فیلتر کردن URL داده‌های خصوصی

Palo Alto Networks®، TRUSTe® را ارائه می‌دهد که مدیریت رسیک حفظ حریم خصوصی مستقل برای بررسی و مستند سازی جریان داده‌ها و شیوه‌های توصیف شده در این داده‌ها را ارائه می‌کند. هدف از این متن ارائه شبکه‌های Palo Alto همراه با اطلاعاتی برای مشتریان است که برای ارزیابی تأثیر این سرویس بر وضعیت خصوصی کلی آنها با جزئیات نحوه دریافت، پردازش و ذخیره اطلاعات شخصی و درون سرویس مورد نیاز است.

خلاصه‌ای درباره محصول

PAN-DB فیلتر URL سرویس مبتنی بر ابر است که قادر به فیلتر کردن URL با حفظ پایگاه داده اصلی است که در آن URLها بر اساس ارتباطشان با دامنه، جهت و سطوح صفحه دسته‌بندی می‌شوند. اطلاعات موجود در PAN-DB توسط دیوار آتش نسل بعدی شبکه‌های Palo Alto برای شناسایی و فیلتر URLها و جلوگیری از دسترسی به سایت‌های بالقوه خطرناک مورد استفاده قرار می‌گیرند. همچنین PAN-DB به‌روزرسانی سرویس سرویس تحلیل تهدید مبتنی بر ابر WildFire™ را برای اطمینان از جدیدترین دسته‌بندی محتوا برای وب‌سایت‌های مخرب اعمال می‌کند. از طریق ادغام آن با دیوار آتش، PAN-DB، URLها قبلاً دسته‌بندی نشده دیوار آتش را برای تحلیل و دسته‌بندی دریافت می‌کند. سرویس فیلتر URL از طریق جستجوهای محلی در حافظه پنهان URLهای شناخته شده ذخیره شده در دستگاه اعمال می‌شود، همچنین با استفاده از پرس‌وجو پایگاه داده طبقه‌بندی اصلی در ابر در صورت عدم تصمیم‌گیری بر پایه نتایج کشف محلی عمل می‌کند.

اطلاعات پردازش شده توسط PAN-DB

سرویس PAN-DB در ارتباط با دیوار آتش نسل بعدی شبکه‌های Palo Alto اعمال می‌شود. همان‌طور که فیلتر URL از بر روی دیوار آتش عمل می‌کند، برخی از عناصر داده‌ای که ممکن است حاوی اطلاعات شخصی باشند (تعریف شده به عنوان داده‌های مربوط به شناسایی منحصر به فرد، منحصر به فرد قابل شناسایی) جمع‌آوری شده و وارد دیوار آتش می‌شوند، از جمله:

- منبع و آدرس‌های IP و درگاه‌ها (از جمله آدرس‌های NAT).
- نام‌های کاربری مرتط با آدرس‌های IP یا معاملات (در صورت فعال بودن توسط مشتری).
- URLهای قابل دسترس (و هر گونه رجیستر).
- دسته‌بندی URLها (در صورت شناسایی).
- عوامل کاربر (به عنوان مثال، نام دوره شروع برنامه).
- اطلاعات مربوط به دوره (لیست کامل در لینک زیر قابل دسترس است)

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/syslog-field-descriptions

مجموعه پیش تعریف شده یا گزارش‌های فیلتر URL سفارشی کامل توسط مشتری قابل مشاهده هستند که در آن دپارتمان IT آنها با مشاهده در فیلتر URL و فعالیت وب مرتبط از طریق موارد زیر قابل مشاهده است:

- گزارش فعالیت‌های کاربر: گزارش فعالیت کاربر منحصر به فرد کاربردهای مورد استفاده، دسته‌بندی‌های URL مشاهده شده، وب‌سایت‌های بازدید شده و گزارش دقیق کلیه URLهای مشاهده شده در طی دوره را نشان می‌دهد.

- گزارش فعالیت‌های URL: انواع گزارش‌های «بالای ۵۰» که در دسته‌بندی‌های URL مشاهده شده، کاربران URL، وب‌سایت‌های بازدید شده، دسته‌بندی‌های بلوکی، کاربران بلوکی، سایت‌های بلوکی و غیره در دسترس هستند.
- ورود به سیستم در زمان حقیقی: ورودی‌ها را می‌توان از طریق ابزار جست‌وجوی آسان برای استفاده از فیلدهای ورودی و عبارات منظم برای تحلیل ترافیک، تهدید یا ادغام وقایع فیلتر کرد. فیلترهای ورودی را می‌توان برای تحلیل عمیق‌تر و اهداف آرشیوی ذخیره و ارسال نمود. ورودی‌ها را می‌توان به سرور syslog ارسال کرد.

درباره URLهای ذخیره‌نشده، URL، آدرس IP مقصد، و حذف برنامه‌های شناسایی شده به محیط تحلیل مبتنی بر ابر شبکه‌های Palo Alto منتقل می‌شوند.

گزینه‌های حریم خصوصی مشتریان

مشتریان نام‌های کاربری را برای دوره‌ها در دیوار آتش کنترل می‌کنند. قابلیت گزارش‌دهی فیلتر URL اجازه می‌دهد تا گزارش‌هایی را ایجاد کنیم که شامل عناصر ارائه شده توسط دیوار آتش هستند، از جمله گزارش‌های مورد استفاده برای نام‌های کاربری خاص. مشتریان گزینه‌ای برای فعال کردن انظیمان اداری برای جلوگیری از نمایش برخی از نام‌های کاربری خاص دارند. همچنین مشتریان گزینه‌ای برای ارائه گزارش‌های مرور زمان دارند که نشان دهنده میزان اینترنت مصرفی کاربر خاص شامل زمان مصرفی در حوزههای خاص است.

دسترسی و افشا

اطلاعات وارد شده در دیوار آتش ذخیره می‌شود و تنها توسط مدیر سیستم مشتری و کاربران مجاز از نظر مدیر قابل دسترسی است. تیم پشتیبانی شبکه‌های Palo Alto نیز در صورت امکان توسط مدیر سیستم به منظور دستیابی به اطلاعات گزارش می‌توانند به آنها دسترسی پیدا کنند.

در موارد نادر، فرایند طبقه‌بندی URL ممکن است فعالیت‌های غیرقانونی و یا دسترسی غیرقانونی به محتوا (مانند پورنوگرافی کودکان) را کشف کند. در چنین مواردی، شبکه‌های Palo Alto تا حد مورد نیاز یا مجاز توسط قانون قابل اجرا می‌توانند اطلاعات لازم بیشتر را در خصوص وقوع رویداد همراه URL و اطلاعات تماس مشتری بررسی کنند.

نگهداری

زمان نگهداری برای داده‌های ورودی دیوار آتش توسط مدیر سیستم مشتری ایجاد می‌شود. درخواست‌ها برای طبقه‌بندی URLهای بدون رونوشت ارسال شده به PAN-DB به مدت شش ماه حفظ می‌شوند.

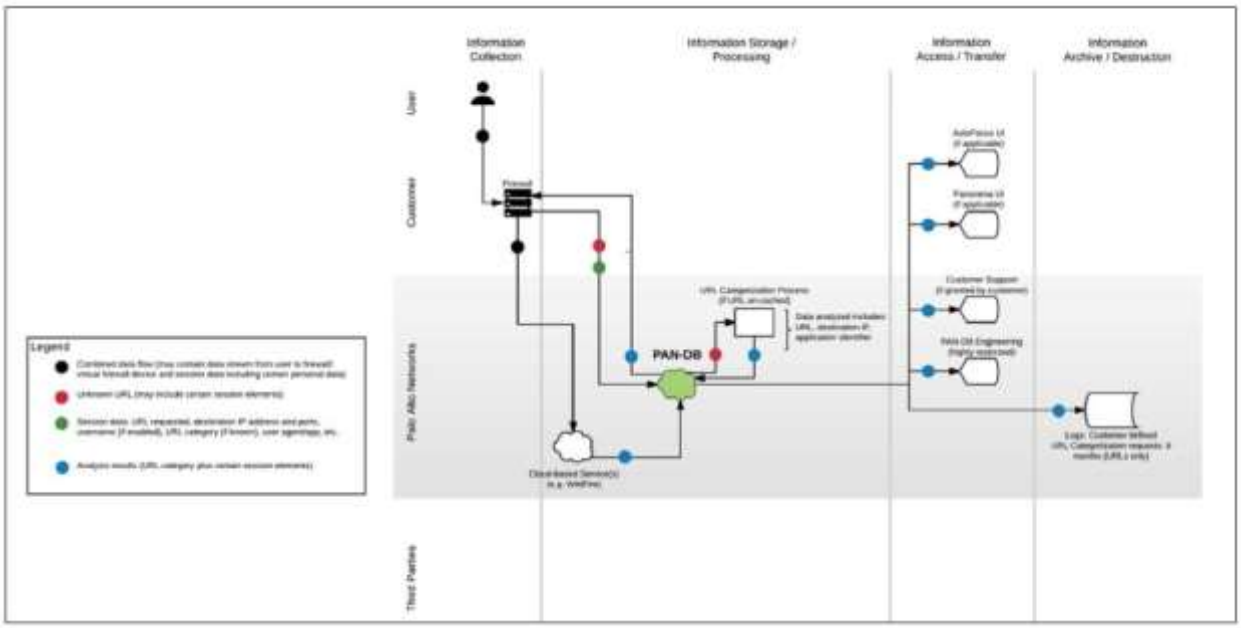
امنیت اطلاعات در PAN-DB

کلیه داده‌های ورودی به صورت محلی بر روی دیوار آتش ذخیره می‌شوند و تنها توسط مدیر سیستم مشتری و کاربران مجاز تعیین شده توسط مدیر قابل دسترس هستند. اطلاعات منتقل شده به PAN-DB در ابر شبکه‌های Palo Alto مانند شبکه‌های Palo Alto دسته‌بندی نشده بیش از ارتباطات SSL رخ می‌دهند.

منابع

- Datasheet – https://www.paloaltonetworks.com/resources/ datasheets/integrated-url-filtering-datasheet
- https://www.paloaltonetworks. com/resources/faq/PAN_AAG_UF_031015
    - در لینک زیر می توان به صفحه نوری فیشینگ دسترسی پیدا کرد.
- https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/url-filtering-pandb

جریان داده



درباره این داده‌ها

اطلاعات موجود در اینجا مبتنی بر بررسی سند و مصاحبه با متخصصان حوزه مربوطه است که در توسعه و بهره‌برداری اطلاعات موجود شرح داده شده است. فرایند کشف بر این عقیده است از صحت اطلاعات ارائه شده اطمینان حاصل شده است؛ TRUSTe ممیزی مستقل انجام نداده و اطلاعات موجود در این صفحه را تأیید نمی‌کند. با این وجود، اطلاعات موجود در اینجا از زمان اولین انتشار در صفحه داده دقیق و کامل بوده است. لطفاً توجه داشته باشید که اطلاعات ارائه شده در این مقاله مربوط به موضوعات فنی یا حرفه‌ای بوده و تنها برای آگاهی عمومی ممکن است تغییر یابد و مشاوره قانونی یا حرفه‌ای را ارائه نمی‌دهد، و برای ضمانت متناسب با هدف خاص یا انطباق با قوانین قابل اجرا مناسب نیست.