بسمه تعالی

معرفی، آموزش نصب و پیکربندی سامانه

HP Arcsight

(بخش دوم)

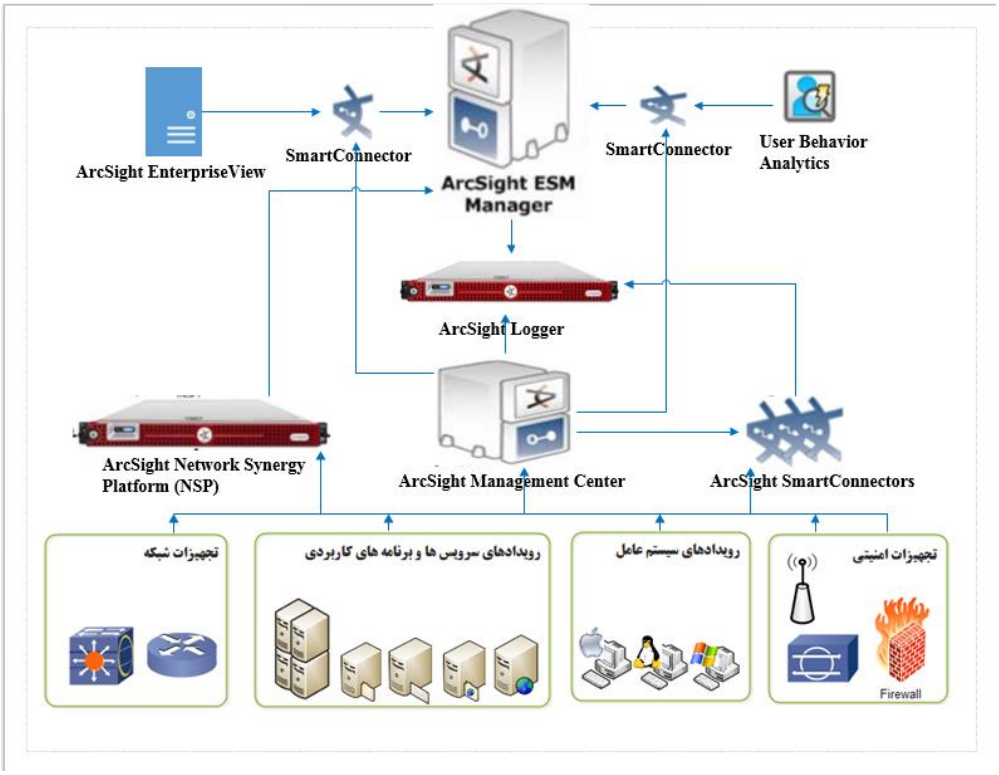
فهرست مطالب

1 مقدمه

برای برقراری امنیت و شناسایی حملات و مقابله با آن‌ها از ابزارهای مختلفی استفاده می‌شود. یکی از این ابزارها SIEM است که در مرکز عملیات امنیت مورد استفاده قرار می‌گیرد. تولیدکنندگان مختلف در سراسر جهان محصولات SIEM متنوعی را تولید کرده‌اند. یکی از این تولیدکنندگان ArcSight است که محصول ESM را در این حوزه ارائه کرده است. شرکت ArcSight علاوه بر ESM محصولات دیگری را نیز تولید کرده است که در حوزه SOC کاربرد دارند. در این سند معماری زیرساخت مرکز عملیات امنیت معرفی و محصول ESM و سایر محصولاتی که در این معماری مورد استفاده قرار می‌گیرند، و به تشخیص، تحلیل و مقابله با حملات کمک می‌کنند، معرفی و تشریح می‌شوند.

2 معرفی معماری ArcSight و اجزای آن

همان‌طور که در گزارش بخش نخست بیان شد، یک مرکز عملیات امنیت از سه بخش افراد، فرآیند و فناوری تشکیل می‌شود. برای ارائه قابلیت‌های مورد انتظار از مرکز عملیات امنیت در بخش فناوری، از تجهیزات مختلفی استفاده می‌شود. شرکت HP محصولات امنیتی متنوعی که در بخش تجهیزات در SOC قابل به‌کارگیری هستند را تولید می‌کند. این شرکت تمام خدماتی که باید یک مرکز عملیات امنیت ارائه کند را توسط یک محصول ارائه نکرده است. انواع محصولاتی که این شرکت برای استفاده در SOC ارائه کرده است در شکل 1 در قالب معماری زیرساخت مرکز عملیات امنیت نمایش داده شده‌است.



شکل 1 معماری زیرساخت مرکز عملیات امنیت

همان‌طور که در شکل 1 ملاحظه می‌شود، در معماری زیرساخت مرکز عملیات امنیت می‌توان از محصولات متنوعی بهره برد، که هر کدام از این محصولات بخشی از قابلیت‌هایی که مرکز عملیات امنیت ارائه می‌دهد را انجام می‌دهند. لیست محصولات مختلفی که در این شکل قرارگرفته‌اند، عبارتند از:

- HP SmartConnector
- HP ArcSight Management Center
- HP ArcSight Network Synergy Platform (NSP)
- HP ArcSight Logger
- HP ArcSight User Behavior Analytics
- HP EnterpriseView
- HP ArcSight ESM

به ابزارهایی که در زیرساخت مرکز عملیات امنیت ArcSight مورد استفاده قرار می‌گیرند، نقش‌های زیر را می‌توان تخصیص داد:

- تشخیص‌دهنده تهدید[1]: این دسته از ابزارها با پایش شبکه تهدیداتی که در آن رخ می‌دهد را شناسایی کرده و یک هشدار را تولید می‌کنند.

[1] Threat Detector

- جمع‌آوری‌کننده: از حس‌گرها[۲] ، اطلاعات ورودی (لاگ، هشدارهای امنیتی، داده‌های متنی، آسیب‌پذیری‌ها، اخبار بولتن‌های خبری و غیره) را دریافت و به تحلیل‌گرها ارسال می‌کند.
- تحلیل‌گر: با انجام پردازش‌های مختلف تحلیل‌هایی را روی داده‌های دریافتی انجام داده و متناسب با عملکردهای تعریف‌شده برای آن‌ها، خروجی را تولید می‌کند.
- ذخیره‌ساز: برای انجام تحلیل‌های تاریخچه‌ای، بررسی‌های قانونی که در آینده ممکن است ضروری باشد، و نیز نگهداری بلندمدت داده‌ها از ذخیره‌ساز استفاده می‌شود.
- ابزارهای واکنش و پاسخ: در صورت وقوع یک تهدید یا حمله در شبکه، ابزارهای واکنش و پاسخ دستورات یا اسکریپت‌هایی را روی سیستم‌های مورد استفاده در مرکز عملیات امنیت، اعمال می‌کنند.
- بصری‌ساز و ارائه‌دهنده گزارش و خروجی: واسط‌هایی که برای مشاهده نتایج تحلیل‌ها استفاده می‌شود.

هنگام معرفی هر محصول نقشی که آن محصول بر عهده دارد، معرفی می‌شود. از میان این ابزارها که در ادامه به اختصار معرفی شده‌اند، ESM، که به‌عنوان SIEM مورد استفاده قرار می‌گیرد، اهمیت بیشتری دارد و محور این گزارش، معرفی این محصول از شرکت ArcSight است. این محصول، خود نیز شامل مؤلفه‌هایی است که در ادامه به‌صورت مفصل تشریح می‌شوند.

در ادامه شرحی از محصولات مختلفی که در شکل 1 قرارگرفته‌اند، بیان می‌شود.

1-2 Smart Connectors

Smart Connector یک برنامه کاربردی است که رویدادهای خام و داده‌های متنی را از حس‌گرها جمع‌آوری کرده و آن‌ها را به رویدادهای امنیتی ArcSight، پردازش می‌کند و به ابزارهای مقصد انتقال می‌دهد. این ابزار نقش جمع‌آوری‌کننده را دارا است. Smart Connectorها واسطی بین Manager و حس‌گرها و ابزارهای شبکه‌ای هستند که داده‌های مرتبط با ESM را تولید می‌کنند. Smart Connectorها داده‌های رویداد را از حس‌گرهای شبکه جمع‌آوری کرده و به دو طریق آن‌ها را نرمال‌سازی می‌کنند. ابتدا مقادیر را (مانند شدت، اولویت و زمان) به یک قالب مشترک، نرمال می‌کنند. همچنین ساختار داده را به یک الگوی مشترک نرمال‌سازی می‌کنند. Smart Connectorها می‌توانند رویدادهایی را فیلتر و تجمیع کنند تا حجم هشدارهای ارسالی به Manager، Logger و سایر مقاصد را کاهش دهند، که این امر منجر به افزایش بهره‌وری و کاهش زمان پردازش هشدارها می‌شود.

وظایفی که Smart Connectorها بر عهده دارند به اختصار عبارتند از:

[2] Sensors

- تمام داده‌هایی را که از یک تجهیز مبدأ نیاز دارید را جمع‌آوری می‌کنند، بنابراین هنگام ممیزی یا تحقیق و بررسی نیازی به مراجعه به تجهیز نیست.
- صرفه‌جویی در پهنای باند شبکه و فضای ذخیره‌سازی با فیلترکردن داده‌هایی که می‌دانید به تحلیل آن‌ها نیازی ندارید.
- تجزیه و تحلیل هر رویداد و نرمال‌سازی آن به یک الگو (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 می‌شود که دیگر ضرورتی نداشته باشد که شما متخصص خواندن تمام قالب‌های لاگ‌هایی که توسط تجهیزات شبکه تولید می‌شوند باشید و استفاده از این طبقه‌بندی‌ها، ایجاد فیلتر، قانون، گزارش و ناظر داده[3] را ساده‌تر می‌کند.
- ارسال رویدادها به Manager پس از این‌که مورد پردازش قرار گرفتند.

2-2 ArcSight Management Center

ArcSight Management Center (ArcMC) یک مرکز مدیریت امنیت متمرکز است که امکان مدیریت متمرکز و یکپارچه راه‌حل‌های ArcSight مانند ArcSight Logger، SmartConnectors، FlexConnectors، Connector Appliance و ArcMCهای راه‌دور را از طریق یک واسط یکپارچه‌ی مدیریت، فراهم می‌کند و عملیات جمع‌آوری و مدیریت لاگ را به‌صورت خودکار انجام می‌دهد. این ابزار برای اعمال پیکربندی‌ها روی ابزارهای جمع‌آوری‌کننده و همچنین ذخیره‌ساز مورد استفاده قرار می‌گیرد. در واقع این ابزار یک راه‌حل سخت‌افزاری است که خدمات زیر را ارائه می‌دهد:

- مدیریت متمرکز راه‌حل ArcSight
- از اجرای عملیات به‌صورت حجمی روی تمام SmartConnectorها پشتیبانی می‌کند و برای محیط‌هایی با تعداد زیاد SmartConnector مناسب است.
- در محیط‌هایی که تنها از Logger استفاده می‌شود امکان مدیریت SmartConnectorها را فراهم کرده است.
- امکان به‌روزرسانی، بهینه‌سازی، پایش و پیکربندی SmartConnectorها را از طریق یک واسط به‌صورت متمرکز فراهم کرده است.

[3] Data Monitor

3-2 ArcSight Network Synergy Platform (NSP)

اغلب زیرساخت‌های شبکه شامل ابزارهایی از انواع مختلف فروشندگان هستند که هیچ روش متمرکزی برای مدیریت آن‌ها وجود ندارد. فناوری NSP به‌سادگی با زیرساخت شبکه موجود ادغام شده و امکان مدیریت اکثر ابزارهای شبکه‌ای که در زیرساخت‌های شبکه‌های امروزی وجود دارند، را فراهم می‌کند. NSP یک دستگاه است، یک سیستم کاملاً خودکار که از طریق SSH یا Telnet با ابزارهای شبکه ارتباط برقرار می‌کند. این دستگاه به‌صورت مستقیم با ابزارهای شبکه، به‌منظور ایجاد درکی از شبکه، ارتباط برقرار می‌کند. اطلاعاتی مانند نوع سیستم‌عامل و پیکربندی ابزارها را جمع‌آوری می‌کند. نقشی که این ابزار در شبکه بر عهده دارد در دسته واکنش و پاسخ قرار می‌گیرد.

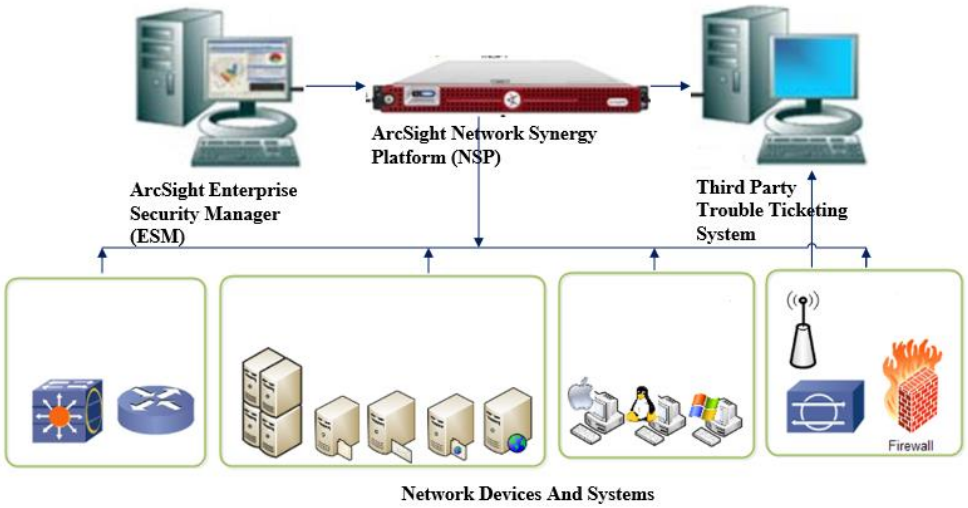
- کتابخانه‌ای از پیکربندی‌های ابزارها را ایجاد و نگهداری می‌کند، به‌این‌ترتیب امکان مقایسه میان پیکربندی‌ها با فشردن یک دکمه، بازگرداندن پیکربندی به هر یک از پیکربندی‌ها در کتابخانه پیکربندی ابزار و انجام سایر عملیات مدیریتی و گزارش‌گیری را فراهم می‌کند.
- به‌صورت متمرکز تغییرات پیکربندی یک ابزار یا گروهی از ابزارها را مدیریت می‌کند.
- تعریف ممیزی، برای اطمینان از این‌که فرآیند کنترل تغییر در شبکه هدف با استانداردهای شما مطابقت دارد.
- فیلترهای پروتکل را برای ممانعت از تلاش برای نفوذ اعمال می‌کند.
- تعیین موقعیت و قرنطینه فوری هر ابزاری که به شبکه متصل می‌شود.
- تعریف فیلتر و قوانین عملیات برای فعال‌سازی عملیات مبتنی بر نقش
- غیرفعال کردن حساب‌های کاربری افراد
- انسداد پروتکل‌های مشخص یا ممانعت از برقراری ارتباط برای محدوده‌ای از آدرس‌های IP مشخص

با استفاده از قابلیت‌هایی که NSP فراهم می‌کند، امکان انجام عملیات زیر به‌وجود می‌آید:

- پیکربندی NSP برای پاسخ خودکار به وقایع امنیتی
- گروه‌بندی ابزارها تا این‌که NSP بتواند آن‌ها را به‌صورت کارآمدتری مدیریت کند
- کنترل عملیاتی که مدیران سطوح پائین شبکه بتوانند در شبکه انجام دهند
- دریافت اخطار در صورتی‌که رویدادهای مورد نظر شما در شبکه رخ دهند

دستگاه NSP با ESM یکپارچه شده و به‌این‌ترتیب یک راه‌حل پاسخ امنیتی انتها به انتها ارائه می‌شود. هنگامی که ESM یک سیستم آلوده را تشخیص دهد، می‌تواند آدرس IP سیستم را به‌صورت خودکار به TRM ارسال کند، و به‌این‌ترتیب سیستم آلوده قرنطینه می‌شود. همچنین امکان ارسال پیغام‌های اخطار NSP به Logger وجود دارد.

در شکل 2 نحوه قرارگیری NSP در شبکه نمایش داده شده است.



شکل 2 نحوه قرارگیری NSP در معماری شبکه

NSP شامل دو مؤلفه نرم‌افزاری زیر است:

- مدیر پاسخ به تهدیدات[4]
- مدیر پیکربندی شبکه[5]

این دو مؤلفه نرم‌افزاری به‌صورت جداگانه به فروش می‌رسند و در صورت خریداری هر کدام یا هر دو، با استفاده از واسط گرافیکی امکان دسترسی به آن‌ها وجود دارد.

2-3-1 مدیر پاسخ به تهدیدات

مدیر پاسخ به تهدیدات، که پیش از این تحت عنوان Network Response Manager (NRM) شناخته می‌شد، امکان پاسخ‌گویی امن و سریع به وقایع امنیتی را فراهم می‌کند. امکان پیکربندی TRM برای پاسخ‌گویی خودکار به وقایع، یا امکان اجرای پاسخ به‌صورت دستی فراهم است.

با استفاده از TRM، هنگامی که یک حادثه گزارش می‌شود، یک مدیر TRM می‌تواند به‌سرعت موقعیت مکانی سیستم را شناسایی کند و آن را به یک VLAN مجزا منتقل کند و سیستم‌های آلوده را از دیگران جدا کند. پس از جدا شدن، سیستم را می‌توان قبل از حذف از قرنطینه، پاک‌سازی کرد. گروه شبکه نه تنها قادر به پاسخ سریع است، بلکه اقدامات انجام شده مانند افرادی که به این حادثه پاسخ دادند، دستگاه‌های شبکه‌ای که درگیر بودند و دستوراتی که اجرا شدند، به‌طور خودکار وارد سیستم می‌شوند و یک پیگیری حسابرسی ایجاد می‌کنند.

[4] Threat Response Manager (TRM)
[5] Network Configuration Manager (NCM)

با استفاده از TRM امکان انجام اقدامات مدیریتی زیر فراهم می‌شود:

- قرنطینه یک گره
- انسداد یک IP یا یک محدوده آدرس IP
- مسدودسازی ترافیک پروتکل مشخصی مانند ICMP یا ترافیک UDP
- غیرفعال‌سازی حساب‌های کاربری

2-3-2 مدیر پیکربندی تغییرات

NCM امکان مدیریت همه کارهای مرتبط با پیکربندی را در محدوده وسیعی از ابزارهای شبکه از یک مکان متمرکز فراهم می‌کند. امکان نگهداری چندین نسخه پیکربندی برای هر ابزار، مقایسه پیکربندی‌ها پیش از اعمال آن‌ها به ابزار، بازگشتن به یک پیکربندی مشخص، اجرای دستور روی ابزارهای شبکه و اعمال استانداردهای پیکربندی، فراهم شده است. NCM می‌تواند به‌صورت خودکار ابزارهای شبکه را کشف کرده و یا این‌که به‌صورت دستی با واردکردن آدرس IP آن‌ها را معرفی کند. NCM با برقراری ارتباط با تجهیز، پیکربندی ابزار را استخراج کرده و آن را به کتابخانه پیکربندی تجهیز اضافه می‌کند.

با استفاده از NCM امکان انجام اقدامات مدیریت پیکربندی زیر فراهم می‌شود:

- اجرای دستورات روی ابزارهای شبکه
- ارسال فایل‌های پیکربندی به ابزارهای شبکه
- بازگشت به پیکربندی قبلی
- به‌روزرسانی سیستم‌عامل ابزار شبکه
- ثبت نشست‌های دسترسی ترمینال
- ممیزی عملیات ابزار شبکه

4-2 ArcSight Logger

Logger یک راه‌حل مدیریت لاگ و ذخیره‌سازی داده‌های رویداد است، که به‌منظور توان عملیاتی بالا با دریافت حجم عظیمی از رویدادها، ذخیره‌سازی بلندمدت کارآمد، و تحلیل سریع داده، بهینه شده است. Logger رویدادها را دریافت و ذخیره می‌کند، از جستجو، بازیابی و گزارش‌گیری پشتیبانی می‌کند و می‌تواند به‌صورت انتخابی رویدادها را ارسال کند. رویدادهای امنیتی را به شکل فشرده شده ذخیره می‌کند و امکان بازیابی رویدادهای تغییرنیافته بر حسب تقاضا، برای تجزیه و تحلیل دادرسی تاریخچه‌ای داده، وجود دارد. Logger می‌تواند به‌صورت مجزا برای دریافت رویدادها از پیغام‌های Syslog یا فایل‌های لاگ، یا دریافت رویدادها به فرمت CEF از SmartConnector، توسعه یابد. Logger می‌تواند رویدادهای انتخاب شده را

به‌عنوان پیغام‌های Syslog به ESM ارسال کند. Logger، نقش ذخیره‌ساز را در مرکز عملیات امنیت بر عهده دارد.

5-2 User Behavior Analytics

یکی دیگر از محصولات شرکت HP که برای تشخیص تهدیدات مورد استفاده قرار می‌گیرد User Behavior Analytics (UBA) است. با بررسی الگوهای رفتاری کاربران به کاهش تهدیدات کمک می‌کند. این محصول به جای این‌که صرفاً بر داده‌های لاگ و رویداد تمرکز داشته‌باشد، تهدیدات ناشناخته را از طریق ایجاد یک پروفایل از رفتار هنجار کاربران و موجودیت‌هایی که در آن تعریف می‌شود و نیز شناسایی ناهنجاری‌های رفتار کاربران و موجودیت‌ها در مقایسه با رفتار هنجار تعریف‌شده، هنگامی که رخ می‌دهند، تشخیص می‌دهد. تهدیدات داخلی و استفاده نامناسب از حساب‌های کاربری به تشخیص و بررسی رفتار کاربران مخرب کمک می‌نماید.

6-2 HP EnterpriseView

EnterpriseView چارچوبی است که افسر امنیت اطلاعات اصلی را قادر می‌سازد که اطلاعات مخاطرات امنیتی را در زمینه کسب و کار تحلیل کند و اقدامات لازم برای کاهش مخاطرات، را اولویت‌دهی کند. با برقراری ارتباط میان مخاطرات فناوری اطلاعات و انطباق اطلاعات با خدمات کسب و کار، هماهنگی با اهداف مدیریت را تضمین می‌کند. شکاف میان عملیات فناوری اطلاعات و اداره امنیت[6] را از طریق اتصال و ادغام فرآیندهای کسب و کار در سراسر سازمان کاهش می‌دهد و پایه‌ای منطقی برای تصمیم‌گیری را ایجاد می‌کند. این محصول شامل یک رویکرد جامع و سازمانی است که اطلاعات آسیب‌پذیری، تهدید، انطباق و مخاطرات را ساده و یکپارچه می‌کند و یک زمینه کسب و کار را به مدیران ارائه می‌دهد. همچنین تهدیدات را پیش‌بینی کرده و پایش مستمر را با به‌روزرسانی و آزمون منظم توابع امنیتی مرتبط، فراهم می‌کند.

این ابزار به شکل ماژولار ارائه شده است، به‌این‌ترتیب مشتری می‌تواند ماژول‌هایی که هم‌اکنون به آن‌ها نیاز دارد را انتخاب کند، و در صورت نیاز ماژول‌های دیگری را نیز در آینده اضافه نماید. HP EnterpriseView دارای ماژول‌های زیر است:

- مدیریت مخاطره: این ماژول شما را قادر می‌سازد تا تمام جنبه‌های چرخه حیات ریسک را مدیریت کنید. همچنین از کتابخانه تهدیدات انعطاف‌پذیر و قابل گسترش برای شناسایی تهدیداتی که ممکن است به‌صورت بالقوه سازمان را به خطر بیاندازند استفاده می‌کند، سناریوهای تهدید را با تخصیص

[6] Security Office

تهدیدات به دارایی‌ها ایجاد می‌کند، ریسک را تحلیل می‌کند، تأثیر و احتمال آن را مشخص می‌کند و ریسک را با استفاده از کنترل‌ها یا سایر اقدامات مؤثر کاهش می‌دهد.

- مدیریت انطباق و سیاست: این ماژول شما را برای ارزیابی و ممیزی دارایی‌های سازمان توانمند می‌سازد. با استفاده از سازنده سیاست[7]، برای اعمال کنترل‌ها به دارایی‌ها، سیاست‌های سفارشی و ویژگی‌های بیانیه کاربرد[8] را ایجاد می‌کند. EnterpriseView شامل سیاست‌های پیش‌فرضی مانند چارچوب یکپارچه انطباق[9] است که قابلیت "یک بار ممیزی کن، با تعداد زیادی مطابقت بده" را فعال می‌کند.
- مدیریت آسیب‌پذیری: این ماژول آسیب‌پذیری‌ها را از ابزارهای ارزیابی آسیب‌پذیری جمع‌آوری می‌کند، موارد تکراری را حذف می‌کند، آن‌ها را به دارایی‌ها تخصیص می‌دهد، اولویت‌دهی می‌کند و اجازه می‌دهد تا فرآیند اصلاح را مدیریت کنید.
- فاکتورهای ریسک خارجی: این ماژول امکان واردکردن اطلاعات فاکتور ریسک از منابع خارجی، مدیریت و نمایش آن در مدل کسب و کار و داشبوردها را فراهم می‌کند.
- مدیریت دارایی: دارایی‌ها بلوک‌های سازنده مدل کسب و کار هستند، که یک پایه برای تمام عملکردهای اصلی EnterpriseView می‌باشند. مدل کسب و کار تمام سازمان، از سطح بالاترین دارایی‌های کسب و کار تا دارایی‌های سطح پایین فناوری اطلاعات، را از این نظر که چه عملیات آسیب‌پذیری، ریسک و سیاستی اجرا شده است، به تصویر می‌کشد. مدل کسب و کار را می‌توان با هماهنگ‌سازی EnterpriseView با یک مخزن دارایی خارجی و یا با استفاده از ماژول دارایی‌ها، ایجاد کرد.
- گزارش‌ها و داشبوردها: این ماژول داشبوردهای اجرایی پیچیده مانند ثبت و گزارش ریسک را در برمی‌گیرد. همچنین شما را قادر می‌سازد که گزارش‌ها و داشبوردهای سفارشی را تولید کنید.
- مدیریت کارها: EnterpriseView شما را قادر می‌سازد تا چارچوب‌های کاری را تولید، مدیریت و پایش کنید. با استفاده از چارچوب‌های کاری می‌توان فرآیندهای سازمان را ساده‌تر کرده و به آن‌ها ساختار داد، و نیز کارهایی را به افراد مرتبط با آن‌ها تخصیص داد.

[7] Policy builder
[8] Statement of Applicability
[9] Unified Compliance Framework

7-2 HPE Security ArcSight Reputation Security Monitor Plus (RepSM Plus)

راه‌حل RepSM Plus، از دانش تهدیدات اینترنت برای تشخیص آلوده‌شدن به بدافزار، حملات روز صفر، دستیابی و بازدید خطرناک[10] از شبکه استفاده می‌کند.

این راه‌حل از مؤلفه‌های زیر تشکیل شده است:

- سرویس HPE RepSM Plus اطلاعات شهرت[11] را از پایگاه‌داده‌های جامع آدرس‌های IP و نام‌های دامنه مخرب دریافت می‌کند.
- HPE Model Import Connector داده‌های شهرت را از HPE RepSM Plus دریافت کرده و به ArcSight ESM یا ESM Express ارسال می‌کند.
- محتویات HPE RepSM Plus روی ArcSight ESM یا ESM Express اجرا شده و داده‌های شهرت را با رویدادهای امنیتی برای تشخیص و اصلاح وقایع و موارد امنیتی همبسته می‌کند.

RepSM Plus می‌تواند شبکه را از تهدیدات مداوم پیشرفته[12] محافظت کند، حملات روز صفر را تحلیل کرده و تشخیص دهد، بینش و شفافیتی را در ارتباطات مخرب ارائه کند، و مرکز عملیات امنیت را بهینه‌سازی نماید.

8-2 ESM

یک مرکز عملیات امنیت برای ارائه خدمات و قابلیت‌هایی که از آن انتظار می‌رود و برای آن تعیین شده است، از فناوری‌های مختلفی استفاده می‌کند. برای ارائه این خدمات و قابلیت‌ها باید میان فناوری‌های مورد استفاده در مرکز عملیات امنیت همکاری و ارتباط برقرار شود. این ارتباط می‌تواند فقط برای ارسال پیغام تا درک کامل پیغام و استفاده از آن، تعریف شود. به‌همین دلیل نیازمند این هستیم که یک فناوری به‌عنوان نقطه اتصال و برقراری ارتباط میان فناوری‌های دیگر و نقطه تمرکز کانون مرکز عملیات امنیت، عمل کند. از این فناوری به‌عنوان قلب مرکز عملیات امنیت تعبیر می‌شود، که همان SIEM یا سامانه مدیریت رویداد و اطلاعات امنیتی است. ArcSight محصول SIEM خود را تحت عنوان ESM معرفی کرده است.

ArcSight ESM یک راه‌حل نرم‌افزاری جامع است که پایش رویدادهای امنیتی سنتی را با هوش شبکه‌ای[13]، همبسته‌سازی زمینه‌ای[14]، تشخیص ناهنجاری، ابزارهای تحلیل تاریخچه‌ای[15] و اصلاح خودکار ترکیب کرده است. یک راه‌حل چندسطحی است که ابزارهایی را برای تحلیل‌گران امنیت شبکه، مدیران سیستم و کاربران

[10] Dangerous Browsing
[11] Reputation Data
[12] Advanced Persistent Threats
[13] Network Intelligence
[14] Context Correlation
[15] Historical Analysis

تجاری ارائه کرده است. این محصول به‌عنوان قلب مرکز عملیات عمل کرده و از فناوری‌هایی که برای تشخیص و پایش و پویش شبکه سازمان مورد استفاده قرار می‌گیرند (سیستم‌های تشخیص نفوذ شبکه و میزبان، دیواره آتش، دیواره آتش برنامه‌های کاربردی وب، بررسی‌کننده صحت فایل، سیستم‌های جلوگیری از نشت اطلاعات، ضد بدافزارها، ابزارهای تشخیص تقلب[16]، ابزارهای تولید رویداد سیستم‌عامل ویندوز و لینوکس، پویش‌گران[17] آسیب‌پذیری) رویدادها و داده‌های متنی را دریافت می‌کند و پردازش‌هایی را (بررسی و تائید رویدادها، همبسته‌سازی، پایش، تحلیل) روی آن‌ها انجام داده و نتایج تحلیل‌های خود را به سایر فناوری‌ها (سیستم واکنش و پاسخ)، درصورتی‌که برای ارائه خدمات مرکز عملیات امنیت مورد نیاز باشد، ارسال می‌کند.

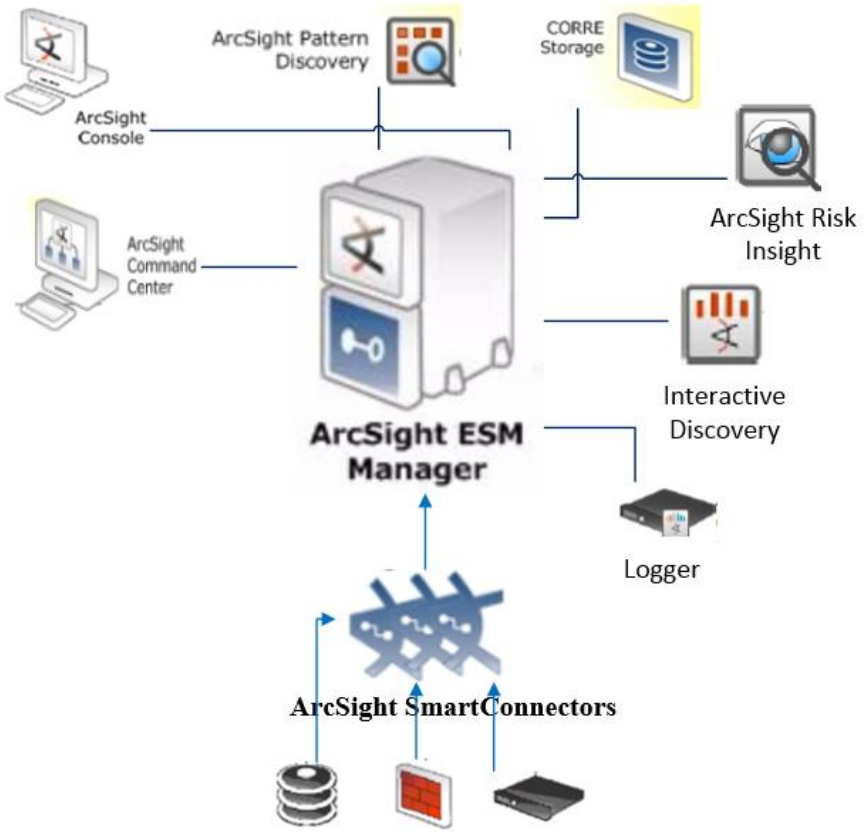
شرکت ArcSight محصول خود را به دو صورت ارائه می‌دهد:

1. سخت‌افزار از پیش آماده شده – Appliance
2. به‌صورت بسته‌ی نرم‌افزاری

به نوع نرم‌افزاری محصول ESM و به نوع Appliance آن ESM Express یا ESM Appliance گفته می‌شود. نسخه ESM Express به‌صورت پیش‌فرض دارای قابلیت‌های بیشتری نسبت به ESM است. البته این قابلیت‌های بیشتر روی ESM قابل اضافه شدن هستند.

معماری مؤلفه‌های محصول ESM مانند شکل 3 است. محصول شامل مؤلفه‌هایی است که در ادامه معرفی می‌شوند.

[16] Fraud Detection
[17] Scanner



شکل 3 معماری مؤلفه‌های ArcSight Express

2-8-1 HP Arcsight Logger

نسخه ArcSight Express شامل مؤلفه Logger نیز می‌شود. این مؤلفه به‌صورت بلندمدت هشدارها را نگهداری کرده و امکان تحلیل تاریخچه‌ای روی آن‌ها را فراهم می‌کند. توضیحات مربوط به Logger در بخش 2-4 آورده شده است.

2-8-2 Arcsight Console

واسط کاربری مبتنی بر ایستگاه کاری است که دسترسی کاملی به ESM را فراهم می‌آورد. از طریق محیط کنسول، که در بخش 4-1-1 به‌صورت مفصل معرفی می‌شود، تمام عملیاتی که برای مدیریت ESM مورد نیاز است را می‌توان انجام داد. تعریف کاربر، افزودن حس‌گر، انجام تنظیمات برای دریافت هشدارها، کاهش و تجمیع هشدارها، مدیریت حس‌گرها، تعریف منابع، ایجاد گزارش، مشاهده هشدارها، اضافه کردن قابلیت‌های جدید از جمله کارهایی است که با استفاده از کنسول می‌توان انجام داد. نسخه کنسول و نسخه Manager باید یکسان باشند.

2-8-3 Arcsight web

یک واسط کاربری مبتنی بر وب است که امکان انجام برخی کارها از جمله گزارش‌گیری، مشاهده داشبوردها، مشاهده کانال‌های فعال، و جستجوی رویدادها را فراهم می‌کند. با استفاده از این واسط نمی‌توان Connectorها را اضافه یا حذف کرد. از این واسط بیشتر برای مدیریت کاربران و حافظه ذخیره‌سازی استفاده می‌شود.

2-8-4 Arcsight smart agent

برای دریافت هشدارها و داده‌های متنی از انواع حس‌گرها و پویش‌گرها از SmartConnector استفاده می‌شود. SmartConnector را می‌توان روی ESM، روی Appliance به‌صورت سخت‌افزاری، و به‌صورت نرم‌افزاری روی حس‌گر یا یک سیستم نصب کرد، هشدارها را دریافت کرد و با انجام تنظیمات، هشدارها و داده‌های دریافتی را به سمت Manager ارسال کرد. امکان دریافت هشدار از چند حس‌گر روی یک SmartConnector وجود دارد. با استفاده از ArcSight Management Center امکان مدیریت همزمان چندین SmartConnector وجود دارد. SmartConnectorها می‌توانند هشدارها را نرمال کنند، آن‌ها را تجمیع کنند یا کاهش دهند.

2-8-5 Arcsight manager

قلب راه‌حل ArcSight Express، Manager است. خدمات، چارچوب‌ها و تحلیل‌ها توسط آن هدایت می‌شوند. هشدارها را دریافت و در CORR-Engine ذخیره کرده، و همزمان آن‌ها را تحلیل و همبسته‌سازی می‌کند. هر رویداد را با مدل شبکه و اطلاعات آسیب‌پذیری ارزیابی کرده تا خلاصه بلادرنگی از تهدیدات ایجاد کند. به‌صورت پیش‌فرض ESM همراه با برخی فیلترها، قوانین، گزارش‌ها، داشبوردها و مدل‌های شبکه ارائه می‌شود، تا هنگامی که محصول در شبکه مستقر شد، بتوان به‌سرعت از خدمات آن بهره‌مند شد.

مؤلفه‌های دیگری نیز وجود دارند که در صورت تمایل باید خریداری شوند. این مؤلفه‌ها در ادامه توضیح داده می‌شوند.

2-8-6 ArcSight Risk Insight

مؤلفه ArcSight Risk Insight کاربران را قادر می‌سازد تا تأثیر تجاری تهدیدات بلادرنگ را بر دارایی‌ها درک کنند. در ESM کاربران لایه‌های دارایی کسب وکار (شامل ایستگاه کاری، سرویس‌دهنده‌ها، لپ‌تاپ) را تعریف می‌کنند، از قوانین برای محاسبه فاکتورهای ریسک روی این دارایی‌ها استفاده می‌کنند و داده‌ها را وارد Risk Insight می‌کنند. به‌این‌ترتیب، Risk Insight امتیازاتی که از مدل کسب و کار به‌دست می‌آید را تجمیع می‌کند، کاربران تأثیر یک تهدید مشخص که ممکن است یک فاکتور ریسک روی مدل کسب و کار باشد، را ارزیابی می‌کنند. کاربران شاخص‌های کارایی کلیدی را برای پایش ریسک‌های سازمان به‌صورت مداوم ایجاد می‌کنند. با استفاده از محیط Command Center امکان دسترسی به Risk Insight وجود دارد.

7-8-2 ArcSight Interactive Discovery

ArcSight Interactive Discovery (AID)، باعث تقویت تشخیص الگو، تحلیل‌های گرافیکی و گزارش و داشبوردها می‌شود. AID قابلیت‌های گزارش‌دهی و تحلیل تاریخچه‌ای داده ارتقا یافته را با استفاده از انتخاب جامع گرافیک‌های آماری پیش‌ساخته تعاملی فراهم می‌کند.

موارد زیر با استفاده از AID امکان‌پذیر است:

- دسترسی بصری سریع به داده‌های امنیتی پیچیده
- اکتشاف و تعمق در داده‌های امنیتی با انعطاف‌پذیری و کنترل دقیق
- شتاب‌بخشیدن به کشف رویدادهایی که ممکن است خطرناک باشند
- ارائه وضعیت امنیت در چکیده‌های بصری
- اثبات ارزش امنیت فناوری اطلاعات و کمک به تعدیل بودجه‌ها

با استفاده از ابزارهای اکتشاف تعاملی بصری می‌توان به سادگی حملات بالقوه را پیدا و مورد تحقیق و بررسی قرار داد. امکان تحلیل فعالیت‌های امنیتی شبکه را با استفاده از چکیده‌سازی‌های گرافیکی داده‌های رویداد فراهم می‌کند. در طول تحلیل‌های روزانه داده‌های روز گذشته، امکان کشف مسائلی که توسط تحلیل‌های خودکار ممکن است در نظر گرفته نشده باشد، فراهم می‌شود. می‌توان از این داده‌ها برای ایجاد قوانین جدید جهت بهبود فرآیند مدیریت امنیت کسب و کار بهره گرفت.

8-8-2 ArcSight Pattern Discovery

کشف الگو[18] می‌تواند به‌صورت خودکار الگوهای بلند مدت و اختصاصی را کشف کند، در غیراین‌صورت در جریان رویدادها به‌صورت غیرقابل کشف باقی می‌ماند. می‌توان از کشف الگو در موارد زیراستفاده کرد:

- کشف حملات روز صفر: به‌دلیل این‌که کشف الگو روی دانش از پیش تعیین شده دامنه (مانند فیلتر و قوانین از پیش تعریف‌شده) تکیه نمی‌کند، می‌تواند الگوهایی که دیده نمی‌شوند یا مختص محیط شبکه یک سازمان هستند را کشف کند.
- کشف حملات کند و با سرعت پائین: کشف الگو می‌تواند تا یک میلیون رویداد را در چندین ثانیه پردازش کند. این امر سبب می‌شود که کشف الگو حتی الگوی حملات کند و آرام را ذخیره کند.
- ایجاد پروفایل از الگوهای رایج در شبکه: الگوهای کشف شده از ترافیک جاری شبکه مانند امضاهایی برای زیرمجموعه مشخصی از ترافیک شبکه هستند. با مطابقت آن‌ها با مخزنی از الگوهای تاریخچه‌ای، می‌توان حملات در جریان را کشف کرد.

[18] Pattern Discovery

- ایجاد قانون به‌صورت خودکار: الگوهایی که کشف شده‌اند، می‌توانند با یک کلیک موشواره، به یک مجموعه قانون کامل تبدیل شوند. قوانینی که به‌این‌ترتیب ایجاد می‌شوند مختص هر سازمانی هستند اما قوانین از پیش نوشته شده باید به اندازه کافی کلی باشند تا توسط تمام سازمان‌ها مورد استفاده قرار گیرند.

3 معرفی انواع محصولات ArcSight و License آن‌ها

در حال حاضر این محصول در انواعی که به‌ترتیب در شکل‌های 4 تا 13 نمایش داده شده است به فروش می‌رسد. License محصول یک ساله است، اما در صورتی‌که به‌صورت نرم‌افزاری خریداری شود امکان استفاده بیش از یک سال را دارد ولی دیگر از سوی شرکت ArcSight پشتیبانی نمی‌شود.

Family	Product	Description	SKU
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7100/E7200/E7400-2 Upgr Svr	TG227AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7100/E7200/E7400-4 Upgr Svr	TG228AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-2 Server	TG229AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-2-HA Server	TG230AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-2-NP Server	TG255AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-4 NP Server	TG475AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-4 Server	TG231AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-4-HA Server	TG232AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-4-NFR Server	TG233AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-8 Server	TG556AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-8-HA Server	TG557AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-8-NP Server	TG558AA
Enterprise Security Manager Appliances	ESM Appliances	HP ArcSight E7400-HW-Server	TG469AA

شکل 4 انواع محصولات ESM Appliance

Family	Product	Description	SKU
Logger Appliances	Logger Appliances	HP ArcSight L3000/L3200/L3400 Upgr Svr	TG234AA
Logger Appliances	Logger Appliances	HP ArcSight L3400 Server	TG238AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-HA Server	TG241AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-NFR Server	TG243AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-NP Server	TG239AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-PCI HA Server	TG245AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-PCI NP Server	TG476AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-PCI Server	TG244AA
Logger Appliances	Logger Appliances	HP ArcSight L3400-PCI-NFR Server	TG246AA
Logger Appliances	Logger Appliances	HP ArcSight L3X00/L3400 PCI-HA Upgr Svr	TG237AA
Logger Appliances	Logger Appliances	HP ArcSight L5000/7X00/7400S-HA Upgr Svr	TG252AA
Logger Appliances	Logger Appliances	HP ArcSight L5000/7X00/7400X-HA Upgr Svr	TG272AA
Logger Appliances	Logger Appliances	HP ArcSight L5000/L7X00/L7400S Upgr Svr	TG251AA
Logger Appliances	Logger Appliances	HP ArcSight L5000X/7X00X/L7400X Upgr Svr	TG269AA
Logger Appliances	Logger Appliances	HP ArcSight L5X/7X/L7400 SAN-HA Upgr Svr	TG248AA
Logger Appliances	Logger Appliances	HP ArcSight L5X00/7200/7400 SAN Upgr Svr	TG249AA
Logger Appliances	Logger Appliances	HP ArcSight L7400S NP Server	TG256AA

شکل 5 انواع محصولات Logger Appliance

Family	Product	Description	SKU
Network Synergy Platform Appliances	NSP Appliances	HP ArcSight NSP N5400 100 Dev Upgr Svr	TG565AA
Network Synergy Platform Appliances	NSP Appliances	HP ArcSight NSP N5400 500 Dev Upgr Svr	TG567AA
Network Synergy Platform Appliances	NSP Appliances	HP ARST NSP N5400 100 Dev Upgr HA Svr	TG566AA
Network Synergy Platform Appliances	NSP Appliances	HP ARST NSP N5400 500 Dev Upgr HA Svr	TG568AA

شکل 6 انواع محصولات NSP

Family	Product	Description	SKU
Enterprise View	Enterprise View	HP ArcSight Ent View 1.00 Eng SW E-Media	TD828AAE
Enterprise View	Enterprise View	HP ArcSight Ent View 1.50 Eng SW E-Media	TD828BAE
Enterprise View	Enterprise View	HP ArcSight EV Add 10k Asset NP SW E-LTU	TD843AAE
Enterprise View	Enterprise View	HP ArcSight EV Add 10k Asset SW E-LTU	TD836AAE
Enterprise View	Enterprise View	HP ArcSight EV PM 10k Asset NP SW E-LTU	TD844AAE
Enterprise View	Enterprise View	HP ArcSight EV PM 10k Asset SW E-LTU	TD837AAE
Enterprise View	Enterprise View	HP ArcSight EV PM per Inst NP SW E-LTU	TD841AAE
Enterprise View	Enterprise View	HP ArcSight EV PM per Inst SW E-LTU	TD834AAE
Enterprise View	Enterprise View	HP ArcSight EV RM 10k Asset NP SW E-LTU	TD845AAE
Enterprise View	Enterprise View	HP ArcSight EV RM 10k Asset SW E-LTU	TD838AAE
Enterprise View	Enterprise View	HP ArcSight EV RM per Inst NP SW E-LTU	TD842AAE
Enterprise View	Enterprise View	HP ArcSight EV RM per Inst SW E-LTU	TD835AAE

شکل 7 انواع محصولات Enterprise View

Family	Product	Description	SKU
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 150 Con HA SW E-LTU	TD901AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 150 Con NP SW E-LTU	TD897AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 150 Con SW E-LTU	TD893AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 4 Con HA SW E-LTU	TD899AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 4 Con NP SW E-LTU	TD895AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 4 Con SW E-LTU	TD891AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 50 Con HA SW E-LTU	TD900AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 50 Con NP SW E-LTU	TD896AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 50 Con SW E-LTU	TD892AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP 6.30 Eng SW E-Media	TH022BAE
Connector Appliance software	Connector Appliance software	HP ArcSight ConApp 6.40 Eng SW E-Media	TH022CAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP Add 25Con HA SW E-LTU	TD902AAE
Connector Appliance software	Connector Appliance software	HP ArcSight CONAPP Add 25Con NP SW E-LTU	TD898AAE

شکل 8 انواع محصولات Connector Appliance software

Family	Product	Description	SKU
Connector Appliances	Connector Appliances	HP ArcSight C1000/C1300/C1400 Upgr Svr	TG212AA
Connector Appliances	Connector Appliances	HP ArcSight C3000/C3200/C3400 Upgr Svr	TG213AA
Connector Appliances	Connector Appliances	HP ArcSight C5100/C5200/C5400 Upgr Svr	TG214AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C1400 HA Server	TG217AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C1400 NP Server	TG474AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C1400 Server	TG216AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C1400-NFR Server	TG218AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C3400 HA Server	TG221AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C3400 NP Server	TG220AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C3400 Server	TG219AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C3400-NFR Server	TG222AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C5400 Server	TG223AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C5400-HA Server	TG225AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C5400-NFR Server	TG226AA
Connector Appliances	Connector Appliances	HP ArcSight CONAPP-C5400-NP Server	TG224AA
Connector Appliances	Connector Appliances	HP ARST CONAPP C3X00/C3400 Upgr HA Svr	TG559AA
Connector Appliances	Connector Appliances	HP ARST CONAPP C5X00/C5400 Upgr HA Svr	TG560AA

شکل 9 انواع محصول Connector Appliance

Family	Product	Description	SKU
Connectors	Flex Connectors Kit	HP ArcSight FlexConnect Kit NFR SW E-LTU	TH332AAE
Connectors	Flex Connectors Kit	HP ArcSight FlexConnect Kit SW E-LTU Svr	TH330AAE

شکل 10 انواع محصول Flex Connector

Family	Product	Description	SKU
Discovery	Interactive Discovery	HP ArcSight AID 4.11 Eng SW E-Media	TH002AAE
Discovery	Interactive Discovery	HP ArcSight Inter Discv Usr SW E-LTU	TH273AAE
Discovery	Pattern Discovery	HP ArcSight PD 100 Gb/d SW E-LTU	TJ605AAE
Discovery	Pattern Discovery	HP ArcSight PD 150 Gb/d SW E-LTU	TJ606AAE
Discovery	Pattern Discovery	HP ArcSight PD 250 Gb/d SW E-LTU	TJ607AAE
Discovery	Pattern Discovery	HP ArcSight PD 5 Gb/d SW E-LTU	TJ628AAE
Discovery	Pattern Discovery	HP ArcSight PD 50 Gb/d SW E-LTU	TJ619AAE
Discovery	Pattern Discovery	HP ArcSight PD MA 5 Gb/d SW E-LTU	TJ629AAE

شکل 11 انواع محصول Interactive Discovery

ESM	ESM Console	HP ArcSight Console EA User SW E-LTU	TH071AAE
ESM	ESM Console	HP ArcSight Console MA User SW E-LTU	TJ439AAE
ESM	ESM Console	HP ArcSight Console User SW E-LTU	TH066AAE

شکل 12 انواع محصول ESM Console

Family	Product	Description	SKU
Logger	Logger	HP ArcSight Lg 160GB/d ulDev HA SW E-LTU	TH488AAE
Logger	Logger	HP ArcSight Lg 160GB/d ulDev NP SW E-LTU	TH484AAE
Logger	Logger	HP ArcSight Lg 250GB/d ulDev HA SW E-LTU	TF422AAE
Logger	Logger	HP ArcSight Lg 250GB/d ulDev NP SW E-LTU	TF423AAE
Logger	Logger	HP ArcSight Lg 30GB/d 200Dev HA SW E-LTU	TH486AAE
Logger	Logger	HP ArcSight Lg 30GB/d 200Dev NP SW E-LTU	TH482AAE
Logger	Logger	HP ArcSight Lg 5GB/d 50Dev HA SW E-LTU	TH485AAE
Logger	Logger	HP ArcSight Lg 5GB/d 50Dev NP SW E-LTU	TH481AAE
Logger	Logger	HP ArcSight Lg 80GB/d 500Dev HA SW E-LTU	TH487AAE
Logger	Logger	HP ArcSight Lg 80GB/d 500Dev NP SW E-LTU	TH483AAE

شکل 13 انواع محصول Logger

4 معرفی مقدماتی محصول

4-1 ورود به محصول ArcSight Express

پس از نصب محصول، به دو طریق می‌توان به محصول دسترسی پیدا کرد:

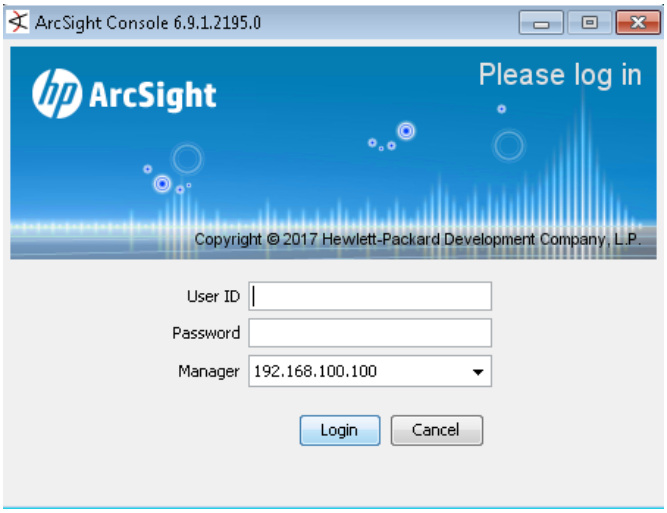
1. از طریق کنسول
2. از طریق Command Center با استفاده از مرورگر وب

با دسترسی به ESM با استفاده از هر دو روش فوق، محیط‌های کاربری متفاوتی مشاهده خواهد شد، تنظیمات متفاوتی را می‌توان انجام داد و گزارش و داشبوردهای متفاوتی دیده می‌شود. در ادامه هر دو روش دستیابی معرفی می‌شوند.

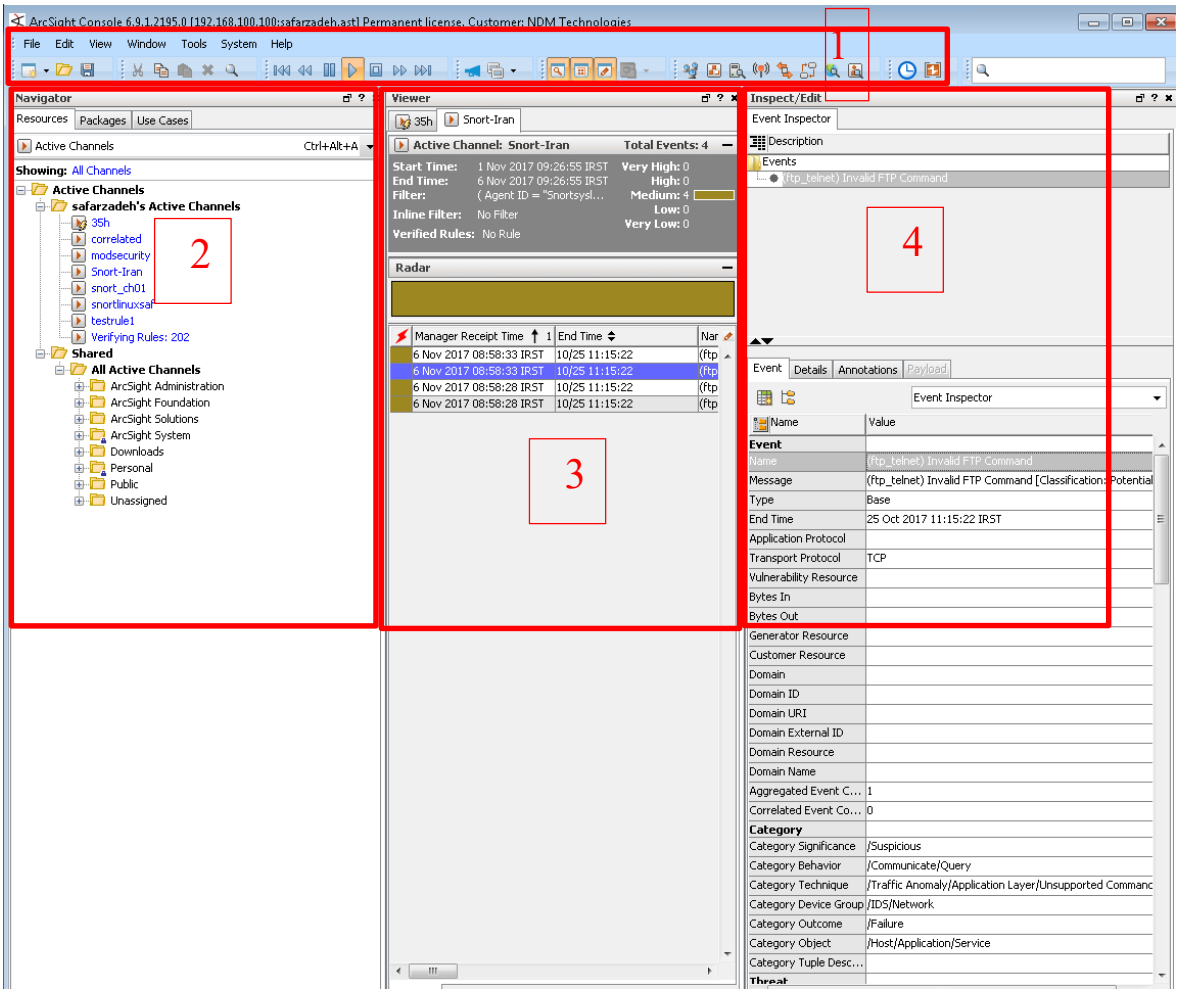
4-1-1 دسترسی به محصول از طریق کنسول

با دوبار کلیک روی آیکون کنسول ArcSight (شکل 14) صفحه ورود باز شده و پس از وارد کردن اطلاعات حساب کاربری در صفحه شکل 15، صفحه اول، که در شکل 16 ملاحظه می‌شود، نمایش داده می‌شود.

شکل 14 آیکون کنسول ArcSight



شکل 15 صفحه ورود اطلاعات حساب کاربری



شکل 16 اولین صفحه هنگام ورود به محصول

همان‌طور که در شکل 16 نمایش داده شده است، اولین صفحه از 4 بخش تشکیل شده است.

4-1-1-1 استفاده از منوهای مختلف

بخش اول شامل منوهای مختلف برای کار با ابزارهای گوناگون است. در ادامه هر کدام از آن‌ها معرفی می‌شوند.

- File: ایجاد، باز کردن و ذخیره منابع توسط این منو انجام می‌شود (شکل 17).

شکل 17 منوی فایل

- Edit: برای بریدن، کپی، چسباندن، پاک کردن و جستجوی متن و منابع مورد استفاده قرار می‌گیرد (شکل 18).

شکل 18 منوی ویرایش

- Channel Controls: برای کار با کانال‌های فعال مورد استفاده قرار می‌گیرد، از چپ به راست به ترتیب به معنی رفتن به شروع، عقب‌رفتن افزایشی، مکث، پخش، توقف، جلورفتن افزایشی، و رفتن به انتها است (شکل 19).

شکل 19 منوی کانال فعال

- Windows: برای نمایش یا بستن بخش‌های Navigator، Viewer و Inspect/Edit مورد استفاده قرار می‌گیرد (شکل 20).

شکل 20 منوی Window

- Network Tools: ابزارهای تحلیل شبکه مبتنی بر آدرس IP را اجرا می‌کند (شکل 21).

شکل 21 منوی ابزارهای شبکه

- System: فهرست کارهای زمان‌بندی شده را باز کرده و دسته‌بندی کاربر را به رویداد انتخاب شده تخصیص می‌دهد (شکل 22).

شکل 22 منوی سیستم

- View: دکمه اعلان[19] اگر آبی باشد به این معنی است که پیغامی وجود ندارد، اگر قرمز باشد، یعنی پیغام اخطاری ایجاد شده است (شکل 23).

[19] Notification

شکل 23 منوی View

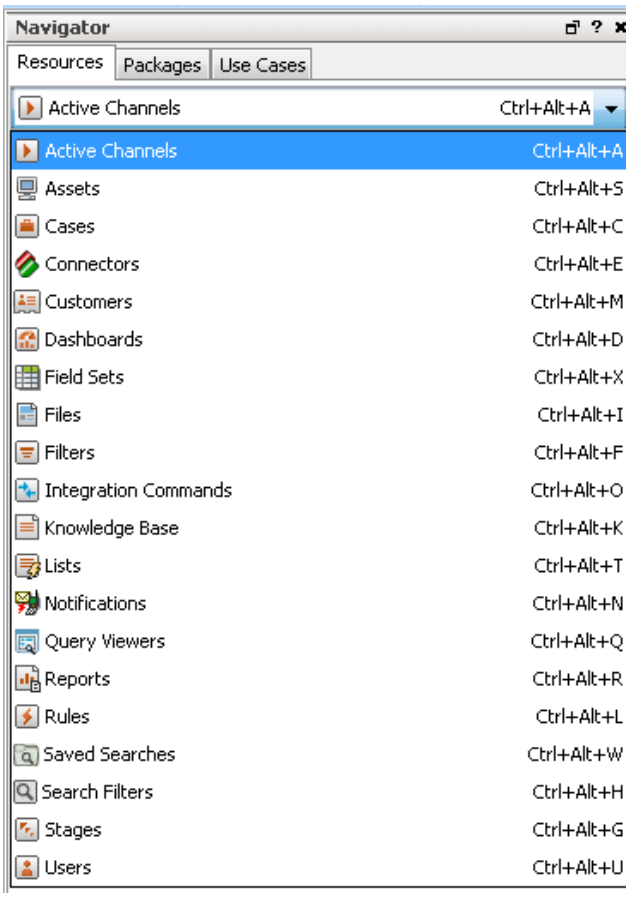
- Status Bar: در قسمت پایینی کنسول قرار دارد و پیغام‌های عملیات کنسول را نمایش می‌دهد. از بخش Windows/Status Bar قابل نمایش و مخفی‌سازی است.

2-1-1-4 Navigator

بخش Navigator که 2 نام دارد از سه برگه مهم و کاربردی Resources، Packages و Use Cases تشکیل شده است و برای مدیریت منابع، بسته‌ها و موارد کاربرد مورد استفاده قرار می‌گیرد. که در ادامه هر کدام از این موارد به‌صورت مفصل تشریح خواهند شد.

1-2-1-1-4 Resources

ESM برای مدیریت منطق پردازش رویدادها از اشیایی به نام منبع استفاده می‌کند. در واقع تمام موجودیت‌هایی که طی پردازش رویدادها ممکن است مورد استفاده قرار گیرند را در قالب منبع تعریف کرده است. با کلیک روی برگه Resources فهرست منابع مانند شکل 24 نمایش داده می‌شود.



شکل 24 فهرست منابع

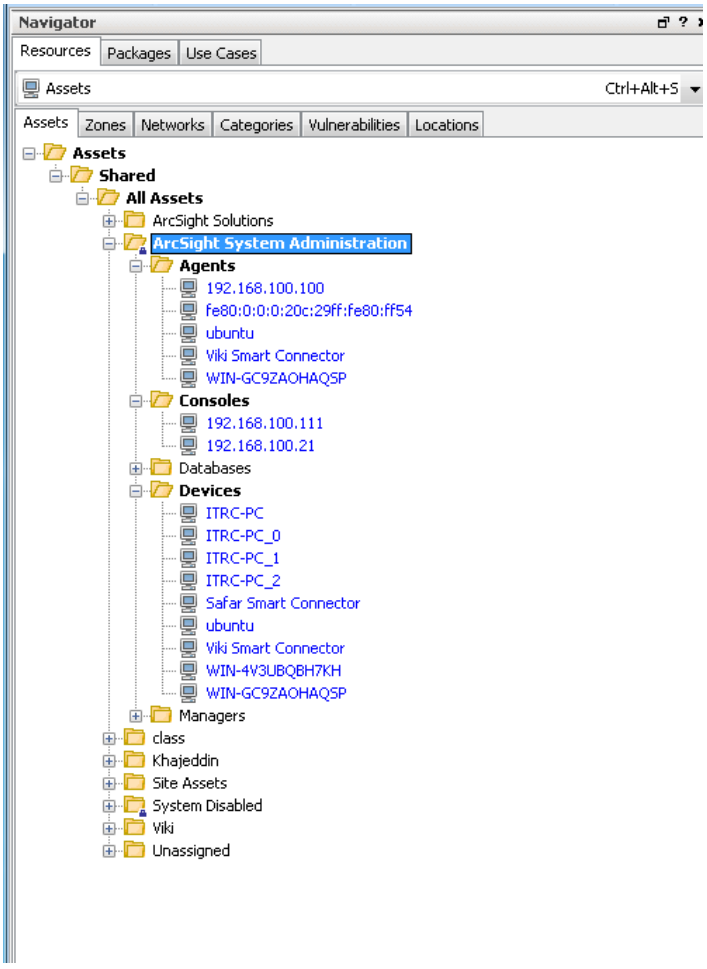
در ادامه هر منبع به‌صورت خلاصه تعریف می‌شود.

- Active Channels

ESM رویدادها را با استفاده از Active Channel نمایش می‌دهد. تعریف یک Active Channel شامل تعیین ویژگی‌هایی است که می‌خواهیم رویدادهایی که قرار است مشاهده کنیم آن‌ها را داشته باشند. در فصل 5 روش تعریف Active Channel به‌صورت مفصل بیان شده است. برای تعریف، تغییر و حذف Active Channel مورد استفاده قرار می‌گیرد.

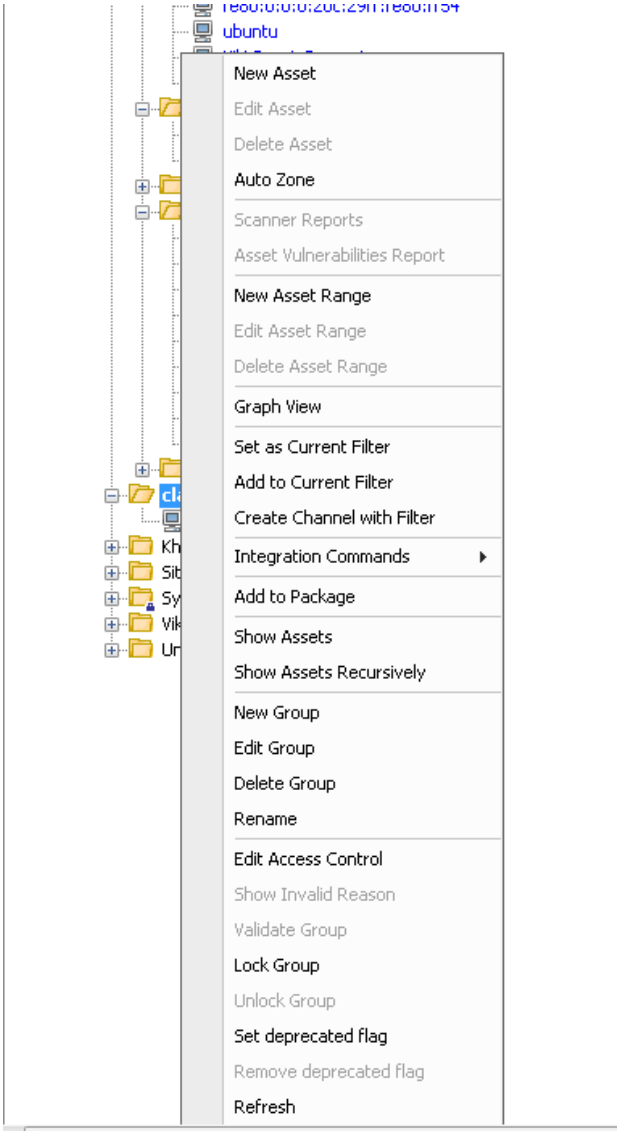
- Assets

امکان تعریف و دسته‌بندی ابزارها، یا گروهی از ابزارها را در شبکه فراهم می‌کند. دارایی‌های سازمان شامل ESM و SmartConnectorهای آن، و میزبان و کارگزارهای موجود در سازمان هستند. نمایشی از دارایی‌های تعریف‌شده در برگه دارایی‌ها در شکل 25 نمایش داده شده است.



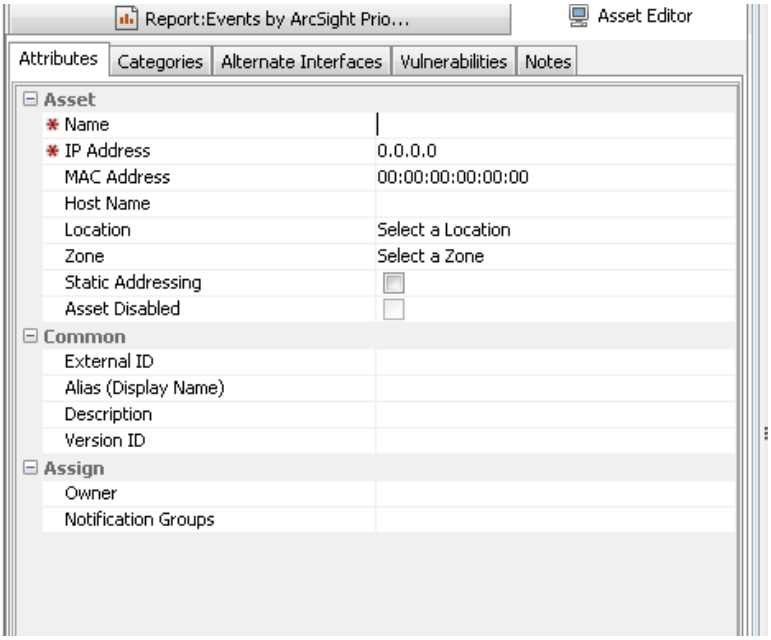
شکل 25 فهرست دارایی‌های موجود

برای تعریف دارایی جدید روی فولدری که قرار است دارایی به آنجا اضافه شود راست کلیک کرده و New Asset را انتخاب می‌کنیم (شکل 26).



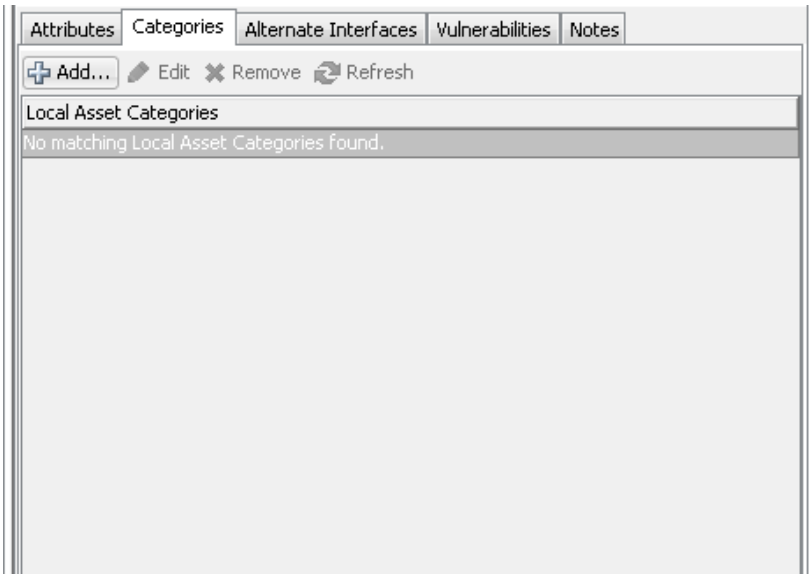
شکل 26 ایجاد دارایی جدید

در بخش Inspect/Edit نیز مشخصات مربوط به دارایی را تنظیم می‌کنیم. نام و آدرس IP، آدرس فیزیکی، محل قرارگیری، منطقه و سایر ویژگی‌ها، همان‌طور که در شکل 27 نمایش داده شده است.

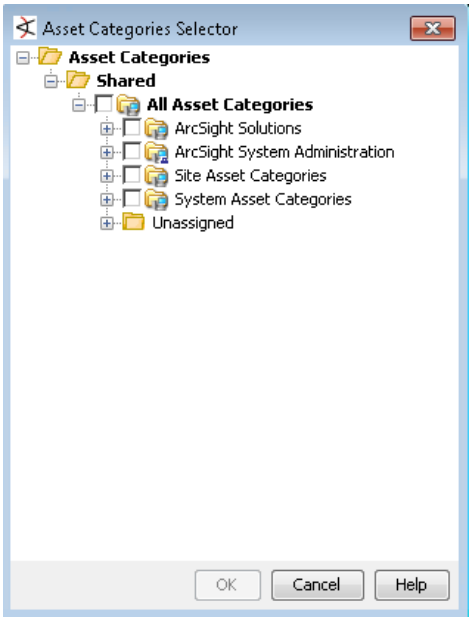


شکل 27 تنظیم مشخصات

سپس در برگه Categories امکان مشخص‌کردن دسته‌بندی دارایی وجود دارد (شکل 28). با انتخاب Add و سپس انتخاب دسته مورد نظر (شکل 29)، دارایی به آن دسته افزوده می‌شود.



شکل 28 برگه دسته‌بندی دارایی

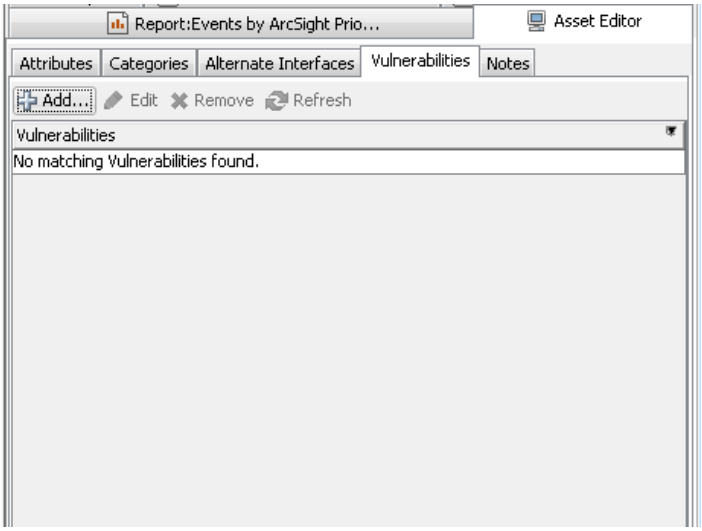


شکل 29 تخصیص دارایی به دسته مورد نظر

در برگه Alternate Interfaces (شکل 30) می‌توان واسط‌های ثانویه را انتخاب کرد.

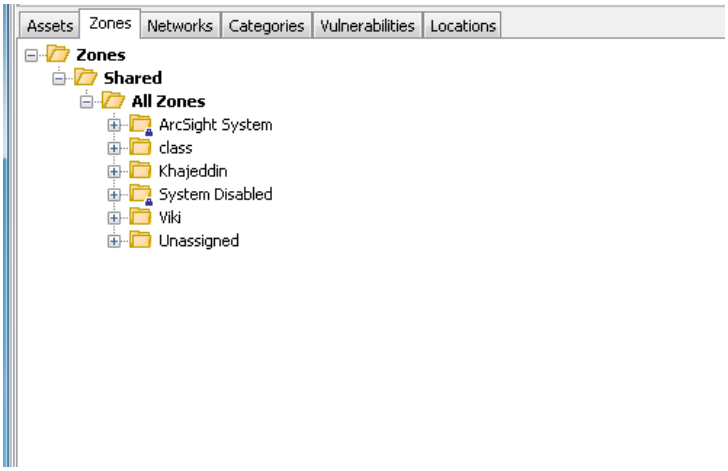
شکل 30 افزودن واسط‌های ثانویه

در بخش Vulnerabilities (شکل 31) فهرست آسیب‌پذیری‌های دارایی قرار می‌گیرد.



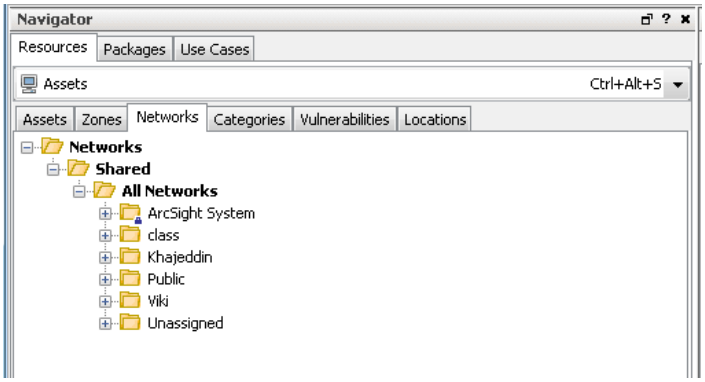
شکل 31 فهرست آسیب‌پذیری‌های دارایی

منبع دارایی‌ها، برگه‌های دیگری نیز دارد، این برگه‌ها در شکل 32 نمایش داده شده است. امکان تعریف منطقه در برگه Zones وجود دارد.



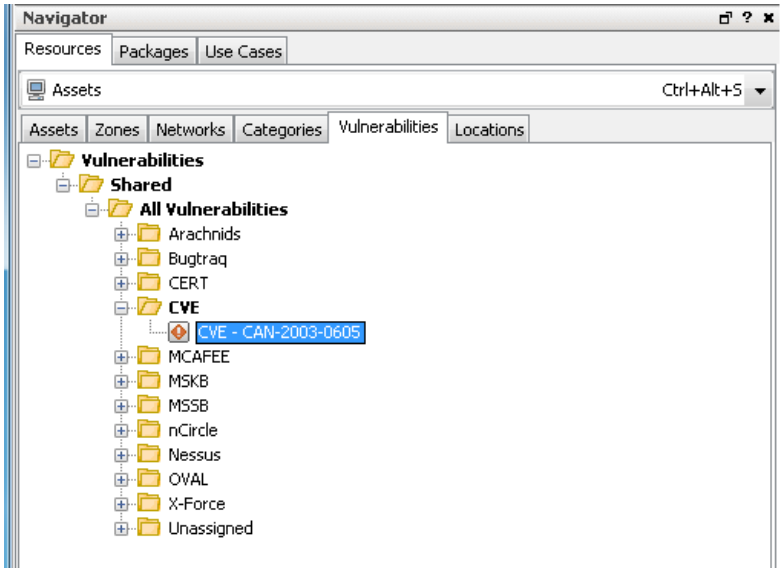
شکل 32 منطقه‌بندی دارایی‌ها

امکان تعریف شبکه در برگه Networks وجود دارد.



شکل 33 تعریف شبکه برای مدل‌کردن دارایی‌ها

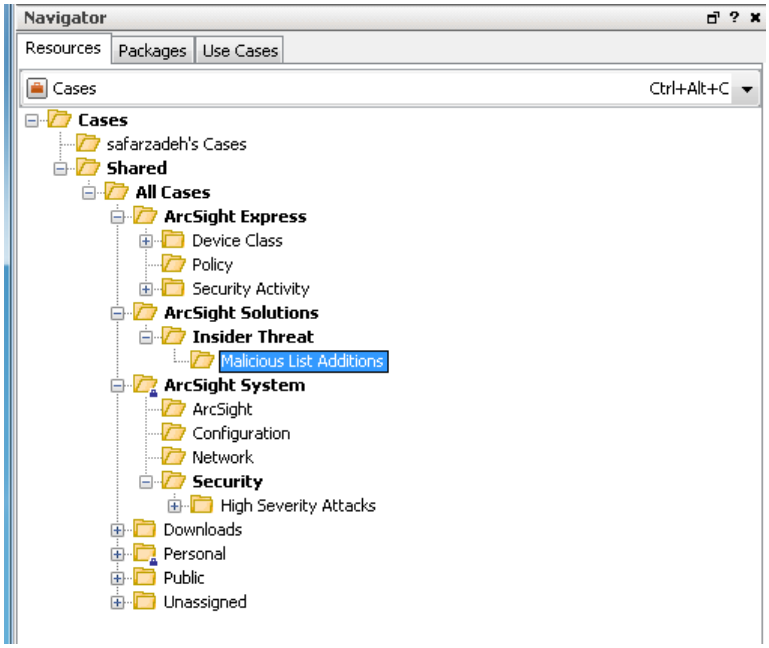
در بخش Vulnerabilities (شکل 34) انواع آسیب‌پذیری‌ها را بر اساس مرجع ارائه‌دهنده، دسته‌بندی شده است.



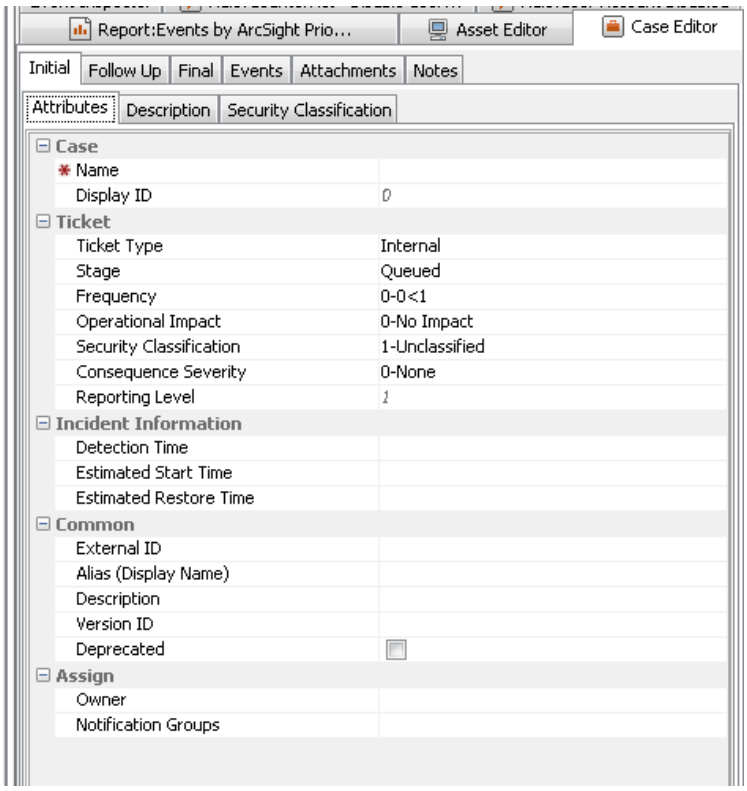
شکل 34 فهرست آسیب‌پذیری‌ها بر اساس مراجع ارائه‌دهنده آن‌ها

- Cases

امکان ردیابی وقایعی که رخ داده است را، بر اساس اولویت و وضعیت آن‌ها، به‌وجود می‌آورد. در برگه Cases (شکل 35) فهرست موارد آورده شده است. به‌عنوان نمونه، در شکل 36 مشخصات یک مورد در بخش Inspect/Edit نمایش داده شده است. همان‌طور که ملاحظه می‌شود، امکان بیان شرح مورد، ضمیمه‌کردن اسناد به آن، شروع و خاتمه مورد، مشاهده رویدادهایی که به آن تخصیص یافته است، یا تخصیص رویداد به آن، و دنبال‌کردن وضعیت رویداد تا خاتمه آن وجود دارد.



شکل 35 منبع Case



شکل 36 مشخصات یک Case

- Connectors

در این بخش امکان مدیریت و مشاهده Connectorهایی که به محصول متصل شده‌اند وجود دارد.

- Customers

مدیریت منابعی که مشتری‌ها درباره آن‌ها نگرانی امنیتی دارند. این مورد برای استفاده در MSSP[20] کاربرد دارد.

- Dashboards

در این بخش انواع پایش‌گران داده‌های رویداد و کتابخانه‌ای از منابع قابل پشتیبانی توسط آن‌ها ارائه می‌شود.

- Field Sets

امکان تعریف زیرمجموعه‌ای از فیلدهای داده موجود را فراهم می‌کند. می‌توان براساس این مجموعه‌های سفارشی ایجادشده، روی زمینه خاصی تمرکز کرد و تنها از زمینه تعریف‌شده گزارش‌گیری نمود، براساس آن کانال فعال تعریف کرد و داشبوردهایی را ایجاد نمود.

- Files

فایل‌هایی که به‌عنوان منبع در Manager ذخیره شده‌اند را مشخص می‌کند. این فایل‌ها شامل فایل‌های ضمیمه شده به موارد، قالب‌ها، و فایل‌های مشترک همه‌منظوره می‌شوند. کاربران متناسب با سطح دسترسی خود امکان مشاهده این فایل‌ها را دارند.

- Filters

در این بخش فیلترهای تعریف‌شده در گروه‌هایی دسته‌بندی می‌شوند.

- Integration Commands

امکان اجرای دستورات روی ابزارها، پیکربندی ابزارها، و پیکربندی اسکریپت‌ها را فراهم می‌کند. به‌عنوان مثال امکان پشتیبانی از Network Synergy Platform را به‌وجود می‌آورد.

- Knowledge Base

پایگاه‌داده‌ای از مقالات که در حل مسائلی که پیش می‌آید مفید هستند را دربرمی‌گیرد.

- Lists

شامل لیست فعال و لیست نشست می‌شود. لیست فعال فهرستی از مبدأهای فعال و آدرس‌های IP دارای اهمیت است که بااستفاده از قوانین تعریف‌شده‌اند. نشست فعال مشابه لیست فعال است اما برای پایش و پرس‌وجوی مبتنی بر زمان بهینه شده است.

- Notifications

مقصدها و تنظیمات برای ارسال پیغام‌های خودکار، تا وضعیت‌های از پیش تعیین‌شده یا رویدادها را اطلاع می‌دهد.

- Query Viewers

یک منبع برای تعریف و اجرای پرس‌وجوهای SQL روی سایر منابع ESM شامل روندها، دارایی‌ها، موارد، Connector، رویدادها و سایر موارد است. هر Query Viewer شامل یک پرس‌وجوی SQL است که برای ایجاد و مقایسه نتایج پایه‌ای، تحلیل تاریخچه‌ای داده، پیداکردن الگوهایی در فعالیت‌های شبکه و انجام تحقیقات عمیق روی جنبه خاصی از نتایج مفید می‌باشد.

[20] Managed Security Services Provider

- Reports

تعریف و استخراج خروجی از فعالیت‌های متنوع را شامل می‌شود.

- Rules

قوانین مربوط به جداسازی، تحلیل و پاسخ به رویدادها در این بخش ایجاد و مدیریت می‌شوند.

- Saved Searches

برای ایجاد جستجو و ذخیره آن‌ها مورد استفاده قرار می‌گیرد. این منبع در Command Center ایجاد می‌شود و در این‌جا تنها با هدف بسته‌بندی و همگامی محتویات آورده شده است.

- Search Filters

برای ایجاد فیلترهای مورد استفاده در جستجو مورد استفاده قرار می‌گیرد. این منبع در Command Center ایجاد می‌شود و در این‌جا تنها با هدف بسته‌بندی و همگامی محتویات آورده شده است.

- Stages

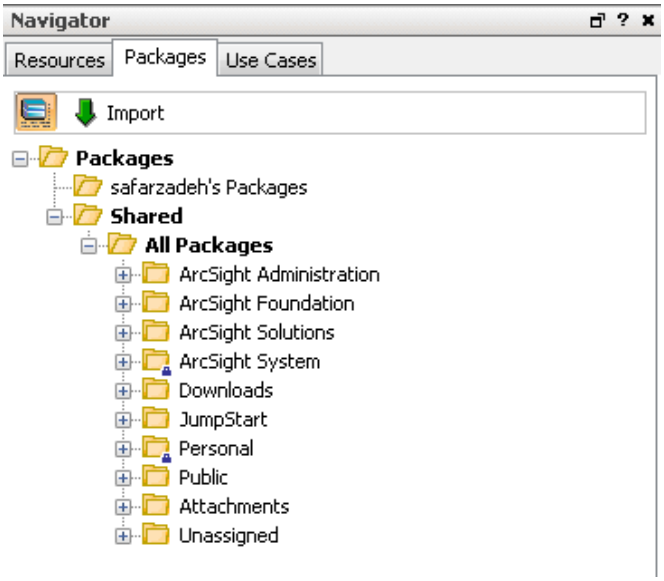
ویژگی‌های چارچوب کاری را شامل می‌شود، برای این‌که تحلیل‌گران به‌صورت بلادرنگ روی رویدادهای امنیتی همکاری کنند.

- Users

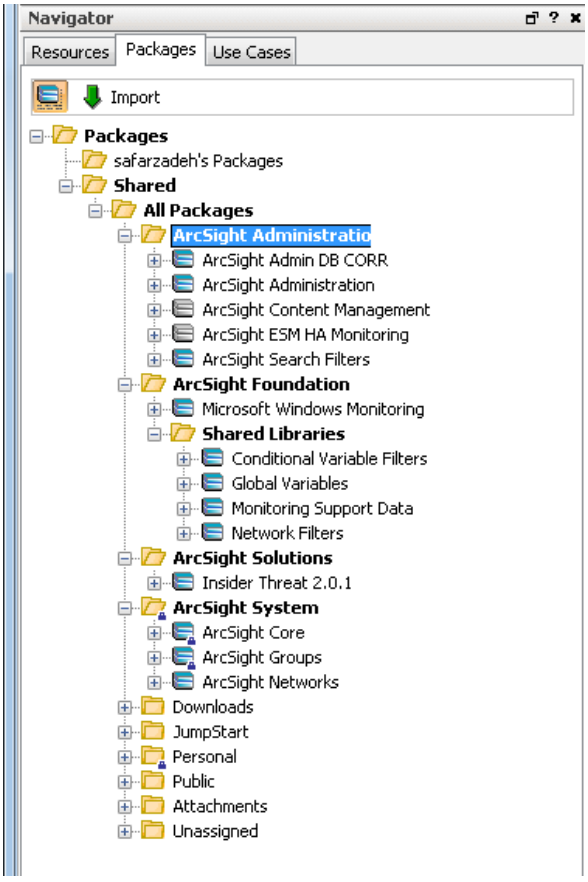
کاربران و گروه‌های آن‌ها را دربرمی‌گیرد.

2-2-1-1-4 Packages

Package منبعی است که خود مجموعه‌ای از منابع را دربرمی‌گیرد. امکان تهیه پشتیبان، انتقال به سایر ESMها، به‌روزرسانی، نصب و بارگذاری آن به‌صورت یک واحد وجود دارد. به‌صورت پیش‌فرض مجموعه‌ای از Packageها در این برگه وجود دارند. امکان دانلود رایگان برخی از Packageها نیز وجود دارد اما بیشتر آن‌ها باید به‌صورت جداگانه از محصول خریداری شوند. در شکل‌های 37 و 38 نمایشی از Packageهای پیش‌فرض محصول مشاهده می‌شود.

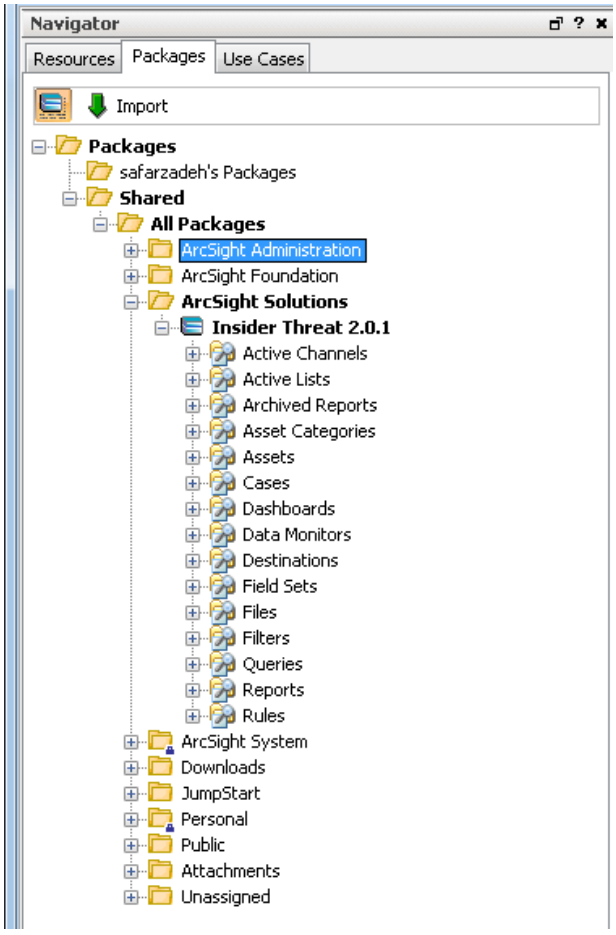


شکل 37 فهرست Packageها



شکل 38 محتویات برخی از Packageها

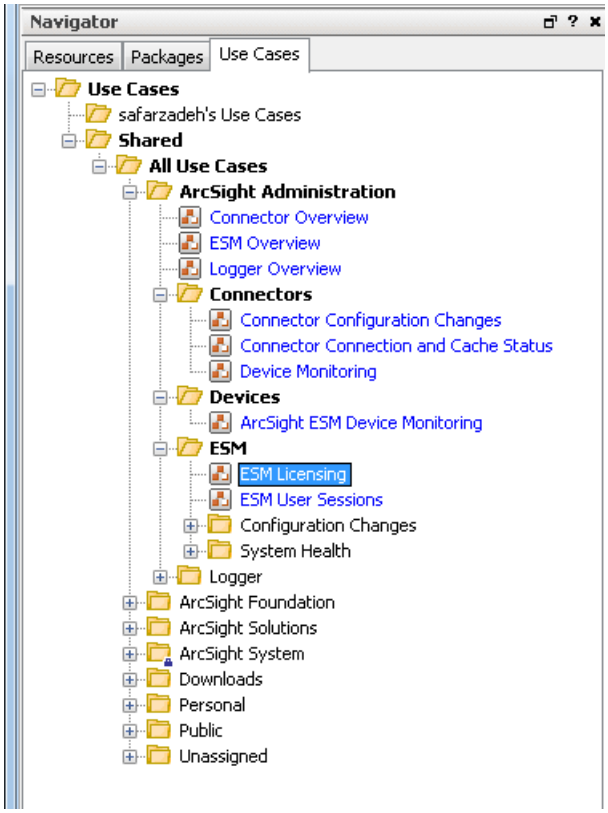
یکی از مزایای استفاده از Package این است که تمام منابع مرتبط با یک حوزه یا زمینه خاص را به‌صورت یک واحد کنار هم قرار می‌دهد. به‌عنوان مثال (شکل 39) برای تهدیدات داخلی می‌توان یک Package تهیه کرد و در این Package، منابع گزارش‌های سفارشی برای این حوزه از تهدیدات، کانال فعال با مشخصات متناسب با تهدیدات داخلی، مجموعه فیلتر و فیلدهای متناسب با این نوع تهدیدات و رویدادهای آن‌ها را قرار داد. برخی از تولیدکنندگان مانند سیسکو برای محصولات خود و شناسایی حملات آن‌ها یا بررسی وضعیت سلامت آن‌ها Package هایی را آماده کرده‌اند. قابل ذکر است که ArcSight تنها برای بررسی وضعیت و سلامت خود محصول Package ارائه کرده است و برای شناسایی حملات و تهیه گزارش از آن‌ها یا تعریف کانال فعال Package روی محصول قرار نمی‌دهد. در صورت تمایل این Packageها باید خریداری شوند.



شکل 39 محتویات بسته Insider Threat

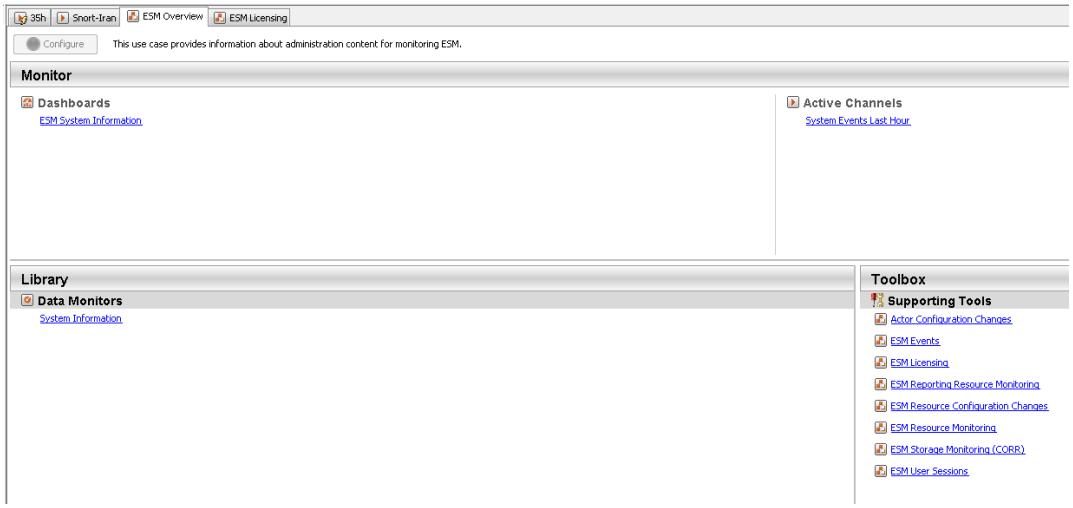
3-2-1-1-4 Use Cases

مجموعه‌ای از محتویات مرتبط که بیان‌گر یک مسئله امنیتی است را یک Use Case می‌گویند. این مجموعه می‌تواند شامل تمام منابعی باشند که به نحوی با رخداد امنیتی که پیش آمده است مرتبط هستند. فهرست Use Caseهای پیش‌فرض محصول در شکل 40 نمایش داده شده است.



شکل 40 فهرست موارد کاربرد

به‌عنوان مثال شکل 41 منابعی چون داشبورد، کانال فعال، مجموعه ابزار و پایش‌گر داده را در Use Case به نام ESM Overview دسته‌بندی کرده است.



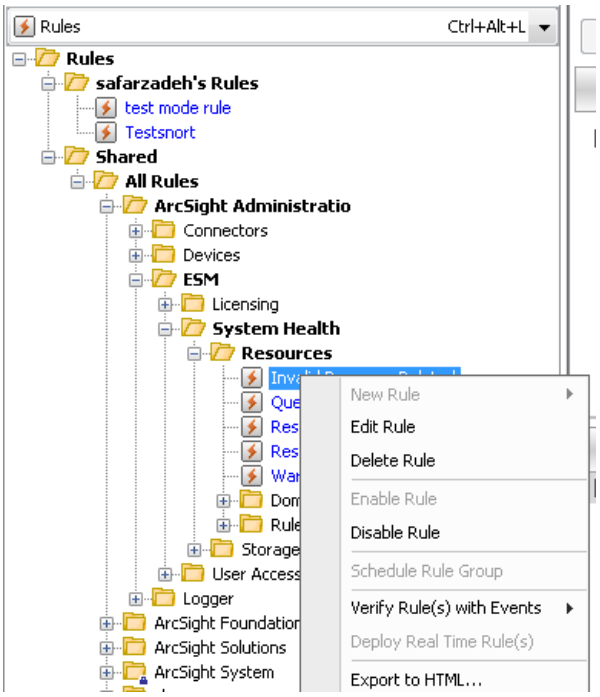
شکل 41 محتویات یک مورد کاربرد

Viewer 3-1-1-4

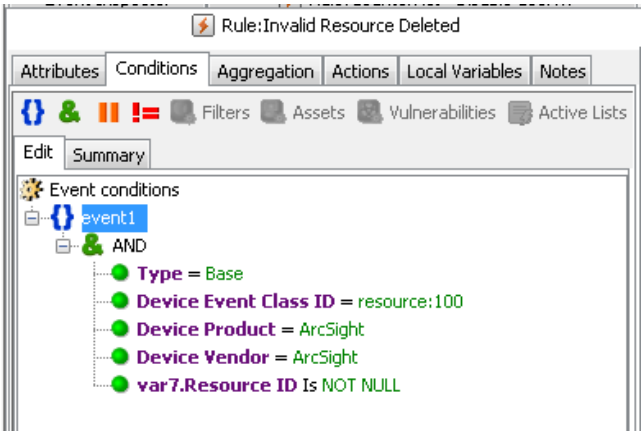
نمایش‌های مختلفی از رویدادها و نتایج تحلیل‌هایی که روی آن‌ها انجام شده است، در این بخش ارائه می‌شود. در بخش 6-1-5 نمونه‌هایی از این نتایج ارائه شده است. در ادامه با معرفی قابلیت‌های محصول نتایجی که در بخش Viewer نمایش داده می‌شود را بیشتر ملاحظه خواهید کرد.

Inspect/Edit 4-1-1-4

برای تغییر یا تعریف ویژگی‌های منابع یا مشاهده جزئیات رویدادها مورد استفاده قرار می‌گیرد. به‌عنوان مثال همان‌طور که در شکل 43 نمایش داده شده است، امکان تغییر مشخصات قانون Invalid Resource Deleted (شکل 42) وجود دارد. در ادامه با معرفی قابلیت‌های محصول با نمونه‌های بیشتری در بخش Inspect/Edit مواجه خواهیم شد.



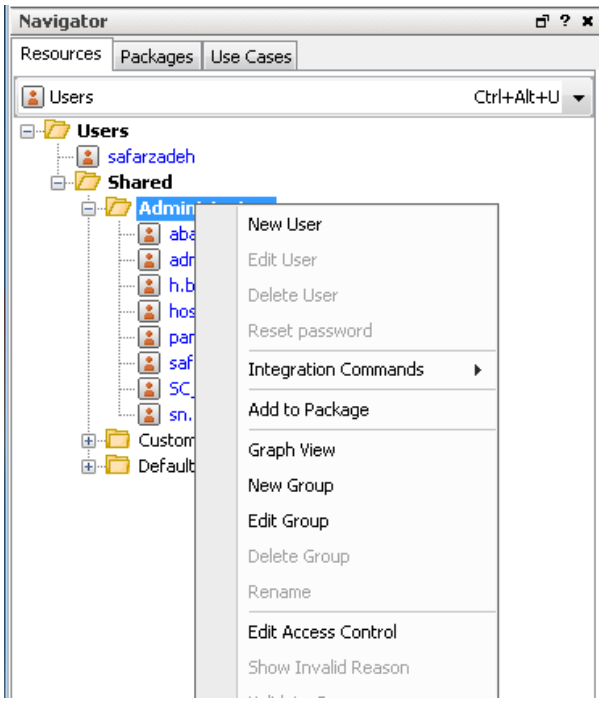
شکل 42 انتخاب قانون برای تغییر مشخصات



شکل 43 مشخصات قانون انتخاب شده در صفحه Inspect/Edit

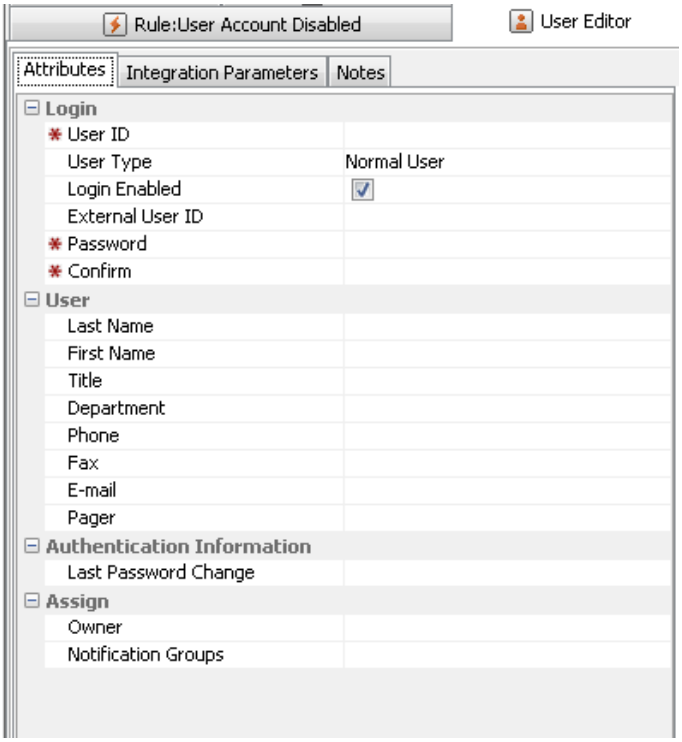
5-1-1-4 تعریف کاربر

برای تعریف کاربر جدید از برگه Resources گزینه Users را انتخاب کرده، سپس روی فولدری که قرار است کاربر جدید در آن ایجاد شود راست کلیک کرده و گزینه New User را انتخاب می‌کنیم (شکل 44).



شکل 44

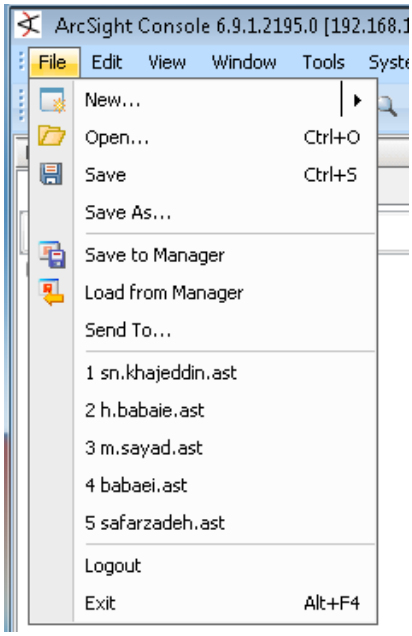
سپس در بخش Inspect/Edit (شکل 45) مشخصات کاربر را وارد کرده و گزینه Apply را انتخاب می‌کنیم.



شکل 45 تعریف مشخصات کاربر جدید

6-1-1-4 خروج از محصول

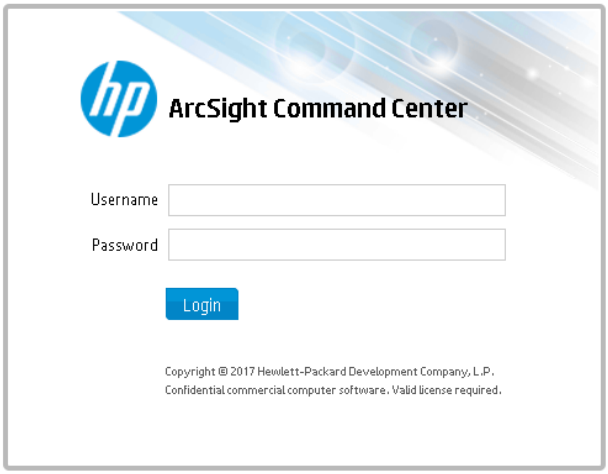
برای خروج از محیط کنسول محصول روی File (شکل 46) در بخش منوهای محصول کلیک کرده و گزینه Log Out را انتخاب می‌کنیم.



شکل 46 خروج از محصول

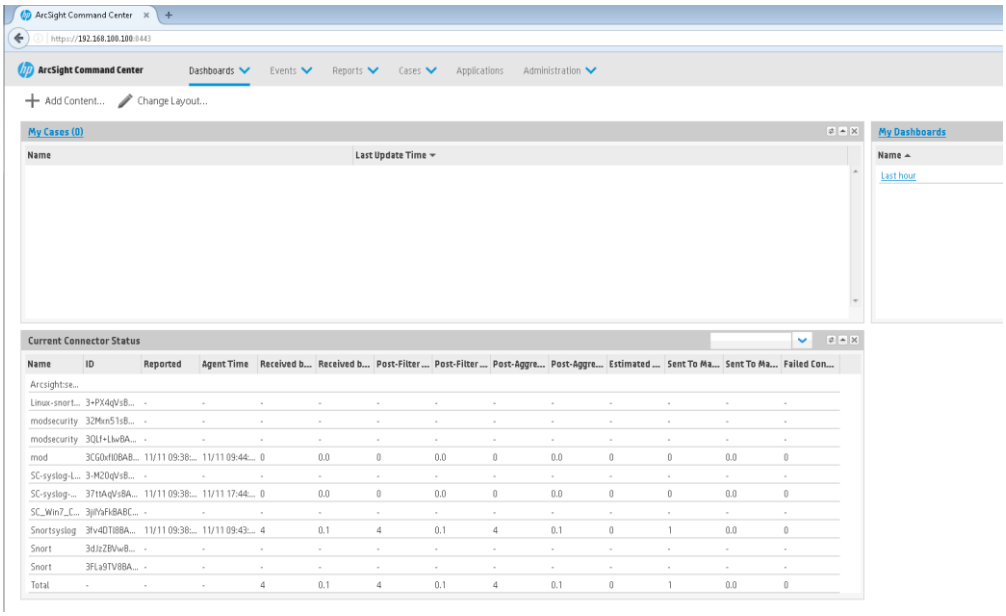
2-4 دسترسی به محصول از طریق Command Center

در مرورگر وب آدرس IP یا نام ESM را وارد کرده و در ادامه شماره درگاه 8443 را به آن الحاق کنید. مانند https://192.168.100.100:8443 به صفحه اول که در شکل 47 نمایش داده شده است، هدایت می‌شوید.



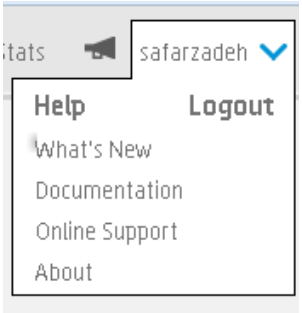
شکل 47 صفحه ورود اطلاعات حساب کاربری

اطلاعات حساب کاربری را وارد کرده، سپس به صفحه شکل 48 وارد می‌شوید.



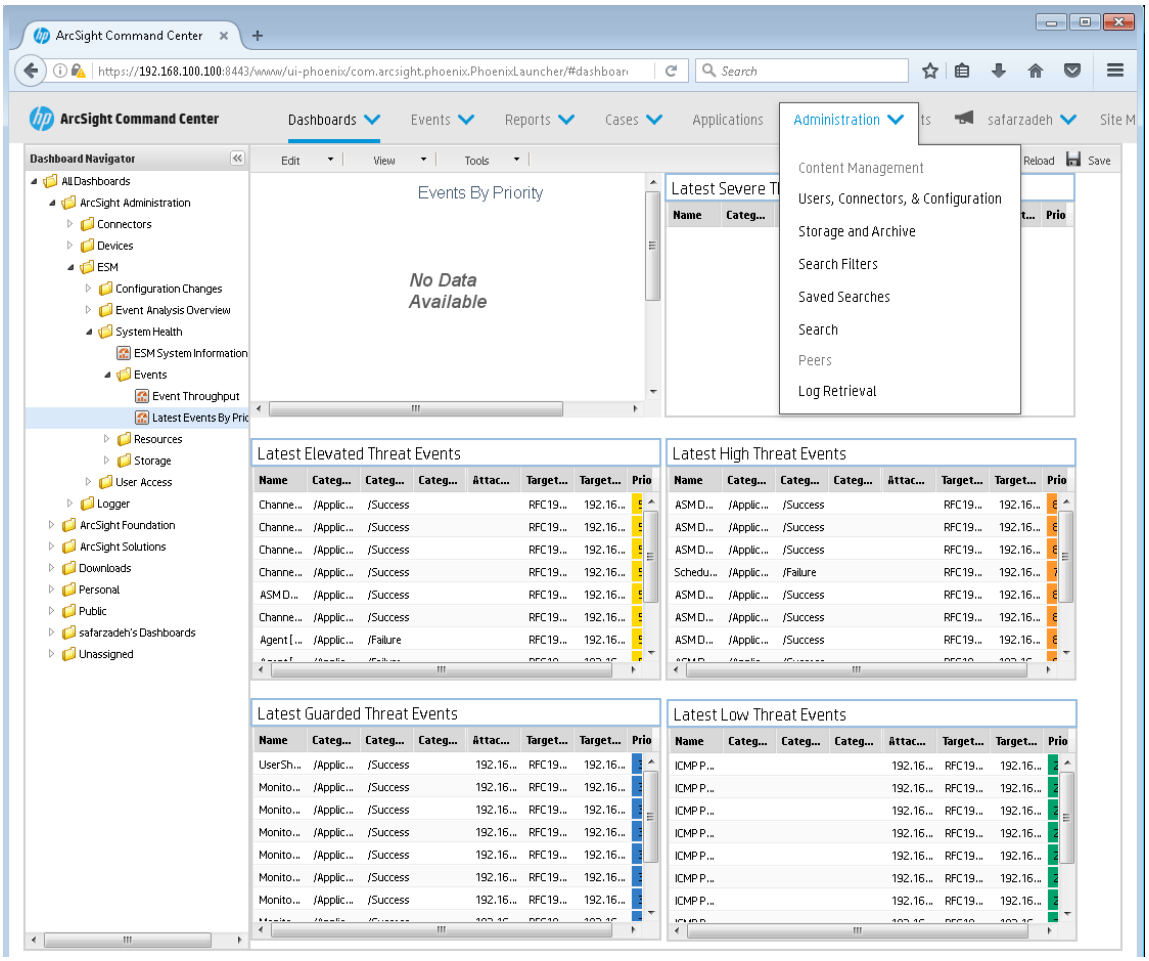
شکل 48 صفحه اول محیط Command Center

برای خروج از محیط Command Center روی نام کاربری کلیک کرده و گزینه Logout را انتخاب می‌کنیم (شکل 49).

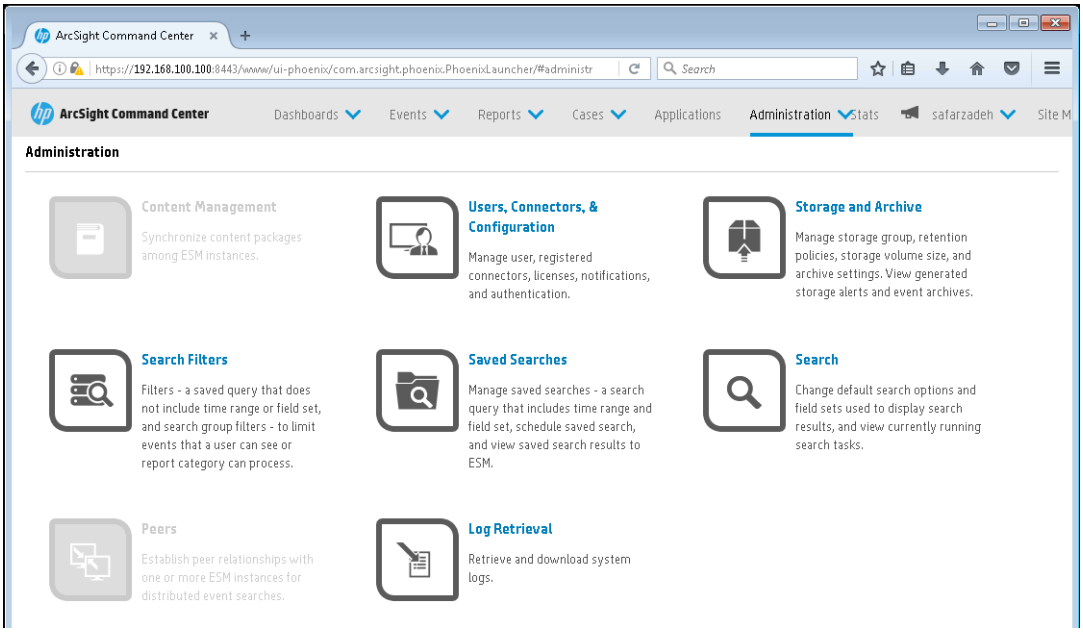


شکل 49 منوی خروج از محصول

در برگه Administration، امکان مدیریت کاربران، Connectorها، بخش ذخیره‌سازی و آرشیو، امکان جستجوی فیلترها، انجام جستجو، مدیریت جستجوهای ذخیره‌شده و بازیابی لاگ‌ها فراهم می‌شود (شکل‌های 50 و 51).

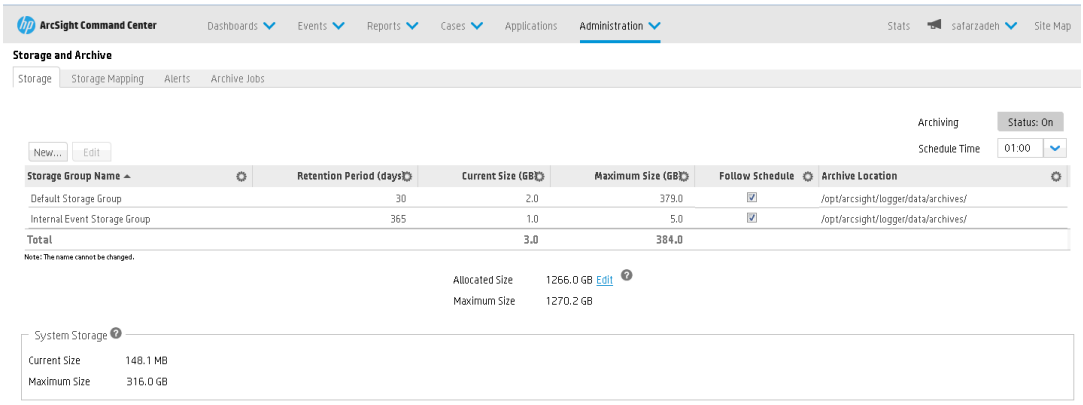


شکل 50 نمایش گزینه‌های منوی Administration



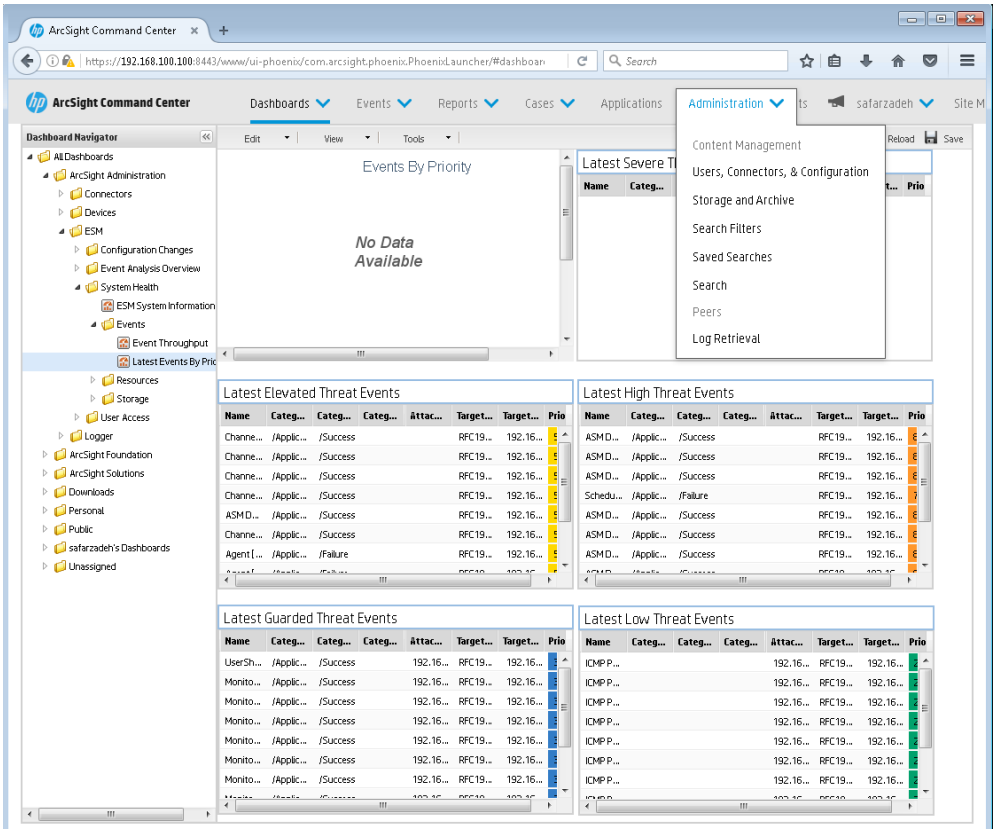
شکل 51 نمایش گزینه‌های مختلف بخش Administration

به‌عنوان مثال، در بخش ذخیره‌سازی و آرشیو حجم داده‌های ذخیره‌شده نمایش داده شده است (شکل 52).



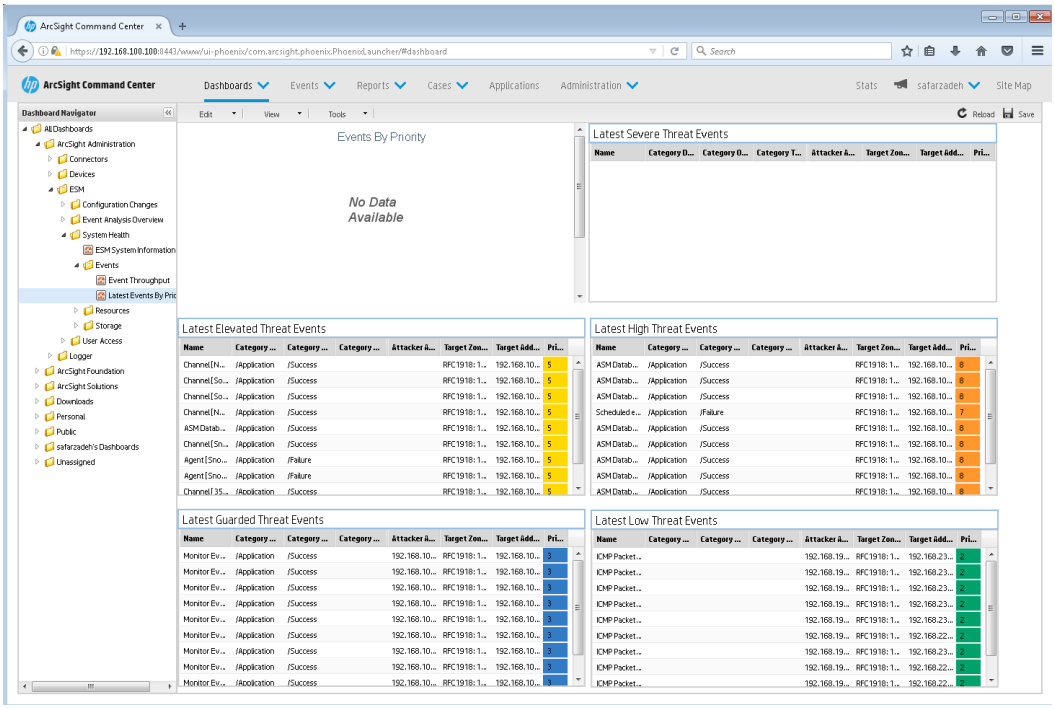
شکل 52 نمایش حجم داده‌های ذخیره شده

یکی از انواع بصری‌سازی و مشاهده خروجی انواع داشبوردها است. با انتخاب برگه داشبورد، انواع داشبوردهای موجود در بخش چپ صفحه نمایش داده می‌شوند (شکل 53).



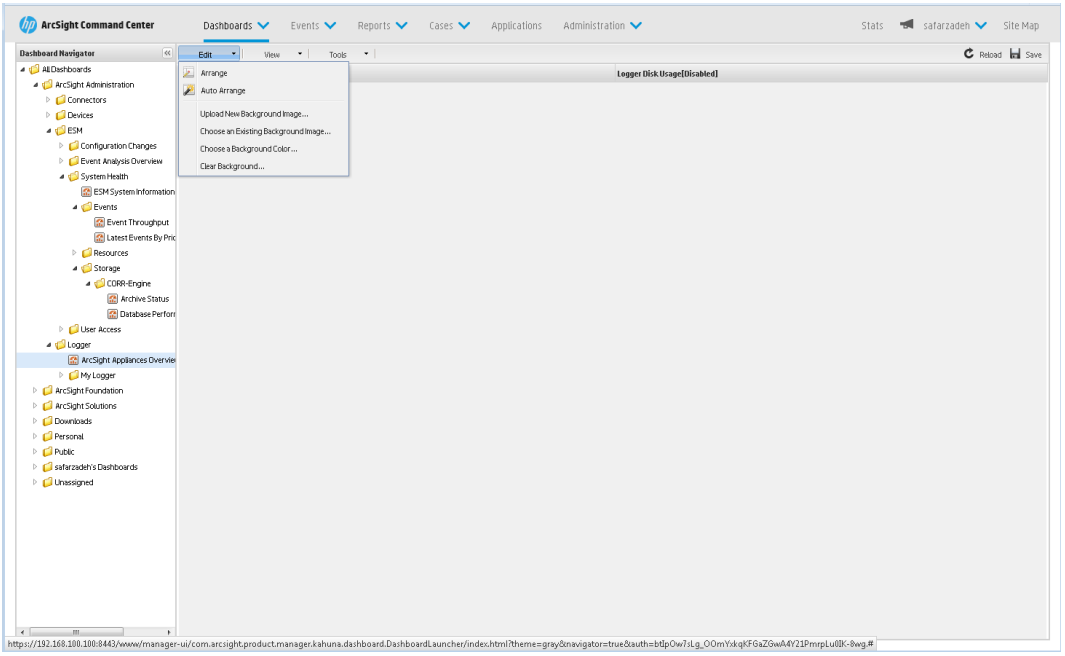
شکل 53 نمایش داشبوردهای تعریف‌شده

با انتخاب یک داشبورد صفحه مربوط به آن نمایش داده می‌شود (شکل 54).

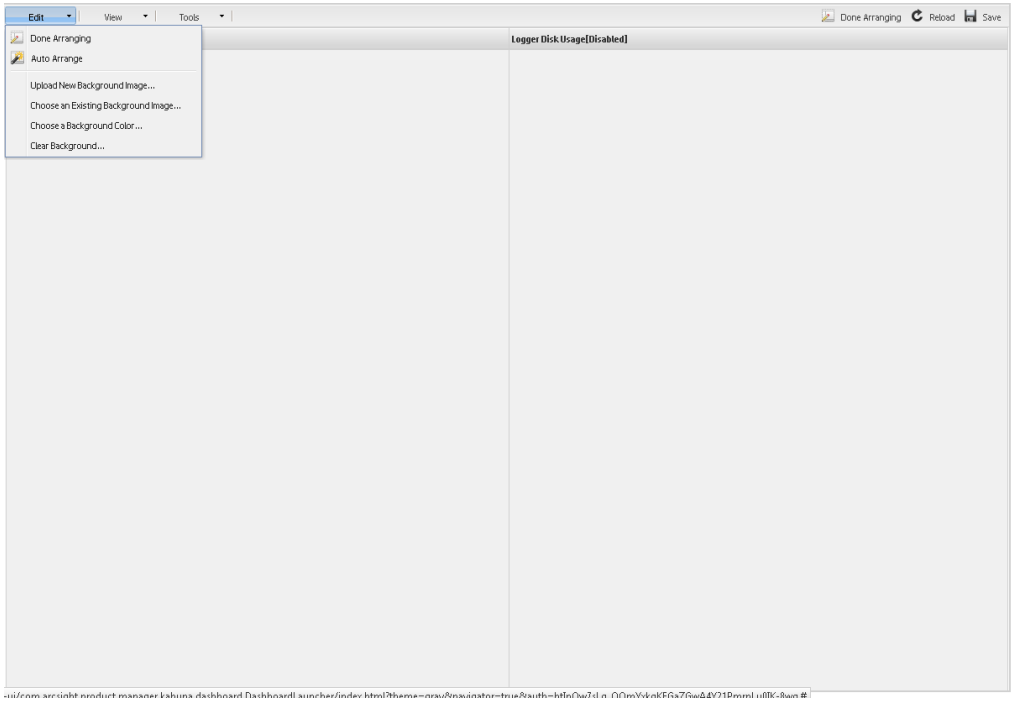


شکل 54 نمایش داشبورد Latest Events By Priority

امکان جابجاکردن بخش‌های مختلفی که در داشبورد هستند فراهم شده‌است. گزینه Edit را انتخاب کرده (شکل 55)، با انتخاب گزینه Arrange امکان جابجایی فراهم و با انتخاب Done Arranging (شکل56) جابجایی تثبیت می‌شود.

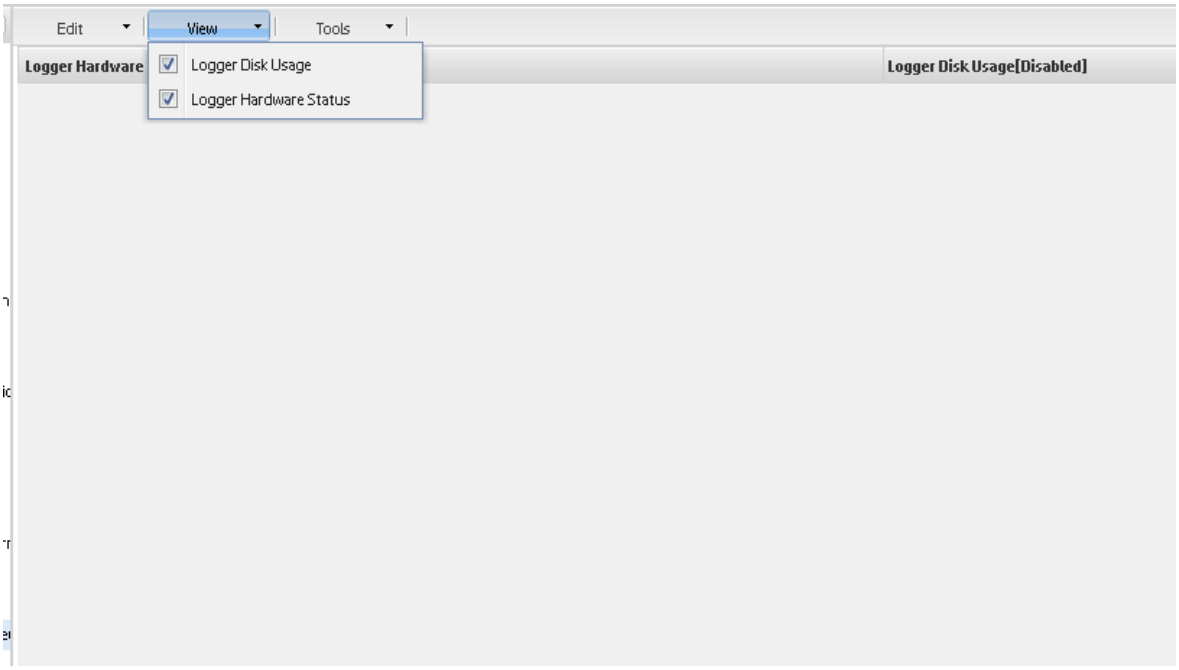


شکل 55 انتخاب گزینه Arrange برای جابجاکردن اجزای تشکیل‌دهنده داشبورد



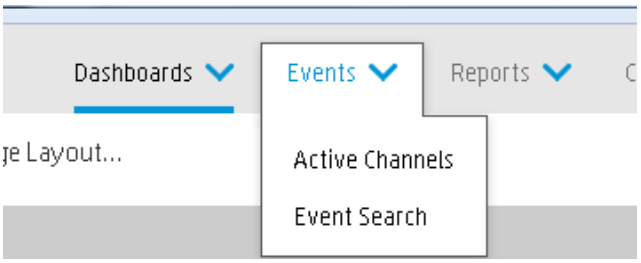
شکل 56 تثبیت جابجایی انجام شده

در بخش View می‌توان تعیین کرد که اگر داشبورد از چندین بخش تشکیل شده است، کدام‌یک از آن‌ها نمایش داده شوند (شکل 57).



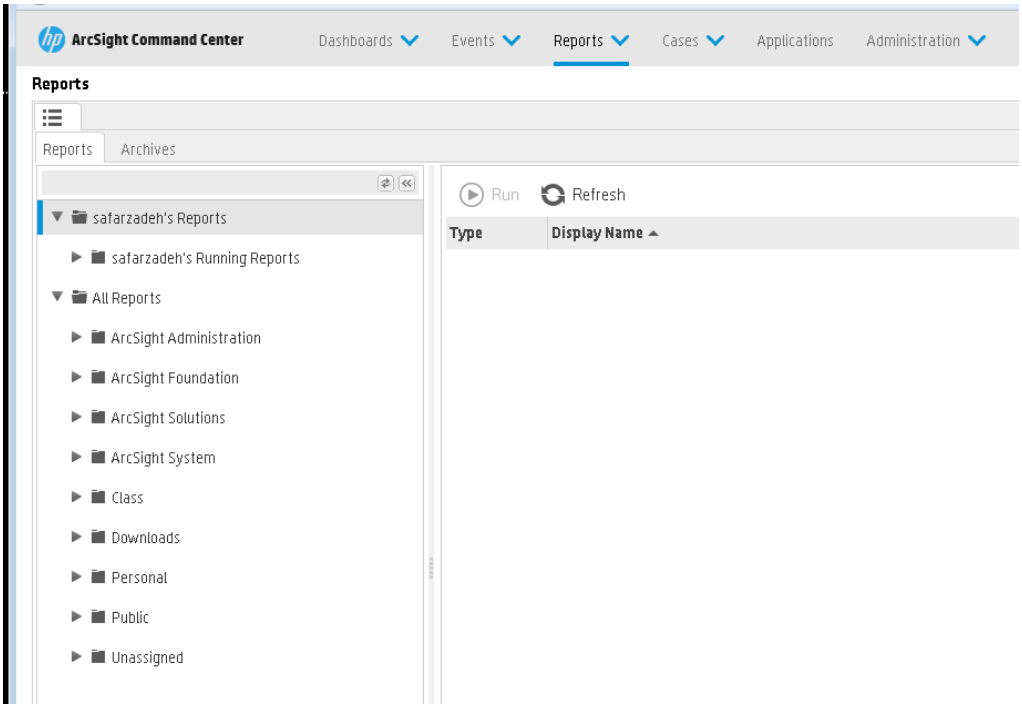
شکل 57 انتخاب اجزای قابل نمایش در صفحه

در برگه Events (شکل 58) می‌توان کانال فعال را انتخاب کرد یا می‌توان صفحه جستجوی رویداد را انتخاب کرد.



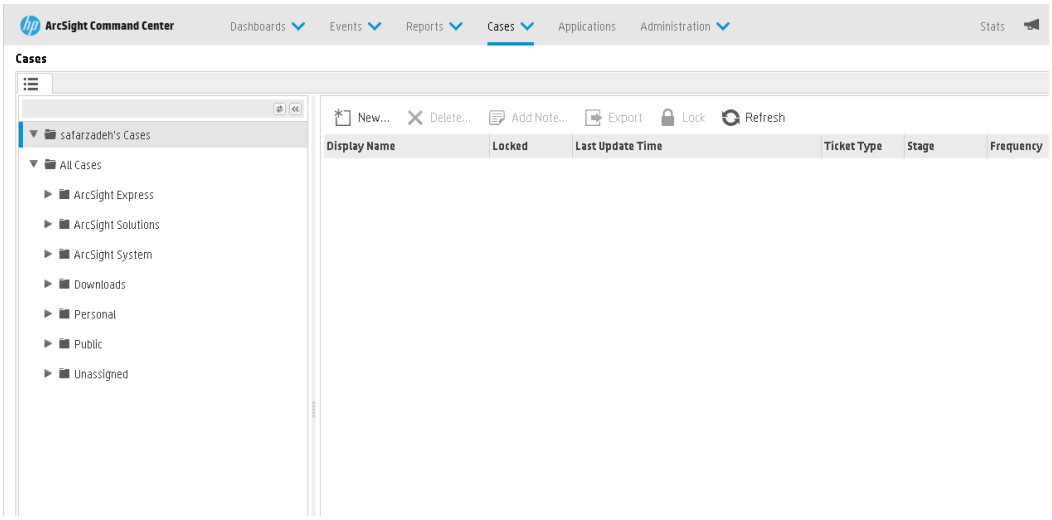
شکل 58 گزینه‌های منوی Events

با انتخاب برگه گزارش انواع گزارش‌ها نمایش داده می‌شوند (شکل 59).



شکل 59 نمایش فهرست گزارش‌های موجود

با انتخاب Cases موارد ایجاد شده نمایش داده می‌شوند.



شکل 60 نمایش فهرست موارد موجود

5 مراجع

[1] RepSM Plus Solution Guide
[2] ESM_101_6.9.1
[3] ESM_ArcSightConsole_UserGuide_6.9.1
[4] ESM_AdminGuide_6.9.1
[5] ESM_InstallGuide_6.9.1c
[6] https://marketplace.microfocus.com/arcsight/content/management-center-arcmc