شرکت مهندسی امن ارتباط سینداد

هوش تهدید

برای شناسایی و پاسخ سریع‌تر، از هوش تهدید استفاده کنید.

سامانه یکپارچه و جامع هوش تهدید مهندسی امن ارتباط سینداد که دارای منابع اطلاعاتی پیشرفته تهدید می باشد؛ قابلیت تشخیص و پاسخ سریع تر به فعالیت‌های مشکوک را که می‌توانند نشانه نفوذ یا حمله به شمار روند را فراهم می کند. برخی از این فعالیت‌ها عبارتند از:

- بازدید از آدرس‌های اینترنتی ناشناخته و خطرناک توسط کاربران
- اتصال IP های ناشناس به زیرساخت‌ها، مانند وب سرورها، فایروال‌ها، پایگاه‌های داده و ...
- اقدام برای اجرای حمله‌های فیشینگ
- تکثیر بدافزارها در نقاط پایانی و پس از آن، در شبکه
- و ...

سامانه هوش تهدید از قابلیت تجزیه و تحلیل استفاده می کند تا داده های مرتبط با تهدیدهای مختلف را از منابع مختلف دریافت کند که شامل داده هایی مانند IP های مخرب، URL های مشکوک، ایمیل‌ها، فایل ها، فرآیندها و عامل کاربران (User Agent) می باشد. سازمان ها به راحتی می‌توانند سیستم های امنیتی خود را با هوش تهدید ادغام کرده و از مزایای آن بهره مند شوند. اطلاعات هوش تهدید می‌تواند برای تشخیص دقیق رفتارهای مخرب از جمله IP های خطرناک که به زیر ساخت داخلی اتصال دارند، اقدام برای حمله های فیشینگ، انتشار بدافزارها، حرکت جانبی در شبکه، ایجاد دسترسی از راه دور و سایر فعالیت های مشکوک استفاده شود.

این سامانه همچنین از گزارش‌های امنیتی، لاگ‌ها و رویداد های محیط شبکه و نقاط پایانی نیز استفاده می‌کند تا شاخصه‌های نفوذ (IOC) و شاخصه‌های حمله (IOA) را همراه با دیگر داده‌های تهدید ذخیره کرده و سازمان را در مقابل تهدیدهایی که در گذشته رخ داده‌اند یا احتمال رخ دادن در آینده را دارند، مقاوم سازد.

مزایای اصلی سامانه هوش تهدید

- راه‌اندازی سریع در محیط امنیتی سازمان و دریافت IOC و IOA
- شناسایی فوری حمله‌های در جریان
- ادغام اطلاعات داخلی تهدیدهای سازمان با منابع خارجی برای کمک به اولویت‌بندی رویدادها و تشخیص حمله‌ها

امکانات اصلی سامانه هوش تهدید

شناسایی و پاسخگویی به تهدیدهای سایبری پیچیده امروزی مستلزم این است که از امکانات زیر برخوردار باشید:

- نظارت وسیع در سطح شبکه
- تجزیه و تحلیل پیشرفته به وسیله هوش مصنوعی
- خودکارسازی عملیات مختلف شناسایی و پاسخ‌دهی
- دریافت اطلاعات دقیق و عملیاتی از منابع خارجی

وسعت دید این سامانه به همراه اطلاعات غنی شده آن، باعث می‌شود سازمان شما بتواند تعداد تشخیص‌های درست حمله را افزایش داده (True-Positive) و رویدادهای نادرست که به نتیجه غلط منتهی می‌شوند (False-Positive) را تا حد زیادی کاهش دهد. در همین راستا، این سامانه شما را قادر می‌سازد متوسط زمان شناسایی تهدیدها را به کمینه حالت رسانده و پاسخ‌دهی را سرعت ببخشید، قبل از اینکه توسط فعالیت‌های مهاجمان تسخیر شوید.

جدول زیر، نمونه‌ای از اطلاعات ارائه شده توسط سامانه هوش تهدید را نشان می‌دهد:

فعالیت‌های مشکوک	ابزارهای فیشینگ	ابزارهای انتشار بدافزها	تخریب اطلاعات	بات نت ها	حملات شناخته شده
IP	IP	IP	IP	IP	IP
URL	URL	URL	URL	URL	URL
	آدرس ایمیل‌های فیشینگ	عوامل کاربر			عوامل کاربر
	تیتر ایمیل‌های فیشینگ	فرایند های مخرب			
		مسیر فایل‌های مخرب			
		عنوان فایل‌های مخرب			

پایگاه اطلاعاتی قدرتمند سامانه هوش تهدید اطلاعات دریافت شده را تجزیه و تحلیل می‌کند تا فعالیت‌های مخرب و تهدیدهای پیشرفته را شناسایی، سیستم‌ها را از آسیب‌پذیری برنامه‌های نصب شده محافظت و سریعترین راهکار پاسخ‌دهی به آن‌ها را ارائه نماید.

پیشگیری از سرقت و مفقود شدن اطلاعات

مشکل: بسیاری از سازمان‌ها نظارت درستی بر روی کاربران داخلی خود ندارند. مشکل گفته شده، محافظت از شبکه را در مقابل تهدیدهایی که از نقاط پایانی دست به حرکت جانبی و ایجاد دسترسی‌های سطح بالاتر می‌پردازند بسیار پیچیده می سازد. گروه‌های مهاجمین سایبری از فعالیت‌هایی مانند اتصال به منابع داخلی، اتصال از طریق برنامه‌های پیش فرض سیستم عامل، اتصال از سرور فرماندهی و کنترل و یا شبکه‌های پراکسی استفاده می‌کنند. کارشناسان امنیتی لازم است فعالیت های قانونی کاربران داخلی را از فعالیت‌های مشکوک تشخیص دهند و از آن جلوگیری کرده یا اقدام اصلاحی به عمل آورند.

اولویت بندی رخدادها

مشکل: حجم عظیمی از فعالیت‌های مشکوک که از شبکه اینترنت نشئت می گیرد و گسترش پیدا می‌کند، متخصصین امنیتی را در تشخیص خطرناک‌ترین آن‌ها عاجز می‌سازد و بالطبع کارشناسان امنیتی در اولویت‌بندی آن‌ها به مشکل بر می‌خورند.

راه‌حل: جزئیات دقیق اطلاعات غنی‌شده‌ی سامانه هوش تهدید سبب می‌شود وظیفه ی اولویت‌بندی رخدادها با کم‌ترین دشواری انجام شود و همچنین داده‌های تهدید و الگوهای حمله با دقت تجمیع شوند که شامل حمله‌های شناخته شده، بات‌نت‌ها، سرقت و مفقودسازی اطلاعات، بدافزار، حمله‌های فیشینگ و فعالیت‌های مشکوک دیگر است. این سامانه همچنین از امکانات رفتارشناسی پیشرفته استفاده می‌کند تا تهدیدها و رخدادها را بهتر مدیریت کرده و نتایج نادرست را کمینه کند.

قابلیت افزوده شده: علاوه بر تهدیدهای گفته شده، این سامانه می‌تواند رفتار گروه های مهاجمین سایبری و تهدید (مانند APT) را نیز ذخیره کند، تا فعالیت‌های مخرب آن‌ها به سرعت شناسایی شده و باعث کوچک‌ترین خللی در سازمان شما نشود.

هوش تهدید
برای شناسایی و پاسخ سریع‌تر، از هوش تهدید استفاده کنید.

راه‌حل: سامانه هوش تهدید مهندسی امن ارتباط سیناد داده‌ها را تجزیه و تحلیل می‌کند تا رفتار تهدیدها و اولویت رخدادهای مرتبط با آن‌ها را برای متخصصین امنیتی مشخص کند. دامنه‌ها و آدرس‌های اینترنتی مشکوک موجود در اطلاعات مرتبط با تهدیدها، در لیست سیاه ذخیره می‌شود تا جلوی اتصالات خطرناک داخلی و خارجی گرفته شود.

قابلیت افزوده شده: اطلاعات فرستاده شده به منابع خارجی خطرناک مانند آدرس‌های اینترنتی مشکوک یا دامنه‌ها در شبکه به طور کامل بازبینی می‌شوند تا عملیات جرم‌یابی موشکافانه نیز بر روی آن‌ها صورت گیرد. برای استفاده از این قابلیت، لازم است سامانه هوش تهدید با ابزارهای رصد امنیتی شبکه ادغام شود.

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