

PT NAD

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

مزایا



شناسایی مهاجمان
در ترافیک افقی (East-West)



شناسایی ابزارهای هکرها
و بدافزارهای تغییر یافته



کمک به برآورده کردن الزامات
حفاظت از اطلاعات



امکان یکپارچه سازی با سیستم های
SIEM و سندباکس ها



استقرار سریع
امکان یکپارچه سازی با سیستم های
SIEM و سندباکس ها

کشف حملات شبکه PT - یک سیستم تحلیل ترافیک شبکه (NTA) است که برای نظارت بر فعالیت های مخرب در محدوده و داخل شبکه استفاده می شود. این ابزار تحقیقاتی مناسب می تواند فعالیت های مخرب را حتی در ترافیک رمزگذاری شده شناسایی کند. PT NAD می داند در شبکه شرکت شما به دنبال چه چیزی بگردد.

مشاهده کامل شبکه

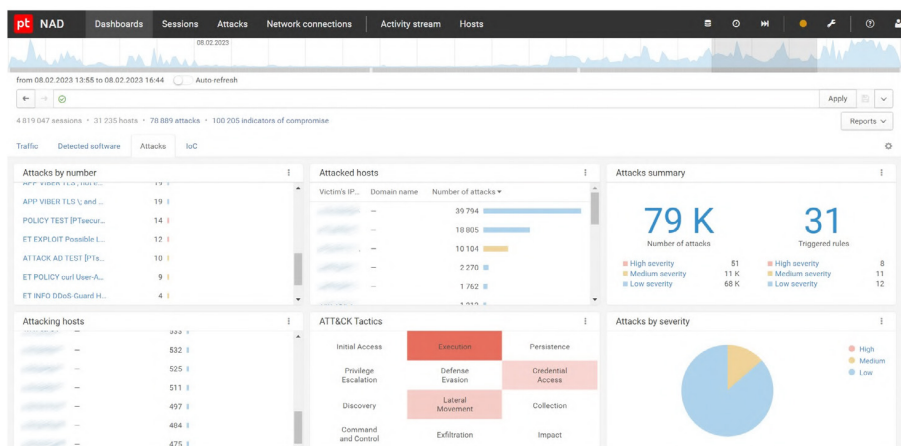
PT NAD بیش از ۱۰۰ پروتکل و ۹ پروتکل تونل را شناسایی کرده و ۳۵ پروتکل رایج را تا لایه ۷ تحلیل می کند. با تجزیه و تحلیل بیش از ۱۲۰۰ پارامتر پروتکلی، PT NAD مدلهایی برای گره های شبکه می سازد. این کار تصویری واضح از وضعیت زیرساخت فراهم می کند و به شناسایی نقص های امنیتی که می توانند امنیت را تضعیف کرده و موجب پیشرفت حملات شوند، کمک می کند. PT NAD تمام میزبان های شبکه را تحت نظر دارد، استفاده از اجزای غیرقابل کنترل زیرساخت IT را به حداقل می رساند و ریسک هک شدن شرکت از طریق این اجزا را کاهش می دهد.

شناسایی تهدیدات مخفی و حملات هدفمند

PT NAD به طور خودکار تلاش های نفوذ به شبکه و حضور مهاجمان در زیرساخت را با استفاده از نشانه های مختلف، از جمله ابزارهای استفاده شده یا داده های منتقل شده به سرورهای مهاجم، شناسایی می کند.

افزایش کارایی مراکز عملیات امنیتی (SOC)

PT NAD منبعی ضروری برای راهکارهای SIEM است. این سیستم متادیتا و ترافیک خام را ذخیره کرده، کمک می کند جلسات مشکوک را سریعاً شناسایی و تحلیل کنید و امکان صدور و وارد کردن ترافیک را فراهم می آورد. PT NAD با ارائه دید کاملی از شبکه به SOC ها، بررسی موفقیت حملات، ردیابی زنجیره حملات و جمع آوری شواهد را آسان تر می کند.



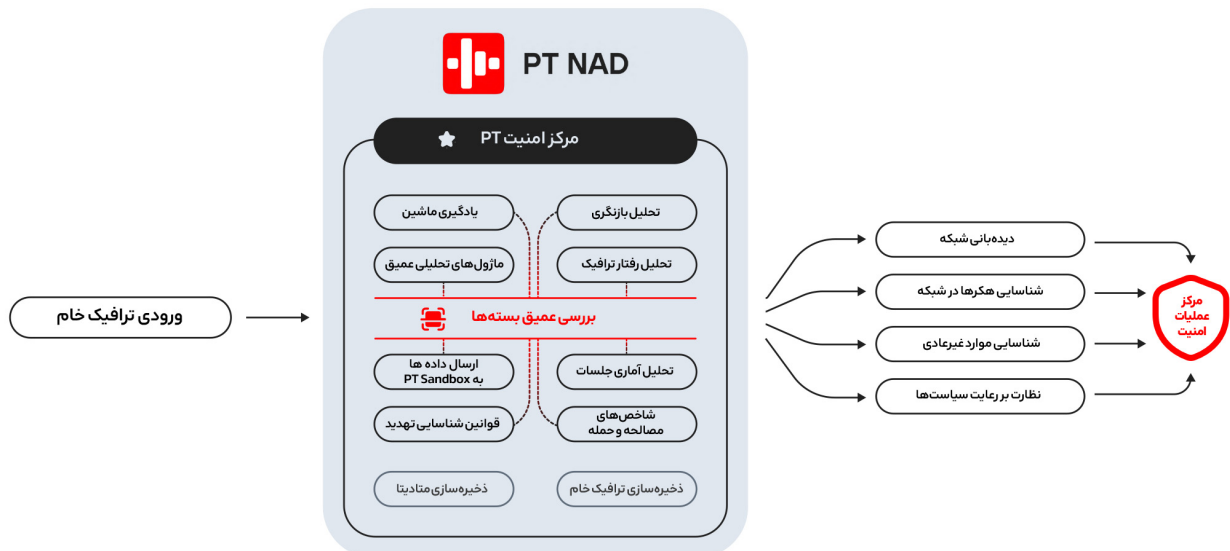
اپراتور در داشبورد اطلاعات دقیقی درباره فعالیت های مشکوک مشاهده می کند.
این امر به واکنش سریع به رخدادها و انجام تحقیقات کمک می کند.

PT NAD شناسایی می‌کند:

- تهدیدات در ترافیک رمزگذاری شده
- استفاده از ابزارهای هکرها، از جمله ابزارهای سفارشی‌سازی شده
- 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 تولید شده
- عدم رعایت سیاست‌های امنیت اطلاعات (IS)

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 به صورت 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 مازول‌های 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، آسیب‌پذیری‌های 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.



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. به عنوان منابع ترافیک می‌توان از دستگاه‌های TAP، شبکه‌های بسته‌ای و تجهیزات فعال شبکه استفاده کرد. با تحلیل کپی ترافیک شبکه با استفاده از مازول‌های 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 داده‌های ترافیک جمع‌آوری شده 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.

آیا شرکت شما تحت حمله قرار گرفته است؟

شبکه و محیط خارجی خود را بررسی کنید

برای درخواست آزمایشی رایگان Positive 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 سریع‌ترین 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.

© Positive Technologies 2016. Positive Technologies و لوگوی آن، علائم تجاری یا علائم ثبت‌شده Positive Technologies هستند. تمام علائم تجاری دیگر ذکر شده متعلق به صاحبان مربوطه هستند.

شرکت فناوری ارتباطات آشیانه امن ارائه‌دهنده خدمات زیرساخت و امنیت شبکه می‌باشد که دارای مجوز توزیع‌کننده و نمایندگی فروش و خدمات محصولات شرکت PT در ایران است همچنین دارای تیمی مجرب در ارائه خدمات امنیت شبکه مانند تست نفوذ و ارزیابی امنیتی و راه‌اندازی و راهبری مرکز عملیات امنیت و اقدامات و محصولات بومی جهت شناسایی حملات فیشینگ و حفاظت از برندهای معتبر می‌باشد.



شرکت Positive Technologies

پیشرو در صنعت امنیت سایبری و ارائه‌دهنده جهانی راهکارهای امنیت اطلاعات است. مأموریت ما: حفاظت از کسب‌وکارها و منابع 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.