positive technologies

PARSPOUYA
NETWORK SECURITY SERVICES

# 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

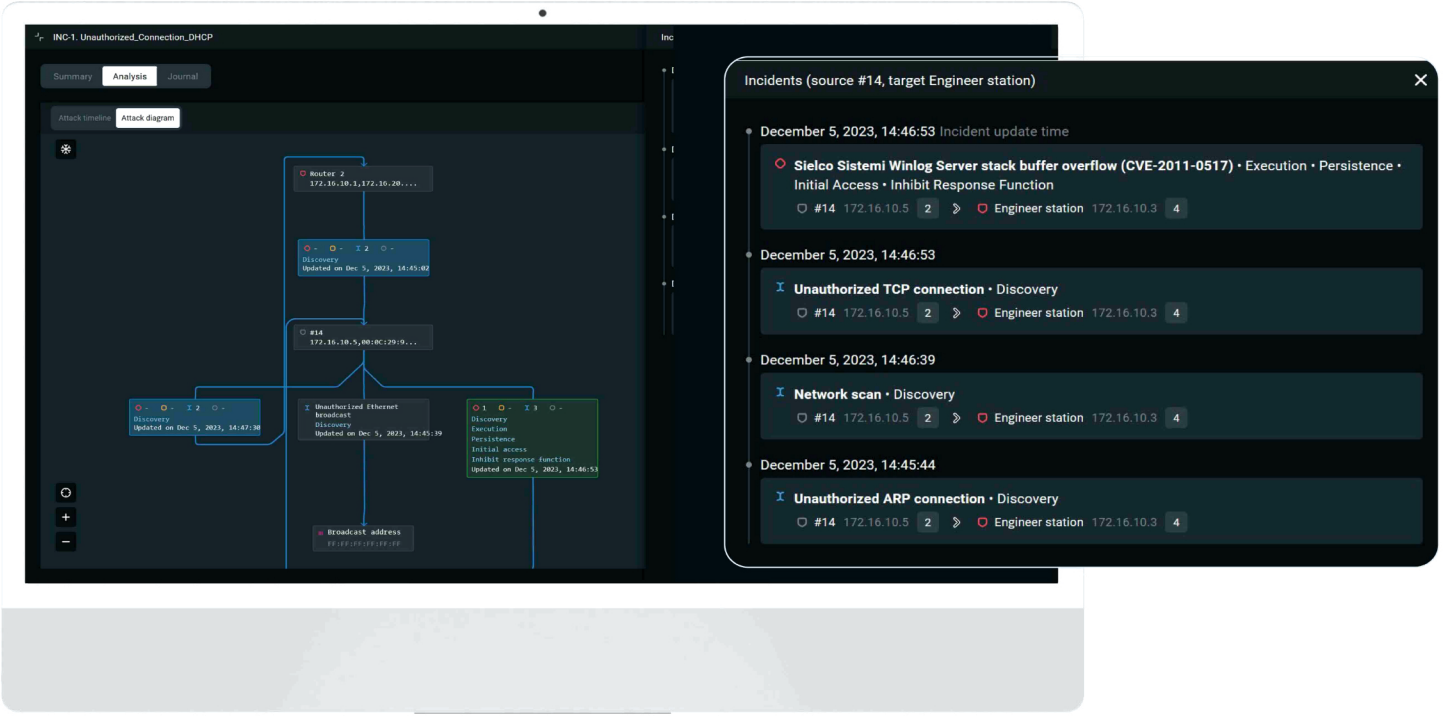
PT ISIM یک سیستم تحلیل عمیق ترافیک برای شبکه‌های OT است که بازرسی دقیق ترافیک را برای پروتکل‌های عمومی و خاص شبکه صنعتی انجام می‌دهد. با نظارت بر ترافیک در محیط خارجی و داخل شبکه کنترل صنعتی، PT ISIM عملیات مخربی را که ممکن است برای فرآیندهای عملیاتی خطرناک باشند شناسایی کرده و اطلاعات ضروری برای بررسی رخدادهای امنیتی را فراهم می‌کند. PT ISIM به پایگاه داده اختصاصی خود از تهدیدات سایبری صنعتی، یعنی شاخص‌های تهدید امنیت صنعتی (PT 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 با 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**

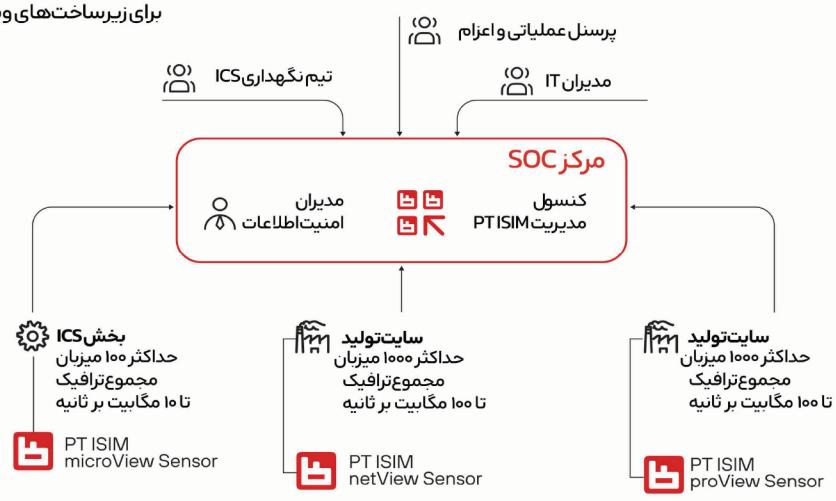
رابط یکپارچه برای نظارت، مدیریت و به روزرسانی مرکزی چندین سنسور ISIM View متصل. معمولاً در سطح SOC یا مرکز داده مستقر می‌شود. مرکز Overview رخدادها را از تمامی سنسورهای متصل دریافت می‌کند.

## 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





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