Symantec

تشخیص و پاسخ نقطه پایانیSymantec

کشف و اصلاح سریع تهدید

دریک نگاه

شناسایی و افشا کردن - زمان کشف نقض را کاهش دهید و دامنه را به سرعت در معرض دید قرار دهید

- از یادگیری ماشین و تجزیه و تحلیل رفتاری برای افشای فعالیت‌های مشکوک، شناسایی و اولویت‌بندی حوادث استفاده کنید.
- شناسایی و ایجاد حوادث برای اسکریپت های مشکوک و سوء استفاده های حافظه
- حملات مبتنی بر حافظه را با تجزیه و تحلیل حافظه فرآیندی افشا کنید

بررسی و مهار - بهره وری واکنش دهنده حادثه را افزایش دهید و از مهار تهدید اطمینان حاصل کنید

- از پخش کامل حادثه با ضبط مداوم فعالیت نقطه پایانی، مشاهده فرآیندهای نقطه پایانی خاص اطمینان حاصل کنید
- با جستجوی شاخص های سازش در تمام نقاط پایانی در زمان واقعی، تهدیدها را جستجو کنید
- حاوی نقاط پایانی احتمالی در معرض خطر در طول بررسی با قرنطینه نقطه پایانی باشد

راه حل - به سرعت مشکلات نقاط پایانی را برطرف کنید و اطمینان حاصل کنید که تهدید برنمی گردد

- فایل های مخرب و ایجاد شده مرتبط را در تمام نقاط پایانی تحت تأثیر حذف کنید
- لیست سیاه و فایل های لیست سفید در نقطه پایانی
- گزارش پیشرفته اجازه می دهد تا هر جدولی برای گزارش های حل حادثه صادر شود

یکپارچه سازی و خودکارسازی - دیدگاه های محقق را متحد کنید، داده ها و جریان های کاری را هماهنگ کنید

- داده ها و اقدامات حادثه را به راحتی در زیرساخت های SOC موجود از جمله Splunk و ServiceNow ادغام کنید
- بهترین شیوه ها و تجزیه و تحلیل بازرسان ماهر را با قوانین playbook حوادث خودکار تکرار کنید
- با جمع‌آوری خودکار مصنوعات، در فعالیت نقطه پایانی دید عمیق پیدا کنید

شرکت ها به طور فزاینده ای در معرض تهدید حملات پیچیده قرار دارند. در واقع، تحقیقات نشان داده است که تهدیدها در داخل وجود دارند
محیط یک مشتری به طور متوسط ۱۹۰ روز است.این تهدیدات پایدار پیشرفته از تکنیک های پنهانی برای فرار از شناسایی و دور زدن دفاع های امنیتی سنتی استفاده می کنند. هنگامی که یک حمله پیشرفته به محیط مشتری دسترسی پیدا می کند مهاجم ابزارهای زیادی برای فرار از شناسایی و شروع به بهره برداری از منابع و داده های ارزشمند دارد.
تیم‌های امنیتی هنگام تلاش برای شناسایی و افشای کامل گستره یک حمله پیشرفته با چالش‌های متعددی مواجه می‌شوند، از جمله جستجوی دستی از طریق منابع داده‌ای بزرگ و متفاوت، عدم مشاهده نقاط کنترل بحرانی، هشدار خستگی ناشی از مثبت کاذب، و مشکل در شناسایی و رفع نقاط پایانی تأثیرگذار.

راه حل **Symantec EDR**
Symantec EDR حملات پیشرفته را با یادگیری ماشینی دقیق و هوشمندی تهدیدات جهانی به حداقل رسانده و به تضمین سطوح بالای بهره‌وری برای تیم‌های امنیتی کمک می‌کند. قابلیت‌های Symantec EDR به پاسخ‌دهنده‌های حادثه اجازه می‌دهد تا در حین بررسی تهدیدها با استفاده از انتخابی از جعبه‌شنودهای داخلی و مبتنی بر ابر، به سرعت جستجو، شناسایی و حاوی تمام نقاط پایانی آسیب‌دیده باشند. همچنین، Symantec EDR بهره‌وری محقق را با کتاب‌های تحقیقاتی خودکار و تجزیه و تحلیل رفتار کاربر افزایش می‌دهد که مهارت‌ها و بهترین شیوه‌های با تجربه‌ترین تحلیلگران امنیتی را برای هر سازمانی به ارمغان می‌آورد و در نتیجه هزینه‌های قابل توجهی کاهش می‌یابد.

علاوه بر این، ضبط مداوم و بر اساس تقاضای فعالیت سیستم از دید کامل نقطه پایانی پشتیبانی می کند. Symantec EDR از تشخیص حملات پیشرفته در نقطه پایانی و تجزیه و تحلیل مبتنی بر ابر برای شناسایی حملات هدفمند مانند تشخیص رخنه، فرمان و کنترل چراغ راهنمایی، حرکت جانبی و اجرای پوسته برق مشکوک استفاده می کند.

افزایش دید و بهره وری

Symantec EDR بهره وری محقق را با اولویت بندی حوادث بر اساس خطر افزایش می دهد. و Symantec EDR به طور خودکار حوادثی را برای حملات هدفمند ایجاد می کند که از طریق تجزیه و تحلیل حمله هدف Symantec و Dynamic Adversary Intelligence شناسایی شده اند.

محققین می توانند از مزایای ثبت فعالیت نقطه پایانی برای جستجوی شاخص های حمله و انجام تجزیه و تحلیل نقطه پایانی استفاده کنند Symantec EDR .از بازیابی مداوم و بر اساس تقاضا برای طیف گسترده ای از رویدادها از جمله جلسه، فرآیند، تغییرات نقطه بار ماژول، عملیات فایل و پوشه و تغییرات رجیستری پشتیبانی می کند. علاوه بر این، رویدادهای شبکه حیاتی برای چندین پروتکل ثبت می شوند (مشتریان می توانند پروتکل های پشتیبانی شده را که ترجیح می دهند ضبط کنند، پیکربندی کنند). رویدادهای شبکه ضبط شده شامل زمان شروع و پایان جلسه، اولین URL مرتبط با جلسه، پروتکلIP ، پورت IP مبدا و مقصد و موارد دیگر است.

بر اساس گزارش ایمنی و تهدید اینترنت سیمانتک(ISTR) ، بیش از ۲۰ درصد از بدافزارها از VM آگاه هستند که به این معنی است که آنها از شناسایی در سندباکس سنتی فرار می کنند Symantec EDR .شامل سندباکس است که می تواند با استفاده از تکنیک های پیشرفته ای که شامل تقلید از رفتار انسان و در صورت لزوم استفاده از سرورهای فیزیکی برای انفجار است، چنین تهدیدات آگاه از VM را شناسایی کند Symantec EDR .از ارسال خودکار فایل های مشکوک به sandbox برای تجزیه و تحلیل پشتیبانی می کند.

Symantec EDR هشدارهای هوشمند حوادث را برای افزایش بهره وری محقق ارائه می دهد

تجزیه و تحلیل حمله مبتنی بر ابر و تشخیص حمله پیشرفته Endpoint

Symantec EDR شامل تجزیه و تحلیل حملات هدفمند (TAA) است TAA .فعالیت های جهانی، خوب و بد، را در تمام شرکت هایی که مجموعه تله متری ما را تشکیل می دهند، تجزیه و تحلیل می کند. الگوریتم‌های هوش مصنوعی مبتنی بر ابر و یادگیری ماشینی پیشرفته سیمانتک به‌طور خودکار با تکنیک‌های حمله جدید سازگار می‌شوند. TAA با تجزیه و تحلیل دقیق مهاجم، تکنیک‌ها، ماشین‌های آسیب‌دیده و راهنمایی‌های اصلاح، یک حادثه بلادرنگ ایجاد می‌کند و آن را به کنسول EDR ارسال می‌کند. این رویکرد تلاش های واکنش دهندگان حادثه را ساده می کند و بهره وری را برای کل تیم امنیتی افزایش می دهد(TAA بدون هزینه اضافی برای مشتریان Symantecبا استفاده از Advanced Threat Protection 3.1 یا بالاتر ارائه می شود.)

Symantec EDRهمچنین از سیاست های رفتاری نقطه پایانی استفاده می کند که به طور مداوم توسط محققان سیمانتک به روز می شود تا تکنیک های حمله پیشرفته (AAT)را فوراً در نقطه پایانی شناسایی کند (بیش از ۳۵۰ مورد در حال حاضر موجود است) .این شناسایی‌ها فعالیت‌هایی را که ممکن است نشان‌دهنده حملات در حال انجام باشد، از جمله تغییرات فایل و رجیستری، فعالیت‌ها و استفاده مشکوک در شبکه و فرآیندها را نشان می‌دهد.

از API های خاص ویندوز که می توانند برای شروع یک رشته مخرب در یک فرآیند موجود استفاده شوند. رویدادهای خاص از شناسایی های AAT را می توان در لیست سفید قرار داد اگر مشخص شود که برای سازمان شما عادی هستند.

به دنبال ناهنجاری در نقاط پایانی باشید

Symantec EDR با ارائه نمای کلی از نرم افزار، حافظه، کاربر و فعالیت پایه شبکه، جستجوی مهاجمان در محیط را ساده می کند. هنگامی که مهاجمان در محیط کار می کنند، بدافزار و فعالیت کاربر آنها به عنوان ناهنجاری یا پرت برجسته می شود.

Symantec EDRموارد پرت را در سراسر محیط نشان می دهد از جمله:

نرم افزارهای پرت - نقاط پایانی را که دارای نرم افزار غیرمعمول، اختلافات ساختمانی، نسخه های سیستم عامل (OS) اصلاح نشده یا قدیمی هستند را در معرض دید قرار دهید.

نقاط پرت حافظه - با استفاده از بررسی پزشکی قانونی حافظه فرآیند، فایل و شی سیستم عامل و تنظیمات سیستم، نقاط پرت ساکن حافظه را شناسایی کنید.

نقاط پرت کاربر – تجزیه و تحلیل رفتار کاربر، مهاجمانی را شناسایی می کند که به عنوان کاربران قانونی فعالیت غیرعادی انجام می دهند

نقاط پرت شبکه – از تجزیه و تحلیل آماری برای شناسایی آدرس‌های IP غیرعادی استفاده کنید، جستجوی شهرت آدرس‌های IP و دامنه‌های مرتبط با استخراج داده‌ها را شناسایی کنید.

Symantec EDRموارد پرت را در سراسر محیط نشان می دهد از جمله:

•نرم افزارهای پرت - نقاط پایانی را که دارای نرم افزار غیرمعمول، اختلافات ساختمانی، نسخه های سیستم عامل (OS) اصلاح نشده یا قدیمی هستند را در معرض دید قرار دهید.

•نقاط پرت حافظه - با استفاده از بررسی پزشکی قانونی حافظه فرآیند، فایل و شی سیستم عامل و تنظیمات سیستم، نقاط پرت ساکن حافظه را شناسایی کنید.

•نقاط پرت کاربر – تجزیه و تحلیل رفتار کاربر، مهاجمانی را شناسایی می کند که به عنوان کاربران قانونی فعالیت غیرعادی انجام می دهند

•نقاط پرت شبکه – از تجزیه و تحلیل آماری برای شناسایی آدرس‌های IP غیرعادی استفاده کنید، جستجوی شهرت آدرس‌های IP و دامنه‌های مرتبط با استخراج داده‌ها را شناسایی کنید.

این تشخیص‌های پرت از طریق سرویس مبتنی بر ابر ارائه می‌شوند و با استفاده از playbookهای داخلی و سفارشی که گزارش‌های خاصی را در مورد طیف گسترده‌ای از فعالیت‌های غیرعادی تولید می‌کنند، در دسترس هستند.

غنی‌سازی رویداد MITER ATT&CK و تجزیه و تحلیل سایبری

Symantec EDR ابزارهایی را برای شناسایی و تجسم چرخه حیات حمله بر اساس چارچوب MITER ATT&CK ارائه می دهد. (MITER یک سازمان غیرانتفاعی که در سازمان دولتی و عمومی/خصوصی برای رسیدگی به مسائل مربوط به امنیت آنلاین کار می کند)

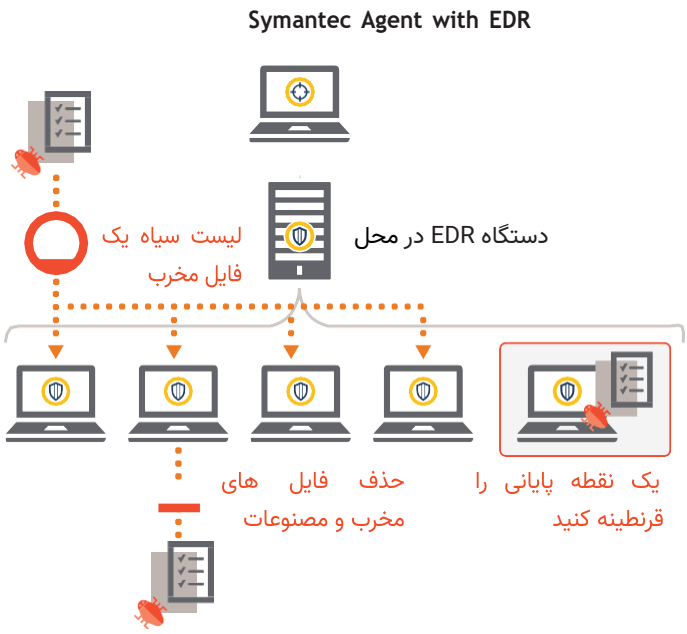
ابزار روش های حمله را بر اساس تاکتیک ها و تکنیک های استاندارد در ماتریس ATT&CKتوصیف می کند. علاوه بر این، فیلترهای سریع، محدود کردن نتایج را به یک یا چند مرحله از چرخه حیات MITER ATT&CK از جمله دسترسی اولیه، پایداری، حرکت جانبی و فرمان و کنترل را برای محققین آسان می‌کند.

به طور حیاتی، Symantec EDR از MITER Cyber Analytics از طریق کتاب‌های تحقیق خودکار پشتیبانی می‌کند. MITER به سازمان‌ها توصیه می‌کند با تحقیق از تفاوت‌های AutoRun، مکان‌های اجرای مشکوک، تزریق‌های بالقوه DDL و نظارت بر رویدادSMB ، رویکردی با اعتماد صفر برای جمع‌آوری و پیگرد قانونی اجرا کنند، Symantec EDR این کار را آسان می کند.

پاک سازی های برنامه ریزی شده را در نقاط پایانی اجرا کنید تا مشخص کنید آیا می توان هر گونه حمله را با استفاده از دانش رایج جامعه مدل های مخالف MITER شناسایی کرد.

تعمیر کامل و سریع نقطه پایانی

Symantec EDR از اصلاح سریع نقاط پایانی آسیب دیده از جمله حذف فایل، لیست سیاه و قرنطینه نقطه پایانی پشتیبانی می کند. با استفاده از قابلیت‌های پاک‌کن قدرتمند تعبیه‌شده درSymantec Agent ، پاسخ‌دهندگان می‌توانند از طریق کنسول EDR اقدام کنند و با یک کلیک یک اصلاح را در چندین نقطه پایانی اعمال کنند .

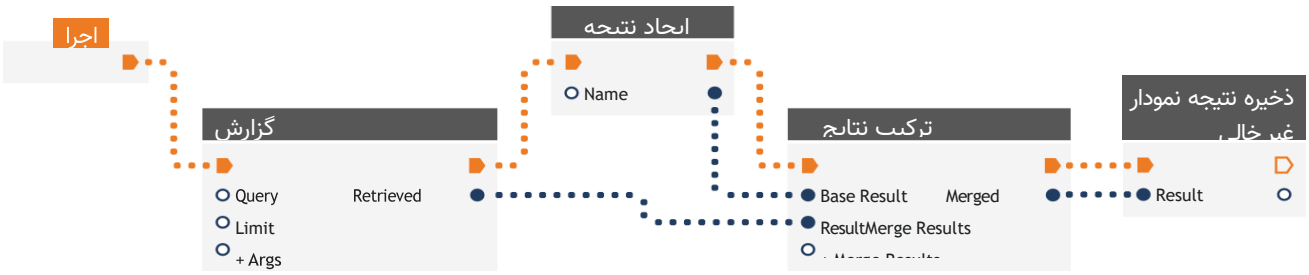


Symantec EDR تضمین می کند که نقطه پایانی به حالت قبل از عفونت باز می گردد.

خودکارسازی پالیسی ها

Symantec EDR از playbook ها پشتیبانی می‌کند که گردش کار پیچیده و چند مرحله‌ای بررسی تحلیلگران امنیتی را خودکار می‌کند. playbook ها داخلی به سرعت رفتارهای مشکوک، تهدیدات ناشناخته، حرکت جانبی و نقض سیاست‌ها را آشکار می‌کنند. Symantec EDR شامل مجموعه گسترده ای از playbook ها برای شناسایی تاکتیک های "Living off the Land" (LOTL) از جمله استفاده از ابزارهای قانونی برای پنهان کردن حملات در فعالیت های عادی است. Symantec EDRاکنون بیش از ۵۰ مورد از این playbook های LOTL را پشتیبانی می کند. playbook های انتخابی را می‌توان برای اجرا در تاریخ، زمان یا فاصله زمانی مشخص برنامه‌ریزی کرد.

تیم امنیتی می‌تواند playbook ها را مشاهده کند تا تکنیک‌های شکار و تحقیق را بیاموزد. علاوه بر این، محققان می‌توانند playbook ها خود را برای خودکارسازی بهترین شیوه‌ها و مستندسازی سناریوهای شکار تهدید خاص ایجاد کنند.



Symantec EDR دارای *playbook* ها ی قدرتمند و خودکار برای جمع آوری فایل های مخرب، بررسی و پاسخ است.

گزینه های استقرار انعطاف پذیر

Symantec EDR یک راه حل انعطاف پذیر است که می تواند در محل یا در فضای ابری مستقر شود. مشتریان Symantec Endpoint می‌توانند از قابلیت‌های EDR یکپارچه در معماری Symantec Single Agent استفاده کنند. با استفاده از ابزار EDR، سازمان‌ها می‌توانند به سرعت EDR را در محیط‌های داخلی Symantec Endpointمستقر کنند. علاوه بر این، مشتریان می‌توانند ماژول‌هایی اضافه کنند که قابلیت مشاهده و ارتباط رویدادهای شبکه و ایمیل را فراهم می‌کنند(ماژول ایمیل به Symantec Email Security.cloud نیاز دارد.)

نقاط پایانی با یا بدون نصب Symantec Agent می‌توانند از پورتال مبتنی بر ابر EDR برای تجزیه و تحلیل داده‌های سایبری، تجزیه و تحلیل پزشکی قانونی و اتوماسیون تحقیقات با استفاده از یک عامل قابل حل و سرور جمع‌آوری در محل (یا عامل خدمات مجموعه اختیاری) استفاده کنند. قابلیت‌های EDR مبتنی بر ابر سیمانتک در عرض چند دقیقه گسترش می‌یابد و به سرعت داده‌ها را از نقاط پایانی جمع‌آوری می‌کند، بدون اینکه تأثیری بر تجربه کاربر نهایی داشته باشد.

تیم عملیات امنیتی خود را گسترش دهید

سرویس تشخیص و پاسخ مدیریت نقطه پایانی Symantec تضمین می‌کند که شرکت‌ها در هر اندازه می‌توانند قابلیت‌های تیم‌های SOC موجود را گسترش دهند یا از تحلیلگران SOC کلاس جهانی Symantec برای استفاده کامل از Symantec برای تریاژ حادثه، شکار تهدید، تجزیه و تحلیل پیگرد قانونی و مهار نقطه پایانی استفاده کنند.

EDRمدیریت شده Symantec تخصص بی نظیر و مقیاس جهانی را ارائه می دهد که تیم های امنیتی را با موارد زیر تقویت می کند:

- ۲٤ x 7 تیم اختصاصی از تحلیلگران که بر اساس تمرکز جغرافیایی و صنعتی مشتریان تعیین شده اند
- شکار تهدید پیشگیرانه که برای به حداقل رساندن تأثیر تجاری تهاجمات احتمالی اعمال می شود
- انتقال یکپارچه از سرویس مدیریت EDR به یک تعامل واکنش به حادثه در صورت لزوم

در ترکیب با ابزارSymantec EDR ، مدیریت EDR تخصص بیشتر و پوشش جهانی را که بسیاری از تیم‌های عملیات امنیتی نیاز دارند، اضافه می‌کند.

افزایش سرمایه گذاری های امنیتی

رویکرد دفاع سایبری یکپارچه سیمانتک سرمایه گذاری موجود سازمان شما را در زیرساخت های امنیتی افزایش می دهد.

راه‌حل‌های Symantec EDR با ابزارهای عملیات امنیتی، از طریق جمع‌آورنده‌ها یا APIهای تبادل دفاع سایبری یکپارچه(Symantec (ICDx ، برای مدیریت رویداد و حوادث، ticketing، اتوماسیون و هماهنگ‌سازی از جمله:

- برنامه های از پیش ساخته شده برای Splunk ، IBM QRadarو ServiceNow
- اتوماسیون و ارکستراسیون یکپارچه با استفاده ازPhantom ، Demisto وCyberSponse
- APIهای عمومی که قابلیت های تشخیص، بررسی و پاسخ را پوشش می دهند

الزامات و گواهینامه

برای نیازهای کامل Symantec EDR به صفحات نیازمندی های سیستم مراجعه کنید:

https://www.symantec.com/products/endpoint-detection-and-response#requirements

Symantec EDR is ISO 27001 Certified.

برای کسب اطلاعات بیشتر در موردSymantec EDR ، ICDxو Symantec

Managed EDRاز صفحات محصول بازدید کنید:

https://go.symantec.com/edr

https://go.symantec.com/managed-edr

https://www.symantec.com/theme/integrated-cyber-defense-exchange

تهران، خیابان شهید بهشتی ، خیابان پاکستان ، کوچه چهارم ، پلاک ۱۱ ، طبقه چهارم ، واحد ۷
تلفن: ۸۸۸۰۴۹۶۱ | دورنگار: ۸۹۷۸۳۷۳۷ | کدپستی : ۱۵۳۱۶۴۵۹۱۸
info@arka.ir www.arka.ir
رایان سامانه آرکا