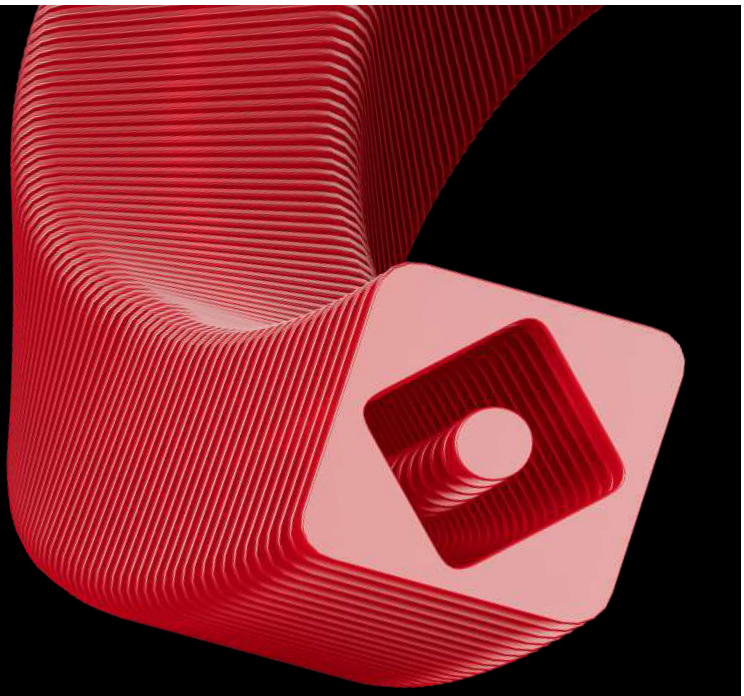
positive technologies



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

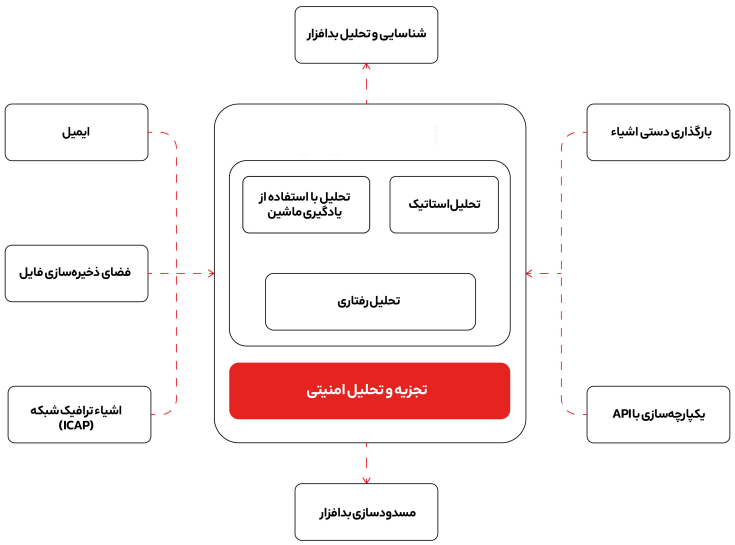
فایل‌های محرمانه در هنگام بررسی از محدوده شرکت خارج نمی‌شوند.

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

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