

آیا سیستم‌های IT و OT شما در معرض خطر هستند؟

همین حالا مطمئن شوید.

سیستم‌های دفاعی سایبری خود را با اسکنر THOR APT تقویت کنید.

اسکنر APT ما، THOR، با انجام ارزیابی‌های خودکار، به شناسایی نفوذها، تحلیل ریسک‌های سایبری و بهبود واکنش به حوادث کمک می‌کند. این ابزار پیشرفته، با بهره‌گیری از بیش از 30,000 امضای YARA، 3,000 قانون Sigma، قوانین متعدد تشخیص ناهنجاری و هزاران شاخص تهدید (IOC)، فرآیند تحلیل‌های قانونی را سریع‌تر و دقیق‌تر می‌کند.

تهدیدات پایدار پیشرفته (APT) می‌توانند مخرب و پرهزینه باشند، اما، با استفاده از ارزیابی خودکار نفوذ، می‌توان این تهدیدات را شناسایی کرد. اسکنر پیشرفته THOR's forensic با بررسی دقیق‌تر، ردپای فعالیت‌های هک را که دیگران از دست می‌دهند، پیدا می‌کند.

کشف کنید که چگونه THOR می‌تواند دفاع‌های سایبری شما را تقویت کرده و پاسخ به حوادث را ساده‌تر کند.

موارد استفاده از THOR

واکنش به رخداد

از THOR برای شناسایی و تحلیل پیشرفته تهدیدات امنیتی پیچیده استفاده کنید. این ابزار با بهره‌گیری از بیش از ۳۰ مازول تشخیص برای اسکن مکان‌ها و حافظه‌های مختلف، تهدیداتی را کشف می‌کند که ممکن است توسط ابزارهای معمولی نادیده گرفته شوند. پایگاه امضای گسترده THOR امکان ارزیابی سریع را با قابلیت اسکن همزمان صدها یا حتی هزاران سیستم فراهم می‌کند. همچنین، این ابزار از شاخص‌ها و قوانین سفارشی پشتیبانی کرده و انعطاف‌پذیری بالایی برای نیازهای خاص امنیتی ارائه می‌دهد، که آن را به یک ابزار اساسی در هر استراتژی کارآمد پاسخ به حادثه تبدیل می‌کند.

ارزیابی مداوم نفوذ

ارزیابی مداوم نفوذ با اسکن منظم سیستم‌ها برای شناسایی فعالیت‌های هکرها و نشانه‌های نفوذ، به طور پیشگیرانه تهدیدات امنیتی را تشخیص می‌دهد. با این کار، THOR بر همه مواردی که توسط آنتی‌ویروس‌ها نادیده گرفته می‌شوند، تمرکز می‌کند. با خودکارسازی ارزیابی‌های نفوذ، THOR امکان تجزیه و تحلیل مداوم را برای شناسایی تغییرات و تهدیدات بالقوه بین اسکن‌ها فراهم می‌کند. این رویکرد به سازمان‌ها اجازه می‌دهد تا محیط‌های دیجیتال خود را نظارت کنند و به سرعت به تهدیدات نوظهور پاسخ دهند. مقایسه پیشرفته هر اسکن با اسکن قبلی در THOR، تنها یافته‌های جدید یا اصلاح‌شده را علامت‌گذاری می‌کند و در نتیجه تجزیه و تحلیل‌های قانونی را در تمام نقاط پایانی ساده‌تر می‌کند.

سیستم مستقل

ابزارهای قدرتمند THOR به متخصصان Forensic Analysis امکان می‌دهد تا اسکن نقاط پایانی و image را تسریع کرده و فرآیند تجزیه و تحلیل شواهد سیستم را در حوادث و نقض‌های امنیتی احتمالی ساده‌تر کنند. با استفاده از قابلیت‌های پیشرفته THOR در تحلیل‌های موردی، منابع بهینه‌سازی می‌شوند و تلاش‌های تحقیقاتی به حداقل می‌رسند، در حالی که اطمینان حاصل می‌شود که بررسی شواهد دیجیتال به شکلی کارآمد و جامع انجام می‌پذیرد.

مزایای کلیدی

نرخ تشخیص چشمگیر

THOR با ارائه تجزیه و تحلیل عمیق و قابلیت‌های خودکار forensic، تلاش‌های جاسوسی صنعتی، حملات باج‌خواهی و سایر فعالیت‌های مخرب هک را شناسایی می‌کند. این تهدیدات پایدار پیشرفته (APT) اغلب توسط آنتی‌ویروس‌ها و EDRها نادیده گرفته می‌شوند.

زمان واکنش

THOR با سرعت بخشیدن به فرآیند تحلیل forensic در شرایط حساس و بحرانی، به شما کمک می‌کند تا در کوتاه‌ترین زمان ممکن به نتایج دقیق دست یابید. این ابزار برای موقعیت‌هایی طراحی شده که واکنش سریع به تهدیدات و جمع‌آوری شواهد برای تصمیم‌گیری‌های مهم امنیتی ضروری است.

استقرار در مقیاس بزرگ

راهکارهای ما این امکان را فراهم می‌کنند که اسکن‌های THOR را به صورت سازمانی و از طریق یک کنسول مدیریت مرکزی اجرا کنید.



تمرکز بر فعالیت‌های هک

برخلاف نرم‌افزارهای آنتی‌ویروس سنتی، THOR بر شناسایی فعالیت‌های مخرب هکرها تمرکز دارد و ردپای ابزارهای نفوذ، خروج داده‌ها، پیکربندی‌های راه‌های مخفی برای دسترسی غیرمجاز به سیستم، web shells و روش‌هایی که به مهاجم اجازه می‌دهد پس از یک بار نفوذ، به طور مداوم به سیستم دسترسی داشته باشد را آشکار می‌کند.

این ابزار، به عنوان مکمل راهکارهای EDR، تجزیه و تحلیل جامعی از forensic artifacts، حافظه‌های پنهان و لاگ‌ها ارائه می‌دهد و نفوذهایی را شناسایی می‌کند که ممکن است در گذشته تشخیص داده نشده باشند. THOR با بهره‌گیری از یک پایگاه داده گسترده شامل بیش از 30,000 امضای YARA، بیش از 3,000 قانون Sigma و 30 مازول تشخیص، پوشش کاملی از انواع تهدیدات پایدار پیشرفته (APT) را تضمین می‌کند.



شناسایی نهایی

THOR با ارائه نرخ تشخیص پیشرو در صنعت و هزاران امضای پیشرفته، نیازهای شکار تهدید در سطح جهانی را برآورده می‌کند. این ابزار قادر است ناهنجاری‌ها، تکنیک‌های پنهان‌سازی و رفتارهای مشکوک را شناسایی کرده و روند ارزیابی نفوذ را تسریع کند، در حالی که بالاترین سطح امنیت را تضمین می‌نماید. THOR به شما امکان می‌دهد تا فوریت حوادث را به سرعت اولویت‌بندی کنید، حملات مشکوک را تأیید نمایید و با ارزیابی مستمر و پیشگیرانه، نقض‌های ناشناخته را شناسایی کنید.



شاخص‌های تهدید سفارشی (IOCs) و قوانین یارا (Yara Rules)

شما می‌توانید به سیستم امنیتی خود، شاخص‌ها و امضاهایی را اضافه کنید که به صورت سفارشی از سوی خودتان یا از منابع خارجی مانند فیدهای تهدید یا گزارش‌های تهدید به دست آمده‌اند. این امکان به شما می‌دهد تا سیستم امنیتی خود را برای شناسایی تهدیدات خاص و منحصر به فرد تنظیم و بهینه‌سازی کنید.



بستن شکاف‌های امنیتی

THOR با هدف شناسایی تهدیدات و آسیب‌پذیری‌های ناشناخته در سیستم‌های شما طراحی شده است و اطمینان کاملی از امنیت فناوری اطلاعات (IT) و فناوری عملیاتی (OT) سازمان تان ارائه می‌دهد. این ابزار با قابلیت عملکرد در انواع مختلف سیستم‌ها، از جمله سیستم‌های عامل قدیمی، پوششی جامع برای اسکن شبکه‌ها، دستگاه‌های تعبیه‌شده، hypervisors، سیستم‌های کنترل صنعتی (ICS) و دستگاه‌های اینترنت اشیا (IoT) فراهم می‌کند. ویژگی حالت آفلاین THOR امکان اسکن دستگاه‌هایی را که دائماً به شبکه متصل نیستند نیز فراهم می‌آورد. با استفاده از THOR، می‌توانید شکاف‌های موجود در تشخیص تهدیداتی که توسط آنتی‌ویروس‌ها و راهکارهای شناسایی و پاسخ نقاط پایانی (EDR) نادیده گرفته می‌شوند، پر کرده و از سیستم‌های خود در برابر تهدیدات پیشرفته محافظت کنید.



هماهنگی بی‌نقص در Security Stack

THOR با ارائه گزینه‌های متنوع و آسان برای یکپارچه سازی، به کاربران امکان می‌دهد تا از آن به عنوان یک ابزار ارزیابی مجدد در کنار سیستم‌های تشخیص و پاسخ به تهدیدات نقاط پایانی (EDR) استفاده کنند. این ابزار همچنین امکان طبقه‌بندی و مدیریت یافته‌های امنیتی در مقیاس گسترده، از طریق ASgard Analysis Cockpit را فراهم می‌کند. علاوه بر این، کاربران می‌توانند یافته‌های امنیتی مهم را در سیستم‌های SIEM/SOAR یا پلتفرم‌های خودکارسازی و هماهنگ‌سازی پاسخ به تهدیدات، به طور مؤثر تجزیه و تحلیل کرده و اقدامات لازم را اجرا کنند.



اولویت اول، قابلیت اطمینان سیستم است

THOR در حین انجام اسکن‌ها، به طور مداوم میزان استفاده از منابع سیستم را نظارت می‌کند. این ابزار به محدودیت‌های استفاده از پردازنده مرکزی (CPU) احترام می‌گذارد و از فراتر رفتن میزان استفاده از CPU از حد تعیین شده جلوگیری می‌کند. همچنین، THOR میزان حافظه آزاد سیستم را کنترل می‌کند تا از بروز مشکلات ناشی از کمبود حافظه جلوگیری کند. علاوه بر این، برای حفظ پایداری سیستم، THOR می‌تواند سرعت اسکن را تنظیم کند (ترافیک را محدود کند) تا از تأثیر منفی اسکن بر عملکرد عادی سیستم جلوگیری شود.