بسمه تعالی

معرفی، آموزش نصب و پیکربندی

ManageEngine EventLogAnalyzer

فهرست مطالب

۱ مقدمه

امنیت اطلاعات و مدیریت رویدادها (SEIM[۱]) یکی از مهم‌ترین نیازهای بخش فناوری اطلاعات در هر سازمانی است. فایل‌های ثبت وقایع تولید شده توسط انواع حس‌گرها و ماشین (که توسط سیستم‌های شبکه، دستگاه‌ها و برنامه‌های کاربردی ایجاد می‌شود)، نیاز به جمع‌آوری، تحلیل، بایگانی، جست‌وجو و گزارش‌گیری برای اهداف بررسی امنیتی فناوری اطلاعات و انطباق با قوانین مختلف مانند PCI-DSS، HIPAA، FISMA، SOX، GLBA و غیره را دارند. این امر به سازمان‌ها برای مواجه شدن با انواع حملات و تهدیدات در راستای اهداف SEIM کمک می‌کند. علاوه بر این، مدیران شبکه و فناوری اطلاعات به فایل‌های ثبت وقایع تولید شده به چشم اطلاعات حیاتی برای تشخیص ناهنجاری در شبکه و مشکلات کارایی سیستم‌ها نگاه می‌کنند. تحلیل کارایی و فایل‌های ثبت وقایع، به کم شدن مدت خاموشی سیستم‌ها، افزایش کارایی شبکه و محکم کردن سیاست‌های یک سازمان کمک می‌کند.

ManageEngines's EventLogAnalyzer یکی از مقرون به صرفه‌ترین نرم‌افزارهای امنیت اطلاعات و مدیریت رویدادها (SIEM) در بازار است. با استفاده از EventLogAnalyzer تمام فرآیند مدیریت فایل‌های ثبت وقایع تولید شده شامل جمع‌آوری، تحلیل، جست‌وجو، گزارش‌گیری و بایگانی در یک میز فرمان مرکزی[۲] انجام می‌شود. به وسیله EventLog Analyzer تحلیل‌های امنیتی رویدادهای روزانه آسان‌تر و بهینه شده و دیگر فرآیندهای پر زحمت جمع‌آوری داده‌ی مناسب و تحلیل آن نیز به‌طور مؤثر و به‌صورت خودکار انجام می‌شود.

۲ معرفی

امروزه زیربنای فناوری اطلاعات و ارتباطات و سرویس‌دهنده‌ها در سازمان‌ها حجم بسیار زیادی از داده‌های فایل ثبت وقایع را به‌صورت روزانه تولید می‌کنند. داده‌های موجود در فایل ثبت، رویدادها شامل اطلاعات حیاتی است که باعث ایجاد بینش و هوشمندی بر روی رفتار کاربران، ناهنجاری‌های شبکه، زمان توقف سیستم‌ها، تخطی سیاست‌ها و تهدیدهای داخلی می‌شود. اگرچه بررسی و تحلیل دستی این حجم از اطلاعات

[۱] Security Information and Event Management

[۲] Console

شامل فایل ثبت وقایع و سرویس‌دهنده ثبت وقایع مقرون به صرفه و گواهی مواقع غیرممکن نمی‌باشد. بنابراین وجود یک سیستم تحلیل‌گر خودکار وقایع ثبت شده کاملا ضروری به نظر می‌رسد.

ManageEngines's EventLogAnalyzer یک سیستم جامع مبتنی بر وب، بی‌درنگ، پایش فایل ثبت وقایع و یک راه‌حل مدیریتی مقبول برای امنیت اطلاعات و مدیریت رویداد است که باعث می‌شود امنیت شبکه داخلی بهبود پیدا کند. هم‌چنین در تطبیق دادن با آخرین نیازهای حسابرسی IT کمک می‌کند. با استفاده از معماری بدون عامل، EventLog Analyzer می‌تواند به جمع‌آوری، تحلیل، جست‌وجوی بایگانی و گزارش‌گیری روی حجم عظیمی از فایل‌های ثبت وقایع تولید شده توسط انواع سیستم‌های عامل (شامل ویندوزی، لینوکسی و غیره)، تجهیزات شبکه (مانند سوئیچ، مسیریاب و غیره) و برنامه‌های کاربردی بپردازد.

ویژگی‌های کلیدی این محصول عبارتند از:

- جمع‌آوری، تحلیل، همبسته‌سازی، جست‌وجو، گزارش‌گیری و بایگانی داده
- اطمینان از صحت فایل
- تحلیل‌های جرم‌یابی رویداد
- پایش کاربران دارای امتیاز یا حق ویژه
- هشدارهای وقایع بی‌درنگ
- بایگانی و گزارش وقایع رویداد
- تحلیل هوشمند رویداد و تضمین پیروی از مقررات
- حسابرسی انطباق تنظیم مقررات
- تولید گزارش فوری
- چندین نوع گزارش: فعالیت‌های کاربر، روند تاریخی و غیره

۲-۱ معماری

EventLog Analyzer یک محصول جامع SIEM است که قابلیت جمع‌آوری فایل ثبت وقایع ویندوزی را به هر دو صورت روش جمع‌آوری مبتنی بر عامل[۳] و بدون عامل[٤] دارد. این دو روش برتری خاصی نسبت به یکدیگر ندارند و هر کدام دارای نقاط ضعف و قوت خود است. انتخاب نوع معماری براساس نیازهای سازمان و اولویت‌های فنی تیم طرح صورت می‌گیرد.

۲-۱-۱ جمع‌آوری گزارش مبتنی بر عامل

معماری مبتنی بر عامل به‌طور خاص برای جمع‌آوری ساده وقایع در شبکه‌های WAN از طریق دیواره‌ی آتش[۵] مفید است. معیاری که باعث استقرار عامل‌ها در جمع‌آوری گزارش می‌شود، در دسترس نبودن اتصال شبکه برقرار شده، است. هم‌چنین عامل‌ها در جمع‌آوری وقایع از دستگاه‌هایی که روی محدوده خاصی از شبکه محدود شده‌اند - مانند DMzها – مفید هستند. روش جمع‌آوری گزارش با عامل، استفاده از پردازش‌گر سرویس‌دهنده را کاهش می‌دهد و بنابراین کنترل بیشتری روی نرخ وقایع ثبت شده در ثانیه (EPS) دارد.

در شرایط زیر، به‌صورت نمونه، می‌توان از روش جمع‌آوری وقایع مبتنی بر عامل استفاده کرد:

- برای سادگی جمع‌آوری وقایع در شبکه‌های WAN.
- برای پایش تغییرات بحرانی روی فایل‌ها و پوشه‌ها از طریق ویژگی نظارت صحت فایل.
- زمانی‌که سیاست‌های امنیتی سازمان اجازه دسترسی به درگاه‌های ارتباطی WMI/DCOM در دستگاه‌های ویندوزی را نمی‌دهد. (دستگاه ویندوزی باید یک سرویس‌دهنده، کنترل‌کننده دامنه یا Workstation باشد.)

۲-۱-۱-۱ روش کار عامل‌ها

عامل به زیرساخت WMI دستگاه دسترسی دارد. WMI یک زیرساخت مدیریتی است که مدیران شبکه را قادر می‌سازد تا بتوانند اشیاء روی یک شبکه را پایش و کنترل کنند. WMI کوتاه شده Windows

---

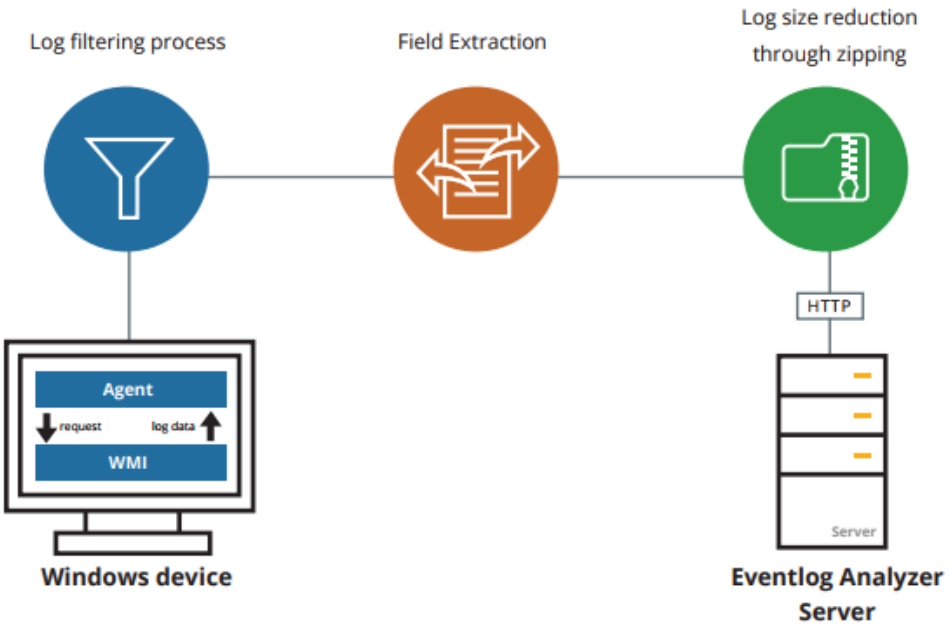
[۳] Agent-based Collection

[٤] Agentless Collection

[۵] Firewall

Management Instrumentation است و در تمامی سیستم‌عامل‌های ویندوز قابل استفاده است. به‌منظور خودکار کردن فرآیندهای امنیتی، می‌توان یک برنامه یا اسکریپت WMI نوشت و آن را به‌صورت محلی و با راه دور به کار برد. با یک پرس‌وجوی WMI می‌توان سیستم‌ها را بر حسب مشخصه خاصی از آن‌ها فیلتر کرد. هدف WMI این است که برای هر برنامه یا اسکریپتی که می‌خواهد به‌صورت محلی یا راه دور به اطلاعات مدیریتی یک سیستم، شبکه یا برنامه دسترسی داشته باشد، رابط یکسان و واحدی را فراهم کند. همه رابط‌های WMI بر پایه COM بنا شده‌اند.

عامل‌ها در EventLog از طریق پرس‌وجوی WMI مستقیما جزئیات فایل ثبت وقایع را مشاهده می‌کنند. زمانی‌که داده‌های فایل ثبت وقایع جمع‌آوری شد، عامل پیش‌پردازشی را انجام می‌دهد که شامل فیلتر کردن وقایع مانند استخراج فیلدها قبل از فشرده کردن فایل‌های ثبت وقایع و ارسال آن‌ها به EventLog Analyzer است. سپس بعد از پردازش در این مرحله، سرویس‌دهنده تنها نیاز دارد که وقایع را اندیس‌گذاری کند تا برای گزارش‌ها و هشدارهای بی‌درنگ آماده شود.



شکل ۱- معماری جمع‌آوری فایل ثبت وقایع مبتنی بر عامل

۲-۱-۲ پیکربندی معماری جمع‌آوری وقایع با روش مبتنی بر عامل

با استفاده از EventLog Analyzer فرآیند پیکربندی و مدیریت عامل‌ها برای جمع‌آوری وقایع بسیار ساده است. EventLog Analyzer داده‌های فایل ثبت وقایع را به‌صورت پیش‌فرض از طریق معماری بدون عامل

جمع‌آوری می‌کند. حتی در صورتی‌که معماری مبتنی بر عامل باشد و عامل‌ها نصب نشده باشند نیز EventLog Analyzer به‌صورت خودکار روی معماری بدون عامل تغییر وضعیت می‌دهد.

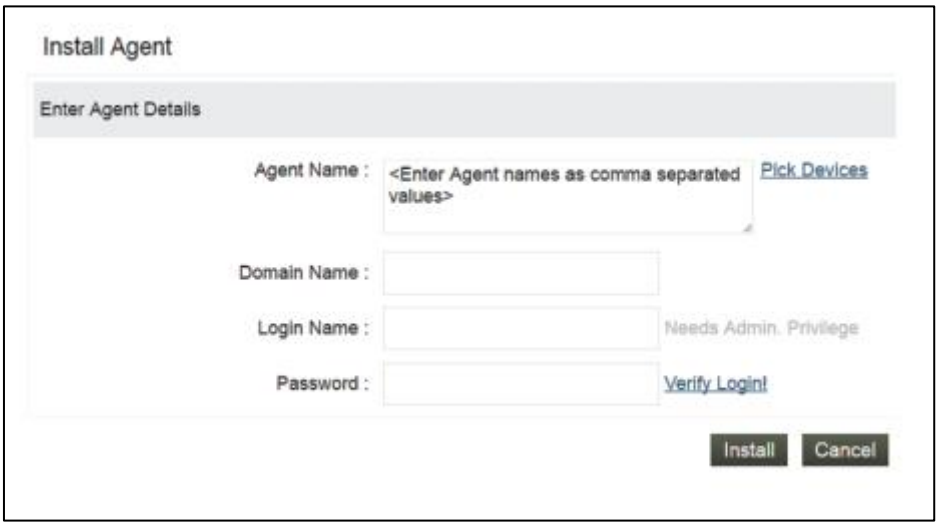
برای پیکربندی عامل ها باید مراحل زیر را انجام داد:

۱. در زبانه Setting قسمت Admin Setting را انتخاب کرده و روی لینک Install Agent کلیک کنید.
۲. نام دستگاه‌ها را برای هر عاملی که نصب می‌شود وارد کنید. در صورتی‌که هنوز دستگاه به EventLog Analyzer اضافه نشده است، در هنگام نصب عامل به‌صورت خودکار نصب خواهد شد. برای وارد کردن نام چندین دستگاه، آن‌ها را با کاما فاصله‌گذاری کنید.

توجه کنید که یک عامل می‌تواند از حداقل ۲۵ دستگاه ویندوزی فایل ثبت وقایع تهیه کند. دستگاه‌ها قابل حذف یا اضافه شدن در یک عامل هستند.

۳. اعتبارنامه مدیر دستگاه را وارد کنید.
٤. ابتدا روی Verify Login کلیک و سپس Install را انتخاب کنید.

EventLog Analyzer به‌صورت خودکار عامل‌های نصب شده روی دستگاه‌ها را پیدا کرده و داده‌های فایل ثبت وقایع را به دست می‌آورد.



شکل ۲- نصب عامل

موارد قابل توجه:

- عامل‌ها می‌توانند توسط GPO[۶] با استفاده از فایل EventLogAgent و اسکریپت InstallEventLog.vbs که در مسیر lib\native در پوشه‌ی Installation موجود است، نیز نصب شوند.
- در صورتی‌که نصب عامل به دلیل مشکلات اتصال شبکه با مشکل مواجه شد، عامل را می‌توان به‌صورت دستی نصب کرد. در این صورت از طریق دانلود فایل MSI که در صفحه مدیر عامل موجود است، می‌توان عامل را به‌صورت مستقیم روی دستگاه نصب کرد.
- زمانی‌که یک دستگاه برای پایش صحت پیکربندی می‌شود عامل به‌صورت خودکار روی دستگاه نصب می‌شود.

۲-۱-۲-۱ مدیریت عامل

عامل‌های نصب شده با استفاده از پیوند Agent Administration در بخش Admin Setting به‌سادگی قابل مدیریت هستند.

شکل ۳- صفحه مدیریت عامل‌ها

در این صفحه، دستگاه‌های اضافه شده به عامل، وضعیت سرویس عامل با گزینه های شروع، خاتمه و راه‌اندازی مجدد قابل مشاهده هستند. هم‌چنین می‌توان عامل را حذف یا ویرایش کرد و یا دستگاه هایی را به عامل حذف یا اضافه کرد.

مدیریت عامل به‌صورت از راه دور نمی‌تواند صورت بگیرد مگر این‌که اتصال شبکه‌ای بین عامل و EventLog Analyzer برقرار شود.

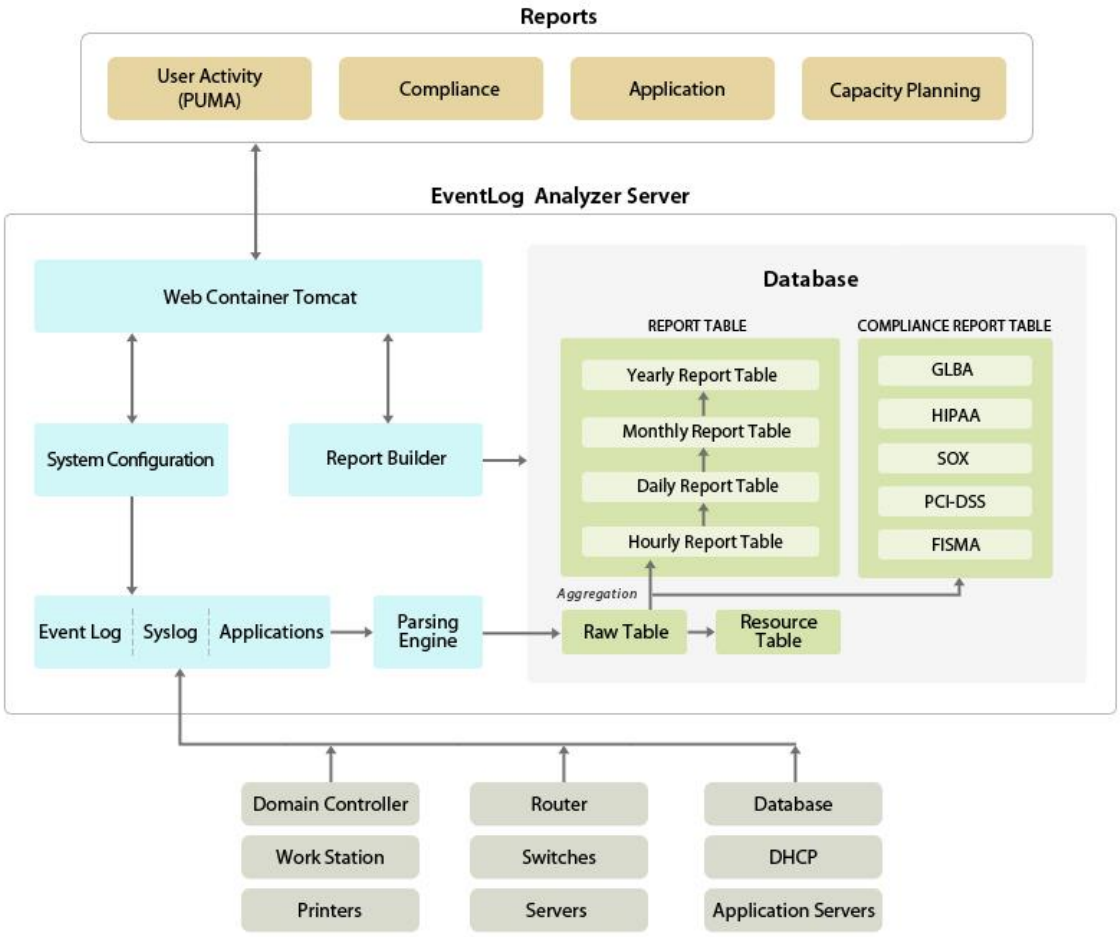
---

[۶] Group Policy Object

۲-۱-۳ جمع‌آوری وقایع بدون عامل

به‌صورت پیش‌فرض، معماری این محصول بدون عامل است که از سرویس‌هایی مانند syslog و سرویس دهنده ثبت رخداد موجود در آن برای ذخیره گزارش رخدادها و هم‌چنین رخدادهای سیستمی به دست آمده از تمام دستگاه‌های پیکربندی شده استفاده می‌کند. این امر به مدیر شبکه کمک می‌کند تا بتواند به تحلیل مشکلات سیستمی بپردازد، امنیت شبکه را ارتقاء دهد، مدت زمان خاموشی سرویس‌دهنده، کنترل‌کننده دامنه و ایستگاه‌های کاری، مسیریاب‌ها و سوییچ‌های شبکه را کاهش دهد. گزارش‌های جمع‌آوری شده تجزیه می شوند و به پایگاه‌داده موجود PostgreSQL برای تحلیل و گزارش‌گیری فرستاده می‌شود.

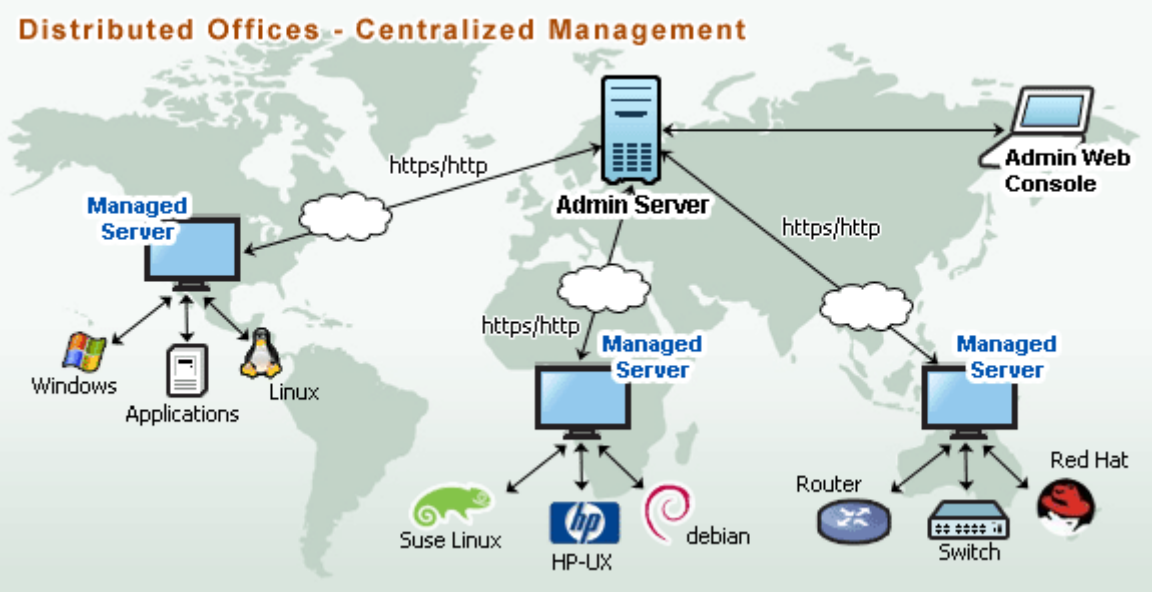
شکل ٤ معماری EventLog Analyzer با روش بدون عامل را نشان می‌دهد.



شکل ٤- معماری جمع‌آوری فایل ثبت وقایع بدون عامل

۲-۱-٤ معماری نسخه توزیع‌شده

نسخه توزیع‌شده[۷] این محصول شامل یک سرویس‌دهنده مدیر[۸] و تعدادی سرویس‌دهنده مدیریت‌شده[۹] است. سرویس‌دهنده‌های مدیریت‌شده در نقاط مختلف جغرافیایی (یکی به ازای هر محیط LAN) نصب می‌شوند و به سرویس‌دهنده مدیر متصل می‌شوند. بدین وسیله مدیر شبکه قادر به دست‌یابی به جزئیات وقایع برنامه‌ها/میزبان‌های نقاط مختلف جغرافیایی در یک مکان مرکزی خواهد بود. تمامی گزارش‌ها، هشدارها و سایر اطلاعات برنامه‌ها/میزبان‌ها از طریق یک میز فرمان مرکزی قابل دسترسی خواهد بود. سازمان‌های بزرگ که چندین شعبه در نقاط مختلف دارند می‌توانند از این نوع معماری سود زیادی ببرند. شکل ۵ معماری توزیع‌شده محصول EventLog Analyzer را نمایش می‌دهد.



شکل ۵- معماری نسخه توزیع‌شده

[۷] Distributed Edition

[۸] Admin Server

[۹] Managed Server

۳ قابلیت‌های EventLog Analyzer

EventLog Analyzer یکی از محصولات جامع SIEM است که امکاناتی نظیر مدیریت وقایع شبکه و برنامه‌های کاربردی، تولید گزارش و هشدار، حسابرسی مطابق با سیاست‌های IT، پایش صحت فایل‌ها، پایش کاربران و سیستم‌ها، تجزیه و تحلیل و جرم‌یابی روی فایل‌های ثبت وقایع و بسیاری از ویژگی‌های مورد نظر مدیران امنیت را فراهم کرده است. در ادامه این بخش مروری مختصر بر ویژگی‌های این محصول خواهیم داشت.

۳-۱ مدیریت فایل ثبت وقایع

فایل ثبت وقایع اطلاعات اولیه‌ای درباره فعالیت‌های شبکه را فراهم می‌کند. مدیریت فایل ثبت وقایع این اطمینان را به‌وجود می‌آورد که داده‌های پنهان شبکه موجود در وقایع به اطلاعات معناداری تبدیل شوند. مدیریت فایل ثبت وقایع اولین اقدام مدیر امنیت برای امن نگه‌داشتن شبکه است. فرآیند مدیریت فایل ثبت وقایع شامل جمع‌آوری، سیستم ذخیره امن‌شده، نرمال‌سازی، تحلیل و تولید گزارش‌ها و هشدارها می‌باشد. مدیریت فایل ثبت وقایع یکی از بخش‌های جدایی‌ناپذیر از نظارت بر امنیت شبکه است.

- **جمع‌آوری وقایع ثبت شده**

جمع‌آوری وقایع ثبت شده باید از دستگاه‌های مختلف شامل سرویس‌دهنده‌ها، برنامه‌های کاربردی و دستگاه‌های موجود در شبکه باشد (بهتر است که جمع‌آوری فایل ثبت وقایع به‌صورت بدون عامل صورت گیرد). در بعضی از شبکه‌ها جمع‌آوری فایل ثبت وقایع با عامل باید به‌صورت انتخابی وجود داشته باشد و وابسته به شرایط شبکه و ارتباطات دارد.

- **سیستم ذخیره‌سازی امن شده**

داده‌های فایل ثبت وقایع باید برای انجام تحلیل‌های جرم‌یابی روی سیستم ذخیره‌سازی امن بایگانی شوند. سیستم ذخیره‌سازی باید با مواردی مانند رمزنگاری امن شود. مدت زمان نگه‌داری و مکان نگه‌داری فایل‌های ثبت وقایع باید توسط کاربر قابل تغییر باشد.

- **نرمال‌سازی فایل ثبت وقایع**

فایل‌های ثبت وقایع منابع ناهمگن باید نرمال شوند تا یک قالب یکسان داشته باشند.

- **تولید گزارش و هشدار**

فایل‌های ثبت وقایع به‌منظور تولید گزارش و هشدار تحلیل می‌شوند. گزارش‌ها باید به‌صورت قابل تنظیم و سفارشی کردن باشد. هم‌چنین گزارش‌ها باید به‌صورت قابل توزیع و با قالب‌های مختلف برنامه‌ریزی شوند. هشدارها باید کاملا بی‌درنگ باشند. سازوکارهای اطلاع‌رسانی بیشتری باید وجود داشته باشد، بدین منظور می توان حتی از سایر برنامه‌ها در جهت اقدامات اصلاحی استفاده کرد.

- **بایگانی وقایع**

در Event Log Analayzer تمامی فایل‌های ثبت وقایع که از دستگاه‌های ویندوزی و لینوکسی مختلف جمع‌آوری می‌شوند، به‌صورت خودکار بایگانی می‌شوند. این فایل‌ها رمزنگاری می‌شوند تا امنیت این داده‌ها برای تحلیل‌های آینده حفظ شود. علاوه بر رمزنگاری از درهم‌سازی و برچسب زمانی نیز برای حفظ امنیت فایل‌ها استفاده می‌شود. به‌صورت پیش‌فرض هر ٢٤ ساعت یک بار عملیات بایگانی از فایل‌های ثبت وقایع صورت می‌گیرد و برای کاهش حجم، بعد از هفت روز این فایل‌های گردآوری شده به‌صورت فشرده (Zip) در می‌آیند. این بازه‌های زمانی قابل پیکربندی هستند. در هر زمان امکان گزارش‌گیری و استفاده از فایل‌های بایگانی‌شده موجود است.

- **تجزیه‌کننده سفارشی**

یکی از بزرگ‌ترین چالش‌های مدیریتی حوزه SIEM تحلیل وقایع از منابع مختلف است. EventLog Analyzer از اکثر منابع که فایل‌های ثبت وقایع را تولید می‌کند، پشتیبانی می‌کند و قابلیت تجزیه‌کننده سفارشی این امکان را فراهم می‌کند تا هر منبعی که فایل ثبت وقایع قابل خواندن برای انسان تولید می‌کند، توسط تجزیه‌کننده سفارشی تحلیل شود. در EventLog Analyzer می‌توان علاوه بر فیلدهای پیش‌فرض، فیلدهای جدید برای استخراج داده‌های بیشتر از فایل ایجاد کرد. مدیران امنیت و فناوری اطلاعات برای داشتن نگاهی عمیق‌تر به اطلاعات بیشتر نیاز دارند. بنابراین ایجاد فیلدهای جدید برای استخراج، برای تحلیل جرم‌یابی فایل ثبت وقایع و گزارش‌دهی می‌تواند بسیار مهم باشد. از طرفی ایجاد الگو برای استخراج فیلدهای جدید می‌تواند پیچیده باشد که این کار توسط EventLog Analyzer به‌سادگی تنها توسط چند کلیک انجام می‌شود.

۲-۳ مدیریت وقایع برنامه‌های کاربردی

EventLog Analyzer یکی از جامع‌ترین برنامه‌های مدیریت فایل ثبت وقایع، تولید گزارش، جمع‌آوری، تحلیل و همبستگی داده‌های فایل ثبت وقایع می‌باشد. مدیران امنیت می‌توانند با استفاده از این گزارش‌ها به شناسایی رفتارهای ناهنجار کاربران و عیب‌یابی برنامه‌ها و تهدیدات امنیتی بپردازند.

این محصول برنامه‌های سرویس‌دهنده وب مانند IIS و Apache، پایگاه‌داده‌ها مانند MS SQL، Oracle و غیره و بسیاری از سرویس‌ها و برنامه‌های دیگر مانند DHCP و سایرین را پایش می‌کند. علاوه بر این، به همراه تجزیه‌کننده فایل ثبت وقایع این ابزار می‌تواند هر فایل ثبت وقایع برنامه محلی یا سفارشی را تجزیه و تحلیل کند. هم‌چنین وجود هشدارهای بی‌درنگ برای هر ناهنجاری در برنامه‌ها باعث کمک به بهبود عملکرد در برابر حملات امنیتی می‌شود. از جمله قالب‌هایی که برای گزارش‌های EventLog Analyzer پشتیبانی می‌شود، می‌توان به موارد زیر اشاره کرد:

- گزارش تحلیل فایل‌های ثبت وقایع سرویس‌دهنده وب IIS W3C
- گزارش تحلیل فایل‌های ثبت وقایع MS SQL
- گزارش‌های تحلیل فایل‌های ثبت وقایع حسابرسی Oracle Live
- گزارش‌های سرویس‌دهنده‌ی وب Apache
- گزارش‌های سرویس‌دهنده Print
- گزارش‌های تحلیل فایل‌های ثبت وقایع DHCP
- و بسیاری دیگر از منابع رویدادها

۳-۳ حسابرسی مطابق با سیاست‌های IT

گزارش‌های تطبیق سیاست‌های کنترلی توسط دولت‌ها و صنایع مجاز اجبار می‌شوند تا از حداقل امنیت IT کاربران در صنایع مختلف مطمئن شوند. عدم تطابق در پنل مبتنی بر وب مشخص می‌شود. EventLog Analayzer تمامی گزارش‌های کنترلی مقررات IT صنایع که مورد نیاز است را تولید می‌کند.

شکل ٦- گزارش‌های تطابقی موجود در EventLog analyzer

عمده سیاست‌هایی که EventLog Analyzer گزارش‌های از پیش تعریف شده آن‌ها را آماده کرده است، شامل PCI-DSS، ISO 27001:2013، HIPPA، FISMA، SOX، GPG13 و GLBA است. گزارش‌های کنترلی تطبیق با سیاست‌های IT می‌توانند با توجه به نیازهای سازمان تغییر یابند. هم‌چنین به مقررات کنترلی IT در

آینده نیز توجه شده است و به همین منظور امکان ایجاد گزارش تطبیقی جدید از طریق کلیک روی دکمه ADD+ فراهم شده است.

گزارش‌های تطبیقی می‌توانند به‌وسیله‌ی گروه‌ها و یا زیرگروه‌های فعالیت‌های تطبیقی، یا به‌وسیله‌ی دستگاه‌های موجود در شبکه فیلتر شوند.

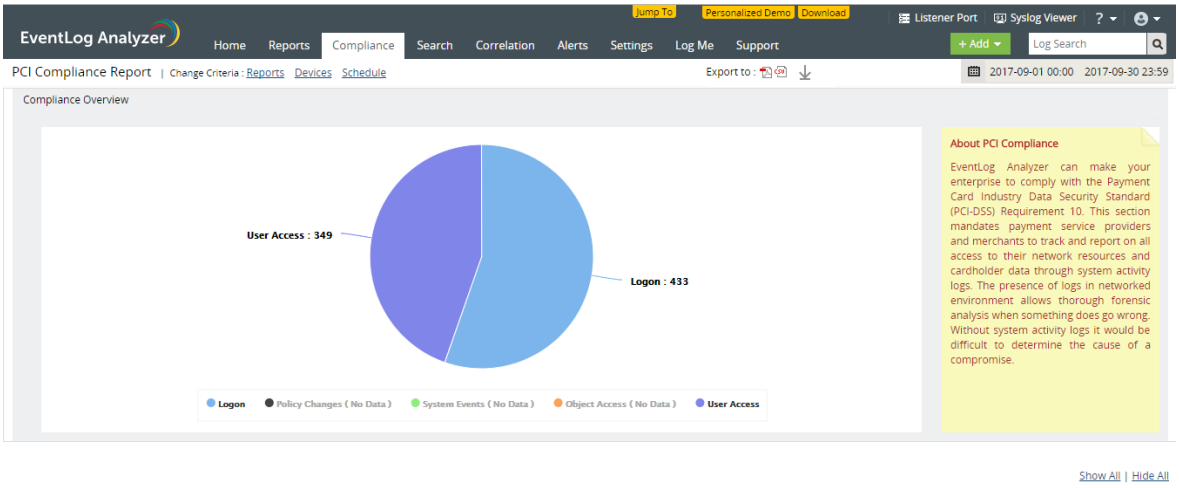
گزارش‌ها برای فایل‌های ثبت وقایع ویندوزی و syslogهای لینوکسی می‌توانند تولید شوند. هم‌چنین گزارش‌ها با قالب‌های مختلف HTML، PDF و یا CSV منتشر می‌شوند.

۳-۳-۱ گزارش PCI-DSS

PCI-DSS[۱۰] (استاندارد امنیت داده برای صنایع کارت‌های اعتباری) یک راهنما برای هر سازمانی است که داده‌های کارت اعتباری مشتریان را پردازش، نگه‌داری و یا انتقال می‌دهد.

EventLog Analyzer نیازمندی‌های بخش ۱۰ سیاست PCI-DSS را تضمین می‌کند. بخش ۱۰، آن دسته از فراهم‌کننده‌های سرویس‌دهنده‌های اعتباری و بازرگانان را ملزم می‌کند تا تمامی دسترسی‌هایشان به منابع شبکه و داده‌های صاحب کارت، از طریق فایل ثبت وقایع، گزارش و پیگیری شوند. زمانی‌که اتفاق نادرستی در شبکه می‌افتد، وجود فایل‌های ثبت وقایع اجازه جرم‌یابی و تحلیل برای پیدا کردن نقطه اشتباه را می‌دهند. بدون سیستم فعالیت فایل ثبت وقایع، پیدا کردن نقطه اشتباه بسیار سخت می‌باشد.

[۱۰] Payment Card Industry - Data Security Standards



شکل ۷- گزارش تطابقی PCI-DSS

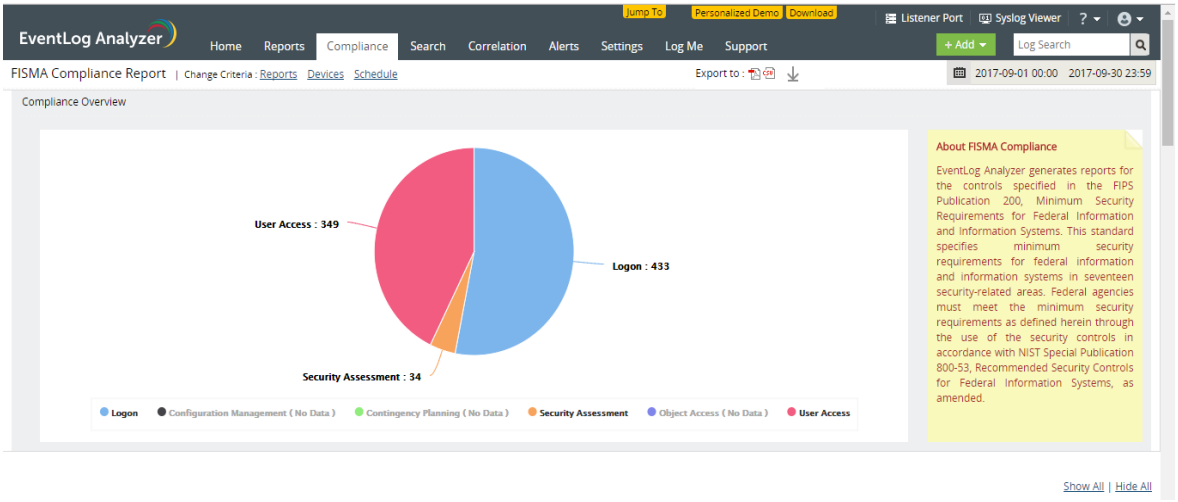
فایل‌های ثبت وقایعی که رویدادهای زیر را دنبال می‌کنند، لازم هستند:

- دسترسی کاربران (PCI-DSS requirements 10.1 & 10.2.2)
  - فعالیت‌های فردی کاربر
- ورود به سیستم (PCI-DSS requirements 10.2.1 & 10.2.3)
  - ورود به سیستم موفق
  - خروج از سیستم موفق
  - ورود به سیستم ناموفق
  - ارتباطات راه دور
- تغییرات سیاست (PCI-DSS requirements 10.2.3)
  - تغییرات سیاست کاربران
  - تغییرات سیاست دامنه
  - تغییرات سیاست بازبینی
- رویدادهای سیستم (PCI-DSS requirements 10.2.6)
  - فایل‌های ثبت وقایع سیستم
  - بازبینی فایل‌های ثبت وقایع پاک شده
- دسترسی اشیا (PCI-DSS requirements 10.2.7)
  - ایجاد شیء
  - اصلاح شیء

- حذف شیء
- مدیریت شیء
- دسترسی شیء

۳-۳-۲ گزارش FISMA

تمامی دفاتر دولتی، پیمانکاران دولتی و سازمان‌هایی که تبادل داده با سیستم‌های دولتی دارند باید راهنمای تطبیقی FISMA[۱۱] (مقررات مدیریت امنیت اطلاعات فدرال) را رعایت کنند. سازمان‌ها باید به پایش و حفظ و نگه‌داری رکوردهای بازبینی تمامی رویدادهای امنیتی بپردازند.



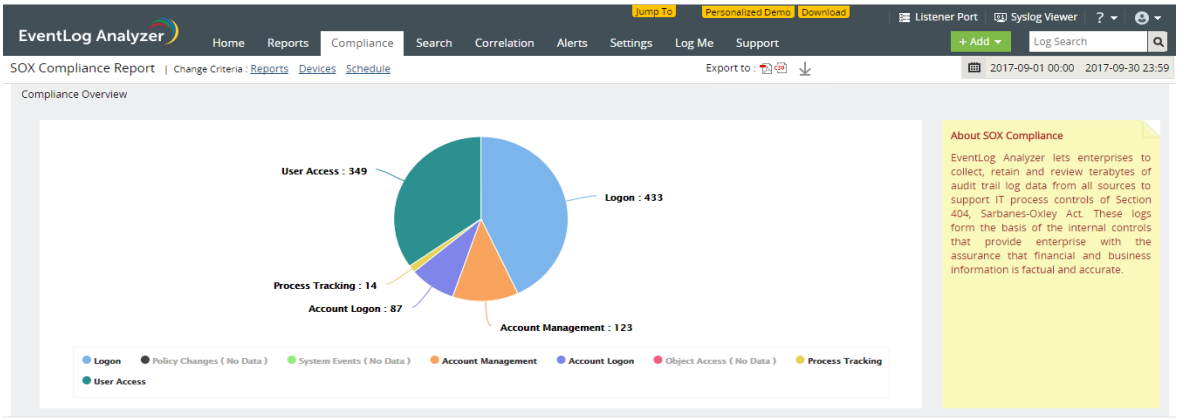
شکل ۸- گزارش تطابقی FISMA

EventLog Analyzer گزارش‌هایی برای کنترل‌های مشخص شده در FIPS publication 200 حداقل امنیت لازم برای اطلاعات فدرال و سیستم‌ها را تولید می‌کند.این استاندارد حداقل امنیت لازم برای اطلاعات فدرال و سیستم‌ها را در حوزه‌های امنیتی مشخص می‌کند

[۱۱] Federal Information Security Management Act

۳-۳-۳ گزارش SOX

استاندارد SOX[۱۲] به تمام شرکت‌های دولتی و شرکت‌های حسابداری عمومی نیاز دارد تا صحت گزارش مالی حسابرسان را به آن‌ها نشان دهد.



شکل ۹- گزارش تطابقی SOX

EventLog Analyzer به سازمان‌ها در جمع‌آوری، نگه‌داری، و بازبینی حجم زیادی از فایل‌های ثبت وقایع (ترابایت‌ها) از تمامی منابع برای پشتیبانی کنترل‌های بخش 404 استاندارد SOX کمک می‌کند. این فایل‌های ثبت وقایع سازمان‌ها را از اطلاعات تجاری و عملیات مالی واقعی و دقیق مطمئن می‌سازد.

۳-۳-٤ گزارش HIPAA

مقررات HIPPA[۱۳] (قانون مسئولیت و انتقال بیمه سلامت) آن دسته از مراقبت‌های سلامتی که اطلاعات بیمار را به‌صورت الکترونیکی مبادله می‌کند تحت تأثیر قرار می‌دهد. مقررات HIPPA به‌منظور محافظت درستی و امنیت اطلاعات درمان دایر شده است. حفاظت اطلاعات می‌تواند در برابر استفاده غیر مجاز یا افشاء اطلاعات صورت گیرد. HIPPA بیان می‌کند که فرآیند مدیریت امنیت به‌منظور محافظت در برابر دسترسی موفق غیرمجاز یا تلاش برای دسترسی، استفاده، افشاء، اصلاح و یا استنتاج اطلاعات با استفاده از فعالیت‌های سیستم، باید وجود داشته باشد.

[۱۲] Sarbanes Oxley

[۱۳] Health Insurance Portability and Accountability Act

EventLog Analyzer به‌سادگی می‌تواند به پایش فعالیت‌های درون و پیرامون دستگاه‌ها (مانند IDS) بپردازد. از طرفی مقررات HIPPA تحلیل تمام فایل‌های ثبت وقایع مربوط به سیستم‌عامل و برنامه‌های کاربردی را اجبار می‌کند.

۳-۳-۵ گزارش GLBA

مقررات GLBA[۱۴] هر مؤسسه مالی را ملزم می‌کند تا به‌منظور حفاظت از اطلاعات شخصی خصوصی در برابر تهدیدها، سیاست‌ها و فرآیندهایی را در نظر بگیرد. ضروری است که برای محافظت در برابر دسترسی غیرمجاز یا تلاش برای دسترسی، افشاء، اصلاح و یا سوءاستفاده و استنتاج از سوابق مشتری باید یک فرآیند مدیریت امنیت وجود داشته باشد. به عبارت دیگر لازم است، که توانایی پایش، گزارش‌دهی و هشدار نسبت به دسترسی موفق غیرمجاز به برنامه‌ها یا سیستم‌هایی که اطلاعات حساس مشتری روی آن ذخیره شده است را داشته باشد.

EventLog Analyzer به تطبیق دادن قانون مدرنیزاسیون خدمات مالی[۱۵] (FMA99) که معمولا با عنوان قانون GLBA شناخته می‌شود، کمک می‌کند. تیتر پنجم از قانون، حاکی از مراحلی است که مؤسسات مالی و شرکت‌های خدمات مالی باید متعهد شوند تا امنیت و محرمانه بودن اطلاعات مشتری را تضمین کنند. این قانون معتقد است که شرکت‌های خدمات مالی باید به‌صورت منظم اطلاعات شخصی خصوصی را از افراد جمع‌آوری کند و در هنگام به اشتراک‌گذاری با خارج از شرکت، اطلاع‌رسانی کند. هم‌چنین در مواردی که از اطلاعات در شرایط خاص، مانند پیشبرد یک معامله خاص مالی، استفاده می‌شود باید اطلاع‌رسانی شود.

۳-۳-۶ گزارش ISO 27001

استانداردهای ISO 27001:2013 سازمان‌ها را قادر می‌سازد تا با محافظت از اطلاعات کسب و کار خود و مدیریت و به حداقل رساندن مخاطرات خطرناک شبکه سازمان، نیازهای سیستم مدیریت امنیت اطلاعات[۱۶] یا ISMS را برآورده کنند.

---

[۱۴] Gramm-Leach-Bliley Act

[۱۵] Financial Services Modernization Act

[۱۶] Information Security Management System

EventLog Analyzer با استفاده از گزارش‌ها و داشبورد بصری گرافیکی، به تطبیق دادن گزارش‌ها با استانداردهای ISO 27001:2013 کمک بسیاری می‌کند. این محصول گزارش‌هایی را فراهم می‌کند که به سازمان‌ها در ثبت کردن رویدادهای مورد نیاز و تولید شواهد کمک می‌کند. هم‌چنین نیازمندی‌های کنترل دسترسی کاربران غیرمجاز و جلوگیری از دسترسی غیرمجاز به سیستم‌ها و سرویس‌دهنده را برآورده می‌کند.

۳-٤ پایش دستگاه‌های شبکه

زیربنای هر شبکه ساده، علاوه بر مشتری‌ها و سرویس‌دهنده‌ها، متشکل از چندین عنصر منحصربه‌فرد و متنوع می‌باشد که پایش آن‌ها بسیار مهم است. پایش دستگاه‌های شبکه بسیار مهم است، چرا که تصویر کاملی از شبکه به ما می‌دهد. برای مثال درصورتی‌که یک عیب در دیواره‌ی آتش موجب دسترسی غیرقانونی به شبکه شود، تنها در صورتی‌که اطلاعاتی از عملکرد دیواره‌ی آتش وجود داشته باشد می‌توان بررسی جرم‌یابی روی آن را انجام داد. قدم اول در پایش امنیت و فعالیت‌های شبکه، جمع‌آوری و تحلیل فایل‌های ثبت وقایع دستگاه‌های شبکه است که EventLog Analyzer این کار را به‌سادگی انجام می‌دهد.

EventLog Analyzer با استفاده از ویژگی‌هایی که دارد، می‌تواند دستگاه‌هایی مانند سوئیچ‌ها، مسیریاب‌ها، سیستم‌های تشخیص نفوذ و دیواره‌ی آتش را پایش کند. حتی می‌توان برای دستگاه‌های ناشناخته موجود در شبکه، با استفاده ویژگی تجزیه‌کننده‌ی سفارشی، فایل ثبت وقایع جدید تعریف کرد. گزارش‌های سفارشی می‌توانند تعریف و برنامه‌ریزی شوند و برای رویدادهای خطرناک هشدارهای بی‌درنگ داده می‌شوند.

۳-٤-۱ سوئیچ‌ها و مسیریاب‌ها

مسیریاب‌ها و سوئیچ‌ها ترافیک شبکه را عبور می‌دهند و بنابراین پایش آن‌ها بسیار مهم است. یکی از نکات مهم پایش دسترسی به این دستگاه‌ها می‌باشد. هم‌چنین این دستگاه‌ها باید از نظر پیکربندی بررسی شوند تا ترافیک را به‌درستی عبور دهند. پایش این دستگاه‌ها می‌تواند به کاهش حملات و امن کردن شبکه کمک کند. EventLog Analyzer تمامی مسیریاب‌ها و سوئیچ‌های سیسکو و سایر برندهای معتبر را پشتیبانی می‌کند.

۳-٤-۲ سیستم‌های تشخیص و جلوگیری از نفوذ

سیستم‌های تشخیص نفوذ[۱۷] برای تشخیص فعالیت‌های مشکوک و ترافیک‌های ورودی به شبکه طراحی شده است. سیستم IDS مسئول هشدار به مدیر و ثبت رویدادها می‌باشد. هم‌چنین وظیفه تشخیص ورود بسته‌های ناخواسته به شبکه و از بین بردن آن‌ها را دارد. بررسی فایل‌های ثبت وقایع که توسط این دستگاه‌ها تولید می‌شوند بسیار مهم و بحرانی است.

۳-٤-۳ دیواره‌ی آتش

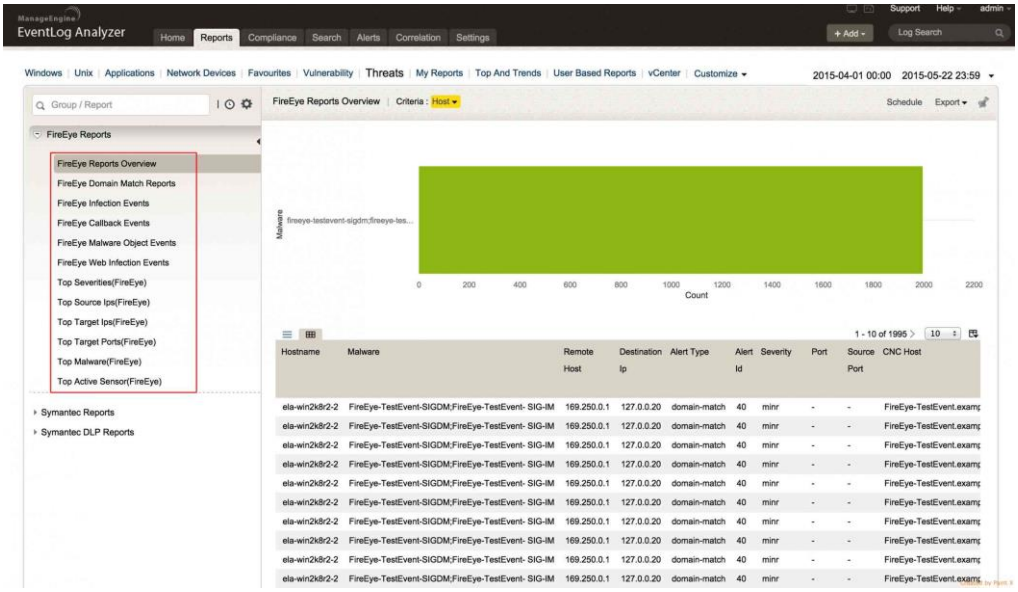
مشابه سیستم تشخیص نفوذ، دیواره‌ی آتش نیز وظیفه کنترل ترافیک و مسدود کردن داده‌های ناخواسته در هنگام ورود و خروج به شبکه را دارد. هم‌چنین سرایند بسته‌ها را برای تطبیق با قوانین بررسی می‌کند، در حالی‌که سیستم تشخیص نفوذ تمام بسته را بررسی می‌کند. بررسی فایل‌های ثبت وقایع دیواره‌ی آتش، اطلاعات مهمی درباره تبادلات بین شبکه سازمان و شبکه‌های خارجی می‌دهد. هم‌چنین تغییرات حساب کاربری کاربران، ورود به سیستم و مجموعه قوانین حاکم بر دیواره آتش را پایش می‌کند.

۳-۵ تجزیه و تحلیل اطلاعات تهدیدات هوشمند

EventLog analyzer پشتیبانی از فایل‌های ثبت وقایع محصولاتی مانند Symantec Endpoint، Symantec DLP و FireEye را فراهم کرده است. این محصول گزارش‌ها و شرایط هشداری که به تشخیص و رسیدگی تهدیدات امنیتی خارجی کمک می‌کنند را نیز فراهم کرده است. گزارش‌های از پیش آماده شده در قالب‌های مختلف شامل PDF، CSV و HTML می‌توانند ایجاد شوند. هم‌چنین تولید گزارش می‌تواند با استفاده از گزینه Schedule report به‌صورت خودکار انجام شود. گزارش‌ها شامل گروه‌های زیر می‌شوند:

- گزارش‌هایی روی داده‌های FireEye
- گزارش‌هایی روی داده‌های محصول Symantec Endpoint
- گزارش‌هایی روی برنامه Symantec DLP

[۱۷] Intrusion Detection System (IDS)



شکل ۱۰- تجزیه و تحلیل داده‌های فایل ثبت وقایع FireEye در EventLog Analyzer

۳-۶ امنیت اطلاعات و مدیریت رویدادها

EventLog Analyzer یکی از به صرفه‌ترین محصولات SIEM در بازار است. EventLog analyzer تمامی قابلیت‌های مهم SIEM، مانند همبسته کردن فایل‌های ثبت وقایع از منابع ناهمگن، جرم‌یابی فایل ثبت وقایع، همبسته‌سازی رویدادها، هشدارهای بی‌درنگ، پایش صحت فایل، تحلیل فایل ثبت وقایع، پایش فعالیت‌های کاربران، رسیدگی دسترسی اشیاء، گزارش تطبیق و نگه‌داری فایل ثبت وقایع، را داراست.

۳-۶-۱ مجتمع‌سازی فایل‌های ثبت وقایع

EventLog Analyzer از منابع مختلف غیرهمگن (ویندوز، لینوکس/یونیکس، برنامه‌های کاربردی، پایگاه‌داده‌ها، مسیریاب‌ها، سوئیچ‌ها، و سایر دستگاه‌های syslog) داده‌ها را در یک مکان مرکزی جمع‌آوری و مجتمع می‌کند. EventLog Analyzer با استفاده از تکنولوژی تجزیه و اندیس‌گذاری جهانی (ULPI)[۱۸] اجازه کدبرداری/کدگذاری هر داده فایل ثبت وقایع را بدون در نظر گرفتن قالب و منبع فایل می‌دهد.

[۱۸] Universal Log Parsing and Indexing

۳-۶-۲ جرم‌یابی فایل ثبت وقایع

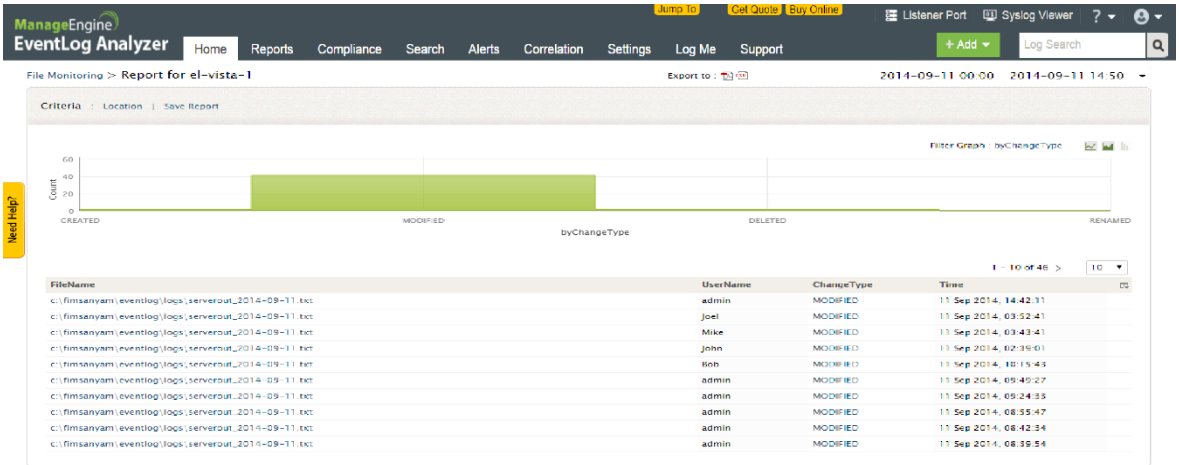
EventLog Analyzer با استفاده از ویژگی قدرتمند جست‌وجوی وقایع برای جست‌وجوی هر دو داده‌ی خام وقالب‌بندی شده، امکان بررسی و جرم‌یابی را آسان نموده است و گزارش‌های جرم‌یابی بر اساس فایل‌های ثبت وقایع را ارائه می‌کند. EventLog Analyzer این امکان را به مدیر شبکه می‌دهد تا به جست‌وجو در فایل‌های ثبت وقایع خام برای پیدا کردن نقطه دقیق، زمان و مکانی که اتفاق امنیتی در آن افتاده است، بپردازد.

۳-۶-۳ همبسته‌سازی رویدادها و هشدارها

همبسته‌سازی رویدادها و تولید هشدارهای بی‌درنگ به مدیر شبکه اجازه می‌دهد تا به‌صورت پیشرفته شبکه را در برابر تهدیدات، امن نگه دارد. با استفاده از EventLog Analyzer می‌توان قوانین و اسکریپت‌هایی برای همبسته‌سازی رویدادها براساس شرایط آستانه یا حوادث غیرمعمول پیکربندی کرد تا در صورت رخداد هرگونه تهدید، هشدارهای بی‌درنگ صادر شود. موتور قدرتمند همبسته‌سازی EventLog Analyzer به همراه ۷۰ قانون که شامل سطح دسترسی کاربر، ورود کاربران، صحت فایل، ایجاد کاربر، سیاست‌های گروهی، نصب نرم‌افزارهای اتفاقی و غیره می‌شود، به امنیت شبکه کمک بسیاری می‌کند.

۳-۶-۴ پایش صحت فایل

EventLog Analyzer ویژگی پایش صحت فایل (FIM) به‌صورت بی‌درنگ را با محافظت از اطلاعات حساس و برآورده کردن نیازمندی‌های تطبیقی فراهم کرده است. با استفاده از این ویژگی فراهم کردن امنیت می‌تواند به‌صورت مرکزی، با دنبال کردن تمامی تغییرات در فایل‌ها و پوشه‌ها (مانند ایجاد، دسترسی، حذف، اصلاح، باز کردن) انجام شود.



شکل ۱۱- پایش صحت فایل

۳-۶-۵ تحلیل فایل ثبت وقایع

EventLog Analyzer وقایع ثبت شده را به‌صورت بی‌درنگ تحلیل می‌کند و نتایج آن را به‌صورت نمودارهای قابل فهم، گراف‌ها و گزارشات نمایش می‌دهد. کاربر به‌سادگی می‌تواند فایل‌ها را پیمایش کند، جزئیات آن‌ها را ببیند و نقطه آغازین یک اتفاق را در چند دقیقه پیدا کند.

۳-۶-۶ پایش کاربران

این محصول گزارش‌های جامعی در ارتباط با کاربران فراهم کرده است. گزارش‌های دقیقی مانند این‌که فعالیت توسط چه کاربری انجام شده، نتیجه فعالیت چه بوده، روی چه سرویس‌دهنده‌ای و چه زمانی اتفاق افتاده است.

۳-۶-۷ بازبینی دسترسی اشیاء

این محصول این امکان را فراهم می‌کند که مدیر بتواند متوجه فعالیت‌هایی در ارتباط با فایل‌ها شود. فعالیت‌هایی مانند این‌که چه شخصی به فایل‌ها و یا پوشه‌ها دسترسی پیدا کرده است، چه کسی آن‌ها را حذف یا اصلاح کرده است، فایل‌ها چه تغییراتی پیدا کرده‌اند و غیره. گزارش این فعالیت‌ها در قالب‌های کاربرپسند CSV و یا PDF صادر می‌شوند و زمانی‌که یک فایل حساس توسط کاربر غیرمجاز مورد دسترسی قرار بگیرد، هشدار بی‌درنگ توسط پست الکترونیکی و یا ایمیل صادر می‌شود.

۳-۶-۸ نگه‌داری فایل ثبت وقایع

EventLog Analyzer داده‌های سلسله مراتبی وقایع را برای جرم‌یابی فایل ثبت وقایع و برآورده کردن نیازمندی‌های تطابقی نگه‌داری می‌کند. تمامی داده‌های موجود در فایل ثبت وقایع نگه‌داری شده و درهم‌سازی شده هستند و برچسب زمانی دارند. تمامی فایل‌های جمع‌آوری شده در یک انبار مرکزی نگه‌داری می‌شوند.

۳-۶-۹ Threat Intelligence

با پیشرفت حملات سایبری، جلوگیری از نفوذ به شبکه بسیار مشکل شده است. از طرفی هشدارهای اشتباه نیز تشخیص تهدیدات واقعی را مشکل ساخته است. با توجه به مشکلات موجود، اشتراک اطلاعات تهدید بین سازمان‌ها و نیز استراتژی‌های پیشگیرانه در مبارزه با حملات سایبری، حیاتی به نظر می‌رسد.

ماژول Threat Inteligence در EventLog Analyzer به‌منظور به اشتراک‌گذاری اطلاعات تهدیدات از طریق پروتکل‌های بین المللی مانند STIX، TAXII و AlienVauilt OTX طراحی شده است. هنگامی که منابع

مخرب با شبکه در ارتباط باشند، هشدارها می‌تواند به‌صورت پیام کوتاه و یا از طریق پست الکترونیکی ارسال شوند.

به‌عنوان نمونه، با استفاده از موارد زیر، حملات در اولین نشانه‌های خود شناسایی می‌شوند:

- همبسته‌سازی لیست سیاه جهانی از IPها با IPهایی که در ارتباط با شبکه هستند و اعلان هشدار به‌صورت ایمیل و پیام کوتاه، در صورتی‌که IP ای با لیست سیاه منطبق گردد.
- استفاده از STIX، یک زبان ساخت‌یافته، برای راه‌حل‌های هوشمندانه تهدیدات سایبری.
- استفاده از TAXII، یک سازوکار انتقال، برای به اشتراک‌گذاری هوشمندی تهدیدات سایبری.
- استفاده از AlienVault OTX، معتبرترین سکوی متن باز برای به اشتراک‌گذاری اطلاعات تهدیدات و تحلیل شبکه.

علاوه بر منابع بالا EventLog Analyzer برای شناسایی حوادث بحرانی مانند حملات بدافزارها، IPهای مبدأ و مقصد و ویروس‌ها، از گزارش‌های محصولات امنیتی شرکت‌های محبوب مانند FireEye، Barracuda، WatchGuard و Symantec نیز پشتیبانی می‌کند.

۳-۶-۹-۱ پروتکل STIX

STIX یک زبان رایج برای تشریح اطلاعات تهدیدات سایبری فراهم می‌کند که قابلیت به اشتراک‌گذاری و ذخیره‌سازی را دارا است. STIX، از طریق تحلیل‌گران سایبری، تحلیل‌گران بدافزار، فروشندگان ابزارهای امنیتی، محققان امنیتی و دسترسی به جوامع به اشتراک‌گذاری تهدیدات، برای استاندارد کردن اطلاعات تهدیدات به حفاظت از شبکه‌ها و سیستم‌ها در برابر تهدیدات سایبری می‌پردازد.

۳-۶-۹-۲ پروتکل TAXII

TAXII تلاش جوامع برای استاندارد کردن اعتماد و تبادل خودکار اطلاعات تهدیدات سایبری است. TAXII مجموعه‌ای از سرویس‌ها و تبادل پیام‌ها را تعریف می‌کند که در صورت پیاده‌سازی، سازمان‌ها را قادر می‌سازد تا اطلاعات تهدیدات سایبری قابل پیگرد را با یکدیگر به اشتراک گذارند.

TXII یک برنامه به اشتراک‌گذاری نیست بلکه مجموعه‌ای از استانداردها برای تبادل اطلاعات تهدیدات سایبری به‌منظور کمک کردن به سازمان‌ها می‌باشد. TAXII سه مدل به اشتراک‌گذاری دارد: مدل نقطه به نقطه، منبع و مشترکان و قطب واقماری[۱۹].

۳-۹-۶-۳ AlienVault OTX

AlienVault OTX[۲۰] یکی از بزرگترین سکوهای امنیت رایانه‌ای موجود است. بیش از ۲۶۰۰۰ شرکت‌کننده از ۱۴۰ کشور، روزانه بیش از یک میلیون تهدید بالقوه را شناسایی می‌کنند. گزارش‌های جامعه OTX و دریافت داده به شکل پالس می‌باشد. یک پالس OTX شامل یک یا چندین نشان‌گر سازش (IOCs) است، که یک تهدید را تشکیل می‌دهد یا مجموعه‌ای از اقداماتی را که می‌تواند برای حملات بر روی دستگاه‌های شبکه و رایانه‌ها استفاده شود، تعریف می‌کند. هم‌چنین پالس‌های OTX اطلاعاتی درباره قابلیت اطمینان اطلاعات تهدید، گزارش‌دهنده تهدید و سایر جزئیات مهم درباره تهدید ارائه می‌دهد.

۳-۶-۱۰ تشخیص تهدیدات با استفاده از پروتکل‌های STIX/TAXII

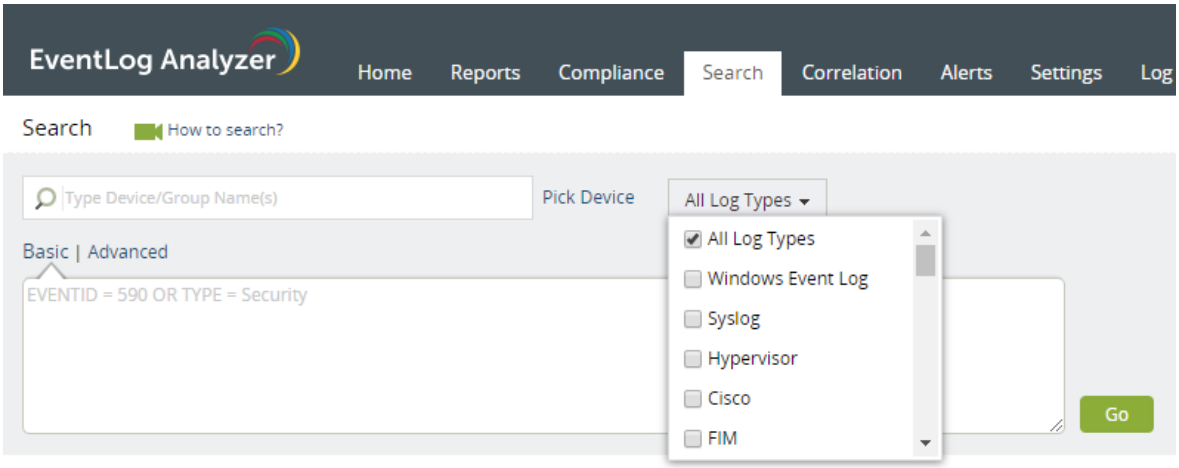
یکی از مهم‌ترین نکات برای مقابله با تهدیدات داشتن اطلاعات به‌روز است. اما معمولا سازمان‌ها برای این نوع اطلاعات داخلی ندارند. به‌همین منظور، برای فراهم کردن استانداردهای قابل اجرای جهانی برای شناسایی و به اشتراک گذاشتن اطلاعات تهدیدات، پروتکل‌های STIX/TAXII ایجاد شده‌اند. یکی از بزرگ‌ترین نقاط قوت تشخیص تهدیدات در EventLog Analyzer، پشتیبانی از پروتکل‌های STIX/TAXII است. فرآیندهای مبتنی بر STIX/TAXII در EventLog Analyzer هشدارهای بی‌درنگ را در زمانی‌که IPها و URLهای موجود در لیست سیاه با شبکه در ارتباط باشند، صادر می‌کنند. با استفاده از این پروتکل‌ها می‌توان به اطلاعات جامعی از تهدیدات دسترسی پیدا کرد. هم‌چنین در EventLog Analyzer اطلاعات تهدیدات به‌صورت پویا نیز به‌روز می‌شوند. برای شروع فرآیند تشخیص، تنها استقرار EventLog Analyzer کافی است و نیازی به پیکربندی خاصی نمی‌باشد.

[۱۹] Hub and Spoke

[۲۰] Open Threat Exchange

۳-۷ جست‌وجو در فایل ثبت وقایع

قابلیت جست‌وجو در EventLog Analyzer بسیار ساده و انعطاف‌پذیر است که از طریق زبانه Search قابل دسترسی می‌باشد. اطلاعات وقایع ثبت‌شده که توسط سرویس‌دهنده جمع‌آوری شده است می‌توانند از نتایج جست‌وجو برای پروفایل کردن گزارشات استفاده شوند که این کار به عیب‌یابی شبکه و تحلیل جرم‌یابی کمک می‌کند.



شکل ۱۲- صفحه‌ی جست‌وجوی فایل ثبت وقایع

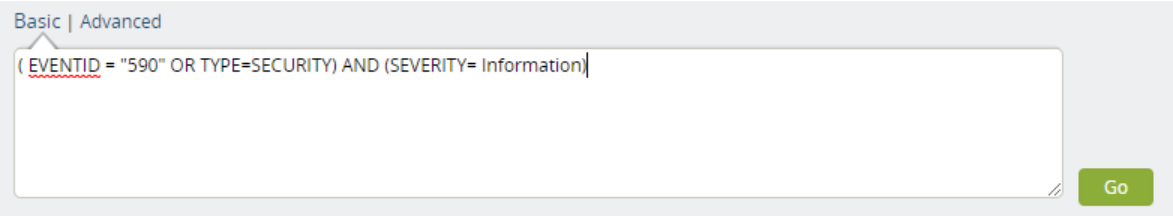
برای جست‌وجو می‌توان براساس نوع دستگاه و یا نوع فایل ثبت وقایع، فیلتر را انجام داد:

- انتخاب دستگاه‌های خاص / گروه دستگاه‌ها برای جست‌وجوی فایل ثبت وقایع

برای محدود کردن دستگاه‌ها برای جست‌وجو، می‌توان دستگاه‌ها و یا گروه دستگاه‌ها را انتخاب کرد. بدین صورت که نام آن‌ها را در قسمت جست‌وجو وارد کرده و یا این‌که با استفاده از پیوند Pick Device از لیست دستگاه‌ها، دستگاه‌های مورد نظر را انتخاب کرد. در صورتی‌که در این قسمت چیزی وارد نشود، تمام دستگاه‌ها مورد جست‌وجو قرار می‌گیرد.

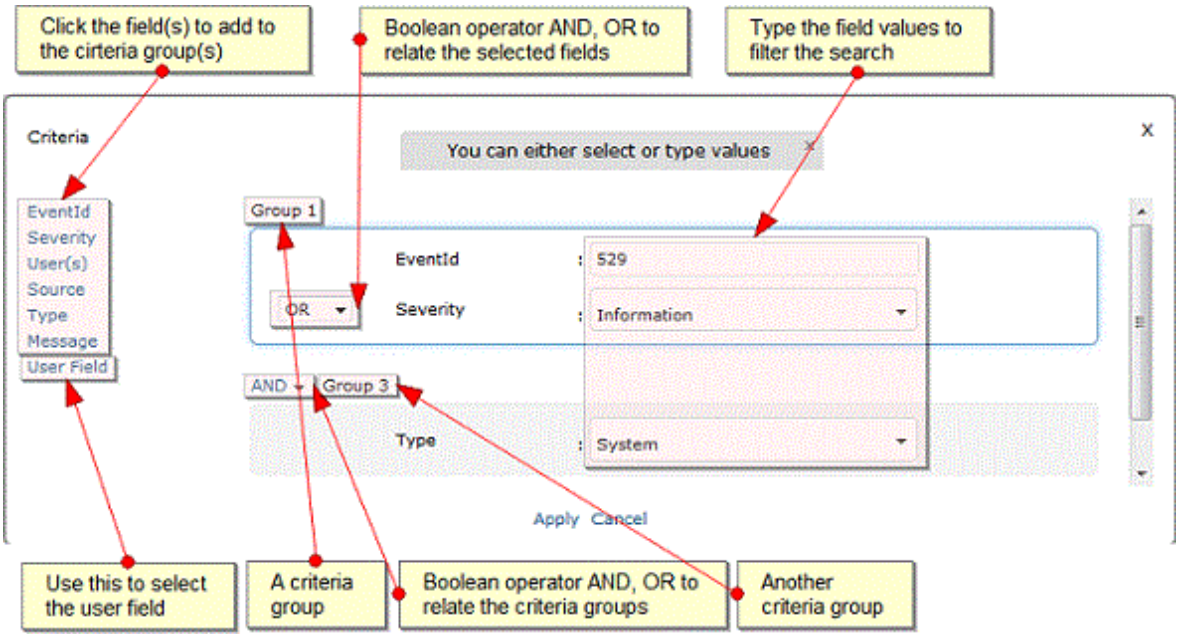
- انتخاب نوع فایل ثبت وقایع برای جست‌وجو

از لیست Log Types نوع فایل ثبت وقایع انتخاب می‌شود. به‌صورت پیش‌فرض All Log Types انتخاب شده است. به دو صورت مبتدی و پیشرفته می‌توان جست‌وجو را انجام داد. در صورت استفاده از نوع مبتدی باید به‌صورت دستی پرس‌وجوی خود را وارد کنید. برای نوشتن پرس‌وجو به‌صورت دستی می‌توان فیلد و مقدار آن را در قسمت جست‌وجو مشخص کرد و با استفاده از AND، OR، NOT و سایر عملوندها، می‌توان عبارات پیچیده‌تر را ایجاد کرد.



شکل ۱۳- نوشتن پرس‌وجو در حالت Basic

در جست‌وجوی پیشرفته تعدادی فیلد در گروه یا گروه‌هایی وجود دارند که برای مشخص کردن معیارهای فیلتر برای جست‌وجو انتخاب می‌شوند. این فیلدها با استفاده از عملوندهای دودویی با یکدیگردر یک گروه و یا با گروه‌های دیگر ارتباط داده می‌شوند.



شکل ۱٤- ایجاد پرس‌وجو در حالت جست‌وجوی پیشرفته

٤ نصب و پیکربندی EventLog Analyzer

در این بخش نصب EventLog Analyzer به همراه پیکربندی‌های مورد نیاز آن توضیح داده خواهد شد. برای نصب لازم است که در ابتدا نیازمندی‌های نرم‌افزاری و سخت‌افزاری را بررسی کنیم. سپس نصب محصول را روی هر دو محیط لینوکس و ویندوز توضیح خواهیم داد. در ادامه پیکربندی‌های مورد نیاز شرح داده خواهد شد.

٤-١ نیازمندی‌های نصب

در این قسمت لیست حداقل نیازمندی‌های لازم برای نصب و کار با Evenlog Analyzer در دو نسخه توزیع‌شده و مستقل آورده شده است.

٤-١-١ نیازمندی‌های سخت‌افزاری

برای نصب این محصول به یک سری حداقل ویژگی‌های سخت‌افزاری نیازمندیم که در جدول ۱ آورده شده است. ستون آخر (ایده‌آل) نشان دهنده بهترین حالت ویژگی سخت‌افزاری برای نصب می‌باشد.

جدول ۱ – نیازمندی‌های سخت‌افزاری

ویژگی سخت‌افزاری	حداقل نیازمندی	ایده‌آل
RAM	2GB	6 GB
Hard Disk	50GB	
Display Resolution	1024*768	
Processor	Dual-core	Quad-core

نسخه توزیع‌شده EventLog Analyzer می‌تواند نرخ گزارش‌ها یا رویدادهای رخ داده در ثانیه (EPS) را مدیریت کند. جدول ۲ ظرفیت مدیریت این محصول را نمایش می‌دهد.

جدول ۲- ظرفیت مدیریت فایل ثبت وقایع

	Average log size	Average EPS	Peak EPS
Syslog	100 bytes	20,000	25,000
Windows event log	2 KB	2,000	2,500

برای افزایش ظرفیت این محصول می‌توان از یک نسخه توزیع‌شده به همراه چندین گره استفاده کرد که می‌تواند حجم بیشتری از فایل‌های ثبت وقایع را مدیریت کند.

٤-١-٢ سیستم‌عامل مورد نیاز

EventLog Analyzer بر روی نسخه‌های سیستم‌عامل که در ادامه آمده است نصب و اجرا می‌شود.

- Windows™ 8
- Windows™ 7
- Windows™ Server 2000/2003/2008/2008 R2/2012/2016
- Linux - RedHat 8.0/9.0
- Mandrake/Mandriva Linux
- SuSE Linux
- Fedora Linux

- CentOS Linux

هم‌چنین این محصول قابلیت اجرا روی هر محیط مجازی را نیز دارا می‌باشد.

٤-١-٣ پایگاه‌داده‌های پشتیبانی شده

پایگاه‌داده PostgreSQL به همراه محصول عرضه شده است و مورد پشتیبانی قرار گرفته است. هم‌چنین از پایگاه‌داده‌های MS SQL نسخه های ۲۰۰۵، ۲۰۰۸، ۲۰۱۲ و ۲۰۱٤ پشتیبانی می‌شود.

به‌منظور افزایش کارایی پایگاه‌داده PostgreSQL توصیه می‌شود که پارامترهای ذکر شده در postgres_ext.txt که در مسیر \pgsql\data\directory موجود است با مقادیر ذکرشده در جدول ۳ جابه‌جا شوند.

جدول ۳- تغییر پارامترهای PostgreSQL به‌منظور افزایش کارایی

پارامترهایی که باید تغییر داده شود	حداقل نیازمندی
shared_buffers=128 MB	128KB
work_mem=12 MB	64KB
maintenance_work_mem=100 MB	1MB
checkpoint_segments=15	هر فایل ثبت وقایع به حداقل فایل‌های 1 و 16MB قطعه بندی می‌شود.
checkpoint_timeout=11 minutes	بازه: ۳۰ ثانیه تا یک ساعت
checkpoint_completion_target=0.9	بین 0.0 – 1.0
seq_page_cost=1.0	این پارامتر در مقیاس دلخواه اندازه‌گیری می‌شود.
random_page_cost=2.0	این پارامتر در مقیاس مشابه پارامتر بالا اندازه گیری می‌شود
effective_cache_size=512MB	
synchronous_commit=off	

بیشتر این تغییرات برای اعمال، نیاز به اجرا شدن دوباره برنامه/سرویس دارند.

٤-١-٤ مرورگرهای پشتیبانی شده

EventLog Analyzer برای پشتیبانی از مرورگرهای زیر آزمایش شده است:

- Internet Explorer نسخه ۸ و بالاتر
- Firefox نسخه ٤ و بالاتر

- Chrome نسخه ۸ و بالاتر

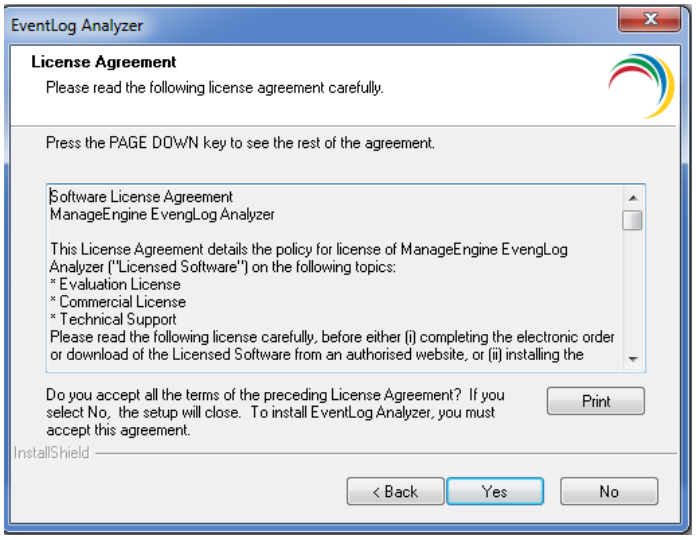
۲-٤ نصب EventLog Analyzer

محصول EventLog Anlayzer برای نصب روی هر دو محیط ویندوز و لینوکس طراحی شده است. در ادامه این قسمت به‌صورت جداگانه به توضیح نصب محصول خواهیم پرداخت.

۱-۲-٤ نصب روی ویندوز

برای نصب این محصول باید مراحل راهنمای نصب را دنبال کنید:

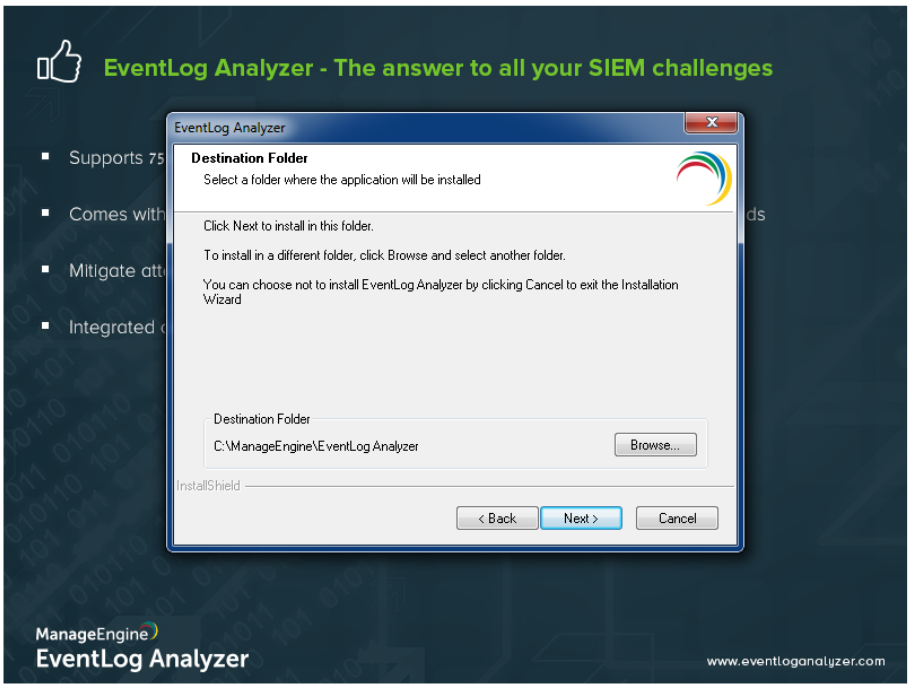
۱. برای نصب باید شرایط گواهینامه را قبول کنید. بهتر است که آن را پرینت بگیرید و نزد خود نگه دارید.



شکل ۱۵- مرحله اول نصب – پذیرش شرایط گواهینامه

۲. نسخه‌های موجود این محصول شامل مستقل، توزیع‌شده و رایگان هستند. برای نصب، نسخه مورد نظر را انتخاب کنید.

۳. مسیر موردنظر برای نصب محصول را انتخاب کنید. مسیر پیش‌فرض در پوشه C:\ManageEngine\EventLog انتخاب شده است.



شکل ۱۶- انتخاب مسیر مورد نظر برای نصب

٤. درگاه ارتباطی وب سرویس‌دهنده را انتخاب کنید. درگاه[۲۱] پیش‌فرض برای این منظور ۸٤۰۰ است. مطمئن شوید که درگاه پیش‌فرض یا درگاه انتخاب شده توسط شما توسط برنامه‌ی دیگری استفاده نشده باشد.

٥. برای انتخاب زبان مورد نظر خود مطمئن شوید که مرورگر آن را پشتیبانی می‌کند. سپس پروتکل وب (HTTP/HTTPS) را انتخاب کنید.

٦. برای نصب محصول به‌صورت یک سرویس ویندوزی گزینه Install EventLog Analyzer as service را انتخاب کنید. به‌صورت پیش‌فرض همین گزینه انتخاب شده است. EventLog Analyzer را می‌توان به‌صورت برنامه کاربردی نیز نصب کرد، اما طبق توصیه ManageEngine بهتر است به‌صورت سرویس نصب شود.

۷. نام پوشه‌ای که برنامه در آن قرار است نصب شود را وارد کنید. به‌صورت پیش‌فرض نام این پوشه، Manage Engine EventLog Analyzer<version number> است.

۸. برای دریافت کمک اطلاعات شخصی خود را وارد کنید.

---

[۲۱] Port

۹. در انتهای فرآیند می‌توانید فایل ReadMe را مطالعه کنید و سرویس‌دهنده EventLog Analyzer را اجرا کنید.

٤-۲-۲ نصب روی لینوکس

نصب محصول روی لینوکس مشابه نصب روی ویندوز می‌باشد. در ادامه مراحل نصب را توضیح می‌دهیم.

۱. قبل از این‌که فایل اجرایی را کلیک کنید باید مطمئن شوید که فایل اجرایی مجوز اجرا شدن را دارا می‌باشد. برای دادن مجوز به فایل باید دستور زیر را در ترمینال یا Shell لینوکس وارد کنید.

```
chmod +x ManageEngine_EventLogAnalyzer.bin
```

۲. اکنون فایل اجرایی ManageEngin_EventLogAnalyzer.bin را با استفاده از دابل کلیک یا نوشتن دستور زیر در ترمینال اجرا کنید.

```
./ManageEngine_EventLogAnalyzer.bin
```

بعد از اجرا شدن نصب کننده‌ی برنامه، مراحل زیر را دنبال کنید.

۳. شرایط گواهینامه را قبول کنید. بهتر است که یک پرینت از آن گرفته و نگه‌داری کنید.

٤. پوشه مورد نظر برای نصب را انتخاب کنید.

۵. درگاه سرویس‌دهنده وب را انتخاب کنید. درگاه پیش‌فرض ۸٤۰۰ می‌باشد. نام پوشه که در پوشه برنامه‌ها نشان داده می‌شود را انتخاب کنید. نام پیش‌فرض ManageEngine EventLog Analyzer است.

٦. اطلاعات شخصی خود را برای دریافت کمک در صورت مشکل وارد کنید.

٤-۳ پیش‌نیازها

قبل از اجرای برنامه در محیط باید پیش‌نیازهای زیر مورد بررسی قرار بگیرد.

درگاه‌های موجود در جدول ٤ برای اجرای برنامه مورد استفاده قرار می‌گیرند. بنابراین باید از اشغال نبودن آن‌ها توسط سایر برنامه‌ها مطمئن شد.

جدول ٤- درگاه‌های مورد استفاده برنامه

شماره درگاه ارتباطی	کاربرد	توضیحات

درگاه پیش‌فرض برای سرویس‌دهنده وب می‌باشد. از این درگاه برای اتصال EventLog Analyzer به وب از طریق مرورگر وب استفاده می‌شود.	سرویس‌دهنده وب	8400 (TCP)
درگاه پیش‌فرض برای syslog Listener در پروتکل UDP	Syslog listener port	513, 514 (UDP)
درگاه پیش‌فرض برای syslog Listener در پروتکل TCP	Syslog listener port	514 (TCP)
این درگاه برای اتصال به پایگاه‌داده است.	درگاه پایگاه‌داده PostgreSQL/MySQL	33335 (TCP)

هم‌چنین EventLog Analyzer از درگاه‌های موجود در جدول ۵ برای WMI، RPC و DCOM استفاده می‌کند.

جدول ۵ – درگاه‌های مورد استفاده برای WMI، RPC و DCOM

توضیحات	کاربرد	شماره درگاه ارتباطی
درگاه‌های مربوط به ترافیک ورودی به سرویس‌دهنده EventLog Analyzer	WMI, DCOM, RPC	135, 445, 139 (TCP)
درگاه‌های مربوط به ترافیک خروجی سرویس‌دهنده EventLog Analyzer DCOM از سازوکار Callback با درگاه‌های تصادفی بین 49152-65534 برای ویندوز سرور ۲۰۰۸ و 1024-65534 برای نسخه قبل آن استفاده می‌کند.	WMI, DCOM, RPC	49152-65534 (TCP)

EventLog Analyzer برای ارتباط عامل‌های محلی با سرویس‌دهنده UDP از درگاه‌های ذکر شده در جدول ٦ استفاده می‌کند.

جدول ٦ – درگاه مورد استفاده برای سرویس‌دهنده UDP

توضیحات	کاربرد	شماره درگاه ارتباطی
EventLog Analyzer از درگاه‌های UDP به‌صورت داخلی برای ارتباط سرویس‌دهنده با عامل‌ها استفاده می‌کند. تعدادی درگاه در بازه (1024-65534) نیز باز خواهد شد که از این درگاه‌ها نیز برای ارتباطات داخلی استفاده می‌شود.	درگاه‌های UDP برای ارتباط EventLog Analyzer با عامل‌های محلی	5000, 5001, 5002 (UDP)

جدول ۷ درگاه‌های مورد نیاز برای ارتباط عامل‌های راه دور با سرویس‌دهنده TCP را نشان می‌دهد.

جدول ۷– درگاه مورد استفاده برای سرویس‌دهنده TCP

توضیحات	کاربرد	شماره درگاه ارتباطی
EventLog Analyzer از این درگاه‌های TCP برای ارتباط راه دور عامل‌ها با سرویس‌دهنده استفاده می‌کند. این درگاه‌ها باید در دیواره‌ی آتش ایجاد شوند. **توجه:** در حین نصب خودکار عامل، درگاه‌های WMI، RPC و DCOM یک مرتبه استفاده می‌شوند.	درگاه‌های TCP برای ارتباط EventLog Analyzer با عامل‌های راه دور	8400 (TCP)

و برای IBM AS/400 درگاه‌های موجود در جدول ۸ باید باز شوند.

جدول ۸– درگاه مورد استفاده برای IBM AS/400

کاربرد	شماره درگاه ارتباطی
این درگاه‌ها برای دسترسی به ماشین‌های IBM AS/400 باز می‌شوند.	446-449, 8470-8476, 9470-9476 (TCP)

٤-٣-١ فرآیند تغییر درگاه مربوط به پایگاه‌داده PostgreSQL

١. فایل databese_params.conf که در محل <EventLog Analyzer Home>\conf موجود است را باز کنید.

٢. درگاه مشخص شده در خط زیر را با درگاه مورد نظر تغییر دهید.

```
url=jdbc:postgresql://localdevice:33335/eventlog?stringtype=unspecified
```

٣. فایل را ذخیره کنید و سرویس‌دهنده را دوباره اجرا کنید.

٤-٣-٢ دادن مجوز به پایگاه‌داده PostgreSQL برای رفع عیب

فایل pg_hba.conf که در مسیر <EventLog Analyzer Home>\pgsql\data موجود است را باز کنید و خط

```
device all all <IP address of the remote machine to be used to troubleshoot>/32 trust
```

را بعد از خط

```
device all all 127.0.0.1/32 trust
```

اضافه کنید. سپس فایل را ذخیره کنید.

٤-٣-٣ فرآیند تغییر درگاه مربوط به MySQL

١. فایل mysql-ds.xml که در مسیر <EventLog Analyzer Home>\server\default\deploy موجود است را باز کنید.

٢. درگاه مشخص شده در خط زیر را با درگاه دلخواه تغییر دهید.

```
<connection-url>jdbc:mysql://localdevice:33336/eventlog</connection-url>
```

٣. فایل را ذخیره کنید و سرویس‌دهنده را دوباره اجرا کنید.

٤-٣-٤ فرآیند تغییر درگاه سرویس‌دهنده وب

١. فایل sample-bindings.xml که در مسیر <EventLog Analyzer Home>\server\default\conf موجود است را باز کنید.

٢. درگاه مشخص شده در خط زیر را با درگاه دلخواه تغییر دهید.

```
<binding port="8400"/>
```

٣. فایل را ذخیره کنید و سرویس‌دهنده را دوباره اجرا کنید.

٤-٤ شروع و خاتمه سرویس‌دهنده‌ها/سرویس‌گیرنده‌ها

در حین نصب EventLog analyzer از شما خواسته می‌شود که نرم‌افزار را به‌عنوان یک سرویس و یا یک برنامه کاربردی نصب کنید. بعد از نصب باید محصول را اجرا کنید. در ادامه این قسمت به‌صورت جداگانه نحوه اجرا و خاتمه به اجرای این محصول به‌صورت برنامه کاربردی و سرویس را توضیح خواهیم داد. دقت کنید که زمانی‌که به اجرای سرویس‌دهنده خاتمه می‌دهید، اتصالات پایگاه‌داده PostgreSQL نیز به‌صورت خودکار بسته می‌شود و تمامی درگاه‌های مربوط به EventLog Analyzer آزاد می‌شود.

٤-٤-١ برنامه کاربردی ویندوزی

برای شروع برنامه کاربردی مراحل زیر را دنبال کنید:

١. آیکون مربوط به محصول در مسیر Desktop و یا در مسیر Start > Programs > ManageEngine Log360 <version number> > Log360 را برای اجرای سرویس‌دهنده انتخاب کنید.
٢. در صورتی‌که سرویس اجرا شد، می‌توانید با آیکون موجود در نوار وظیفه به EventLog Analyzer متصل شوید.

برای خاتمه دادن به برنامه نیز مراحل زیر را انجام دهید:

١. به مسیری که EventLog Analyzer در آن نصب شده است بروید. به‌صورت پیش‌فرض این مسیر Start > Programs > ManageEngine Log360 <version number> است. سپس گزینه Shut Down EventLog Analyzer را انتخاب کنید.
٢. هم‌چنین می‌توانید به پوشه <EventLog Analyzer Home>\bin بروید و فایل shutdown.bat را اجرا کنید.

٤-٤-٢ سرویس‌دهنده ویندوزی

برای اجرای سرویس‌دهنده ویندوزی EventLog Analyzer باید مراحل زیر را طی کنید:

١. به مسیر Control Panel > Administrative Tools > Services بروید.
٢. روی سرویس <ManageEngine EventLog Analyzer <version number راست کلیک کرده و در منوی سمت چپ روی شروع کلیک کنید.

برای خاتمه دادن به اجرای سرویس‌دهنده طبق مراحل زیر پیش بروید:

۱. Control panel را باز کنید و Administrative Tools > Services را انتخاب کنید.
۲. روی ManageEngine EventLog Analyzer <version number> راست کلیک کرده و از منو خاتمه را انتخاب کنید.

٤-٤-٣ برنامه کاربردی لینوکسی

برای اجرای EventLog Analyzer در محیط لینوکس به‌صورت برنامه کاربردی مراحل زیر را طی کنید.

۱. به مسیر <EventLog Analyzer Home>/bin بروید و فایل run.sh. را اجرا کنید.
۲. زمانی‌که فایل run.sh اجرا شد، یک صفحه باز می‌شود که اطلاعات اجرا شدن ماژول‌های EventLog Analyzer را نمایش می‌دهد. زمانی‌که تمامی ماژول‌ها به‌طور موفقیت آمیزی اجرا شد، پیام زیر نمایش داده می‌شود:

```
Server started.
Please connect your client at http://localdevice:8400
```

برای خاتمه دادن به برنامه در مسیر <EventLog Analyzer Home>\bin فایل shutdown.sh را اجرا کنید.

٤-٤-٤ سرویس‌دهنده لینوکسی

برای اجرای سرویس‌دهنده روی لینوکس مراحل زیر را انجام دهید:

۱. زمانی‌که نرم‌افزار به‌صورت یک سرویس‌دهنده نصب شد، برای اجرای سرویس‌دهنده، دستور زیر را در یک ترمینال اجرا کنید.

```
/etc/init.d/eventloganalyzer start
```

۲. وضعیت سرویس‌دهنده EventLog Analyzer را با اجرای دستور زیر بررسی کنید.

```
/etc/init.d/eventloganalyzer status
```

برای مثال خروجی دستور بالا میتواند به این شکل باشد:

```
ManageEngine EventLog Analyzer 11.0 is running (<Process ID>).
```

برای خاتمه دادن به اجرای سرویس باید مراحل زیر را اجرا کنید:

۱. دستور زیر را در ترمینال وارد کنید.

```
/etc/init.d/eventloganalyzer stop
```

خروجی می‌تواند به شکل زیر باشد:

```
Stopping ManageEngine EventLog Analyzer <version number>...
Stopped ManageEngine EventLog Analyzer <version number>
```

۲. با دستور زیر وضعیت سرویس‌دهنده را بررسی کنید:

```
/etc/init.d/eventloganalyzer status
```

خروجی به‌صورت زیر می‌باشد:

```
ManageEngine EventLog Analyzer <version number> is not running.
```

٤-٥ اتصال به سرویس‌دهنده‌ی وب

در صورتی‌که EventLog Analyzer به‌صورت سرویس نصب شود، Web Client به‌صورت خودکار اجرا می‌شود. در غیر این صورت یک مرورگر را باز کنید و از طریق تایپ آدرس Http://<hostname>:8400 (که <hostname> نام ماشینی است که EventLog Analyzer روی آن اجرا شده و ۸٤۰۰ درگاه سرویس‌دهنده وب پیش‌فرض می‌باشد) به EventLog Analyzer متصل شوید. سپس از طریق ترکیب نام کاربری و رمز عبور admin/admin وارد نرم‌افزار شوید.

درصورتی‌که از Active Directory کاربر وارد کرده باشید و یا جزئیات سرویس‌دهنده‌ی RADIUS را اضافه کرده باشید، گزینه‌هایی در زیر فیلد رمز عبور لیست خواهد شد. در این حالت علاوه بر نام کاربری و رمز عبور باید یکی از سه گزینه‌ی احراز اصالت محلی، احراز اصالت RADIUS و یا نام دامنه را انتخاب کنید. سپس روی دکمه Login کلیک کنید و به EventLog Analyzer متصل شوید.

EventLog Analyzer علاوه بر احراز اصالت محلی دو مدل احراز اصالت دیگر را نیز فراهم کرده است. که عبارتند از Active Directory و Remote Authentication Dial in User Service (RADIUS). فیلد Log on to گزینه‌های زیر را لیست خواهد کرد.

- احراز اصالت محلی: اطلاعات کاربر باید در پایگاه‌داده کاربر سرویس‌دهنده محلی EventLog Analyzer موجود باشد.
- احراز اصالت RADIUS: در صورتی‌که اطلاعات کاربر در سرویس‌دهنده RADIUS در دسترس و پیکربندی شده باشد.
- Domain Names(s): در صورتی‌که مشخصات کاربر یک دامنه از Active Directory به پایگاه‌داده کاربر سرویس‌دهنده محلی EventLog Analyzer وارد شده باشد.

٤-٦ اضافه کردن دستگاه‌ها

در این قسمت اضافه کردن میزبان‌های لینوکسی و ویندوزی به EventLog Analyzer به‌صورت جداگانه توضیح داده خواهد شد.

٤-٦-١ اضافه کردن دستگاه ویندوزی

برای دسترسی به صفحه‌ی اضافه کردن میزبان/دستگاه باید به یکی از روش‌های زیر عمل کرد.

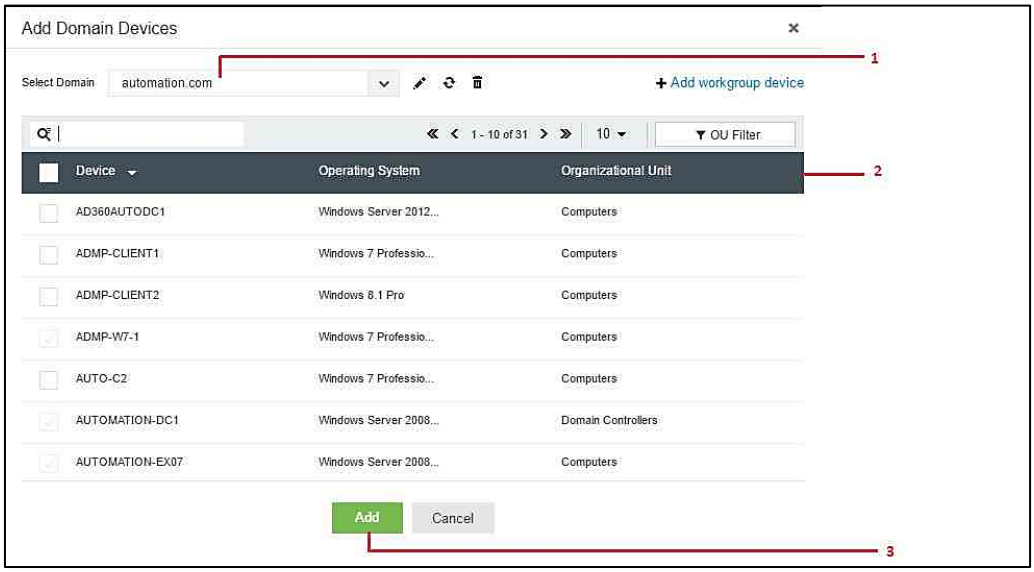
- در زبانه Home به مسیر Manage Devices > Devices > +Device بروید.
- در قسمت +ADD گزینه Device را انتخاب کنید.
- در زبانه Settings به مسیر Configurations > Device Managment > +Add Device(s) بروید.

دستگاه‌ها را می‌توان در یک گروه مشخص، گروه‌بندی کرد. گروه‌های پیش‌فرض شامل Windows Group، Unix Group و Defult Group (که شامل همه دستگاه‌ها می‌شود) هستند. برای اضافه کردن یک گروه میزبان روی پیوند ADD در کنار فیلد Device Group در صفحه Device Group Management کلیک کنید. در این صفحه می‌توان گروه‌ها را مدیریت کرد.

تمام میزبان‌های ویندوزی، که با EventLog Analyzer پایش می‌شوند باید WMI و DCOM را فعال داشته باشند. ثبت کردن وقایع برای module/objectهای مربوطه فعال است. دقت کنید که اگر EventLog Analyzer روی ماشین لینوکسی نصب شده باشد، قادر به جمع‌آوری فایل ثبت وقایع از روی ماشین‌های ویندوزی نمی‌باشد. بدین منظور می‌توان از برنامه دیگری به نام SNARE برای تبدیل فایل‌های ثبت وقایع ویندوزی به syslog استفاده کرد و آن‌ها را برای EventLog Analyzer فرستاد.

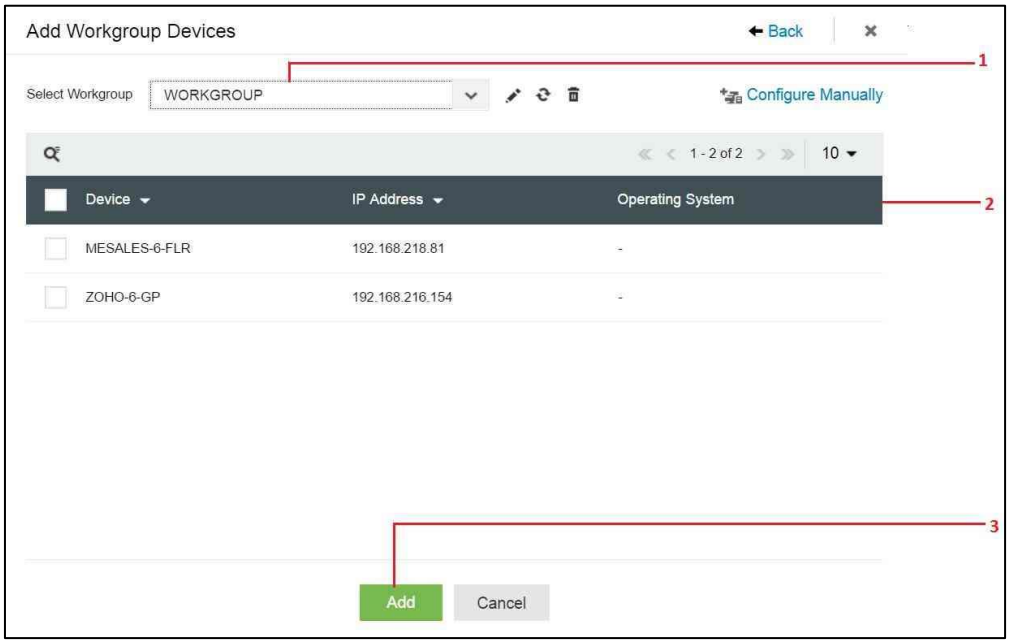
مراحل زیر را برای اضافه کردن یک دستگاه از دامنه انجام دهید.

١. از لیست، دامنه مورد نظر را انتخاب کنید. دستگاه‌های موجود در دامنه به صورت خودکار شناخته می‌شوند و نمایش داده می‌شوند.
٢. دستگاه(ها) مورد نظر را انتخاب کنید. با استفاده از گزینه OU Filter می‌توان جست‌وجوی مبتنی بر فیلتر روی OU ها برای پیدا کردن دستگاه مورد نظر را انجام داد.
٣. روی دکمه Add کلیک کنید تا دستگاه برای پایش اضافه شود.



شکل ۱۷- اضافه کردن دستگاه از دامنه

هم‌چنین می‌توان دستگاه را از یک Workgroup انتخاب کرد. برای این کار روی پیوند Add workgroup device کلیک کنید. لیست دستگاه‌های موجودر در Workgroup نمایش داده خواهند شد.



شکل ۱۸- اضافه کردن دستگاه از workgroup

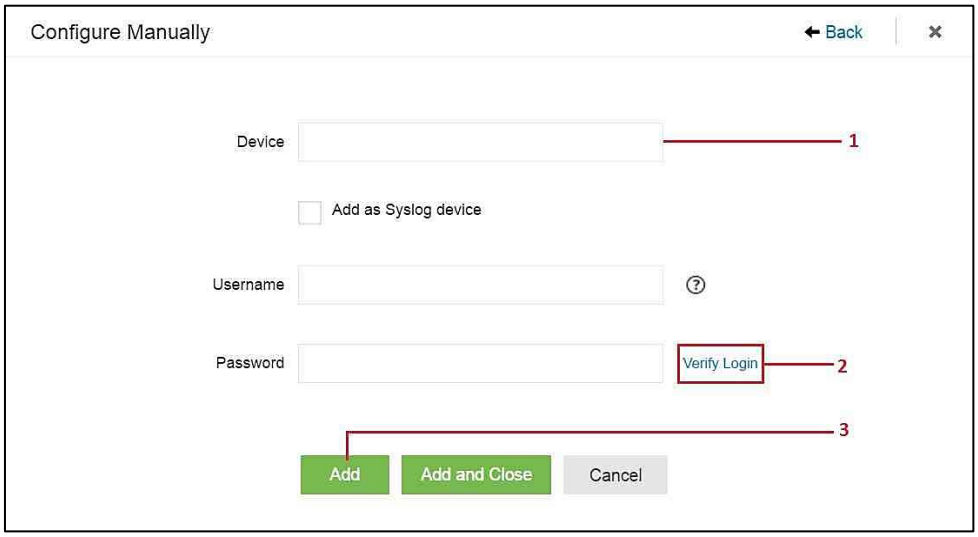
مراحل زیر را برای اضافه کردن دستگاه در workgroup انجام دهید.

۱. از منوی Select Workgroup گزینه workgroup را انتخاب کنید.

۲. دستگاه‌های مورد نظر را انتخاب کنید.

۳. برای پایش دستگاه‌ها روی دکمه Add کلیک کنید.

اضافه کردن یک دستگاه می‌تواند به‌صورت دستی نیز انجام شود. برای این کار روی پیوند Configure Manually کلیک کنید.

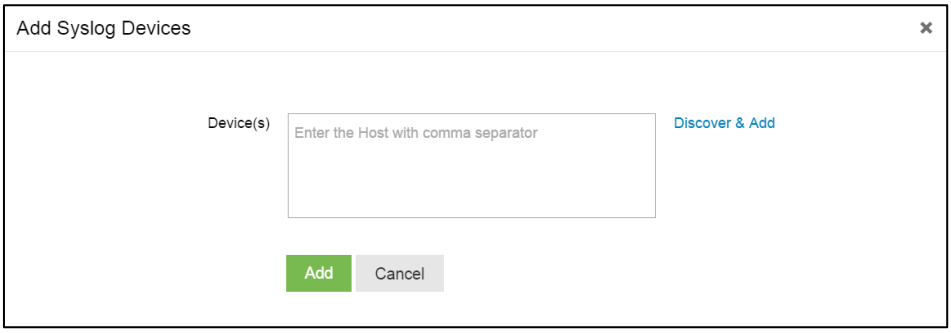


شکل ۱۹- اضافه کردن دستگاه به‌صورت دستی

۱. نام دستگاه و یا آدرس IP را وارد کنید. می‌توانید دستگاه را به‌عنوان یک دستگاه Syslog انتخاب کنید. برای این کار Add as Syslog device را انتخاب کنید.
۲. نام کاربری و رمز عبور را با اعتبارنامه مدیر وارد کنید. سپس روی پیوند Verify Login بزنید.
۳. روی دکمه Add کلیک کنید تا دستگاه برای پایش به لیست دستگاه‌ها اضافه شود.

٤-٦-٢ اضافه کردن دستگاه‌های Syslog

در صفحه Device Management به زبانه Syslog Devices بروید و روی دکمه Add Device(s)+ کلیک کنید.



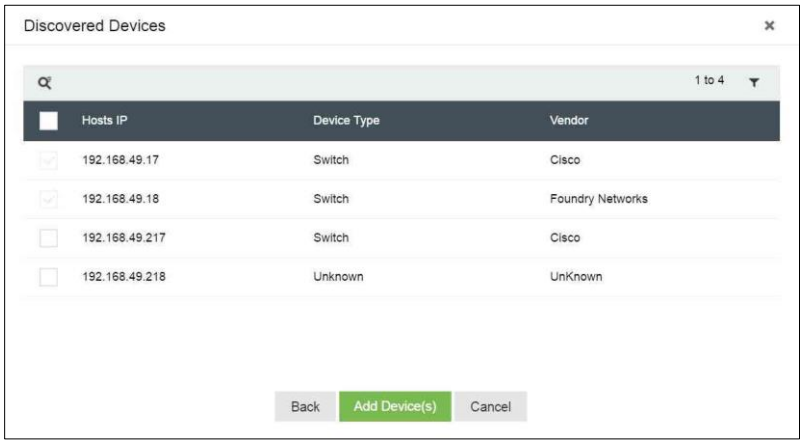
شکل ۲۰- اضافه کردن دستگاه‌های Syslog

نام دستگاه و یا آدرس IP را در فیلد Device(s) وارد کنید و دکمه Add را بزنید. گام‌های زیر را برای پیدا کردن خودکار دستگاه‌های syslog در شبکه انجام دهید.

۱. در پنجره‌ی Add Syslog Devices روی پیوند Discover & Add کلیک کنید. برای پیدا کردن دستگاه‌های Syslog در شبکه می‌توان از بازه IP یا CIDR نیز استفاده کرد.
۲. IP شروع و پایان یا بازه CIDR را به‌منظور پیدا کردن دستگاه‌های Syslog وارد کنید.

شکل ۲۱- مشخص کردن بازه شروع و انتهای IP برای دستگاه‌های Syslog

۳. شناسه SNMP را انتخاب کنید تا به‌طور خودکار دستگاه‌ها را در شبکه خود کشف کنید. به‌صورت پیش‌فرض شناسه عمومی SNMP برای استفاده به‌منظور کشف دستگاه‌ها استفاده می‌شود.
٤. هم‌چنین برای اضافه کردن شناسه SNMP می‌توان روی Add Credential+ کلیک کرد. زمانی‌که شناسه را انتخاب کردید، می‌توانید با زدن دکمه Scan به‌صورت خودکار دستگاه‌ها را پیدا کنید.
۵. دستگاه‌های مورد نظر را انتخاب کنید. با فیلتر براساس نوع دستگاه و شرکت تولید کننده می‌توان دستگاه مورد نظر را جست‌وجو کرد.

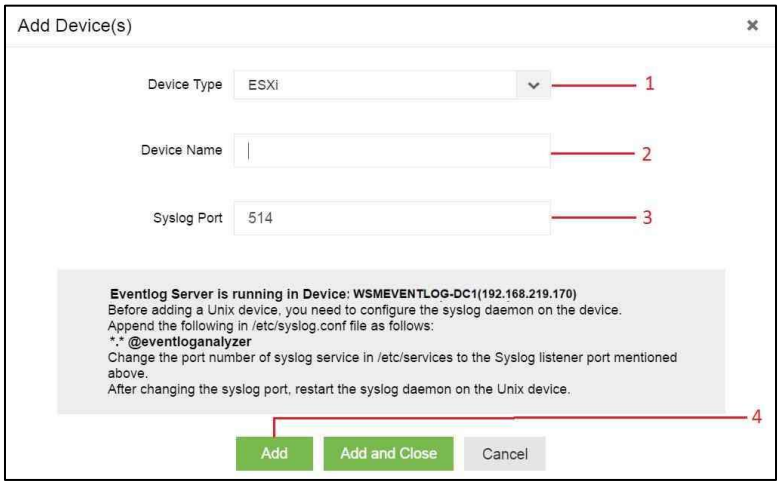


شکل ۲۲- انتخاب دستگاه از لیست دستگاه‌های کشف شده براساس بازه IP

۶. روی دکمه Add Device(s) برای اضافه شدن دستگاه برای پایش کلیک کنید.

٤-٦-٣ اضافه کردن سایر دستگاه‌ها

در صفحه Device Management روی زبانه Other Devices کلیک کنید.



شکل ۲۳- اضافه کردن سایر دستگاه‌ها

۱. نوع دستگاه (ESXi/IBM AS/400) را انتخاب کنید.

۲. نام دستگاه را وارد کنید.

۳. شماره درگاه syslog را وارد کنید.

٤. روی دکمه Add کلیک کنید تا به لیست دستگاه‌های مورد پایش اضافه شود.

۷-٤ جمع‌آوری فایل‌های ثبت وقایع برنامه‌های کاربردی

فایل‌های ثبت وقایع برنامه‌های کاربردی باید در برنامه EventLog Analyzer جمع‌آوری شوند. اما فایل‌های ثبت وقایع برنامه‌های Oracle، سرویس‌دهنده چاپ و برنامه IMB iSeries می‌توانند به‌صورت بی‌درنگ اضافه شوند. نرم‌افزار می‌تواند به‌صورت منظم و خودکار فایل‌های ثبت وقایع را جمع‌آوری کند.

برای جمع‌آوری فایل ثبت وقایع از برنامه‌ها ابتدا باید صفحه Import Log File را از طریق یکی از روش‌های زیر باز کنید.

- در زبانه Home به مسیر Applications > Actions > +Import بروید.
- در زبانه Home به مسیر Applications > Imported Logs > Import Log File بروید.
- در قسمت ADD+ گزینه Import Logs را انتخاب کنید.
- در زبانه Setting مسیر Configurations> Import logs> Import Log را انتخاب کنید.

سپس مراحل زیر را انجام دهید.

۱. برای جمع‌آوری فایل‌های ثبت وقایع ماشین محلی گزینه Local Host را انتخاب کنید. برای دسترسی به EventLog Analyzer نیز از وب استفاده کنید. حداکثر اندازه فایل برای جمع‌آوری فایل ثبت وقایع از ماشین محلی 1GB می‌باشد.

۲. برای جمع‌آوری فایل‌های ثبت وقایع از ماشین راه دور گزینه Remote Host را انتخاب کنید. حداکثر اندازه فایل برای جمع‌آوری فایل ثبت وقایع برنامه از ماشین راه دور 2GB می‌باشد.

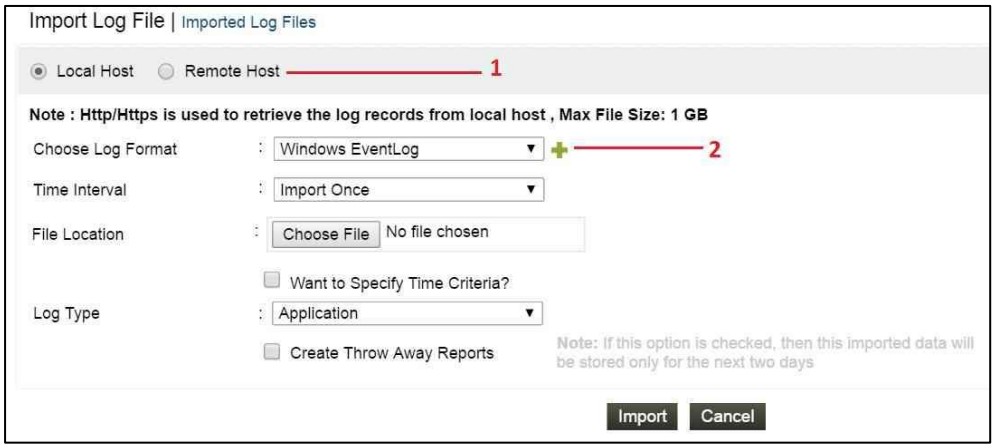
۳. قالب فایل ثبت وقایعی که قرار است جمع‌آوری شود را انتخاب کنید. (قالب‌های موجود شامل: IIS W3C Log، DHCP Windows ، MSSQL Server Logs ،IIS W3C FTP Logs ،Web Server Logs، DHCP linux logs، Syslogs ،Apache Access Logs ،IBM Maximo Logs است.)

٤. زمان‌بندی جمع‌آوری فایل ثبت وقایع از برنامه را انتخاب کنید (یک بار، هر یک ساعت، هر یک روز و غیره)

توجه کنید، در صورتی‌که در ابتدا Local Host را انتخاب کرده باشید، با انتخاب گزینه : Time Interval Import Once اجازه جمع‌آوری فایل‌های ثبت وقایع محلی از مشتری/میزبان‌های EventLog Analyzer داده می‌شود. اما با انتخاب زمان‌بندی دوره‌ای تنها اجازه جمع‌آوری فایل ثبت وقایع از سرویس‌دهنده EventLog Analyzer داده می‌شود.

۵. محل فایل مورد نظر را انتخاب کنید.

٦. روی دکمه Import کلیک کنید تا فرآیند جمع‌آوری فایل‌های ثبت وقایع آغاز شود.



شکل ٢٤- صفحه جمع‌آوری فایل ثبت وقایع از سایر برنامه‌های کاربردی

٤-٧-١ جمع‌آوری فایل‌های ثبت وقایع از ماشین راه دور

در صورتی‌که Remote Host را انتخاب کرده‌اید در قسمت File Location باید آدرس مکانی که فایل ثبت وقایع در ماشین راه دور ذخیره شده است را به‌صورت دستی تایپ کنید یا این‌که از پیوند Select Remote File برای به دست آوردن مکان فایل استفاده کنید.

١. از گزینه Want to Specify Time Criteria به‌منظور جمع‌آوری فایل‌های ثبت وقایع یک بازه‌ی خاص زمانی استفاده کنید. ابتدا و انتهای بازه زمانی را در فیلدهای From و To مشخص کنید. این گزینه تنها برای فایل‌های ثبت وقایع ویندوزی موجود است.

٢. برای قالب ثبت وقایع رویداد ویندوزی از لیست گزینه Log Type یکی از موارد Application، Security، DNS Server، File Replication Service و یا Directory Service را انتخاب کنید.

٣. گزینه Create Throw Away Reports را به‌منظور جمع‌آوری فایل ثبت وقایع برای تولید گزارش موقت انتخاب کنید. فایل‌های ثبت وقایع جمع‌آوری شده برای مدت دو روز نگه‌داری می‌شوند و بعد از این مدت پاک می‌شوند.

٤-٨ پشتیبان‌گیری از پایگاه‌داده

در این قسمت فرآیند پشتیبان‌گیری از پایگاه‌داده‌های PostgreSQL، MySQL و MS SQL توضیح داده می‌شود. توجه شود که قبل از فرآیند پشتیان‌گیری باید سرویس‌دهنده‌ی EventLog Analyzer متوقف شود.

٤-٨-١ پشتیبان‌گیری از پایگاه‌داده PostgreSQL

برای پشتیبان‌گیری از پایگاه‌داده PostgreSQL کافی است که محتویات پوشه <EventLog Analyzer Home>\pgsql را به‌صورت یک فایل Zip مانند pgsql_backup.zip درآورید و در مسیر <EventLog Analyzer Home> ذخیره کنید.

٤-٨-٢ پشتیبان‌گیری از پایگاه‌داده MySQL

برای پشتیبان‌گیری مشابه پایگاه‌داده PostgreSQL عمل کنید و در مسیر <EventLog Analyzer Home>\mysql ذخیره کنید.

٤-٨-٣ پشتیبان‌گیری از پایگاه‌داده MS SQL

١. با استفاده از دستور زیر مکان فعلی داده و فایل ثبت وقایع پایگاه‌داده eventlog را پیدا کنید.

```
use eventlog
go
sp_helpfile
go
```

٢. با استفاده از دستور زیر اتصال پایگاه‌داده را قطع کنید.

```
use master
go
sp_detach_db 'eventlog'
go
```

٣. از فایل داده و فایل ثبت وقایع در مکان فعلی <MSSQL_Home>\data\eventlog.mdf و <MSSQL_Home>\data\eventlog_log.LDF پشتیبان بگیرید و در مسیر جدید < New Location>\eventlog.mdf و <New Location>\eventlog_log.LDF ذخیره کنید.

٤. پایگاه‌داده را دوباره متصل کنید و با استفاده از دستور زیر به مکان قبلی اشاره کنید.

```
use master
go
sp_attach_db 'eventlog' , '<MSSQL Home>/data/eventlog.mdf' ,<MSSQL_Home>/data/eventlog_log.LDF
go
```

۹-٤ پیکربندی گزارش‌های EventLog Analyzer

زبانه Reports در UI نرم‌افزار EventLog analyzer گزارش‌های آماده بسیاری را پیشنهاد داده است. گزارش‌ها می‌توانند در صورت لزوم برنامه‌ریزی شوند. برای دادن مجوز به گزارش‌های از پیش ساخته باید پیکربندی زیر را در دستگاه‌های ویندوزی انجام دهید.

۱. Regedit.msc را باز کنید.

۲. به مسیر HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Service > eventlog بروید.

۳. کلیدهای جدول ۹ را ایجاد کنید.

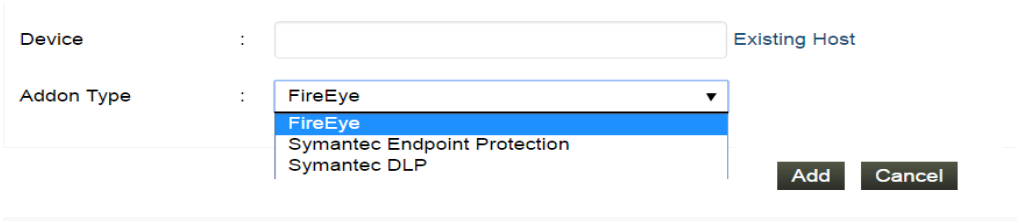
جدول ۹- ایجاد کلید برای پیکربندی گزارشات

گزارش‌ها	کلید جدید
Program Inventory Reports	Microsoft-Windows-Application-Experience/Program-Inventory
Application Whitelisting Reports	Microsoft-Windows-AppLocker/EXE and DLL Microsoft-Windows-AppLocker/MSI and Script
Windows Backup & Restore Reports	Microsoft-Windows-Backup
Windows Firewall Auditing Reports	Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
USB Plugged in & out	Microsoft-Windows-DriverFrameworks-UserMode/Operational
Windows System Events	Microsoft-Windows-GroupPolicy/Operational Microsoft-Windows-NetworkProfile/Operational Microsoft-Windows-WindowsUpdateClient/Operational Microsoft-Windows-Winlogon/Operational Microsoft-Windows-WLAN-AutoConfig/Operational Microsoft-Windows-TerminalServices-Gateway/Operational Microsoft-Windows-TerminalServices-RDPClient/Operational Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational Microsoft-Windows-Wired-AutoConfig/Operational
Hyper-V Server Events Hyper-V VM Management Reports	Microsoft-Windows-Hyper-V-Worker-Admin Microsoft-Windows-Hyper-V-VMMS-Storage Microsoft-Windows-Hyper-V-VMMS-Networking Microsoft-Windows-Hyper-V-VMMS-Admin Microsoft-Windows-Hyper-V-Hypervisor-Operational

۱۰-٤ اضافه کردن محصول تحلیل تهدید

برای اضافه کردن محصول تجزیه و تحلیل تهدیدات باید طبق مراحل زیر عمل کنید.

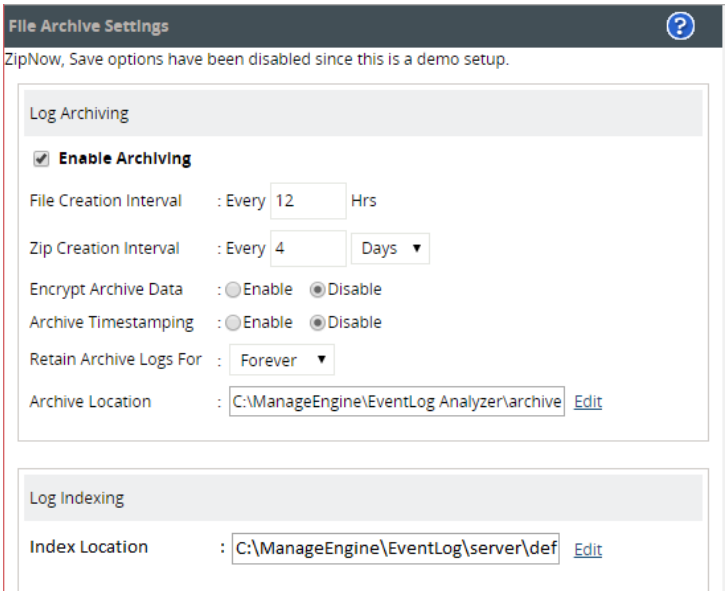
۱. به مسیر Settings > Configurations > Threats > Add Source بروید.
۲. دستگاهی که محصول روی آن نصب است را انتخاب کنید. تمامی فایل‌های ثبت وقایع از روی این دستگاه انتخاب می‌شوند.
۳. نوع برنامه را انتخاب کنید.



شکل ۲۵- انتخاب محصول برای تجزیه و تحلیل تهدیدات

۱۱-٤ پیکربندی بایگانی فایل‌های ثبت وقایع

در این قسمت پیکربندی بازه‌های بایگانی، مدت زمان نگه‌داری، گزینه‌های رمزنگاری، برچسب زمانی فایل‌ها و مکان ذخیره‌سازی برای نگه‌داری فایل‌ها توضیح داده می‌شود.



شکل ۲٦- تنظیمات بایگانی فایل

۱. از فعال بودن گزینه انتخاب جهت بایگانی، اطمینان حاصل کنید.

۲. فایل‌های ثبت وقایع در فایل‌های یک دست در دوره زمانی ۱۲ ساعته نوشته می‌شوند. در صورت دلخواه می‌توان بازه زمانی را تغییر داد.
۳. این فایل‌های یک دست به‌صورت دوره‌ای برای کاهش فضا (نسبت ۲۰:۱) به‌صورت فشرده در می‌آیند. به‌صورت پیش‌فرض این دوره ٤ روز درنظر گرفته شده است که قابل تغییر است.
٤. برای امنیت فایل‌های بایگانی، گزینه رمزنگاری را فعال کنید. به‌صورت پیش‌فرض این گزینه غیرفعال است.
٥. برای تضمین درستی فایل‌ها برچسب زمانی فایل‌ها را فعال کنید. به‌صورت پیش‌فرض این گزینه غیر فعال است.
٦. دوره زمان نگه‌داری فایل را انتخاب کنید. به‌صورت پیش‌فرض "برای همیشه" انتخاب شده است.
۷. مکان ذخیره‌سازی پیش‌فرض فایل‌های بایگانی در شکل ۲۳ نشان داده شده است. در صورت نیاز می‌توان آن را با استفاده از پیوند Edit تغییر داد.
۸. مکان ذخیره‌سازی پیش‌فرض داده‌های اندیس شده در شکل ۲۳ نشان داده شده است. در صورت نیاز می‌توان آن را با استفاده از پیوند Edit تغییر داد.
۹. تنظیمات را ذخیره کنید و پنجره را ببندید. برای گرفتن بایگانی در همین لحظه روی دکمه Zip Now کلیک کنید.

در صورتی‌که بخواهید یک کلید پویا برای رمزنگاری فایل‌های بایگانی تنظیم کنید، باید مراحل زیر را دنبال کنید:

۱. به مکان بایگانی بروید. به‌صورت پیش‌فرض، فایل‌ها در مسیر <EventLog Analyzer Home>\archive ذخیره شده است. یک فایل با نام EncryptedKey.enc ایجاد کنید.
۲. فایل را با استفاده از یک ویرایشگر باز کنید و کلید پویا را به‌عنوان متن وارد کنید. کلید باید دقیقا شامل ١٦ کاراکتر از نظر طولی باشد.
۳. سرویس‌دهنده EventLog Analyzer را دوباره اجرا کنید.

در صورتی‌که بخواهید فایل‌های بایگانی شده را با این کلید پویا در نسخه دیگری از EventLog Analyzer جمع‌آوری کنید، مراحل زیر را دنبال کنید:

۱. فایل EncryptedKey.enc را در مکان بایگانی محصول کپی کنید.
۲. محصول را دوباره اجرا کنید.

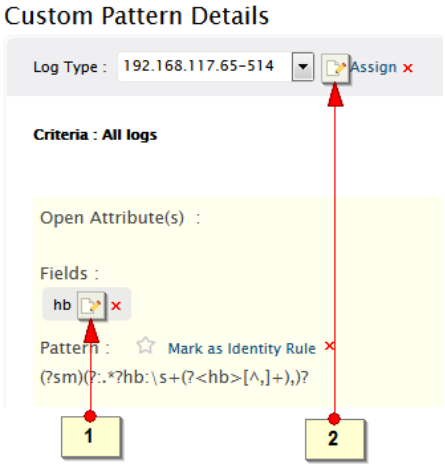
۳. فایل‌های بایگانی مورد نیاز را وارد کنید.

٤-۱۲ سفارشی کردن الگو برای تجزیه‌کننده

در این بخش نحوه ویرایش الگوی سفارشی، حذف و تغییر تجزیه‌کننده و غیره، توضیح داده می‌شود.

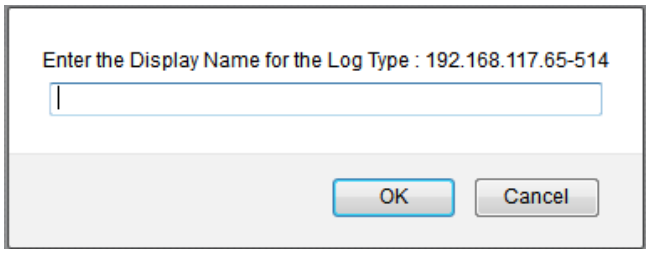
٤-۱۲-۱ ویرایش الگو سفارشی

در این قسمت می‌توان نام فیلدها و نوع فایل ثبت وقایع را تعیین کرد.



شکل ۲۷- تغییر الگو سفارشی

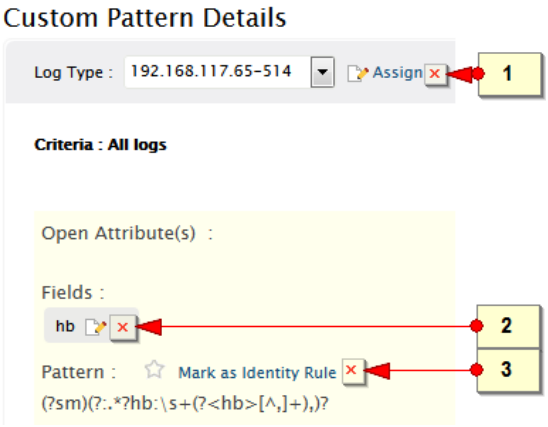
- برای ویرایش نام فیلد روی آیکون Field Edit کیک کنید و نام جدید را وارد کنید. (شماره ۱ در شکل ۲۷)
- برای ویرایش نوع فایل روی آیکون Log Type Edit کلیک کنید و نام نوع فایل را وارد کنید.(شماره ۲ در شکل ۲۷)



شکل ۲۸- وارد کردن نام برای نوع فایل ثبت وقایع

- برای حذف نوع فایل ثبت وقایع جدید روی آیکون Log Type Delete کلیک کنید. حذف کردن نوع فایل باعث حذف قوانین تجزیه‌کننده برای این نوع فایل می‌شود. (شماره ۱ در شکل ۲۹)

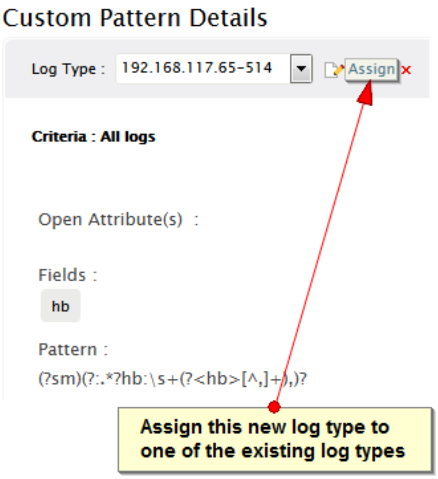
- برای حذف فیلد جدید روی Field Delete کلیک کنید. (شماره ۲ در شکل ۲۹)
- برای حذف الگوی جدید روی آیکون Pattern Delete کلیک کنید. (شماره ۳ در شکل ۲۹)



شکل ۲۹- تغییر الگوی سفارشی

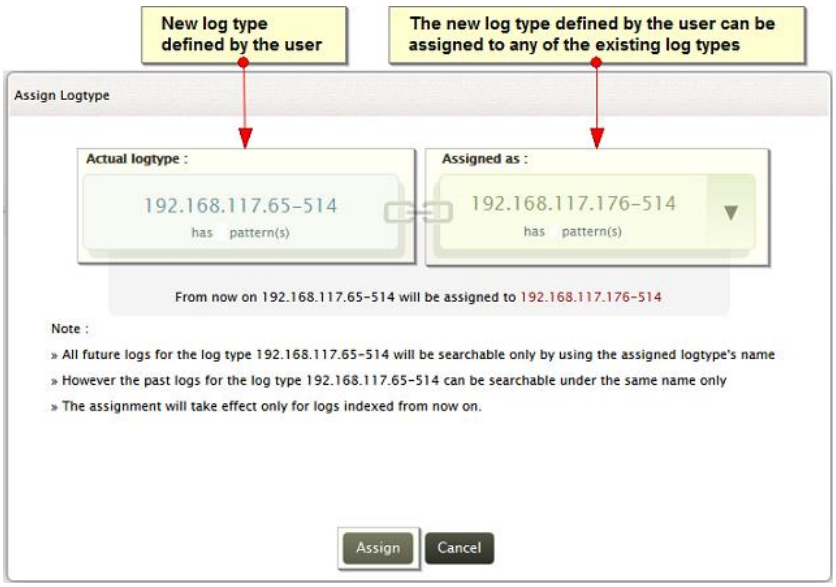
٤-۱۲-۲ انتساب نوع فایل ثبت وقایع به نوع فایل دیگر

نوع فایل ثبت وقایع می‌تواند به یک نوع فایل دیگر تخصیص داده شود. در این مورد تجزیه‌کننده قوانین نوع فایل اصلی نشان داده نخواهد شد و تجزیه‌کننده‌ی نوع فایل جدید اعمال خواهد شد. فرآیند انجام این کار در ادامه توضیح داده می‌شود.



شکل ۳۰- انتخاب نوع فایل ثبت وقایع

- روی آیکون Assign کلیک کنید.
- نوع فایل جدید توسط کاربر تعریف می‌شود و به یکی از نوع فایل های موجود تخصیص داده می‌شود.
- روی دکمه Assign جهت اعمال کلیک شود.



شکل ۳۱- انتساب نوع فایل ثبت وقایع

۵ جمع‌بندی

یکی از مهم‌ترین نیازهای بخش فناوری اطلاعات در سازمان‌ها، امنیت اطلاعات و مدیریت رویدادها می‌باشد. فایل‌های ثبت وقایع تولید شده توسط ماشین اطلاعات حیاتی برای تشخیص ناهنجاری در شبکه و مشکلات کارایی سیستم‌ها هستند. تحلیل کارایی فایل‌های ثبت وقایع به کم شدن مدت خاموشی سیستم‌ها، افزایش کارایی شبکه و محکم کردن سیاست‌های یک سازمان کمک می‌کند. از طرفی با توجه به گسترده شدن حجم تولید فایل‌های ثبت وقایع دیگر امکان بررسی دستی این اطلاعات نمی‌باشد و نیازمند یک سیستم خودکار با قابلیت‌های تحلیل و بررسی و گزارش‌دهی و سایر امکانات وجود دارد.

ManageEngines's EventLogAnalyzer یکی از مقرون‌به‌صرفه‌ترین نرم‌افزارهای امنیت اطلاعات و مدیریت رویدادها در بازار می‌باشد. توسط EventLogAnalyzer تمام فرآیند مدیریت فایل‌های ثبت وقایع تولید شده شامل جمع‌آوری، تحلیل، جست‌وجو، گزارش‌گیری و بایگانی در یک میز فرمان مرکزی صورت می‌گیرد. در این گزارش درباره ویژگی‌های کلیدی این محصول شامل اطمینان از صحت فایل، تحلیل‌های جرم‌یابی رویداد، هشدارهای وقایع بی‌درنگ، بایگانی و گزارش وقایع رویداد، تحلیل هوشمند رویداد و تضمین پیروی از مقررات، تولید گزارش فوری و متنوع و غیره بحث گردید و پیکربندی‌های مرتبط با آن‌ها و نحوه‌ی نصب اولیه محصول توضیح ارائه گردید.