بسمه تعالی

معرفی، آموزش نصب، و پیکربندی سامانه

HP Archsight

(بخش اول)

فهرست مطالب

۱ مقدمه ۱

۲ مروری بر SOC و محصولات SIEM ۲

۲-۱ مقدمه ۲

۲-۲ مرکز عملیات امنیت ٤

2-2-1 نسل‌های مرکز عملیات امنیت ۵

۲-۲-۲ ویژگی‌های یک مرکز عملیات امنیت مؤثر ۹

۲-۲-۳ قابلیت‌های مرکز عملیات امنیت ۱۱

۲-۳ تعریف SIEM و معرفی قابلیت‌های آن ۲۱

2-3-1 قابلیت‌های SIEM ۲۲

2-3-2 ارزیابی محصولات SIEM ۲۷

۳ معرفی سامانه ArcSight ۲۹

۳-۱ قابلیت‌های ESM ۲۹

۳-۱-۱ آگاهی وضعیتی ۲۹

۳-۱-۲ همبسته‌سازی ۳۰

۳-۱-۳ نظارت ۳۰

۳-۱-٤ چارچوب ۳۰

۳-۱-۵ تحلیل ۳۰

۳-۱-٦ گزارش‌دهی ۳۱

3-2 آناتومی ESM ۳۱

۳-۲-۱ SmartConnector ۳۲

۳-۲-۲ منابع داده پشتیبانی شده ۳۳

۳-۲-۳ FlexConnector ۳۵

۳-۲-٤ Forwarding Connector ۳۵

۳-۲-۵ ArcSight Manager ۳۵

۳-۲-٦ ذخیره‌ساز CORR-Engine ۳٦

۳-۲-۷ واسط‌های کاربری ۳٦

3-3 چرخه حیات رویدادها در ESM ۳٦

۳-٤ معرفی قابلیت‌های فنی محصول ۳۸

۳-٤-۱ جمع‌آوری طیف وسیعی از داده‌های مرتبط با رویداد و پردازش ۳۸

۳-٤-۲ مدیریت کاربران ٤۱

۳-٤-۳ مدیریت مجوزها ٤۱

۳-٤-٤ مدیریت اخطارها ٤۲

۳-٤-۵ نظارت بر رویدادها ٤۳
3-4-6 فیلترکردن رویدادها ٤۳
۳-٤-۷ ایجاد گزارش ٤٤
۳-٤-۸ همبسته‌سازی ٤۵
۳-٤-۹ همبسته‌سازی هویت ٤۷
3-4-10 مدیریت موارد ٤۷

۱ مقدمه

ArcSight Enterprise Security Management[۱] یک راه‌حل نرم‌افزاری جامع است که نظارت بر رویدادهای امنیتی سنتی را با هوش شبکه‌ای[۲]، همبسته‌سازی محتوایی[۳]، تشخیص ناهنجاری، ابزارهای تحلیل تاریخچه‌ای[۴]، و اصلاح خودکار ترکیب کرده است. ArcSight ESM همچنین یک راه‌حل چندسطحی است که ابزارهایی را برای تحلیل‌گران امنیت شبکه، مدیران سیستم و کاربران تجاری ارائه کرده است. HPE ArcSight ESM هر رویدادی که در سراسر سازمان رخ می‌دهد (ورود، خروج، دسترسی به فایل، پرس‌وجو از پایگاه‌داده) را برای اولویت‌دهی دقیق از خطرات امنیتی و نقض انطباق، تحلیل و همبسته می‌کند. این سامانه همچنین یک راهبرد پیشرو در بازار برای جمع‌آوری، همکاری و گزارش‌دادن در مورد اطلاعات رویدادهای امنیتی است. HPE ArcSight ESM به برآورده نمودن اهداف زیر کمک می‌کند:

- همبسته‌سازی داده‌ها[۵] از هر منبعی به‌صورت بی‌درنگ برای تشخیص وقایع[۶]، پیش از این که آن‌ها به یک حفره[۷] تبدیل شوند.
- مسائل را سریع‌تر حل می‌کند. به پرسش‌هایی مانند چه کسی چه کاری را انجام داده؟ چه وقت؟ کجا؟ و چطور؟ پاسخ می‌دهد.
- هر رویدادی را از هر منبعی و در هر زمانی جمع‌آوری، ذخیره‌سازی، و تحلیل می‌کند.
- بسته‌های اختیاری انطباق، امکان تهیه گزارش برای بررسی مطابقت با استانداردهای PCI، SOX و مدیریت فناوری اطلاعات را فراهم می‌کند.
- ساخت و نگهداری مرکز عملیات امنیت (SOC) از طریق تجزیه و تحلیل امنیت بزرگ داده.

---

[۱] ArcSight ESM
[۲] Network Intelligence
[۳] Context Correlation
[۴] Historical Analysis
[۵] Data Correlation
[۶] Incident
[۷] Breach

- ادغام SOC در سراسر فناوری اطلاعات با عملیات شبکه، خدمات میزبان، CMDB، هوش تجاری، هادوپ، امنیت ایمیل، امنیت برنامه کاربردی و غیره.
- عمق، محدوده، و سرعت بی‌نظیر جمع‌آوری رویدادها با استفاده از ابزارهای مدیریت لاگ ثبت شده.

در ادامه این سند در بخش ۲ ابتدا به معرفی SOC و استفاده از محصول SIEM به عنوان قلب آن پرداخته می شود، سپس محصولات SIEM مرور و رتبه‌بندی می‌شوند. در بخش ۳ با توجه به این‌که ضرورت استفاده از ابزار تجاری ArcSight در بخش ۲ بیان شده است، به معرفی این محصول و بیان ویژگی‌های آن می‌پردازیم.

۲ مروری بر SOC و محصولات SIEM

۲-۱ مقدمه

تهدیدات امنیت سایبری صرف‌نظر از اندازه و نوع سازمان بر اساس گزارش‌های Verizon 2016 Data Breach Investigation Report، Trustwave 2016 Global Security Report و Symantec Internet Security Threat Report 2016 به شکل چشم‌گیری افزایش یافته است. برای محافظت و دفاع در برابر چنین تهدیداتی، هر سازمان باید قابلیت تشخیص وقایع امنیتی و پاسخ به آن‌ها را داشته باشد. به همین منظور سازمان ها ابزارهای امنیتی و نظارتی متنوع را در سطوح مختلف برنامه کاربردی، سیستم‌عامل، و شبکه به‌کار گرفته و از داده و اطلاعات متنی، که با انجام آزمون نفوذپذیری و یا با مراجعه به بولتن‌های خبری و استانداردها که بهترین اقدامات را ارائه می‌کنند به‌دست می‌آیند، بهره‌برداری می‌کنند. از جمله این ابزارها می‌توان سیستم‌های تشخیص نفوذ شبکه و میزبان، دیواره آتش، دیواره آتش برنامه‌های کاربردی وب، بررسی‌کننده صحت فایل، سیستم‌های جلوگیری از نشت اطلاعات، ضد بدافزارها، ابزارهای تولید رویداد سیستم‌عامل ویندوز و لینوکس، پویش‌گران[۸] آسیب‌پذیری را نام برد. هر کدام از این ابزارها هشدارهای امنیتی و لاگ‌های خود را به‌صورت محلی ذخیره می‌کنند. در این صورت حجم زیادی از رویدادهای امنیتی و لاگ‌ها به‌صورت پراکنده در ابزارهای

[۸] Scanner

مختلف به‌صورت محلی نگهداری می‌شوند، بدون این‌که میان آن‌ها با یکدیگر و همچنین میان آن‌ها و داده‌های متنی[۹] گردآوری شده، ارتباطی برقرار شود. به‌دلیل حجم زیاد و پراکندگی رویدادهای امنیتی و لاگ‌ها، بررسی و تأیید، کاهش و برقراری ارتباط بین آن‌ها با یکدیگر و با داده‌های متنی توسط کارشناسان امنیتی، امری غیرممکن است. بدین‌ترتیب نمی‌توان به یک دید یکپارچه از وضعیت امنیتی شبکه دست پیدا کرد.

همچنین این ابزارها به‌دلیل این‌که تنها از دید خود، تهدیدات را تشخیص داده و ارزیابی می‌کنند و در کنار داده های حمله، فاقد داده‌های متنی مکمل داده‌های حمله هستند، در تشخیص حملات دارای نواقصی می‌باشند که در ادامه به برخی از آن‌ها اشاره می‌شود. در میان هشدارهای امنیتی، هشدارهای مثبت نادرست وجود دارند. به عبارت دیگر ممکن است توسط یک ابزار امنیتی، هشداری نادرست از حادثه‌ای که رخ نداده صادر شود، در صورتی که از داده‌های مکمل استفاده نشود امکان شناسایی و تفکیک این هشدارها وجود ندارد. ممکن است برای حمله‌ای به دلیل نبود الگو هشدار امنیتی تولید نشود، یا به‌عبارت دیگر عملکرد سیستم امنیتی منفی نادرست داشته باشد، اما به دلیل وقوع رویداد، ابزارهای ثبت رویداد برای آن لاگی را تولید کنند. اگر تنها به ابزارهای امنیتی تکیه کنیم متوجه وقوع این دسته از حملات نخواهیم شد. ممکن است در میان هشدارهای امنیتی و لاگ‌ها موارد تکراری وجود داشته باشد، بررسی این هشدارها و لاگ‌های تکراری که روی ابزارها به‌صورت محلی ذخیره شده است، مستلزم صرف زمان است. همچنین ممکن است برای یک حمله هشدارهای امنیتی و لاگ‌های مختلفی تولید شوند، که این داده‌های حمله روی ابزارهای مختلفی به‌صورت محلی ذخیره شده‌اند. برقراری ارتباط بین این هشدارها توسط کارشناس امنیتی امری دشوار است. یا این‌که بخواهیم در پاسخ به حملات واکنشی نشان دهیم در این شرایط باید واکنش و سیاست امنیتی روی تمام ابزارها تنظیم شود، و این در شرایطی است که تمام این ابزارها از اعمال سیاست‌های امنیتی و انجام واکنش پشتیبانی کنند. ممکن است مهاجم سناریوی حمله‌ای را اجرا کند و تمام هشدارهای تولیدشده در نتیجه اجرای سناریو در یکی از این ابزارها برای استخراج سناریو حمله وجود نداشته باشد. به همین دلیل استفاده از این ابزارها و بررسی

[۹] Context Data

هشدارها به‌صورت محلی به تنهایی کافی نیست. همان‌طور که در سند " Security Operations Centre (SOC) in a Utility Organization " نیز اشاره شده است یکی از دلایلی که منجر به ضعف در دفاع می‌شود عدم استفاده از ابزارهای مناسب است. از جمله ابزارهای مناسبی که در سند فوق به استفاده از آن در فرآیند مدیریت وقایع امنیتی توصیه شده است SIEM است.

ابزار SIEM هشدارهای امنیتی، لاگ‌های ثبت شده، داده و اطلاعات متنی را به‌صورت متمرکز جمع‌آوری کرده و با ارائه قابلیت‌های زیر به برطرف‌کردن یا کاهش چالش‌های مطرح شده فوق، کمک می‌کند.

- دریافت انواع هشدارهای امنیتی و فایل‌های ثبت وقایع
- کاهش تکرار هشدارها و دسته‌بندی آن‌ها
- بررسی و تأیید هشدارها با استفاده از اطلاعات مکمل و داده‌های متنی
- برقراری ارتباط و همبسته‌سازی اثرات مختلف یک حمله که توسط ابزارهای متنوع تولید شده‌اند
- اعمال سیاست امنیتی و انجام واکنش به‌صورت متمرکز

همچنین سازمان امنیت ملی آمریکا در گزارش "Critical Infrastructure Security and Resilience"، ۱۶ زیرساخت را به عنوان زیرساخت‌های حیاتی معرفی کرده است. حملات روی این زیرساخت‌ها در سال‌های اخیر افزایش یافته است. لذا ضروری است که تیمی در SOC با به‌کارگیری ابزارهای مناسب مانند SIEM به عنوان قلب آن، به تأمین امنیت این زیرساخت‌ها بپردازد.

۲-۲ مرکز عملیات امنیت

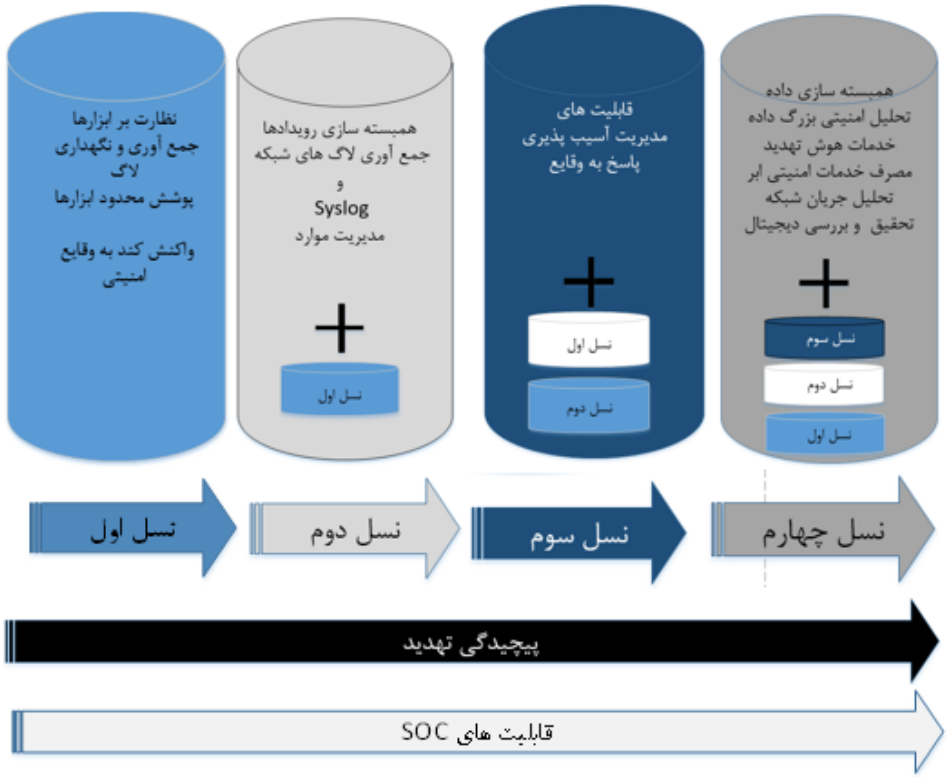
مرکز عملیات امنیت یا SOC[۱۰] با به‌کارگیری فرآیندهای گوناگون، کارشناسان خبره، و زیرسیستم‌های هوشمند، می‌تواند سرویس‌های امنیتی را به‌صورت مدیریت شده ارائه نماید. این سرویس‌ها، گستره‌ی وسیعی را شامل

[۱۰] Security Operations Center

می‌شوند که با توجه به نیازها و اهداف تعیین شده برای تضمین ابعاد گوناگون امنیتی سرویس گیرنده‌ها، تعیین می‌شوند.

۲-۲-۱ نسل‌های مرکز عملیات امنیت

درک ما از مؤلفه‌های SOC و خدمات مورد انتظار در طول زمان تغییر کرده است. این امر بازتابی از تعدیل ادراک ما در ارتباط با میزان اهمیت تضمین اطلاعات و عملیات امنیت است. این تحول در واکنش به تغییرات چشم‌انداز تهدید امنیتی به‌وجود می‌آید. علاوه بر این‌که به‌صورت فزاینده‌ای با استانداردهای رسمی امنیت اطلاعات وفق پیدا می‌کنیم، به استقرار و مدیریت فرآیندهای مرور و مدل عملیات امنیت رسمی نیز نیاز داریم. مسیری که مرکز عملیات امنیت در ۱۵ سال اخیر طی کرده، به چهار نسل افزایشی که در شکل ۱ نشان داده شده، تقسیم شده است.



شکل ۱: چهار نسل مرکز عملیات امنیت

چهار نسل، قابلیت‌های SOC را در پاسخ به افزایش فزاینده پیچیدگی حملات انعکاس می‌دهند. در ادامه به بیان جزئیات خدماتی می‌پردازیم که در هر نسل ارائه شده است.

۲-۲-۱-۱ نسل اول SOC

در این نسل تیم عملیات فناوری اطلاعات متوجه شد که چه خدمات و عملیاتی باید به عنوان SOC در نظر گرفته شود. هنوز ضرورتی نداشت که این تیم برای اداره‌کردن وقایع[۱۱] و رویداد[۱۲]های امنیت اطلاعات مهارت داشته باشد یا آموزش دیده باشد. عملیات امنیت با استقرار یک SOC رسمی ارائه نمی‌شد و در بیشتر موارد توسط یک فرد یا تیم عملیات فناوری اطلاعات که بر ترکیبی از وظایف تمرکز داشتند، این عملیات انجام می‌گردید. این وظایف شامل مسئولیت پایش سلامت شبکه و تجهیزات، مدیریت امنیت ضد بدافزار در سراسر سازمان، و جمع‌آوری فایل‌های ثبت وقایع است. جمع‌آوری فایل‌های ثبت وقایع در نسل اول SOC به تعدادی از منابع و تجهیزاتی که لاگ تولید می‌کنند، مانند دیواره آتش، محدود شده بود. در بیشتر موارد پیغام‌های ثبت شده به‌صورت محلی ذخیره می‌شد. در موارد اندکی یک تجهیز ثبت وقایع متمرکز برای دریافت اطلاعات لاگ در قالب پیغام‌های syslog رمز نشده یا SNMP تدارک دیده می‌شد. در این نسل پیغام‌های ثبت وقایع به ندرت تجزیه و تحلیل می‌شدند و تنها زمانی که یک واقعه گزارش می‌شد یا نوعی عیب‌یابی مورد نیاز بود به آن‌ها مراجعه می‌شد. علاوه بر این، پاسخ به وقایع[۱۳] امنیت اطلاعات به‌صورت رسمی مورد توجه قرار نگرفت و برقرار نشد. همچنین فرآیند شناسایی، مکاتبه‌کردن و واکنش به‌صورت کلی به کندی صورت می‌گرفت.

پیغام‌های فایل‌های ثبت وقایع به‌صورت محلی روی هر سیستم ذخیره می‌شد، به جای این‌که روی یک سیستم جمع‌آوری متمرکز مانند SIEM ذخیره شود. به‌عنوان مثال رویدادهای تلاش ناموفق برای ورود به سیستم در محل ذخیره‌سازی لاگ‌های امنیتی ویندوز ذخیره می‌شد و زیر حجم عظیمی از رویدادهای تولید شده توسط سایر فعالیت‌ها دفن می‌شد.

---

[۱۱] Incident

[۱۲] Event

[۱۳] Incident Response

۲-۲-۱-۲ نسل دوم SOC

در این نسل ابزارهای SIEM شروع به بروز و ظهور کردند. نسل‌های اولیه ارائه‌دهندگان SIEM مانند netForensics، Network Intelligence و Cisco Security Monitoring, Analysis, and Response System (MARS)، وعده‌هایی را مبنی بر تشخیص تهدیدات شبکه، آزادسازی مدیران از انجام کارهای پیچیده و در اغلب موارد غیرممکن مانند تحلیل حجم عظیمی از اطلاعات لاگ، دادند. ارائه دهندگان اولیه چنین ابزارهایی روی مدیریت تهدیدات امنیتی، که تحت نام مدیریت رویدادهای امنیتی نیز مورد ارجاع قرار می‌گیرد تمرکز کردند، که تحلیل بی‌درنگ لاگ‌ها با هدف تشخیص تهدیدات را ارائه می‌دهد. این ابزارها اطلاعات لاگ تولید شده توسط منابع متنوع در قالب‌های متفاوت را می‌پذیرند و فرآیند تشخیص وقایع امنیتی بالقوه را سرعت می‌دهند. ایده اولیه اصلی SEM این است که ابتدا اطلاعات لاگ را در قالب رویدادها از منابع متنوع مانند سیستم‌عامل، تجهیزات امنیتی، و برنامه‌های کاربردی، تجمیع[۱۴] می‌کند. سپس رویدادها به‌منظور این‌که روابط احتمالی بین آن‌ها شناسایی شوند، با یکدیگر همبسته می‌شوند. در نهایت حوادث به‌صورت هشدار در داشبورد، به اپراتور برای بررسی بیشتر گزارش می‌شوند.

۲-۲-۱-۳ نسل سوم SOC

هنگامی که ابزارهای SIEM اهمیت خود را بیشتر نشان دادند، سایر خدمات امنیتی مسیر خود را به SOC پیدا کردند. در این نسل تیم SOC مسئولیت رسیدگی به مدیریت آسیب‌پذیری را بر عهده داشت. علاوه بر این به شدت در اجرا و رسمی‌سازی کارهای مرتبط با واکنش به وقایع درگیر شدند. تیم SOC ممکن است فرآیند مدیریت آسیب‌پذیری را با سایر واحدها انجام دهد یا برخی از کارهای آن را به دیگران واگذار کند.

[۱۴] Aggregate

۲-۲-۱-٤ نسل چهارم SOC

این نسل خدمات امنیتی پیشرفته‌ای که تلاش می‌کردند از عهده تهدیدات امنیتی جدید برآیند را معرفی کرد. اولین مفهوم جدید بسط همبسته‌سازی رویداد محدودی است که در نسل‌های پیشین SIEM داشتیم، به امنیت بزرگ داده. تحلیل‌های امنیتی بزرگ داده می‌توانند به‌عنوان توانایی تحلیل حجم عظیمی از داده در بازه‌های زمانی طولانی برای کشف تهدیدات و سپس ارائه و بصری‌سازی نتایج تعریف شوند. پلت‌فرم بزرگ داده برای مصرف داده از هر منبعی با سرعت بالا و با حجم عظیم توسعه داده می‌شود، در حالی‌که قادر است تحلیل‌های پیچیده امنیتی بی‌درنگ و غیربی‌درنگ را انجام دهد.

مفهوم جدید دیگر در مرکز عملیات امنیت نسل چهارم غنی‌سازی داده[۱۵] از طریق استفاده از منابعی همچون اطلاعات جغرافیایی، داده‌های سیستم نام دامنه، یکپارچه‌سازی کنترل دسترسی شبکه، و خدمات اعتبار دامنه و IP است. اطلاعات شبکه تله متری برای شبکه‌های پیچیده و نظارت امنیتی مورد استفاده قرار می‌گیرد و اساساً تجهیزات شبکه مشترک را به درگاه‌های حسگر امنیتی تبدیل می‌کند. تکنولوژی‌های جدیدی که توسط SOC برای جرم‌یابی و تشخیص حفره[۱۶]های شبکه مورد استفاده قرار می‌گیرد، همچنین به‌عنوان راه‌حل‌های تشخیص حفره شناخته می‌شوند. از یکپارچه‌سازی متقابل محصولات به‌منظور خودکارسازی اصلاح بهره‌برداری می‌شود، مانند این سناریو، سیستم تشخیص نفوذی که یک تهدید را شناسایی می‌کند و از یک تکنولوژی کنترل دسترسی شبکه برای انجام اصلاح خودکار بهره می‌برد.

به‌طور خلاصه چهارمین نسل مرکز عملیات، امنیت منابع اطلاعات تهدید را گسترش می‌دهد، قابلیت‌های امنیتی متفاوت را برای مبارزه با تهدیدات پیشرفته‌تر لایه‌بندی می‌کند، و امنیت را برای بهبود زمان واکنش به حوادث خودکارسازی می‌کند.

---

[۱۵] Data Enrichment

[۱۶] Breach

۲-۲-۲ ویژگی‌های یک مرکز عملیات امنیت مؤثر

برای ایجاد و عملیاتی‌کردن یک مرکز عملیات مؤثر، سازمان‌ها باید تعدادی از عوامل حیاتی موفقیت را در نظر بگیرند. برخی اقداماتی که تقریباً در تمام سازمان‌هایی که یک مرکز عملیات امنیت موفقیت‌آمیز را راه‌اندازی کرده‌اند، یافت می‌شود، به شرح زیر است:

- **حامی اجرایی**[۱۷]: برنامه SOC باید حامی اجرایی داشته باشد. این حمایت مالی باید به شکلی باشد که حامی مالی، مأموریت مالی را امضا کند و تیم SOC به‌روزرسانی‌های دوره‌ای را به حامی مالی ارائه کند، و انتظار می‌رود که در تصمیمات مهمی که برای یا توسط SOC گرفته می‌شود درگیر باشد (به‌عنوان مثال استفاده از ابزارهای جدید یا گسترش تیم SOC). CIO و در برخی موارد CEO حامی های اجرایی داخلی ایده‌آلی برای برنامه SOC هستند.
- **حکومت**[۱۸]: ایجاد یک ساختار حکومتی برای موفقیت هر برنامه امنیتی حیاتی است. بایستی معیارهایی برای سنجش اثربخشی قابلیت‌های SOC تعیین شود. این معیارها باید دیدگاه کافی و قابل توجهی را در مورد عملکرد SOC به تیم مدیریت سازمان ارائه دهند و زمینه‌هایی که در آن‌ها بهبود و سرمایه گذاری مورد نیاز است را شناسایی کنند.
- **عملیاتی‌کردن SOC به عنوان یک برنامه:** سازمان‌ها باید SOC را به عنوان یک برنامه نسبت به یک پروژه تنها، عملیاتی کنند. انجام چنین کاری بر اهمیت و میزان منابع لازم برای طراحی، ساخت و اجرای خدمات مختلف ارائه شده توسط SOC تکیه دارد. داشتن یک استراتژی واضح خدمات SOC با اهداف و اولویت‌های واضح، اندازه برنامه SOC، جدول زمانی و میزان منابع مورد نیاز برای تحقق اهداف برنامه را تعیین می‌کند.

---

[۱۷] Executive Sponsorship

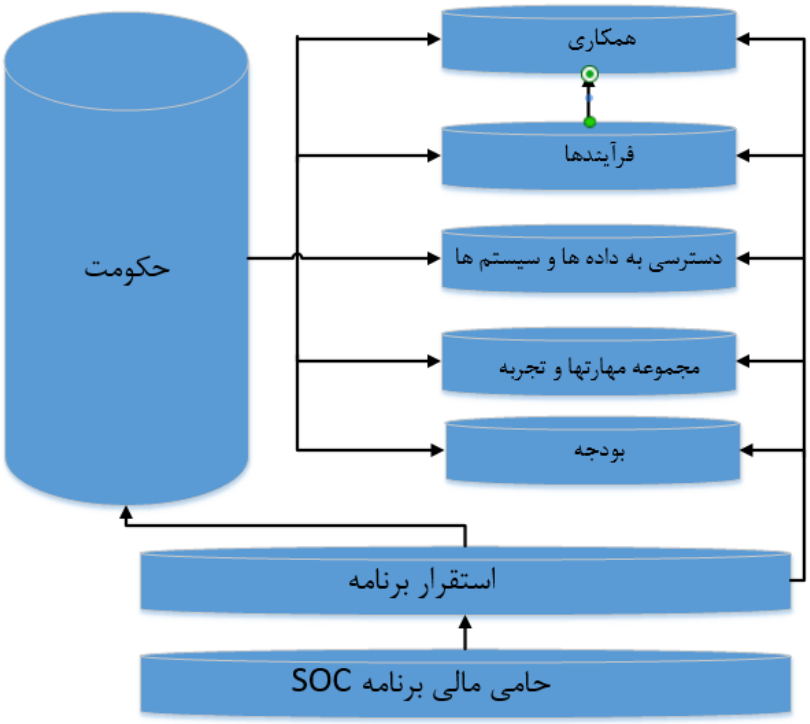
[۱۸] Governance

- **همکاری**: واحدهای متفاوت در یک سازمان باید در طول فازهای برنامه‌ریزی، طراحی، ساخت، و عملیاتی‌کردن SOC با یکدیگر همکاری کنند. همکاری دقیق و روابط بین ادارات باید در حین فاز طراحی و ساخت SOC بطور رسمی تعریف شود.
- **دسترسی به داده‌ها و سیستم‌ها**: دسترسی به اطلاعات و سیستم‌های مورد نیاز باید به تیم SOC داده شود تا بتوانند وظایف خود را انجام دهند: قبل، در حین و پس از حادثه امنیتی. تعریف دقیق دسترسی باید در طول فازهای طراحی و ساخت SOC ایجاد شود. برای مثال می‌تواند شامل دسترسی به داده های ورود یا دسترسی به پیکربندی سیستم باشد. در پایین‌ترین سطح ابزارهای SOC باید پیغام‌های لاگ را از سیستم‌ها و برنامه‌های کاربردی متنوع دریافت کنند.
- **رویه[۱۹]ها و فرآیندهای قابل اجرا**: تیم SOC باید با فرآیندها و دانش برقرار شده مجهز شود و با یک مجموعه مناسب از ابزارها تقویت شود. فرآیندهای ایجاد شده طی فازهای طراحی و ساخت، باید قابلیت‌های جاری و مطلوب را در نظر بگیرند.
- **مجموعه مهارت و تجربه**: تیم SOC باید با مجموعه مهارت‌های مناسبی که آن‌ها را برای اجرای وظایف‌شان از نظر تکنولوژی‌های عملیاتی و تحقیق و بررسی در مورد حوادث قادر می‌سازد، مجهز شود. سازمان باید آموزش کارمندان موجود یا جذب نیرو با مهارت‌های مورد نیاز را در نظر بگیرد.
- **بودجه**: موضوع بودجه نسبی است. بودجه‌ای که به ساخت و عملیاتی‌کردن فازها تخصیص داده می شود، به فاکتورهایی مانند موارد زیر وابسته است:
  - ایجاد SOC در سازمان و یا برون‌سپاری آن
  - خدمات ارائه شده توسط SOC
  - ساعات عملیاتی‌بودن SOC
  - فاصله مجموعه مهارت‌ها

[۱۹] Procedure

- نقشه راه سطح صلاحیت مطلوب

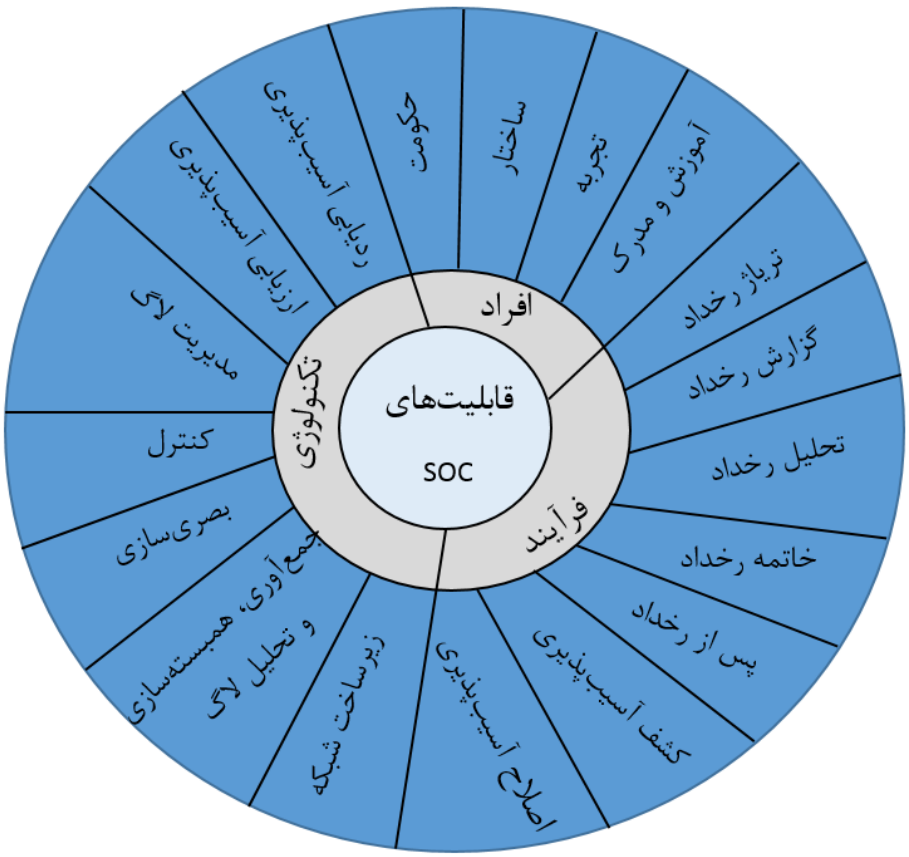
رابطه بین ویژگی‌های مختلف در شکل ۲ نمایش داده شده است.



شکل ۲: ویژگی‌های یک مرکز عملیات امنیت مؤثر

۲-۲-۳ قابلیت‌های مرکز عملیات امنیت

بر اساس رویکردی قابلیت‌های SOC به دسته‌های افراد، فرآیند و فناوری تقسیم می‌شوند. این قابلیت‌ها در شکل ۳ به تصویر کشیده شده است. می‌توان از این قابلیت‌های متنوع برای ارزیابی یک سازمان استفاده کرد. برای هر قابلیت موضوعاتی مطرح می‌شود، نتایج این موضوعات برداشت کلی از سطح بلوغ هر قابلیت را ارائه می‌کند.



شکل ۳: قابلیت‌های مرکز عملیات امنیت

۲-۲-۳-۱ افراد

افراد[۲۰]، هسته هر SOC موفق هستند. هنگامی که قابلیت‌های مرتبط با افراد را ارزیابی می‌کنید، باید زمینه‌هایی که به حکومت، ساختار، تجربه، و آموزش و مدرک مربوط هستند را در نظر بگیرید. در ادامه برخی از مواردی آمده است که باید هنگام بررسی افراد و با توجه به قابلیت‌های فناوری اطلاعات، مورد توجه قرار گیرند.

[۲۰] People

۲-۲-۳-۱-۱ حکومت

مهم است بدانیم که SOC چگونه مدیریت می‌شود. همچنین مهم است بدانیم که سازمان چگونه SOC را می بیند و مدیریت می‌کند. در اینجا برخی از نمونه‌های ارزیابی حاکمیت آورده شده است:

- ارزیابی سطح آگاهی مدیریت ارشد از اهمیت SOC
- ارزیابی مشارکت و سرمایه‌گذاری مدیریت ارشد در حمایت از پروژه‌ها و فعالیت‌های عملیات امنیتی
- شناسایی قابلیت‌های گزارش موجود در رابطه با انجام ممیزی و شناسایی وضعیت فعلی امنیت
- مستندسازی عملکرد مدیریت هنگام تشدید رخداد از نظر طبقه‌بندی و اصلاح آن

۲-۲-۳-۱-۲ ساختار[۲۱]

برای این‌که بتوانید افرادی که دارای صلاحیت مناسب برای پاسخگویی به سوالات شما هستند را شناسایی کنید، مهم است که ساختار سازمان را بدانید. (و به این ترتیب می‌توانید مسئولیت‌های مربوط به وظایف مختلف را درک کنید). در اینجا برخی از نمونه‌های ارزیابی ساختار آورده شده است:

- درکی از ساختار سازمانی کلی به‌دست آورده و مدل گزارش‌دهی را ارزیابی کنید. روی بخش یا واحدی که SOC در آن کار می‌کند تمرکز کنید.
- آیا ساختار سازمانی، رسمی و مستند شده است؟ آیا یک واحد یا تیم وجود دارد که به عملیات امنیتی و نظارت بر وقایع امنیتی متعهد باشد؟
- آیا موارد تضاد منافع وجود دارد که در آن، برای مثال، فرد یکسانی می‌تواند وظایف مربوط به امنیت را درخواست و تأیید کند و یا تغییراتی در آن‌ها اعمال کند؟
- درک روابط بین نقش‌ها و بخش‌های مختلف که در عملیات امنیتی شرکت دارند.

---

[۲۱] Structure

- نمونه‌هایی از نقش‌هایی که شما به طور معمول از آن‌ها تحقیق می‌کنید عبارتند از: مدیر ریسک، تحلیل‌گر امنیتی، محقق امنیتی، و متخصص امنیت شبکه.
- ارزیابی این‌که آیا فرآیندهای رسمی برای تبادل اطلاعات امنیتی بین بخش‌های سازمان وجود دارد؟

۲-۲-۳-۱-۳ کارآزمودگی

سازمان‌ها معمولا منابعی دارند، خواه درون سازمان یا به‌صورت برون‌سپاری شده، که می‌توانند کنترل‌های امنیتی شبکه و سیستم را طراحی و مدیریت کنند. اگر چه این‌ها منابع ارزشمندی هستند که می‌خواهید در برنامه SOC خود از آن‌ها بهره ببرید، دیگر بخش‌های حیاتی و تخصصی کارآزمودگی SOC وجود دارد که باید ارزیابی کنید. از جمله می‌توان موارد زیر را در نظر گرفت:

- اداره‌کردن رخداد[۲۲]
- تحقیق و بررسی دیجیتال[۲۳]
- ارزیابی آسیب‌پذیری
- مدیریت لاگ[۲۴]
- کار با ابزارهای مدیریت اطلاعات و رویدادهای امنیتی
- هوش تهدیدات[۲۵]
- فناوری‌های بزرگ داده
- مدیریت افراد
- تجزیه و تحلیل داده[۲۶]

---

[۲۲] Incident Handling
[۲۳] Digital Investigation
[۲۴] Log Management
[۲۵] Threat Intelligence
[۲۶] Data Analytics

سایر جنبه‌های کارآزمودگی SOC که باید ارزیابی شود شامل کار تحت فشار، به ویژه تحت رخدادهای مهم امنیتی و مجموعه مهارت‌ها است. بیشتر نقش‌های شغلی مهارت‌های خاصی را نیاز دارند. به عنوان مثال افرادی که مسئول تحقیقات دیجیتال هستند باید تجربه جرم‌یابی و دانش ابزارهایی مانند EnCase را داشته باشند.

۲-۲-۳-۱-٤ آموزش و مدرک

درک اقدامات آموزشی برای شناسایی این‌که چگونه SOC با تغییرات و نیازهای رضایت شغلی کارکنان وفق داده می‌شود، مهم است. بسیاری از مردم می‌خواهند فرصتی برای رشد در کاری که انجام می‌دهند داشته باشند، و به طور معمول نیازمند آموزش و کسب گواهی‌نامه برای اعتباردهی به دستاوردهای جدید هستند. در اینجا چند راه برای جستجوی این اطلاعات وجود دارد:

- جمع‌آوری اطلاعات در مورد دوره‌های آموزشی مربوطه که افراد در آن‌ها شرکت کرده‌اند و گواهی نامه‌هایی که دریافت کرده‌اند.
- ارزیابی این‌که آیا فرآیندهایی برای شناسایی دوره‌های آموزشی مورد نیاز برای عملیات امنیت اطلاعات وجود دارد. در بسیاری از موارد، متوجه خواهید شد که کسب دانش جدید بر روی تلاش‌های فردی متکی است نه به برنامه آموزشی خوب طراحی شده.
- شناسایی هر مقرراتی که در اهداف فناوری اطلاعات یافت می‌شود که افراد به دلیل وجود آن‌ها نیاز به داشتن گواهینامه خاص دارند. ارزیابی این‌که آیا گواهینامه برای این نیازمندی‌ها مورد تأیید قرار گرفته است.
- تطبیق فناوری‌ها از اهداف فناوری اطلاعات با آموزش و گواهینامه‌های به دست آمده و یا در حال به دست آمدن.

۲-۲-۳-۲ فرآیندها

فرآیندها توانمندسازهای بین افراد و تکنولوژی‌ها هستند. فرآیندهای عملیات امنیتی که می‌خواهید ارزیابی کنید و مربوط به نحوه برخورد با حوادث و آسیب‌پذیری‌های امنیتی است. درک و ثبت وضعیت فعلی فرآیندهای

SOC برای توسعه یک نقشه راه مناسب و واقع‌بینانه مهم است. فرآیندهای SOC را می‌توان به تریاژ رخداد[۲۷]، گزارش رخداد، تحلیل رخدادها، خاتمه رخداد[۲۸]، پس از رخداد، کشف آسیب‌پذیری، و ردیابی و اصلاح آسیب‌پذیری طبقه‌بندی کرد. در اینجا برخی زمینه‌های کشف کلی وجود دارند که باید هنگام جمع‌آوری اطلاعات برای این فرآیندها در نظر گرفته شود.

۲-۲-۳-۲-۱ تریاژ رخداد

- ارزیابی این‌که آیا طرحی برای پاسخ به رخداد امنیتی کامپیوتر که فرآیند تریاژ را رسمی کند، وجود دارد؟
- ارزیابی این‌که آیا کانال‌ها و قالب‌های رسمی برای گزارش حوادث امنیتی وجود دارند. آیا اعضای سازمان این کانال‌ها را می‌شناسند؟
- ارزیابی این‌که آیا فرآیندهایی برای طبقه‌بندی و اولویت‌بندی رویدادها وجود دارد؟
- ارزیابی این‌که آیا توافقنامه سطح خدمات داخلی یا خارجی وجود دارد (SLA[۲۹]) که سازمان باید آن را در نظر بگیرد؟

۲-۲-۳-۲-۲ گزارش رخداد

- ارزیابی این‌که آیا فرآیندهایی برای شناسایی گزارش‌های مورد نیاز، تعداد دفعات گزارش‌ها، ساختار گزارش‌ها و مواردی که باید در طول حیات یک رخداد مطلع شوند، وجود دارند؟
- ارزیابی قابلیت‌های گزارش‌دهی رخداد در طول ساعات اداری و بعد از آن

---

[۲۷] Incident Triage

[۲۸] Incident Closer

[۲۹] Service Level Agreement

۲-۲-۳-۳ تحلیل رخداد

- ارزیابی این‌که آیا فرآیندهایی برای تحلیل رخدادهای امنیتی نگاشت شده به طبقه‌بندی رخدادها وجود دارد
- ارزیابی این‌که آیا روش‌هایی برای بازیابی و تجزیه و تحلیل داده‌ها از عناصر مختلف فنی وجود دارد و این که آیا این فرآیندها به فناوری که در حال گسترش است مرتبط است
- ارزیابی این‌که آیا فرآیندهای تحلیل رخداد به موارد کاربرد امنیتی مرتبط شده است
- ارزیابی این‌که آیا فرآیندهایی برای درگیر کردن گروه‌های خارجی و داخلی در تحلیل و بررسی رخدادهای امنیتی وجود دارد

۲-۲-۳-٤ خاتمه رخداد

- ارزیابی این‌که آیا موافقت‌نامه‌های سطح سرویسی که شامل رخدادها شود، وجود دارد
- ارزیابی این‌که آیا موافقت‌نامه‌های سطح سرویس برای ریشه‌کن کردن رخدادها و درنهایت بازگرداندن سرویس‌ها وجود دارد
- ارزیابی این‌که آیا فرآیندهایی برای برچسب‌گذاری رخدادها به عنوان خاتمه یافته وجود دارد

۲-۲-۳-۵ پس از رخداد

- آیا فرآیندی برای ذخیره اطلاعات جمع‌آوری شده و مکاتباتی که در حین حادثه رد و بدل می‌شوند، وجود دارد
- آیا تمرین یادگرفته شده‌ای هست که در برنامه مدیریت مخاطره قرار گیرد
- آیا حوادث عمده در جلسات کمیته (مثلا کمیته کنترل امنیت اطلاعات یا کمیته مدیریت مخاطره) مورد بحث قرار می‌گیرند

۲-۲-۳-٦ کشف آسیب‌پذیری

- ارزیابی این‌که آیا مراحل کشف آسیب‌پذیری وجود دارد
- ارزیابی این‌که آیا فرآیندهای دریافت و استفاده از اخبار آسیب‌پذیری وجود دارند

- ارزیابی این‌که آیا فرآیندهایی برای ارزیابی تأثیر آسیب‌پذیری‌ها و اولویت‌بندی فعالیت‌های اصلاح بر اساس تأثیر آن‌ها، وجود دارد
- ارزیابی فاصله‌های بین اقدامات کشف و بخشی از شبکه که ارزیابی شده است

۲-۲-۳-۲-۷ ردیابی و اصلاح آسیب‌پذیری

- ارزیابی این‌که آیا فرآیندهایی برای مکاتبه آسیب‌پذیری به صاحبان سیستم و اپراتورها وجود دارد
- ارزیابی این‌که که آیا فرآیندهایی برای بازبینی و ردیابی وضعیت آسیب‌پذیری‌های کشف شده وجود دارد

۲-۲-۳-۳ فناوری

همانند افراد و فرآیندها، استفاده از فناوری مناسب برای موفقیت SOC بسیار مهم است. دسته‌های فناوری که باید مورد ارزیابی قرار بگیرند مربوط به آمادگی زیرساخت، جمع‌آوری و پردازش لاگ، نظارت بر سیستم، موقعیت کنترل امنیتی و مدیریت آسیب‌پذیری است. در ادامه زمینه‌هایی که برای جمع‌آوری اطلاعات باید درنظر بگیرید آورده شده است.

۲-۲-۳-۳-۱ آمادگی زیرساخت شبکه

- بررسی این‌که آیا یک شبکه مدیریتی خارج از محدوده سیستم‌ها، برای نظارت و مدیریت سیستم‌ها مورد استفاده قرار می‌گیرد، در صورت وجود، دامنه و محدوده پوشش این شبکه را بررسی کنید
- ارزیابی قابلیت‌ها برای دسترس‌پذیری بالای سیستم‌های حیاتی
- بررسی سطوح عملکرد شبکه مانند تجهیزات اشباع شده یا فناوری‌های از دسترس خارج شده، که منجر به نارضایتی مشتری یا کاربر می‌شوند

۲-۲-۳-۳-۲ جمع‌آوری، همبسته‌سازی و تحلیل رویدادها

- ارزیابی این‌که آیا طراح جمع‌آوری لاگ در محل وجود دارد
- بررسی مقیاس‌پذیری پلت‌فرم جمع‌آوری، همبسته‌سازی و تحلیل رویداد

- ارزیابی این‌که آیا سیستم‌ها برای ارسال رویدادهای خود پیکربندی شده‌اند
- ارزیابی این‌که آیا لیستی از موارد کاربرد امنیتی وجود دارد
- ارزیابی این‌که آیا پلت‌فرم تجزیه و تحلیل رویداد و همبستگی برای لیست موارد کاربرد بهینه شده است. دلیل این امر این است که سیستم رویدادهای خاصی را دریافت می‌کند با این‌که تمام رویدادها را دریافت می‌کند

۲-۲-۳-۳-۳ نظارت[۳۰]

- بررسی این‌که آیا جریان‌های شبکه گرفته شده و تحلیل می‌شوند
- ارزیابی این‌که آیا بسته‌های شبکه گرفته شده و تحلیل می‌شوند
- ارزیابی قابلیت‌های گزارش‌گیری
- ارزیابی شکاف در نظارت، مانند نظارت بر نقاط کور، تأخیر بین گزارش‌دهی و غیره
- ارزیابی قابلیت‌های نظارت در طول عملیات عادی و بعد از ساعت‌ها

۲-۲-۳-۳-٤ کنترل

- بررسی این‌که آیا کنترل‌های امنیتی مناسب توسعه داده شده‌اند، این مهم است زیرا رویدادها توسط کنترل‌های امنیتی تولید و توسط SOC ذخیره می‌شوند. به عنوان مثال بررسی این‌که آیا دیواره آتش یا سیستم‌های تشخیص/جلوگیری از نفوذ برای محافظت از داده‌های مرکز داده وجود دارند
- ارزیابی این‌که آیا امنیت به درستی پیکربندی شده است تا اقدامات مناسب انجام شود و رویدادهای مربوطه ایجاد شوند
- ارزیابی این‌که آیا کنترل دسترسی مبتنی بر نقش بر روی تمام تجهیزات مهم فعال شده است، به‌منظور حصول اطمینان از دسترسی افراد مجاز به آن‌ها

---

[۳۰] Monitoring

۲-۲-۳-۳-۵ مدیریت فایل‌های ثبت وقایع

- ارزیابی این‌که آیا یک بستر مدیریت فایل‌های ثبت وقایع برای ذخیره رویدادها، در رابطه با سیاست نگهداری لاگ‌های سازمان، مورد استفاده قرار می‌گیرد
- بررسی این‌که چه تجهیزاتی لاگ‌ها را ارسال می‌کنند و چه تجهیزات دیگری هستند که از قلم افتاده اند اما دریافت لاگ از آن‌ها می‌تواند ارزش بیشتری را برای SOC فراهم کند
- بررسی گزارش‌دهی و تولید آلارم راه‌حل مدیریت لاگ و قابلیت اشتراک اطلاعات با سایر سیستم‌ها

۲-۲-۳-۳-۶ ارزیابی آسیب‌پذیری

- بررسی این‌که آیا ابزارهایی برای کشف آسیب‌پذیری وجود دارد
- بررسی این‌که آیا این ابزارها می‌توانند انواع مختلف آسیب‌پذیری را تشخیص دهند: پویش‌گر شبکه، پویش‌گر وب و غیره. این کار شامل این است که آسیب‌پذیری‌ها چگونه ارزیابی می‌شوند، مانند پویش امضاهای آسیب‌پذیری در مقایسه با اجرای کد سوءاستفاده در برابر یک آسیب‌پذیری برای تأیید آن
- بررسی این‌که آیا ابزارها نگهداری می‌شوند
- بررسی این‌که آیا خروجی این ابزارها با سایر پلت‌فرم‌های امنیتی مانند مدیریت مخاطره و SIEM یکپارچه شده است

۲-۲-۳-۳-۷ ردیابی آسیب‌پذیری

- ارزیابی این‌که آیا از ابزارهایی برای ردیابی وضعیت آسیب‌پذیری‌های کشف شده استفاده می‌شود

۲-۲-۳-۳-۸ بلیط دهی

- جمع‌آوری اطلاعات در مورد سیستم بلیط‌دهی و این‌که آیا از آن برای اهداف عملیات امنیتی استفاده می‌شود
- بررسی این‌که آیا سیستم بلیط‌دهی با ابزارهای دیگر مانند SIEM و ابزارهای مدیریت آسیب‌پذیری یکپارچه شده است

- شناسایی این‌که آیا سلامت عملیات تجاری می‌تواند بر اساس مؤثر بودن سیستم بلیط‌دهی اندازه‌گیری شود

۹-۳-۳-۲-۲ همکاری

- ارزیابی این‌که آیا پلت‌فرمی وجود دارد که تیم SOC بتواند از آن به طور ایمن برای اشتراک‌گذاری و انتشار اسناد استفاده کند
- ارزیابی این‌که همکاری بین بخشهای مختلف طی وقوع یک رخداد با چه سرعتی می‌تواند به‌وجود آید
- تشخیص این‌که چه تیم‌هایی خارج از SOC با SOC همکاری می‌کنند

برای این‌که SOC بتواند به خوبی وظایف محول شده به خود را انجام دهد، ضروری است از ابزارهای مناسبی در آن استفاده شود. یکی از این ابزارها که در دسته فناوری قرار می‌گیرد SIEM است که از آن به عنوان قلب SOC یاد می‌شود. در ادامه به تعریف SIEM و معرفی قابلیت‌های آن می‌پردازیم.

۳-۲ تعریف SIEM و معرفی قابلیت‌های آن

سامانه مدیریت اطلاعات و رویدادهای امنیتی، سامانه‌ای است که با هدف مدیریت رویداد و اطلاعات امنیتی، طیف گسترده‌ای از هشدارهای امنیتی، لاگ‌ها و منابع داده متنی را به‌صورت بی‌درنگ و غیر بی‌درنگ جمع آوری کرده و به شکل کوتاه‌مدت و بلندمدت ذخیره می‌کند. سامانه مدیریت رویداد و اطلاعات امنیتی با به کارگیری توابعی، به‌صورت بی‌درنگ و تحلیل تاریخچه‌ای، سعی در تأیید و تجمیع هشدارهای امنیتی و لاگ ها و همبسته‌سازی چندین هشدار امنیتی و لاگ که متعلق به یک توالی یا زنجیره حمله هستند، دارد. SIEM به رخدادهای امنیتی شناسایی شده واکنش نشان داده و نتایج تحلیل را در قالب گزارش و به‌صورت بی‌درنگ در داشبوردهایی ارائه می‌کند. در این سامانه هشدارهای امنیتی و لاگ‌های جمع‌آوری شده به‌صورت بلندمدت نگهداری می‌شوند. سامانه مدیریت رویداد و اطلاعات امنیتی با تحلیل تاریخچه‌ای آن‌ها از بررسی رخداد، جرم‌یابی، و ارائه گزارش مطابقت با استانداردها پشتیبانی می‌کند.

۲-۳-۱ قابلیت‌های SIEM

یکی از مسائل پراهمیت انتخاب این سامانه‌ها برای دریافت خدمات مورد نیاز است. گارتنر که یک مؤسسه تحقیقاتی است و در زمینه فناوری اطلاعات کارهای تحقیقاتی و مشاوره‌ای انجام می‌دهد از سال ۲۰۰۸ تا سال ۲۰۱۶ میلادی به ارزیابی SIEMها پرداخته و هر ساله SIEMها را رتبه‌بندی می‌کند. گارتنر بر اساس مجموعه ای از قابلیت‌ها که آن‌ها را قابلیت‌های کلیدی می‌نامد SIEMها را رتبه‌بندی می‌کند. در ادامه این قابلیت‌ها بیان می‌شوند.

۲-۳-۱-۱ معماری مقیاس‌پذیر و توسعه انعطاف‌پذیر

مقیاس‌پذیری از تصمیمات طراحی‌های در زمینه‌های معماری محصول، تکنیک‌های جمع‌آوری داده‌ها، طراحی های عامل، و شیوه‌های برنامه‌نویسی حاصل می‌شود. مقیاس‌پذیری می‌تواند به‌وسیله موارد زیر به‌دست آید:

- سلسله‌مراتبی از کارگزارهای SIEM: سطح‌بندی سیستم‌هایی که داده را ذخیره، تجمیع و همبسته می کنند
- عملکردهای کارگزار به بخش‌هایی تقسیم می‌شوند: تخصیص کارگزارهایی برای همبسته‌سازی مجموعه، ذخیره، گزارش‌دهی، و نمایش
- ترکیبی از سلسله‌مراتب و تقسیم‌بندی به منظور پشتیبانی از مقیاس‌پذیری افقی

در طول فاز برنامه‌ریزی، بسیاری از سازمان‌ها حجم داده‌های رویدادی که جمع‌آوری خواهند شد و همچنین دامنه گزارش‌های تجزیه و تحلیلی که مورد نیاز است را دست پائین می‌گیرند. معماری که از مقیاس‌پذیری و انعطاف‌پذیری توسعه پشتیبانی می‌کند، یک سازمان را قادر می‌سازد تا توسعه آن را با توجه به حجم رویداد و تجزیه و تحلیل‌های غیرمنتظره سازگار سازد.

۲-۳-۱-۲ جمع‌آوری بی‌درنگ داده‌های رویداد

محصولات SIEM داده‌های رویداد را در زمانی نزدیک به زمان واقعی به شیوه‌ای که تحلیل بی‌درنگ را امکان پذیر می‌سازد، جمع‌آوری می‌کنند. روش‌های جمع‌آوری داده عبارتند از:

- دریافت جریان داده syslog از منبع رویداد تحت نظارت

- عامل‌ها به‌صورت مستقیم روی منبع رویداد تحت نظارت یا در یک نقطه تجمیع مانند یک کارگزار syslog نصب شده‌اند
- فراخوانی رابط خط فرمان سیستم تحت نظارت
- APIهای ارائه شده توسط منبع رویداد تحت نظارت
- جمع‌آوری‌کننده‌های خارجی که توسط ابزار SIEM ارائه شده‌اند

نکته: این تکنولوژی همچنین باید از جمع‌آوری داده‌های دسته‌ای برای مواردی که جمع‌آوری زمان واقعی عملی نیست یا مورد نیاز نیست، پشتیبانی کند.

گزینه‌های فیلترکردن در منبع، به‌خصوص برای توسعه‌های توزیع‌شده در شبکه‌های با پهنای باند محدود نیز روش‌های مهمی برای کاهش داده‌ها هستند. چنان‌چه سازمان‌ها بار کاری خود را روی زیرساخت‌های عمومی و مجازی به عنوان یک خدمات محیط ابر انتقال دهند، گزینه‌های جمع‌آوری مبتنی بر عامل و گزینه‌های زیرساخت SIEM مجازی اهمیت بیشتری پیدا خواهند کرد. تعداد روزافزون سازمان‌هایی که تکنولوژی SIEM را مستقر کرده‌اند، باید منابع داده‌ای که به طور رسمی توسط فروشندگان SIEM پشتیبانی نمی‌شوند را به آن اضافه کنند. محصولات SIEM باید APIها یا سایر توابع را برای پشتیبانی از ادغام منابع داده بیشتر توسط کاربر، ارائه کنند. این قابلیت مهم‌تر از آن است که سازمان‌ها تکنولوژی SIEM را برای نظارت بر لایه کاربردی اعمال کنند.

۲-۳-۱-۳ نرمال‌سازی رویداد و دسته‌بندی[۳۱]

این نگاشتی از اطلاعات منابع ناهمگن به یک قالب مشترک طبقه‌بندی رویداد است. یک طبقه‌بندی به تشخیص الگو کمک می‌کند و همچنین دامنه و پایداری قوانین همبسته‌سازی را بهبود می‌بخشد. هنگامی که رویدادها از منابع ناهمگن نرمال‌سازی می‌شوند، آن‌ها می‌توانند توسط تعداد کمتری قانون همبسته‌سازی تجزیه و تحلیل

[۳۱] Taxonomy

شوند، که این امر منجر به کاهش کار توسعه و پشتیبانی است. علاوه بر این هنگام توسعه گزارش و داشبوردها کار با رویدادهای نرمال‌سازی‌شده راحت‌تر است.

۲-۳-۱-٤ نظارت بی‌درنگ

همبسته‌سازی رویداد رابطه بین رویدادها و پیغام‌هایی که توسط ابزارها، سیستم‌ها یا برنامه‌های کاربردی تولید شده‌اند را بر اساس ویژگی‌هایی مانند مبدأ، مقصد، پروتکل، و نوع رویداد برقرار می‌کند. همچنین باید یک کتابخانه از قوانین همبسته‌سازی از پیش تعریف شده وجود داشته باشد و توانایی سفارشی‌سازی این قوانین به‌راحتی فراهم باشد. یک کنسول رویداد امنیتی باید نمایش زمان واقعی رویداها و رخدادهای امنیتی را ارائه کند.

۲-۳-۱-٥ پروفایل‌سازی رفتار[۳۲]

پروفایل‌سازی رفتار با استفاده از یک فاز یادگیری، پروفایلی از فعالیت‌های هنجار برای دسته‌های متنوع رویداد مانند جریان‌های شبکه، فعالیت کاربر، دسترسی به کارگزار، و غیره می‌سازد. فاز نظارت هنگام انحراف از حالت هنجار هشدار تولید می‌کند. پروفایل‌سازی و تشخیص ناهنجاری، قابلیت‌های جدید SIEM هستند که مکمل همبسته‌سازی مبتنی بر قانون هستند.

۲-۳-۱-٦ دانش تهدیدات[۳۳]

دانش درباره محیط تهدیدات جاری در منابع متنوعی مانند لیست‌های منبع باز، محتوای تهدید و اعتبار توسعه داده شده و نگهداری شده توسط تیم‌های تحقیقاتی امنیتی فروشندگان امنیتی، و داده‌های توسعه داده شده توسط امنیت مدیریت شده و سایر ارائه دهندگان خدمات، وجود دارد. داده‌های اطلاعات تهدیدات می‌توانند

---

[۳۲] Behavior Profiling

[۳۳] Threat Intelligence

با یک SIEM در قالب لیست‌های قابل مشاهده، پرس‌وجو و قوانین همبسته‌سازی به شیوه‌ای که میزان موفقیت تشخیص زود هنگام را افزایش می‌دهد، تجمیع شوند.

۲-۳-۱-۷ مدیریت لاگ و گزارش سازگاری[۳۴]

عملکردها از ذخیره مقرون‌به‌صرفه و تحلیل منبع بزرگی از اطلاعات شامل جمع‌آوری، شاخص‌گذاری و ذخیره سازی همه داده‌های لاگ و رویداد از هر منبعی، همچنین قابلیت جستجو و گزارش‌گیری روی آن داده‌ها پشتیبانی می‌کنند. قابلیت‌های گزارش‌دهی باید شامل گزارش‌های از پیش تعریف شده، همچنین توانایی تعریف گزارش‌های خاص، یا استفاده از ابزارهای گزارش‌دهی شخص ثالث باشد.

۲-۳-۱-۸ تحلیل

تجزیه و تحلیل رویدادهای امنیتی شامل نمایه‌های داشبورد، عملکردهای پرس‌وجوی خاص و گزارش‌ها برای پشتیبانی از بررسی فعالیت کاربر دسترسی به منابع به منظور شناسایی تهدید، نقض یا سوءاستفاده از حقوق دسترسی است.

۲-۳-۱-۹ پشتیبانی از مدیریت رخدادها

پشتیبانی ویژه از مدیریت رویداد و گردش کار باید در محصول SIEM تعبیه شود تا بتواند از سازمان امنیت فناوری اطلاعات پشتیبانی کند. محصولات باید با سیستم‌های تجاری جریان کاری یکپارچه شوند و باید از پرس‌وجوهای متفاوت برای بررسی رخدادها پشتیبانی کنند.

---

[۳۴] Compliance Reporting

۲-۳-۱-۱۰ نظارت بر فعالیت کاربران و دسترسی به داده

این قابلیت اطلاعات زمینه‌ای مربوط به داده و کاربر را برقرار می‌کند و امکان پایش فعالیت و دسترسی به داده را فراهم می‌کند. توابع شامل ادغام با زیرساخت‌های مدیریت دسترسی و هویت (IAM) برای به دست آوردن اطلاعات زمینه‌ای کاربر، و استفاده از اطلاعات زمینه‌ای کاربر در همبستگی، تجزیه و تحلیل، و گزارش‌دهی می‌باشند. پایش دسترسی به داده شامل عملکردهای نظارت بر سیستم‌های مدیریت دسترسی پایگاه‌داده (DBMSs)، و ادغام با نظارت بر یکپارچگی فایل (FIM) و جلوگیری از، از دست رفتن داده (DLP) می‌شود. پایش DBMS می‌تواند سه شکل داشته باشد: تجزیه و تحلیل لاگ‌های ممیزی DBMS، ادغام با عملکردهای پایش فعالیت‌های پایگاه‌داده (DAM) شخص ثالث یا عملکردهای جاسازی‌شده DAM. FIM می‌تواند توسط محصولات SIEM به‌صورت مستقیم یا از طریق ادغام با محصولات شخص ثالث ارائه شود.

۲-۳-۱-۱۱ نظارت بر برنامه کاربردی

توانایی تجزیه و تحلیل جریان فعالیت‌های برنامه‌های کاربردی بسته‌بندی شده، امکان پایش لایه کاربرد را برای آن مؤلفه ها فراهم می‌کند، و توانایی شناسایی و تجزیه و تحلیل جریان فعالیت‌ها برای برنامه‌های کاربردی سفارشی، امکان پایش لایه کاربرد را برای برنامه‌های توسعه یافته در درون سازمان فراهم می‌کند. ادغام با برنامه های بسته‌بندی‌شده یک واسط که اجازه می‌دهد مشتری‌ها فرمت‌های لاگ را برای منابع رویدادی که پشتیبانی نمی‌شوند تعریف کنند، و شامل اطلاعات زمینه‌ای کاربر و برنامه کاربردی قابلیت‌های مهمی هستند که پایش فعالیت‌های کاربردی را برای تشخیص حملات لایه کاربرد، تشخیص تقلب، و گزارش سازگاری فراهم می کنند.

۲-۳-۱-۱۲ سادگی پشتیبانی و توسعه

سادگی پشتیبانی و توسعه، از طریق ترکیبی از دانش جاسازی‌شده موارد کاربرد SIEM و یک طرح عمومی که کارهای توسعه و پشتیبانی را به حداقل می‌رساند، به‌دست می‌آید. دانش جاسازی‌شده به‌وسیله دیدهای داشبورد از پیش تعریف‌شده، گزارش‌های کارهای نظارتی خاص و نیازمندی‌های قانونی، کتابخانه‌ای از قوانین همبسته

سازی برای سناریوهای پایش و فیلترهای رویداد برای منابع مشترک، به‌دست می‌آید. همچنین باید روشی ساده برای تغییر عملکردهای پیش‌فرض برای این‌که نیازمندیهای خاص یک سازمان را تأمین کند، وجود داشته باشد.

۲-۳-۲ ارزیابی محصولات SIEM

مؤسسه گارتنر بر اساس معیارهای فوق محصولات SIEM متنوع را ارزیابی می‌کند، نتایج این ارزیابی برای سه سال اخیر و رتبه‌بندی محصولات SIEM به ترتیب در شکل‌های ٤ تا ٦ نمایش داده شده است.

شکل ٤: رتبه‌بندی محصولات SIEM در سال ۲۰۱٦

شکل ۵: رتبه‌بندی محصولات SIEM در سال ۲۰۱۵

شکل ٦: رتبه‌بندی محصولات SIEM در سال ۲۰۱٤

همان‌طور که ملاحظه کردید محصول ArcSight در سه سال اخیر به‌عنوان Leader معرفی شده است و در جایگاه اول تا سوم در میان SIEMهای مورد ارزیابی قرار گرفته است. در ادامه قابلیت‌های این محصول را معرفی می‌کنیم.

۳ معرفی سامانه ArcSight

ESM، مدیریت امنیتی سازمانی جامع، بررسی[۳۵] و تحلیل پیشرفته، گزینه‌هایی برای اصلاح، و راه‌حل‌های گسترش‌یافته را ارائه می‌کند که بلافاصله پس از بیرون آوردن دستگاه از جعبه قابل پیکربندی و استفاده است. ESM، داده‌های سراسر شبکه سازمانی را نرمال‌سازی و تجمیع[۳۶] می‌کند، ابزارهایی برای تجزیه و تحلیل و بررسی پیشرفته ارائه می‌دهد، و گزینه‌هایی برای اصلاح[۳۷] خودکار و با چارچوب کاری مدیریت شده پیشنهاد می‌دهد. ESM، دید جامعی از وضعیت امنیتی تمام سیستم‌های مرتبط با فناوری اطلاعات ارائه می‌دهد و امنیت را درون چارچوب‌ها و فرآیندهای مدیریتی موجود یکپارچه می‌کند.

۳-۱ قابلیت‌های ESM

ESM قابلیت‌های زیر را ارائه می‌دهد:

۳-۱-۱ آگاهی وضعیتی[۳۸]

ESM میلیون‌ها رویداد از هزاران دارایی در سراسر شبکه را جمع‌آوری، نرمال، تجمیع، و فیلتر می‌کند و به جریان قابل مدیریتی که بر اساس ریسک، آسیب‌پذیری، و میزان اهمیت دارایی اولویت‌دهی می‌شود، تبدیل می‌کند. این رویدادهای اولیت‌دهی شده سپس می‌توانند توسط ابزارهای ESM همبسته شوند، مورد بررسی و

[۳۵] Investigation
[۳۶] Aggregate
[۳۷] Remediation
[۳۸] Situational Awareness

تحقیق قرار گیرند، تجزیه و تحلیل و اصلاح شوند، و آگاهی وضعیتی و زمان واکنش رخداد بی‌درنگ را ارائه می‌کنند.

۳-۱-۲ همبسته‌سازی

فعالیت‌های جالب توجه زیادی توسط بیش از یک رویداد نمایش داده می‌شوند. همبسته‌سازی فرآیندی است که رابطه بین رویدادها را کشف می‌کند، میزان اهمیت این روابط را استنباط می‌کند، آن‌ها را اولویت‌دهی کرده، سپس چارچوبی برای ردیابی آن‌ها ارائه می‌دهد.

۳-۱-۳ نظارت

رویدادها برای مشخص کردن بحرانی‌ترین و خطرناک‌ترین آن‌ها، پردازش و همبسته‌سازی می‌شوند. ESM ابزارهای انعطاف‌پذیر نظارتی را ارائه می‌دهد که شما را قادر می‌سازند تا تهدیدات بالقوه را، پیش از آن‌که بتوانند به شبکه آسیب برسانند، بررسی و اصلاح کنید.

۳-۱-٤ چارچوب

چارچوب گردش کار یک ساختار قابل سفارشی‌سازی از سطوح تخصیص ارائه می‌دهد تا اطمینان حاصل کند که رویدادها به افراد مناسب و در بازه زمانی مناسب تخصیص داده می‌شوند. این امر اعضای تیم شما را قادر می‌سازد تا به‌سرعت تحقیق و بررسی را انجام داده، تصمیمات گرفته شده را اطلاع دهند، و اقدامات مناسب را در زمان صحیح آن انجام دهند.

۳-۱-۵ تحلیل

هنگامی که رویدادهایی که نیاز به تحقیق و بررسی دارند به وقوع بپیوندند، ESM آرایه‌ای از ابزارهای تحقیق و بررسی را فراهم می‌کند. این ابزارها، افراد تیم را قادر می‌سازند تا برای کشف جزئیات و اتصالات آن در یک رویداد عمیق شوند، و عملکردهایی مانند NSlookup، Ping، PortInfo، Traceroute، Websearch و Whois را اجرا کنند.

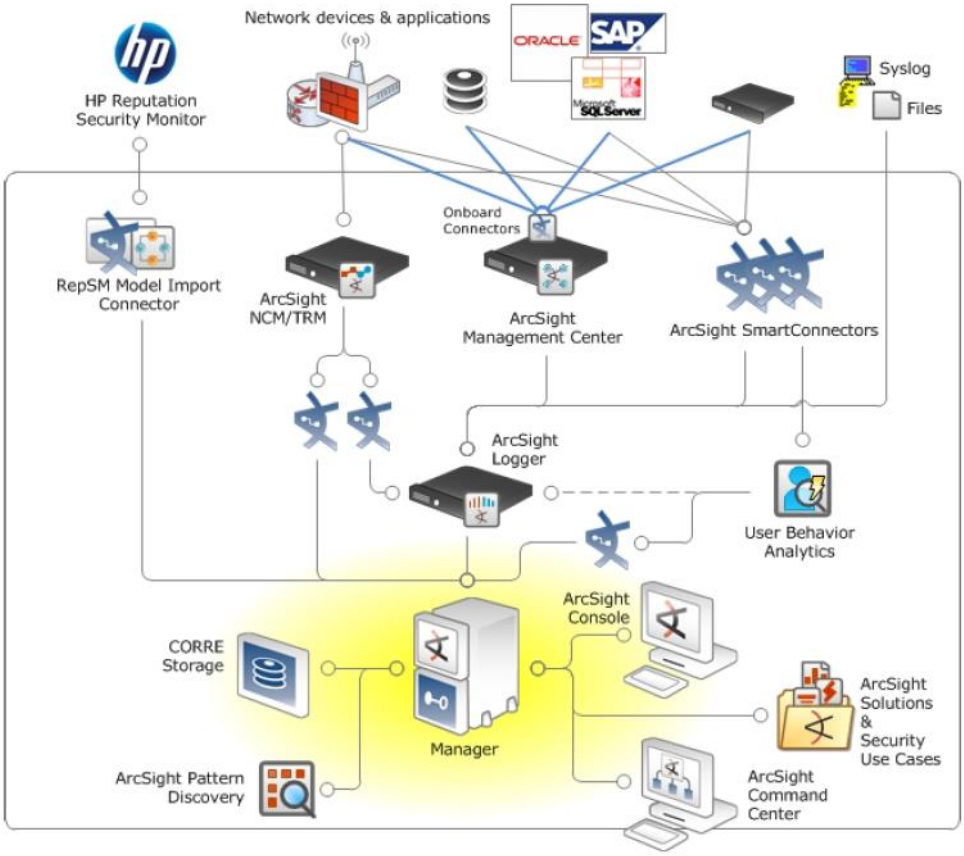
۳-۱-۶ گزارش‌دهی

ارائه خلاصه‌ای از وضعیت امنیتی شبکه به ذی‌نفعان سلامت شبکه شامل مدیران فناوری اطلاعات و امنیت، مدیریت اجرایی، و ممیزی‌های قوانین، ضروری است. ابزارهای گزارش‌دهی ESM می‌توانند به‌صورت خودکار یا دستی در زمان‌بندی مشخصی مورد استفاده قرار گیرند و گزارش‌های چند عنصری را تولید کنند که روی موضوعات کوچک تمرکز کنند یا وضعیت کلی سیستم را گزارش دهند.

۳-۲ آناتومی ESM

ESM برای جمع‌آوری اطلاعات از شبکه، از SmartConnectorها استفاده می‌کند. SmartConnectorها داده-های رویداد دریافت شده از تجهیزات را به الگوی[۳۹] نرمال شده که برای همبسته‌سازی راحت‌تر است، ترجمه می‌کنند. Manager داده‌های رویداد را پردازش کرده و در CORR-Engine ذخیره می‌کند. کاربران بر رویدادها با استفاده از کنسول یا مرکز دستور ArcSight نظارت می‌کنند، و به این ترتیب می‌توانند گزارش‌ها را تولید کرده، منابع را توسعه دهند، و مدیریت سیستم و تحقیق و بررسی را انجام دهند. معماری پایه‌ای ESM چارچوبی برای بیشتر محصولات ArcSight ایجاد می‌کند تا جریان رویداد را مدیریت کند، تحلیل رویداد را تسهیل کند و هشدارهای امنیتی و واکنش به رخداد را ارائه دهد. این معماری در شکل ۷ نمایش داده شده است. در ادامه مؤلفه‌های آن را تشریح می‌کنیم.

[۳۹] Schema



شکل ۷: معماری مؤلفه‌های زیرساخت ArcSight

۳-۲-۱ SmartConnector

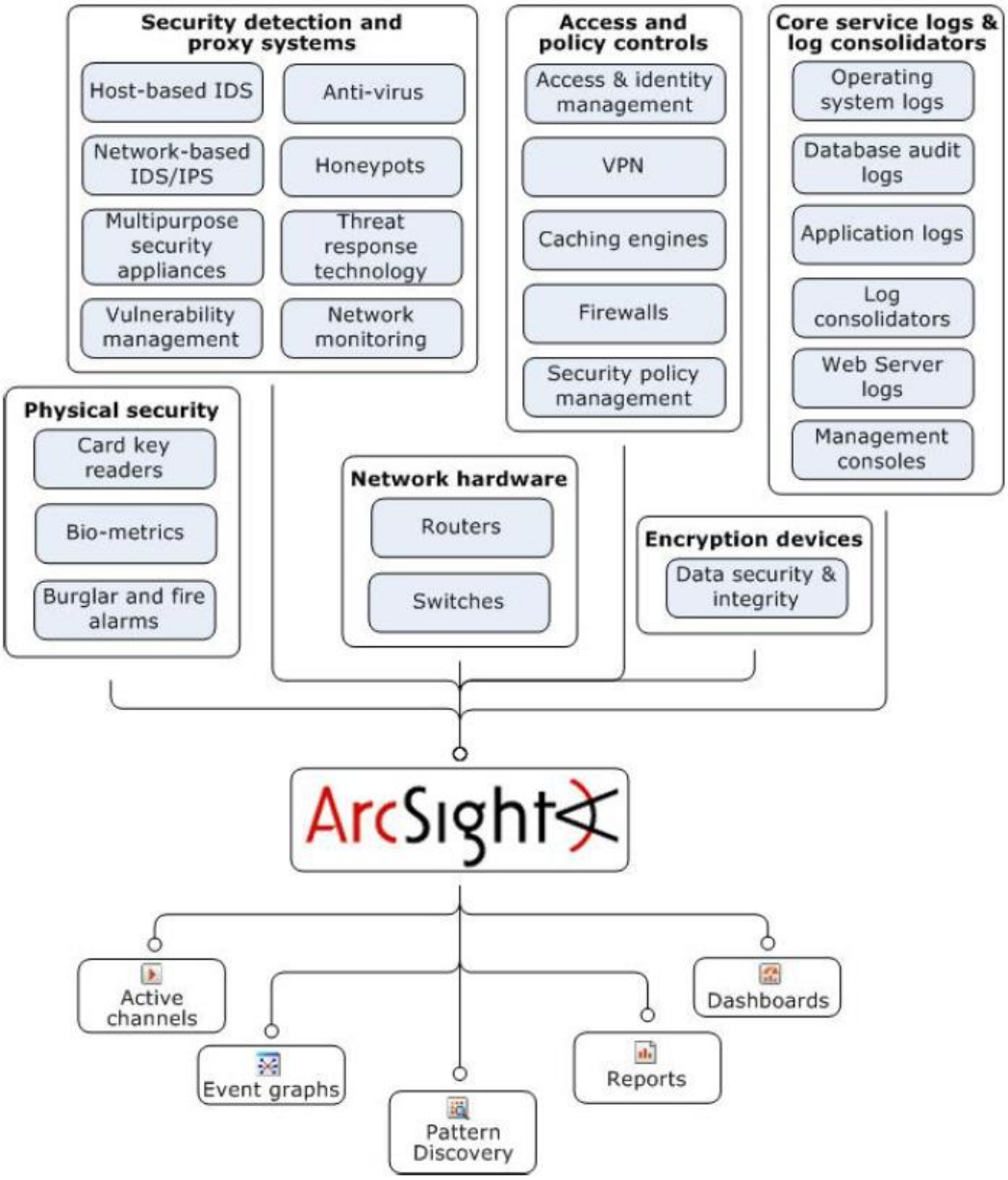
SmartConnectorها واسطی برای ارتباط با تجهیزات شبکه هستند که داده‌های مرتبط با همبسته‌سازی را تولید می‌کنند. پس از جمع‌آوری داده‌ها از تجهیزات شبکه، آن‌ها را به دو شکل نرمال‌سازی می‌کنند: نرمال‌سازی مقدار (مانند شدت، اولویت، و زمان) به یک قالب مشترک و نرمال‌سازی ساختار داده به یک الگوی مشترک. SmartConnectorها می‌توانند رویدادها را فیلتر و تجمیع کنند تا حجم رویدادهای ارسالی به Manager را کاهش، کارایی و دقت ESM را افزایش، و زمان پردازش رویداد را کاهش دهند. امکان اجرای دستورات را روی میزبان‌ها فراهم می‌کنند مانند ارسال دستورالعمل به پویش‌گر آسیب‌پذیری برای اجرای یک پویش. SmartConnectorها اطلاعاتی مانند جستجوی IP و یا نام میزبان را به داده‌هایی که جمع‌آوری می‌کنند، اضافه می‌کنند. SmartConnectorها عملکردهای زیر را اجرا می‌کنند:

- تمام داده‌هایی که از یک تجهیز مبدأ نیاز دارید را جمع‌آوری می‌کنند، بنابراین هنگام ممیزی یا تحقیق و بررسی نیاز نیست به تجهیز مراجعه کنید.
- صرفه‌جویی در پهنای باند شبکه و فضای ذخیره‌سازی با فیلتر کردن داده‌هایی که می‌دانید به تحلیل آن‌ها نیازی ندارید.
- تجزیه و تحلیل هر رویداد و نرمال‌سازی آن به یک الگوی (قالب) مشترک برای استفاده در ESM.
- تجمیع رویدادها برای کاهش تعداد رویدادهایی که به سمت Manager ارسال می‌شوند.
- طبقه‌بندی رویدادها با استفاده از یک قالب مشترک و قابل خواندن توسط انسان. این امر باعث می شود دیگر ضرورتی نداشته باشد که شما متخصص خواندن تمام قالب‌های لاگ‌هایی که توسط تجهیزات شبکه تولید می‌شوند باشید. استفاده از این طبقه‌بندی‌ها ایجاد فیلتر، قانون، گزارش، و ناظر داده[٤٠] را راحت‌تر می‌کند.
- ارسال رویدادها به Manager پس از این‌که پردازش شدند.
- بسته به تجهیز شبکه، برخی SmartConnectorها می‌توانند به تجهیز دستور اجرای دستورالعمل‌هایی را بدهند. این اقدامات می‌توانند به‌صورت دستی یا از طریق اقدامات خودکار از قوانین و برخی ناظرین داده اجرا شوند.

۳-۲-۲ منابع داده پشتیبانی شده

ESM خروجی منابع داده‌ای مانند گره‌های شبکه، سیستم‌های تشخیص و جلوگیری از نفوذ، ابزارهای ارزیابی آسیب‌پذیری، دیواره‌های آتش، ابزارهای ضد هرزنامه و ضد بدافزار، ابزارهای رمزنگاری، لاگ‌های ممیزی برنامه‌های کاربردی، و ابزارهای امنیت فیزیکی، را جمع‌آوری می‌کند. شکل ۸ منابع داده‌ای را که ESM پشتیبانی می‌کند و روشی که می‌توانید آن‌ها را تجزیه و تحلیل کنید، را نمایش می‌دهد.

[٤٠] Data Monitor



شکل ۸: منابع داده پشتیبانی‌شده

SmartConnectorها می‌توانند به‌صورت مستقیم روی تجهیزات یا روی کارگزار مشخصی که به‌منظور جمع آوری لاگ‌ها درنظرگرفته شده است، نصب شوند.

۳-۲-۳ FlexConnector

چارچوب FlexConnector یک کیت توسعه نرم‌افزار (SDK) است که شما را قادر می‌سازد که برای گره‌های شبکه‌ای که SmartConnectorای برای آن‌ها وجود ندارد، SmartConnector خود را ایجاد کنید. انواع FlexConnector شامل خواننده فایل، خواننده فایل عبارت منظم[۴۱]، خواننده پایگاه‌داده مبتنی بر زمان، خواننده های Syslog و SNMP، می‌باشند.

۴-۲-۳ Forwarding Connector

Forwarding Connector هشدارها را بین چندین Manager در یک ساختار توسعه سلسله‌مراتبی ESM و/یا توسعه یک یا چند Logger ارسال می‌کند.

۵-۲-۳ ArcSight Manager

این بخش قلب راه‌حل است. یک کارگزار مبتنی بر جاوا است که در آن تجزیه و تحلیل، گردش‌کار، و خدمات در حال اجرا است. همچنین خروجی طیف وسیعی از ابزارهای امنیتی را با یکدیگر همبسته می‌کند. Manager رویدادها را همان‌طور که به سیستم وارد می‌شوند در CORR-Engine ذخیره می‌کند. به‌صورت همزمان آن‌ها را در موتور همبسته‌سازی همبسته می‌کند، که هر رویداد را با مدل شبکه و اطلاعات آسیب‌پذیری برای تهیه خلاصه تهدید زمان‌واقعی می‌سنجد. ESM همراه با پیکربندی‌های پیش‌فرض و موارد کاربرد پایه‌ای استاندارد شامل فیلترها، قوانین، گزارش‌ها، ناظران داده، داشبوردها، و مدل‌های شبکه ارائه می‌شود که منجر به این می‌گردد که پس از نصب استفاده از آن راحت باشد. شما می‌توانید کل فرآیندی که Manager اجرا می‌کند، تشخیص، همبسته‌سازی و تخصیص، را طراحی کنید.

[۴۱] Regular Expression

۳-۲-۶ ذخیره‌ساز CORR-Engine[۴۲]

موتور همبسته‌سازی، بهینه‌سازی، حفظ، و بازسازی، یک چارچوب ذخیره و بازیابی اختصاصی است که رویدادها را در نرخ‌های بالا دریافت و پردازش می‌کند و جستجوهای با سرعت بالا را انجام می‌دهد.

۳-۲-۷ واسط‌های کاربری

ESM واسط‌های زیر را، بسته به نقش شما و وظایفی که باید انجام دهید، ارائه می‌دهد:

- مرکز دستور ArcSight[۴۳]

  واسط کاربری تحت وب است که امکان انجام برخی عملکردها را فراهم کرده است

- کنسول ArcSight

  واسط کاربری مبتنی بر ایستگاه کاری است که دسترسی کاملی به ESM را فراهم می‌کند.

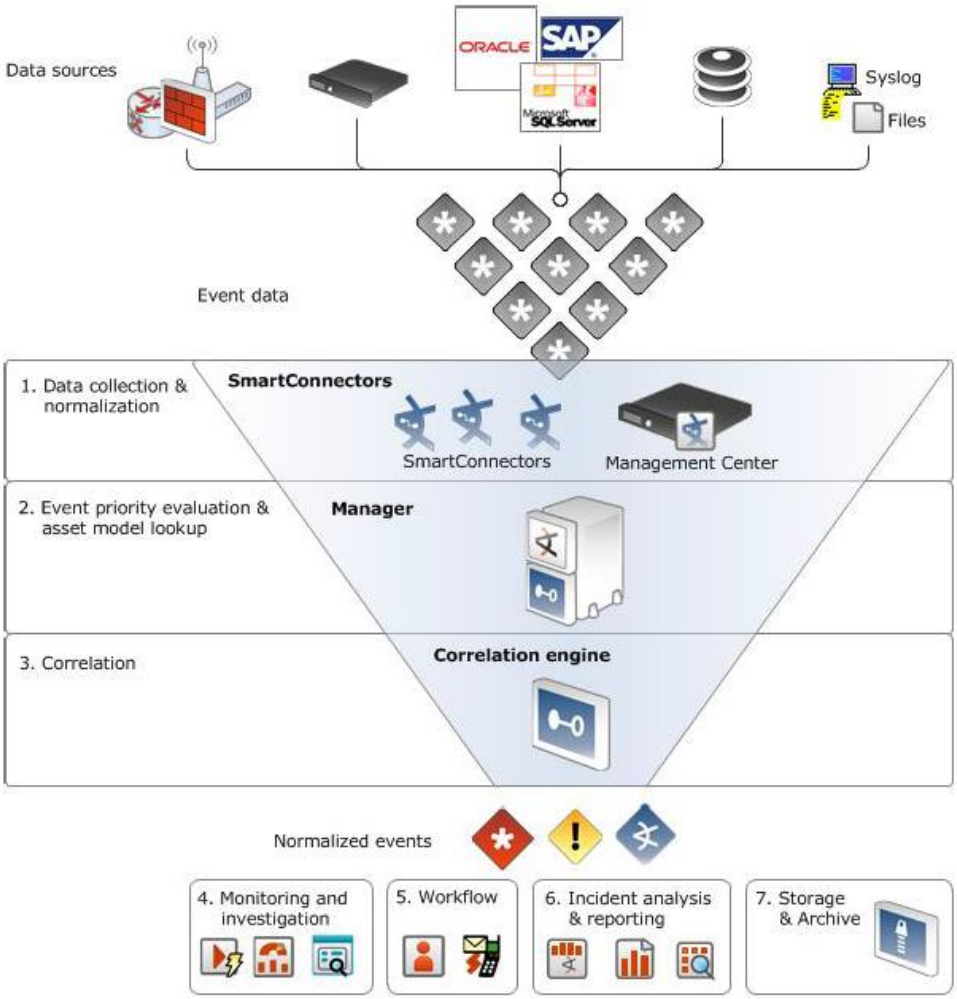
۳-۳ چرخه حیات رویدادها در ESM

در این بخش، چرخه حیات رویدادها در ESM شرح داده می‌شود. رویدادها از ابتدای ورود به زیرساخت ArcSight، دچار تغییراتی شده یا اقداماتی روی آن‌ها صورت می‌گیرد. ESM رویدادها را در مرحله‌هایی برای شناسایی و اقدام روی رویدادهای دارای اهمیت برای سازمان، پردازش می‌کند. شکل ۹ نمای کلی از گام‌های اصلی چرخه حیات یک رویداد را نمایش می‌دهد.

---

[۴۲] Correlation Optimized Retention and Retrieval

[۴۳] Command Center



شکل ۹: چرخه حیات یک رویداد

- منابع داده هزاران رویداد را تولید می‌کنند.
- SmartConnectorها آن‌ها را به قالب رویداد ESM تجزیه[۴۴] می‌کنند.
- در هر مرحله با اعمالی که انجام می‌شود، روی رویدادهایی که برای سازمان اهمیت بیشتری دارند تمرکز می‌شود. هنگامی که جریان رویدادهایی که برای سازمان اهمیت دارند استخراج شد ESM

[۴۴] Parse

ابزارهایی را برای پایش و تحقیق و بررسی رویدادها، ردیابی، تجزیه و تحلیل، و گزارش‌گیری از رویدادها فراهم می‌کند.

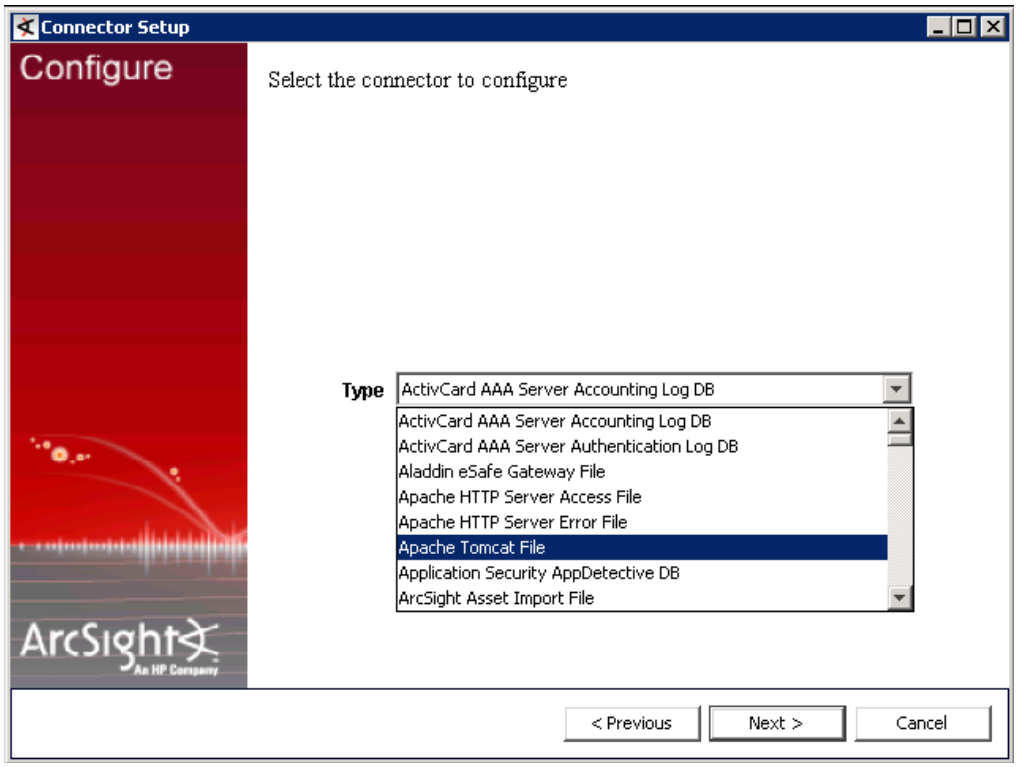
- داده‌های رویداد مطابق با سیاست‌هایی که در طول پیکربندی تنظیم شده‌اند ذخیره و آرشیو می‌شوند.

۳-٤ معرفی قابلیت‌های فنی محصول

محصول ESM با فرآهم آوردن راه‌حل یکپارچه‌ای به مدیریت امنیت و نظارت وضعیت امنیتی در شبکه می پردازند. برای نظارت و مدیریت بهینه و مناسب امنیت شبکه، این محصول عملکردهای مختلف و متنوعی را گردآوری کرده است که در ادامه به معرفی آن‌ها می‌پردازیم.

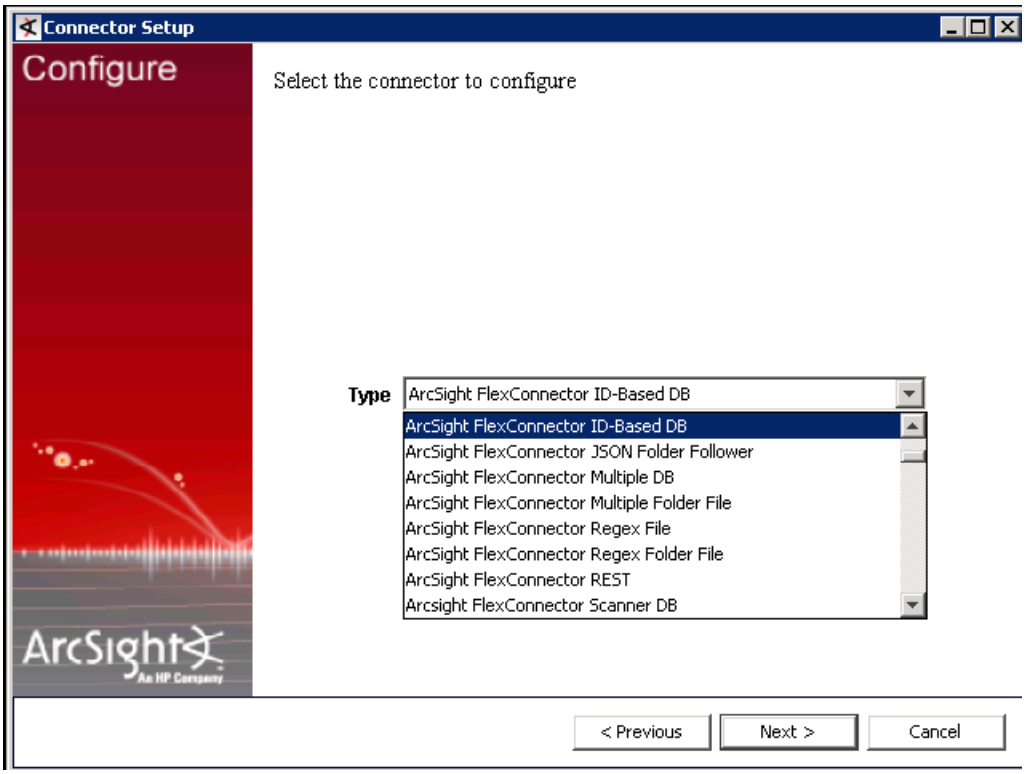
۳-٤-۱ جمع‌آوری طیف وسیعی از داده‌های مرتبط با رویداد و پردازش

ESM می‌تواند از طیف وسیعی از منابع داده با استفاده از SmartConnector یا FlexConnector، داده‌های مرتبط با رویداد را دریافت کند. به‌صورت پیش‌فرض می‌تواند از طیف گسترده‌ای از منابع داده با انتخاب محصول (مانند آنچه در شکل ۱۰ نمایش داده شده است) و انجام پیکربندی مورد نیاز با استفاده از SmartConnector، داده‌های مرتبط با رویداد را دریافت کند.



شکل ۱۰: انتخاب نوع منبع داده از SmartConnector

در صورتی که برای منبع داده‌ای SmartConnector وجود نداشته باشد، با استفاده از FlexConnector و انتخاب نوع و انجام پیکربندی، امکان سفارشی‌سازی و دریافت داده‌ها فراهم شده است (شکل ۱۱). این امر نشان‌دهنده قابلیت انعطاف و توسعه پذیری محصول است. بدین ترتیب امکان دریافت رویدادهای محصولات بومی نیز وجود دارد.



شکل ۱۱: انتخاب نوع منبع داده برای توسعه FlexConnector

پس از جمع‌آوری، داده‌های رویداد به لحاظ الگو و مقادیر نرمال‌سازی می‌شوند. سپس بر اساس فیلدهای رویداد طبقه‌بندی شده و با استفاده از مدل شبکه تعریف شده ناحیه[۴۵] و نام آن، جستجو می‌شوند. رویدادهای دریافتی بر اساس فیلترهای نوشته شده، فیلتر شده و تنها رویدادهایی که از نظر سیاست‌های امنیتی سازمان دارای اهمیت هستند، دریافت می‌شوند. سپس رویدادهای دریافت شده بر اساس قوانینی که پیشتر توسط مدیر نوشته شده‌اند با یکدیگر تجمیع شده و بدین ترتیب تعداد رویدادها به‌صورت بهینه و به مقدار قابل توجهی کاهش پیدا می‌کند. هشدارهای کاهش داده شده به سمت Manager ارسال می‌شوند.

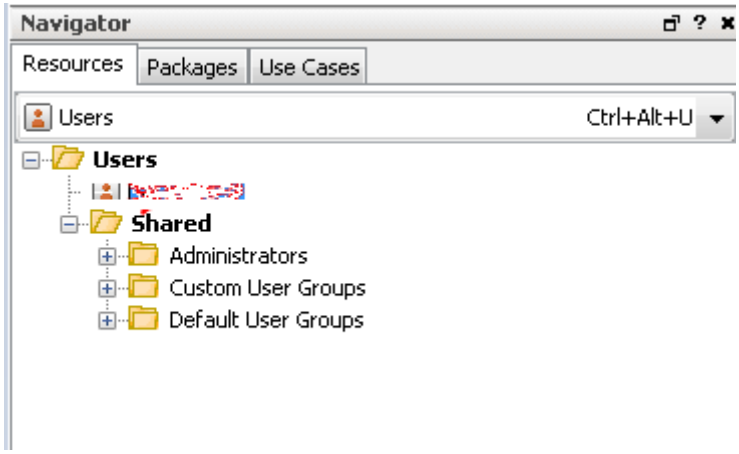
[۴۵] Zone

۳-٤-۲ مدیریت کاربران

ESM کاربران را در گروه‌های متنوعی بر اساس نقش و مجوزی که قرار است داشته باشند، گروه‌بندی می‌کند. سه نوع کاربر در ESM قابل تعریف است (شکل ۱۲).

- Administrators: تمام امتیازات و مجوزها را دارد.
- Custom User Groups: کمترین امتیازات و مجوزها را دارد.
- Default User Groups: به زیر نقش‌هایی در SOC تقسیم می‌شود. این زیرنقش‌ها عبارتند از:
  - Analyzer administrators
  - Operators
  - Operators/Analyst

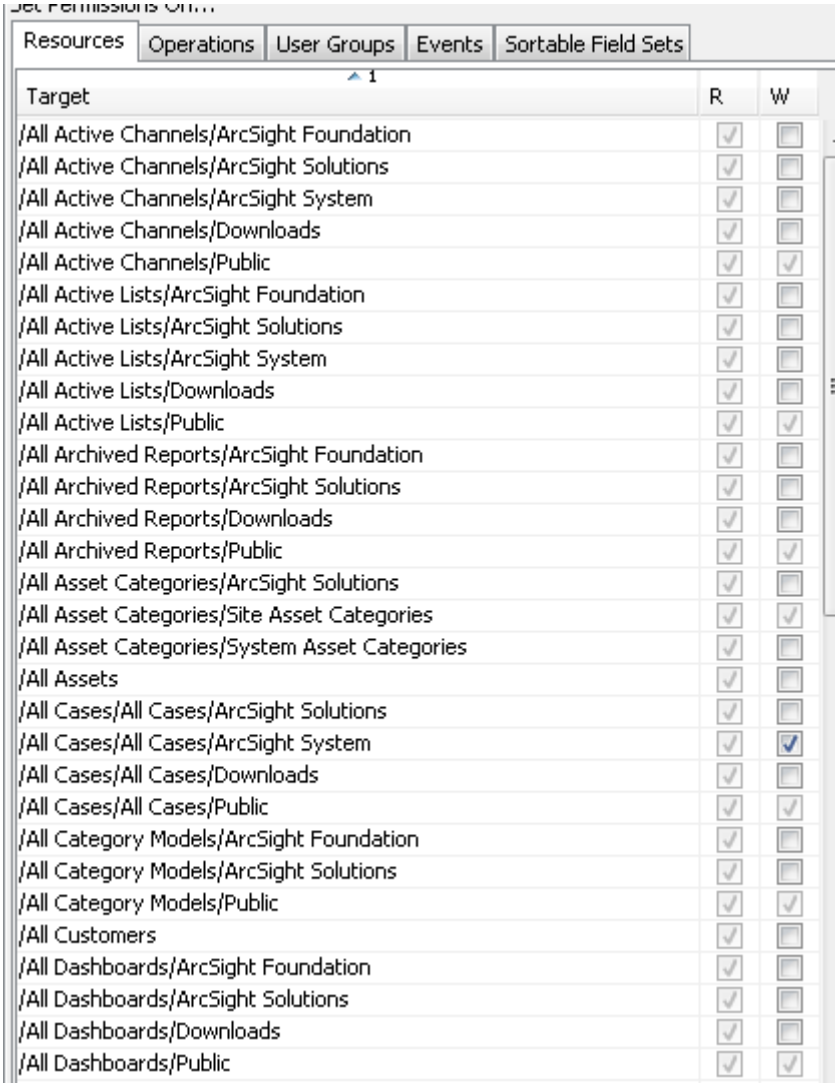
ESM امکان مدیریت کاربران (ایجاد، فعال‌سازی، اعطای مجوز، پاک‌کردن، و غیره) را فراهم کرده است.



شکل ۱۲: انواع کاربرانی که قابل تعریف هستند

۳-٤-۳ مدیریت مجوزها

ESM امکان تعریف مجوزهای مختلف را با تعریف ACLها فراهم کرده است. می‌توان برای هر گروه از کاربران مجوزهای مختلفی را تنظیم کرد. همان‌طور که در شکل ۱۳ نمایش داده شده است، امکان تعریف مجوز روی منابع، عملیات، گروه‌های کاربران، رویدادها، و فیلدهای داده وجود دارد.



شکل ۱۳: مجوزهای قابل اعمال به منابع مختلف

۳-٤-٤ مدیریت اخطارها

با پیکربندی قوانین همبسته‌سازی امکان تولید اخطار به عنوان واکنش به یک قانون خاص وجود دارد. به این ترتیب می‌توان برای قوانینی که اهمیت خاصی برای سازمان دارند، تولید اخطار را تنظیم کرد، تا هنگام وقوع این دسته از حملات به‌صورت ویژه کاربران SOC از حملات آگاه شوند. انواع دسته‌های اخطار در شکل ١٤ نمایش داده شده است.

شکل ١٤: انواع دسته‌های اخطار

هر اخطار دارای ۵ فیلد داده است که میزان اهمیت و دلیل تولید آن را نمایش می‌دهد. از جمله این فیلدها می‌توان به اولویت، رویدادی که منجر به تولید اخطار شده، سطح ارتقا، و زمان تولید، اشاره کرد.

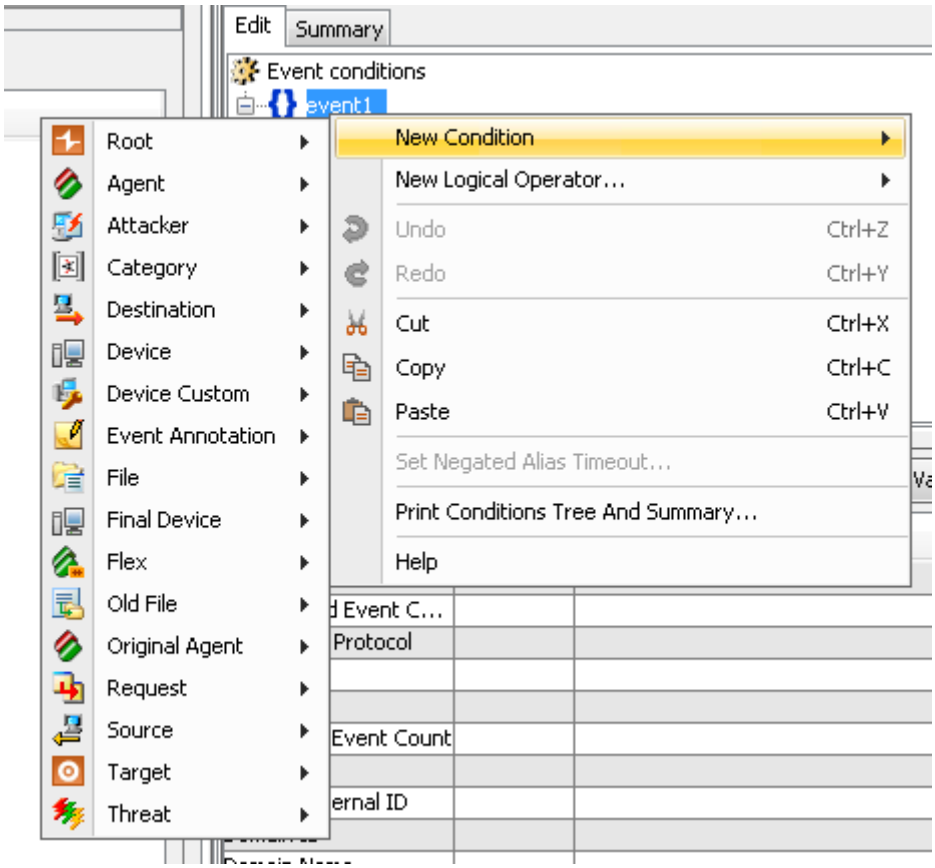
٣-٤-٥ نظارت بر رویدادها

امکان پایش رویدادهایی که از SmartConnector می‌آیند با استفاده از ابزارهای متنوعی که در ESM وجود دارد فراهم شده است. می‌توان از طریق مجموعه غنی از Viewها شامل کانال فعال[٤٦] و Grid، داشبورد و جدول‌ها، و لیست‌های فعال رویدادها را پایش کرد.

٣-٤-٦ فیلترکردن رویدادها

امکان سفارشی‌سازی دریافت رویدادها از منابع داده با تعریف فیلترها وجود دارد. با تعریف فیلترهایی که روی فیلدهای مختلف رویدادهای دریافتی از منابع داده، شرایطی را (همان‌طور که در شکل ۱۵ نمایش داده شده است) اعمال می‌کنند، این امکان فراهم شده است. به این ترتیب SmartConnectorها تنها رویداهایی که به لحاظ سیاست امنیتی سازمان دارای اهمیت هستند را دریافت و به سمت Manager ارسال می‌کنند.

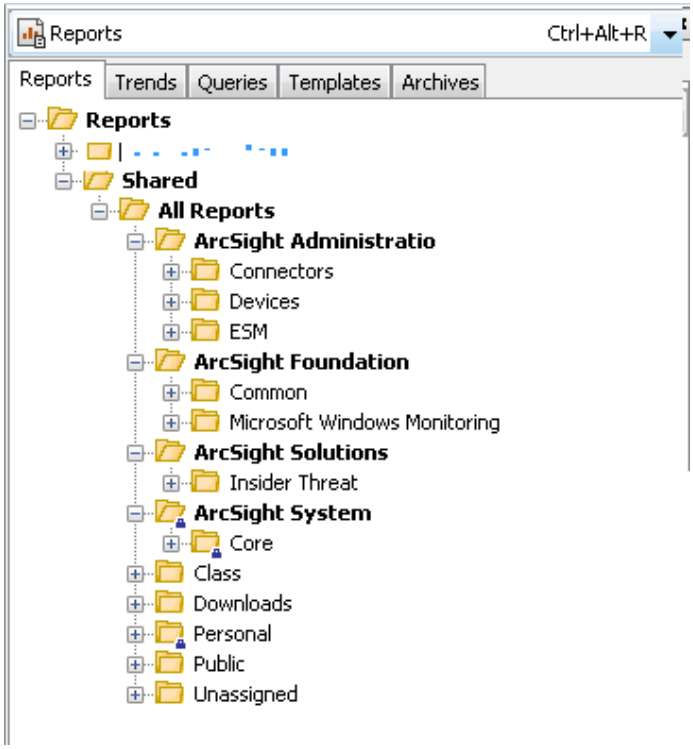
[٤٦] Active Channel



شکل ۱۵: تعریف شرایط برای فیلترها

۳-٤-۷ ایجاد گزارش

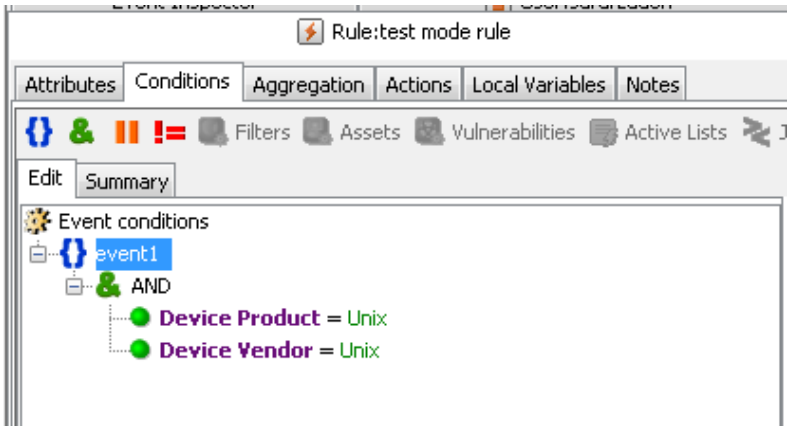
ESM به‌صورت پیش‌فرض قالب‌هایی برای تهیه و ارائه گزارش دارد (شکل ١٦). در هر دسته گزارش‌هایی قرار دارد. امکان تعریف قالب‌های گزارش‌گیری جدید نیز وجود دارد. با توجه به این قابلیت امکان تعریف قالب‌های گزارش‌گیری برای بررسی مطابقت پیکربندی و تجهیزات به‌کار رفته در سازمان با استانداردهایی مانند ISO 270002، PCIDSS، و غیره وجود دارد.



شکل ١٦: گزارش‌های پیش‌فرض

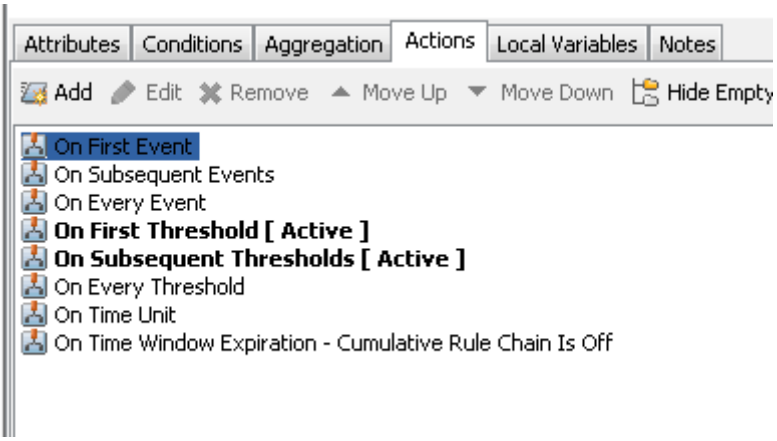
٣-٤-٨ همبسته‌سازی

روش همبسته‌سازی ESM بر اساس قانون است. همان‌طور که در شکل ١٧ نمایش داده شده است، برای تعریف هر قانون ابتدا نام و مشخصات آن را وارد کرده، سپس شرایطی که قانون در صورت مشاهده آن شرایط باید فعال شود را در بخش Condition وارد کرده، در ادامه شرایط تجمیع هشدارها را در پنجره زمانی مشخصی تعیین کرده، و در بخش Action نیز واکنشی که هنگام مواجه با حمله باید صورت گیرد را معین می‌کنیم.



شکل ۱۷: یک نمونه قانون

واکنش‌هایی که ESM می‌تواند انجام دهد در شکل ۱۸ نمایش داده شده است.



شکل ۱۸: واکنش‌های قابل انجام توسط ESM

امکان تعریف سه نوع قانون در ESM وجود دارد.

- قوانین استاندارد[٤٧]: کامل‌ترین نوع قانون است. امکان ایجاد قانون دارای چندین شرط، تجمیع فیلدهای داده، و انجام واکنش روی شرایط مختلف را دارد.

[٤٧] Standard rules

- قوانین سبک‌وزن[۴۸]: به منظور سرعت و سادگی از این نوع قانون استفاده می‌شود. تنها یک شرط را می‌توان برای آن تعریف کرد. نمی‌تواند فیلدهای داده را تجمیع کند. تنها یک نوع واکنش از مجموعه واکنش‌های شکل ۱۸ را می‌توان برای آن تعریف کرد. قبل از قوانین استاندارد اعمال می‌شود.
- قوانین پیش‌پا افتاده[۴۹]: برای تحلیل مقدماتی می‌توان از آن استفاده کرد. تنها یک شرط را می‌توان برای آن تعریف کرد. قبل از قوانین سبک‌وزن و استاندارد اعمال می‌شود. نمی‌تواند رویداد همبسته‌سازی تولید کند.

یکی از مزایایی که ESM در همبسته‌سازی دارد امکان تعریف قوانین همبسته‌سازی با مقایسه محتویات رویداد دریافتی است.

۳-٤-۹ همبسته‌سازی هویت

امکان مدل‌کردن کاربران و برقراری ارتباط بین آن‌ها و رویدادها را فراهم می‌کند. همبسته‌سازی هویت می‌تواند در برخی سناریوها بر اساس لیست‌های نشست[۵۰] و در سناریوهای دیگر با استفاده از لیست‌های فعال[۵۱] انجام شود. امکان ذخیره و ثبت داده‌های وابسته به نشست در یک لیست نشست که بر اساس کاربر تعریف شده وجود دارد. این لیست می‌تواند برای اهدافی در شناسایی و ردیابی کاربران در ارتباط با آدرس‌های MAC، آدرس‌های IP، میزبان‌ها و ورود به شبکه مورد استفاده قرار گیرد.

۳-٤-۱۰ مدیریت موارد[۵۲]

هنگامی که رخدادی در شبکه به وقوع می‌پیوندد، ESM این امکان را به‌وجود آورده است تا برای ردیابی، یک مورد[۵۳] را برای آن ایجاد کنیم. از آنجایی‌که یک یا چند رویداد ممکن است با آن رخداد مرتبط باشد، امکان ضمیمه‌کردن رویداد به مورد وجود دارد. یک مورد شامل اطلاعاتی درباره یک رخداد است به همراه

---

[۴۸] Lightweight Rules
[۴۹] Pre-persistence rules
[۵۰] Session List
[۵۱] Active List
[۵۲] Case Management
[۵۳] Case

رویدادهایی که به آن ضمیمه شده است. از موارد برای ردیابی، تحقیق و بررسی، و ترجمه رویدادها استفاده می‌شود. موارد یک یا چندین رویداد را ردیابی کرده و داده‌های رویداد را به محصولات دیگر ارسال می‌کنند. موارد می‌توانند به‌صورت مجزا کار کنند یا با سیستم‌های مدیریت موارد دیگر یکپارچه شوند. امکان تخصیص نفرات بر اساس تخصصشان به موارد برای حل کردن آن‌ها وجود دارد. همچنین امکان تخصیص یک مورد به گروهی از کاربران وجود دارد. پس از تخصیص اعلانی مبنی بر دریافت یک مورد به آن کاربران ارسال می شود.