اطلاعات فنی محصولات

شرکت مهندس امن ارتباط سینداد (سینداسک)

با ما شکار نمی شوید!

پانای TDR

معرفی محصول

سامانه تشخیص پیشرفته تهدید در تمامی سطوح سازمان

با به‌کارگیری پانای، کلیه لاگ‌ها در یک محیط یکپارچه در اختیار شماست.
پانای به‌عنوان بخشی از سامانه یکپارچه نخجیرپان (XDR) عمل می‌نماید و جمع‌آوری و یکپارچه‌سازی لاگ‌ها را به عهده دارد.

پانای، تهدیدهای مختلف لایه‌های امنیتی سازمان را شناسایی کرده و به آن‌ها پاسخ می‌دهد. این سامانه که یکی از مهم‌ترین اجزا دفاع امنیتی به شمار می‌رود، مثل یک رادار هوشمند، نسبت به جمع‌آوری و دسته‌بندی و لاگ‌ها اقدام و به تشخیص تهدیدها و حمله‌های سایبری کمک شایانی می‌نماید.

تجمیع‌سازی، همسان‌سازی و غنی‌سازی اطلاعات

یکی از اصلی‌ترین وظایف راهکار پانای (SIEM)، جمع‌آوری لاگ شبکه و نقاط پایانی جهت تحلیل و همبسته‌سازی آن‌ها است. این راهکار یکپارچه‌سازی شده، کلید پاسخ به مسائل متعددی را ارائه می‌دهد، از جمله:

- مدیریت لاگ‌ها: جست‌وجو در سطوح مختلف سازمان، شناسایی رویدادهای امنیتی بخش IT و امنیت و بررسی سریع مشکلات امنیتی
- تجزیه‌وتحلیل: حداقل‌سازی هشدارهای امنیتی بی‌معنی، تشخیص فعالیت‌های مخرب در سرتاسر سازمان به‌وسیلهٔ موارد کاربردی تشخیص (Use Case) و اولویت‌بندی هشدارهای امنیتی بر اساس میزان پایداری تهدیدها

راهکار SIEM (مدیریت اطلاعات و رویدادهای امنیتی)، سازمان را قادر می‌سازد به ماژول‌های متعدد، امکانات مدیریتی و قواعد امنیتی

امکانات اصلی

برای اینکه زمان شناسایی و زمان پاسخ‌دهی به تهدیدهای امنیتی به کمترین میزان خود برسند، SIEM امکاناتی را فراهم می‌سازد تا اجزای مختلف سیستم تشخیص به طور دقیق فعالیت کنند.

- جمع‌آوری اطلاعات: گردآوری، ساده‌سازی و تجزیه و تحلیل داده‌ها و لاگ‌ها از نقاط پایانی و تجهیزات شبکه
- کشف مشکل امنیتی: بهره‌گیری از تعداد زیادی از قواعد از پیش تعریف شده در سامانه، و امکان تعریف قواعد جدید
- غنی‌سازی: تجزیه‌وتحلیل تهدیدها، استفاده از هوش تهدید و اولویت‌بندی رویدادها به جهت متمرکزسازی توجه تیم مرکز عملیات امنیت (SOC)
- بازسازی: مشاهده کامل جریان ورود تهدیدها، همراه با جزئیاتی مانند سیستم‌های آلوده شده و استراتژی آن‌ها به‌صورت یکپارچه‌سازی شده

مزایای اصلی

- آخرین قواعد رفتاری حمله‌های جدید
- شخصی‌سازی بر اساس نیاز سازمان
- شکار تهدیدها در تمام سطوح لاگ
- سیستم غنی‌سازی لاگ‌ها
- سیستم غنی‌سازی هشدارها
- امکان دریافت لاگ از هر منبع لاگ استاندارد
- جستجوی بسیار فوری در لاگ‌ها
- دسته بندی حمله‌ها و هشدارها بر اساس MITRE ATT&CK
- سازگاری کامل با هویان (EDR) و هولاد (NDR)
- امکان پیاده‌سازی در شبکه‌های بدون اینترنت

دسترسی پیدا کند تا اهداف اصلی مرکز عملیات امنیت را با کمترین هزینه مادی و معنوی محقق سازد.
می توان به اهداف زیر اشاره نمود:

- رصد نمودن تهدیدات سایبری،
- شکار تهدیدها،
- بررسی، تجزیه و تحلیل تهدیدها

021-91031548 021-28420878
INFO@sindadsec.ir
تهران، بزرگراه رسالت، کوچه هجدهم، خیابان خواجه عبدالله انصاری، پلاک ۴، طبقه ۱
www.sindadsec.ir