positive technologies

PARSPOUYA
NETWORK SECURITY SERVICES

MaxPatrol O2

هدایت خودکار برای امنیت سایبری مبتنی بر نتایج

MaxPatrol O2 مهاجمان را شناسایی می‌کند، دارایی‌های نقض‌شده را تعیین می‌کند، سناریوی حمله را با توجه به رخدادهای غیرقابل‌تحمل مخصوص شرکت پیش‌بینی کرده و قبل از وارد آمدن آسیب جبران‌ناپذیر، حمله را متوقف می‌سازد.

مدل‌سازی اقدامات احتمالی مهاجمان:

پیش‌بینی رخدادهای غیرقابل‌تحملی که فعالیت مشکوک ممکن است منجر به آن‌ها شود و تعداد مراحل باقی‌مانده تا تحقق ریسک‌ها.

شناسایی زنجیره‌های فعالیت هکری:

تحلیل داده‌های حسگرهای Positive Technologies در محصول متاپرداکت و تفکیک منابع مهاجم، هدف‌گیری شده و تصرف‌شده. همبستگی منابع برای ساخت زنجیره‌های فعالیت با استفاده از دانش تاکتیک‌ها، تکنیک‌ها و پروسه‌های مهاجمان. هر زنجیره شامل تجسم مسیر مهاجمان و پیش‌بینی حرکت بعدی آن‌هاست.

خودکارسازی تحقیقات:

استفاده از داده‌های حسگرهای Positive Technologies برای ساختن یک زمینه کامل از حمله و انجام تحقیقات.

ارزیابی شدت تهدید:

MaxPatrol O2 منابع تصرف‌شده را مشاهده و نزدیکی به رخداد غیرقابل‌تحمل را ارزیابی می‌کند. پس از دریافت این اطلاعات، سیستم وضعیت زنجیره حمله را به "نیازمند توجه" ارتقاء می‌دهد و سپس مهاجم را متوقف کرده یا از اپراتور می‌خواهد تصمیم بگیرد.

متوقف‌سازی مهاجم:

با در نظر گرفتن ریسک‌های فرآیندهای تجاری، بهترین سناریوی پاسخ را پیشنهاد می‌دهد. این سناریو می‌تواند به صورت خودکار یا دستی در صورت نیاز به تنظیمات اعمال شود.

90%

از شرکت‌ها با کمبود متخصصان امنیت اطلاعات مواجه‌اند

71%

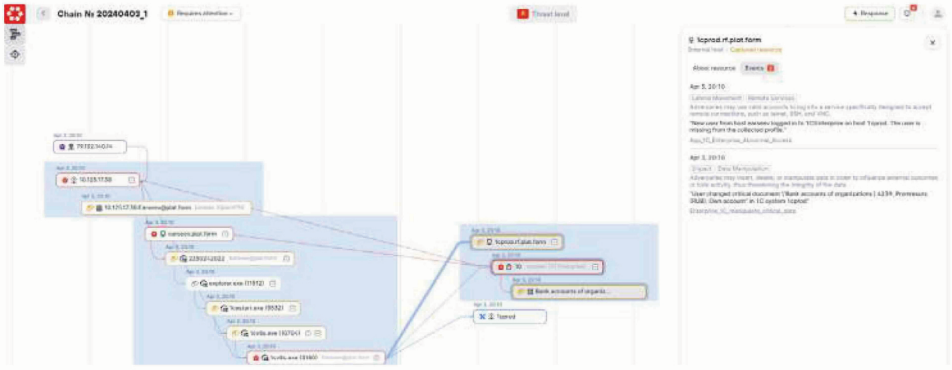
از رخدادهای غیرقابل‌تحمل می‌توانند توسط مهاجمان در عرض یک ماه اجرا شوند.

100%

از زیرساخت‌ها می‌توانند به‌طور کامل توسط مهاجمان داخلی تصرف شوند.

93%

از محیط‌های شبکه می‌توانند توسط مهاجمان عبور شده و به دسترسی شبکه محلی منجر شوند.



محصولات Positive Technologies را گرد هم می‌آورد که به عنوان حسگر عمل می‌کنند، دانش را تبادل می‌کنند و با حداقل دخالت انسانی، حفاظت کاملی از سیستم‌های IT ارائه می‌دهند.

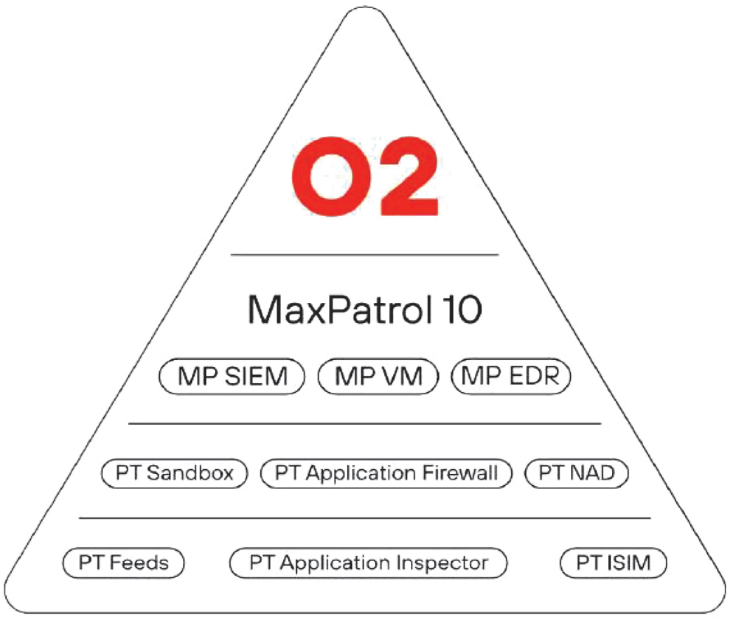
اکوسیستم
Positive Technologies

رخدادهای غیرقابل‌تحمل برای کسب‌وکار را حذف می‌کند.

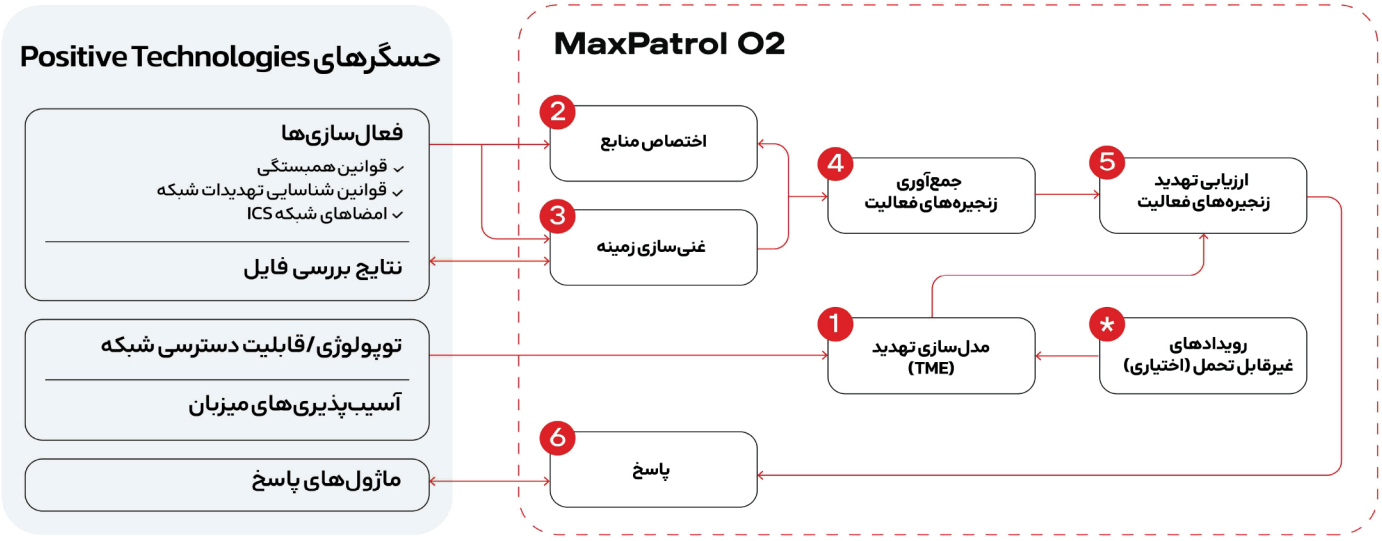
فعالیت‌های SOC را برای شناسایی، تحقیق و واکنش به رخدادها خودکار می‌کند.

به لطف تجربه Positive Technologies در تمرینات سایبری منظم، Positive Dream Hunting، Bug Bounty، و Standoff، می‌داند که مهاجمان چگونه عمل می‌کنند.

بدون نیاز به مهارت‌های خاص برای مؤثر بودن متاپرداکت‌ها.



نحوه کار MaxPatrol O2



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

Info@parspouya.com
Info@ptsecurity.info