positive technologies

PT Industrial Security Incident Manager

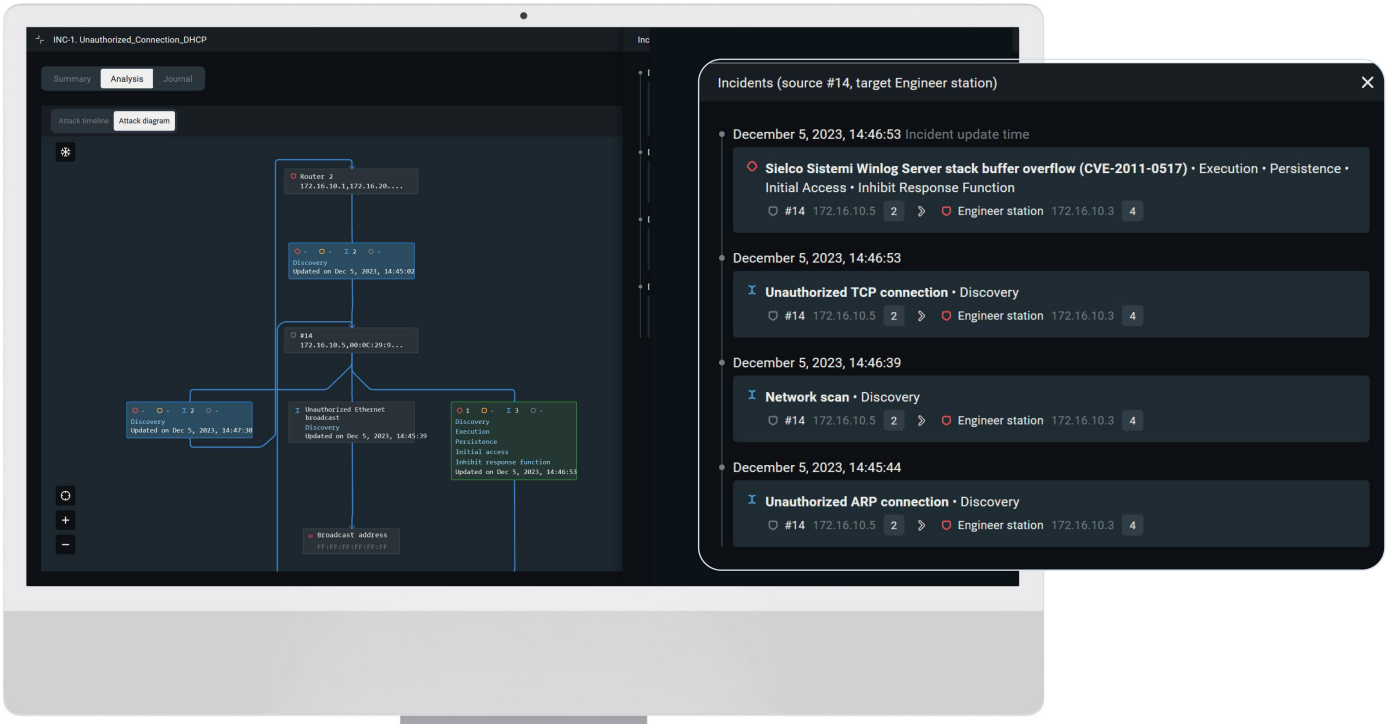
PT ISIM امنیت شبکه OT را تضمین می‌کند و امکانات نظارتی برای زیرساخت‌های OT و IIoT در تأسیسات صنعتی و ساختمانی فراهم می‌سازد.

PT Industrial Security Incident Manager

PT ISIM یک سیستم تحلیل عمیق ترافیک برای شبکه‌های OT است که بازرسی دقیق ترافیک را برای پروتکل‌های عمومی و خاص شبکه صنعتی انجام می‌دهد. با نظارت بر ترافیک در محیط خارجی و داخل شبکه کنترل صنعتی، PT ISIM عملیات مخربی را که ممکن است برای فرآیندهای عملیاتی خطرناک باشند شناسایی کرده و اطلاعات ضروری برای بررسی رخدادهای امنیتی را فراهم می‌کند. PT ISIM به پایگاه داده اختصاصی خود از تهدیدات سایبری صنعتی، یعنی شاخص‌های تهدید امنیت صنعتی PT (PT ISTI) متکی است. این دانش تخصصی از پیش آماده، امکان شروع نظارت و شناسایی تهدیدات را بدون نیاز به تنظیمات زمان‌بر یک سنسور شبکه فراهم می‌سازد.

پیشنهاد ارزش

- PT ISIM بیش از ۱۳۰ پروتکل شبکه را شناسایی می‌کند و می‌تواند در هر زیرساخت صنعتی یا محیط IIoT، مانند سیستم‌های مدیریت ساختمان و تجهیزات بهداشتی مبتنی بر DICOM استفاده شود.
- PT ISIM تمامی ارتباطات داخل شبکه OT را کنترل کرده و ناهنجاری‌ها، تهدیدات، نقص‌های پیکربندی OT و حتی دستورات کنترلی خطرناک را شناسایی می‌کند؛ این امر برای هر شرکت صنعتی حیاتی است.
- PT ISIM دارایی‌های پنهان IT را در زیرساخت OT آشکار می‌سازد. درک واضح ساختار شبکه OT برای اطمینان از عملکرد قوی OT ضروری است.



موارد استفاده

- فهرست‌برداری از شبکه OT و شناسایی دارایی‌های جدید
- شناسایی ناهنجاری ها، دستورات مخرب و خطرناک
- بهره‌برداری از آسیب پذیری‌ها و سایر تکنیک‌های مخرب
- تطبیق با الزامات مقرراتی
- شناسایی بدافزار و صدور فایل‌های مشکوک برای تحلیل آماری و رفتاری کامل در PT Sandbox

PT ISIM به تمامی خدمات فنی و بخش‌هایی که از مشاهده‌پذیری و پیش‌بینی زیرساخت OT و نظارت امنیتی بهره می‌برند، کمک می‌کند:

- پرسنل امنیتی : می‌توانند زیرساخت‌های حساس OT را در برابر تهدیدات سایبری واقعی ایمن کنند.
- پرسنل نگهداری OT : می‌توانند مقاومت زیرساخت OT و عملیات بدون وقفه فرآیندهای حساس را تضمین کنند.
- مدیران OT و پرسنل اعزام : می‌توانند کارخانه را با خیال راحت راه‌اندازی کرده و با کاهش کافی ریسک‌های سایبری به KPI تولید دست یابند

صنایع

- سیستم‌های کنترل صنعتی (ICS)
- سیستم‌های زیرساخت حیاتی
- سیستم‌های مدیریت ساختمان (BMS)
- سیستم‌های کنترل حمل‌ونقل ریلی
- شرکت‌های صنعتی پراکنده
- تجهیزات و سیستم‌های بهداشتی سازگار با DICOM

اجزا

سنسورهای PT ISIM View - سنسورهای شبکه

اجزای اصلی سیستم که ترافیک شبکه OT را ضبط و ذخیره می‌کنند. سنسورها در داخل زیرساخت OT مستقر شده و به شبکه OT متصل می‌شوند که شامل PLCها، سرورهای SCADA، و ایستگاه‌های کاری مهندسی و اپراتوری است.

مرکز PT ISIM Overview - کنسول مدیریت

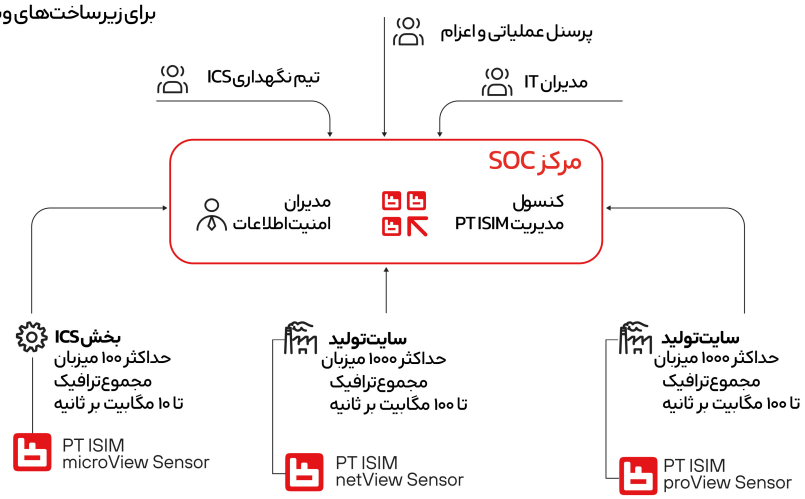
رابط یکپارچه برای نظارت، مدیریت و به روزرسانی مرکزی چندین سنسور ISIM View متصل. معمولاً در سطح SOC یا مرکز داده مستقر می‌شود. مرکز Overview رخدادها را از تمامی سنسورهای متصل دریافت می‌کند.

نحوه کار

PT ISIM یک کپی از ترافیک شبکه OT را از پورت SPAN یک سوئیچ صنعتی دریافت کرده و تمامی بسته‌ها و ارتباطات ضبط‌شده را تحلیل می‌کند. این سیستم توپولوژی شبکه را با نمایش تمامی میزبان‌ها و ارتباطات شبکه تجسم می‌کند. در صورت شناسایی عملیات مخرب یا ناهنجاری، PT ISIM یک هشدار ایجاد کرده و ترافیک خام را برای بررسی‌های بعدی ذخیره می‌کند. سپس می‌تواند سیستم SIEM در SOC، مانند MaxPatrol SIEM، را مطلع سازد.

8000+

۸۰۰۰ قانون و شاخص تهدید صنعتی به‌صورت از پیش آماده موجود و قابل استفاده برای زیرساخت‌های ویندوز و لینوکس هستند



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