شرکت مهندسی امن ارتباط سینداد

خدمات بهبود SIEM

با تنظیم صحیح SIEM مرکز عملیات امنیت خود، خطاهای ناشی از هشدارهای غلط را کاهش دهید.

SIEM یا سیستم مدیریت اطلاعات و رخدادهای امنیتی، لاگ ها و داده‌های امنیتی سرتاسر سازمان را جمع‌آوری و با ایجاد هشدار، به شما این اجازه را می‌دهد که از رخدادهای امنیتی سطوح مختلف با خبر شوید. با این حال، در صورتی که SIEM سازمان شما از معماری صحیح و استانداردی برخوردار نباشد، ممکن است شما را در حجم انبوهی از داده‌ها، لاگ‌ها و رخدادها غرق کند و مانع از تشخیص درست رخدادهای امنیتی و بالطبع، تهدیدها و حمله‌های امنیتی شود.

در طول بازطراحی معماری، متخصصین با تجربه ما هشدارها، رخدادها و قواعد SIEM سازمان شما را تنظیم می‌کنند تا داده هایی عملیاتی و در عین حال مختصر برای شما ایجاد شوند. در این خدمت سیستم SIEM شما ارتقا پیدا کرده تا میزان هشدارهای کاذب و لاگ‌های بی اهمیت به کمینه حالت خود رسیده و تیم امنیتی شما صرفا از رخدادهای مهم باخبر شود.

سطح امنیتی خود را بهبود ببخشید

- شناسایی راه‌های نفوذ مهاجمان
- ایجاد قواعد پیشرفته برای خلع سلاح کردن مهاجمان
- طراحی موارد کاربری اختصاصی برای رفع نقاط کور
- کاهش هشدارهای تکراری و نامربوط
- ایجاد رخداد برای برنامه‌ها و سیستم های افزوده شده جدید
- اولویت بندی رخدادها

کاهش هشدارهای سربار

محیط‌های شبکه‌ای دائما در حال رشد و گسترش با سخت‌افزارها، نرم‌افزارها، برنامه‌ها و داده‌های جدید هستند و پیوسته با استخدام نیروی انسانی، لازم است به آن‌ها دسترسی داده شود. در صورتی که به این تغییرات پاسخ داده نشود، هشدارهای ایجاد شده از SIEM، تبدیل به سربار برای تیم امنیت می شود. همانطور که تجهیزات شبکه با گذر زمان و تغییر ساختار شبکه نیازمند تغییر پیکربندی هستند، SIEM نیز لازم است به صورت دوره‌ای و با تغییرات شبکه مجدا تنظیم شده تا شما از امنیت سطوح مختلف سازمان خود اطمینان پیدا کنید.

خدمات بهبود SIEM

با تنظیم صحیح SIEM مرکز عملیات امنیت خود، خطاهای ناشی از هشدارهای غلط را کاهش دهید.

بهبود دقت هشدارها

تنظیم کردن SIEM و بازطراحی معماری آن کاری تخصصی و زمان‌بر است که به متخصصین امنیتی با مهارت‌های ویژه احتیاج دارد. متخصصین ما همگام با کارشناسان شما، به بررسی این سیستم پیچیده و جامع می‌پردازند تا آن را به دقیق ترین شکل اثربخش و کارآمد سازند. تنظیم دقیق جمع‌آوری داده‌ها و لاگ‌ها، خودکار سازی قواعد، موارد کاربری و رویه های ذخیره شده باعث می‌شود هشدارهای کاذب به حداقل رسیده و SIEM به صورت منظم و طبق برنامه کار کند.

کیفیت داده‌ها در عملکرد SIEM تاثیر می‌گذارد

داده‌ها و لاگ‌های غنی شده باعث می‌شوند اطلاعاتی که متخصصین شما از SIEM سازمان دریافت می‌کنند زمان‌بندی شده، دقیق و بخش‌بندی شده باشد. مهندسی امن ارتباط سیناد با اجرای تنظیمات دوره‌ای به شما کمک می‌کند هشدارهای کاذب را رفع کرده و قواعد یکپارچه‌سازی شده‌ای را در SIEM خود اجرا نمایید. در خدمت بازطراحی و تنظیم، متخصصین ما با اجرای اقدامات زیر، کیفیت داده‌ها و لاگ‌های جمع‌آوری شده و قواعد تشخیص SIEM شما را بالاتر می‌برند:

- سرشماری نقاط پایانی و تجزیه و تحلیل شکاف‌های امنیتی موجود جهت بررسی وضعیت رصد و لاگ‌گیری در آن‌ها
- ارزیابی راه‌های نفوذ تهدیدها جهت ایجاد موارد کاربری و هشدارهای جدید
- تعریف سطوح اولویت بندی برای منظم سازی هشدارها و رسیدگی به مهم‌ترین آن‌ها
- شناسایی اتصالات داخلی و خارجی جهت شناسایی نقاط بالقوه نفوذ به سازمان
- بازبینی اطلاعات تهدیدهای جدید و استراتژی ورود آن‌ها برای هشیار کردن SIEM
- حذف رصد برنامه‌ها و سیستم‌های حذف شد
- ایجاد قواعد برای مدیریت تغییر سطح دسترسی کاربران

درباره خدمات شرکت مهندسی امن ارتباط سیناد

شرکت مهندسی امن ارتباط سیناد خدمات خود را در دو حوزه
آفندی(Offensive)
پدآفندی(Defensive)
به سازمان‌ها ارائه می‌کند که در حوزه آفندی مواردی مانند تست نفوذ، رد تیمینگ، شبیه‌سازی حمله‌های پیشرفته مانا(APT)و ... را در بر می‌گیرد، و در حوزه پدآفندی شامل خدماتی مانند
پاسخ به حادثه(Incident Response)،
بازطراحی و معماری SIEM،
ارزیابی تسخیرشدگی(CompromiseAssessment)
و ... می‌شود.

ما به مشتریان خود کمک می‌کنیم تا محیط سایبری خود را ارزیابی کرده و چشم‌انداز امنیتی خود را گسترش دهند. توان دفاعی خود در مقابل حمله‌های دنیای واقعی را بسنجند، به حوادث امنیتی پاسخ دهند، ردپای تهدیدهای سازمان خود را بشناسند، و در نهایت پس از مواجه با نفوذهای امنیتی در سازمان خود، دوباره به حالت عادی بازگردند. با سامانه‌های ابری (SaaS)و مدیریت شده(Managed)امنیتی به شما کمک می‌کنیم مخاطرات امنیتی مرتبط با بخش‌های ضروری سازمان شما را به طور کامل شناخته و تهدیدهای مرتبط با خود را شناسایی و ردیابی کرده و از وقوع حمله‌هایی که سعی در تخریب کسب‌وکار و برند شما دارند، جلوگیری کنید.

ما شما را از شکار به شکارچی تبدیل می‌کنیم.

www.sindadsec.ir
info@sindadsec.ir
sindadsec
sindadsec
sindadsec