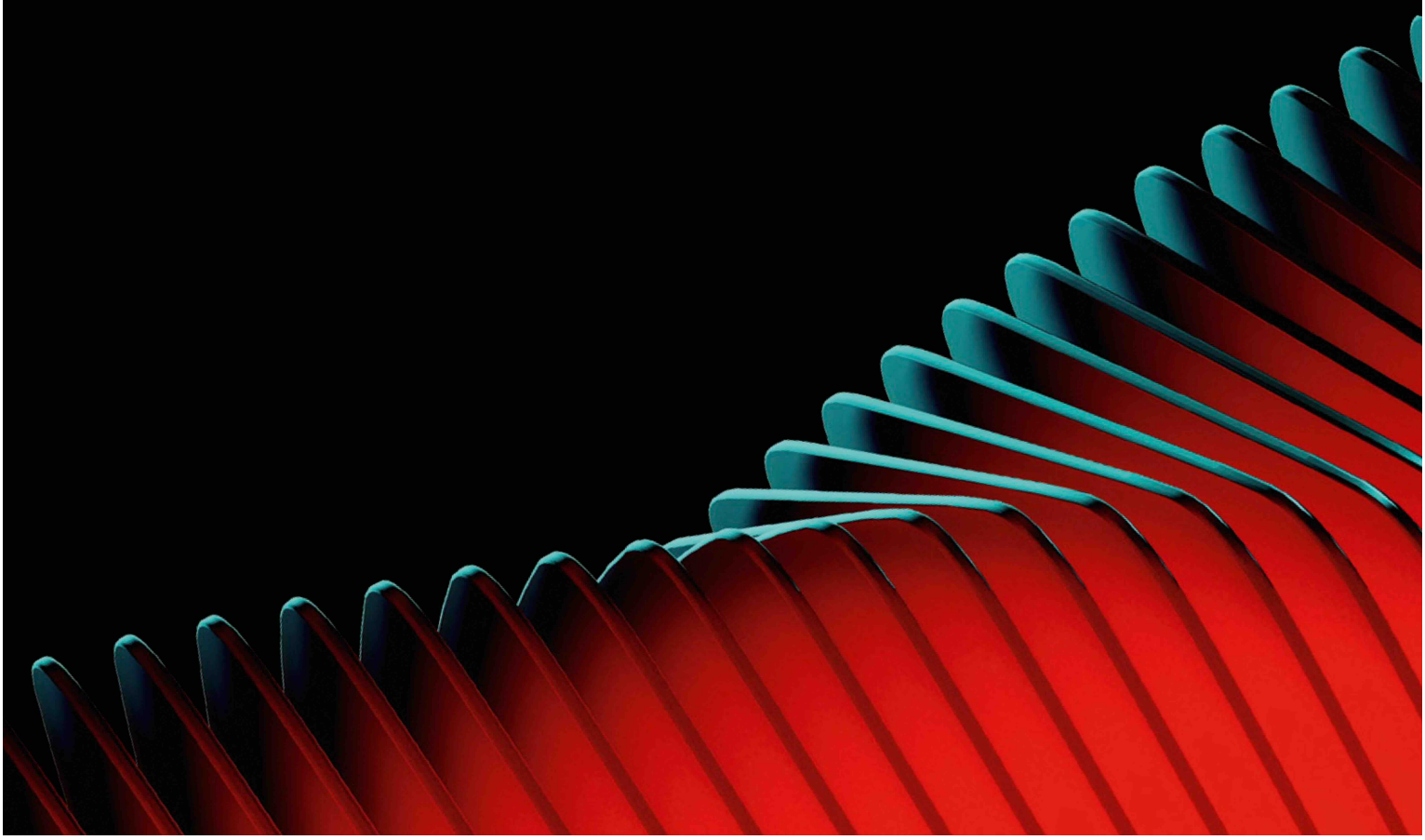
positive technologies

معرفی محصولات و خدمات

بزرگترین اپراتور امنیت سایبری روسیه



آنچه باید در مورد PT بدانیم

بیش از ۲۰۰۰ کارمند و ۸۰۰ متخصص امنیت

اپراتور اول امنیت سایبری در روسیه

کشف بیش از ۲۵۰ باگ Zero-Day در هر سال

بیش از ۲۰ سال سابقه در کشف آسیب پذیری

بیش از ۲۰ محصول در حوزه IT - OT - CT

کارفرمایان خصوصی و صنعتی

در بیست سال گذشته شرکت PT توانسته با سازمانهای بسیار زیادی در روسیه و سایر کشورهای دنیا خدمات و محصولات خود را ارایه کند برخی از آنها :

- ۴ از ۴ : شرکتهای اپراتور موبایل و زیرساخت روسیه
- ۸ از ۱۰ : بزرگترین بانکها و موسسات مالی روسیه
- ۸ از ۱۰ : شرکتهای بزرگ ارایه محصولات نفت و گاز در روسیه
- ۳ از ۴ : شرکتهای بزرگ در صنعت حمل و نقل در روسیه

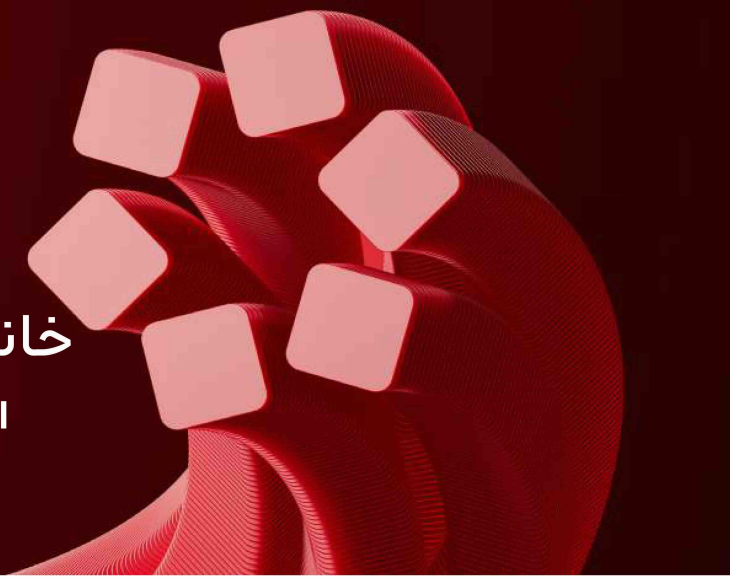
کارفرمایان دولتی

- وزارت انرژی روسیه
- وزارت بهداشت روسیه
- وزارت حمل و نقل روسیه
- وزارت کشور روسیه
- وزارت دفاع روسیه
- وزارت توسعه دیجیتال روسیه و ...

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.

positive technologies



خانواده محصولات پازتیو تکنولوژی

ارایه شده از بزرگترین اپراتور امنیت سایبری روسیه

PT NAD

یک سیستم کامل تحلیل ترافیک شبکه با هدف شناسایی حملات در تمامی لایه های شبکه و تحلیل اقدامات غیر طبیعی با استفاده از ML که میتواند به عنوان سنسور به همه SOC ها خدمات دهد.

90%

از شرکت‌ها با کمبود متخصصان امنیت اطلاعات مواجه‌اند

PT ISIM

محصولی منحصر به فرد که قابلیت تحلیل شبکه های صنعتی و پروتکلهای خاص آن را دارد و با شناخت کامل از تجهیزات رایج مانند siemens schneider abb رفتارهای خطرناک را شناسایی میکند

71%

از رخدادهای غیرقابل‌تحمل می‌توانند توسط مهاجمان در عرض یک ماه اجرا شوند.

PT AF

محصولی جامع برای کنترل حملات وب که به صورت ماشین مجازی ارایه میشود و پایگاه دانش آن به صورت روزانه بروزرسانی میشود امکان استقرار برنامه های داخلی سازمان پشت WAF اختصاصی را فراهم میکند .

100%

از زیرساخت‌ها می‌توانند به‌طور کامل توسط مهاجمان داخلی تصرف شوند.

PT SANDBOX

بررسی فایلهای مبادله شده در شبکه یا دریافتی از طریق ایمیلهای سازمان و شناسایی تهدیدات وظیفه این محصول است و میتواند بین شبکه های داخلی و اینترنت جهت انتقال امن فایلها کمک کند .

93%

از محیط‌های شبکه می‌توانند توسط مهاجمان عبور شده و به دسترسی شبکه محلی منجر شوند.

PT AI

Application Inspector میتواند در ساختار توسعه نرم افزاری سازمانها نقش موثری داشته باشد و به کمک آن آسیب پذیریهای نرم افزاری از طریق تحلیل سورس کدها شناسایی شوند .

positive technologies

PT NAD

تشخیص زودهنگام تهدیدات و حملات هدفمند
بررسی تخصصی با استفاده از کپی ترافیک شبکه

کشف حملات شبکه PT – یک سیستم تحلیل ترافیک شبکه (NTA) است که برای نظارت بر فعالیت‌های مخرب در محدوده و داخل شبکه استفاده می‌شود. این ابزار تحقیقاتی مناسب می‌تواند فعالیت‌های مخرب را حتی در ترافیک رمزگذاری‌شده شناسایی کند. PT NAD می‌داند در شبکه شرکت شما به دنبال چه چیزی بگردد.

مشاهده کامل شبکه

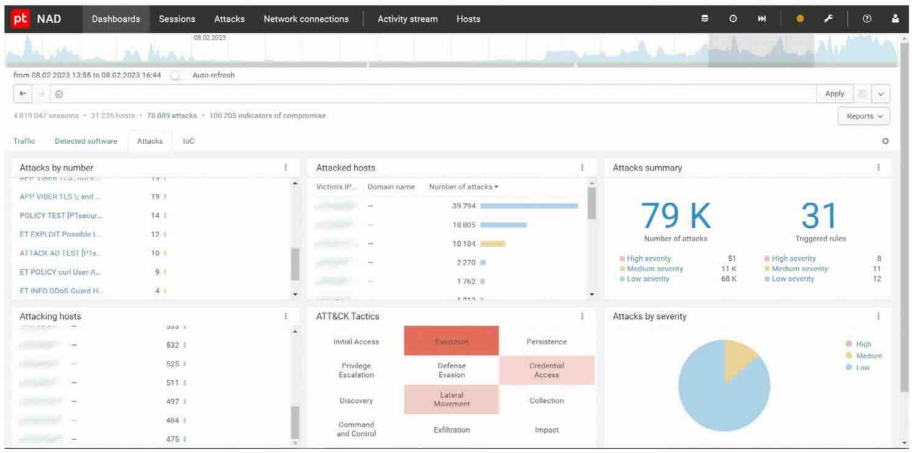
PT NAD بیش از ۱۰۰ پروتکل و ۹ پروتکل تونل را شناسایی کرده و ۳۵ پروتکل رایج را تا لایه L۷ تحلیل می‌کند. با تجزیه و تحلیل بیش از ۱۲۰۰ پارامتر پروتکلی، PT NAD مدل‌هایی برای گره‌های شبکه می‌سازد. این کار تصویری واضح از وضعیت زیرساخت فراهم می‌کند و به شناسایی نقص‌های امنیتی که می‌توانند امنیت را تضعیف کرده و موجب پیشرفت حملات شوند، کمک می‌کند.
PT NAD تمام میزبان‌های شبکه را تحت نظر دارد، استفاده از اجزای غیرقابل کنترل زیرساخت IT را به حداقل می‌رساند و ریسک هک شدن شرکت از طریق این اجزا را کاهش می‌دهد.

شناسایی تهدیدات مخفی و حملات هدفمند

PT NAD به‌طور خودکار تلاش‌های نفوذ به شبکه و حضور مهاجمان در زیرساخت را با استفاده از نشانه‌های مختلف، از جمله ابزارهای استفاده‌شده یا داده‌های منتقل‌شده به سرورهای مهاجم، شناسایی می‌کند.

افزایش کارایی مراکز عملیات امنیتی (SOC)

PT NAD منبعی ضروری برای راهکارهای SIEM است. این سیستم متادیتا و ترافیک خام را ذخیره کرده، کمک می‌کند جلسات مشکوک را سریعاً شناسایی و تحلیل کنید و امکان صدور و وارد کردن ترافیک را فراهم می‌آورد. PT NAD با ارائه دید کاملی از شبکه به SOCها، بررسی موفقیت حملات، ردیابی زنجیره حملات و جمع‌آوری شواهد را آسان‌تر می‌کند.



اپراتور در داشبورد اطلاعات دقیقی درباره فعالیت‌های مشکوک مشاهده می‌کند.
این امر به واکنش سریع به رخدادها و انجام تحقیقات کمک می‌کند.

مزایا

شناسایی مهاجمان
در ترافیک افقی (East-West)

شناسایی ابزارهای هکرها
و بدافزارهای تغییر یافته

کمک به برآورده کردن الزامات
حفاظت از اطلاعات

امکان یکپارچه‌سازی با سیستم‌های
SIEM و سندباکس‌ها

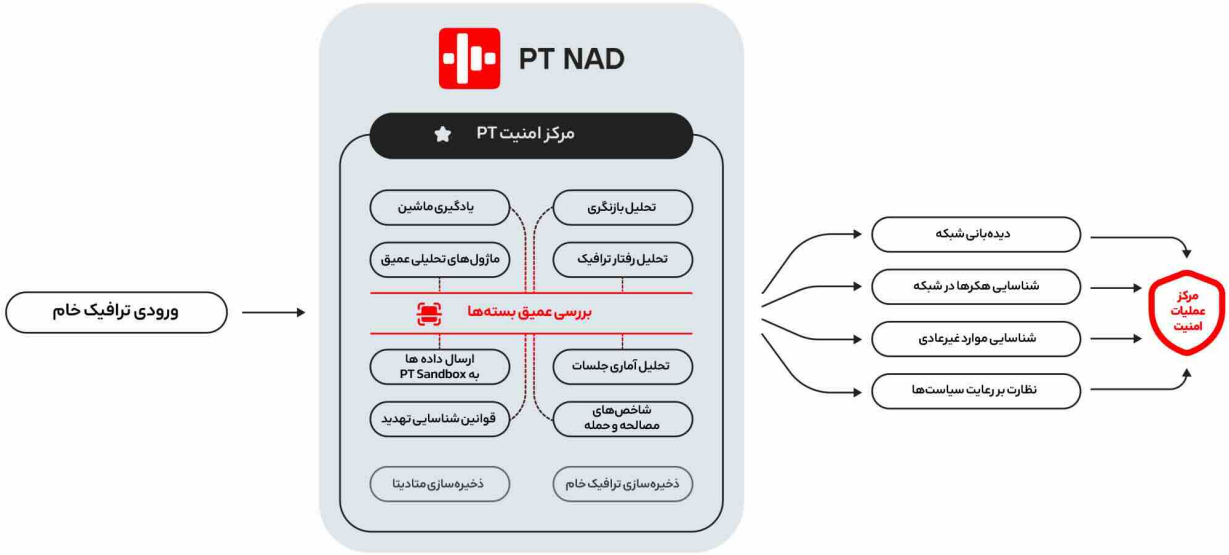
استقرار سریع
امکان یکپارچه‌سازی با سیستم‌های
SIEM و سندباکس‌ها

سناریوهای کاربرد

- **نظارت بر رعایت سیاست‌های امنیتی:** PT NAD مشکلات پیکربندی و موارد عدم رعایت سیاست‌های امنیتی را شناسایی می‌کند که می‌توانند راهی برای نفوذ مهاجمان باشند. نمونه‌ها شامل اعتبارنامه‌هایی است که به‌صورت متن ساده ارسال می‌شوند، رمزهای ضعیف، ابزارهای دسترسی از راه دور و ابزارهایی که فعالیت شبکه را پنهان می‌کنند.
- **شناسایی حملات در محیط خارجی و زیرساخت:** به لطف ماژول‌های تجزیه و تحلیل عمیق داخلی، قوانین خاص شناسایی تهدید، شاخص‌های مصالحه و تحلیل بازنگری، PT NAD می‌تواند حملات را هم در مراحل اولیه و هم پس از نفوذ مهاجمان به زیرساخت شناسایی کند.
- **تحقیقات حملات:** کارشناسان امنیت اطلاعات می‌توانند یک حمله را مکان‌یابی کرده، زنجیره حمله را ردیابی، آسیب‌پذیری های زیرساخت را شناسایی و اقدامات متقابل برای جلوگیری از حوادث آینده را اجرا کنند.
- **شکار تهدیدات:** PT NAD به سازماندهی عملیات شکار تهدیدات در شرکت کمک می‌کند، فرضیه‌هایی مانند حضور هکرها در شبکه را بررسی کرده و تهدیدات پنهانی که با ابزارهای استاندارد امنیت سایبری قابل شناسایی نیستند را شناسایی می‌کند.

PT NAD شناسایی می‌کند:

- تهدیدات در ترافیک رمزگذاری‌شده
- استفاده از ابزارهای هکرها، از جمله ابزارهای سفارشی‌سازی‌شده
- حرکت جانبی مهاجمان در شبکه
- ناهنجاری‌های شبکه
- میزبان‌های آلوده در شبکه
- حملات به کنترلر دامنه
- نشانه‌هایی از حملات قبلی که شناسایی نشده‌اند
- بهره‌برداری از آسیب‌پذیری‌های موجود در شبکه
- نشانه‌هایی از فعالیت‌های مخرب که از دید ابزارهای امنیتی پنهان شده‌اند
- اتصالات به دامنه‌های به‌طور خودکار تولیدشده
- عدم رعایت سیاست‌های امنیت اطلاعات (IS)



نحوه کار PT NAD

PT NAD ترافیک شبکه را در محیط خارجی و زیرساخت با استفاده از فناوری داخلی DPI (بررسی عمیق بسته‌ها) ضبط و تحلیل می‌کند. به‌عنوان منابع ترافیک می‌توان از دستگاه‌های TAP، شبکه‌های بسته‌ای و تجهیزات فعال شبکه استفاده کرد. با تحلیل کپی ترافیک شبکه با استفاده از ماژول‌های آماری و رفتاری، PT NAD فعالیت‌های هکری را در مراحل اولیه نفوذ به شبکه و همچنین هنگام تلاش مهاجمان برای تثبیت موقعیت خود در شبکه و ادامه حمله شناسایی می‌کند.
PT NAD یک کپی از ترافیک خام را ذخیره کرده و از آن برای تولید متادیتا جهت تحلیل بازنگری استفاده می‌کند. پس از به روزرسانی قوانین شناسایی تهدیدات و شاخص‌های مصالحه (IoC) از مرکز امنیتی PT NAD، PT Expert به‌طور خودکار داده های ترافیک جمع‌آوری‌شده را بررسی کرده و تحلیل‌گران SOC را از حضور مخفیانه مهاجمان در شبکه مطلع می‌سازد.
با ترکیب چندین مکانیزم برای شناسایی تهدیدات پیچیده، PT NAD دیدی جامع از شبکه شرکت ارائه داده، اتصالات مشکوک و ناهنجاری‌های شبکه را شناسایی کرده و به رعایت الزامات امنیت اطلاعات کمک می‌کند.

global.ptsecurity.com
info@ptsecurity.com

positive technologies

PT Industrial Security Incident Manager

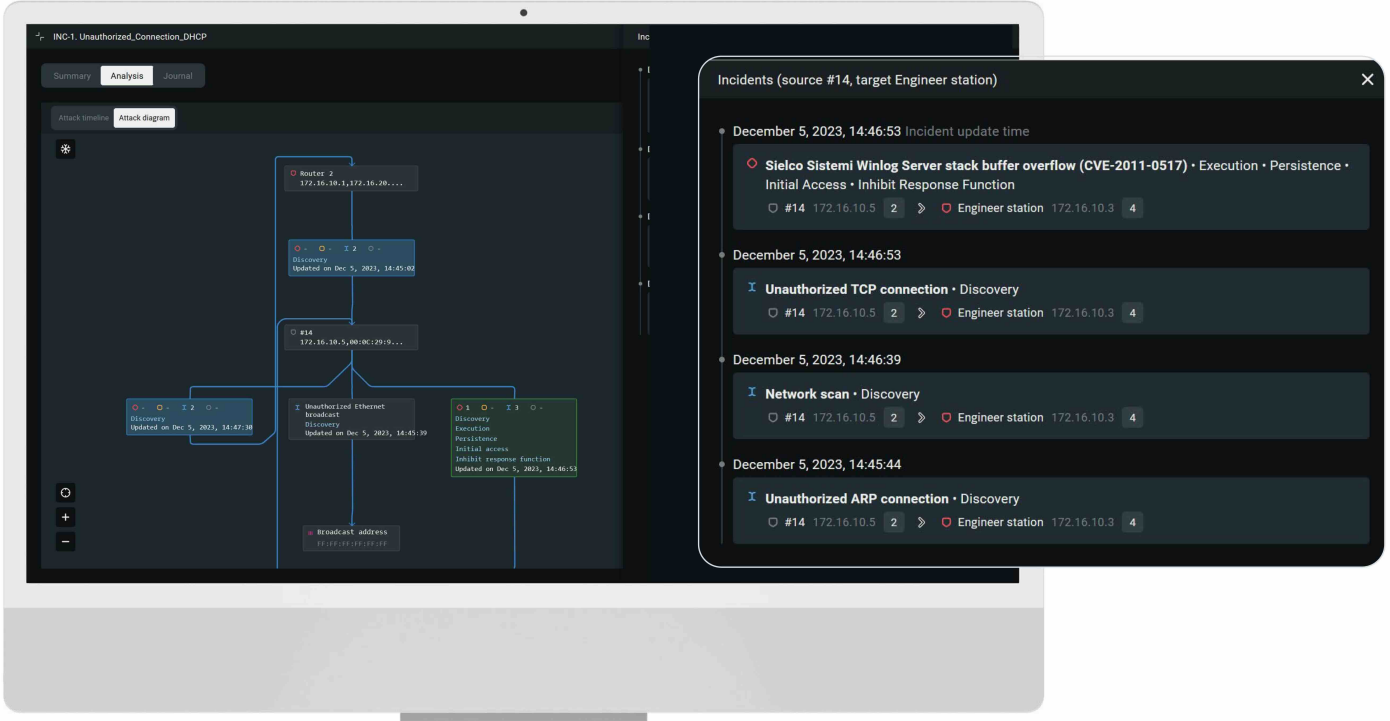
PT ISIM امنیت شبکه OT را تضمین می‌کند و امکانات نظارتی برای زیرساخت‌های OT و IIoT در تأسیسات صنعتی و ساختمانی فراهم می‌سازد.

PT Industrial Security Incident Manager

PT ISIM یک سیستم تحلیل عمیق ترافیک برای شبکه‌های OT است که بازرسی دقیق ترافیک را برای پروتکل‌های عمومی و خاص شبکه صنعتی انجام می‌دهد. با نظارت بر ترافیک در محیط خارجی و داخل شبکه کنترل صنعتی، PT ISIM عملیات مخربی را که ممکن است برای فرآیندهای عملیاتی خطرناک باشند شناسایی کرده و اطلاعات ضروری برای بررسی رخدادهای امنیتی را فراهم می‌کند. PT ISIM به پایگاه داده اختصاصی خود از تهدیدات سایبری صنعتی، یعنی شاخص‌های تهدید امنیت صنعتی PT (PT ISTI) متکی است. این دانش تخصصی از پیش آماده، امکان شروع نظارت و شناسایی تهدیدات را بدون نیاز به تنظیمات زمان‌بر یک سنسور شبکه فراهم می‌سازد.

پیشنهاد ارزش

- PT ISIM بیش از ۱۳۰ پروتکل شبکه را شناسایی می‌کند و می‌تواند در هر زیرساخت صنعتی یا محیط IIoT، مانند سیستم‌های مدیریت ساختمان و تجهیزات بهداشتی مبتنی بر DICOM استفاده شود.
- PT ISIM تمامی ارتباطات داخل شبکه OT را کنترل کرده و ناهنجاری‌ها، تهدیدات، نقص‌های پیکربندی OT و حتی دستورات کنترلی خطرناک را شناسایی می‌کند؛ این امر برای هر شرکت صنعتی حیاتی است.
- PT ISIM دارایی‌های پنهان IT را در زیرساخت OT آشکار می‌سازد. درک واضح ساختار شبکه OT برای اطمینان از عملکرد قوی OT ضروری است.



موارد استفاده

فهرست‌برداری از شبکه OT و شناسایی دارایی‌های جدید

شناسایی ناهنجاری ها، دستورات مخرب و خطرناک

بهره‌برداری از آسیب پذیری‌ها و سایر تکنیک‌های مخرب

تطبیق با الزامات مقرراتی

شناسایی بدافزار و صدور فایل‌های مشکوک برای تحلیل آماری و رفتاری کامل در PT Sandbox

PT ISIM به تمامی خدمات فنی و بخش‌هایی که از مشاهده‌پذیری و پیش‌بینی زیرساخت OT و نظارت امنیتی بهره می‌برند، کمک می‌کند:

- پرسنل امنیتی : می‌توانند زیرساخت‌های حساس OT را در برابر تهدیدات سایبری واقعی ایمن کنند.
- پرسنل نگهداری OT : می‌توانند مقاومت زیرساخت OT و عملیات بدون وقفه فرآیندهای حساس را تضمین کنند.
- مدیران OT و پرسنل اعزام : می‌توانند کارخانه را با خیال راحت راه‌اندازی کرده و با کاهش کافی ریسک‌های سایبری به KPI تولید دست یابند

صنایع

- سیستم‌های کنترل صنعتی (ICS)
- سیستم‌های زیرساخت حیاتی
- سیستم‌های مدیریت ساختمان (BMS)
- سیستم‌های کنترل حمل‌ونقل ریلی
- شرکت‌های صنعتی پراکنده
- تجهیزات و سیستم‌های بهداشتی سازگار با DICOM

اجزا

سنسورهای PT ISIM View - سنسورهای شبکه

اجزای اصلی سیستم که ترافیک شبکه OT را ضبط و ذخیره می‌کنند. سنسورها در داخل زیرساخت OT مستقر شده و به شبکه OT متصل می‌شوند که شامل PLCها، سرورهای SCADA، و ایستگاه‌های کاری مهندسی و اپراتوری است.

مرکز PT ISIM Overview - کنسول مدیریت

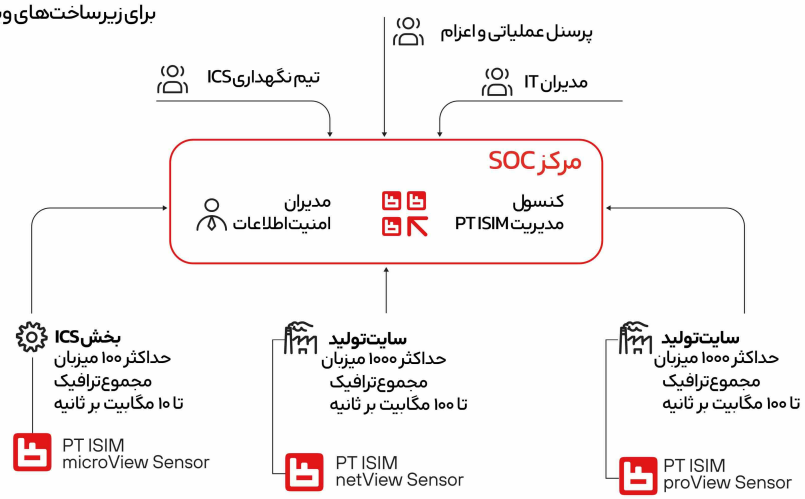
رابط یکپارچه برای نظارت، مدیریت و به روزرسانی مرکزی چندین سنسور ISIM View متصل. معمولاً در سطح SOC یا مرکز داده مستقر می‌شود. مرکز Overview رخدادها را از تمامی سنسورهای متصل دریافت می‌کند.

نحوه کار

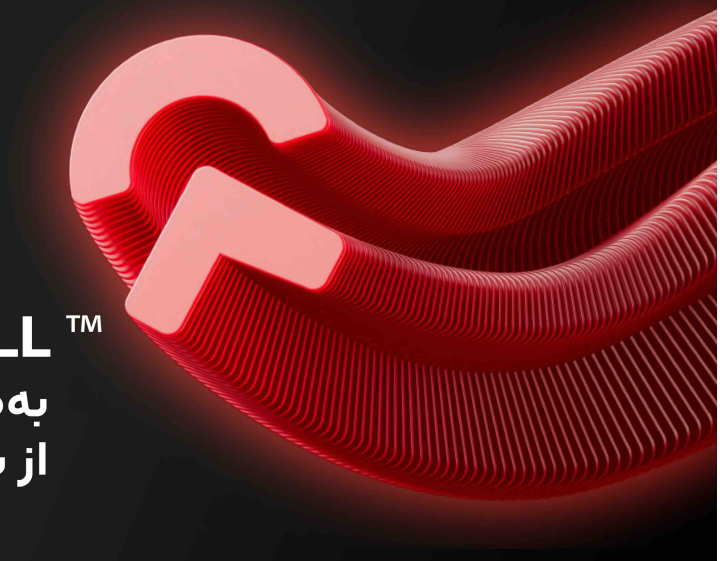
PT ISIM یک کپی از ترافیک شبکه OT را از پورت SPAN یک سوئیچ صنعتی دریافت کرده و تمامی بسته‌ها و ارتباطات ضبط‌شده را تحلیل می‌کند. این سیستم توپولوژی شبکه را با نمایش تمامی میزبان‌ها و ارتباطات شبکه تجسم می‌کند. در صورت شناسایی عملیات مخرب یا ناهنجاری، PT ISIM یک هشدار ایجاد کرده و ترافیک خام را برای بررسی‌های بعدی ذخیره می‌کند. سپس می‌تواند سیستم SIEM در SOC، مانند MaxPatrol SIEM، را مطلع سازد.

8000+

۸۰۰۰ قانون و شاخص تهدید صنعتی به‌صورت از پیش آماده موجود و قابل استفاده برای زیرساخت‌های ویندوز و لینوکس هستند



positive technologies



PT APPLICATION FIREWALL ™

به‌صورت هوشمند
از برنامه‌های تجاری خود محافظت کنید

"Positive Technologies به عنوان بزرگترین اپراتور امنیت سایبری روسیه فعالیت میکند و بسیاری از زیرساختهای مهم روسیه در بخش دولتی و بانکی و مخابراتی از محصولات آن استفاده میکنند."

(گزارش Gartner Magic Quadrant برای فایروال‌های برنامه‌های وب ۲۰۱۵)

تقریباً هر شرکت مدرن از صدها برنامه وب، موبایل یا ERP برای پیشبرد عملیات خود استفاده می‌کند. اما با افزایش تعداد این برنامه‌ها، تعداد آسیب‌پذیری‌های امنیتی موجود در آن‌ها نیز افزایش می‌یابد که می‌توانند برای آسیب رساندن به کسب‌وکار شما بهره‌برداری شوند. گزارش Verizon Data Breach Investigation Report (DBIR) ۲۰۱۴ نشان می‌دهد که در سال گذشته ۳۵٪ از نفوذهای امنیتی شامل حملات علیه برنامه‌های وب بوده که نسبت به سال ۲۰۱۲، ۱۴٪ افزایش داشته است. همچنین، حملات به برنامه‌های وب اصلی‌ترین عامل نقض داده‌ها بوده‌اند، و پس از آن جاسوسی سایبری، نفوذ به سیستم‌های POS و سوء استفاده داخلی قرار دارند.

+ چرا این مهاجمان موفق هستند؟ واقعیت این است که اکثر تهدیدات امنیتی برنامه‌ها ناشی از اشتباهات توسعه‌دهندگان است که با اسکنرهای امنیتی سنتی، IDS یا فایروال‌ها قابل حل نیستند:

+ مهاجمان اغلب از آسیب‌پذیری‌های روز صفر بهره‌برداری می‌کنند، که تحلیل بر پایه امضا را منسوخ و نیاز به راهکارهای انطباقی، خودآموز و تحلیل رفتاری را تأیید می‌کند.

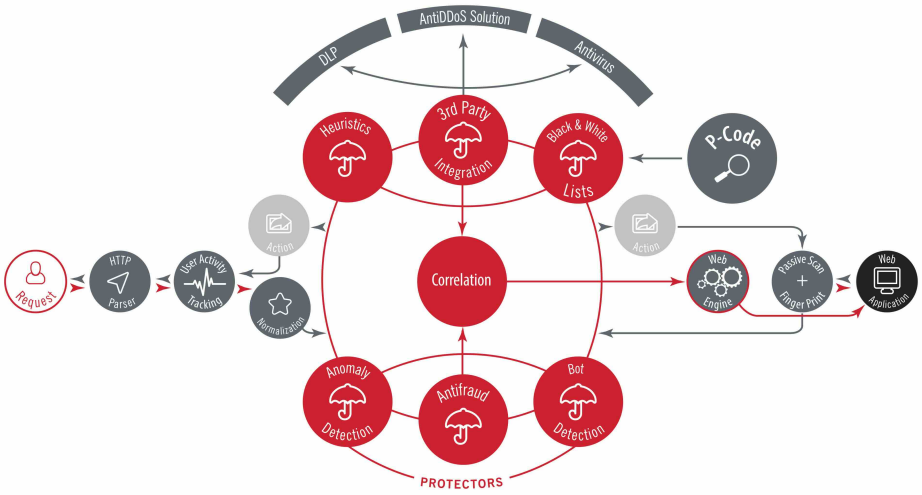
+ برنامه‌های شرکتی مدرن از زبان‌ها، پروتکل‌ها و فناوری‌های مختلفی استفاده می‌کنند و شامل راهکارهای سفارشی و کدهای شخص ثالث هستند. حفاظت از این برنامه‌ها نیاز به تحلیل دقیق ساختار برنامه، الگوهای تعامل کاربران و بستر استفاده دارد.

+ فایروال‌های مدرن با هزاران حادثه مشکوک مواجه می‌شوند. متخصصان امنیتی زمان کافی برای بررسی دستی همه این حوادث به منظور شناسایی تهدیدات واقعی را ندارند. نیاز مبرم به مرتب‌سازی، رتبه‌بندی و تجسم هوشمند رویدادهای امنیتی به‌صورت خودکار وجود دارد.

+ حتی آسیب‌پذیری‌های شناخته‌شده نیز نمی‌توانند بلافاصله اصلاح شوند؛ رفع آسیب‌پذیری‌های سیستم‌های ERP یا بانکداری الکترونیکی ممکن است ماه‌ها به طول بینجامد. یک سیستم امنیت برنامه باید دارای مکانیزمی برای کاهش اثرات نقص‌ها در حین رفع کد توسط توسعه‌دهندگان باشد.

+ Secure SDL می‌تواند به طور چشم‌گیری هزینه اشتباهات را کاهش دهد، مشروط بر اینکه این اشتباهات در مراحل اولیه کدنویسی اصلاح شوند، اما یافتن راه‌حل‌های خودکار موثر برای تحلیل کد کار دشواری است.

PT Application Firewall™: Modules and Engines



مزایای کلیدی

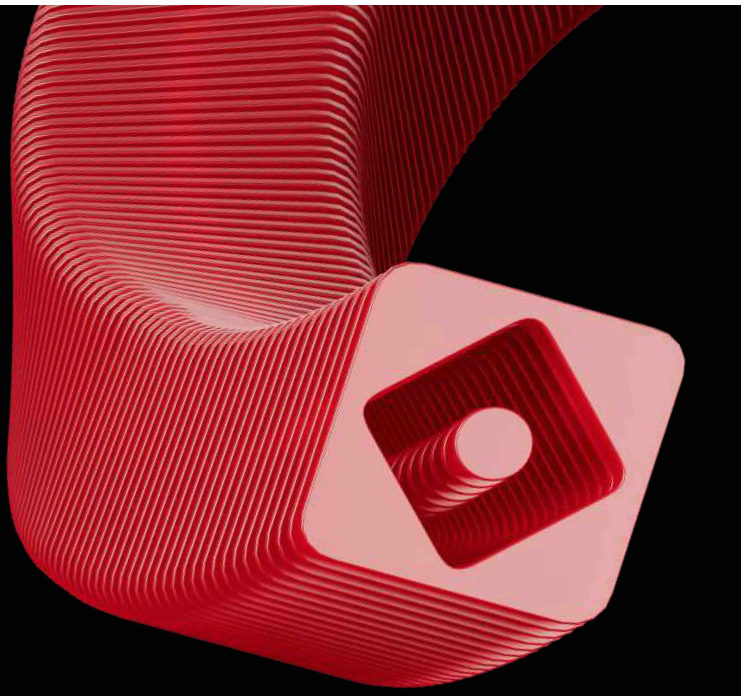
مکانیزم‌های حفاظت برتر – تطبیق سریع و پیوسته با سیستم‌های شما
به جای استفاده از روش کلاسیک مبتنی بر امضا، فایروال برنامه کاربردی PT™ ترافیک شبکه، لاگ‌ها و فعالیت کاربران را تحلیل کرده و یک مدل آماری در لحظه از عملکرد عادی برنامه ایجاد می‌کند؛ این مدل برای شناسایی رفتار غیرعادی سیستم استفاده می‌شود. به همراه سایر مکانیزم‌های حفاظتی، این روش تضمین می‌کند که ۸۰٪ از حملات روز صفر بدون نیاز به تنظیمات خاص مسدود می‌شوند.

کاهش تلاش‌های عملیاتی و تمرکز بر تهدیدات اصلی
PT AF™ تلاش‌های نامرتبط برای حمله را فیلتر کرده، حوادث مشابه را گروه‌بندی کرده و زنجیره‌های حمله را شناسایی می‌کند – از جاسوسی تا سرقت داده یا ایجاد درب پشتی. به جای دریافت هزاران پیام بالقوه تهدید، متخصصان امنیت اطلاعات فقط ده‌ها پیام مهم دریافت می‌کنند.

P-Code: مسدودسازی آنی
تکنیک وصله مجازی ما به شما امکان می‌دهد تا از برنامه محافظت کنید، حتی قبل از اینکه کد ناامن اصلاح شود. اما اکثر WAF‌ها برای ایجاد هر وصله مجازی به کار دستی نیاز دارند. فناوری منحصر به فرد PT برای تحلیل کد منبع با مکانیزم تولید اکسپلویت (P-Code)، شناسایی خودکار آسیب‌پذیری‌ها و ایجاد وصله مجازی برای فایروال برنامه کاربردی PT™ را فراهم می‌کند. همین ماژول P-Code اطلاعات دقیقی درباره کد نادرست به توسعه‌دهندگان ارائه می‌دهد و هزینه‌های اصلاح و تست را به شدت کاهش می‌دهد.

حذف بای‌پس‌های امنیتی
PT AF™ داده‌ها را با توجه به پشته فناوری سرور محافظت‌شده پردازش کرده و پروتکل‌های JSON، XML و دیگر پروتکل‌های معمول در پورتال‌ها و برنامه‌های موبایل مدرن را تحلیل می‌کند. این ویژگی از بیشتر روش‌های دور زدن فایروال مانند HPP، HPC و دستکاری افعال محافظت می‌کند.

positive technologies



PT SANDBOX

برای شناسایی حملات بدافزار پیچیده و هدفمند

PT SANDBOX راهکاری قدرتمند برای تحلیل و شناسایی بدافزارهای پیشرفته و حملات هدفمند در شبکه‌های سازمانی است. این سیستم با بررسی دقیق فعالیت های مشکوک و تحلیل پویا، به شناسایی و مقابله با تهدیدات ناشناخته کمک می‌کند.

PT SANDBOX

تهدیدات را در بخش‌های زیر شناسایی می‌کند:

- ایمیل
- ذخیره‌سازی فایل
- ترافیک وب کاربران
- ترافیک شبکه سازمانی
- پورتال‌های وب که در آن‌ها فایل‌ها به صورت دستی اسکن می‌شوند
- سیستم‌های سازمانی، از جمله سیستم‌های مدیریت اسناد

PT EXPERT SECURITY CENTER (PT ESC)

مرکز تخصصی امنیتی

PT ESC مرکز تخصصی امنیتی شرکت POSITIVE TECHNOLOGIES است.
متخصصان PT ESC حوادث امنیتی را در شرکت های بزرگ بررسی می‌کنند و به صورت مداوم فعالیت گروه‌های هکری را پایش می‌کنند. اطلاعات تهدیدی که در طی این تحقیقات به دست می‌آید، به سرعت به PT SANDBOX انتقال داده می‌شود.

نیمی از تمامی حملات سایبری با استفاده از بدافزارهایی انجام می‌شود که به صورت فایل‌ها و لینک‌های معمولی مخفی شده‌اند تا بتوانند از نرم‌افزارهای آنتی‌ویروس، فایروال‌ها، IDSها، IPSها، و درگاه‌های ایمیل و وب عبور کنند. طبق گزارش POSITIVE TECHNOLOGIES هفتاد درصد از شرکت‌ها با فعالیت بدافزاری مواجه شده‌اند که توسط ابزارهای حفاظتی پایه نادیده گرفته شده است.

راه حل:

PT SANDBOX یک سندباکس شبکه‌ای مبتنی بر ریسک است که تهدیدات سایبری پیچیده را حتی در صورت پنهان شدن مهاجم در شبکه شناسایی می‌کند. PT SANDBOX از حملات بدافزارهای هدفمند و گسترده و تهدیدات روز صفر محافظت می‌کند و هر دو نوع بدافزارهای رایج (نظیر بدافزارهای رمزگذاری، باج‌افزارها، جاسوس‌افزارها، ابزارهای کنترل از راه دور و لودرها) و ابزارهای پیشرفته هکرها مانند روتکیت‌ها و بوتکیت ها را شناسایی می‌کند.

هر شیء در PT SANDBOX با استفاده از فناوری‌های یادگیری ماشین، روش‌های استاتیک و پویا، و قوانین منحصر به فرد PT EXPERT SECURITY CENTER (PT ESC) تحلیل می‌شود و توسط چندین موتور آنتی ویروس اسکن می‌شود.

دانش تخصصی PT ESC در مورد آخرین تهدیدات در کمتر از 2.5 ساعت به PT SANDBOX اضافه می‌شود. این ویژگی به شما امکان می‌دهد از شرکت خود در برابر حملات سایبری که مهاجمین سعی دارند از یک آسیب پذیری روز صفر (که هنوز هیچ پچی برای آن منتشر نشده) سوءاستفاده کنند، محافظت کنید.

مزایا:

سازگاری با ویژگی‌های خاص کسب‌وکار شما

یکی از ویژگی‌های کلیدی PT SANDBOX این است که می‌تواند حفاظت را با زیرساخت‌های IT و فرآیندهای کسب‌وکار خاص شرکت‌ها سازگار کند. برای این منظور، مکانیزم‌های زیر در نظر گرفته شده است:

- **پشتیبانی از محیط‌های مجازی برای تحلیل** (ویندوز در نسخه‌های مختلف و سیستم‌عامل‌های روسی مانند ASTRA LINUX و RED OS). PT SANDBOX به‌طور کامل تاکتیک‌ها و تکنیک‌های MITRE ATT&CK را که مهاجمین ممکن است برای حمله به این سیستم‌عامل‌ها استفاده کنند، پوشش می‌دهد.
- **شخصی‌سازی انعطاف‌پذیر محیط‌های مجازی.** شما می‌توانید با افزودن نرم‌افزارها یا نسخه‌های نرم‌افزاری خاصی که در شرکت شما استفاده می‌شود و می‌تواند به عنوان نقطه ورود برای مهاجمین عمل کند، محیط‌های مجازی خود را ارتقاء دهید.
- **شناسایی تهدیدات در هر دو بخش شرکتی و صنعتی.** نسخه صنعتی PT SANDBOX اشیاء را در محیط مجازی صنعتی تحلیل کرده و بدافزارهای خاصی که به اجزای ICS حمله می‌کنند را شناسایی می‌کند.
- **HONEYPOTهایی که بدافزارها را تحریک به فعالیت می‌کنند و مهاجم را آشکار می‌سازند.** فایل‌های ایجاد شده به عنوان HONEYPOT شامل اطلاعات جعلی مانند اعتبارنامه‌های تقلبی، فایل‌های پیکربندی یا دیگر داده‌های ظاهراً ارزشمند هستند. فرآیندهای HONEYPOT فعالیت‌های سیستم‌های بانکی، نرم‌افزارهای توسعه و فعالیت کاربران را تقلید می‌کنند.
PT SANDBOX تلاش‌های نفوذ یا سرقت از HONEYPOTها را شناسایی می‌کند. بیشتر HONEYPOTهای ویندوز و لینوکس آماده استفاده هستند؛ PT ESC همچنین می‌تواند HONEYPOTهای سفارشی برای تقلید از سیستم‌های حساس کسب‌وکار شما ایجاد کند.

PT SANDBOX را در شرکت خود آزمایش کنید

برای ارزیابی کارایی PT SANDBOX در زیرساخت خود، برای یک پروژه آزمایشی ثبت‌نام کنید.

سایر قابلیت ها

عملکرد بالا

مدیریت انعطاف‌پذیر پردازش فایل‌ها و لینک‌ها و مقیاس‌پذیری افقی نامحدود PT SANDBOX عملکرد بالایی را تحت هر بار کاری تضمین می‌کند.

حالت‌های نظارت و مسدودسازی

PT SANDBOX تهدیدات را نظارت کرده و به صورت خودکار بدافزارها را مسدود می‌کند.

ادغام آسان

PT SANDBOX از گزینه‌های مختلف آماده برای ادغام پشتیبانی می‌کند و دارای API انعطاف‌پذیری است که به شما امکان می‌دهد محصول را در هر پیکربندی از سیستم‌های اطلاعاتی استفاده کنید.

پشتیبانی از اکوسیستم POSITIVE TECHNOLOGIES

PT SANDBOX به راحتی می‌تواند با MAXPATROL SIEM، PT APPLICATION FIREWALL، PT ISIM، PT NETWORK ATTACK DISCOVERY، و PT XDR ادغام شود.

گزینه نصب داخلی

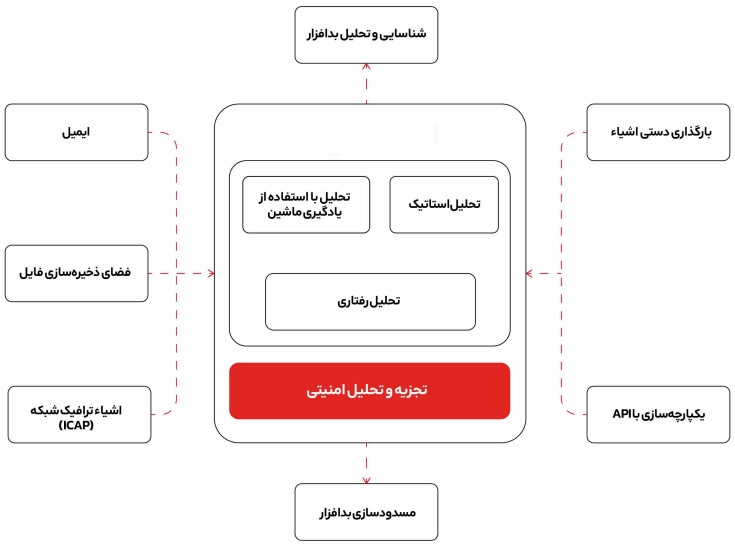
فایل‌های محرمانه در هنگام بررسی از محدوده شرکت خارج نمی‌شوند.

شناسایی تهدیدات از دست رفته قبلی

PT SANDBOX پس از به‌روزرسانی پایگاه دانش، به‌طور منظم تحلیل‌های گذشته‌نگر از فایل‌های قبلاً بررسی‌شده انجام می‌دهد. این امکان به شما داده می‌شود که تهدیدات پنهان در زیرساخت را به سرعت شناسایی کرده و پیش از رسیدن مجرمان به هدف خود به حملات واکنش نشان دهید.

شناسایی تهدیدات در فایل‌ها و ترافیک

PT SANDBOX فایل‌ها را بررسی کرده، ترافیکی که در طی تحلیل فایل ایجاد شده را تجزیه و تحلیل می‌کند و فعالیت‌های مخرب پنهان شده توسط رمزنگاری TLS را شناسایی می‌کند. این روش به‌طور قابل‌توجهی کارایی شناسایی حملات را حتی در ترافیک رمزگذاری‌شده بهبود می‌بخشد.



نحوه کار PT SANDBOX

درباره Positive Technologies

Positive Technologies یک پیشرو در صنعت امنیت سایبری نتیجه‌محور و یکی از ارائه‌دهندگان بزرگ جهانی در راهکارهای امنیت اطلاعات است. مأموریت ما محافظت از کسب‌وکارها و صنایع مختلف در برابر حملات سایبری و آسیب‌های غیرقابل‌تحمل است.

global.ptsecurity.com
info@ptsecurity.com

positive technologies

Application Inspector

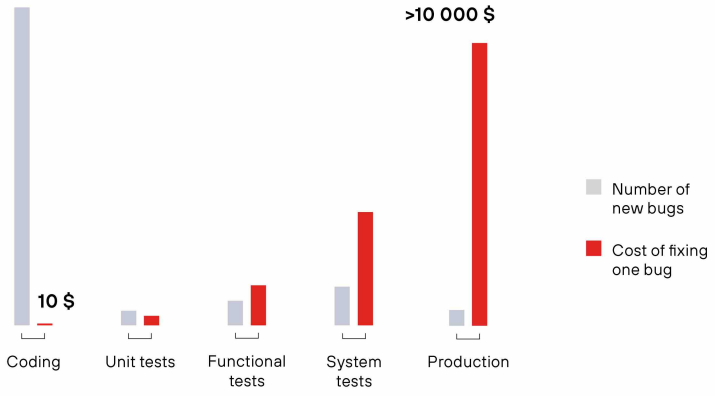
تحلیل کد منبع.
شناسایی دقیق آسیب‌پذیری‌ها.
یکپارچه‌سازی با فرآیندهای توسعه فعلی.

یک ابزار برای شناسایی آسیب‌پذیری‌ها هم در کد منبع و هم در برنامه در حال اجرا است و با حذف آن‌ها در مراحل اولیه، از فرآیند توسعه امن پشتیبانی می‌کند.

برنامه‌های وب همچنان یک هدف محبوب برای مهاجمان باقی مانده‌اند. تحقیقات ما نشان می‌دهد که از هر پنج حمله، یکی به منابع وب سازمان‌ها هدف‌گیری شده است، که اغلب این حملات به نهادهای دولتی و مالی، خدمات آنلاین، مراکز علمی و آموزشی، و شرکت‌های IT انجام می‌شود.

مهاجمان از آسیب‌پذیری‌های موجود بهره‌برداری می‌کنند: به‌طور میانگین، هر برنامه شامل بیش از دو ده آسیب‌پذیری است که یک‌پنجم آن‌ها حیاتی محسوب می‌شود. اگر مهاجمان از این آسیب‌پذیری‌ها استفاده کنند، شرکت ممکن است با ریسک‌های مالی و اعتباری جدی مواجه شود: سرقت داده‌های مهم، نفوذ به زیرساخت‌ها، زمان‌های توقف، یا حتی خاموشی کامل سیستم‌های اطلاعاتی.

بیشتر آسیب‌پذیری‌ها در کد منبع وجود دارند و بهتر است که در مراحل اولیه توسعه برنامه‌ها حذف شوند. این روش بسیار موثرتر از حذف آسیب‌پذیری‌ها در مرحله عملیاتی است.



هزینه رفع نقص در مراحل مختلف چرخه عمر برنامه

مزایای PT Application Inspector

ترکیب چهار نوع تحلیل: PT Application Inspector شامل تحلیل آماری (SAST)، پویا (DAST)، تعاملی (IAST)، و تحلیل اجزای جانبی (SCA) است. این ترکیب بیشترین تعداد آسیب‌پذیری‌ها را پوشش می‌دهد و سیستم فیلترگذاری انعطاف‌پذیر امکان اولویت‌بندی آسیب‌پذیری‌ها را بر اساس میزان بحرانی بودن فراهم می‌کند.

تولید اکسپلویت‌های آزمایشی: این ابزار اکسپلویت‌های آزمایشی برای بررسی امکان بهره‌برداری از آسیب‌پذیری تولید می‌کند. با در نظر گرفتن قواعد گرامری و آزمون فازینگ در محیط اجراء، هزینه‌های تیم‌های توسعه برای تأیید آسیب پذیری‌ها را کاهش می‌دهد.

سیستم لایسنس‌دهی راحت و شفاف: سیستم لایسنس‌دهی به‌گونه‌ای طراحی شده که امکان مشارکت کل تیم را در تعداد نامحدودی از پروژه‌ها فراهم می‌سازد.

نسخه آزمایشی رایگان

آسیب‌پذیری‌های موجود در کد خود را بررسی کنید – پروژه آزمایشی رایگان PT Application Inspector را سفارش دهید.

PT Application Inspector به‌طور موثر در فرآیندهای توسعه یکپارچه می‌شود. این ابزار از یکپارچگی با GitLab CI، TeamCity، Jenkins، و Azure** پشتیبانی می‌کند و دارای مدل کنترل دسترسی مبتنی بر نقش و پلاگین‌های آماده برای اتصال به سیستم‌های ساخت و تحویل برنامه، باگ ترکرها، و محیط‌های توسعه (IDE) است.

Supported languages:
Java, PHP, C#, Visual Basic .NET, JavaScript, TypeScript, Python, Kotlin, Go, C/C++, Objective-C, Swift, SQL (T-SQL, PL/SQL, MySQL)

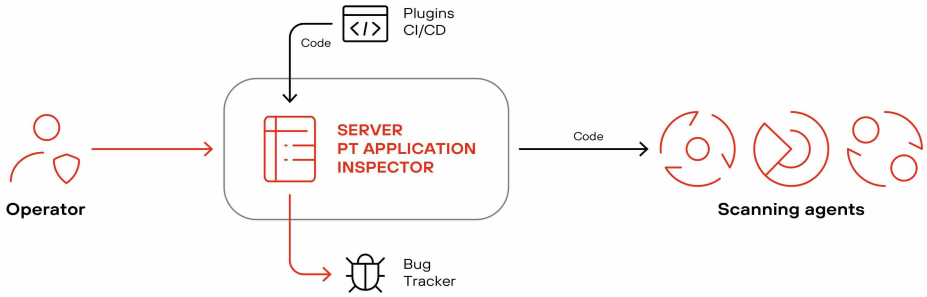
Deployment: Linux + Docker containers + SSO (SAML, OpenID Connect, LDAP)

CI/CD integration: Jenkins, TeamCity, GitLab CI (CLI), Azure

IDE integration: JetBrains, Visual Studio Code

Bug tracker integration: Jira

API: REST API (Swagger)



طرح یکپارچه‌سازی PT Application Inspector در فرآیند توسعه موجود

How it works

PT Application Inspector تنها تحلیلگر کد منبع در بازار روسیه است که ابزارهای کاربردی برای تأیید خودکار آسیب‌پذیری‌ها ارائه می‌دهد، که به‌طور قابل توجهی در زمان صرفه‌جویی کرده و تعامل بین متخصصان امنیت اطلاعات و توسعه‌دهندگان را تسهیل می‌کند.

- Abstract interpretation
- Pattern matching
- Configuration compliance
- Analysis of third-party components
- Dynamic analysis
- Automatic check using exploits

About Positive Technologies

ptsecurity.com
pt@ptsecurity.com

Positive Technologies یک ارائه‌دهنده پیشرو جهانی در راهکارهای امنیت اطلاعات است. بیش از ۳٬۳۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند. در طول ۲۰ سال گذشته، مأموریت ما مقابله با اقدامات هکرها قبل از وارد آمدن آسیب غیرقابل‌قبول به کسب‌وکارها یا صنایع مختلف بوده است.

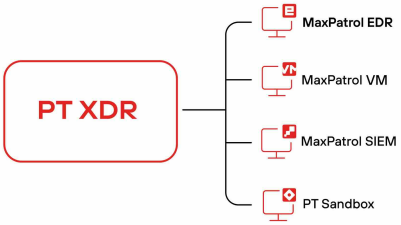
Positive Technologies اولین و تنها شرکت امنیت سایبری در روسیه است که در بورس مسکو (MOEX: POSI) عمومی شده است. ما را در شبکه‌های اجتماعی (Habr، Twitter) و بخش اخبار در ptsecurity.com دنبال کنید.

positive technologies

PT Extended Detection and Response

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

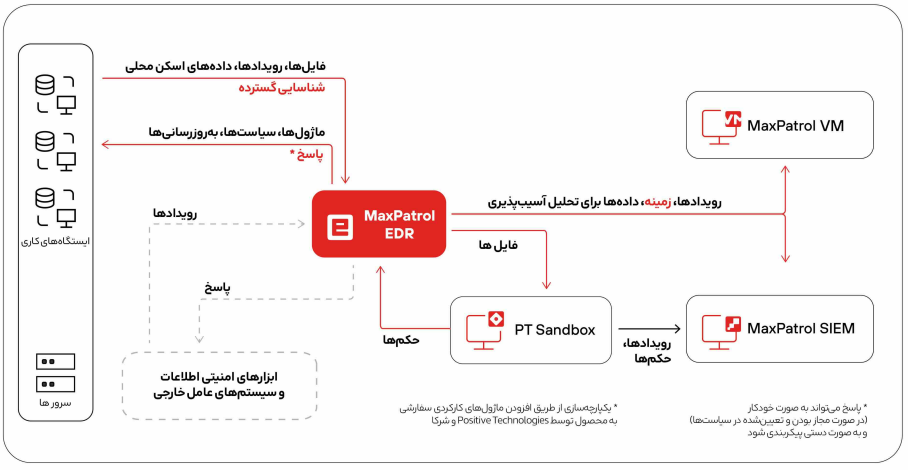
PT Extended Detection and Response (PT XDR) برای مدیریت جمع‌آوری اطلاعات، شناسایی حملات پیشرفته، و همچنین بررسی و پاسخ سریع به رخدادها طراحی شده است. PT XDR داده‌ها را از ایستگاه‌های کاری و سرورها جمع آوری و تقویت می‌کند، تحلیل استاتیک و داینامیک تهدیدات را هم در دستگاه‌ها و هم در سیستم‌های خارجی انجام 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).

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
- 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.



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، جریان 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.

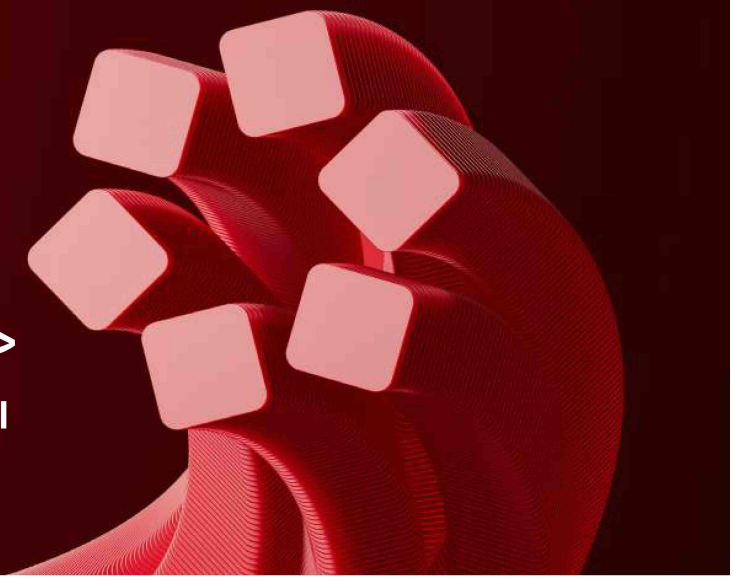
کاهش تعداد هشدارهای کاذب
بر اساس زمینه خاص و پردازش رویدادها از منابع مختلف، PT XDR تعیین می‌کند که کدام رویدادها کاذب هستند و کدام نه. این کار نیاز به تحلیل و بررسی دستی هر رویداد توسط تحلیل‌گر SOC را از بین می‌برد.

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.

global.ptsecurity.com
info@ptsecurity.com

positive technologies



خانواده محصولات مکس پاترول

ارایه شده از بزرگترین اپراتور امنیت سایبری روسیه

MaxPatrol O2

محصولات Positive Technologies را گرد هم می‌آورد که به عنوان حسگر عمل می‌کنند، دانش را تبادل می‌کنند و با حداقل دخالت انسانی، حفاظت کاملی از سیستم‌های IT ارائه می‌دهند.

90%

از شرکت‌ها با کمبود متخصصان امنیت اطلاعات مواجه‌اند

MaxPatrol SIEM

محصولی کاربردی با قابلیت تجمیع رویدادهای تمامی تجهیزات شبکه سازمان شما که با کمک بانک دانش اختصاصی تمامی تهدیدات و حملات را شناسایی می کند و متخصصین امنیت سایبری را یاری میدهد.

71%

از رخدادهای غیرقابل‌تحمل می‌توانند توسط مهاجمان در عرض یک ماه اجرا شوند.

MaxPatrol VM

قابلیت شناسایی آسیب پذیریهای رایج بر روی کلیه تجهیزات سازمان و پیگیری یک آسیب پذیری یا زمان رفع کامل ترکیبی است که شرکت PT در یک محصول گرداوری کرده است ترکیبی از VA+VM با امکان HCC

100%

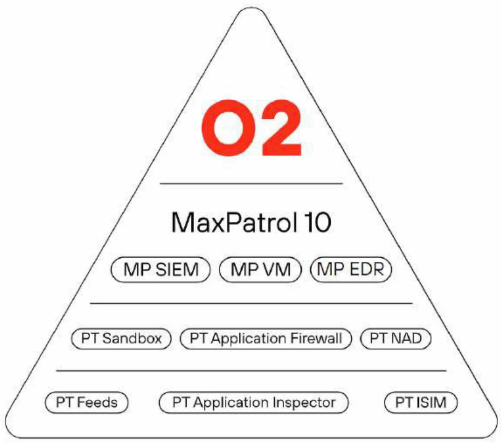
از زیرساخت‌ها می‌توانند به‌طور کامل توسط مهاجمان داخلی تصرف شوند.

MaxPatrol EDR

راهکار مستقر در سیستمهای نهایی شبکه سازمان که در تجمیع رویدادها و شناسایی رفتارهای مشکوک موثر است همچنین قابلیت کنترل موثر تهدیدات را به کارشناسان امنیت سایبری ارایه میدهد.

93%

از محیط‌های شبکه می‌توانند توسط مهاجمان عبور شده و به دسترسی شبکه محلی منجر شوند.



positive technologies

MaxPatrol O2

هدایت خودکار برای امنیت سایبری مبتنی بر نتایج

MaxPatrol O2 مهاجمان را شناسایی می‌کند، دارایی‌های نقض‌شده را تعیین می‌کند، سناریوی حمله را با توجه به رخدادهای غیرقابل‌تحمل مخصوص شرکت پیش‌بینی کرده و قبل از وارد آمدن آسیب جبران‌ناپذیر، حمله را متوقف می‌سازد.

مدل‌سازی اقدامات احتمالی مهاجمان:

پیش‌بینی رخدادهای غیرقابل‌تحملی که فعالیت مشکوک ممکن است منجر به آن‌ها شود و تعداد مراحل باقی‌مانده تا تحقق ریسک‌ها.

شناسایی زنجیره‌های فعالیت هکری:

تحلیل داده‌های حسگرهای Positive Technologies در محصول متاپرداکت و تفکیک منابع مهاجم، هدف‌گیری شده و تصرف‌شده. همبستگی منابع برای ساخت زنجیره‌های فعالیت با استفاده از دانش تاکتیک‌ها، تکنیک‌ها و پروسه‌های مهاجمان. هر زنجیره شامل تجسم مسیر مهاجمان و پیش‌بینی حرکت بعدی آن‌هاست.

خودکارسازی تحقیقات:

استفاده از داده‌های حسگرهای Positive Technologies برای ساختن یک زمینه کامل از حمله و انجام تحقیقات.

ارزیابی شدت تهدید:

MaxPatrol O2 منابع تصرف‌شده را مشاهده و نزدیکی به رخداد غیرقابل‌تحمل را ارزیابی می‌کند. پس از دریافت این اطلاعات، سیستم وضعیت زنجیره حمله را به "نیازمند توجه" ارتقاء می‌دهد و سپس مهاجم را متوقف کرده یا از اپراتور می‌خواهد تصمیم بگیرد.

متوقف‌سازی مهاجم:

با در نظر گرفتن ریسک‌های فرآیندهای تجاری، بهترین سناریوی پاسخ را پیشنهاد می‌دهد. این سناریو می‌تواند به صورت خودکار یا دستی در صورت نیاز به تنظیمات اعمال شود.

90%

از شرکت‌ها با کمبود متخصصان امنیت اطلاعات مواجه‌اند

71%

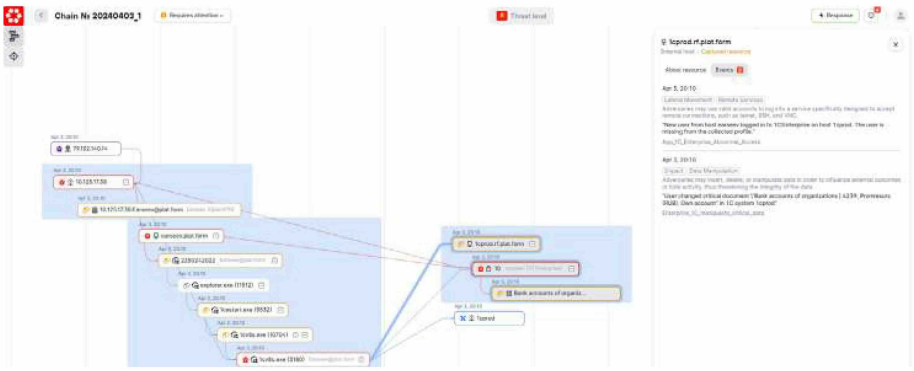
از رخدادهای غیرقابل‌تحمل می‌توانند توسط مهاجمان در عرض یک ماه اجرا شوند.

100%

از زیرساخت‌ها می‌توانند به‌طور کامل توسط مهاجمان داخلی تصرف شوند.

93%

از محیط‌های شبکه می‌توانند توسط مهاجمان عبور شده و به دسترسی شبکه محلی منجر شوند.



بیشتر درباره امنیت
سایبری خودکار بیاموزید

محصولات Positive Technologies را گرد هم می‌آورد که به عنوان حسگر عمل می‌کنند، دانش را تبادل می‌کنند و با حداقل دخالت انسانی، حفاظت کاملی از سیستم‌های IT ارائه می‌دهند.

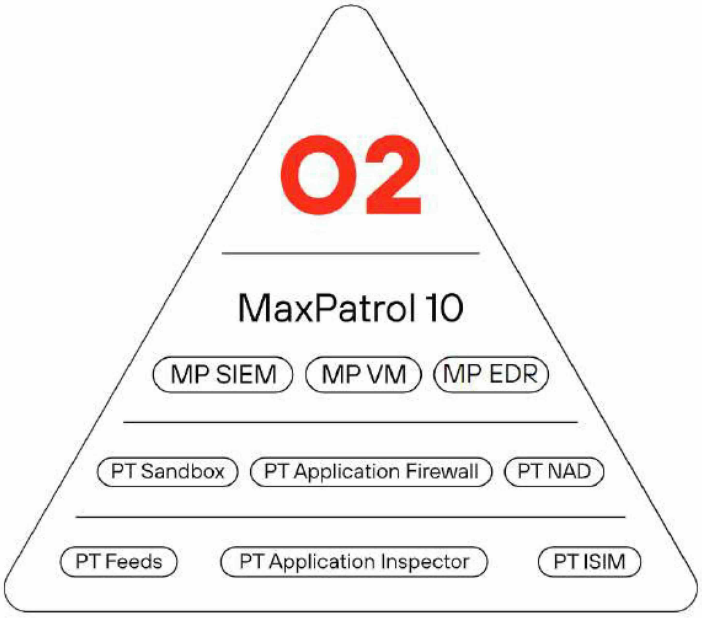
اکوسیستم Positive Technologies

رخدادهای غیرقابل‌تحمل برای کسب‌وکار را حذف می‌کند.

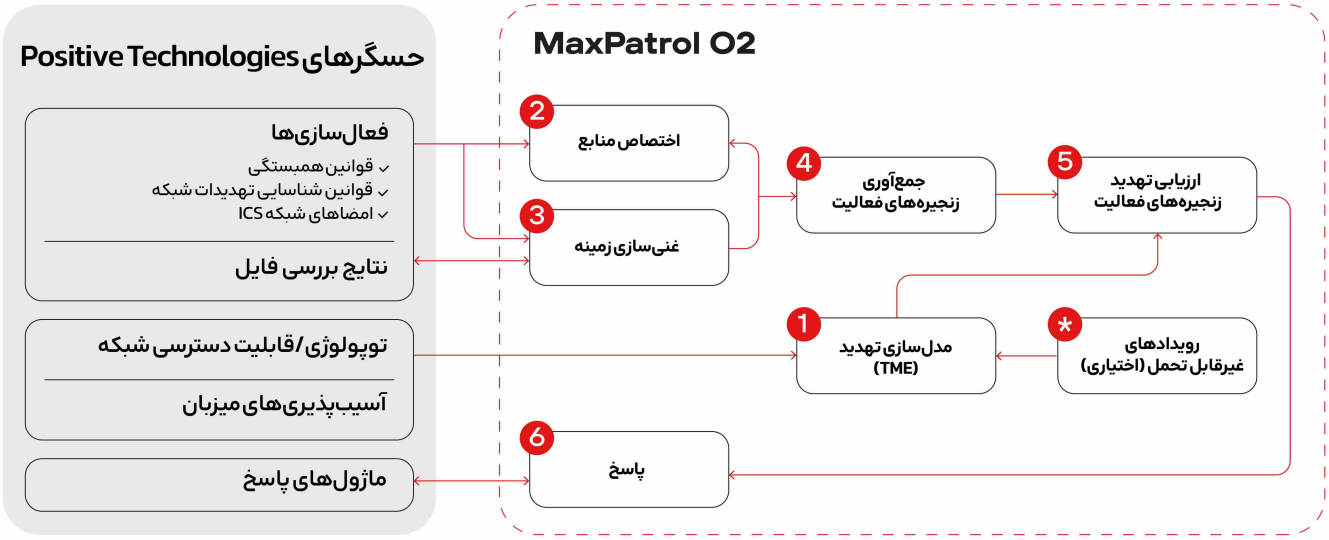
فعالیت‌های SOC را برای شناسایی، تحقیق و واکنش به رخدادها خودکار می‌کند.

به لطف تجربه Positive Technologies در تمرینات سایبری منظم، Positive Dream Hunting، Bug Bounty، و Standoff، می‌داند که مهاجمان چگونه عمل می‌کنند.

بدون نیاز به مهارت‌های خاص برای مؤثر بودن متاپرداکت‌ها.



نحوه کار MaxPatrol O2



global.ptsecurity.com
info@ptsecurity.com

MP-O2_A4.ENG.0001.09.APR.2024

positive technologies

MaxPatrol SIEM

زیرساخت شما را با جزئیات می‌شناسد و رخدادها را به‌دقت شناسایی می‌کند

MaxPatrol SIEM
رخدادهای امنیت اطلاعات منجر به رویدادهای غیرقابل‌تحمل و هرگونه تلاش برای به خطر انداختن تاب‌آوری سایبری شرکت را شناسایی می‌کند

نتایج سریع:
بدون نیاز به سرمایه‌گذاری یا تغییرات اضافی. به سرعت راه‌اندازی می‌شود تا بتوانید نظارت بر زیرساخت را با تخصص از پیش آماده شروع کنید.

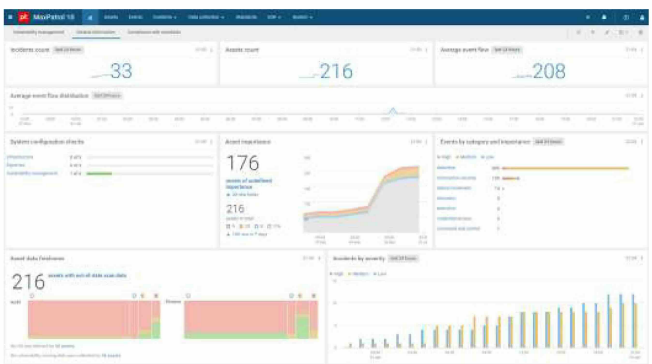
بانک سناریوهای به‌روز شده:
MaxPatrol SIEM هر ماه به‌صورت خودکار با یک بسته جدید به‌روزرسانی می‌شود و قوانین قبلی به طور مداوم به‌روزرسانی و بهبود می‌یابند این بانک توسط متخصصین PT دایما تولید و منتشر میشود تا بانک حملات و سناریوهای نفوذ به صورت بیش از ۸۰۰۰ User-Case مدلسازی شود .

قابلیت انطباق با تغییرات:
سازگاری سریع با تغییرات زیرساخت و شناسایی شفاف دارایی‌های IT. گروه‌بندی دارایی‌ها تنظیم قوانین همبستگی را ساده‌تر می‌کند.

کمک به تصمیم‌گیری:
MaxPatrol SIEM با ویژگی تشخیص ناهنجاری رفتاری (BAD) به عنوان یک دستیار هوش مصنوعی برای افزایش اثربخشی شناسایی حملات با ارزیابی جایگزین رویدادها عمل می‌کند.

ساده و آسان:
تلاش‌های ما برای بهبود تجربه تحلیل‌گر (AX) متمرکز است. کارت‌های رویداد راحت به شناسایی رویدادهای مرتبط، بررسی فایل‌های بالقوه خطرناک و پاسخ به رخدادها در همان پنجره کمک می‌کند.

نظارت در سطح سازمانی:
MaxPatrol SIEM می‌تواند بیش از ۵۴۰,۰۰۰ EPS را با یک هسته و تخصص کامل مدیریت کند. به لطف سیستم مدیریت پایگاه داده اختصاصی LogSpace، تنها نیمی از منابع نسبت به راه‌حل‌های مشابه متن باز مصرف می‌شود.



داشبوردهای سفارشی به نظارت بر وضعیت کلی امنیت اطلاعات سازمان کمک می‌کنند

همه کارها را با MaxPatrol SIEM انجام دهید

- نظارت بر امنیت اطلاعات در زیرساخت های بزرگ و سلسله‌مراتبی
- مشاهده زیرساخت IT
- تأیید پیکربندی سیستم با استفاده از چک‌لیست
- ایجاد قوانین همبستگی سفارشی با سازنده انعطاف‌پذیر
- افزودن خودکار محرک‌های معتبر به لیست سفید
- بررسی فرضیات با مشاهده رویدادهای همبسته مرتبط
- جستجوی داده‌ها در سیستم‌ها و خدمات شخص ثالث مستقیماً در کارت رویداد

درخواست پروژه آزمایشی

بیایید که زیرساخت شما چگونه می‌تواند از MaxPatrol SIEM بهره‌مند شود.

رهبر راهکار SIEM داخلی

این محصول توسط بیش از ۶۰۰ شرکت صنعتی، حمل‌ونقل و مالی، همچنین در بخش‌های خصوصی و دولتی و توسط نهادهای دولتی مورد استفاده قرار می‌گیرد.

به‌روزرسانی‌های منظم بسته تخصصی برای شناسایی تهدیدات

تخصص موجود در MaxPatrol SIEM از تحقیقات ما در زمینه رخدادهای پیچیده، پژوهش در تهدیدات نوظهور و روش‌های هک علیه شرکت‌ها و رصد فعالیت های تمامی گروه‌های هکری بزرگ در سراسر جهان به دست می‌آید.

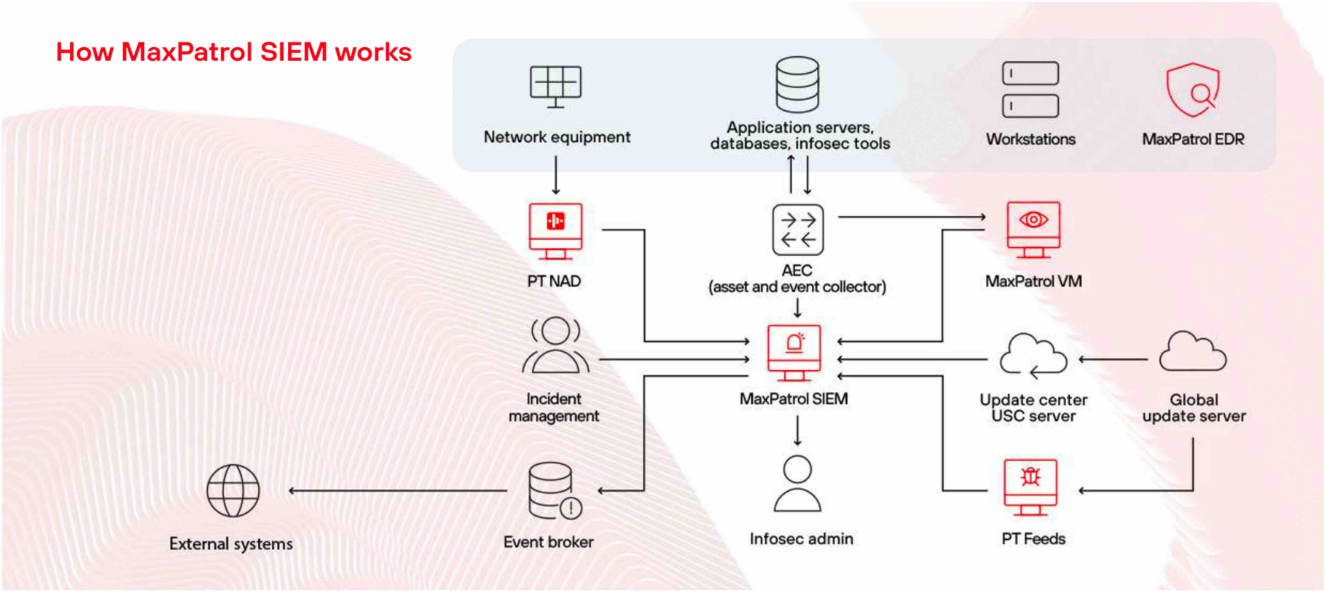
توسعه‌های جامعه و مستقل

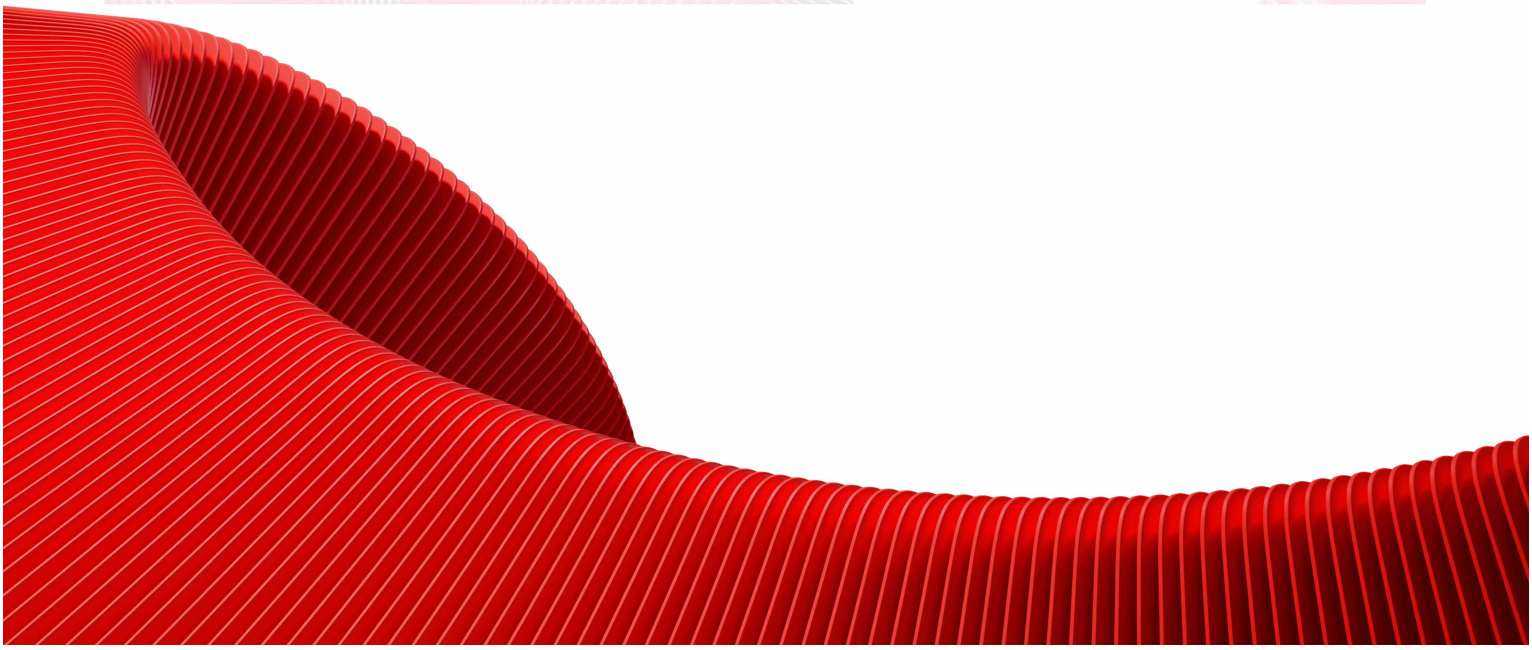
فهرست افزونه‌ها شامل افزونه‌ها، قوانین و کانکتورهایی است که توسط جامعه متخصص برای MaxPatrol SIEM توسعه یافته‌اند تا حل انواع مشکلات را ساده‌تر کنند.

رشد سریع

با دو نسخه جدید در هر سال، ما به‌طور منظم فناوری‌های جدید معرفی می‌کنیم و تیم توسعه محصول خود را به‌طور مداوم گسترش می‌دهیم.

How MaxPatrol SIEM works





positive technologies

MaxPatrol VM

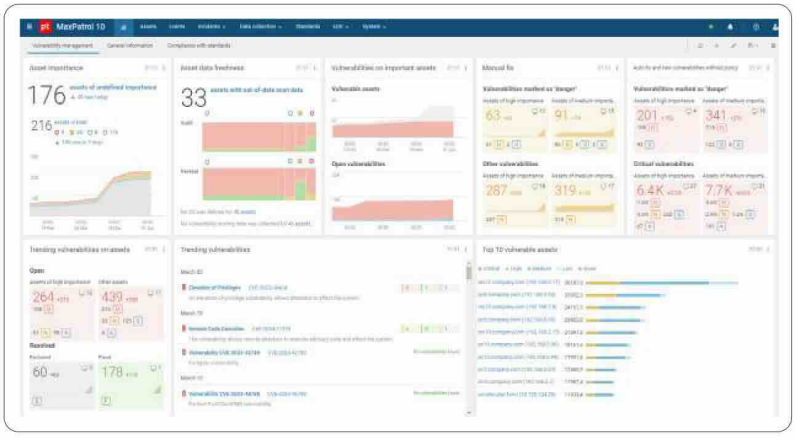
یک سیستم مدیریت آسیب‌پذیری

MaxPatrol VM یک سیستم پیشرفته است که به ایجاد فرآیند کامل مدیریت آسیب‌پذیری کمک می‌کند و نفوذ به شبکه را برای مهاجمان دشوار و پرهزینه می‌سازد. **این راهکار هوشمند اطلاعات مرتبط با آسیب‌پذیری های نوظهور را در کمتر از ۱۲ ساعت ارائه می‌دهد.**

MaxPatrol VM بر اساس فناوری منحصر به فرد مدیریت دارایی‌های امنیتی (SAM) ساخته شده است که امکان جمع‌آوری داده‌ها در حالت‌های فعال و غیرفعال، شناسایی دارایی‌ها با چندین پارامتر و ایجاد مدل به‌روزی از زیرساخت IT را فراهم می‌کند. این مدل به تیم امنیت سایبری یک نمای کامل از محیط IT برای محافظت ارائه می‌دهد. با استفاده از این اطلاعات، تیم می‌تواند فرآیند مدیریت آسیب‌پذیری را با در نظر گرفتن اهمیت اجزای شبکه برای فرآیندهای تجاری و تغییرات زیرساختی، به‌صورت خودکار ایجاد و مدیریت کند.
MaxPatrol VM اطلاعات دارایی‌ها و شناسایی آسیب‌پذیری‌ها را از هم جدا می‌کند. این سیستم نتایج اسکن‌های قبلی دارایی‌ها را به خاطر می‌سپارد و از آن‌ها برای محاسبه خودکار ارتباط آسیب‌پذیری‌های جدید با میزبان‌های شبکه شما استفاده می‌کند.

این رویکرد به شناسایی سریع‌تر آسیب‌پذیری‌های جدید بدون نیاز به اسکن مجدد کمک می‌کند و امکان واکنش سریع‌تر با شروع ترمیم فوری یا اعمال کنترل‌های جبرانی را فراهم می‌آورد.

ماژول MaxPatrol HCC در MaxPatrol VM امکان بررسی انطباق زیرساخت شما با استانداردهای عملی امنیت سایبری را فراهم می‌سازد. این سیستم دارای داشبوردهای دینامیکی است که به شما کمک می‌کند تا تحقق الزامات حیاتی مربوط به دارایی‌هایتان را پیگیری کنید. همچنین می‌توانید بررسی‌ها را بر اساس نیازهای خاص شرکت خود سفارشی کرده و مهلت‌های ترمیم تعیین کنید.



داشبورد تعاملی MaxPatrol VM

قابلیت‌های MaxPatrol VM

بروزرسانی مداوم اطلاعات زیرساخت IT

MaxPatrol VM با استفاده از مکانیزم های فعال و غیرفعال جمع‌آوری داده ها، اطلاعات جامعی از دارایی‌ها به دست می‌آورد.

خودکارسازی مدیریت دارایی‌ها

MaxPatrol VM به طور خودکار دارایی ها را شناسایی می‌کند و امکان ارزیابی اهمیت آن‌ها، تخصیص به گروه‌ها، و کنترل اسکن و ماندگاری داده‌ها را فراهم می‌سازد.

شناسایی و اولویت‌بندی آسیب پذیری‌ها

MaxPatrol VM از پایگاه دانش به‌روز شده خود برای ارزیابی سطح امنیتی دارایی‌ها استفاده می‌کند.

کمک به ایجاد فرآیند مدیریت آسیب‌پذیری‌ها

MaxPatrol VM به شما امکان می‌دهد تا سیاست‌های اسکن و ترمیم را تعریف کرده و تطابق با آن‌ها را کنترل کنید.

پایش آسیب‌پذیری‌های نوظهور

Positive Technologies در کمتر از ۱۲ ساعت اطلاعات تخصصی در مورد آسیب پذیری‌های حیاتی و مرتبط ارائه می دهد.

با MaxPatrol VM، شما می‌توانید:

- اطلاعات کامل و به‌روز درباره زیرساخت IT خود را دریافت کنید.
- اهمیت دارایی‌های مورد نیاز برای حفاظت را در نظر بگیرید.
- آسیب‌پذیری‌ها را شناسایی و اولویت‌بندی کرده و قوانین پردازش آن‌ها را تنظیم کنید.
- آسیب‌پذیری‌های جدید و با شدت بالا را به سرعت شناسایی کنید.
- روند رفع آسیب‌پذیری‌ها را کنترل کرده و وضعیت کلی امنیت شرکت را نظارت کنید.

نحوه کار MaxPatrol VM

نگهداری از پایگاه داده به‌روز دارایی‌ها

MaxPatrol VM کامل‌ترین اطلاعات دارایی‌ها را جمع‌آوری می‌کند. این پایگاه داده با داده‌های حاصل از اسکن‌های black-box و white-box و همچنین واردات داده از منابع مختلف پرمی‌شود: دایرکتوری‌های خارجی (مانند SCCM، ActiveDirectory، هایپروایزرها) و سایر راهکارهای امنیت سایبری که رویدادها و ترافیک را تحلیل می‌کنند (سیستم های SIEM و NTA). یک الگوریتم اختصاصی کشف دارایی اطلاعات را حتی در صورتی که از منابع متعدد باشد، در مورد یک میزبان خاص تلفیق می‌کند.

ارزیابی و طبقه‌بندی دارایی‌ها

طبقه‌بندی دارایی‌ها بر اساس سطح اهمیت، تمرکز را بر میزبان‌های با اولویت بالا نگه می‌دارد و به شناسایی دارایی‌های جدید کمک می‌کند. سیستم همچنین دارایی‌های ارزیابی‌نشده را گزارش می‌دهد و به دارایی‌هایی که بالقوه مهم هستند هشدار می‌دهد.

شناسایی و اولویت‌بندی آسیب‌پذیری‌ها

MaxPatrol VM زیرساخت IT شما را به‌طور عمیق بررسی می‌کند: آسیب‌پذیری‌ها و خطاهای پیکربندی را در اجزای سیستم اطلاعاتی شناسایی می‌کند و به شما در تنظیم فعالیت‌های ترمیمی کمک می‌کند، با در نظر گرفتن سطح شدت آسیب‌پذیری و پارامترهای دارایی آسیب‌پذیر (مانند سازنده، نسخه سیستم‌عامل و تنظیمات).

تعریف سیاست‌ها

سیاست‌های اسکن و ترمیم در MaxPatrol VM عملیات مختلفی را بر روی دارایی‌ها و آسیب‌پذیری‌های شناسایی‌شده خودکار می‌کنند. به عنوان مثال، می‌توانید زمان‌بندی اسکن یا تاریخی برای پردازش دوره‌ای آسیب‌پذیری‌ها در چندین دارایی را تعریف کنید.

پایش آسیب‌پذیری‌های نوظهور

Positive Technologies اطلاعاتی درباره آسیب‌پذیری‌های جدید و با شدت بالا در کمتر از ۱۲ ساعت ارائه می‌دهد. این امر به شما امکان می‌دهد آن‌ها را سریعاً در زیرساخت خود شناسایی کنید و اسکن با اولویت بالا را برای سیستم‌های بالقوه آسیب‌پذیر برنامه‌ریزی کنید.

هماهنگی مدیریت آسیب‌پذیری‌ها

MaxPatrol VM آمار اسکن‌های منظم را ردیابی می‌کند. این اطلاعات به کارشناسان امنیت سایبری کمک می‌کند تا کیفیت اسکن را کنترل کنند. علاوه بر این، تحلیل گذشته‌نگر به شما امکان می‌دهد پیشرفت رفع آسیب‌پذیری‌ها، سطح امنیت زیرساخت و تطابق با سیاست‌ها را ارزیابی و نظارت کنید.

مزایای MaxPatrol VM

یکپارچگی عمیق با سیستم‌های SIEM و NTA و غنی‌سازی اطلاعات دارایی

تصویر کامل از محیط IT شما با فناوری منحصربه‌فرد شناسایی دارایی

شناسایی سریع آسیب‌پذیری‌ها بدون نیاز به اسکن مجدد با استفاده از اطلاعات دارایی‌های ذخیره‌شده

پشتیبانی تخصصی و اطلاع‌رسانی درباره آسیب‌پذیری‌های جدید و با شدت بالا در کمتر از ۱۲ ساعت

اتوماسیون جامع در تحلیل امنیت و مدیریت دارایی‌ها

نسخه آزمایشی را امتحان کنید

MaxPatrol VM را روی زیرساخت خود تست کنید. فرم را در وب‌سایت ما پر کنید و فرآیند مدیریت آسیب‌پذیری خود را آغاز کنید.

global.ptsecurity.com
info@ptsecurity.com

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.

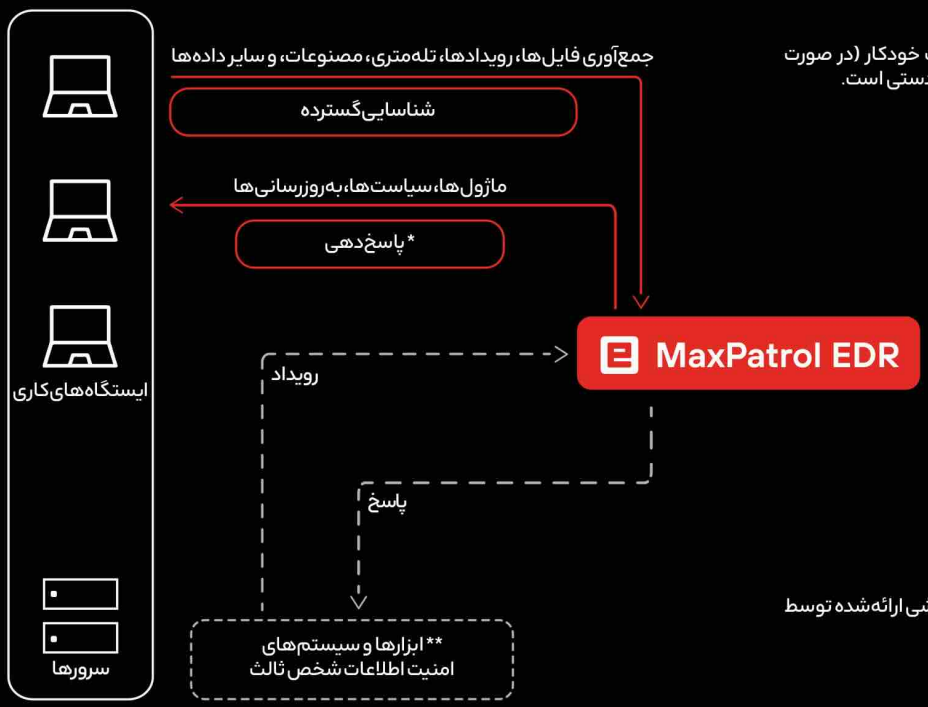
انطباق با ویژگی‌های زیرساخت
امکان تنظیم انعطاف‌پذیر سیاست‌های شناسایی و پاسخ‌دهی را متناسب با معماری فراهم می‌کند. تعادلی ایده‌آل بین بار میزبان و برآورده‌سازی نیازهای SOC حفظ می‌شود.

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.