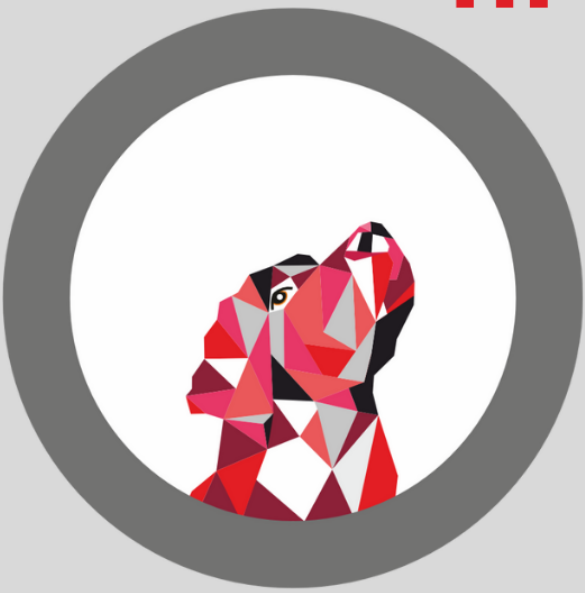
اطلاعات فنی محصولات

شرکت مهندس امن ارتباط سینداد (سینداداسک)

با ما شکار نمی شوید!

نخجیرپان XDR



معرفی محصول

راهکار گسترده شناسایی و پاسخ

سامانه نخجیرپان یک محصول امنیت سایبری است که با ادغام ابزارهای امنیتی و مهارت‌های متخصصین حوزه امنیت، اقدام به نظارت، شکار تهدیدات و ارائه پاسخ در برابر حملات و تهدیدات پیچیده امنیتی می‌نماید.

بزرگ‌ترین مزیت نخجیرپان، در ابتدا شکار و شناسایی بسیار سریع تهدیدات و سپس پیشگیری و کاهش تأثیرات مخرب حملات و تهدیدات امنیتی می‌باشد. این کارکرد به‌صورت در لحظه و با ارائه پاسخ فوری به تهدیدات و بدون نیاز به نیروی انسانی مضاعف ارائه می‌شود.

نخجیرپان محصولی است که امکان کشف حملات، رسیدگی به حملات و پاسخ به آنها را به‌صورت یکپارچه فراهم می‌نماید. در هر سازمان طیف متنوعی از ابزارهای امنیتی مورداستفاده قرار می‌گیرد و هدف اصلی نخجیرپان ایجاد همبستگی (Correlation) در داده‌های ورودی و امکان افزایش حداکثری بهره‌وری در کشف و شناسایی و رسیدگی به حملات می‌باشد. این افزایش بهره‌وری با استفاده از تحلیل خودکار و به‌کارگیری هوش مصنوعی در کشف حملات تکمیل می‌گردد.

در واقع نخجیرپان به گونه طراحی شده که طیف وسیعی از حملات را مورد پوشش قرار داده و با ارائه پاسخ لحظه‌ای به حملات، ارزش‌افزوده فراوانی در لایه امنیت سازمان ایجاد نماید. این حملات شامل ابزارهای ساده هکری تا حملات پیچیده؛ مانند باج‌افزارها و Lateral movement خواهند بود و همگی در یک بستر یکپارچه رسیدگی خواهد شد.

شناسایی تهدیدهای امنیتی پیشرفته با روش‌های سنتی و بخصوص در مراحل اولیه بسیار دشوار خواهد بود؛ زیرا این تهدیدها بین لاگ‌ها و داده‌های امنیتی پنهان گردیده و باگذشت زمان منتشر می‌شوند. ایجاد همبستگی و تجمیع اطلاعات از یک سو و پاسخ فوری به رخداد از سوی دیگر، طیف وسیعی از حملات پنهان را آشکار می‌نماید.

سامانه نخجیرپان متشکل از ابزارهای امنیتی زیر می‌باشد:

- هوپان EDR (راهکار شناسایی و پاسخ در نقطه پایانی): سیستم تشخیص و پاسخ‌دهی در نقاط پایانی که شامل سیستم‌عامل‌ها، ماشین‌ها، کلاینت‌ها و سرورها می‌باشد.
- هولاد NDR (راهکار تشخیص و پاسخ در شبکه): کلیه ترافیک شبکه در نقاط دلخواه را رصد کرده و تهدیدهای مرتبط با آن را شناسایی و از آنها جلوگیری می‌نماید.
- پانای TDR (راهکار تشخیص و پاسخ به تهدید): داده‌های امنیتی موردنیاز برای کشف رخدادها و تهدیدهای امنیتی را از تمامی سطوح جمع‌آوری و یکپارچه می‌کند تا با انجام تجزیه‌وتحلیل بر روی آن‌ها، مانع از انجام فعالیت‌های مخرب در سازمان شود.
- وریا TIP (راهکار شناسایی و پاسخ باهوش تهدید): این سیستم به تیم امنیتی کمک می‌کند از جدیدترین تهدیدهای موجود در دنیای واقعی، مانند بدافزارها، باج‌افزارها، تروجان‌ها، تهدیدهای APT و ... باخبر شده و با به‌کارگیری تکنیک، تاکتیک و فرایندهای (TTPs) آن‌ها را شکار نماید.
- هویر ASM (راهکار نظارت بر سطوح حملات): این سیستم با بررسی سطوح حمله، از نشت اطلاعات و آسیب‌پذیری‌های فعال مطلع می‌گردد.
- تلماسه Sandbox (راهکار رفتارشناسی فایل‌های مشکوک): جهت اطمینان از عملکرد سیستم‌ها، برنامه‌ها و فایل‌های مشکوک و یا جدید، پیش از انتقال به محیط عملیاتی استفاده می‌گردد.
- قناری Canary (راهکار گمراه‌سازی مهاجم): با استفاده از محیطی شبیه‌سازی‌شده، مهاجم را گمراه کرده و رفتارها و تکنیک‌های مهاجم یا فایل آلوده بررسی می‌گردد.
- داروک VDR (راهکار مدیریت آسیب‌پذیری‌ها): ضمن شناسایی و مدیریت آسیب‌پذیری‌ها، قابلیت اولویت بندی، بررسی ریسک و آسیب‌پذیری‌ها را فراهم می آورد.

*حتی درصورتی‌که هر سازمان بخشی از سرویس‌های فوق را از پیش به‌واسطه سیستم‌های دیگر پیاده‌سازی نموده باشد، امکان یکپارچگی و دریافت لاگ‌ها استاندارد بین ماژول‌ها فراهم می‌باشد.

تمامی این راهکارها با یکدیگر در جهت مدیریت و نظارت کامل ادغام و یکپارچه‌سازی شده و قابلیت پیاده‌سازی SOC نسل بعد (NextGen SOC) را برای سازمان‌ها فراهم می‌نماید.

مزایای اصلی

- اولویت‌بندی رخدادها
- شکار تهدیدات
- امکان رسیدگی به رخدادها (Investigate)
- پاسخ‌دهی هوشمند و خودکار
- امکان ارتباط و یکپارچه‌سازی با محصولات امنیتی موجود و مستقر در سازمان‌ها
- کاهش هزینه موردنیاز جذب و استخدام متخصصین متعدد

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