ASGARD
ANALYSIS COCKPIT

رویداد Optimized THOR
Analysis در مقیاس وسیع

دید کامل با ASGARD Analysis Cockpit

پلتفرم ASGARD Analysis Cockpit دیدگاه جامعی از تمامی تطابق‌های شاخص‌های حمله شما ارائه می‌دهد و به عنوان یک ابزار ایده‌آل برای تحلیل نتایج اسکن‌های THOR عمل می‌کند. این پلتفرم به شما امکان می‌دهد تا یک خط مبنا ایجاد کرده و تغییرات مرتبط با امنیت را در محیط سازمانی خود شناسایی و بررسی کنید.

در صورت وقوع حادثه امنیتی گسترده، ASGARD Analysis Cockpit با ارائه دید کلی جامع از محیط شبکه، امکان شناسایی دقیق و سریع تهدیدات را فراهم می‌آورد. این پلتفرم با تمرکز بر یافته‌های مرتبط با امنیت در میان هزاران دارایی و بهره گیری از قابلیت‌های پیشرفته مدیریت پرونده، دید روشنی از وضعیت موجود ارائه می‌دهد و به تحلیلگران کمک می‌کند تا اقدامات اصلاحی لازم را به صورت موثر اجرا کنند

موارد استفاده از THOR

مدیریت بحران امنیتی

در صورت وقوع یک حادثه امنیتی که تعداد زیادی از نقاط پایانی را درگیر می‌کند، ASGARD Analysis Cockpit دید کاملی را ارائه می‌دهد. این پلتفرم به شما امکان می‌دهد تا تمرکز خود را بر روی یافته‌های مرتبط با امنیت در میان هزاران دارایی متمرکز کنید و با استفاده از قابلیت‌های پیشرفته مدیریت پرونده، دید جامعی از وضعیت فعلی بدست آورید.
برای شناسایی و تحلیل دقیق تهدیدات امنیتی، ASGARD Analysis Cockpit از قابلیت‌های پیشرفته ابزار THOR بهره می‌برد. این ابزار با بیش از ۳۰,۰۰۰ امضای دستی YARA، ۳,۰۰۰ قانون Sigma، قوانین متعدد برای تشخیص ناهنجاری و هزاران شاخص حمله (IOC)، به طور مؤثری تهدیدات پایدار پیشرفته (APT) را در سیستم‌های فناوری اطلاعات (IT) و فناوری عملیاتی (OT) شناسایی می‌کند.

یکپارچگی کامل با ASGARD Management Center امکان مدیریت و هماهنگی یکپارچه عملیات امنیتی را فراهم می‌کند. این قابلیت با ارائه یک رویکرد متمرکز برای شناسایی و مقابله با تهدیدات، فرآیندهای امنیتی را بهینه‌سازی کرده و دسترسی سریع و آسان به تمامی داده‌ها و نتایج مرتبط را تضمین می‌نماید.

ارزیابی مداوم نفوذ

با استفاده از ASGARD Analysis Cockpit، می‌توان اسکن‌های منظم با THOR را برنامه‌ریزی و مدیریت کرد و رویدادهای تولیدشده توسط THOR را به صورت خودکار به این پلتفرم ارسال نمود. این فرآیند به شناسایی و رسیدگی سریع به یافته‌های امنیتی در مراحل اولیه کمک می‌کند. ارزیابی‌های مستمر نفوذ، احتمال شناسایی سریع مهاجمان را افزایش داده و به کاهش خسارات احتمالی کمک می‌کند.
این رویکرد پیشگیرانه، امکان واکنش به موقع در برابر تهدیدات بالقوه را فراهم می‌سازد ASGARD Analysis Cockpit که به طور خاص برای مدیریت نتایج اسکن‌های THOR طراحی شده است، توانایی جمع‌آوری و ارتباط دادن حجم زیادی از رویدادها را بدون نیاز به ارزیابی تک‌تک آن‌ها ارائه می‌دهد. این مدیریت سیستماتیک حوادث امنیتی، به سازمان‌ها کمک می‌کند تا به سطح پیشرفته‌تری از حفاظت و امنیت دست یابند.

مزایای کلیدی

مدیریت متمرکز پرونده

دسته‌بندی یافته‌های امنیتی برای تحلیل سریع و واکنش مؤثر

اعلان‌ها

شما می‌توانید نحوه دریافت اعلان ها را به دلخواه تنظیم کنید. این اعلان‌ها می‌توانند از طریق پیام های SYSLOG، ایمیل یا وب‌هوک‌ها ارسال شوند و اطلاعاتی مانند به روزرسانی پرونده‌های در حال بررسی یا رویدادهای جدید مرتبط با پرونده‌های بسته‌شده قبلی را ارائه دهند.

داشبورد پایه

شما می‌توانید نحوه نمایش اطلاعات در این بخش را مطابق نیازهای خود تنظیم کنید تا دسترسی به داده‌های موردنظر ساده‌تر شود. همچنین، امکان ایجاد داشبوردهای سفارشی برای نمایش اطلاعات حیاتی وجود دارد که می‌توانید این داشبوردها را با سایر کاربران به اشتراک بگذارید.

قابلیت‌های اصلی

مرور کلی بخش پایه

بخش پایه: این بخش تمامی تطابق‌های شاخص‌های تهدید (IOC) را که خارج از خط‌مشی پایه فعلی سیستم شناسایی شده‌اند، نمایش می‌دهد. این تطابق‌ها به عنوان مواردی که نیازمند بررسی دقیق‌تر هستند، به‌طور برجسته ارائه می‌شوند. بخش پایه با بهره‌مندی از ابزارهای پیشرفته تجسم و فیلترسازی، همراه با گروه بندی خودکار، فرآیند تحلیل، دسته‌بندی و ایجاد پرونده های مرتبط را به‌طور چشمگیری تسهیل می‌کند.

یکپارچگی با ChatGPT: با استفاده از ChatGPT در بخش پایه یا نمای کلی رویدادها، می‌توانید درک عمیق‌تری از رویدادهای مورد بررسی به دست آورید و تحلیل‌های خود را بهبود بخشید.

این بخش از یک سیستم امنیتی، به تحلیل و بررسی رویدادهای مشکوک می‌پردازد. با استفاده از ابزارهای پیشرفته و هوش مصنوعی (ChatGPT)، کارشناسان امنیت می توانند به سرعت و دقت، تهدیدات احتمالی را شناسایی و مقابله کنند.

مدیریت یکپارچه پرونده‌ها

سیستم مدیریت یکپارچه پرونده‌ها، یک رابط کاربری ساده و کارآمد ارائه می‌دهد که همکاری مؤثر میان تحلیلگران را در بررسی تطابق‌های شاخص‌های تهدید (IOC) تسهیل می‌کند. این سیستم با قابلیت تنظیم بالا، امکان تعریف و پیاده‌سازی گردش‌کارهای سفارشی را بر اساس نیازهای خاص تیم‌های تحلیل فراهم می‌سازد. همچنین، مدل تحلیلی دو سطحی و قابل توسعه آن، پشتیبانی کامل از عملیات چندلایه را به‌طور مؤثر تضمین می‌کند.

. با استفاده از این سیستم، تحلیلگران می‌توانند به صورت مشترک بر روی اطلاعات مرتبط با تهدیدات سایبری کار کنند و با توجه به نیازهای خود، گردش کارها را تنظیم کنند. همچنین، این سیستم قابلیت پشتیبانی از ساختارهای سازمانی پیچیده با سطوح مختلف دسترسی را دارد.

یکپارچگی API - API‌های قدرتمند

پلتفرم تحلیلی Analysis Cockpit مجموعه‌ای جامع از رابط های برنامه‌نویسی کاربردی (API) را در اختیار کاربران قرار می دهد. این APIها امکان ادغام و تعامل با سایر سیستم‌ها را فراهم می‌کنند و به کاربران اجازه می‌دهند از این پلتفرم برای مدیریت مؤثر پرونده‌های امنیتی، جمع‌آوری و تحلیل اطلاعات تهدیدات و یکپارچه‌سازی با محیط‌های sandbox جهت بررسی رفتار فایل‌ها استفاده کنند. این ویژگی‌ها تحلیل امنیتی را بهبود بخشیده و فرآیندهای شناسایی و پاسخ به تهدیدات را تسهیل می‌کند.

بخش گزارش‌دهی پیشرفته

بخش گزارش‌دهی، مجموعه‌ای جامع از گزارش‌های داخلی را ارائه می‌دهد که به طور کامل تطابق‌های شاخص‌های تهدید (IOC) و فعالیت‌های مرتبط با مدیریت پرونده‌ها را پوشش می‌دهد. این گزارش‌ها شامل آمارهای کلی درباره تمامی فعالیت‌ها و رویدادهای ثبت شده در پلتفرم تحلیل بوده و با ارائه شاخص‌های کلیدی عملکرد (KPI)، به سازمان‌ها در بهینه‌سازی فرآیندهای عملیاتی کمک می‌کنند. کاربران می‌توانند گزارش‌های سفارشی ایجاد و زمان‌بندی کنند تا اطلاعات موردنیاز خود را به‌صورت خودکار دریافت نمایند. علاوه بر این، قابلیت یکپارچه‌سازی با موتورهای گزارش‌دهی خارجی نیز از طریق صادرات زمان‌بندی‌شده داده‌های خام فراهم شده است، که امکان تجزیه و تحلیل پیشرفته‌تر را مهیا می‌سازد.