kaspersky

Kaspersky Sandbox

TooslIran Co. | Morteza Saremi

051-38458482 | 09151065542

مقدمه :

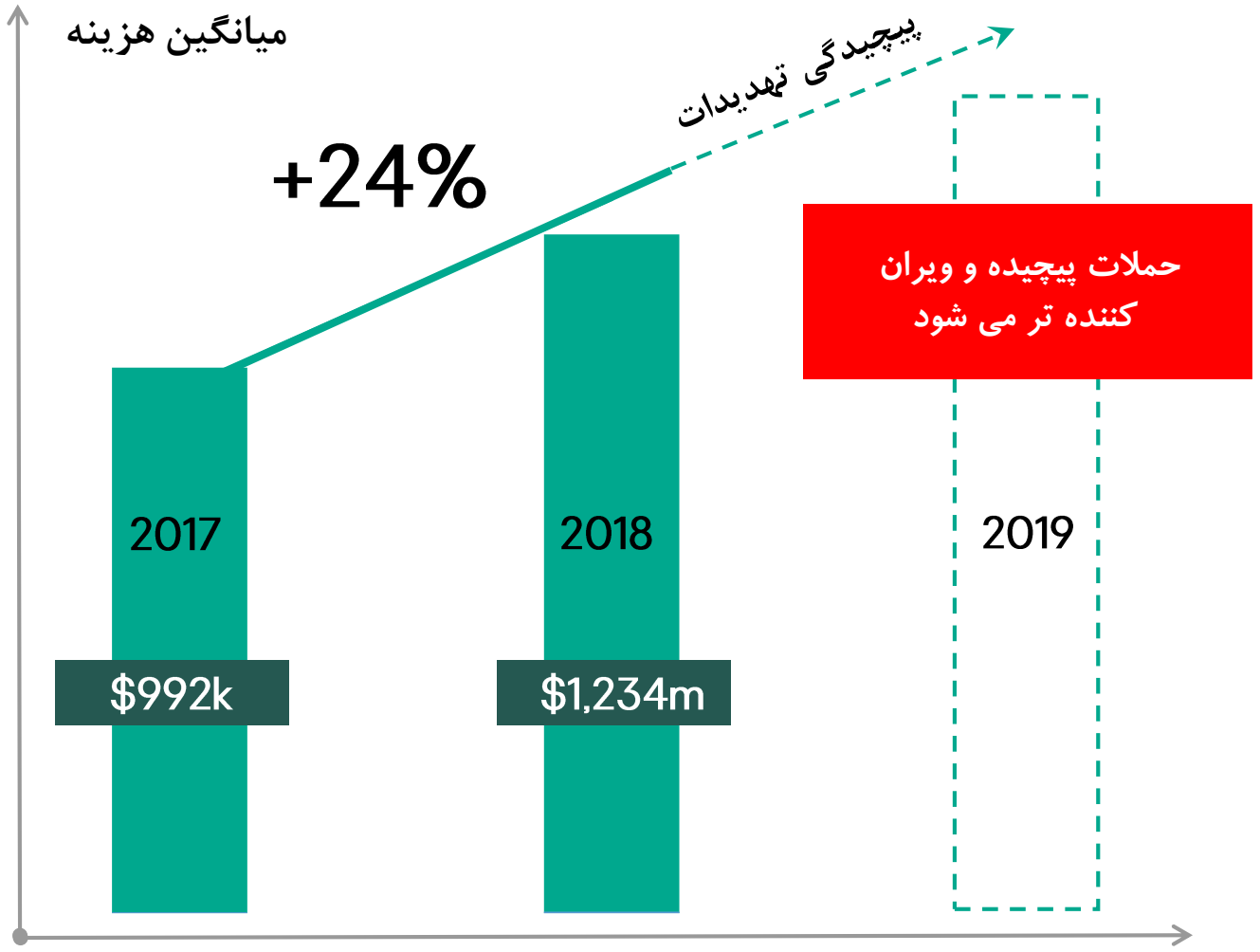
حملات سایبری پیشرفته امروز قدرت فلج کردن شرکت ها و ویرانی فسادهای مالی و اعتباری را دارد. سرقت دارایی های مالی و اسرار تجاری ، از بین رفتن اعتماد به نفس مشتری به دلیل خدمات کاهش یافته و بسیاری از اثرات منفی دیگر که تهدیدات پیچیده ، تأثیر مستقیمی بر ثبات و رونق تجارت شما را دارد.

برای جلوگیری از بروز سریع حملات سایبری ، ابزارهای سنتی طراحی شده برای محافظت از محیط شبکه از جمله آنتی ویروس ها فایروال ها به خودی خود به تنهایی کافی نیستند.

به همین دلیل است که شرکت های آینده نگر باید به طور جدی ابزارهای تخصصی را برای کشف ، تحقیق و واکنش به حوادث پیچیده در نظر بگیرند. که برای این کار نیاز به استخدام نیروهایی با توانایی . تسلط کامل به حوزه امنیت فناوری اطلاعات می باشد که روزانه و هر لحظه در حال آنالیز تمامی ساختار شبکه و اطلاعات رد و بدل شده در آن باشند و علاوه بر آن به تمامی تکنیک های مقابله با تهدیدات پیشرفته آشنایی کاملی داشته باشند.

در ادامه به میانگین هزینه های پرداخت شده در کشور ایران بر اثر حملات باج افزار ها و تهدیدات پیشرفته می پردازیم که به دلیل عدم رعایت مسائل امنیتی مجبور به پرداخت چنین هزینه هایی جهت بازگردانی فایل ها که غالبا قابل برگشت نیستند شدند و یا به دلیل از بین رفتن کامل اطلاعات به علت خراب شدن فایل ها و ساختار پایگاه های داده آن ها که هزینه های غیر قابل جبرانی به آن سازمان تحمیل نموده است.

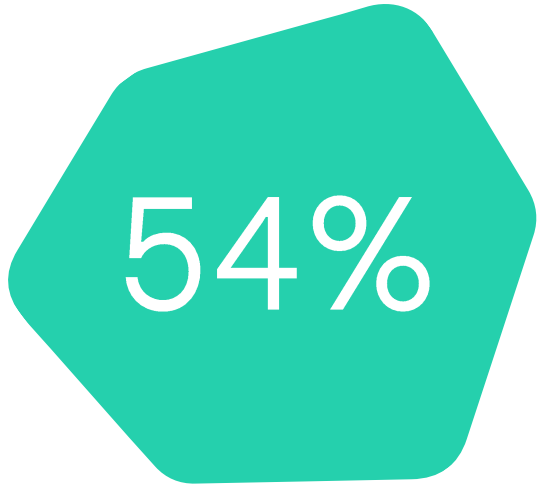
هزینه های پرداخت شده در طی سال های اخیر بر اثر حملات هدفمند



سالانه خسارت های زیادی حملات پیشرفته هدفمند به سازمان ها وارد میکنند و هدف این حملات آسیب به تجارت و حساس ترین نقاط سازمان می باشد. این حملات ماه ها و سال ها وقت خود را برای نفوظ با بیشترین تاثیر برای عملیات خرابکارانه صرف می نمایند.

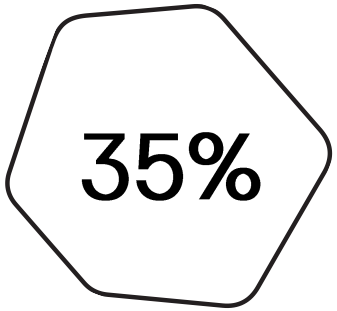
Source: On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives, Kaspersky, 2018

یکی از دلایل اصلی افزایش حملات پیشرفته سایبری کمبود مهارت و آگاهی برای مقابله با حملات هدفمند می باشد.



۵۴ درصد از سازمان ها این را میگویند که پرسنل امنیتی دارند که به اندازه کافی آموزش دیده نیستند.

جرائم سایبری بیش از سه برابر تعداد مشاغل ناخواسته در زمینه امنیت سایبر است که پیش بینی می شود تا سال ۲۰۲۱ به ۳.۵ میلیون نفر برسد



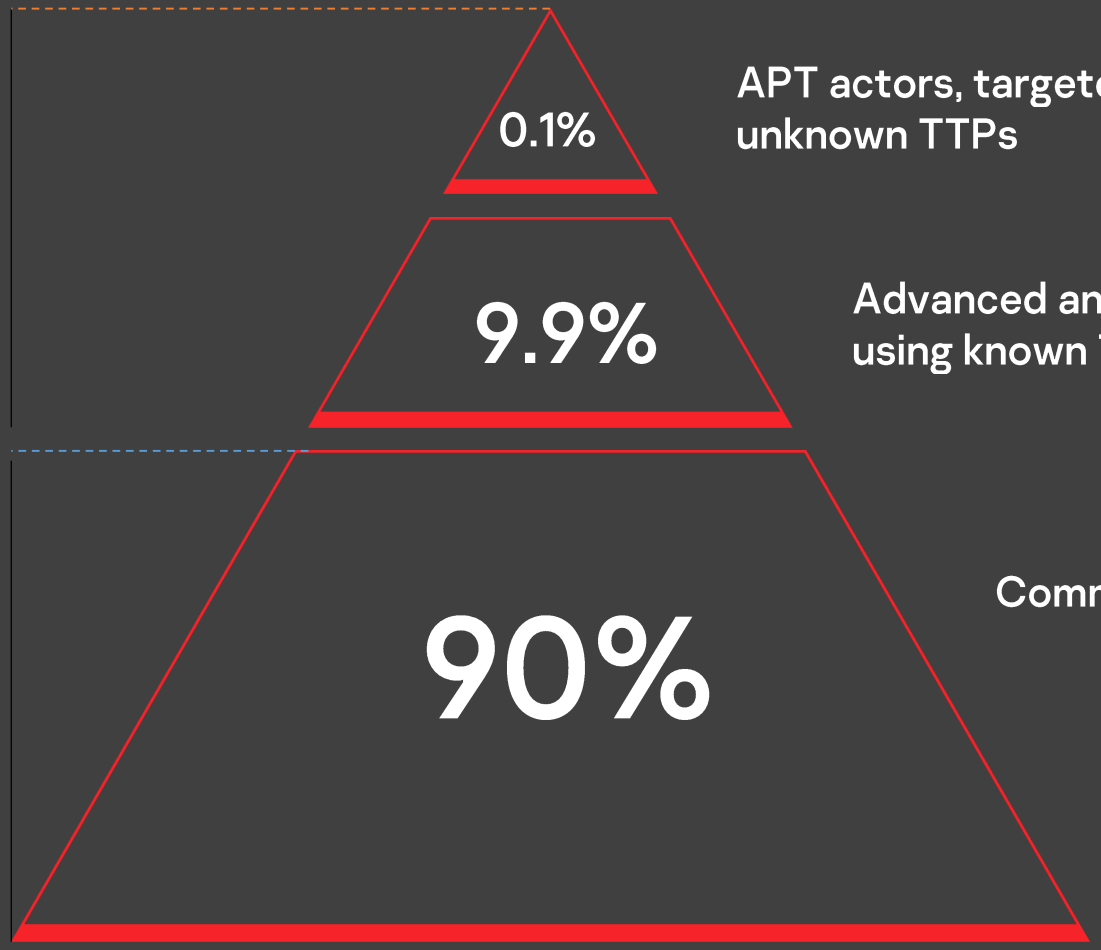
۳۵ درصد از کارمندان شرکت سیسکو فقط در حال آموزش برای دفاع از حملات سایبری هستند،و اولویت اصلی آن ها می باشد.

*FS-ISAC's 2018 Cybersecurity Trends Report
**Surviving the IT Security Skills Shortage, Dark Reading
***Cybersecurity Ventures “Cybersecurity Jobs Report 2018-2021”

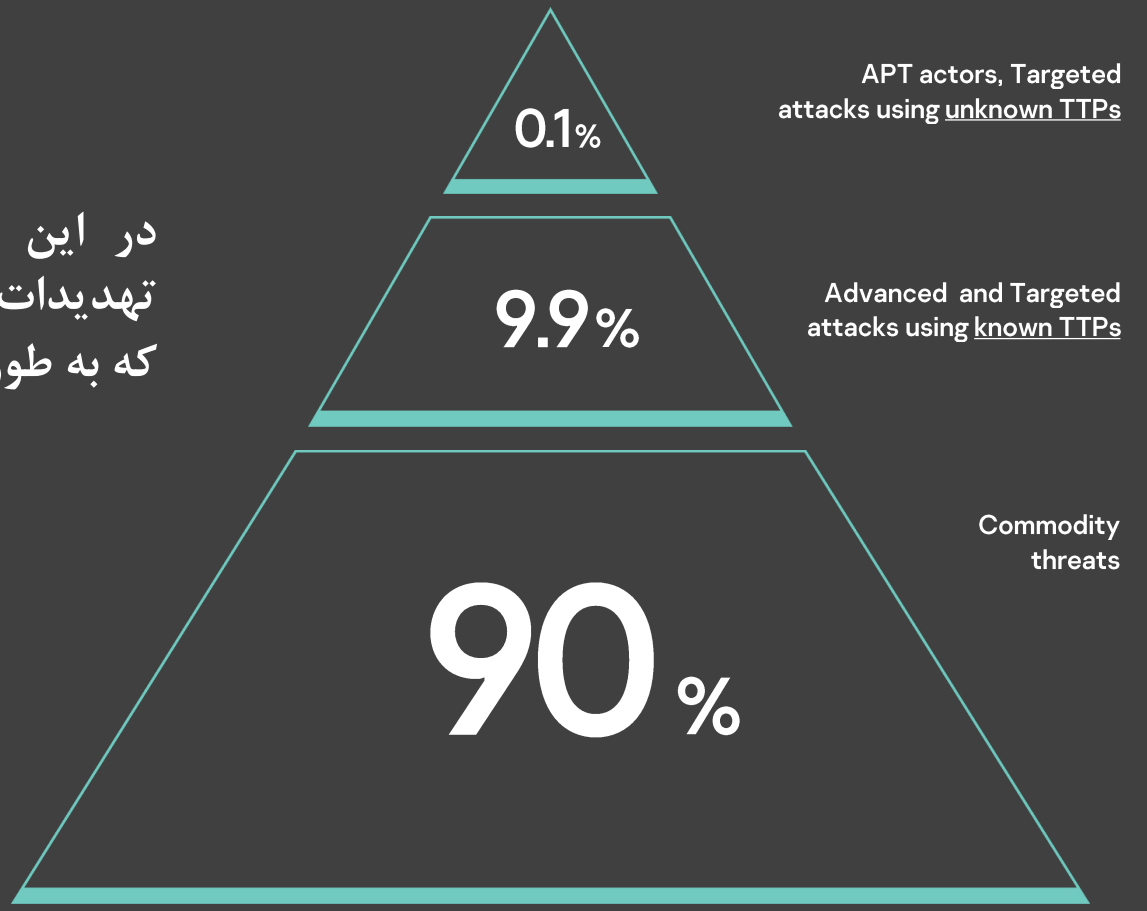
هرم قدرت راه حل های امنیتی:

راه حل های امنیتی مدرن از جمله:
Kaspersky Sandbox

آنتی ویروس ها و دیگر ابزارهای سنتی محافظت



در این قسمت می توانید ببینید که با افزایش تهدیدات نیاز به نیروی متخصص بیشتر خواهد شد که به طور مرتب در حال رصد شبکه سازمان باشد.



تیم امنیتی مسلط و بالغ در حوزه IT و SOC

مدیر امنیت فناوری اطلاعات

مدیر فناوری اطلاعات

معرفی محصول :

Kaspersky Sandbox براساس فناوری ثبت شده (ثبت اختراع شماره B2 ۱۰۳۳۹۳۰۱) به سازمانها کمک می کند تا با تعداد فزاینده و پیچیدگی تهدیدهای مدرن که می توانند از حمایت نهایی نقطه کنونی موجود جلوگیری کنند ، مبارزه کنند.

Kaspersky Sandbox با تکمیل کارایی امنیت Kaspersky Endpoint Security for Business، به سازمانها این امکان را می دهد تا سطح حفاظت از ایستگاههای کاری(کلاینت ها) و سرورهای خود را در برابر بدافزارهای ناشناخته ، ویروسهای جدید و باج افزارها افزایش دهد به طوری که این محصول در تمامی تست های گرفته شده در این زمینه به موفقیت صد در صدی رسیده و تنها محصول بدون هیچ خطایی در این حوزه می باشد.

از ویژگی های منحصر به فرد این محصول پاسخ اتوماتیک به تمامی تهدیدات می باشد به طوری که سازمان ها دیگر نیازی به استخدام کارشناسان حرفه ای امنیت فناوری اطلاعات(SOC) ندارند.

کسپرسکی سند باکس بهترین روش های مبارزه متخصصان با تهدیدات پیچیده و حملات در سطح APT را دریافت کرده، و کاملا با Kaspersky Endpoint Security For Business ادغام می شود، این راهکار از سوی Kaspersky Security Center،به عنوان کنسول مدیریتی یکپارچه سیاست محور ما، مدیریت می شود.

ایجنت Kaspersky Endpoint Securityاطلاعات درباره یک شی مشکوک را از مخزن عملیانی نتایج،که برروی یک سرور کسپرسکی سندباکس قرار دارد، درخواست می کند.(لازم به ذکر است سرور سند باکس تعداد زیادی ماشین مجازی که برروی آن نسخه های مختلف ویندوز نصب و در حال اجرا می باشد که برای متوجه نشدن هکر ها همیشه فایل های آن از جمله فایل ورد،اکسل یا هر نرم افزاری که نشان دهد کاربر فعال می باشد در حال اجرا نیز می باشد)اگر شی مورد نظر بیش از این اسکن شده باشد،KESB نتیجه اسکن را دریافت کرده و یک یا چند گزینه اصلاحی را اعمال می کند:

۱.حذف و قرنطینه

۲.اعلان به کاربر

۳.شروع اسکن نواحی حیاتی

۴.به دنبال شی شناسایی شده برروی ماشین های دیگر در شبکه جستجو می کند.

اگر نتیجه اعتبار یک شی قابل دریافت از مخزن نباشد، ایجنت آنتی ویروس کسپرسکی(KESB) فایل مشکوک را به سند باکس فرستاده و منتظر پاسخ می شود.سند باکس درخواست برای اسکن شی را دریافت کرده، در این نقطه شی مورد آزمایش در یک محیط ایزوله از زیر ساخت حقیقی اجرا می شود.

اسکن فایل درون ماشین های مجازی ،که ابزار های مقلد یک محیط کاری معمول(سیستم عامل ها/برنامه های نصب شده) مجهز شده اند، انجام میشود. برای شناسایی قصد مخرب یک شی،تحلیل رفتاری انجام شده،Artifict ها جمع آوری و تحلیل می شوند،و اگر شی اقدامات مخربی انجام دهد،سند باکس آن را به عنوان بد افزار خواهد شناخت.در طول تحلیل سند باکس،یک نتیجه به شی اختصاص خواهد گرفت.

به محض آنکه روند شبیه سازی شی تکمیل می شود، نتیجه بلادرنگ به مخزن مشترک عملیاتی نتایج ارسال شده،و اجازه می دهد تا دستگاه های دیگری که KESB برروی آن ها نصب است،سریعا اطلاعات مربوط به اعتبار آن شی را بدون آنکه نیاز باشد دوباره تحلیلی روی آن شی صورت گیرد، به دست آورند.این رویکرد از پردازش سریع اشیای مشکوک اطمینان حاصل کرده، بار موجود برروی سرور های کسپرسکی سندباکس را کاهش داده، و سرعت و کارایی پاسخ ها به تهدید را بهبود می بخشد.

Kaspersky Sandbox یک افزودنی ضروری به Kaspersky Endpoint Security for Business است. این راهکار به صورت خودکار تهدیدات پیشرفته، ناشناس و پیچیده را بدون نیاز به منبع اضافی مسدود کرده، و تحلیل گران امنیت فناوری اطلاعات آزاد خواهند بود که بر روی وظایف دیگر تمرکز کنند.

گزینه های تحویل و پیاده سازی: کسپرسکی سندباکس به صورت یک فایل ISO Image با CentOS نسخه ۷ از پیش پیکربندی شده و تمامی مولفه های ضروری راهکار آماده است. می توان آن را بر روی سرور فیزیکی و یا سرورهای مجازی بر پایه VMware ESXI پیاده سازی کرد.

ادغام:

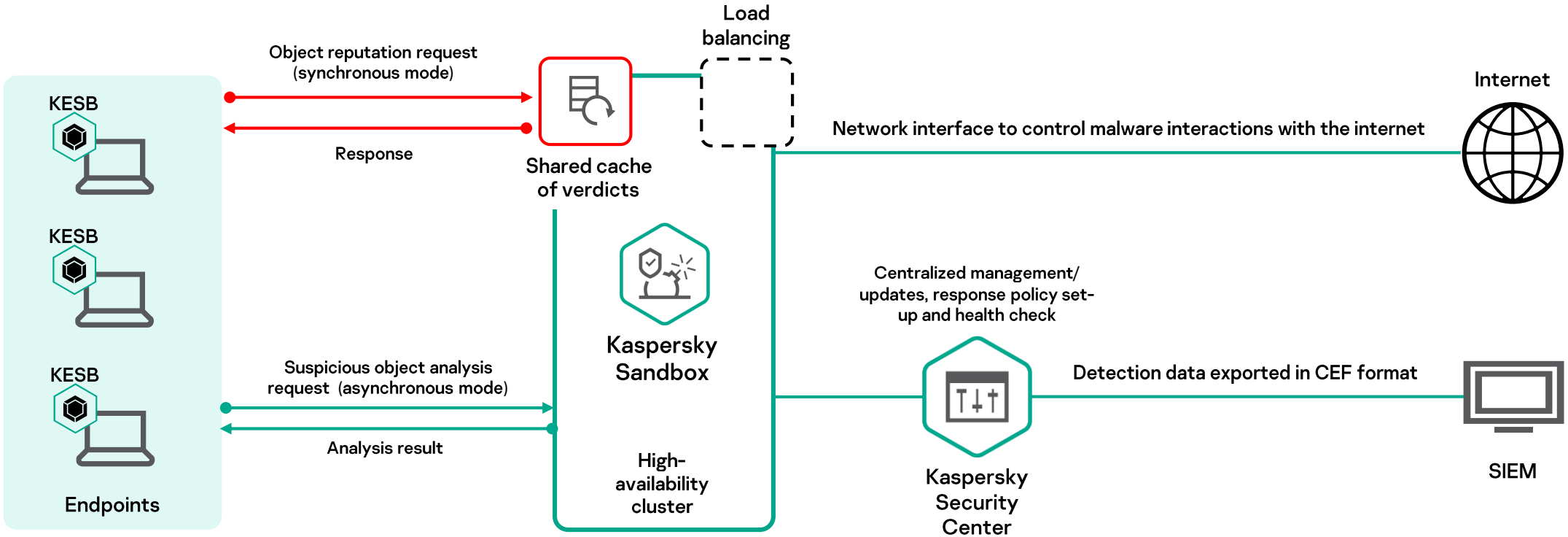
- سیستم های SIEM می توانند اطلاعات مربوط به شناسایی هایی که توسط کسپرسکی سندباکس انجا شده است را دریافت کنند. این اطلاعات از طریق Kaspersky Security Center در قالب جریان رویدادهای معمول ارسال می شود.
- یک API در کسپرسکی سندباکس برای ادغام با سایر راهکار تعبیه شده است. تا بتوان فایل ها رای برای اسکن کسپرسکی سندباکس ارسال و از آن، میزان اعتبار فایل را درخواست کرد.

معرفی محصول :

کسپرسکی سند باکس مناسب است برای :

۱. شرکت هایی بدون تیم امنیت اطلاعات اختصاصی که نقش امنیت اطلاعات را به واحد فناوری اطلاعات محول کرده اند
۲. کسب و کار های کوچکی که نمیخواهند منابع مضاعفی را برای امنیت فناوری اطلاعات متحمل شوند.
۳. ارگان های بزرگی که زیر ساخت آن ها از لحاض جغرافیایی توزیه یافته است و متخصص امنیت فناوری اطلاعات در مجل ندارند.
۴. شرکت هایی که باید اطمینان حاص کنند که تمرکز تحلیل گران تمام وقت امنیت فناوری اطلاعات آن ها کاملا برروی امور حیاتی است.

Kaspersky Sandbox*



* The product is planned to be released in November 2019. The release date is subject to change without notice.

kaspersky

Thank you!

TooslIran.com

kaspersky