kaspersky BRING ON THE FUTURE

تشخیص و پاسخ بهینه نقطه پایانی کسپرسکی

دفاع نقطه پایانی خود را به سطح بعدی ببرید و بدون هیچ زحمتی با تهدیدات فراری مقابله کنید.

وقت آن است که یک سطح را بالا ببریم. شما نه تنها آماده هستید که از سازمان خود با فناوری های رایج ضد بدافزار محافظت کنید، بلکه برای شناسایی، تجزیه و تحلیل و به طور موثر آن تهدیدهایی را که عمداً برای فرار از حفاظت سنتی طراحی شده اند، و آماده به انجام بدترین کارهای خود را در اعماق سیستم های خود دفن کنید.

ابزارهای سیستم قانونی در حدود ۳۰ درصد از حملات موفقیت آمیز برای راه اندازی اسکریپت ها و برنامه ها، بارگیری بارها، اسکن شبکه ها یا دسترسی از راه دور به میزبان آلوده استفاده می شود.
گزارش تحلیلگر واکنش به رویداد، کسپرسکی، ۲۰۲۰

اختلال بدتر

امنیت سایبری در بیشتر موارد مربوط به یافتن تعادل بهینه بین منابع موجود و بالاترین سطح حفاظتی است که به طور واقع بینانه قابل دستیابی است. و زمان متخصص IT شما یکی از کمیاب ترین منابع است.

زیرساخت های پیچیده

امنیت سایبری در بیشتر موارد مربوط به یافتن تعادل بهینه بین منابع موجود و بالاترین سطح حفاظتی است که به طور واقع بینانه قابل دستیابی است. و زمان متخصص IT شما یکی از کمیاب ترین منابع است .

یافتن تعادل

بدافزارها، باج‌افزارها، جاسوس‌افزارهای مالی و سایر تهدیدها برای فرار از شناسایی هوشمندتر می‌شوند و نصب حملات ارزان‌تر می‌شود. بنابراین خطر یک حمله جدی بیشتر از همیشه است، همانطور که سطوح آسیب و اختلال در آن وجود دارد..

پاسخ

Kaspersky Endpoint Detection and Response (EDR) Optimum به شما کمک می کند تا با ارائه تشخیص پیشرفته با کاربری آسان، بررسی ساده و پاسخ خودکار، تهدیدات فراری را شناسایی، تجزیه و تحلیل و خنثی کنید.

حتی در حملات موفقیت آمیز، در صورت پاسخ سریع به نقض، ضررهای مالی ۳۲ درصد کمتر بود.
گزارش تحلیلگر واکنش به رویداد، کسپرسکی، ۲۰۲۰

ساده و کارامد

Kaspersky EDR Optimumبرای تیم‌های امنیت سایبری کوچکتر با منابع محدود ساخته شده است که به دنبال ارتقای قابلیت‌های پاسخگویی به حوادث هستند.
عملکرد برای حداکثر بهره وری و حداقل نیروی انسانی بهینه شده است و با اتوماسیون و متمرکز کردن کلیه مدیریت ها و ساده کردن گردش کار، از زمان متخصصان امنیتی شما حداکثر استفاده را می برد.

یک راه حل واحد

Kaspersky EDR Optimum قابلیت‌های تشخیص، تجزیه و تحلیل و پاسخ پیشرفته را به اکوسیستم امنیتی Kaspersky می‌آورد و دفاع را در طیف کاملی از نقاط پایانی، از جمله لپ‌تاپ‌ها، سرورها، بارهای کاری ابری و محیط‌های مجازی افزایش می‌دهد. استقرار متمرکز و مدیریت یکپارچه Kaspersky EDR Optimum از ابر یا در محل در دسترس است..

کاملا مسلح و آماده

Kaspersky EDR Optimum بر اساس مکانیسم‌های تشخیص پیشرفته، از جمله یادگیری ماشینی و تجزیه و تحلیل رفتار بهبودیافته، دید عمیقی از تهدیدها، ابزارهای تحلیل و بررسی ساده و پاسخ خودکار به شما می‌دهد. شما می توانید تهدید را ببینید، آن را درک کنید، دامنه کامل آن را آشکار کنید و فورا پاسخ، جلوگیری از اختلال کسب و کاردهید.

مزایای کلیدی

- از خود در برابر تهدیدهای فراری مکرر و مخرب تر محافظت کنید
- از هر نقطه پایانی دفاع کنید: لپ تاپ ها، سرورها، بارهای کاری ابری
- علت اصلی تهدید و چگونگی وقوع آن را درک کنید
- با پاسخ خودکار سریع از آسیب بیشتر جلوگیری کنید
- صرفه جویی در زمان و منابع با یک دفاع ساده و خودکار از هر نقطه پایانی: لپ تاپ، سرور، بار کاری ابری

موارد استفاده مهم از EDR

به سرعت پاسخ دهید

به تهدیدها با یک کلیک یا با یک پاسخ خودکار به محض کشف آنها پاسخ دهید:

- از اجرا و انتشار فایل مخرب در سراسر شبکه در حین یا پس از بررسی خود جلوگیری کنید
- به طور خودکار فایل های مرتبط با تهدیدات فرار را در تمام نقاط پایانی قرنطینه کنید
- به صورت خودکار میزبان های آلوده را با یافتن نشانگر ایزوله کنید
- سازش (IoC) مرتبط با تهدیدی که به سرعت در حال گسترش است

به سوالات حیاتی پاسخ دهید

تهدیدهای فراری اغلب در دید آشکار پنهان می شوند و باید بررسی شوند تا به طور کامل ریشه کن شوند .EDR با یافتن پاسخ به این سوالات کمک می کند:

- آیا در حال حاضر مورد حمله قرار گرفته ام؟
- آیا این حمله در سطح صنعت به زیرساخت های من رسیده است؟
- این تهدید از کجا آمده است؟
- توانسته روی هاست من چه کند؟
- آیا لایه های پنهانی برای این تهدید وجود دارد؟
- آیا سایر نقاط پایانی تحت تأثیر قرار می گیرند؟

تشخیص پیشرفته

تشخیص پیشرفته برای کشف تهدیدات فراری ضروری است:

- تشخیص تهدید رفتار و پیشگیری از سوء استفاده با یادگیری ماشین(ML)
- کتشافی، سوابق هوشمند، فن آوری های مبتنی برML
- شبیه ساز داخلی برای تشخیص رفتار مخرب قبل از اجرا
- جعبه ایمنی برای تجزیه و تحلیل رفتار بهبودیافته) با Kaspersky Sandbox موجود است(
- داده های اطلاعاتی تهدید جهانی که در آزمایشگاه توسط سیستم ها و کارشناسان مبتنی بر هوش مصنوعی جمع آوری و تجزیه و تحلیل شد

حالا شما می توانید کارهای خیلی بیشتری انجام دهید

اکنون می‌توانید دامنه کامل هر تهدیدی که به شما حمله می‌کند و نحوه ایجاد آن در نقاط پایانی خود، با استفاده از تشخیص پیشرفته مبتنی بر یادگیری ماشین و قابلیت مشاهده در شناسایی‌ها، درک کنید. و می توانید اطمینان حاصل کنید که با هر تهدیدی به طور کامل مقابله شده است. هیچ چیز هنوز در جایی در داخل سیستم شما پنهان نشده است و بررسی می کند که چقدر می تواند آسیب برساند.

پاسخ خود را خودکار کنید

در طول بررسی با گزینه‌های «یک کلیک» موجود در کارت حادثه، فوراً به تهدیدات پاسخ دهید یا بر اساس اسکن‌هایIoC ، پس از کشف، پاسخ‌های خودکار را تنظیم کنید. اقدامات پاسخگویی عبارتند از:

- میزبان را جدا کنید
- قرنطینه فایل
- جلوگیری از اجرا شدن
- اسکن مناطق بحرانی

تهدیدات را تحلیل کنید

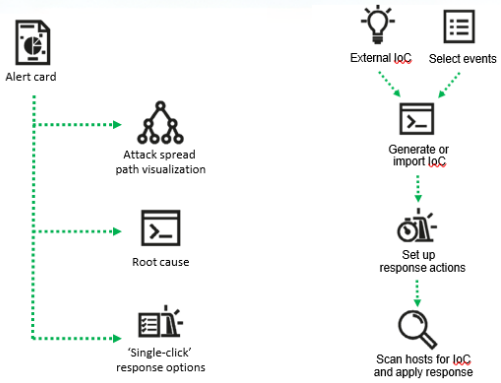
در یک کارت حادثه واحد، داده های غنی شده در مورد شناسایی و یک مسیر گسترش حمله مته به پایین جمع آوری می شود تا تجزیه و تحلیل سریع انجام شود و تصمیمات آگاهانه برای یک "یک کلیک" یا پاسخ خودکار اتخاذ شود. ها را می توان از منابع مطمئن وارد کرد یا بر Ioc اساس تحقیقات به منظور کشف تهدیدهای فراری که در نقاط پایانی در زیرساخت شما پنهان شده اند، تولید شوند.

دفاع از زیرساخت های هیبریدی

زیرساخت های ترکیبی چالش های امنیتی منحصر به فردی و همچنین مزایای قابل توجهی را به همراه دارند. اکنون می‌توانید حفاظت از داده‌ها و زیرساخت‌های خود را برای سرورهای مجازی و فیزیکی، استقرار VDI و بارهای کاری ابر عمومی با عملکرد ضروری EDR افزایش دهید.

با مدیریت متمرکز در تمام نقاط پایانی ترکیبی و بارهای کاری و گردش کار EDR ساده از فضای ابری یا داخلی، از خستگی هشدار اجتناب کنید و از منابع خود استفاده کامل کنید.

حفاظت از نقطه پایانی چند سطحی



فن‌آوری‌های EDR در خلاء وجود ندارند - آنها فقط می‌توانند به طور مؤثر از یک پایه محکم از محافظت نقطه پایانی قوی کار کنند. حفاظت چندسطحی نقطه پایانی تضمین می‌کند که با مدیریت تهدیدات و حوادث کالایی که قبلاً باید توسط نرم‌افزار ضد بدافزار خودکار مقابله می‌شد، حواس شما پرت نشود. به همین دلیل است که Kaspersky EDR Optimum در ارتباط با یکی از آزمایش‌شده‌ترین و پر جایزه‌ترین پلت‌فرم‌های حفاظت نقطه پایانی ما کار می‌کندKaspersky Endpoint Security for Business : و Kaspersky Hybrid Cloud Security

پلتفرم امنیتی Kaspersky Optimum شما

EDR بخشی از اکوسیستمی است که فناوری‌ها، ابزارها و خدمات متعددی را در بر می‌گیرد Kaspersky EDR Optimum :جزء کلیدی Kaspersky Optimum Securityاست، راه‌حلی گسترده‌تر که جنبه‌های مختلف دفاع شما را در برابر تهدیدات فراری تقویت می‌کند، در حالی که منابع شما را آسان می‌کند:

رویکرد مرحله به مرحله

Kaspersky Optimum Securityبر اساس Kaspersky Security Foundations ساخته شده است. اگر و زمانی که برای انجام این کار آماده باشید، می‌توانید با Kaspersky Expert Securityبه راحتی به استفاده از ابزارهای قدرتمندی که در برابر پیشرفته‌ترین تهدیدها محافظت می‌کنند رشد کنید.

Kaspersky Expert Securitv

آمادگی برای حملات پیچیده و مشابهحملات APTبرای مشاغل با:

- محیط های پیچیده و توزیع شدهIT
- یک تیم امنیت IT بالغ یا یک مرکز عملیات امنیتی تاسیس شده(SOC)
- تمایل کم به ریسک به دلیل هزینه های بالاتر حوادث امنیتی و نقض داده ها

Kaspersky Optimum Security

دفاع خود را در برابر تهدیدات فراری ایجاد کنید. ایده آل برای مشاغل با:

یک تیم کوچک امنیت فناوری اطلاعات با تخصص اولیه امنیت سایبری داشته باشید

یک محیط IT که در اندازه و پیچیدگی رشد می کند و سطح حمله را افزایش می دهد

کمبود منابع امنیت سایبری - برخلاف نیاز به حفاظت بیشتر

Kaspersky Security foundation

اکثریت قریب به اتفاق تهدیدها را بطور خودکار مسدود کنید.

پیشگیری خودکار چند بردار از حوادث ناشی از تهدیدات کالا اکثریت قریب به اتفاق همه حملات سایبری

مرحله پایه گذاری برای سازمان ها با هر اندازه و پیچیدگی در ساخت یک استراتژی دفاعی یکپارچه

محافظت از نقطه پایانی قابل اعتماد برای کسانی که تیم های کوچک فناوری اطلاعات و تخصص امنیتی در حال ظهور دارند

تهران، خیابان شهید بهشتی، خیابان پاکستان، کوچه چهارم، پلاک ۱۱، طبقه چهارم، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی: ۱۵۳۱۶۴۵۹۱۸
info@arka.ir | www.arka.ir
رایان سامانه آرکا