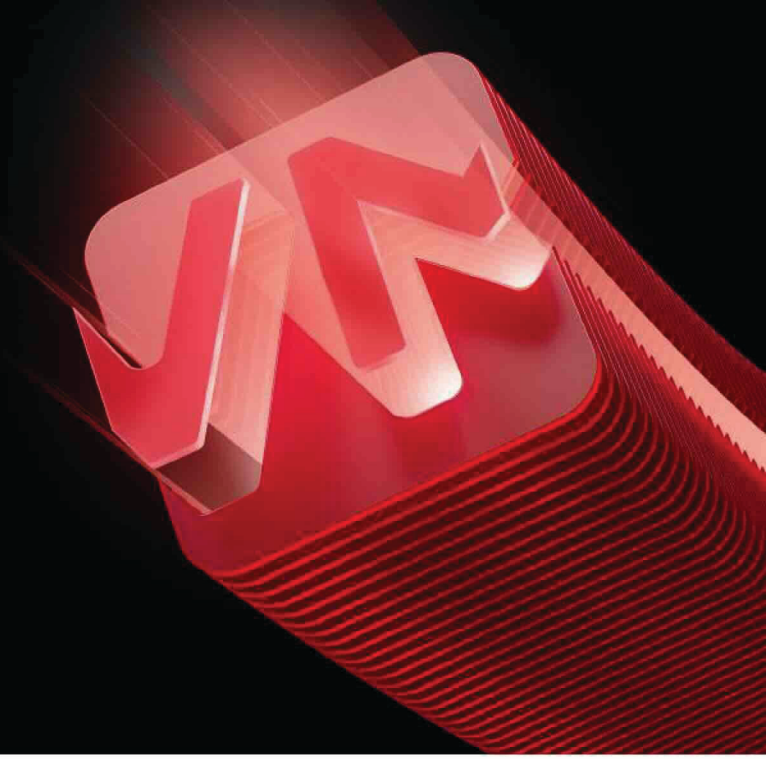
positive technologies

PARSPOUYA
NETWORK SECURITY SERVICES



MaxPatrol VM

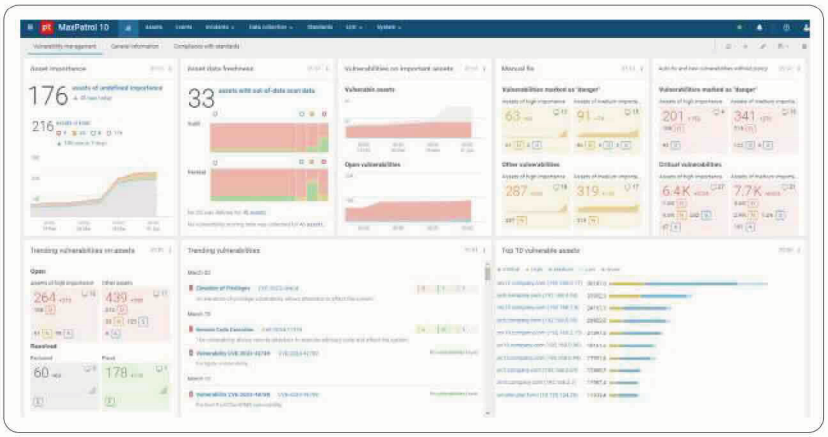
یک سیستم مدیریت آسیب‌پذیری

MaxPatrol VM یک سیستم پیشرفته است که به ایجاد فرآیند کامل مدیریت آسیب‌پذیری کمک می‌کند و نفوذ به شبکه را برای مهاجمان دشوار و پرهزینه می‌سازد. **این راهکار هوشمند اطلاعات مرتبط با آسیب‌پذیری های نوظهور را در کمتر از ۱۲ ساعت ارائه می‌دهد.**

MaxPatrol VM بر اساس فناوری منحصر به فرد مدیریت دارایی‌های امنیتی (SAM) ساخته شده است که امکان جمع‌آوری داده‌ها در حالت‌های فعال و غیرفعال، شناسایی دارایی‌ها با چندین پارامتر و ایجاد مدل به‌روزی از زیرساخت IT را فراهم می‌کند. این مدل به تیم امنیت سایبری یک نمای کامل از محیط IT برای محافظت ارائه می‌دهد. با استفاده از این اطلاعات، تیم می‌تواند فرآیند مدیریت آسیب‌پذیری را با در نظر گرفتن اهمیت اجزای شبکه برای فرآیندهای تجاری و تغییرات زیرساختی، به‌صورت خودکار ایجاد و مدیریت کند.
MaxPatrol VM اطلاعات دارایی‌ها و شناسایی آسیب‌پذیری‌ها را از هم جدا می‌کند. این سیستم نتایج اسکن‌های قبلی دارایی‌ها را به خاطر می‌سپارد و از آن‌ها برای محاسبه خودکار ارتباط آسیب‌پذیری‌های جدید با میزبان‌های شبکه شما استفاده می‌کند.

این رویکرد به شناسایی سریع‌تر آسیب‌پذیری‌های جدید بدون نیاز به اسکن مجدد کمک می‌کند و امکان واکنش سریع‌تر با شروع ترمیم فوری یا اعمال کنترل‌های جبرانی را فراهم می‌آورد.

ماژول MaxPatrol HCC در MaxPatrol VM امکان بررسی انطباق زیرساخت شما با استانداردهای عملی امنیت سایبری را فراهم می‌سازد. این سیستم دارای داشبوردهای دینامیکی است که به شما کمک می‌کند تا تحقق الزامات حیاتی مربوط به دارایی‌هایتان را پیگیری کنید. همچنین می‌توانید بررسی‌ها را بر اساس نیازهای خاص شرکت خود سفارشی کرده و مهلت‌های ترمیم تعیین کنید.



داشبورد تعاملی MaxPatrol VM

قابلیت‌های MaxPatrol VM

بروزرسانی مداوم اطلاعات زیرساخت IT

MaxPatrol VM با استفاده از مکانیزم های فعال و غیرفعال جمع‌آوری داده ها، اطلاعات جامعی از دارایی‌ها به دست می‌آورد.

خودکارسازی مدیریت دارایی‌ها

MaxPatrol VM به طور خودکار دارایی ها را شناسایی می‌کند و امکان ارزیابی اهمیت آن‌ها، تخصیص به گروه‌ها، و کنترل اسکن و ماندگاری داده‌ها را فراهم می‌سازد.

شناسایی و اولویت‌بندی آسیب پذیری‌ها

MaxPatrol VM از پایگاه دانش به‌روز شده خود برای ارزیابی سطح امنیتی دارایی‌ها استفاده می‌کند.

کمک به ایجاد فرآیند مدیریت آسیب‌پذیری‌ها

MaxPatrol VM به شما امکان می‌دهد تا سیاست‌های اسکن و ترمیم را تعریف کرده و تطابق با آن‌ها را کنترل کنید.

پایش آسیب‌پذیری‌های نوظهور

Positive Technologies در کمتر از ۱۲ ساعت اطلاعات تخصصی در مورد آسیب پذیری‌های حیاتی و مرتبط ارائه می دهد.

با MaxPatrol VM، شما می‌توانید:

- اطلاعات کامل و به‌روز درباره زیرساخت IT خود را دریافت کنید.
- اهمیت دارایی‌های مورد نیاز برای حفاظت را در نظر بگیرید.
- آسیب‌پذیری‌ها را شناسایی و اولویت‌بندی کرده و قوانین پردازش آن‌ها را تنظیم کنید.
- آسیب‌پذیری‌های جدید و با شدت بالا را به سرعت شناسایی کنید.
- روند رفع آسیب‌پذیری‌ها را کنترل کرده و وضعیت کلی امنیت شرکت را نظارت کنید.

نحوه کار MaxPatrol VM

نگهداری از پایگاه داده به‌روز دارایی‌ها

MaxPatrol VM کامل‌ترین اطلاعات دارایی‌ها را جمع‌آوری می‌کند. این پایگاه داده با داده‌های حاصل از اسکن‌های black-box و white-box و همچنین واردات داده از منابع مختلف پرمی‌شود: دایرکتوری‌های خارجی (مانند SCCM، ActiveDirectory، هایپروایزرها) و سایر راهکارهای امنیت سایبری که رویدادها و ترافیک را تحلیل می‌کنند (سیستم های SIEM و NTA). یک الگوریتم اختصاصی کشف دارایی اطلاعات را حتی در صورتی که از منابع متعدد باشد، در مورد یک میزبان خاص تلفیق می‌کند.

ارزیابی و طبقه‌بندی دارایی‌ها

طبقه‌بندی دارایی‌ها بر اساس سطح اهمیت، تمرکز را بر میزبان‌های با اولویت بالا نگه می‌دارد و به شناسایی دارایی‌های جدید کمک می‌کند. سیستم همچنین دارایی‌های ارزیابی‌نشده را گزارش می‌دهد و به دارایی‌هایی که بالقوه مهم هستند هشدار می‌دهد.

شناسایی و اولویت‌بندی آسیب‌پذیری‌ها

MaxPatrol VM زیرساخت IT شما را به‌طور عمیق بررسی می‌کند: آسیب‌پذیری‌ها و خطاهای پیکربندی را در اجزای سیستم اطلاعاتی شناسایی می‌کند و به شما در تنظیم فعالیت‌های ترمیمی کمک می‌کند، با در نظر گرفتن سطح شدت آسیب‌پذیری و پارامترهای دارایی آسیب‌پذیر (مانند سازنده، نسخه سیستم‌عامل و تنظیمات).

تعریف سیاست‌ها

سیاست‌های اسکن و ترمیم در MaxPatrol VM عملیات مختلفی را بر روی دارایی‌ها و آسیب‌پذیری‌های شناسایی‌شده خودکار می‌کنند. به عنوان مثال، می‌توانید زمان‌بندی اسکن یا تاریخی برای پردازش دوره‌ای آسیب‌پذیری‌ها در چندین دارایی را تعریف کنید.

پایش آسیب‌پذیری‌های نوظهور

Positive Technologies اطلاعاتی درباره آسیب‌پذیری‌های جدید و با شدت بالا در کمتر از ۱۲ ساعت ارائه می‌دهد. این امر به شما امکان می‌دهد آن‌ها را سریعاً در زیرساخت خود شناسایی کنید و اسکن با اولویت بالا را برای سیستم‌های بالقوه آسیب‌پذیر برنامه‌ریزی کنید.

هماهنگی مدیریت آسیب‌پذیری‌ها

MaxPatrol VM آمار اسکن‌های منظم را ردیابی می‌کند. این اطلاعات به کارشناسان امنیت سایبری کمک می‌کند تا کیفیت اسکن را کنترل کنند. علاوه بر این، تحلیل گذشته‌نگر به شما امکان می‌دهد پیشرفت رفع آسیب‌پذیری‌ها، سطح امنیت زیرساخت و تطابق با سیاست‌ها را ارزیابی و نظارت کنید.

مزایای MaxPatrol VM

یکپارچگی عمیق با سیستم‌های SIEM و NTA و غنی‌سازی اطلاعات دارایی

تصویر کامل از محیط IT شما با فناوری منحصربه‌فرد شناسایی دارایی

شناسایی سریع آسیب‌پذیری‌ها بدون نیاز به اسکن مجدد با استفاده از اطلاعات دارایی‌های ذخیره‌شده

پشتیبانی تخصصی و اطلاع‌رسانی درباره آسیب‌پذیری‌های جدید و با شدت بالا در کمتر از ۱۲ ساعت

اتوماسیون جامع در تحلیل امنیت و مدیریت دارایی‌ها

ویرا ارتباط پارس پویا
آدرس: تهران، خیابان شریعتی، دوراهی قلهک
کوچه مرشدی، پلاک ۲، واحد ۲
تلفن: ۷۵۳۹۷-۰۲۱ داخلی ۲۰۰ و ۲۰۰۰

Info@parspouya.com
Info@ptsecurity.info