**EDR و XDR هر دو برای جایگزینی رویکردهای قدیمی و واکنشی به امنیت سایبری طراحی شده اند. در نتیجه EDR و XDR از چند جهت مشابه هستند، مانند:**

* **رویکرد پیشگیرانه:** راه‌حل‌های امنیتی سنتی اغلب بر شناسایی و اصلاح تهدیدات مداوم متمرکز هستند. EDR و XDR با جمع‌آوری داده‌های عمیق و استفاده از تجزیه و تحلیل داده‌ها و اطلاعات تهدید برای شناسایی تهدیدها قبل از وقوع، سعی در جلوگیری از حوادث امنیتی دارند.
* **پاسخ سریع تهدید:** EDR و XDR هر دو از تشخیص و پاسخ خودکار تهدید پشتیبانی می کنند. این یک سازمان را قادر می‌سازد تا هزینه، تأثیر و آسیب ناشی از یک حمله سایبری را با پیشگیری یا اصلاح سریع آن به حداقل برساند.
* **پشتیبانی Threat Hunting:** Threat Huntingبا اجازه دادن به تحلیلگران برای شناسایی و اصلاح مسائل امنیتی احتمالی قبل از سوء استفاده توسط مهاجم، امنیت پیشگیرانه را امکان پذیر می کند. EDR و XDR دید عمیق و دسترسی آسان به داده ها را فراهم می کنند که به تلاش های شکار تهدید کمک می کند.

**علیرغم شباهت‌هایشان، EDR و XDR رویکردهای متفاوتی برای امنیت سایبری دارند. برخی از تفاوت های اولیه بین EDR و XDR عبارتند از:**

* **تمرکز:** EDR بر محافظت از Endpoint، ارائه دید عمیق و پیشگیری از تهدید برای یک دستگاه خاص متمرکز است. XDR دید وسیع تری دارد و امنیت را در Endpoint، محاسبات ابری، ایمیل و سایر راه حل ها یکپارچه می کند.
* **یکپارچه‌سازی راه‌حل:** راه‌حل‌های EDR می‌توانند بهترین محافظت را برای نقاط پایانی فراهم کنند، و یک سازمان ممکن است بتواند به صورت دستی آنها را با مجموعه‌ای از راه‌حل‌های نقطه‌ای ادغام کند. XDR برای ارائه دید یکپارچه و مدیریت تهدید در یک راه حل واحد طراحی شده است و معماری امنیتی سازمان را به طور چشمگیری ساده می کند.

**نقاط قوت و مزایای EDR:**

EDR، یا Endpoint Detection and Response، داده‌ها را از چندین Endpoint جمع‌آوری و تجزیه و تحلیل می‌کند تا انحرافات رفتاری، داده‌های حادثه و مرتب‌سازی هشدارهایی را که می‌تواند تهدیدی برای Endpoint ها را به طور بالقوه برای سیستم اطلاعاتی که به آن متصل است ، شناسایی کند.

EDR به عنوان دسته‌ای از ابزارها و راه‌حل‌ها تعریف می شود که در شناسایی فعالیت‌های مشکوک به طور مستقیم بر روی میزبان‌های سیستم اطلاعاتی تمرکز دارند به زبان ساده، EDR نسل جدیدی از ضد بدافزارها است که دیگر به Signature سیستم‌های برای تشخیص رفتار مخرب متکی نیست. EDR قابلیت های تحلیل فرآیند رفتاری را برای تعیین انحراف اضافه می کند.

XDR (EXtended Detection Response) تکمیل شده ی EDR است. و این تکامل در چند محور صورت می گیرد.

XDR یک فناوری ارائه‌شده در فضای ابری است که شامل راه‌حل‌های چند نقطه‌ای و تجزیه و تحلیل‌های پیشرفته برای مرتبط کردن هشدارها از چندین منبع به حوادث از سیگنال‌های ضعیف‌تر فردی برای ایجاد تشخیص دقیق‌تر است. هدف آن کاهش محصولات اضافه ، کاهش هشدار های اضافه ، چالش‌های یکپارچه‌سازی و هزینه‌های عملیاتی است، این محصول برای تیم‌های عملیات امنیتی که برای مدیریت مجموعه‌ای از SIEM یا SOAR استفاده میکنند ، جذاب خواهد بود.

در حالی که EDR در سطح Endpoint تشخیص می دهد، XDR فراتر از آن است. قادر به جمع آوری و شناسایی فعالیت های انحرافی و بالقوه مخرب در دستگاه هایی مانند سرورها، ابرها، شبکه ها و …

اما فراتر آن XDR قابلیت‌های پیچیده‌تری را ارائه می‌کند ، به‌عنوان مثال، امکان افزایش سطح زمینه‌سازی با اتصال به CTI را فراهم می‌کند، با تلاقی اطلاعات فنی شناسایی‌شده با محتوای خارجی، ظرفیت پیش‌بینی بیشتری را به همراه می‌آورد تا اصلاح شود.