Kaspersky Anti Targeted Attack platform
Kaspersky Endpoint Detection and Response

تحول دیجیتال، کلید رشد و اثربخشی نهادی در سراسر جهان است. اما تأمین امنیت زیرساخت های سازمان دیجیتال چالش مهمی است. تهدیدات پیشرفته و حملات هدفمند در بخش های مختلف یک شبکه، پنهان و غیر مستقیم تا زمانی که اجرا شوند، به ریسک های موجود در تحولات دیجیتال می افزایند و رشد کسب و کار را به خطر می اندازند. در حالی که تکنیک های استفاده شده توسط مجرمان سایبری دائما در حال تکامل و به طور فزاینده ای روی محیط های هدفمند متمرکز هستند، بسیاری از سازمان ها هنوز به تکنولوژی های امنیتی متداول متکی هستند تا از تهدیدات فعلی و آینده محافظت کنند.

پلتفرم KATA (Kaspersky Anti Targeted Attack platform)

یک تجزیه و تحلیل رقابتی از محافظت APT در پلتفرم KATA به عنوان لیدر قرار داده شده است. پلتفرم KATA یک شناسایی در تمام لایه ها از حملات هدفمند و تهدیدات پیشرفته در اختیار می گذارد.

سیستم ضد حملات هدفمند

کشف تهدیدات پیشرفته در تمام لایه های زیرساخت فناوری اطلاعات که شامل مجموعه ای جامع از فناوری ها برای شناسایی تهدیدات ناشناخته و حملات هدفمند و ارتباط بین شاخص های مختلف در شبکه برای کمک به کسب و کارها (برای کشف پیچیده ترین حملات) می باشد.

در اختیار قرار دادن یک استراتژی چند لایه و سازگار

پلتفرم KATA قسمتی از یک رویکرد یکپارچه و سازگار برای دستیابی به امنیت است. کنترل دائم ترافیک شبکه و تحلیل رفتار دستگاه ها یک دید کامل و گسترده درباره اتفاقات پیرامون تجهیزات IT شرکت ها در اختیار افراد قرار می دهد. این رویکرد امنیتی سازگار، از شرکت ها در مقابل تهدیدات پیچیده ، حملات هدفمند و بدافزارهای جدید که شامل باج افزارها و جاسوس افزارها و APTها می باشد محافظت می کند.

KATA یک شناسایی دقیق از تهدیدات پیچیده و یک بررسی و تحقیق گذشته نگر را فراهم می کند.

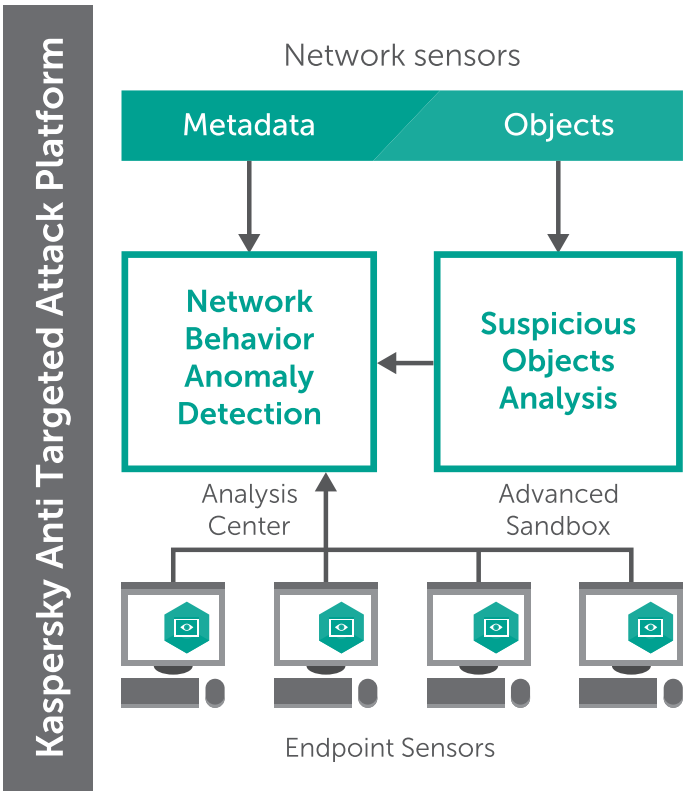
بررسی رفتارهای مشکوک و کشف APT

برای انجام بررسی و تحلیل های چند لایه برروی رفتارها ، KATA شامل موارد زیر می باشد :

- سنسورهای شبکه که ترافیک شبکه را با فعال کردن نشانگر شناسایی حملات سایبری مانیتور می کند.
- سنسورهای ایمیل که به صورت بالقوه رفتارهای مشکوک مخرب را از پیوست ایمیل ها جدا می کند.
- تکنولوژی پیشرفته Sandbox یک محیط مجازی و امن فراهم می کند، جایی که رفتارهای مشکوک در شبکه ، ایمیل و سنسورهای وب می توانند مورد مطالعه قرار بگیرند.
- سنسورهای وب که رفتارها را از ترافیک وب با استفاده از پروتکل ICAP جدا می کند.

اطلاعات شبکه ها و سنسور دستگاه ها با هم ترکیب می شوند و سپس با آنالیزور حملات هدفمند مقایسه می شود تا فعالیت های مشکوک را شناسایی کند و به شما در فراهم کردن امنیت تیم خود با استفاده از هشدارهای دقیق و منظم کمک کند.

Sandbox پیشرفته به تکنولوژی های متعددی تجهیز شده است که از بدافزارها در قبال شناسایی شدن جلوگیری می کند. بنابراین بدافزارها نمی توانند به صورت اتوماتیک فعالیت خود را متوقف کنند چرا که موجب انتشار اطلاعاتی درباره فعالیت آنها می شود.



مشاهده رفتار مشکوک و غیر نرمال

برای نشان دادن تحلیل رفتاری شبکه های پیشرفته، KATA شامل موارد زیر می باشد:

- سنسور دستگاه ها که اطلاعاتی درباره فرایند شبکه های فعال را جمع آوری می کند.
- سنسورهای شبکه که از فعالیت های اینترنتی و ترافیک IPاهای اولیه برای ازبین بردن فراداده ها جلوگیری می کند.

یک آنالیزور حملات هدفمند یک درک از الگوی رفتاری نرمال را به وجود می آورد و سپس با مانیتور سنسورهای فراداده شبکه و اطلاعات دریافتی از سنسور دستگاه ها، انحراف و نابسامانی های موجود در شبکه را شناسایی می کند.

یک راه حل امنیتی قابل اطمینان برای حفظ کامل حریم خصوصی

برای شرکت ها با سیاست های سخت و محکم، تجزیه و تحلیل در داخل شرکت ها بدون جریان داده های خروجی از طریق ادغام با شبکه امنیت خصوصی کسپرسکی انجام می شود.

نصب به موقع به روزرسانی ها به حفظ کامل اطلاعات سازمان ها کمک می کند.

KATA در سطح شبکه ارائه می دهد:

- کشف رخدادهای چند بعدی و همبستگی رویدادی
- جلوگیری از تهدیدات مبتنی بر ایمیل
- ادغام با راه حل های امنیتی شبکه برای تجزیه و تحلیل ترافیک و به اشتراک گذاری تصمیمات

در طول سه فصل جاری، راهکارهای آزمایشگاه کسپرسکی ۱۰۰% تهدیدات را شناسایی کرد و خطای ۰% را تولید کرد.

https://www.icsalabs.com/product/kata

۷/۲۴ حذف تهدیدها - سرویس محافظت مدیریت شده کسپرسکی

- شرکت ها را قادر می سازد تا دنبال تخصص حرفه ای در نابودی تهدیدات باشند و منابع خود را با مهارت و تجربه نابودکنندگان تهدیدات گسترش دهند.
- بررسی داده های جمع آوری شده در محیط های سازمانی
- اطلاع سریع به تیم امنیتی سازمان ها - در صورت شناسایی فعالیت های مخرب
- ارائه راهکار در مورد چگونگی پاسخ و مقابله با تهدیداتف

KEDR (Kaspersky Endpoint Detection and Response)

شناسایی و پاسخ با مدیریت متمرکز رخدادها در تمام Endpoint ها در سراسر شبکه. نتیجه، یک گردش کار یکپارچه است که طیف گسترده ای از پاسخ های اتوماتیک را در اختیار شما قرار می دهد و به جلوگیری از خرابی های گرانقیمت و افزایش بهره وری نسبت به روش های قدیمی مانند پاک کردن و بازنویسی کمک می کند.

KEDR در سطح endpoint ها ارائه می دهد:

- کشف تهدیدات پیشرفته
- حذف تهدیدات در زمان واقعی و از طریق بررسی پایگاه داده گذشته نگر
- پاسخ سازگار با یک رابط وب متمرکز در مقابل تهدیدات

فراهم آوردن:

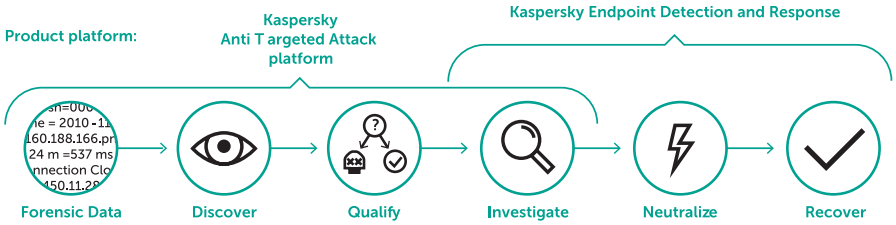
- مجموعه ای جامع از اطلاعات برای توانمند سازی SOC های موجود
- SOC مدیریت شده، ارائه شده توسط کارشناسان آزمایشگاه کسپرسکی
- بررسی های علمی و خدمات پاسخگویی به رخدادها
- پورتال اطلاعات تهدیدها

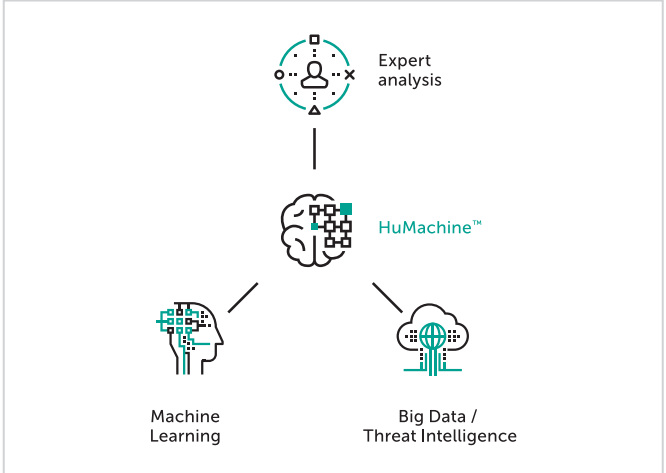
سرویس های امنیت سایبری کسپرسکی

برای کمک به ایجاد مهارت ها و تجربه های تیم امنیتی IT در داخل کشور، ما همواره آماده هستیم که با تخصص و دانش عمیق خود با ارائه دسترسی به آخرین اطلاعات تهدیدات و واکنش سریع به رخدادها با کمک تیم های نابودکننده تهدیدات، از شما حمایت کنیم.

نسخه رایگان

نسخه آزمایشی را نصب کنید و بیابید که چرا تنها Cybersecurity حقیقی، تکنولوژی های پیشرفته را با Machine Learning ترکیب می کند تا از کسب و کار شما در مقابل تمامی تهدیدها محافظت کند. جهت دریافت نسخه آزمایشی به شرکت داده پردازان دوران، نمایندگی رسمی و پلاتینیوم این کمپانی در ایران مراجعه کنید.





شرکت داده پردازان دوران

نماینده رسمی آنتی ویروس کسپرسکی در ایران

آدرس : تهران، خیابان شهید بهشتی، خیابان صابونچی، کوچه ایازی، پلاک ۶۲

سایت: www.douran.com

ایمیل: sales@douran.com

www.kaspersky.com