‌اند؛ به‌گونه‌ای که ۴۶ درصد آن‌ها اعلام کرده‌اند که قابلیت‌های AI قوی برای NDR ضروری و حیاتی است. همچنین ۴۵ درصد آن‌ها ذکر کردند که وجود AI قوی، حائز اهمیت است. قطعاً AI می‌تواند حملات را بهتر شناسایی کند؛ به‌گونه‌ای که ۶۱ درصد سازمان‌ها به NDR هایی علاقه‌مند هستند که مجهز به AI است تا دقت تشخیص را بهبود بخشند. ۵۹ درصد سازمان‌ها نیز به‌سرعت تشخیص بهتر اشاره کردند.

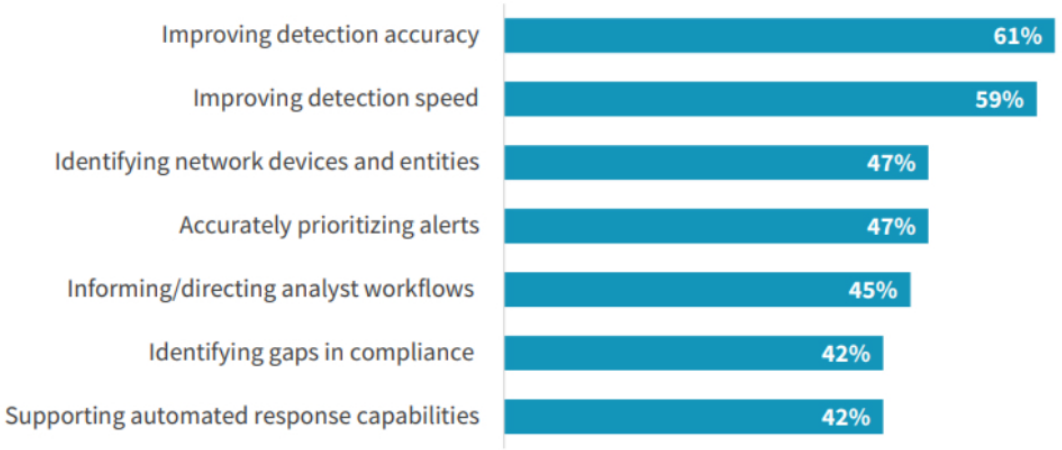
AI/ML از منظر کارآمدی و جریان کاری نیز مزایایی به همراه دارد. به‌طور مشخص، سازمان‌های پاسخ‌دهنده مکرراً به موارد زیر اشاره کردند: اولویت‌بندی دقیق هشدارها (۴۷ درصد)، اطلاع‌رسانی / هدایت جریان‌های کاری تحلیلی (۴۵ درصد) و خودکارسازی پاسخ (۴۲ درصد). این قابلیت‌ها به‌خصوص در محیط‌های ابری که مقیاس و سرعت حیاتی هستند، می‌تواند به تیم‌های امنیتی کمک کند تا با این مشخصه‌ها همگام شوند.

اهمیت AI در ابزارهای NDR

46%
Strong AI capabilities are a **critical** attribute of NDR tools

45%
Strong AI capabilities are an **important** attribute of NDR tools

دلایل استفاده از قابلیت‌های AI/ML به‌عنوان بخشی از راه‌حل‌های NDR



۶۱ درصد: بهبود دقت شناسایی

۵۹ درصد: بهبود سرعت شناسایی

۴۷ درصد: شناسایی دستگاه‌ها و موجودیت‌های شبکه

۴۷ درصد: اولویت‌بندی دقیق هشدارها

۴۵ درصد: اطلاع‌رسانی / هدایت جریان‌های کاری تحلیلی

۴۲ درصد: شناسایی شکاف‌ها در پذیرش

۴۲ درصد: پشتیبانی از قابلیت‌های پاسخ خودکار

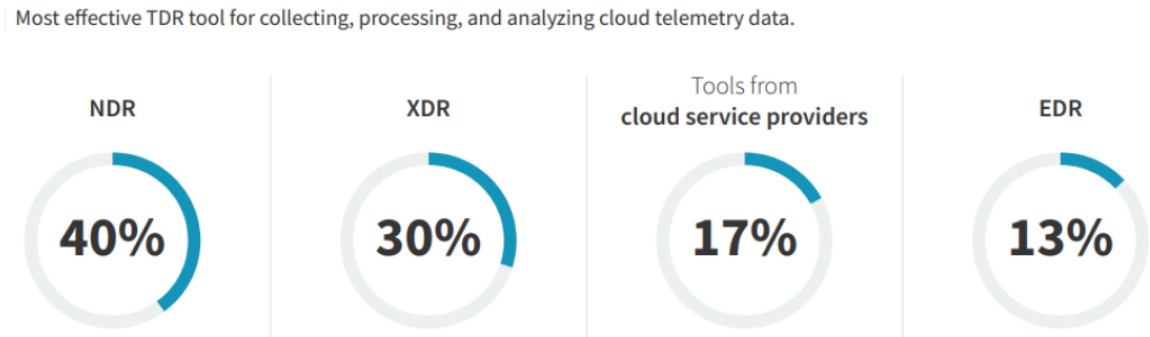
NDRبه‌عنوان یک مؤلفه کلیدی در راهبردهای XDR نمایان شد

اغلب سازمان‌ها NDR را به‌عنوان یک مؤلفه بنیادی در XDR در نظر می‌گیرند.

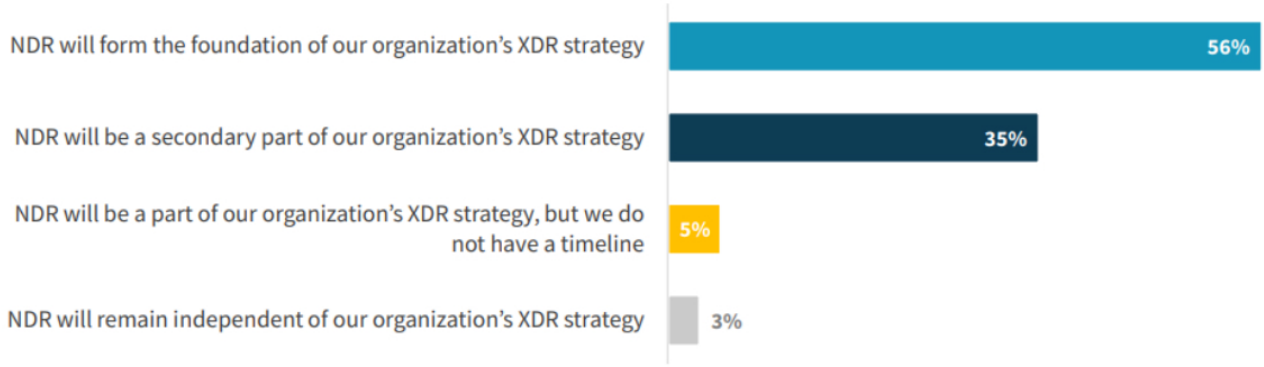
XDR در وسعت دید بسیاری از سازمان‌ها قرار دارد. درواقع بیش از نیمی از سازمان‌ها (۵۲ درصد) اعلام کردند در حال استقرار XDR هستند. ۴۱ درصد آن‌ها قصد دارند در ۱۲ الی ۲۴ ماهه آینده، XDR را مستقر کنند. اگرچه زمانی XDR به‌عنوان تعمیمی از EDR در نظر گرفته می‌شد، اما به نظر می‌رسد اغلب سازمان‌ها با این توصیف مخالف هستند. به‌طور مشخص، ۵۶ درصد آن‌ها اعلام کردند NDR اساس راهبرد XDR سازمان آن‌ها را شکل می‌دهد. بیش از یک‌سوم آن‌ها (۳۵ درصد) گفتند NDR بخش فرعی XDR است. تنها ۳ درصد سازمان‌ها اعلام کردند که NDR مستقل از XDR است. از دید بسیاری از سازمان‌ها، XDR اساس راهبردهای تشخیص و پاسخ ابری آن‌ها را تشکیل خواهد داد. ۴۰ درصد آن‌ها اعلام کردند که NDR مؤثرترین روش در جمع‌آوری، پردازش و تحلیل داده‌های دورسنجی ابری است. ۳۰ درصد نیز معتقدند XDR مؤثرترین ابزار است.

۵۲ درصد سازمان‌ها در فرآیند استقرار یک راه‌حل XDR هستند.

مؤثرترین ابزار TDR برای جمع‌آوری، پردازش و تحلیل داده‌های دورسنجی ابر



نقش NDR در یک راهبرد XDR



۵۶ درصد: NDR اساس راهبرد NDR سازمان را تشکیل می‌دهد.
۳۵ درصد: NDR بخش فرعی راهبرد NDR سازمان خواهد بود.
۵ درصد: NDR بخشی از راهبرد XDR سازمان بوده، اما ما یک خط زمانی نداریم.
۳ درصد: NDR مستقل از راهبرد XDR سازمان ما است.

توافق محدودشده در خصوص نحوه استفاده از NDR

تقریباً نیمی از سازمان‌ها (۴۸ درصد) ترجیح می‌دهند NDR و دیگر قابلیت‌های XDR را از یک فروشنده دریافت کنند. ۴۳ درصد آن‌ها اعلام کردند که استفاده از یک رویکرد مشارکتی، بیشترین اثربخشی را خواهد داشت. به‌طورکلی، ۸۹ درصد به ارائه‌دهندگان خدمت مراجعه خواهند کرد (برای ادغام یا مدیریت).بنابراین، درحالی‌که یک توافق نظر وجود دارد که XDR باید توسط فروشنده هدایت شود، نه فراهم‌کننده خدمات، اما سازمان‌ها در خصوص بهترین رویکرد توافق نظر ندارند. درنهایت، انتخاب بهترین مسیر به موارد زیر بستگی دارد: ابزارهایی که مستقرشده‌اند، روابط میان فروشندگان و خروجی که از XDR انتظار داریم.

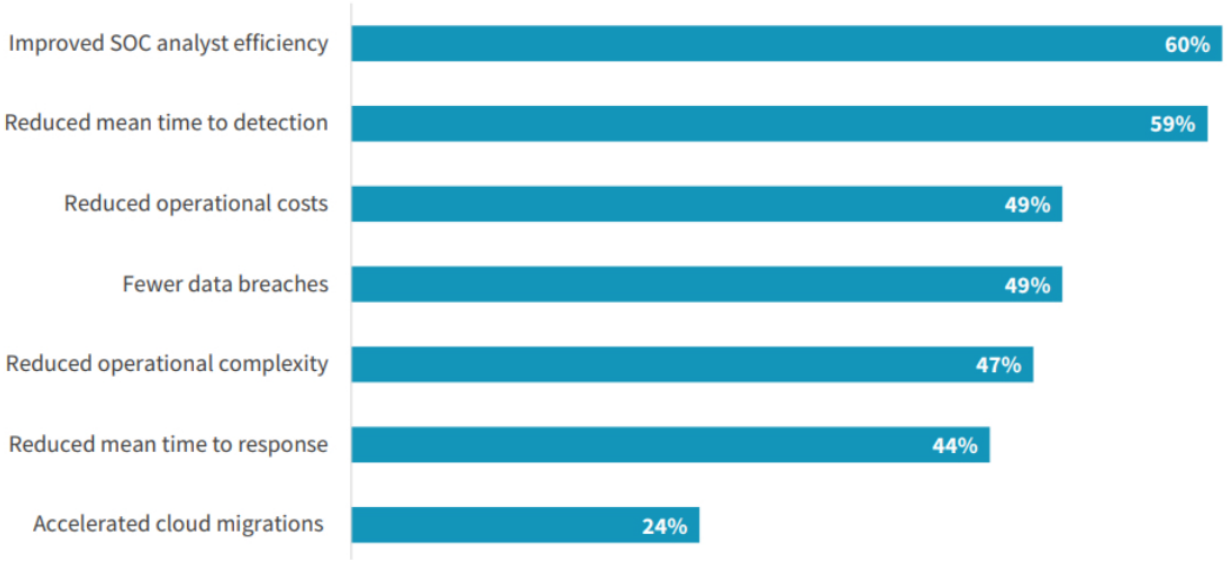
چگونه از XDR به‌عنوان بخشی از یک راهبرد XDR استفاده خواهد شد؟

۴۸ درصد: ما ترجیح می‌دهیم NDR را از همان فروشنده‌ای دریافت کنیم که سایر ابزارهایی را از آن خریداری کردیم که از راهبرد XDR ما پشتیبانی می‌کند.
۴۳ درصد: ما ترجیح می‌دهیم فروشنده NDR ما به‌صورت مشترک با دیگر فروشندگان همکاری کند تا از راهبرد XDR ما پشتیبانی کند.
۶ درصد: ما ترجیح می‌دهیم NDR و دیگر ابزارهایی که از راهبرد XDRپشتیبانی می‌کنند، توسط یک ارائه‌دهنده خدمات، فراهم شود.
۲ درصد: ما ترجیح می‌دهیم از NDR و دیگر ابزارهایی که از راهبرد XDR ما پشتیبانی می‌کنند، به‌عنوان یک خدمت مدیریت‌شده استفاده کنیم.

تیم های امنیتی به مزایای امنیتی و کسب‌وکاری NDR اشاره کردند.
بهبود کارآمدی تحلیل و زمان تشخیص حمله، مزایای رایج NDR هستند

تیم‌های امنیتی گزارش کردند که استفاده از NDR مزایای بسیاری برای سازمان آن‌ها در بردارد. درواقع، سازمان‌های شرکت‌کننده در بررسی ادعا کردند که استفاده از NDR به‌طور متوسط سه مزیت برای آن‌ها دارد. ۶۰ درصد سازمان‌ها به بهبود کارآمدی تحلیل SOC اشاره کردند. ۵۹ درصد کاهش میانگین زمان تشخیص و ۴۹ درصد کاهش نقض داده‌ها را مطرح کردند. ۴۹ درصد سازمان‌ها، علاوه بر خروجی‌های امنیتی مثبت به کاهش هزینه‌های عملیاتی اشاره کردند. ۴۷ درصد کاهش پیچیدگی عملیاتی را مطرح کردند. تقریباً یک‌چهارم (۲۴ درصد) سازمان‌ها اعلام کردند NDR به تسریع مهاجرت ابری کمک کرده است. بنابراین، باوجوداینکه راهبردهای تشخیص حمله و پاسخ به آن بسیار گوناگون است، NDR در دستیابی به خروجی‌های امنیتی و کسب‌وکاری بهتر به سازمان‌ها کمک خواهد کرد.
سازمان‌های پاسخگو ادعا کردند که استفاده از NDR حداقل، به‌طور متوسط سه مزیت برای آن‌ها در پی دارد.

مزایای NDR



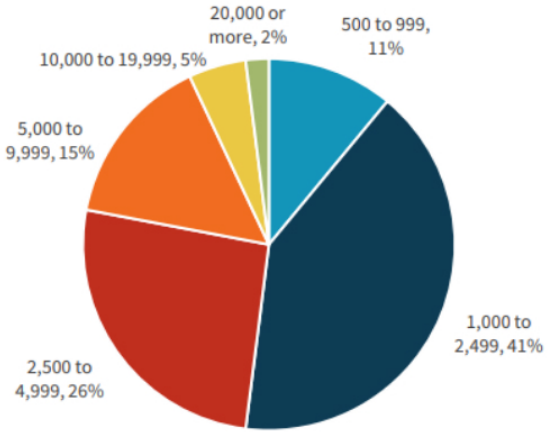
۶۰ درصد: بهبود کارآمدی تحلیل SOC
۵۹ درصد: کاهش میانگین زمان تشخیص
۴۹ درصد: کاهش هزینه‌های عملیاتی
۴۹ درصد: کاهش نقض داده
۴۷ درصد: کاهش پیچیدگی عملیاتی
۴۴ درصد: کاهش میانگین زمان پاسخ
۲۴ درصد: تسریع مهاجرت ابری

روش تحقیق و اطلاعات آماری

برای جمع‌آوری داده‌ها در این گزارش، ESG یک بررسی آنلاین جامع روی متخصصان IT، امنیت سایبری و شبکه در سازمان‌های دولتی و خصوصی در شمال آمریکا از تاریخ ۵ اوت ۲۰۲۲ تا ۱۶ اوت ۲۲ انجام داده است. پاسخ‌دهندگان برای آنکه در این بررسی واجد شرایط باشند، باید در حوزه IT، امنیتی سایبری یا شبکه متخصص بوده و مسئول ارزیابی، خرید و مدیریت محصولات و خدمات امنیتی شبکه برای سازمان خود باشند. از تمامی پاسخ‌دهندگان خواسته شد تا بررسی آماری را در ازای دریافت پول نقد یا معادل آن انجام دهند.

به منظور یکپارچگی داده‌ها، پاسخ‌دهندگانی که واجد شرایط نبودند و پاسخ‌های تکراری حذف‌شده و پاسخ‌های کامل شده باقیمانده غربالگری شدند (بر اساس تعداد معیارها). درنهایت، یک نمونه از ۳۷۶ متخصص IT، امنیت سایبری و شبکه باقی ماند.

پاسخ‌دهندگان برحسب تعداد کارکنان



پاسخ‌دهندگان برحسب سن شرکت