اطلاعات فنی محصولات

با ما شکار نمی شوید!

هوپان EDR

معرفی محصول

راهکار شناسایی و پاسخ در نقطه پایانی

هوپان بعنوان بخشی از سامانه یکپارچه نخجیرپان (XDR) عمل می نماید و امنیت نقاط پایانی را به عهده دارد.

تهدیدهای امنیتی پیشرفته، در مراحل اولیه و با روش‌های سنتی، به‌سختی قابل‌شناسایی هستند. این تهدیدها بین لاگ‌ها، داده‌های امنیتی و هشدارهای راهکارهای تشخیص و دفاع، پنهان و باگذشت زمان منتشر می‌شوند. تحلیلگران امنیتی همواره برای بررسی و کشف آن‌ها با استفاده از ابزارهای غیریکپارچه تشخیص حمله در میان انبوهی از داده‌ها، در حال تلاش هستند.

راهکار هوپان (EDR) یک ابزار امنیتی است که کلیهٔ رخدادها و رفتارهای مشکوک ایجاد شده در نقاط پایانی را نظارت و جمع‌آوری می‌نماید. سپس با استفاده از قابلیت همبسته سازی (Correlation) و نظارت بلادرنگ، امکان پاسخگویی خودکار مانند ایزوله‌سازی نقطه پایانی را به‌صورت بلادرنگ فراهم می‌سازد.

هوپان، این داده‌ها را با استفاده از یک رویکرد جامع برای تشخیص و پاسخ تجزیه می‌کند، همچنین داده‌های شناسایی شده و بسیار جزئی را به‌صورت عمیق در چندین لایه امنیتی جمع‌آوری و مرتبط می‌کند. با تجزیه‌وتحلیل خودکار این مجموعه از داده‌ها، تهدیدها سریع‌تر شناسایی می‌شوند.

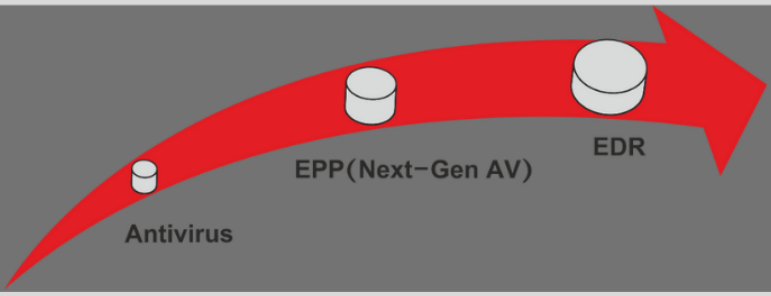
در هوپان، تیم دفاع آماده است تا با تمرکز و به‌دست‌آوردن زمان بیشتر، اهداف امنیتی سازمان را به‌راحتی دنبال کند.

امکانات اصلی

- به‌کارگیری آخرین قواعد رفتاری حملات جدید و شاخص‌های حملات در نقطه پایانی
- نظارت بر صحت فایل‌ها و داده‌ها در نقطه پایانی
- شکار تهدیدها در نقطه پایانی
- تشخیص حملات ناهنجار در نقطه پایانی
- تشخیص فایل‌های ناهنجار در نقطه پایانی
- دسترسی به فرایندها، هندل‌ها و سوکت‌ها در نقطه پایانی
- نمایش لیست دارایی‌های نرم‌افزاری و سخت‌افزاری
- امکان پرس‌وجو از نقطه پایانی (OS Query)
- امکان اسکن فایل‌ها بر اساس Yara
- تشخصی و جلوگیری بدافزار
- تشخیص باج‌افزار
- جلوگیری و کشف حملات بدون فایل در نقطه پایانی
- جستجو بر اساس IOC (نشانه نفوذ)
- دسته‌بندی حملات و هشدارها بر اساس MITRE ATT&CK
- به‌کارگیری هوش تهدید در طی یکپارچگی با راهکار "وریا" (TIP)
- امکان پیاده‌سازی در شبکه‌های بدون اینترنت
- قابلیت یکپارچگی با ابزارهای هوش تهدید
- جلوگیری خودکار از گسترش حملات

مزایای اصلی

- ارائه قابلیت‌های دفاع، تشخیص و واکنش سریع و بهبودیافته در نقطه پایانی
- بهبود و افزایش بهره‌وری پرسنل عملیاتی
- امکان پاسخ‌دهی لحظه‌ای در نقطه پایانی
- سازگاری عملکرد یکپارچه با راهکارهای "هولاد" (NDR) و "پانای" (TDR)
- نگارش سناریوی قواعد پیچیده رفتاری بر اساس تاکتیک‌ها، تکنیک‌ها و فرایندها
- هزینه کمتر مشتری برای شناسایی و پاسخ موثر به تهدیدهای امنیتی



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