اطلاعات فنی محصولات

با ما شکار نمی شوید!

وریا TIP

معرفی محصول

راهکار شناسایی و پاسخ به هوش تهدید

به‌کارگیری هوش تهدید به‌منظور درک صحیح تهدیدات و ریسک‌ها
وریا به‌عنوان بخشی از سامانه یکپارچه نخجیرپان (XDR) عمل می‌نماید و ابزارهای موردنیاز هوش تهدید را فراهم می‌آورد.

به‌کارگیری ابزارهای هوش تهدید در سازمان باعث ایجاد چشم‌انداز واقعی از وضعیت امنیتی و ریسک‌های بالقوه موجود در سازمان می‌گردد، این دیدگاه به تیم‌های عملیات امنیت SOC کمک می‌کند تا استراتژی‌های امنیتی خود را به‌درستی انتخاب نموده و سیاست‌ها و برنامه‌های امنیتی جهت پاسخ به حملات را به آگاهی کامل طراحی و اجرا نمایند.
بزرگ‌ترین چالش تیم‌های SOC، جمع‌آوری میزان کافی از قوانین مرتبط باهوش تهدید می‌باشد که به‌صورت کلی از طریق منابع متن‌باز و یا منابع تجاری تأمین می‌شود.
نکته قابل‌اهمیت آن است که منابع متن‌باز و تجاری هوش تهدید (CTI) باعث ایجاد کنترل امنیتی کافی نخواهند شد؛ زیرا بدون توجه به نوع فعالیت سازمان و سطوح حمله متنوع صرفاً بخشی از کنترل امنیتی را فراهم خواهند نمود.

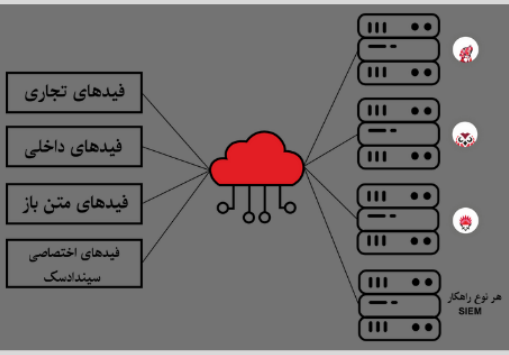
ماژول وریا (TIP) به‌عنوان بخشی از پلتفرم یکپارچه نخجیرپان (XDR)، خوراک لازم جهت آنالیز و تهیهٔ Artifactها در اختیار خواهد داشت، این اطلاعات به‌واسطه ماژول‌های هوپان، هولاد، هویر به‌صورت تجمیعی و یکپارچه در دسترس تیم‌های امنیتی قرار می‌گیرد و همچنین ابزارهای غنی‌سازی باعث تکمیل اطلاعات شده و تیم هوش تهدید ابزار بسیار کارآمدی جهت تولید IOC در اختیار خواهد داشت.
خوراک هوش تهدید می تواند از منابع مختلفی تامین گردد:

- منابع متن باز
- منابع تجاری
- دارک وب
- هانی پات ها
- پایش شبکه های داخلی و نقاط پایانی
- هشدارهای مرتبط با بدافزار و فیشینگ

چالش بزرگ در برابر تیم های SOC پایش تعداد زیادی هشدارها، حذف تعداد زیادی از هشدارهای False-Positive، تحلیل هشدارهای باقیمانده و تولید محتوای هوش تهدید متناسب با وضعیت کشف شده می باشد که زمان و انرژی بسیار زیادی مصرف می نماید.
از طرفی صرف خارج نمودن IOC ها از منابع مختلف و تزریق آنها در سیستم هوش تهدید، بدون دسته بندی مناسب و اعمال سیاست های تیم SOC در طولانی مدت باعث سردرگمی و افزایش False-positive خواهد شد.

مزایای اصلی

- مطابق با MITRE ATT&CK
- بهبود حملات Zero Day در سریعترین حالت ممکن
- پشتیبانی از شکار حملات بصورت فعال
- مخزن یکپارچه و مشترک حملات
- تنوع بسیار زیاد قوانین کشف شده (IOAs)



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