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

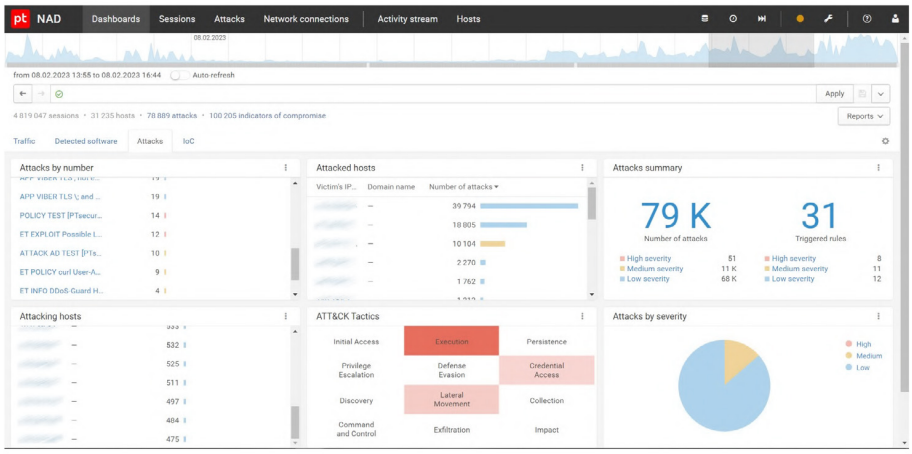
PT NAD بیش از ۱۰۰ پروتکل و ۹ پروتکل تونل را شناسایی کرده و ۳۵ پروتکل رایج را تا لایه L۷ تحلیل می‌کند. با تجزیه و تحلیل بیش از ۱۲۰۰ پارامتر پروتکلی، PT NAD مدل‌هایی برای گره‌های شبکه می‌سازد. این کار تصویری واضح از وضعیت زیرساخت فراهم می‌کند و به شناسایی نقص‌های امنیتی که می‌توانند امنیت را تضعیف کرده 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

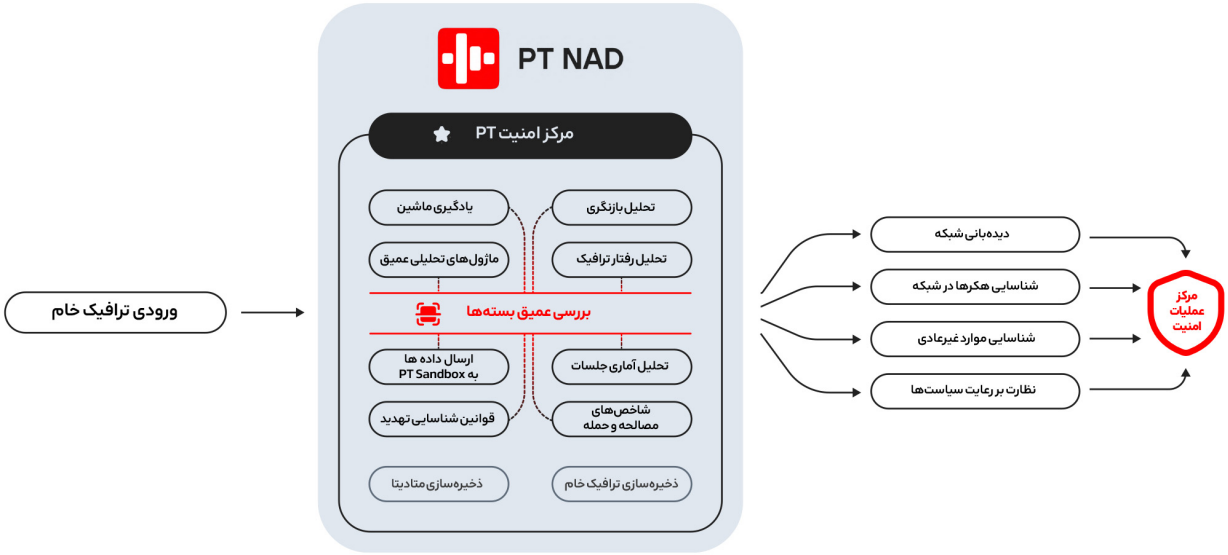
استقرار سریع
امکان یکپارچه‌سازی با سیستم‌های
SIEM و سندباکس‌ها

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

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید.برای درخواست آزمایشی رایگان PT ، با ما تماس بگیرید.

pt@magsaco.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.

MAGSA magsaco.ir شرکت مگسا (مهندسی گسترش سامانه امن) یکی از شرکت های با سابقه و فعال در حوزه امنیت فضای تولید و تبادل اطلاعات است که در سال ۱۳۸۲ شکل گرفت و در سال ۱۳۸۴ تاسیس شد. حوزه های اصلی فعالیت این شرکت با دو رویکرد اصلی است.

رویکرد فنی امنیت که شامل امنیت نرم افزار، امنیت شبکه، امنیت اطلاعات و امنیت زیرساختهای صنعتی است. رویکرد مدیریت امنیت که شامل طراحی طرحهای جامع امنیت شبکه، طرح جامع امنیت سایبر، ارزیابی سطح بلوغ امنیت سایبری و پیاده سازی سیستم مدیریت امنیت اطلاعات است. طی دو دهه گذشته، خدمات گوناگونی در هر دو حوزه توسط شرکت به سازمانها، نهادها، شرکت ها و سایر مشتریان شرکت ارائه شده است.

درحال حاضر مگسا به عنوان شرکت توزیع کننده محصولات PT در ایران فعالیت میکند

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.

ptsecurity.com