positive technologies

MaxPatrol Endpoint Detection and Response

محافظت از دستگاه‌های شرکت و کارکنان در برابر حملات پیچیده و هدفمند

٪۷۸ از حملات در سال ۲۰۲۳ هدفمند بودند

۳ نوع برتر روندهای فعلی نشان می‌دهند که مهاجمان از روش های زیر استفاده می‌کنند:

باج‌افزارها، سرقت‌کننده‌های اطلاعات، تروجان‌های دسترسی از راه دور

Trends

MaxPatrol EDR

MaxPatrol EDR به شناسایی سریع حملات پیچیده و هدفمند کمک می‌کند و با در نظر گرفتن ویژگی‌های زیرساخت و فرآیندهای امنیتی شرکت شما، امکان پاسخگویی مطمئن و خودکارسازی عملیات‌های روزمره را فراهم می‌آورد.

- شناسایی حملات در حال توسعه روی دستگاه‌ها در مراحل اولیه که ممکن است توسط سایر ابزارهای امنیتی نادیده گرفته شوند.
- جمع‌آوری داده‌های مهم برای تحقیقات و بررسی‌های دقیق.
- توقف مهاجم در عرض چند ثانیه.
- کمک به تحلیل‌گران SOC و مدیران خدمات امنیت سایبری در بررسی و جلوگیری از حملات از طریق مسدودسازی اقدامات مخرب روی دستگاه‌های انتهایی.

- قابلیت عملیات خودکار عامل
- تحلیل استاتیک و رفتاری روی عامل
- پیکربندی انعطاف‌پذیر قوانین شناسایی و پاسخ
- عدم تداخل با سایر راهکارهای امنیتی
- عدم تداخل با سایر راهکارهای امنیتی
- سفارشی‌سازی محیط ایزوله‌سازی فایل‌ها (sandboxing)
- پشتیبانی از سیستم‌عامل‌های Linux، Windows و macOS

پاسخ آنی روی میزبان‌ها

شناسایی به‌موقع و پیوسته بدافزار، با مجموعه گسترده‌ای از اقدامات برای پاسخ‌دهی خودکار و سریع: توقف فرآیند، حذف فایل، ایزوله کردن دستگاه، ارسال فایل‌ها برای تحلیل و ایجاد sinkhole.

شناسایی پویا تهدیدات

شناسایی حملاتی که از ابزارهای مشروع مانند، PowerShell، WMI، CMD، و Bash استفاده می‌کنند و ممکن است توسط تحلیل مبتنی بر امضا نادیده گرفته شوند.

مجموعه قوانین تخصصی PT ESC

شامل قوانینی است که تهدیدات و تاکتیک‌ها و تکنیک‌های مهاجمان را بر اساس ماتریس MITRE ATT&CK شناسایی می‌کند (برترین ۵۰ مورد برای ویندوز و ۲۰ مورد برتر برای لینوکس).

یکپارچگی آسان در زیرساخت‌ها

به عنوان یک عامل واحد برای شناسایی، پاسخ‌دهی، جمع‌آوری داده های تله‌متری و اطلاعات آسیب‌پذیری روی میزبان‌ها عمل می‌کند از تمامی سیستم‌عامل‌های محبوب، از جمله سیستم‌عامل‌های روسی و ساختارهای VDI پشتیبانی می‌کند.

مناسب برای سازمان های مختلف

صرفه‌جویی در زمان و منابع متخصصان
ایجاد حفاظت چندلایه بر اساس راهکارهای جامع یا ادغام محصولات متعدد همیشه در بودجه سازمان نیست. با MaxPatrol EDR، می‌توانید با هزینه مناسب، حفاظت از دستگاه‌های کارکنان و سازمان را آغاز کرده و به‌تدریج فرآیندهای امنیتی را پیاده‌سازی کنید.

عدم تداخل با سایر راهکارهای امنیتی
سازمان‌ها می‌توانند از چندین راهکار حفاظتی استفاده کرده و از تخصص متنوع ارائه‌دهندگان مختلف بدون تأثیر بر فرآیندهای کسب‌وکار بهره ببرند.

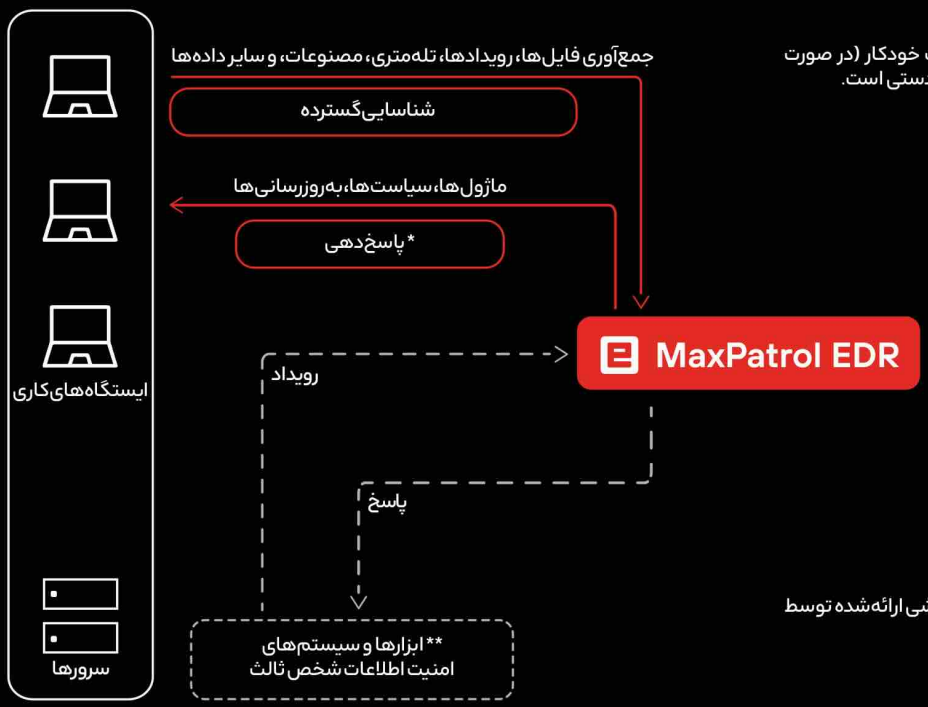
انطباق با ویژگی‌های زیرساخت
امکان تنظیم انعطاف‌پذیر سیاست‌های شناسایی و پاسخ‌دهی را متناسب با معماری فراهم می‌کند. تعادلی ایده‌آل بین بار میزبان و برآورده‌سازی نیازهای SOC حفظ می‌شود.

خودکارسازی عملکردهای پاسخ‌دهی
اکثر راهکارهای EDR تنها عملکردهای پاسخ‌دهی مانند توقف فرآیندها و حذف فایل‌ها را ارائه می‌دهند. MaxPatrol EDR به شما امکان می‌دهد منطق پاسخ‌دهی را کنترل کنید و از تمام گزینه‌های موجود برای پاسخ‌دهی به‌صورت دستی یا خودکار استفاده کنید.

عملکرد در بخش‌های بسته
برای عملکرد به اتصال اینترنت نیاز ندارد. به‌روزرسانی‌های تخصصی را می‌توان در صورت نیاز به انتقال یک‌طرفه از طریق سرور واسط ارائه کرد.

منطق و رابط کاربری آشنا
MaxPatrol EDR به سبک سایر محصولات Positive Technologies طراحی شده و موجودیت‌ها، احراز هویت، خدمات، و سناریوهای میان‌محصولی آشنا را ارائه می‌دهد و به کاربر کمک می‌کند تا به‌راحتی شروع کند.

نحوه کار MaxPatrol EDR



* پاسخ‌دهی قابل پیکربندی در هر دو حالت خودکار (در صورت مجاز بودن و پشتیبانی توسط سیاست‌ها) و دستی است.

** ادغام با افزودن ماژول‌های کاربردی سفارشی ارائه‌شده توسط Positive Technologies و شرکا

global.ptsecurity.com
info@ptsecurity.com

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید

.برای درخواست آزمایشی رایگانPositive Technologies، با ما تماس بگیرید.

PT@SafeNEST.ir

درباره Positive Technologies

Positive Technologies یکی از ارائه‌دهندگان برتر راهکارهای ارزیابی آسیب‌پذیری، مدیریت تطبیق و تحلیل تهدیدات به بیش از ۳,۰۰۰ مشتری در سطح جهانی است. راهکارهای ما به‌طور یکپارچه در سراسر کسب‌وکار شما کار می‌کنند: حفاظت از برنامه‌ها در حال توسعه، ارزیابی آسیب‌پذیری‌های شبکه و برنامه‌ها، اطمینان از تطبیق با الزامات قانونی و مسدودسازی حملات در زمان واقعی. تعهد ما به مشتریان و پژوهش‌ها به Positive Technologies شهرتی به عنوان یکی از معتبرترین مراجع در امنیت SCADA، بانکداری، مخابرات، برنامه‌های وب و ERP داده است و در گزارش IDC به عنوان سریع ترین شرکت در حال رشد در مدیریت امنیت و آسیب‌پذیری در سال ۲۰۱۲ شناخته شده است. برای اطلاعات بیشتر درباره Positive Technologies، به سایت ptsecurity.com مراجعه کنید.

منبع: پیش‌بینی جهانی مدیریت امنیت و آسیب‌پذیری IDC 2013–2017 و سهم فروشندگان در سال ۲۰۱۲، سند شماره 242465، آگوست ۲۰۱۳. بر اساس رشد درآمد سالانه در سال ۲۰۱۲ برای فروشندگانی با درآمد بیش از ۲۰ میلیون دلار.

SAFE NEST IT COMPANY

Safenest.ir Safe NEST شرکت فناوری ارتباطات آشیانه امن ارائه دهنده خدمات زیرساخت و امنیت شبکه می باشد که دارای مجوز توزیع کننده و نمایندگی فروش و خدمات محصولات شرکت PT در ایران است همچنین دارای تیمی مجرب در ارایه خدمات امنیت شبکه مانند تست نفوذ و ارزیابی امنیتی و راه اندازی و راهبری مرکز عملیات امنیت و اقدامات و محصولات بومی جهت شناسایی حملات فیشینگ و حفاظت از برندهای معتبر می باشد.

شرکت Positive Technologies

Positive Technologies پیشرو در صنعت امنیت سایبری و ارائه‌دهنده جهانی راهکارهای امنیت اطلاعات است.
ماموریت ما: حفاظت از کسب‌وکارها و صنایع مختلف در برابر حملات سایبری و آسیب‌های غیرقابل‌تحمل.
بیش از ۳,۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند.