# AUTOFOCUS

سرویس تهدید اطلاعات متنی Palo Alto Networks® AutoFocus™تحلیل تهدید را همراه با متن کامل ارائه می‌دهد، که تنها برای کارکنان امنیتی تخصصی، برای هر سازمان امنیتی در دسترس است. این سرویس‌دهندگان سرویس امنیتی با اطمینان از اطلاعات هوشمند، همبستگی، متن و جریان‌های خودکار، با پیشگیری مورد نیاز برای شناسایی و پاسخ به وقایع به صورت بلادرنگ، امنیت سایبری را ارائه می دهند.

## تسلیحاتی که اطلاعات شما را تهدید می کند

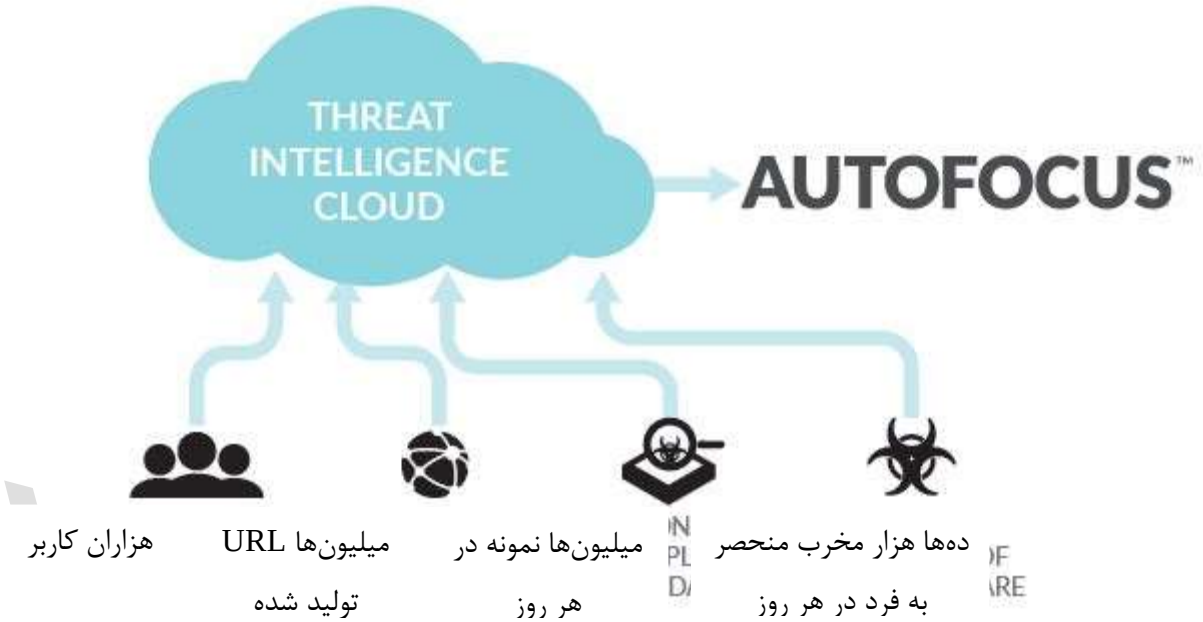
- تهدید اطلاعات فوق محرمانه در صفر روز از طریق ادغام محلی با مجموعه داده های WildFire.
- واحد ۲۴، تیم تحقیقاتی تهدید شبکه های Palo Alto، شامل اطلاعات مخربی درباره خانواده، مخالفان، مبارزات، رفتارهای مخرب و سوء استفاده.
- جمع آوری و همبستگی هر تهدید اطلاعاتی توسط شخص ثالث با استفاده از MineMeld برای AutoFocus از جمله استخراج خودکار و به اشتراک گذاری شاخص‌های با ارزش برای پیشگیری.
- گسترش پلت‌فرم امنیتی Palo Alto، با مفهوم تهدیدی برای AutoFocus که در PAN-OS و Panorama، مانند API باز برای ادغام سیستم‌های شخص ثالث در دسترس است.

## گسترش پلت‌فرم شبکه Palo Alto

تیم های امنیتی با هشدارها و تهدید اطلاعات احاطه شده اند و زمان لازم برای پیگیری هر رویدادی را ندارند، به جز تحقیق درباره حملات پیشرفته و هدفمند. مسأله کمبود اطلاعات نیست، بلکه ناتوانی در جلوگیری از تهدیدات شدید اطلاعات و بدست آوردن پیشگیری خودکار برای تهدیدات فعلی است که شما دارید. این حقیقت جدید مستلزم رویکرد پیشگیرانه‌ای است که به

طور خودکار حملات سایبری موفق را متوقف می‌کند در حالی که فرایند شناسایی، پاسخ و پیشگیری تهدید اطلاعات و ابزار تهدیدآمیز را سرعت می‌بخشد.

AutoFocus ، پلت‌فرم امنیتی نسل بعدی شبکه های Palo Alto را برای تهدید اطلاعات داخلی، صنعتی و جهانی با زمینه تهدیدی برای سرعت بخشیدن جریان‌های تحلیلی، قانونی و پیشگیرانه ارائه می‌دهد. به علاوه، پلت فرم و AutoFocus به تیم‌های امنیتی اجازه می‌دهند تا روش‌های قدیمی را متوقف کنند که بر ادغام هشدارها و تمرکز بر تشخیص و کاهش پس-رویداد متکی بودند. در حال حاضر، اکثر حملات به طور خودکار با تحلیل پیشگیرانه و به دام انداختن تهدید با استفاده از AutoFocus جلوگیری می‌شوند.



**هشدارهای امنیتی**

AutoFocus تیم‌های امنیتی را قادر می‌سازد تا مهم‌ترین تهدیدات روزمره را در رویدادهای متنی در شبکه شما یا داده‌های عمومی با برچسب‌ها تشخیص دهند. AutoFocus منحصر به فرد، برچسب‌ها رویدادهای تهدیدی را همراه با خانواده‌های مخرب، مخالفان، مبارزات، رفتارهای مخرب و سوء استفاده نشان می‌دهد. هنگامی که Tag با رویدادی در شبکه شما مطابقت دارد، هشدار اولیه از طریق ایمیل، در مجموعه اطلاعات AutoFocus یا از طریق پست HTTP ارسال می‌شود که شامل متن Tag شده است. هشدارها بسیار قابل تنظیم هستند، آنها جریان‌های امنیتی موجود در خود را با اولویت‌بندی و زمینه‌سازی برای مهم‌ترین تهدیدات افزایش می‌دهند.

**برچسب‌ها (Tag)**

Tag با استفاده از اطلاعات متنی کامل، دید شما را به خطرناک‌ترین تهدیدات می‌گشایند. آنها را می‌توان در هر نشان‌گر میزبان یا مبتنی بر شبکه در AutoFocus ایجاد کرد و به شما هشدار می‌دهند که تهدید مشخصی در سازمان یا صنعت شما مشاهده شده است. علاوه بر هشدارهای اولویتی، کلیه Tagها قابل جستجو هستند، به شما اجازه می‌دهند تا بلافاصله با نمونه یا شاخص‌های مخرب ارتباط برقرار کنید. همان‌طور که تهدیدات جدید شناسایی می‌شوند، سازمان شما، جامعه متخصصان جهانی AutoFocus و تیم تحقیقاتی تهدید شبکه های Palo Alto، واحد ۴۲، Tagها را به سرویس اضافه می‌کنند.

**تیم تهدید اطلاعات واحد ۲۴**

AutoFocus ابزار تحلیل اولیه مورد استفاده توسط واحد ۲۴ برای شناسایی تهدیدات جدید، مرتبط کردن داده‌های جهانی، شناسایی ارتباط بین نمونه های مخرب و ایجاد پروفایل‌های طرفدارن یا متخلفان است. شما می‌توانید آخرین تحقیقات واحد ۲۴

را که درباره تشخیص AutoFocus است در اینجا[1] مشاهده کنید. همراه با خدمات، واحد ۲۴ هوش مصنوعی را با ایجاد برچسب‌هایی بر پایه تحقیقاتش به AutoFocus اضافه کرده است که زمینه و اولویت‌بندی را برای شناسایی تهدیدات و گسترش تیم امنیتی‌اش با توجه به دانش خود ارائه می‌دهد.

**جلوگیری از حملات به طور خودکار**

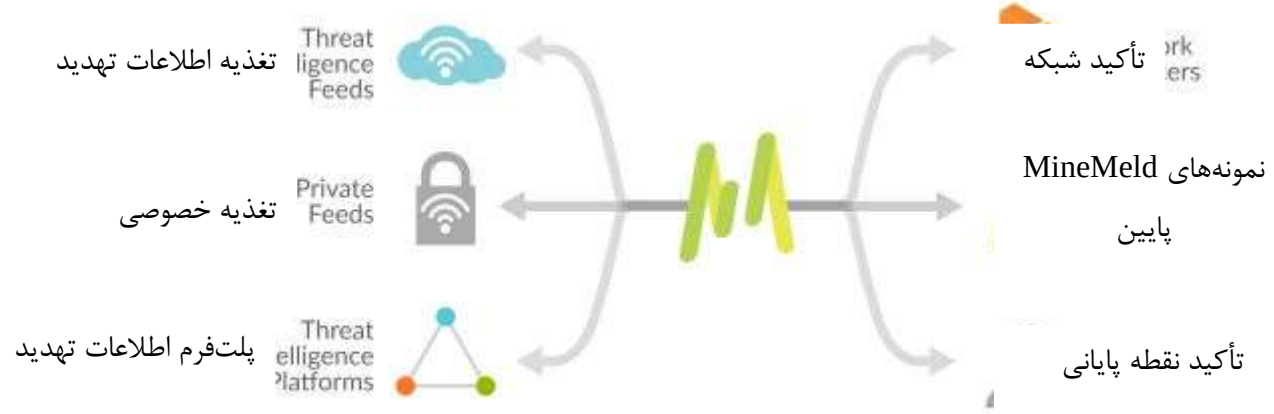
تیم‌های امنیتی نیاز بیشتری به اطلاعات تهدیدی خام دارند- آنها باید به طور خودکار آن را کنترل کرده و به طور عملی از حملات آینده جلوگیری کنند. AutoFocus گردش کار را برای ایجاد و کنترل‌های جدید ساده‌سازی می‌کند، برای هدایت کاربر به طور کاملاً خودکار در پلتفرم امنیتی به صورت یکپارچه عمل می‌کند:

- استخراج کاملاً اتوماتیک برای جلوگیری از شاخص‌های ارزشمند سازشی (IoCs). تیم‌های امنیتی می‌توانند از MineMeld میزبان همراه با AutoFocus به عنوان اهرمی برای استخراج کاملاً اتوماتیک خودکار برای جلوگیری از شاخص‌های ارزشمند سازشی بزرگتر اطلاعات محلی برای خدمات یا منابع اطلاعاتی شخص ثالث استفاده کنند و در شبکه‌های Palo Alto بدون نیاز به دخالت انسانی اجرا کنند.
- نوسان کاربر هدایت شده شاخص های ارزشمند و گروه‌بندی آنها برای صدور به پلتفرم شبکه‌های Palo Alto (با استفاده از لیست‌های بلوکی خارجی سیستم عملیاتی امنیتی PAN-OS® یا گروه‌های آدرس پویا)، یا دستگاه‌های امنیتی شخص ثالث در فرمت CSV استاندارد. هر شاخص را می‌توان از طریق AutoFocus با استفاده از MineMeld به طور مستقیم یا از طریق API جمع‌آوری و صادر کرد.

[1] .https://researchcenter.paloaltonetworks.com/unit42/

## جستجو

در طی یک حمله فعال، سرعت تحقیق و توانایی ارتباط معنی‌دار داده‌ها بسیار مهم است. AutoFocus به شما امکان جستجوی پیشرفته چندلایه را در سطح تصنعی میزبان می‌دهد، و جستجوی شما را با ابتکار در دوره زمانی و سایر فیلترها مورد هدف قرار می‌دهد، به شما اجازه می‌دهد که ارتباطات ناشناخته قبلی را میان حملات حول محور اطلاعات‌تان ایجاد کنید. AutoFocus کلیه اطلاعات مربوط به امنیت اطلاعات شبکه‌های Palo Alto و همچنین منابع شخص ثالث را در اختیارتان قرار می‌دهد و زمان لازم برای تحلیل و بررسی‌های قانونی یا تلاش برای تسخیر را به طور چشم‌گیری کاهش می‌دهد.




## برنامه MineMeld

بسیاری از سازمان‌ها به منابع تهدید اطلاعاتی چندگانه متکی هستند تا از دید وسیع‌تر به وجود آمده اطمینان داشته باشند، اما برای جمع‌آوری، همبستگی، اعتبارسنجی و به اشتراک‌گذاری شاخص‌ها در فیلدهای مختلف تلاش می‌کنند. به عنوان بخشی از

AutoFocus، موتور تهدید اطلاعات هوش مصنوعی MineMeld™ سیستم تهدید یکپارچه را ارائه کرده و تهدید را نشان می‌دهد. تیم‌های امنیتی می‌توانند MineMeld را به عنوان اهرمی برای موارد زیر در نظر بگیرند:

- جمع‌آوری و همبستگی هر منبع اطلاعات شخص ثالث در AutoFocus.
- شناسایی و استخراج خودکار شاخص‌های با ارزش کلیه منابع با استفاده از شاخص‌های ارزشمند هوش مصنوعی محلی برای تأیید استخراج کاملاً اتوماتیک برای جلوگیری از شاخص‌های ارزشمند سازشی.
- تغذیه زمان حقیقی، کنترل‌های مبتنی بر پیشگیری برای پلت‌فرم امنیتی شبکه‌های Palo Alto برای اجرا.
- ایجاد اطلاعات تهدید برای به اشتراک‌گذاری ساده برای سرویس‌های خدمات شخص ثالث یا شرکای مورد اعتماد.

**موتور تحلیل آماری**

هنگام تحلیل تهدید، تیم‌های امنیتی باید سریعاً مشخص کنند که کدام شاخص‌ها بهترین مسیر را برای پژوهش‌های بیشتر ارائه می‌دهند. هر فایل به طور بالقوه دارای صدها و هزاران اثر با تعداد کم و منحصر به فرد استخراج کاملاً اتوماتیک برای جلوگیری از شاخص‌های ارزشمند سازشی است که می‌توانند به نمایه بزرگتر دشمن یا حملات مرتبط متصل شوند. AutoFocus از موتور تحلیل آماری استفاده می‌کند، با همبستگی میلیاردها محصول تصنعی در مجموعه داده‌های کلی، شاخص‌های ارزشمند مرتبط با حملات فعال را به ارمغان می‌آورند. این سرویس به طور خودکار یک سیستم وزنی بصری منحصر به فرد برای شناسایی استخراج کاملاً اتوماتیک برای جلوگیری از شاخص‌های ارزشمند سازشی منحصر به فرد و ضروری است که هدایت تحلیل، پاسخ و اقدامات پیشگیری کمتر از مسیر مربوطه را اجرا می‌کند.

**گسترش پلت‌فرم با اطلاعات تهدید**

AutoFocus به جای آن‌که به گروه کوچکی از متخصصان عملیات امنیتی بسیار تخصصی متکی باشد، کل تیم امنیت فناوری اطلاعات را به شکارچیان پیشرفته تهدید تبدیل می کند. اطلاعات تهدید خدمات به طور مستقیم ساخته شده که در پلت‌فرم شبکه‌های Palo Alto، از جمله PAN-OS و مدیریت امنیت شبکه Panorama™ در دسترس هستند. AutoFocus سرعت گردش کار موجود را در تیم امنیت افزایش می‌دهد و اجازه می‌دهد تا تحقیق اساسی در فعالیت‌های مشکوک انجام شود. هنگامی که تحلیل بیشتری مورد نیاز است، کاربران می‌توانند میان AutoFocus و PAN-OS یا Panorama، همراه با جستجوهای پیش جمعیت برای هر دو سیستم، جستجو کنند.

با استفاده از AutoFocus و پلت‌فرم، کاربران می‌توانند از موارد زیر مطمئن شوند:

- چگونگی تهدید یا تهدید منحصر به فرد مشاهده شده در یک شبکه
- نمونه‌های مخرب مرتبط برای بررسی بیشتر.
- تاریخچه وضوح دامنه برای شناسایی پرونده‌های DNS مشکوک.

**منابع اطلاعاتی و معماری AutoFocus**

AutoFocus در محیط محاسباتی توزیع شده در محدوده وسیعی ساخته شده است که در ابر اطلاعاتی تهدید شبکه‌های Palo Alto میزبان قرار دارند. بر خلاف سایر روش‌ها، این سرویس اطلاعات تهدید شده را به صورت کاملاً اتوماتیک برای جلوگیری از شاخص‌های ارزشمند سازشی قابل دسترس و قابل اجراست و فراتر از ارائه گزارش خلاصه شده عملیات از منابع مختلف در داشبورد است. AutoFocus دارای چشم‌انداز بی‌نظیر با بینش جمعی هزارن شرکت جهانی ارائه دهنده خدمات نسبت به تهدید است، دولت‌ها خدمات را دریافت می‌کنند. این اطلاعات به صورت تفکیک شده بدست می‌آیند

- سرویس تحلیل تهدید مبتنی بر ابر WildFire™ (بزرگترین محیط تحلیل بدافزار در صنعت)
- فیلتر URL با PAN-DB
- برنامه MineMeld
- حفاظت نقطه پایانی پیشرفته Traps™
- سرویس امنیتی Aperture™ SaaS
- اطلاعات تهدید واحد ۲۴ و گروه تحقیقاتی
- شرکای فناوری مانند Proofpoint™
- شبکه DNS منفعل جهانی شبکه‌های Palo Alto

AutoFocus شامل میلیاردها نمونه و جلسه است، از جمله میلیاردها مصنوعات که بلافاصله برای تحلیل امنیتی و تلاش‌های واکنشی اقدام می‌کنند.

**یکپارچگی‌های شخص ثالث ساده**

تحلیل تهدید، بررسی‌های قانونی و تیم‌های واکنش به حادثه اغلب به طیف وسیعی از متن‌ها، ابزارهای منبع باز، ابزارهای امنیتی و خدمات برای بررسی حوادث احتمالی تکیه دارند.

AutoFocus می تواند از طریق موارد زیر، زمان لازم برای بررسی خدمات شخص ثالث را به طور چشم‌گیری کاهش دهد:

- **MineMeld**: تهدیدات اطلاعات هوشمند سفارشی همراه با MineMeld با منابع اطلاعتی AutoFocus و هر ارائه‌دهنده شخص ثالث ارائه می‌شود که به راحتی می‌توانند توسط سایر سیستم‌های امنیتی مورد استفاده قرار گیرد.

- **AutoFocus API**: در چارچوب RESTful برای استفاده آسان ساخته شده است، AutoFocus API اجازه ادغام ساده صدها نمونه، از قبیل تغذیه هوشمند ابزار اطلاعات امنیتی موجود و مدیریت رویداد (SIEM)، ایجاد داده‌های دردسترس برای تحلیل تهدید اضافی یا اتوماسیون تهدید- توقف خودکار را می‌دهد.
- **قابلیت جابجایی از راه دور**: کاربران AutoFocus به طور غیرمستقیم از خدمات برای شبکه‌های Palo Alto و سیستم‌های خارجی شخص ثالث، می‌توانند به طور مستقیم از AutoFocus، عبور کنند. تیم‌ها می توانند ۱۰ سیستم خارجی را تعریف کنند، به طوری که بتوانند به طور یکپارچه کل زیرساخت‌های خود را تحلیل کنند، مانند پیوند متن‌های مربوط به دیوارهای آتش نسل بعدی یا جستجو در ابزار اطلاعات امنیتی موجود و مدیریت رویداد.
- فرمت داده STIX™: AutoFocus ادغام خارج از محفظه را با زیرساخت STIX همراه با داده‌های موجود برای صدور در قالب داده‌های STIX ارائه می‌دهد.

**حفظ حریم خصوصی**

برای جلوگیری از دسترسی به اطلاعات حساس یا قابل شناسایی، AutoFocus دارای حریم خصوصی و کنترل‌های امنیتی است. این سرویس به کاربران اجازه می‌دهد تا تنها اطلاعات مربوط به سازمان خود را با مکانیزم اختیاری «انتخاب» در اختیار شما قرار دهند تا داده‌های ناشناس را با دیگران به اشتراک بگذارید. AutoFocus اجازه دسترسی به هر گونه فایل منبع مشتری را در سرویس نمی‌دهد، تنها ارائه نتایج تحلیل برای نمونه مشاهده شده در هر شبکه مشتری بدون افشای محتوای اصلی. AutoFocus هر منبع اطلاعاتی شخص ثالث را از طریق برنامه میزبان MineMeld به سرویس اضافه می کند که اجازه مشاهده و دسترسی را تنها به سازمان ارسال کننده می‌دهد. می‌توانید اطلاعات بیشتری را درباره ویژگی‌های AutoFocus بدست بیاورید.

## الزامات AutoFocus

AutoFocus به عنوان سرویس امنیتی میزبان ارائه می‌شود که نیازی به تغییرات پیکربندی در دیوار آتش نسل بعدی شبکه‌های Palo Alto ندارد و عملکرد دستگاه را تحت تأثیر قرار نمی‌دهد. برای استفاده از خدمات، مشتریان باید حساب معتبر شبکه‌های Palo Alto را داشته باشند، که شامل افرادی است که دیوار آتش نسل بعدی یا تله‌ها را خریداری می‌کنند. چون AutoFocus به سخت‌افزار وابسته نیست و نیازی به تغییر در دستگاه ندارد؛ نسخه به خصوصی از نرم‌افزار PAN-OS یا سخت‌افزار اضافی مورد نیاز نیست. به اشتراک‌گذاری دیوار آتش (PAN-OS 4.1 یا بالاتر) را برای استفاده کامل از AutoFocus توصیه می‌کنیم.

## صدور مجوز اطلاعات

AutoFocus به صورت اشتراک سالانه در هر مکان ارائه می‌شود. لطفاً برای کسب اطلاعات بیشتر درباره مجوز صدور با شریک یا نماینده فروش شبکه‌های Palo Alto تماس بگیرید