

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 فعالیت‌های مشکوک و تحلیل پویا، به شناسایی و مقابله با تهدیدات ناشناخته کمک می‌کند.

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، IDS، IPS، 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 بوتکیت‌ها 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 آنتی‌ویروس 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 PT SANDBOX (RED OS و ASTRA LINUX). به طور 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

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 شرکت‌های 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.

سایر قابلیت ها

عملکرد بالا

مدیریت انعطاف پذیر پردازش فایل ها و لینک ها و مقیاس پذیری افقی نامحدود PT SANDBOX عملکرد بالایی را تحت هر بار کاری تضمین می کند.

حالت های نظارت و مسدودسازی

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

ادغام آسان

از PT SANDBOX گزینه های مختلف آماده برای ادغام پشتیبانی می کند و دارای API انعطاف پذیر است که به شما امکان می دهد محصول را در هر پیکربندی از سیستم های اطلاعاتی استفاده کنید.

پشتیبانی از اکوسیستم POSITIVE TECHNOLOGIES

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

گزینه نصب داخلی

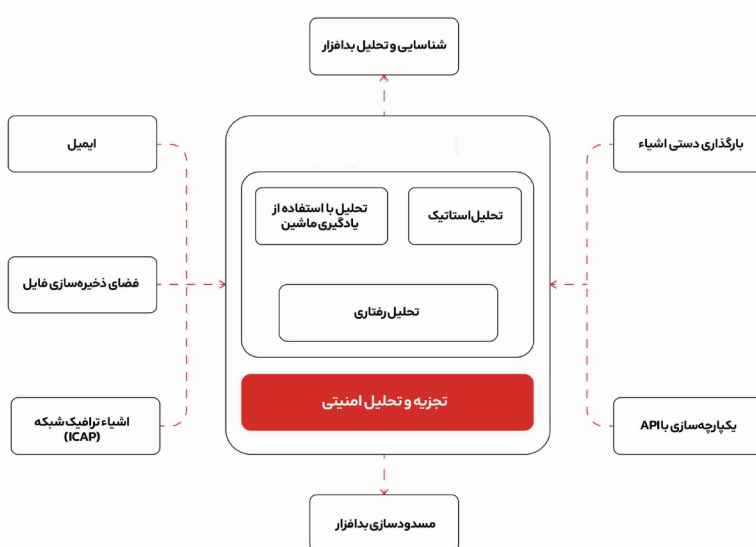
فایل های محرمانه در هنگام بررسی از محدوده شرکت خارج نمی شوند.

شناسایی تهدیدات از دست رفته قبلی

PT SANDBOX پس از به روزرسانی پایگاه دانش، به طور منظم تحلیل های گذشته نگر از فایل های قبلاً بررسی شده انجام می دهد. این امکان به شما داده می شود 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 فایل ها و ترافیک

PT SANDBOX فایل ها را بررسی کرده، ترافیکی که در طی تحلیل فایل ایجاد شده را تجزیه و تحلیل می کند و فعالیت های مخرب پنهان شده توسط رمزنگاری TLS را شناسایی می کند. این روش به طور قابل توجهی کارایی شناسایی حملات را حتی در ترافیک رمزگذاری شده بهبود می بخشد.



نحوه کار PT SANDBOX