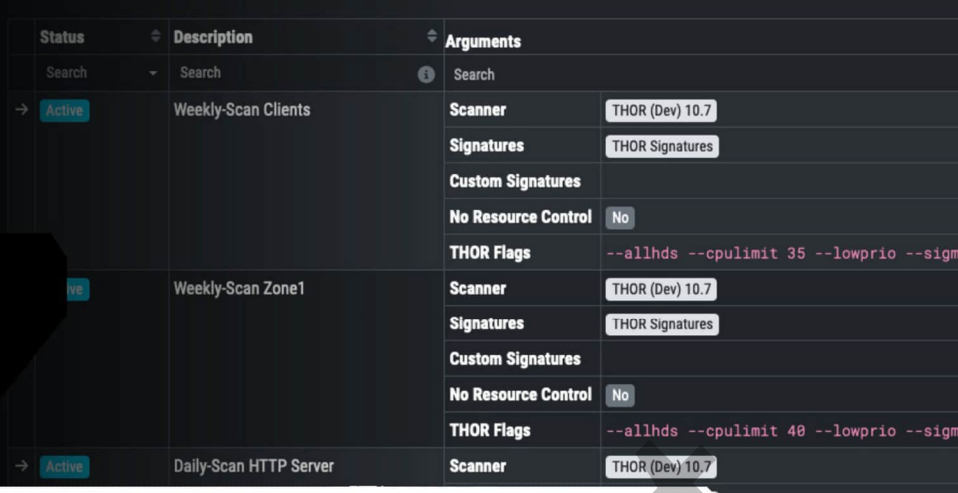
ASGARD
MANAGEMENT CENTER

اسکن‌های خودکار و متمرکز THOR به صورت گسترده



مدیریت متمرکز و هماهنگ امنیت، برای افزایش بهره‌وری

ASGARD Management Center یک ابزار قدرتمند و ساده برای مدیریت اسکن‌های THOR در سراسر سازمان ارائه می‌دهد. این ابزار امکان پیکربندی، زمان‌بندی و نظارت بر اسکن‌ها را برای حداکثر 25000 دستگاه در هر نمونه فراهم می‌کند و از طریق Master ASGARD می‌تواند بیش از 1 میلیون دستگاه را مدیریت کند. شما می‌توانید شاخص‌های تهدید (IOC) را به راحتی یکپارچه و مدیریت کنید و از قابلیت‌های پیشرفته برای پاسخگویی مؤثر به تهدیدات سایبری بهره‌مند شوید. رابط کاربری ساده این مرکز به شما اجازه می‌دهد تا اقدامات پاسخگویی پیچیده را تنها از یک کنسول بر روی یک میلیون دستگاه اجرا کنید.

موارد کاربرد

رسیدگی به بحران‌ها در مقیاس وسیع

ASGARD Management Center یک راهکار ایده‌آل برای مدیریت و رسیدگی به حوادث امنیتی در مقیاس بزرگ مانند حملات سایبری گسترده است. این مرکز از agent سبک برای سیستم‌های ویندوز، لینوکس و macOS بهره می‌برد که با سرعت و کارایی بالا، شواهد و اطلاعات مربوط به حوادث امنیتی را جمع‌آوری می‌کنند.
agent سبک، نرم‌افزارهای کوچکی هستند که بدون اشغال منابع سیستم، وظایف جمع‌آوری داده‌ها را انجام می‌دهند و حتی در سیستم‌های با منابع محدود نیز عملکرد موثری دارند. این عوامل به راحتی نصب، پیکربندی، به‌روزرسانی یا حذف می‌شوند و امکان اجرای عملیات اسکن به صورت خودکار یا آفلاین را فراهم می‌کنند.
علاوه بر این، ASGARD شامل یک کنسول راه دور قدرتمند است که به کارشناسان امنیتی امکان می‌دهد تا به صورت بی‌درنگ به بررسی حوادث، جمع‌آوری فایل‌ها و تحلیل تهدیدات بپردازند.

امنیت OT

ASGARD Management Center به شما کمک می‌کند تا به راحتی و به طور متمرکز، اسکن‌های THOR را در کل سازمان خود مدیریت کنید. این مرکز با سیستم THOR Thunderstorm که در محل شرکت شما نصب می‌شود و می‌تواند هزاران نمونه را در هر دقیقه پردازش کند، هماهنگ می‌شود. این اتصال باعث می‌شود که بتوانید محیط‌های IT (فناوری اطلاعات) و OT (فناوری عملیاتی) خود را به صورت یکپارچه مدیریت کنید.
THOR Thunderstorm به خصوص برای شبکه‌های ICS (سیستم‌های کنترل صنعتی) که بسیار حساس هستند و نمی‌توان از روش‌های معمول برای جمع‌آوری فایل‌ها در آنها استفاده کرد، بسیار مفید است. این سیستم، جمع‌آوری و ارسال فایل‌ها را در این شبکه‌ها بسیار ساده می‌کند.
همچنین، مرکز مدیریت ASGARD می‌تواند سیستم‌های خاص و محدود مانند Citrix، ESXi و محیط‌های OT را نیز اسکن کند

ارزیابی مستمر مخاطرات

ASGARD Management Center امکان اجرای ارزیابی‌های جامع برای شناسایی ناهنجاری‌ها و فعالیت‌های مشکوک را فراهم می‌کند. با ادغام این مرکز با ASGARD Analysis Cockpit ، که به طور دقیق خط پایه‌ای از تمامی نتایج اسکن را نگهداری می‌کند، فرآیند ارزیابی مخاطرات بهینه و ساده‌تر می‌شود. این رویکرد نه‌تنها بهره‌وری در ارزیابی مداوم را افزایش می‌دهد، بلکه به طور قابل توجهی زمان لازم برای پاسخ به حوادث امنیتی را کاهش می‌دهد و کارایی عملیات را ارتقا می‌بخشد.

مزایای کلیدی

مدیریت متمرکز اسکن THOR

با بهره‌گیری از یک سیستم مدیریت اسکن پیشرفته، می‌توانید تمامی جنبه‌های مرتبط با اسکن های THOR (حداکثر 25,000 نقطه پایانی در هر نمونه) در سازمان خود، از جمله پیکربندی، زمان‌بندی، کنترل و نظارت را به‌صورت متمرکز و از یک پلتفرم واحد مدیریت نمایید.

مدیریت مؤثر IOCs

مرکز مدیریت ASGARD امکان مدیریت و سفارشی‌سازی کارآمد شاخص‌های سازش (IOCs) و قوانین YARA را فراهم می‌کند. با ادغام این پلتفرم با MISP، می‌توانید فرآیندهای تحقیقاتی خود را بهبود دهید و IOCهای سفارشی و یکپارچه را بر اساس نیازهای سازمان، به تمامی نقاط پایانی اعمال کنید.

یکپارچه‌سازی بدون نقص با SIEM

نتایج حاصل از اسکن‌های THOR را به صورت خودکار از طریق ASGARD Management Center و ASGARD Analysis Platform به سیستم SIEM خود منتقل کنید. با افزودن Forensic Artifacts به داده‌های SIEM، تحلیل‌ها را غنی‌تر کرده و سرعت واکنش به تهدیدات را افزایش دهید.

قابلیت‌های اصلی

عوامل چندگانه پلتفرم

عامل ASGARD از مایکروسافت ویندوز، لینوکس و MacOS پشتیبانی می‌کند.

API قدرتمند

ASGARD API امکان ادغام بدون مشکل با فریمورک های SOAR، سیستم‌های SIEM، فیدهای IOC (مانند MISP) و تقریباً هر زیرساخت امنیتی را فراهم می‌کند.

ریموت کنسول

با استفاده از کنسول راه دور ASGARD به سیستم‌های راه دور دسترسی پیدا کنید. از PowerShell در ویندوز برای اسکریپت‌نویسی پیشرفته و از پوسته محلی در لینوکس یا macOS بهره‌مند شوید. تمامی جلسات به‌صورت کامل ضبط شده و قابل بازبینی هستند، که شفافیت و امکان ردیابی دقیق را فراهم می‌کند.

داشبورد

این سیستم با ارائه آمار دقیق از اسکن‌های اخیر و تجسم پیشرفته نحوه مدیریت خطاها، امکان نظارت مؤثر بر عملکرد سیستم و دستیابی به بینش‌های شفاف را فراهم می‌کند.

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

اضافه کردن و مدیریت نشانگرهای سفارشی، مانند نام فایل‌ها، کلمات کلیدی، C2 یا هش‌ها، به همراه امضاها از فیدهای تهدید و بررسی‌ها

دستورالعمل‌ها یی برای خودکارسازی پاسخ به حوادث امنیتی

پلی‌بوک‌های پاسخ سفارشی مجموعه‌ای از دستورالعمل ها هستند که برای خودکارسازی پاسخ به حوادث امنیتی استفاده می‌شوند. طراحی و اجرای پلی‌بوک‌های پاسخ سفارشی با حداکثر 16 مرحله متوالی، که رسیدگی دقیق و مؤثر به حادثه را تضمین می‌کند.

گزینه‌های اسکن انعطاف‌پذیر

علاوه بر عامل پیشنهادی ASGARD، روش‌های پشتیبانی شده برای اسکن شامل استفاده از بسته‌های آفلاین THOR، ایجاد چندین مجوز و انجام اسکن بدون نیاز به عامل از طریق اسکریپت‌های PowerShell است.

Forensics لحظه ای تجزیه و تحلیل سیستم تک‌کاربره

(Forensics) به مجموعه‌ای از روش‌ها و تکنیک‌ها گفته می‌شود که برای جمع‌آوری، تحلیل، و تفسیر شواهد به منظور استفاده در تحقیقات قانونی به کار می‌رود. Live Forensics به جمع‌آوری اطلاعات از سیستم در حال اجرا (مثلاً یک کامپیوتر روشن) اشاره دارد، که شامل استخراج اطلاعات حافظه، پردازش‌های فعال، یا داده‌های شبکه می‌شود، بدون اینکه سیستم خاموش یا دست‌کاری شود

ASGARD به شما امکان می‌دهد تا یک اسکن بررسی forensics لحظه ای را روی هر نقطه پایانی متصل اجرا کنید و تجزیه و تحلیل عمیق‌تری ارائه دهد و در زمان و هزینه های تحلیلگران صرفه‌جویی کند.