مدیران شبکه برنا
Borna Network Managers

برنا، سپر قدرتمند شما

تخصص ما در ارائه راهکارهای پیشرفته امنیت شبکه، از جمله فایروال، DLP، XDR، EDR و سایر محصولات سازمانی است. با سال‌ها تجربه در تامین امنیت زیرساخت‌های IT، خدمات ما پاسخ‌گوی نیازهای پیچیده سازمان‌های بزرگ و دولتی می‌باشد.

www.bornanetwork.co
info@bornanetwork.co
۰۲۱-۷۴۰۲۸

فهرست

مقدمه ۲
آنتـی ویروس ۳
• ESET ۴
• KASPERSKY ۵
• SANGFOR ۶
• Quick Heal ۷
ابـزار DLP ۸
• Safetica ۹
• ZECURION ۱۰
ابـزار PAM ۱۱
• ARCON ۱۲
سـرویس EDR ۱۳
سـرویس XDR ۱۴
• ESET ۱۵
• KASPERSKY ۱۶
• SANGFOR ۱۷
• Quick Heal ۱۸
سـرویس NDR ۱۹
• GREYCORTEX ۲۰
سـرویس DRM ۲۱
• SECLORE ۲۲
ابزار Firewall ۲۳
• FORTINET ۲۴
• SANGFOR ۲۵
مشـتریان ما ۲۶
سـخن پایانی ۲۷

مقدمه

شرکت مدیران شبکه برنا (سهامی خاص) از سال ۱۳۹۷ به مدیریت خانم افسانه خلیلیان و با شماره ثبت ۵۳۲۹۸۰ در اداره ثبت شرکتها به ثبت رسمی رسیده است. مدیریت مجموعه برنا از سال ۱۳۸۸ در حوزه آنتی ویروس و فایروال با ارائه پورپوزال های فنی و فروش به اکثر سازمانهای دولتی و شرکتهای خصوصی، بهترین خدمات و پشتیبانی را ارائه داده اند.

زمینه فعالیت شرکت عبارت است از: انجام فعالیت در حوزه فناوری اطلاعات و ارتباطات شامل کلیه فعالیت های کامپیوتری اعم از تولید و پشتیبانی و بسته بندی نرم افزار و پیاده سازی و پشتیبانی شبکه داده ها و ارائه پشتیبانی بسته های نرم افزاری و بسته ها و فایل های اطلاعاتی تولید داخل و ارائه و پشتبانی نرم افزاری خارجی اس آی و سیستم ها و نصب و راه اندازی سیستم های اتوماسیون اداری و صنعتی و خرید و فروش و واردات و صادرات تجهیزات رایانه و عقد قرارداد با اشخاص حقیقی و حقوقی و اخذ تسهیلات از بانکهای داخلی و خارجی و اخذ تسهیلات از بانکهای داخلی و خارجی و اخذ و اعطای نمایندگی و شعبه به شرکتهای داخلی و خارجی که در حوزه فناوری اطلاعات و ارتباطات فعال می باشد، همچنین شرکت در مناقصات و مزایدات داخلی و خارجی و در زمینه فعالیت شرکت می باشد.

در راستای تحقق برنامه های استراتژیک توسعه فناوری اطلاعات و ارتباطات (ICT) و توسعه صنعت IT کشور و با توکل بر الطاف الهی و بهره گیری از مدیران، کارشناسان و مهندسین مجرب و کارآزموده در زمینه های تخصصی آنتی ویروس و زیرساختهای مورد نیاز علوم و فناوری مرتبط با IT و همینطور استفاده از محصولات سخت افزاری و نرم افزاری با برندهای معروف و خوش نام در ایران، با باور و رویکرد مشتری محوری و با تعهد و همکاری مدیران و کارکنان بخش های مختلف مهندسی فروش و فنی، مهندسی سخت افزار و نرم افزار، خدمات و پشتیبانی پس از فروش تاسیس گردید و با عضویت در سازمانهایی از جمله شورای عالی انفورماتیک و سازمان نظام صنفی رایانه با روندی رو به رشد و در حال توسعه کیفیت خدمات مهندسی و بازرگانی خود می باشد.

از دیگر ماموریت‌های این شرکت در جهت توسعه و ارتقاء مشتری مداری تشکیل دپارتمان امنیت شبکه بوده تا بتواند به نوعی تامین کننده نیازهای سازمانها و موسسات در جهت ارتقاء سطح امنیت محیط های تحت شبکه و همچنین انتقال دیتا در محیط امن باشد.

برنا در جهت استانداردسازی و مدیریت منابع انسانی ، تقسیم وظایف و خدمات رسانی به مشتریان خود را بر عهده دپارتمان‌های مختلف قرار داده تا بتواند به عنوان یک شرکت پیشرو با چارت استاندارد سازمانی به وظایف خود عمل نماید؛ این شرکت دارای دپارتمان‌های فروش از جمله فروش آنتی ویروس و فروش محصولات امنیت شبکه می باشد؛ همچنین شایان ذکر است دپارتمان فنی و مهندسی این شرکت دارای نیروهای تخصصی جهت پشتیبانی شبکه بر اساس آخرین استانداردهای روز دنیا می باشد.

آنتی ویروس

Antivirus کامپیوتر نقش یک محافظ از اطلاعات شما در برابر بد افزار ها و هکر ها را بازی میکند و اگر یک آنتی ویروس اورجینال و سالم را بر روی دستگاه خود نصب نکنید ممکن است در زمان نگه داری از اطلاعات دچار مشکل شده و نتواند وظیفه خود را به درستی انجام دهد.آنتی ویروس (Anti Virus) به نرم افزاری گفته می‌شود که مسئولیت پاکسازی و جلوگیری از ورود ویروس و عوامل مخرب به کامپیوتر را بر عهده دارد. در واقع آنتی ویروس یک برنامه کامپیوتری است که برای مرور فایل ها و تشخیص و حذف ویروس ها و دیگر بدافزارها از آن استفاده می شود.

آنتی ویروس در زمان اسکن، تمامی فایل‌ها و اطلاعات شما را با دیتابیس خود مقایسه می کند؛ با شناسایی فایل‌های مخرب و مشکوک ، تمامی این فایل های به لیست سیاه آنتی ویروس فرستاده میشود آنتی ویروس آن ها را چک می کند و در صورت نیاز برای بررسی بیشتر آن ها را به لابراتوار آنتی ویروس می فرستد. شرکت های سازنده آنتی ویروس دارای لابراتوری‌هستند و کاربران آنتی ویروس از طریق ورود در سایت به این لابراتوار متصل می شوند، این سایت فایل های مشکوک کاربران را دریافت کرده سپس آن ها را کنترل و اسکن میکنند. با این کار ویروس ها و بد افزار های کاربران با جدیدترین تکنولوژی های روز دنیا شناسایی و پاک میشوند.

• در راستای محصولات نامبرده شرکت برنا گواهینامه نمایندگی رسمی محصولات ،Kaspersky Sangfor، ESET را در ایران و فعال در حوزه امنیت سازمانی می باشد. لذا در همین راستا سرویس های مربوط به محصولات-Kaspersky Industrial Cy bersecurity و ESET Dynamic Threat Defense مجموعه ای از سرویس ها و فناوری ها برای امن شدن لایه های صنعتی، شامل سرورهای SCADA، پنل های HMI، ایستگاه های کاری مهندسین، PLC ها، ارتباطات شبکه و افراد، بدون تحت تاثیر قرار دادن استمرار و ثبات عملیات می باشد.

• همچنین سرویس های مربوط به KATA وESET Dynamic Threat Defense که شامل امنیت ایستگاههای کاری، جلو گیری از کلاهبرداری های آنلاین در تراکنش های بانکی، جلوگیری از تهدید های پیشرفته و هدفمند، سرویس های آموزشی آشنایی با امنیت برای کارکنان و امنیت پیشرفته برای کارشناسان فنی، مانتیتور کردن عملیات مهندسی در پالایشگاههای نفتی و همچنین مرکز عملیات امنیت می باشد.

همکاری شرکت برنا برای ارائه Antivirusبا کمپانی های Quick Heal، Kaspersky، ESET و Sangfor می باشد.

شرکت ESET کار خود را به عنوان یکی از پیشگامان راهکار آنتی ویروس آغاز نمود. در سال ۱۹۸۷ آنتی ویروس NOD به وجود آمد و در سال ۱۹۹۲ این شرکت با نام ESET در شهر براتیسلاوا در کشور اسلواکی کار خود را آغاز کرد. در این ۳۰ سال ESET تنها بر روی امنیت تمرکز نموده و توانسته است با دانش کارمندان خود راهکارهای امنیتی متناسب با نیازهای سازمان ها و صنایع مختلف را تولید نماید. بیش از یک سوم کارمندان این شرکت در بخش تحقیق و توسعه فعالیت می نماید و با توجه به این موضوع توانسته است راهکارهای جدید و به روز برای مقابله با تهدیدات جدید و ناشناخته را تولید نمایند.

این شرکت در حال حاضر یک برند جهانی در حوزه امنیت اطلاعات می باشد که بیش از ۱۱۰ میلیون کاربر را در بیش از ۲۰۲ کشور در حوزه های مختلف پشتیبانی می نماید. قادر ساختن کاربران برای استفاده از پتانسیل کامل خود در دنیای دیجیتال امن، چشم انداز ESET در این حوزه می باشد. تخصص، یکپارچگی، استقلال: این موارد اجزایی هستند که معتقدیم برای ساختن راهکارهای امنیتی سایبری اهمیت دارند.

در ESET، ما تنها به یک فرمول تکیه نمی کنیم. در عوض، کارشناسان نخبه ما دهه ها تجربه صنعت را با دانش عمیق و قدرت یادگیری ماشین برای ایجاد حفاظت چند لایه ی منحصر به فرد ترکیب می کنند.

این رویکرد، همراه با خدمات حرفه ای ESET، این امکان را به ما می دهد تا اطمینان حاصل کنیم که مشتریان ما چه در برابر تهدیدات موجود و چه در برابر تهدیدات آینده ایمن خواهند بود.

به عنوان یکی از اعضای انجمن جامعه سایبری، تحقیقات ارزشمند خود را به اشتراک گذاشته، و با سخنرانی در دانشگاه ها به مبارزه با جرایم اینترنتی کمک می کنیم. وبلاگ ما به آدرس welivesecurity.com، یکی از بهترین ها در این زمینه محسوب می شود.

ما افتخار می کنیم که یکی از کمپانی های خصوصی در زمینه امنیتی سایبری هستیم. و بدون فشار سرمایه گذاران، حق داریم که انتخاب های مناسب را انجام دهیم تا هرآنچه لازم است برای حفاظت نهایی همه مشتریان انجام دهیم.

ESET در این ۳۰ سال توانسته است جوایز متعددی را در حوزه های مختلف کسب نماید و در حال حاضر برند شماره ۱ در حوزه امنیت نقاط انتهایی در اروپا می باشد.

این شرکت توانسته است رکورد ۱۰۰ جایزه VB۱۰۰ را از موسسه مستقل Virus Bulletin دریافت نماید.

kaspersky

شرکت Kaspersky یک شرکت امنیت سایبری روسی است که در سال ۱۹۹۷ توسط «یوجین کسپرسکی» با هدف ارائه نرم‌افزارهای امنیتی برای سیستم‌های کامپیوتری تأسیس شد. دفتر مرکزی این شرکت در مسکو قرار دارد و بیش از ۱۷۰۰ کارشناس متخصص در زمینه‌های مختلف امنیت اطلاعات در آن مشغول به کار هستند. محصول اصلی این شرکت، Kaspersky Anti-Virus، به‌طور مداوم در آزمون‌هایی که توسط مراکز پژوهشی بین‌المللی معتبر و نشریات تخصصی حوزه IT برگزار می‌شود، موفق به دریافت جوایز و رتبه‌های برتر شده است.

لابراتوار کسپرسکی همواره یکی از پیشگامان توسعه استانداردهای فناوری در صنعت آنتی‌ویروس بوده است. این شرکت راه‌حل‌های جامع امنیتی را برای سیستم‌عامل‌هایی همچون لینوکس، یونیکس و Net-Ware ارائه داده و تحلیل‌گرهای شهودی نسل جدیدی را برای شناسایی ویروس‌های نوظهور توسعه داده است. همچنین، برخورداری از پایگاه داده به‌روزرسانی‌شونده، محافظت پیشرفته در برابر ویروس‌های کلان، چندریختی و تکنولوژی‌های نوآورانه جهت تشخیص بدافزارها در فایل‌های فشرده از دیگر مزایای محصولات این شرکت است.

بین سال‌های ۲۰۰۵ تا ۲۰۱۰، شرکت Kaspersky موفق شد دامنه فعالیت خود را به سطح جهانی گسترش دهد و با حضور در بازارهای بین‌المللی، جایگاه ویژه‌ای در صنعت امنیت سایبری کسب کند. این شرکت نخستین شرکت روسی بود که در فهرست شرکت‌های برتر نرم‌افزاری جهان قرار گرفت و توانست با رقبای بزرگ بین‌المللی رقابت کند.

در سال‌های اخیر، Kaspersky تمرکز خود را فراتر از آنتی‌ویروس‌های سنتی برده و راه‌حل‌هایی نظیر EDR (تشخیص و پاسخ پیشرفته)، حفاظت از زیرساخت‌های صنعتی (ICS)، و امنیت فضای ابری را به سبد محصولات خود افزوده است. همچنین این شرکت با همکاری نهادهای بین‌المللی، در شناسایی تهدیدات پیچیده سایبری نقش فعالی دارد و گزارش‌های تحلیلی آن در حوزه تهدیدات پیشرفته مکرراً مورد استناد قرار می‌گیرد.

در دنیـای امـروز، شـبکه‌های سـازمانی پیچیده‌تـر مـی شـوند و ایمن‌سـازی آنهـا دشـوارتر اسـت. تهدیـدات امنیـت سـایبری هـر روز در حـال افزایـش اسـت وحـملات APT (Advanced Persistent Threats) بصـورت مسـتمر بـر روی سـازمان هـای دولتـی و شـرکت هـای انترپرایـس تجـاری انجـام مـی پذیـرد در حالیکـه روش هـای امنیتـی سـنتی بـرای محافظـت از شـبکه هـای سـازمانی کافـی نیسـت.امروزه بـا توجـه بـه اسـتفاده از ChatGTP توسـط کـد نویسـان بـد افزار،میـزان اسـتفاده از بـد افزارهـای روز صفـر بـه طـرز قابـل توجهـی در حـملات سـازمانی افزایـش یافتـه اسـت. یکـی از راه حـل هـای برطـرف کـردن ایـن مشـکلات اسـتفاده از سیسـتم هـای یکپارچـه کـه مبتنـی بـر هـوش مصنوعـی بـا قابلیـت شناسـایی انـواع رفتـار مشـکوک در پروتـکل هـا ،کاربـران و برنامـه هـای کاربـردی می باشد.

تهدیـدات پیوسـته پیشـرفته (APT) حـملات شـبکه ای ترکیبـی مـی باشـند کـه در آنهـا از مراحـل متعـدد و تکنیـک هـای مختلـف حملـه اسـتفاده مـی شـود، APTهـا حملاتـی نیسـتند کـه در لحظـه تصـور یـا اجـرا شـوند. بلکـه ، مهاجمـان بـه عمـد اسـتراتژی هـای حملـه خـود را علیـه اهـداف خـاص برنامـه ریـزی مـی کننـد و حملـه را در یـک دوره زمانـی طولانـی انجـام مـی دهنـد.APT هـا حـملات ترکیبـی شـامل مراحـل متعـدد و انـواع تکنیـک هـای حملـه هسـتند که براساس Mitre attack قابل پیگیری هستند.

بسـیاری از APT بـا اکسـپلویت هـای روز صفـر و بدافـزار قـادر بـه تخریـب دیتـا و زیـر سـاخت مـورد هـدف مـی باشند.

بـرای شناسـایی و مقابلـه بـا ایـن نـوع حـملات اسـتفاده از راهکارهـای مبتنـی بـر یادگیـری ماشـین و نیـز بررسـی Meta Data هـم بـر روی ترافیـک شـبکه وMeta Data روی اپلیکشـن هـا لازم و ضـروری مـی باشـد تـا بـا پیـدا کـردن abnormally هـا و نیـز شـبیه سـازی DNA فایـل هـای مخـرب، شناسـایی و پاسـخ گویـی بـه حـملات APT صـورت پذیـرد. در پروپـزال امـن سـازی پیـش رو سـعی شـده از روش هـای نویـن امـن سـازی کـه مبتنـی بـر هـوش مصنوعـی و یادگیـری ماشـین مـی باشـد اسـتفاده شـود تـا از حـملات APT جلوگیـری شود.

برنـد سـنگفور یـک اکـو سیسـتم هوشـمند بـوده از زیـر سـاخت تـا لایـه سـرویس را کاملا پوشـش مـی دهـد در ایـن مسـتند سـعی شـده فقـط دو راهـکار در لایـه سـرویس ایـن برنـد معرفـی و بررسـی شـود و راهکارهـای زیرسـاخت اختصاصـی VDI اختصاصـی فایـروال پیشـرفته و ... کـه کاملا یکپارچـه و همانطـور کـه بیـان شـد اکـو سیسـتم مـی باشـد در اینجـا بررسـی نمی شود.

راهـکار XDR برنـد سـنگفور کـه بـا نـام تجـاری End-point Secure شـناخته مـی شـود کـه مسـئول عملیـات شناسـایی،دفاع وپاسـخگویی تهدیـدات در سـمت کلاینـت هـا و سـرورها مـی باشـد کـه در چندیـن مرحلـه و بـا ماژول‌هـای مختلـف ایـن امـر را بـه انجـام مـی رسـاند، ایـن راهـکار بـا ایجـاد هانـی پـات در کلاینـت هـا تـا ده درصـد فضـا بـه ایـن امـر تخصیـص داده و عملیات شـکار تهدید را اجرایی می نماید.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸

Quick Heal

Security Simplified

Quick Heal یکی از برندهای مطرح و معتبر در حوزه امنیت سایبری است که مقر اصلی آن در کشور هند قرار دارد. این شرکت فعالیت خود را از سال 1995 آغاز کرده و با تمرکز بر توسعه راهکارهای امنیتی برای کاربران خانگی، کسب‌وکارها و سازمان‌های بزرگ، توانسته جایگاه قابل توجهی در بازار جهانی آنتی ویروس‌ها به دست آورد. راهکارهای Quick Heal شامل طیف وسیعی از محصولات مانند آنتی‌ویروس، اینترنت سکیوریتی، توتال سکیوریتی و راهکارهای پیشرفته برای حفاظت از سرورها، موبایل‌ها و شبکه‌ها است.

محصول آنتی‌ویروس Quick Heal

محصول آنتی‌ویروس Quick Heal یک راهکار امنیتی جامع است که برای حفاظت بلادرنگ (Real-Time Protection) از سیستم‌های خانگی و سازمانی در برابر انواع تهدیدات سایبری مانند ویروس‌ها، تروجان‌ها، باج افزارها، بدافزارها و حملات فیشینگ طراحی شده است. این نرم‌افزار با بهره‌گیری از تکنولوژی‌های پیشرفته‌ای نظیر Behavioral Detection، تحلیل استاتیک و دینامیک، و قابلیت‌های ابری، توانایی بالایی در شناسایی تهدیدات نوظهور دارد.

ویژگی‌ها و قابلیت‌های کلیدی:

- **Real-Time Protection:** محافظت مستمر از سیستم در برابر تهدیدات در حال اجرا و جلوگیری از اجرای کدهای مشکوک.
- **Advanced DNAScan:** تکنولوژی اختصاصی برای شناسایی بدافزارهای ناشناخته بر پایه الگوهای رفتاری و تحلیل DNA فایل‌ها.
- **Anti-Ransomware:** مکانیزم پیشرفته مقابله با باج‌افزارها با قابلیت تشخیص، توقف و بازیابی فایل‌های رمزگذاری‌شده.
- **Web Security:** جلوگیری از دسترسی به وب سایت‌های آلوده، فیشینگ یا مخرب برای تأمین امنیت کاربران هنگام مرور اینترنت.
- **Firewall Protection:** فایروال داخلی جهت کنترل ترافیک ورودی و خروجی شبکه و جلوگیری از نفوذ هکرها.
- **Email Security:** اسکن ضمیمه‌ها و محتوای ایمیل برای شناسایی فایل‌های آلوده و پیوندهای خطرناک.
- **Parental Control:** امکان تعریف محدودیت برای دسترسی کودکان به محتوای خاص در اینترنت.

Quick Heal با ارائه راهکارهای جامع، قابل اطمینان و به‌روز، یکی از گزینه‌های مناسب برای حفاظت از داده‌ها و زیرساخت‌های IT در برابر تهدیدات سایبری محسوب می‌شود.

ابزار DLP

افزایش وابستگی سازمان‌ها به داده‌های دیجیتال، خطراتی مانند نشت، از دست رفتن یا سرقت اطلاعات حساس را به همراه داشته است. ابزار Data Loss Pre-vention (DLP) با هدف جلوگیری از انتقال غیرمجاز داده های محرمانه از سازمان طراحی شده است؛ این داده‌ها ممکن است شامل اطلاعات مالی، مشتریان، اسرار تجاری یا اسناد مهندسی باشند. نشت داده می‌تواند از طریق روش‌های فیزیکی مانند سرقت هارد یا USB، یا از راه‌های نرم‌افزاری مانند ارسال اطلاعات از طریق ایمیل یا پیام‌رسان‌ها رخ دهد.

از سوی دیگر، Data Loss به خطاهایی اشاره دارد که در آن اطلاعات به دلیل خرابی سیستم، نقص در انتقال یا پردازش نابود می‌شوند. در این موارد، راهکارهایی مانند پشتیبان‌گیری (Backup) و بازیابی پس از بحران (Disaster Recovery) ضرورت دارد. همچنین، در شرایطی مانند نقض داده‌ها (Data Breach)، اطلاعات به دست مهاجمان سایبری می‌افتد که گاهی به‌اشتباه با نشت داده یکسان در نظر گرفته می‌شود.

ابزار DLP با بهره‌گیری از فناوری‌های طبقه‌بندی، شناسایی، رمزنگاری و مسدودسازی اطلاعات، کنترل دقیق بر جریان داده‌های سازمان فراهم می‌کند. موتورهای شناسایی محتوا (Detection Engine) و قابلیت Data Blocker محتوای خروجی را تحلیل کرده و مشخص می‌سازد کدام اطلاعات مجاز به خروج هستند و کدام باید مسدود شوند.

یکی از الزامات اجرای موفق DLP، طبقه‌بندی اطلاعات بر اساس میزان حساسیت آن‌هاست. این ابزار امکان تعریف سیاست‌های امنیتی دقیق بر اساس نوع اطلاعات، مانند اطلاعات کارکنان، اسناد مالی، نقشه‌های مهندسی یا لیست‌های مشتریان را فراهم می‌سازد تا برای هر نوع داده، سطح مناسبی از حفاظت اعمال گردد.

ابزار DLP مانند دیواره آتش محتوای داده‌های خروجی را بررسی می‌کند و در قالب یک appliance شبکه، با زیرساخت امنیتی فعلی سازمان هماهنگ می‌شود. این ابزار همچنین محافظت از دستگاه های قابل حمل مانند لپ‌تاپ، فلش مموری و Bluetooth را نیز دربر می‌گیرد و نشت داده‌ها از طریق آن‌ها را کاهش می‌دهد.

یکی از قابلیت‌های کلیدی ابزار DLP، رمزگذاری خودکار اطلاعات در ابزارهای ذخیره‌سازی قابل‌حمل است. راهکارهایی نظیر EasyLock و Endpoint Pro-tector تمامی داده‌های حساس منتقل‌شده به حافظه‌های USB را رمزگذاری کرده و امکان مدیریت مرکزی آن‌ها را برای مدیران فناوری اطلاعات فراهم می‌سازند. این راهکار از سیستم‌عامل‌های Win-dows و macOS نیز پشتیبانی می‌کند.

در مجموع، ابزار DLP با شناسایی، کنترل و محافظت پیشرفته از داده‌ها، مانع نشت، سرقت یا از دست رفتن اطلاعات حیاتی سازمان می‌شود. با استفاده از این فناوری، امنیت داده‌ها در بستر شبکه، فضای ذخیره‌سازی و تجهیزات قابل‌حمل تأمین خواهد شد.

همکاری شرکت برنا برای ارائه راهکار DLP با کمپانی های Safetica، Falcongaze و Zecurion می باشد.

www.bornanetwork.co info@bornanetwork.co ۰۲۱-۷۴۰۲۸

safetica

Safetica یک راهکار جامع در حوزه پیشگیری از نشت اطلاعات DLP و مدیریت ریسک‌های داخلی Insider Risk Management است که برای سازمان‌هایی با اندازه‌های مختلف طراحی شده است. این ابزار با تمرکز بر حفاظت از داده‌های حساس، شناسایی تهدیدات داخلی و رعایت الزامات قانونی، امنیت اطلاعات سازمان را به‌طور مؤثری تضمین می‌کند.

کشف و طبقه‌بندی داده‌ها

Safetica با استفاده از قابلیت Unified Classification، داده‌های حساس را بر اساس محتوا، منبع، نوع فایل و حتی طبقه‌بندی‌های شخص ثالث شناسایی و محافظت می‌کند. این ابزار می‌تواند فایل‌های حساس را در پوشه‌های انتخاب‌شده روی نقاط پایانی و در اشتراک‌های شبکه جستجو کند.

پیشگیری از نشت داده‌ها

Safetica با نظارت بر عملیات کاربران مانند صادرات، بارگذاری و دانلود فایل‌ها، باز کردن فایل‌ها، کپی فایل‌ها به مسیرهای مختلف، بارگذاری فایل‌ها از طریق مرورگرهای وب، ارسال فایل‌ها از طریق ایمیل یا برنامه‌های پیام‌رسان و سایر موارد، از نشت داده‌ها جلوگیری می‌کند.

مدیریت تهدیدات داخلی

این ابزار با تحلیل رفتار کاربران، تهدیدات داخلی را شناسایی و بر اساس زمینه رفتاری، ریسک‌ها را کاهش می‌دهد. Safetica می‌تواند کارمندان با ریسک بالا (از جمله کسانی که در حال ترک سازمان هستند، با اخراج مواجه‌اند، از راه دور کار می‌کنند یا پیمانکاران) را شناسایی و ارزیابی کند و راهنمایی‌هایی برای تغییر رفتار آن‌ها ارائه دهد تا از وقوع حوادث احتمالی جلوگیری شود.ین کرده و از وقوع حوادث امنیتی جلوگیری کنند.

قابلیت‌های کلیدی

- **کشف و طبقه‌بندی داده‌ها:** شناسایی و محافظت از داده‌های حساس بر اساس محتوا، منبع و نوع فایل.
- **پیشگیری از نشت داده‌ها:** نظارت بر عملیات کاربران و جلوگیری از نشت داده‌ها از طریق کانال های مختلف.
- **مدیریت تهدیدات داخلی:** شناسایی و کاهش ریسک‌های ناشی از رفتارهای کاربران داخلی.
- حفاظت از داده‌ها در فضای ابری: ادغام با Micro-soft ۳۶۵ و جلوگیری از نشت داده‌ها به فضای ابری.
- **گزارش‌دهی و هشدارهای آنی:** ارائه گزارش های قابل تنظیم و هشدارهای فوری در صورت وقوع حوادث امنیتی.
- **پشتیبانی از چند پلتفرم:** حفاظت از داده‌ها در سیستم‌عامل‌های مختلف و محیط‌های ابری.

Safetica با ارائه این قابلیت‌ها، به سازمان‌ها کمک می‌کند تا امنیت داده‌های خود را تضمین کرده و از وقوع حوادث امنیتی جلوگیری کنند.

ZECURION

Zecurion یکی از پیشگامان در حوزه امنیت سایبری است که از سال ۲۰۰۱ با تمرکز بر پیشگیری از تهدیدات داخلی و نشت داده‌ها فعالیت می‌کند. محصول اصلی این شرکت، Zecurion Data Loss Prevention (DLP)، راهکاری جامع برای حفاظت از اطلاعات حساس در برابر نشت، سوءاستفاده و تهدیدات داخلی است.

کشف و طبقه‌بندی داده‌ها

ماژول Discovery در Zecurion DLP با بهره‌گیری از بیش از ۱۰ فناوری پیشرفته مانند اثرانگشت دیجیتال، تحلیل زبانی و تشخیص الگو، داده‌های حساس را در ایستگاه های کاری، سرورها، پایگاه‌های داده و فضای ابری شناسایی و طبقه‌بندی می‌کند. این قابلیت به سازمان ها امکان می‌دهد تا پیش از وقوع نشت اطلاعات، داده‌های مهم را شناسایی و محافظت کنند.

کنترل ترافیک و دستگاه‌ها

Zecurion DLP با نظارت بر بیش از ۱۰۰ کانال ارتباطی، از جمله ایمیل، پیام‌رسان‌ها، شبکه‌های اجتماعی و دستگاه‌های ذخیره‌سازی قابل حمل، از نشت داده‌ها جلوگیری می‌کند. ماژول Device Control با تحلیل محتوای پیشگیرانه، از نوشتن اطلاعات حساس بر روی رسانه‌های خارجی جلوگیری کرده و در صورت نیاز، فایل ها را به‌طور خودکار رمزگذاری می‌کند.

تحلیل رفتار کاربران (UBA)

ماژول User Behavior Analytics با تحلیل بیش از ۱۰ شاخص رفتاری و پروفایل‌های احساسی، رفتار کاربران را پایش کرده و انحرافات مشکوک را شناسایی می‌کند. این قابلیت به تیم‌های امنیتی امکان می‌دهد تا تهدیدات داخلی را پیش از وقوع شناسایی و اقدامات پیشگیرانه انجام دهند.

کنترل کارکنان و بهره‌وری

ماژول Staff Control با ثبت فعالیت‌های کاربران، از جمله ساعات کاری، استفاده از برنامه‌ها و وب‌سایت ها، بهره‌وری کارکنان را ارزیابی می‌کند. این اطلاعات به مدیران کمک می‌کند تا رفتارهای غیرمعمول را شناسایی و از انحراف از سیاست‌های سازمانی جلوگیری کنند.

تشخیص عکس‌برداری از صفحه‌نمایش

قابلیت Screen Photo Detector با استفاده از دو شبکه عصبی مصنوعی، تلاش برای عکس‌برداری از صفحه‌نمایش توسط گوشی هوشمند را در کمتر از ۰.۰۶ ثانیه شناسایی کرده و به‌طور خودکار رایانه را قفل می‌کند که نشت اطلاعات از طریق روش‌های غیرمتعارف جلوگیری می‌کند.

مزایا و افتخارات

Zecurion DLP با پشتیبانی از بیش از ۵۰۰ فرمت فایل، قابلیت کشف داده‌ها در شبکه‌های بدون دامنه و ارائه گزارش‌های تعاملی، راهکاری قدرتمند برای سازمان‌ها با اندازه‌های مختلف است. این محصول در بیش از ۷۰ کشور مورد استفاده قرار گرفته و توسط مؤسسات معتبری مانند Gartner، IDC و Forrester به رسمیت شناخته شده است.

ابزار PAM

Privileged Access Management یا به اختصار (PAM) امروزه مدیران ارشد سازمان‌ها برای بالا بردن سطح امنیت و حفاظت از دارایی‌های اطلاعاتی خود سرمایه گذاری ویژه‌ای می‌کنند و از محصولات و راهکارهای متنوعی بهره می‌برند. برای مثال: درگاه‌های شبکه را به انواع دیوارهای آتش، UTM، WAF، IPS و ... مجهز می کنند. حتی از روش‌ها و استانداردهای امنیتی، مانند: PCI-DSS و ISO۲۷۰۰۱ بهره می‌گیرند. اما در نهایت برای اینکه کار سازمان به انجام برسد، به ناچار مجبور هستند دسترسی‌های سطح بالا، به سامانه‌های اطلاعاتی، نرم‌افزارها، سخت‌افزارها و سرورهای سازمان را به پیمانکار و یا افرادی بسپارند که شاید به‌صورت تمام و کمال مورد اطمینان و وثوق‌شان نباشند. آمارها نشان می‌دهند که در سازمان‌های بزرگ، ریسک‌ها و تأثیر آسیب‌هایی که این افراد به مجموعه وارد می کنند، بسیار قابل‌تأمل است. فارغ از اینکه علت و انگیزه چه می‌تواند باشد و یا اینکه حوادث رخداده عمدی بوده‌اند یا سهوی، نتیجه و تأثیر بسیاری از وقایع غیرقابل‌جبران است.

بنابراین راهکاری بایستی اتخاذ گردد که بتواند این ریسک را پوشش داده تا به هر فردی اعتماد نکرده و منابع سازمان را بتوانیم با خیال آسوده در اختیار این کاربران قرار دهیم. این راهکار با نام اختصاری PAM (Privileged Access Manager) شناخته می‌شود.

ابزار PAM با کنترل، مدیریت و نظارت بر دسترسی کاربران دارای سطح دسترسی بالا (مانند مدیران سیستم، پیمانکاران IT یا کاربران ممتاز) به منابع حیاتی سازمان، خطرات ناشی از سوءاستفاده یا نفوذ احتمالی را به‌طور چشمگیری کاهش می دهد. این ابزار با قابلیت ضبط کامل نشست‌های کاری، احراز هویت چندمرحله‌ای، اعمال سیاست های Least Privilege و تفکیک وظایف (Segregation of Duties) به سازمان‌ها کمک می‌کند تا کنترل کاملی بر نحوه و زمان استفاده از دسترسی های ویژه داشته باشند. همچنین می‌توان دسترسی‌های موقت یا مبتنی بر درخواست را برای کاربران تعریف کرد و به‌صورت بلادرنگ هشدارهای لازم را دریافت نمود.

همکاری شرکت برنا برای ارائه راهکار امنیتی PAM با کمپانی Arcon می‌باشد. راهکار PAM شرکت Arcon یکی از محصولات پیشرو در بازار جهانی محسوب می‌شود که با قابلیت‌هایی نظیر مدیریت دسترسی بر اساس نقش، کنترل نشست ها، ضبط و بازبینی فعالیت‌ها، تعریف سطوح مختلف دسترسی و گزارش‌دهی پیشرفته، به سازمان‌ها در رعایت الزامات قانونی و بهبود وضعیت امنیتی کمک می‌کند. این محصول در صنایع حیاتی مانند بانکداری، انرژی، مخابرات، دولت و بهداشت و درمان مورد استفاده قرار گرفته و با معماری منعطف خود امکان استقرار در محیط های ابری، فیزیکی یا ترکیبی را داراست.

همکاری شرکت برنا برای ارائه راهکار امنیتی PAM با کمپانی Arconمی باشد.

راهکار مدیریت دسترسی ممتاز (PAM) شرکت ARCON، یک راه‌حل جامع و پیشرفته برای مدیریت، کنترل و نظارت بر دسترسی‌های سطح بالا در سازمان‌ها است. این سیستم با تمرکز بر امنیت هویت‌های دیجیتال و محافظت از دارایی‌های حیاتی، به سازمان‌ها کمک می‌کند تا خطرات ناشی از دسترسی‌های غیرمجاز را کاهش دهند و الزامات قانونی را برآورده سازند.

مدیریت دسترسی و احراز هویت

ARCON | PAM با بهره‌گیری از احراز هویت چندمرحله ای (MFA) و اصول "اعتماد صفر" (Zero Trust)، اطمینان حاصل می‌کند که تنها کاربران مجاز به منابع حساس دسترسی دارند. این سیستم از پروتکل‌های استانداردی مانند OAuth۲/۰، OpenID Connect و SAML برای پیاده سازی Single Sign-On (SSO) استفاده می‌کند و با ابزارهای احراز هویت مدرن مانند Google Authentica- tor و Microsoft Authenticator یکپارچه می‌شود.

کنترل دسترسی و اصل کمترین امتیاز

با پیاده‌سازی اصل "کمترین امتیاز" (Least Privilege)، ARCON | PAM دسترسی کاربران را بر اساس نقش‌ها، مسئولیت‌ها و وظایفشان مدیریت می‌کند. این رویکرد به کاهش خطرات ناشی از دسترسی‌های غیرمجاز و سوءاستفاده از سیستم‌ها و داده‌های حساس کمک می کند.

مدیریت رمز عبور و خزانه‌داری

سیستم خزانه‌داری رمز عبور ARCON، رمزهای عبور را به‌صورت ایمن ذخیره کرده و به‌طور خودکار آن ها را به‌روزرسانی و چرخش می‌دهد. این ویژگی با استفاده از الگوریتم‌های رمزنگاری قوی مانند AES ۲۵۶-bit، از دسترسی غیرمجاز به رمزهای عبور جلوگیری می‌کند و با الزامات امنیتی مانند FIPS مطابقت دارد.

نظارت بر نشست‌ها و گزارش‌گیری

ARCON | PAM تمامی نشست‌های کاربران ممتاز را به‌صورت زنده نظارت کرده و فعالیت‌ها را در قالب های متنی و ویدیویی ضبط می‌کند. این قابلیت ها به تیم‌های امنیتی امکان می‌دهد تا فعالیت های کاربران را بررسی کرده و در صورت بروز رفتارهای مشکوک، اقدامات لازم را انجام دهند.

قابلیت‌های پیشرفته و انعطاف‌پذیری

ویژگی‌هایی مانند دسترسی موقت (Just-in-Time Access)، مدیریت کلیدهای SSH، و پشتیبانی از محیط‌های ابری و DevOps، به سازمان‌ها امکان می‌دهد تا به‌طور مؤثری دسترسی‌های ممتاز را مدیریت کنند. این سیستم با معماری مبتنی بر میکروسرویس‌ها، امکان استقرار در محیط‌های فیزیکی، ابری یا ترکیبی را فراهم می‌کند.

در مجموع، ARCON | PAM یک راهکار قدرتمند و انعطاف‌پذیر برای مدیریت دسترسی‌های ممتاز است که با ارائه قابلیت‌های پیشرفته و تطابق با استانداردهای بین‌المللی، به سازمان‌ها کمک می کند تا امنیت اطلاعات خود را تضمین کنند.

سرویس EDR

EDR؛ راهکار مدرن دفاع از نقطه پایانی

راهکار EDR یا Endpoint Detection and Response، یک سامانه پیشرفته امنیت سایبری است که با تمرکز بر نقاط پایانی شبکه، مانند رایانه‌ها، لپ‌تاپ‌ها، سرورها و دستگاه‌های موبایل، فعالیت‌های مشکوک و تهدیدات سایبری را به‌صورت لحظه‌ای شناسایی، تحلیل و کنترل می‌کند. این مفهوم نخستین بار توسط آنتون چوواکین، تحلیل‌گر سابق گارتنر، معرفی شد تا دسته ای از ابزارهای امنیتی نوظهور را توصیف کند که توانایی مقابله با تهدیدات پیچیده و هدفمند را در لایه Endpoint فراهم می‌سازند.

EDR با جمع‌آوری مداوم داده‌ها از فعالیت‌های نقاط پایانی، نظارت زنده بر رفتار سیستم‌ها، و استفاده از تحلیل‌های رفتاری، الگوریتم‌های یادگیری ماشین و قواعد از پیش تعریف‌شده، تلاش می‌کند تا کوچک ترین نشانه‌های نفوذ یا سوءاستفاده از منابع را کشف کند. برخلاف آنتی‌ویروس‌های سنتی که صرفاً بر شناسایی و حذف بدافزارها تمرکز دارند، EDR می‌تواند رفتارهای مخرب بدون امضای مشخص را نیز تشخیص دهد.

از جمله قابلیت‌های کلیدی EDR می‌توان به موارد زیر اشاره کرد:

- **نظارت پیوسته و جمع‌آوری داده‌ها** از فرآیندها، رجیستری، ترافیک شبکه و فایل‌های اجرا شده روی هر دستگاه
- **تحلیل پیشرفته و تشخیص تهدید** از طریق الگوریتم‌های تحلیل رفتاری و شاخص‌های تهدید (IOCs)
- **پاسخ خودکار و دستی به تهدیدات** شامل قرنطینه کردن فایل‌ها، متوقف کردن فرآیندها یا قطع دسترسی کاربر
- **امکان بررسی جرم‌شناسانه (Forensics)** برای ریشه‌یابی حملات و تحلیل مسیر نفوذ مهاجم
- **یکپارچگی با سیستم‌های SIEM و SOAR** برای ارتقاء دید امنیتی و خودکارسازی عملیات پاسخ

راهکارهای EDR معمولاً با داشبوردی جامع ارائه می‌شوند که قابلیت مشاهده‌ی تهدیدات بلادرنگ، اجرای اقدامات اصلاحی، و تولید گزارش‌های سفارشی را فراهم می‌کند. برخی از پلتفرم‌های پیشرفته‌تر EDR با فناوری‌های XDR (Extended Detection and Response) و Threat Intelligence نیز ادغام شده‌اند تا دامنه دید تهدیدات را از نقاط پایانی به کل زیرساخت شبکه گسترش دهند.

در نهایت، EDR به عنوان یک لایه ضروری در دفاع سایبری مدرن شناخته می‌شود و نقش مهمی در مقابله با حملات هدفمند، تهدیدات ماندگار (APT)، باج‌افزارها و نفوذهای داخلی دارد. این راهکار به سازمان‌ها امکان می‌دهد که پیش از آسیب، تهدید را شناسایی و مهار کنند و تحلیل دقیق‌تری از ریسک‌های امنیتی داشته باشند.

همکاری شرکت برنا برای ارائه راهکار امنیتی EDR با کمپانی های Kaspersky و ESET می باشد.

سرویس XDR

XDR؛ نسل بعدی تشخیص و پاسخ امنیتی

راهکار XDR یا Extended Detection and Response، یک راه‌حل امنیتی پیشرفته و یکپارچه است که با هدف شناسایی و پاسخ‌دهی مؤثر به تهدیدات سایبری در سراسر لایه‌های مختلف زیرساخت سازمانی طراحی شده است. برخلاف راهکارهای سنتی مانند EDR که تمرکز آن‌ها صرفاً بر نقاط پایانی است، XDR با گردآوری، همبسته‌سازی و تحلیل داده‌های امنیتی از منابع مختلف مانند نقاط پایانی (endpoints)، شبکه (network)، ایمیل، سرورها، فضای ابری و اپلیکیشن‌ها، دید گسترده‌تری از وضعیت امنیتی ارائه می‌دهد.

هدف اصلی XDR، ساده‌سازی فرآیند مدیریت تهدیدات برای تیم‌های امنیتی و SOC است. در بسیاری از سازمان‌ها، استفاده از چندین محصول امنیتی به‌صورت هم‌زمان موجب افزایش پیچیدگی، بار عملیاتی و بروز شکاف‌های امنیتی می‌شود. XDR با ایجاد یک بستر متمرکز برای جمع‌آوری و تحلیل اطلاعات از محصولات امنیتی گوناگون، نه تنها امکان دید جامع و بلادرنگ از تهدیدات را فراهم می‌سازد، بلکه با استفاده از هوش مصنوعی، یادگیری ماشین و قواعد امنیتی پیشرفته، پاسخ‌دهی خودکار و مؤثرتری به تهدیدات ارائه می دهد.

قابلیت‌های کلیدی XDR عبارت‌اند از:

- **یکپارچه‌سازی داده‌ها از منابع مختلف** امنیتی مانند فایروال‌ها، EDR، سیستم‌های ایمیل، ترافیک شبکه و سرویس‌های ابری
- **تحلیل رفتار مشکوک و همبسته‌سازی رویدادها** با هدف شناسایی تهدیدهای پیچیده و چندمرحله‌ای
- **پاسخ خودکار و متمرکز به تهدیدات** از طریق مسدودسازی دسترسی، قرنطینه کردن منابع آلوده یا هشداردهی به اپراتور
- **داشبورد جامع و ساده‌شده** برای تیم‌های امنیتی به‌منظور مشاهده وضعیت تهدیدات و مدیریت رخدادها در یک پنل متمرکز
- **افزایش دقت و کاهش هشدارهای غلط (False Positives)** با بهره‌گیری از تحلیل‌های هوشمند و بینش امنیتی یکپارچه

XDR علاوه بر کاهش زمان تشخیص و پاسخ به تهدیدات (MTTD و MTTR)، موجب افزایش هماهنگی بین سامانه‌های امنیتی و اثربخشی بیشتر تیم‌های عملیاتی می‌شود. این راهکار، امکان بررسی سریع ریشه تهدیدات و واکنش هماهنگ در سراسر اکوسیستم IT را فراهم می‌کند.

در مجموع، XDR به عنوان یک تحول مهم در چشم انداز امنیت سایبری، برای سازمان‌هایی که با حجم بالای داده‌های امنیتی و تهدیدات پیچیده مواجه هستند، انتخابی هوشمندانه و ضروری به شمار می‌رود.

همکاری شرکت برنا برای ارائه راهکار امنیتی XDR با کمپانی های Seceon, Sangfor و ESET می باشد.

معرفی راهکارهای EDR و XDR شرکت ESET برای امنیت سازمانی

شرکت ESET به عنوان یکی از برندهای پیشرو در حوزه امنیت سایبری، راهکارهای حرفه‌ای EDR و XDR خود را با هدف شناسایی، تحلیل و پاسخ به تهدیدات پیچیده سایبری در سازمان‌ها ارائه می‌دهد. این راهکارها که تحت عنوان ESET Inspect (نسخه جدید EDR/XDR سازمانی این شرکت) شناخته می‌شوند، بخشی از پلتفرم امنیتی یکپارچه ESET PROTECT هستند.

ESET Inspect به عنوان راهکار EDR/XDR پیشرفته، قابلیت نظارت مداوم بر رفتار دستگاه‌ها، تحلیل تهدیدات مشکوک، شکار تهدید (Threat Hunting) و پاسخ خودکار به رخدادهای امنیتی را فراهم می‌سازد. این محصول به مدیران امنیت این امکان را می‌دهد که در سریع‌ترین زمان ممکن، تهدیدات فعال یا پنهان را در سیستم‌های macOS، Windows و Linux شناسایی کرده و با آنها مقابله کنند.

ESET با ترکیب فناوری‌های شناسایی مبتنی بر رفتار، یادگیری ماشین، تحلیل حافظه و همبسته‌سازی داده‌ها در سطوح مختلف، در قالب XDR نیز قابلیت‌های پیشرفته‌ای ارائه می‌دهد. این معماری، اطلاعات امنیتی از منابع مختلف مانند EDR، فایروال، ایمیل، فضای ابری و سایر تجهیزات شبکه گردآوری کرده و در یک داشبورد متمرکز تحلیل می‌کند.

این امکان باعث می‌شود تیم امنیتی سازمان، دید جامعی از وضعیت امنیتی داشته باشند و با سرعت بالا به تهدیدات واکنش نشان دهند.

از ویژگی‌های کلیدی راهکار ESET Inspect می‌توان به موارد زیر اشاره کرد:

- مشاهده رفتارهای مشکوک در نقاط انتهایی و تحلیل دقیق فعالیت‌ها
- تشخیص بدافزارهای ناشناخته، حملات بدون فایل و تهدیدات داخلی
- ایجاد سیاست‌های امنیتی قابل تنظیم بر اساس نیاز سازمان
- ارائه هشدارهای دقیق با حداقل false positive
- قابلیت ادغام با SIEM و ابزارهای پاسخ خودکار

این راهکارها به ویژه برای سازمان‌هایی مناسب است که به دنبال امنیت چندلایه، شفافیت در رخدادها، و پاسخ سریع به تهدیدات در مقیاس بزرگ هستند. با بهره‌گیری از EDR/XDR برند ESET، سازمان‌ها می‌توانند از سرمایه اطلاعاتی خود به بهترین شکل محافظت کرده و امنیت عملیاتی پایداری ایجاد نمایند.

kaspersky

محصولات EDR و XDR برند Kaspersky در قالب مجموعه ای لایه‌مند شامل Next EDR Foundations، Next EDR Optimum و Next XDR Expert عرضه می‌شوند. این مجموعه با هدف محافظت پیشرفته از سازمان‌ها در برابر تهدیدات سایبری طراحی شده و متناسب با نیاز تیم‌های IT معمولی تا تیم‌های SOC حرفه‌ای، سطوح مختلفی از قابلیت‌ها را ارائه می‌دهد.

Next EDR Foundations

این نسخه برای سازمان‌هایی مناسب است که به دنبال پیاده‌سازی اولیه امنیت نقطه پایانی با هزینه بهینه هستند.

ویژگی‌ها و قابلیت‌های کلیدی:

- محافظت چندلایه با استفاده از آنتی‌ویروس، آنتی‌باج افزار و محافظت رفتاری
- کنترل تجهیزات جانبی (USB Device Control) برای جلوگیری از نشت داده
- وب‌فیلترینگ و کنترل برنامه‌ها برای کاهش سطح حمله
- پشتیبانی از انواع سیستم‌عامل‌ها: Windows، macOS، Linux
- مدیریت مرکزی از طریق ESET Protect Cloud یا On-Premise
- نصب سریع، بدون نیاز به زیرساخت SOC

Next EDR Optimum

این نسخه مناسب سازمان‌هایی است که فراتر از محافظت پایه، نیاز به شناسایی، تحلیل و پاسخ فعال به تهدیدات هدفمند دارند.

ویژگی‌ها و قابلیت‌های کلیدی:

- دید عمیق نسبت به زنجیره حملات (Attack Chain Visibility)
- تحلیل خودکار وقایع مشکوک با اولویت‌بندی تهدیدها
- قابلیت قرنطینه، بلاک و Rollback از راه دور برای کاهش زمان پاسخ
- جستجوی تهدیدات شناخته‌شده با IoC
- گزارش گرافیکی و ساده برای تصمیم‌گیری سریع

Next XDR Expert

این نسخه کامل‌ترین و پیشرفته‌ترین راهکار تشخیص و پاسخ کسپرسکی است که با همبست سازی داده‌ها از چندین لایه زیرساختی مانند end-point، شبکه، سرور، ایمیل و فضای ابری، یک دید جامع از تهدیدات ارائه می‌دهد.

ویژگی‌ها و قابلیت‌های کلیدی:

- موتور تحلیل همبسته (Correlation Engine) برای کشف حملات چندمرحله‌ای
- زبان جستجوی (KQL) برای شکار تهدیدات (Threat Hunting)
- مدیریت پیشرفته رخدادها و عملیات (Incident & Response Playbooks)
- ادغام با SIEM و SOAR برای اتوماسیون کامل امنیت سازمان
- تحلیل جرم‌شناسی دیجیتال و شناسایی lateral movement
- پشتیبانی از تهدیدات ناشناخته و تحلیل رفتار با AI

SANGFOR

شرکت Sangfor Technologies با بیش از دو دهه تجربه در حوزه امنیت شبکه، رایانش ابری و زیرساخت های دیجیتال، محصولات امنیتی پیشرفته‌ای را برای مقابله با تهدیدات سایبری نوظهور ارائه کرده است. در این میان، Sangfor Endpoint Secure (EDR) و Cyber Command (XDR) به‌عنوان دو راهکار قدرتمند تشخیص و پاسخ، نقش مهمی در دفاع چندلایه و هوشمند از شبکه‌های سازمانی ایفا می‌کنند.

Sangfor Endpoint Secure (EDR)

Sangfor EDR یک راهکار محافظتی برای دستگاه‌های پایانی است که با ترکیب آنتی‌ویروس نسل جدید، تحلیل رفتاری، و هوش مصنوعی، تهدیدات ناشناخته را شناسایی و مهار می‌کند. Sangfor EDR علاوه‌بر جلوگیری از آلودگی، توانایی شناسایی ریشه حمله (Root Cause Analysis) و حذف کامل اثرات آن را نیز دارد.

ویژگی‌های مهم:

- تشخیص تهدیدات پیشرفته مانند باج‌افزار، حملات Zero-Day و فایل‌های مخرب بدون امضا
- پاسخ خودکار به تهدیدات شامل قرنطینه، بستن فرآیندها و ایزوله کردن سیستم آلوده
- دید کامل از فعالیت کاربران و فرآیندها برای ریشه یابی حملات
- مدیریت مرکزی و ساده برای مانیتورینگ تمام نقاط پایانی سازمان

Sangfor Cyber Command (XDR)

Cyber Command راهکار XDR سانگفور است که با گردآوری داده‌ها از منابع مختلف شبکه (مانند EDR، فایروال، ترافیک شبکه، سرورها و ...) یک دید جامع از حملات در سطح سازمان فراهم می‌سازد. این پلتفرم با بهره‌گیری از AI و الگوریتم‌های UEBA (تحلیل رفتار کاربران و موجودیت‌ها)، الگوهای مشکوک را در سراسر محیط IT شناسایی می‌کند.

ویژگی‌های کلیدی:

- ادغام اطلاعات از چندین لایه امنیتی برای تشخیص حملات زنجیره‌ای
- پاسخ سریع و هماهنگ به تهدیدات در سطح شبکه و نقاط پایانی
- دید بلادرنگ از مسیر حمله و رفتار مهاجم (Kill Chain Visualization)
- کاهش چشم‌گیر زمان شناسایی (MTTD) و واکنش (MTTR)

Sangfor با ترکیب EDR و XDR، راهکاری قدرتمند و منسجم برای سازمان‌هایی فراهم کرده که به دنبال محافظت فعال و پاسخ سریع به تهدیدات پیشرفته هستند. این راهکارها با رویکرد Zero Trust و تحلیل دقیق تهدیدات، امنیت را در سطح جدیدی تعریف می‌کنند.

Quick Heal

Security Simplified

Quick Heal Technologies یکی از برندهای معتبر در حوزه امنیت سایبری است که محصولات آن توسط شرکت‌های کوچک تا سازمان‌های بزرگ در سراسر جهان مورد استفاده قرار می‌گیرد. این شرکت با ارائه راهکارهای مدرن EDR و XDR تحت پلتفرم Seqrite، حفاظت جامعی را در برابر حملات هدفمند، تهدیدات ناشناخته و بدافزارهای پیچیده فراهم می‌سازد.

Seqrite Endpoint Detection & Response (EDR)

EDR کوییک‌هیل (Seqrite EDR) ابزاری توانمند برای نظارت، تشخیص و واکنش نسبت به تهدیدات در دستگاه‌های پایانی است. این راهکار با تحلیل رفتار کاربران، اپلیکیشن‌ها و فرآیندها، حملات مشکوک را شناسایی و متوقف می‌کند.

ویژگی‌های مهم:

- شناسایی تهدیدات پیشرفته مانند حملات بدون فایل (fileless) و باج‌افزارها
- داشبورد مدیریتی یکپارچه برای دید کامل به وضعیت امنیتی کل شبکه
- پاسخ سریع با اقدامات خودکار مانند قرنطینه، مسدودسازی فایل، و توقف فرآیندهای مشکوک
- بررسی علت حملات (Root Cause Analysis) برای جلوگیری از تکرار آن‌ها

Seqrite Extended Detection & Response (XDR)

راهکار XDR برند کوییک‌هیل با نام Seqrite Hawk XDR شناخته می‌شود. این پلتفرم با جمع‌آوری و تحلیل اطلاعات امنیتی از منابع مختلف مانند فایروال‌ها، ایمیل‌ها، سرورها و نقاط پایانی، دید کاملی از حملات سایبری در کل سازمان ارائه می دهد.

ویژگی‌های کلیدی:

- همبستسازی داده‌ها از چندین لایه امنیتی برای تشخیص سریع‌تر تهدیدات
- بهره‌گیری از هوش مصنوعی و یادگیری ماشین برای تحلیل رفتارهای غیرعادی
- کاهش زمان شناسایی و پاسخ به تهدیدات MTTD و MTTR
- قابلیت پاسخ خودکار به تهدیدات در چندین نقطه از شبکه

راهکارهای EDR و XDR کوییک‌هیل از طریق پلتفرم Seqrite، امنیت سازمان‌ها را به‌صورت هوشمند، یکپارچه و مبتنی بر تحلیل رفتاری فراهم می‌کنند. این راهکارها با کاهش وابستگی به نیروی انسانی در تحلیل لاگ‌ها، قابلیت واکنش سریع به تهدیدات پیچیده را در اختیار تیم‌های امنیتی قرار می‌دهند. Quick Heal گزینه‌ای مناسب برای سازمان‌هایی است که به‌دنبال امنیت چندلایه، کارآمد و قابل اعتماد هستند.

سرویس NDR

Network Detection And Response یا NDR راهکارهای تشخیص و پاسخ‌دهی شبکه ترکیبی از تکنیک‌های تحلیلی پیشرفته مانند یادگیری ماشین هستند که مبتنی بر امضاء نیستند (non-signature-based) تا فعالیت مشکوک شبکه را شناسایی کنند. این راهکار، تیم‌ها را قادر می‌سازد تا پاسخگوی ترافیک و تهدیدهای غیرعادی یا مخربی باشند که دیگر ابزارهای امنیتی تشخیص نمی‌دهند.

راهکارهای تشخیص و پاسخ‌دهی شبکه (NDR)، ترافیک خام شبکه‌ی سازمانی را همواره پایش و تحلیل می‌کنند و یک خط مبنا از رفتار عادی شبکه ارائه می‌دهند. ابزارهای تشخیص و پاسخ‌دهی شبکه (NDR) به محض تشخیص الگوهای ترافیک شبکه‌ی مشکوک و منحرف شده از این خط مبنا، تیم‌های امنیتی را از احتمال وجود تهدید در محیط با خبر می‌کنند.

راهکارها و ابزارهای تشخیص و پاسخ‌دهی شبکه (NDR) می‌توانند امور زیر را انجام دهند:

• تشخیص ترافیک غیرعادی شبکه که ابزارهای مرسوم تشخیص نمی‌دهند و انجام این کار با استفاده از تکنیک‌های تشخیصی که مبتنی بر امضاء نیستند (مانند تحلیل رفتاری و یادگیری ماشین) است.

• مدل‌سازی خط مبنا از رفتار عادی شبکه و هشداردهی به تیم‌های امنیتی در رابطه با هر ترافیک مشکوک که خارج از محدوده‌ی عادی است.

• پایش تمام جریان‌های ترافیکی (چه ورود و خروج از شبکه و چه حرکت در درون شبکه) بدون توجه به اینکه تهدید از کجا نشأت گرفته است، به طوری که تیم‌ها دید وسیع و لازم برای تشخیص و کاهش حوادث امنیتی را داشته باشند.

• تحلیل تله‌متری یا دورسنجی خام شبکه در زمان واقعی یا نزدیک به زمان واقعی و هشداردهی به موقع تا تیم‌ها زمان پاسخگویی به حادثه را بهبود ببخشند.

• تخصیص رفتار مخرب به یک آدرس IPاخاص و انجام تحلیل‌های قانونی (forensic analyses) برای تعیین این موضوع که تهدیدها چگونه به صورت جانبی در یک محیط حرکت کرده‌اند. این امر سبب می‌شود تا تیم‌ها دریابند چه دستگاه‌های دیگری ممکن است آلوده شوند. همچنین به واکنش سریع‌تر به حادثه و مهار تهدید و حفاظت بیشتر در برابر تأثیرات نامطلوب تجاری منجر می شود.

• ارائه‌ی قابلیت‌های پاسخ‌دهی‌ای که می‌توانند پاسخ‌دهی دستی به حادثه و تلاش‌های شکار تهدید (threat hunting) را افزایش دهند، یا عملیات ها را کارآمدتر کنند و از طریق خودکارسازی (auto-mation) در زمان تیم‌ها صرفه‌جویی کنند.

همکاری شرکت برنا برای ارائه راهکار امنیتی NDR با کمپانی های Greycortex می باشد.

GREYCORTEX

شرکت GREYCORTEX، مستقر در جمهوری چک، یکی از ارائه‌دهندگان پیشرو در زمینه راهکارهای Network De-tection and Response (NDR) برای شبکه‌های فناوری اطلاعات (IT) و فناوری عملیاتی (OT) است. محصول اصلی این شرکت، GREYCORTEX Mendel، با بهره گیری از یادگیری ماشین، تحلیل پیشرفته داده‌ها و هوش مصنوعی، دید کاملی از شبکه ارائه می‌دهد و تهدیدات را در مراحل اولیه شناسایی می‌کند.

معرفی GREYCORTEX Mendel

Mendel یک راهکار NDR پیشرفته است که با تحلیل ترافیک شبکه، فعالیت‌های مخرب و تهدیدات پیشرفته را شناسایی می‌کند. این ابزار به تیم‌های امنیتی امکان می‌دهد تا رویدادهای عملیاتی و امنیتی را بررسی کرده، علت اصلی آن‌ها را بیابند و به سرعت واکنش نشان دهند.

ویژگی‌ها و قابلیت‌های کلیدی

- **دید کامل از شبکه :** Mendel تمامی دستگاه‌ها و کاربران متصل به شبکه را تا لایه ۷ (لایه کاربرد) مشاهده می‌کند و ارتباطات آن‌ها را تحلیل می‌نماید.
- **شناسایی تهدیدات پیشرفته :** با استفاده از الگوریتم های یادگیری ماشین و تحلیل رفتاری، Mendel تهدیداتی مانند باج‌افزار، تروجان، حملات صفر روز و فعالیت‌های مشکوک داخلی را شناسایی می‌کند.
- **پاسخ سریع به تهدیدات:** Mendel با ادغام با ابزارهای امنیتی مانند SIEM، فایروال‌ها و سیستم های کنترل دسترسی، امکان پاسخ خودکار و سریع به تهدیدات را فراهم می‌کند.
- **تحلیل دقیق و جرم‌شناسی :** این ابزار امکان ذخیره‌سازی داده‌های ترافیکی برای مدت طولانی را فراهم می‌کند، که به تحلیل دقیق رویدادها و یافتن علت اصلی تهدیدات کمک می‌کند.
- **پشتیبانی از شبکه‌های IT و OT :** Mendel برای محیط‌های صنعتی مانند SCADA و ICS طراحی شده و با نظارت غیرفعال، امنیت این شبکه‌ها را بدون ایجاد اختلال تضمین می‌کند.

GREYCORTEX WDR

علاوه بر GREYCORTEX Mendel، ماژول Wireless Detection and Response (WDR) را ارائه می‌دهد که نظارت مداوم بر ترافیک بی‌سیم و شناسایی تهدیدات امنیتی در شبکه‌های Wi-Fi را فراهم می کند. این ماژول با تحلیل استانداردهای IEEE ۸۰۲/۱۱، تهدیداتی مانند دستگاه‌های ناشناس، رمزنگاری ضعیف و حملات DoS را شناسایی می‌کند.

محصولات GREYCORTEX، به‌ویژه Mendel و WDR، راهکارهای جامع و پیشرفته‌ای برای شناسایی و پاسخ به تهدیدات در شبکه‌های IT و OT ارائه می دهند. با بهره‌گیری از تحلیل پیشرفته، یادگیری ماشین و ادغام با ابزارهای امنیتی موجود، این محصولات به سازمان‌ها کمک می‌کنند تا امنیت شبکه‌های خود را به‌طور مؤثر مدیریت کنند.

سرویس DRM

حقوق دیجیتال Digital rights management یا به اختصار (DRM) راهی برای محافظت از حق نسخه برداری (DMCA) برای رسانه های دیجیتال است. این رویکرد شامل استفاده از تکنولوژی هایی است که کپی کردن و استفاده از آثار دارای حق نسخه برداری و نرم افزار اختصاصی را محدود می کند. به طریقی، مدیریت حقوق دیجیتال به ناشران یا نویسندگان اجازه می دهد تا آنچه را که کاربران می توانند با نرم افزار های خریداری شده انجام دهند را کنترل کنند.

برای شرکت ها، اجرای سیستم های مدیریت حقوق دیجیتال یا فرآیندها می تواند به جلوگیری از دسترسی کاربران به یا استفاده از دارایی های خاص کمک کند و به سازمان اجازه می دهد که از مسائل حقوقی ناشی از استفاده غیر مجاز جلوگیری کند. امروزه DRM نقش مهمی در امنیت داده ایفا می کند.

اگر چه محتوای دیجیتال توسط قوانین حق تکثیر محافظت می شود، نظارت بر وب و گرفتن مجرمان بسیار دشوار است. با افزایش خدمات مبادله ی فایل به صورت peer-to-peer مانند سایت های torrent، دزدی آنلاین مانند زهری برای محصولات تجاری شده است. فن آوری های DRM کسانی را که درگیر دزدی آنلاین هستند نمی گیرند در عوض، امکان سرقت یا اشتراک محتوا را در همان وهله ی اول نمی دهند.

مدیریت عملکرد دیجیتال چگونه کار می کند؟

در اغلب موارد، مدیریت حقوق دیجیتال شامل کد هایی است که کپی را ممنوع کرده یا کد هایی که محدودیت زمان یا تعداد دستگاه هایی را که ممکن است به یک محصول خاص دسترسی پیدا کند محدود می کند.

ناشران، نویسندگان و سایر سازندگان محتوا از یک برنامه کاربردی استفاده می کنند که رسانه ها، داده ها، کتاب الکترونیکی، محتوا، نرم افزار یا هر گونه مواد دارای حق تکثیر را رمزگذاری می کند. فقط با کلید رمزگشایی می توان دسترسی پیدا کرد.

DRM به شما اجازه می دهد تا:

۱. دسترسی کاربران به محصول و محتوا محدود کرده و ارسال، ویرایش و ذخیره آن را ممنوع کنید.

۲.محدود کردن یا جلوگیری از چاپ محتوا

۳. تصویر برداری از محتوا را ممنوع کنید.

۴. یک تاریخ انقضا را در سند یا رسانه تنظیم کنید که بعد از آن امکان دسترسی نباشد.

۵. دسترسی به آدرس های IP خاص، مکان‌ها یا دستگاه ها محدود باشد. بدان معنی که رسانه های شما برای ipهای ایران در دسترس باشد.

۶. ایجاد watermark روی آثار هنری جهت تثبیت و ایجاد مالکیت.

۷. مدیریت حقوق دیجیتال به ناشران برای مشاهده افراد و زمانهای دسترسی به رسانه ها، محتوا یا نرم افزارها استفاده می شود. به عنوان مثال، می توانید ببینید که یک کتاب الکترونیکی به چه صورت دریافت شده، چاپ شده و چه کسی به آن دسترسی پیدا کرده است.

همکاری شرکت برنا برای ارائه راهکار امنیتی DRM با کمپانی Seclore می باشد.

SECLORE

Seclore DRM یکی از پیشرفته‌ترین راهکارهای مدیریت حقوق دیجیتال (Digital Rights Management) در جهان است که توسط شرکت Seclore ارائه می‌شود. این محصول به سازمان‌ها کمک می‌کند تا کنترل کامل و دائمی بر فایل‌ها و اطلاعات حساس خود—even پس از اشتراک‌گذاری آن‌ها با کاربران داخلی یا خارجی—داشته باشند.

شرکت Seclore با بیش از ۱۰۰۰ مشتری سازمانی در بیش از ۳۰ کشور، یکی از شرکت‌های پیشرو در حوزه امنیت اطلاعات است که تمرکز اصلی آن بر محافظت از داده‌ها در لحظه، بدون وابستگی به محیط ذخیره‌سازی یا حمل‌ونقل است.

قابلیت‌های کلیدی DRM برند Seclore:

- **کنترل سطح دسترسی به محتوا:** سازمان‌ها می‌توانند به‌طور دقیق تعیین کنند چه کسی به محتوا دسترسی داشته باشد و چه عملیاتی (خواندن، چاپ، ویرایش، اسکرین‌شات، فوروارد) مجاز است.
- **رمزنگاری پویا و قابل سفارشی‌سازی:** فایل‌ها به صورت خودکار رمزنگاری می‌شوند و فقط توسط کاربران مجاز و در شرایط مشخص (مکان، زمان، IP، دستگاه خاص) قابل مشاهده هستند.
- **اعمال محدودیت زمانی و مکانی:** می‌توان زمان اعتبار یک سند را تعیین کرد یا دسترسی را فقط به آدرس‌های IP، کشور یا دستگاه‌های خاص محدود کرد.
- **واترمارک پویا (Dynamic Watermarking):** درج خودکار نام کاربر، تاریخ یا شماره IP به‌صورت نامرئی یا قابل مشاهده روی فایل‌ها برای جلوگیری از نشت محتوا از طریق اسکرین‌شات یا پرینت.
- **ردیابی و گزارش‌دهی کامل:** تمامی فعالیت‌ها روی فایل‌ها به‌صورت دقیق ثبت می‌شوند؛ از جمله زمان باز شدن، مکان دسترسی، عملیات انجام‌شده و حتی تلاش‌های ناموفق برای دسترسی.
- **قابلیت لغو دسترسی پس از اشتراک‌گذاری:** حتی اگر فایل برای فردی ایمیل یا آپلود شده باشد، می‌توان بعداً دسترسی او را لغو کرد یا فایل را از راه دور غیرقابل استفاده ساخت.

ویژگی‌های محصول DRM برند SECLORE:

- سازگاری با Microsoft ۳۶۵، Google Workspace، Salesforce و دیگر ابزارهای سازمانی
- رعایت الزامات قانونی مانند GDPR، HIPAA، ISO ۲۷۰۰۱
- افزایش امنیت داده‌ها بدون ایجاد اختلال در روند کاری کاربران

در نهایت، Seclore DRM راهکاری هوشمندانه برای حفاظت مستمر از دارایی‌های دیجیتال در هر مکان و زمان است—حتی خارج از مرزهای شبکه سازمانی.

ابزار Firewall

فایروال و نقش حیاتی آن در امنیت سازمان‌ها

فایروال (Firewall) یا دیواره آتش، یکی از مهم‌ترین ابزارهای امنیت شبکه است که به‌منظور کنترل و نظارت بر ترافیک ورودی و خروجی شبکه استفاده می شود. فایروال‌ها به‌صورت نرم‌افزاری یا سخت‌افزاری در دسترس هستند. در محیط‌های سازمانی، استفاده از فایروال به دلیل امنیت بالا، عملکرد مستقل از سیستم عامل و قابلیت‌های پیشرفته توصیه می‌شود.

فایروال یک دستگاه مستقل است که معمولاً بین شبکه داخلی سازمان و اینترنت قرار می‌گیرد. این دستگاه به‌عنوان یک گذرگاه هوشمند، تمام داده‌هایی را که وارد یا خارج می‌شوند بررسی کرده و تنها ترافیک مجاز را عبور می‌دهد. مانند درب ورودی یک خانه که فقط به افراد شناخته‌شده اجازه ورود می‌دهد، فایروال نیز همین نقش را برای داده‌ها ایفا می‌کند.

مزایای فایروال

• **جداسازی محیط امن از محیط ناامن:** فایروال به عنوان لایه‌ای میان شبکه سازمانی و دنیای بیرونی، مانع دسترسی غیرمجاز به منابع داخلی می‌شود.

• **کنترل و فیلترینگ ترافیک:** با استفاده از قوانین سفارشی، می‌توان مشخص کرد کدام پورت‌ها، آدرس ها یا پروتکل‌ها اجازه تبادل داده دارند.

• **حفاظت در برابر تهدیدات پیچیده:** بسیاری از فایروال‌های مدرن دارای قابلیت‌هایی مانند تشخیص و جلوگیری از نفوذ (IPS/IDS)، شناسایی رفتارهای مشکوک، فیلترینگ وب، کنترل برنامه‌ها، و حتی مقابله با حملات DDoS هستند.

• **عملکرد مستقل از کلاینت‌ها:** برخلاف فایروال های نرم‌افزاری، فایروال بر روی هیچ دستگاهی نصب نمی‌شود و به سیستم‌عامل خاصی وابسته نیست، در نتیجه نفوذپذیری کمتری دارد.

• **مدیریت مرکزی و پایش لحظه‌ای:** مدیران شبکه می‌توانند از طریق پنل مدیریتی، تنظیمات امنیتی را به‌روز کرده، گزارش‌گیری کنند و رخدادهای مشکوک را بررسی نمایند.

فایروال یکی از مؤثرترین راهکارهای دفاعی در برابر تهدیدات سایبری است. بدون استفاده از چنین تجهیزاتی، راه برای هکرها، بدافزارها و حملات سازمان‌یافته باز خواهد بود. این ابزار، لایه‌ای حیاتی از امنیت را برای هر سازمان فراهم می‌کند و باید به‌عنوان بخش جدانشدنی از معماری امنیتی شبکه در نظر گرفته شود.

همکاری شرکت برنا برای ارائه راهکار امنیتی Firewall با کمپانی های Fortinet می باشد.

FortiGate محصول فایروال نسل بعدی (Next Generation Firewall - NGFW) از شرکت Fortinet است که یکی از معتبرترین برندهای جهان در حوزه امنیت سایبری به شمار می‌رود. FortiGate یک راهکار سخت‌افزاری و نرم افزاری است که برای حفاظت از شبکه‌های سازمانی در برابر انواع تهدیدات پیچیده طراحی شده است.

معرفی شرکت Fortinet

Fortinet یک شرکت پیشرو در زمینه امنیت شبکه است که در سال ۲۰۰۰ تأسیس شد. این شرکت با ارائه طیف گسترده‌ای از محصولات امنیتی، از جمله فایروال، EDR، SD-WAN، امنیت ابری، و Zero Trust، به سازمان‌ها کمک می‌کند تا از دارایی‌های دیجیتال خود در برابر حملات سایبری محافظت کنند. محصولات Fortinet به دلیل بهره‌گیری از سیستم‌عامل اختصاصی FortiOS، عملکرد بالا و امنیت پیشرفته‌ای ارائه می‌دهند.

ویژگی‌های فایروال FortiGate

۱. **فیلترینگ ترافیک بازرسی عمیق (Deep Packet Inspection):** FortiGate قابلیت بازرسی پیشرفته ترافیک را دارد و می‌تواند تهدیدات پنهان در لایه‌های مختلف شبکه را شناسایی و مسدود کند.

۲. **تشخیص و جلوگیری از نفوذ (IPS):** با استفاده از سیستم IPS داخلی، این فایروال می‌تواند تهدیدات روز صفر، حملات Exploit و سوءاستفاده از آسیب‌پذیری‌ها را شناسایی کند.

۳. **کنترل نرم‌افزار و فیلترینگ وب:** FortiGate امکان کنترل دسترسی به برنامه‌ها و وب‌سایت‌ها را بر اساس سیاست‌های امنیتی فراهم می‌کند تا مصرف پهنای باند مدیریت و امنیت اطلاعات حفظ شود.

۴. **پشتیبانی از VPN و Remote Access:** اتصال ایمن کاربران از راه دور به شبکه سازمانی از طریق IPsec یا SSL VPN، از دیگر قابلیت‌های FortiGate است.

۵. **پشتیبانی از SD-WAN و تقسیم‌بندی شبکه:** این محصول، انتخابی عالی برای شبکه‌های مدرن با نیاز به چندین نقطه دسترسی، مدیریت WAN و ایجاد معماری مبتنی بر Zero Trust است.

فایروال FortiGate با عملکرد بالا، مدیریت مرکزی، انعطاف‌پذیری در پیاده‌سازی و امنیت لایه‌ای، یک انتخاب قابل اعتماد برای سازمان‌هایی است که به دنبال یک راهکار امنیتی قدرتمند و مقیاس‌پذیر هستند. این محصول در اندازه‌ها و مدل‌های مختلف برای سازمان‌های کوچک تا بزرگ عرضه می‌شود.

SANGFOR

Sangfor NGAF یکی از پیشرفته‌ترین فایروال‌های نسل بعد (Next Generation Application Firewall) است که برای محافظت از شبکه سازمان‌ها در برابر تهدیدات پیچیده و روزافزون سایبری طراحی شده است. این محصول، راهکاری جامع برای شناسایی، پیشگیری و پاسخ به تهدیدات ارائه می‌دهد و در عین حال مدیریت امنیت را ساده‌سازی می‌کند.

Sangfor Technologies یکی از شرکت‌های نوآور در حوزه امنیت سایبری، رایانش ابری و زیرساخت شبکه است که در سال ۲۰۰۰ تأسیس شده و در بیش از ۶۰ کشور جهان حضور دارد. این شرکت با تمرکز بر تحقیق و توسعه، محصولات خود را با رویکردی مبتنی بر هوش مصنوعی و امنیت پیشگیرانه طراحی کرده و توانسته اعتماد هزاران سازمان دولتی و خصوصی را جلب کند.

ویژگی‌های کلیدی Sangfor NGAF

۱. **تشخیص و پیشگیری هوشمند تهدیدات (ATP):** با تکیه بر تحلیل رفتاری، تهدیدات ناشناخته، حملات هدفمند و باج‌افزارها به صورت پیشگیرانه شناسایی و مسدود می‌شوند.

۲. **سیستم مدیریت ریسک جامع (IRM):** ارائه دیدی دقیق و متمرکز از وضعیت امنیتی دارایی‌های شبکه و سطح تهدیدات در لحظه، برای تسهیل تصمیم‌گیری سریع و آگاهانه.

۳. **بازرسی عمیق ترافیک و کنترل لایه ۷:** توانایی شناسایی و کنترل بیش از ۳۵۰۰ برنامه مختلف، همراه با تعیین سیاست‌های امنیتی مبتنی بر محتوا و رفتار کاربران.

۴. **ترکیب قابلیت‌های امنیتی در یک پلتفرم:** از جمله فیلترینگ URL، ضدویروس، ضدباج‌افزار، کنترل محتوا، VPN و IPS که باعث افزایش کارایی و کاهش پیچیدگی‌های مدیریتی می‌شود.

۵. **ادغام با سایر راهکارهای Sangfor:** از جمله EDR، NDR و سیستم‌های پاسخ خودکار، که همگی در راستای اجرای مدل امنیتی Zero Trust عمل می کنند.

Sangfor NGAF گزینه‌ای قابل اتکا برای سازمان هایی است که به دنبال امنیت هوشمند، قابلیت تطبیق با تهدیدات نوظهور و مدیریت ساده‌تر زیرساخت امنیتی خود هستند. این فایروال با بهره گیری از فناوری‌های پیشرفته، تجربه‌ای امن و پایدار برای شبکه‌های امروزی فراهم می‌آورد و نیازهای امنیتی انواع کسب‌وکارها را پاسخ می‌دهد.

برخی از مشتریان ما

سخن پایانی

شرکت «مدیران شبکه برنا» با پشتوانه‌ای از تجربه، دانش تخصصی و تمرکز بر ارائه راهکارهای نوین امنیت شبکه، همواره تلاش کرده است تا نیازهای امنیتی سازمان‌ها و شرکت‌ها را در بالاترین سطح پوشش دهد. ما با بهره‌گیری از محصولات و فناوری های برتر جهانی در حوزه‌هایی چون DLP، XDR، EDR، فایروال، آنتی‌ویروس، DRM و NDR، سعی کرده‌ایم فضای سایبری امن و پایدار برای مشتریان خود فراهم کنیم.

مأموریت ما فراتر از ارائه محصول است؛ ما به دنبال ارائه راهکارهایی هستیم که نه تنها امنیت شبکه و داده های سازمان‌ها را تضمین می‌کنند، بلکه امکان مدیریت هوشمند تهدیدات، انطباق‌پذیری با الزامات قانونی، و افزایش بهره‌وری فناوری اطلاعات را نیز به همراه دارند. در این مسیر، تیم فنی متخصص، پشتیبانی سریع و ارائه مشاوره دقیق، از ارزش‌های محوری شرکت ما به‌شمار می‌آیند.

ما باور داریم که امنیت سایبری صرفاً یک محصول نیست، بلکه یک تعهد دائمی و یک رویکرد حرفه‌ای برای حفظ سرمایه‌های اطلاعاتی سازمان‌هاست. شرکت مدیران شبکه برنا همواره همراهی قابل اعتماد برای سازمان‌ها و مدیران فناوری اطلاعات بوده و خواهد بود.

در پایان، امیدواریم این رزومه بتواند نمایی شفاف از توانمندی‌ها، حوزه‌های تخصصی و خدمات ما ارائه دهد و زمینه‌ساز همکاری‌های حرفه‌ای و مؤثر با سازمان شما باشد. آماده‌ایم تا در کنار شما، گامی مطمئن در مسیر توسعه و امنیت برداریم.