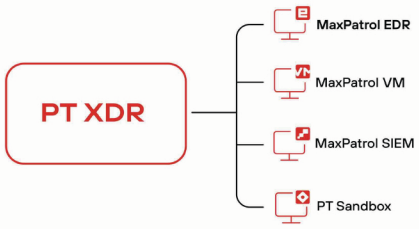
positive technologies

PARSPOUYA
NETWORK SECURITY SERVICES

PT Extended Detection and Response

یک راهکار XDR برای شناسایی پیشرفته و پاسخ به تهدیدات پیچیده و حملات هدفمند

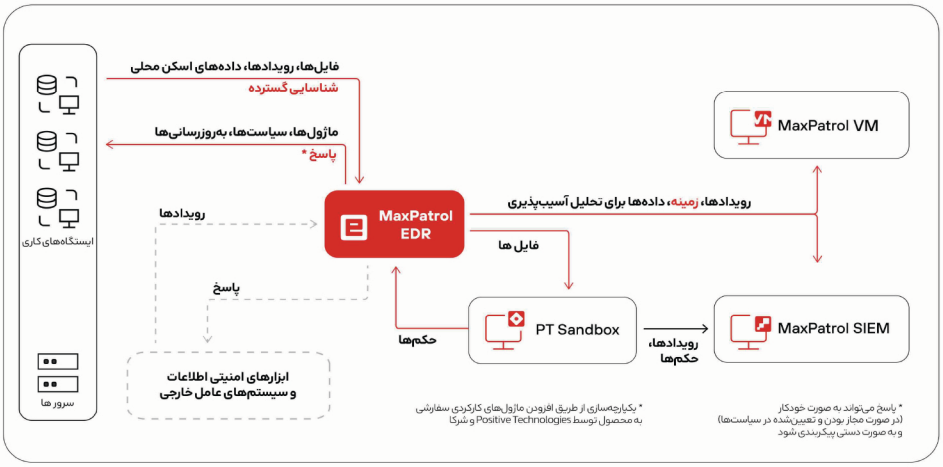
PT Extended Detection and Response (PT XDR) برای مدیریت جمع‌آوری اطلاعات، شناسایی حملات پیشرفته، و همچنین بررسی و پاسخ سریع به رخدادها طراحی شده است. PT XDR داده‌ها را از ایستگاه‌های کاری و سرورها جمع آوری و تقویت می‌کند، تحلیل استاتیک و داینامیک تهدیدات را هم در دستگاه‌ها و هم در سیستم‌های خارجی انجام می‌دهد، حملات پیچیده و هدفمند در زیرساخت را شناسایی کرده و به شما امکان می‌دهد تا به این تهدیدات هم به صورت دستی و هم به صورت خودکار پاسخ دهید.



- جمع‌آوری رویدادهای امنیتی
- اطلاعات امنیتی را جمع‌آوری کرده و داده‌های به‌دست‌آمده از ابزارهای نظارت داخلی و Sysmon را تقویت می‌کند.
- شناسایی تهدیدات: تجزیه و تحلیل فایل‌ها و فرآیندها، اسکن YARA، همبستگی، شناسایی رفتاری و تحلیل رفتار کاربر (در حال توسعه).
- پاسخ به تهدیدات: حذف فایل‌ها، ایزوله کردن گره‌ها، توقف فرآیندها، تفسیر Lua، مسدودسازی IP، حذف فایل‌ها از استارت آپ و قرار دادن فایل‌ها در قرنطینه.
- تضمین یکپارچگی: ارسال رویدادها به سرور Syslog و MaxPatrol VM، ارسال گزارش‌ها به MaxPatrol VM، بررسی فایل‌ها در PT Sandbox و صدور داده‌ها به سیستم‌های خارجی.

به‌محض شناسایی یک تهدید، PT XDR می‌تواند به صورت خودکار اقدامات زیر را انجام دهد:

- حذف فایل
- پایان دادن به یک یا چند فرآیند
- مسدودسازی ترافیک شبکه
- ارسال فایل برای بررسی به PT Sandbox



قابلیت‌های PT XDR

مجموعه XDR خودکار و تخصصی:
مجموعه‌ای خودکار برای تحلیل و شناسایی تهدیدات پیشرفته. اپراتورهای SOC می‌توانند به طور مستقل فرضیه‌های مربوط به نقص امنیتی در گره‌ها را با استفاده از داده‌های تله‌متری آزمایش کنند.

پشتیبانی از همه پلتفرم‌ها:
PT XDR از عوامل روی سیستم‌عامل‌های ویندوز، لینوکس، و macOS پشتیبانی می‌کند.

یکپارچگی آسان:
کانکتورهای لازم برای یکپارچگی اجزا به‌صورت پیش‌فرض موجود است و تنها نیاز به اتصال شبکه برای تنظیم آن‌ها دارید.

خودکارسازی پاسخ به تهدیدات و کاهش زمان متوقف‌سازی حمله:
به‌طور خودکار گزینه‌های پاسخ به تهدید را پیشنهاد می‌دهد و سیستم‌های شبکه را به سلامت کامل بازمی‌گرداند.

کاهش نیاز به منابع و مهارت تیم PT XDR :
SOC فرآیندهای روزمره را خودکار می‌کند، اولویت بندی صف تحلیل را انجام می‌دهد و اطلاعات مرتبط با حملات و دلایل نقص امنیتی را فراهم می‌کند.

قابلیت‌های ارزشمند PT XDR

MaxPatrol EDR

- **ماژول YARA** برای تحلیل فایل‌ها و فرآیندها با امکان استفاده از قوانین سفارشی
- **درایور اختصاصی جمع‌آوری رویدادها**
- **ماژول جمع‌آوری مصنوعات** برای بررسی رخدادها
- **پیکربندی انعطاف‌پذیر** سیاست‌های شناسایی و پاسخ
- **شناسایی تزریق کتابخانه‌های مخرب**، بوت کیت‌ها، رمزگذاری‌ها و سایر بدافزارها
- **ماژول اجرای دستورات و اسکریپت‌های دلخواه**
- **عوامل برای ویندوز، لینوکس و macOS**
- **چندریسمانی**: ماژول‌ها می‌توانند به صورت موازی کار کنند
- **عامل خودکفا**: ماژول‌های اصلی پاسخ بدون اتصال به سرور C2 عمل می‌کنند و رویدادها ذخیره‌سازی می‌شوند

PT XDR = MaxPatrol EDR, MaxPatrol SIEM, MaxPatrol VM, PT Sandbox

- **دارای موتور همبستگی روی گره**، بیش از ۲۵۰ قانون آماده برای استفاده و امکان نوشتن قوانین سفارشی.
- **شناسایی تهدیدات** در زیرساخت و ساخت سیستم‌های پاسخ‌دهی پیچیده، از حمله با استفاده از محصولات شخص ثالث.
- **یکپارچگی بومی با MaxPatrol SIEM**: انجام موجودی‌گیری، همبستگی رویداد بین گره‌ها و شناسایی حوادث.
- **خودکارسازی شناسایی و رفع آسیب‌پذیری‌ها با استفاده از MaxPatrol VM**. تعیین اولویت‌ها بر اساس تخصص Positive Technologies و فهرست آسیب‌پذیری‌های رایج.
- **شناسایی بدافزارهای استفاده‌شده در حملات APT با کمک PT Sandbox**. مسدودسازی حملاتی که شامل انتقال بدافزار از طریق پیام رسان‌ها یا ترافیک رمزگذاری‌شده کاربران است
- **گسترش تخصص PT XDR** با کمک پلتفرم اطلاعات تهدید PT Feeds
- **امکان سفارشی‌سازی** برای تعامل با محصولات شخص ثالث و استفاده از اسکریپت‌های مشتری.
- **امکان ارسال فایل‌های تا ۱ گیگابایت برای تحلیل** در یک سندباکس با استفاده از ماژول http loader.

مزایای PT XDR

پاسخ خودکار به رخدادهای امنیتی
این کار باعث کاهش زمان لازم برای مدیریت رخدادهای فردی دریافتی از ابزارهای حفاظتی می‌شود و ورود به سیستم XDR را برای کاربران آسان‌تر می‌کند؛ به این معنی که برای تحقیق و پاسخ به رخدادها نیازی به تخصص بالا نیست.

یکپارچه‌سازی رویدادهای شناسایی‌شده توسط ابزارهای مختلف حفاظتی در یک زنجیره حمله
PT XDR رویدادهای ورودی را پردازش کرده و آن‌ها را به زنجیره‌های حمله قابل فهم ترکیب می‌کند و گزینه های پاسخ‌دهی ارائه می‌دهد؛ به‌عبارتی دیگر، حریان بزرگ رویدادها را به چند زنجیره برای پردازش توسط تحلیل‌گر SOC تبدیل می‌کند.

شناسایی نقطه اولیه حمله
هنگامی که یک زنجیره حمله ایجاد می‌شود، PT XDR علت حمله را شناسایی می‌کند. برای این کار، با سایر ابزارهای حفاظتی تعامل دارد تا زمینه هر مرحله از حمله را بدست آورد، مثلاً اطلاعات مربوط به حرکت جانبی مهاجم از سیستم NDR.

کاهش تعداد هشدارهای کاذب
بر اساس زمینه خاص و پردازش رویدادها از منابع مختلف، PT XDR تعیین می‌کند که کدام رویدادها کاذب هستند و کدام نه. این کار نیاز به تحلیل و بررسی دستی هر رویداد توسط تحلیل‌گر SOC را از بین می‌برد.

بهبود شکار تهدیدات پیشگیرانه
با استفاده از داده‌های تله‌متری خارج از گره، PT XDR قابلیت‌های شکار تهدیدات را گسترش می‌دهد. تحلیل‌گر نیازی به جابجایی بین کنسول‌ها برای اسکن تهدیدات ندارد و سطح تخصص بالایی نیز نیاز نیست.

پاسخ به تهدیدات
PT XDR شامل MaxPatrol EDR برای شناسایی و پاسخ به تهدیدات است.

ویرا ارتباط پارس پویا
آدرس:تهران،خیابان شریعتی،دوراهی قلهک
کوچه مرشدی،پلاک ۲،واحد ۲
تلفن:۷۵۳۹۷-۰۲۱ داخلی ۲۰۰ و ۲۰۰۰

Info@parspouya.com
Info@ptsecurity.info