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.

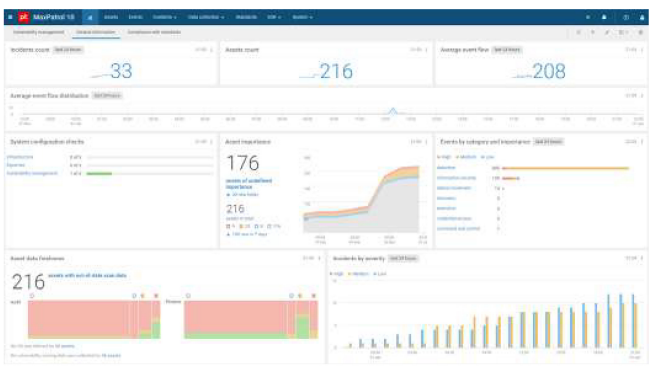
بانک سناریوهای به‌روز شده:
MaxPatrol SIEM هر ماه به‌صورت خودکار با یک بسته جدید به‌روزرسانی می‌شود و قوانین قبلی به طور مداوم به‌روزرسانی و بهبود می‌یابند این بانک توسط متخصصین PT دایما تولید و منتشر میشود تا بانک حملات و سناریوهای نفوذ به صورت بیش از ۸۰۰۰ User-Case مدلسازی شود .

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 EPS ۵۴۰,۰۰۰ 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.

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. بیش از ۴,۰۰۰ سازمان در سراسر جهان از فناوری‌ها و خدمات توسعه‌یافته توسط شرکت ما استفاده می‌کنند.

magsaco.ir MAGSA 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