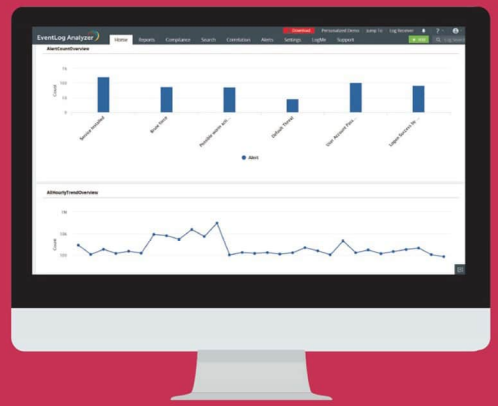
ManageEngine

# EventLog Analyzer

## مدیریت متمرکز لاگ‌ها، شناسایی تهدیدات و انطباق با استانداردهای امنیتی

## شریک ایده‌آل شما در امنیت و حسابرسی فناوری اطلاعات



## درباره EVENTLOG ANALYZER

EVENTLOG ANALYZER یک راهکار تحت وب برای مدیریت لحظه‌ای (REAL-TIME) لاگ‌ها و رعایت الزامات انطباق IT (IT COMPLIANCE) است که سازمان‌ها را در مقابله با تهدیدات و حملات امنیتی شبکه یاری می‌کند. این نرم‌افزار با ارائه قابلیت‌های جامع مدیریت لاگ، امکان جمع‌آوری، تحلیل و گزارش‌دهی لاگ‌ها را از منابع مختلف فراهم کرده و فرآیندهای بازرسی و حسابرسی (AUDITING) را ساده و مؤثر می‌سازد.

علاوه بر این، EVENTLOG ANALYZER شامل گزارش‌ها و هشدارهای آماده (OUT-OF-THE-BOX) است که به سرعت الزامات سخت‌گیرانه چارچوب‌های قانونی و استانداردهای نظارتی IT را پوشش می‌دهد، و سازمان‌ها را قادر می‌سازد به صورت سریع و مطمئن در برابر مشکلات امنیتی و ریسک‌های انطباق واکنش نشان دهند.


MR LICENSE

WWW.MRLICENSE.NET
INFO@MRLICENSE.NET


- مدل لایسنس‌گذاری منعطف؛ پرداخت متناسب با نیاز سازمان
- استقرار سریع و راه‌اندازی بدون پیچیدگی
- رابط کاربری هوشمند و کاربرپسند

### سادگی در استقرار و بهره‌برداری

## مزیت راهکار

### پوشش جامع و یکپارچه

- همبسته‌سازی پیشرفته رویدادها
- تهدیدشناسی پویا مبتنی بر هوش تهدیدات جهانی
- مدیریت متمرکز و کارآمد حوادث امنیتی

### فناوری پیشرفته و به‌روز

- پشتیبانی از بیش از 700 منبع ثبت رویداد
- سازگاری با بیش از 50 تولیدکننده معتبر جهانی
- بیش از 1000 قالب گزارش و پروفایل هشدار از پیش

لاگ‌های ویندوز و SYSLOG دستگاه‌ها نمایی لحظه‌ای از فعالیت‌ها و رویدادهای جاری در سیستم‌ها و شبکه ارائه می‌دهند. تحلیل دقیق این داده‌ها برای شناسایی تهدیدات و ناهنجاری‌های امنیتی ضروری است.

EVENTLOG ANALYZER راهکاری مقرون به صرفه و کاربرپسند است که با تحلیل متمرکز لاگ‌ها و ارسال هشدارهای بلادرنگ و گزارش‌های زمان‌بندی شده، امکان نظارت مستمر بر وضعیت شبکه را فراهم می‌کند. این نرم‌افزار با قابلیت‌های پیشرفته تشخیص رویداد، در سطح سامانه‌های شناسایی نفوذ (IDS) عمل می‌کند و به کشف سریع تهدیدات کمک می‌نماید.

**Jim Lloyd**
Information Systems Manager,
First Mountain Bank

# امنیت شبکه
## NETWORK SECURITY

### همبستگی لحظه‌ای رویدادهای لاگ

تشخیص سریع رخدادهای امنیتی با تحلیل همزمان رویدادها در سراسر شبکه. شامل بیش از 30 قانون همبستگی از پیش تعریف‌شده و امکان ساخت قوانین همبستگی سفارشی برای نیازهای خاص سازمان.

### هوش تهدید پویا (DYNAMIC THREAT INTELLIGENCE)

شناسایی تعاملات با موجودیت‌های مخرب از طریق ماژول هوش تهدید داخلی، برای پیشگیری سریع و مؤثر از حملات امنیتی.

### تحلیل و جرم‌شناسی پیشرفته لاگ‌ها

جستجوی سریع و دقیق در حجم بالای لاگ‌ها
با بهره‌گیری از قابلیت‌های جستجوی پیشرفته و فیلترهای منعطف.
شناسایی علت اصلی حملات و رخدادهای امنیتی
برای درک دقیق نحوه وقوع نفوذ و جلوگیری از تکرار آن.
پشتیبانی از تحقیقات جرم‌شناسی دیجیتال
تحلیل شواهد ثبت‌شده در لاگ‌ها برای بررسی عمیق حوادث امنیتی و مستندسازی آن‌ها.

### تحلیل و جرم‌شناسی پیشرفته لاگ‌ها

- سیستم داخلی ثبت و پیگیری تیکت‌ها

تبدیل خودکار رخدادها به تیکت برای تخصیص، پیگیری وضعیت و تسریع در رفع مشکل.

- یکپارچه‌سازی با ابزارهای HELP DESK سازمانی

ارسال اطلاعات حوادث و ایجاد تیکت در سیستم‌هایی مانند SERVICENOW، SERVICEDESK PLUS، JIRA و ZENDESK برای مدیریت متمرکز و سریع‌تر رخدادها.

# حسابرسی و تحلیل پیشرفته رویدادها

### حسابرسی و تحلیل عمیق لاگ‌ها

بیش از 1000 گزارش و هشدار از پیش آماده برای تحلیل دقیق رویدادها از منابع مختلف لاگ، شامل:

- تجهیزات شبکه:
  تغییرات در پیکربندی‌ها و قوانین
  سوءاستفاده از حساب‌های کاربری دارای دسترسی ویژه
  تلاش‌های ناموفق ورود به سیستم
- اپلیکیشن‌ها:
  فعالیت‌های پایگاه داده
  بررسی یکپارچگی ستون‌ها
  تغییرات در حساب‌های کاربری
- سرورها و ایستگاه‌های کاری:
  فعالیت‌های ورود به سیستم
  تغییرات در رجیستری
  دستورات اجراشده در سیستم
- شناسایی آسیب‌پذیری‌ها و درگاه‌های پرخطر شبکه:
  شناسایی آسیب‌پذیری‌های بحرانی
  پورت‌های باز و در معرض تهدید

### پایش لحظه‌ای یکپارچگی فایل‌های حیاتی در ویندوز و لینوکس (FIM)

ردیابی سریع هرگونه تغییر غیرمجاز در فایل‌ها و پوشه‌های حساس سازمان، برای جلوگیری از دستکاری، خطا یا تهدیدهای امنیتی.

# مدیریت لاگ و انطباق با استانداردهای امنیتی

### جمع‌آوری هوشمند و یکپارچه لاگ‌ها برای کنترل کامل زیرساخت IT ازیرساخت IT

- پایش لاگ‌های سرورها، اپلیکیشن‌ها و تجهیزات شبکه
- شناسایی خودکار و بدون خطای منابع تولید لاگ
- جمع‌آوری متمرکز و امن لاگ ها با معماری منعطف
- تحلیل پیشرفته با PARSER سفارشی و انعطاف‌پذیر

### آرشیو امن و بلندمدت لاگ‌های سازمانی

نگهداری منعطف داده‌های لاگ مطابق با سیاست های داخلی و الزامات نظارتی
حفظ یکپارچگی آرشیو با TIME STAMPING و HASHING پیشرفته

### مدیریت یکپارچه و هوشمند الزامات COMPLIANCE سازمانی

- گزارش‌ها و هشدارهای آماده برای استانداردهای PCI DSS، FISMA، ISO 27001، GLBA، HIPAA، SOX و GDPR جهت تسهیل فرآیند بررسی، ارزیابی و تطبیق عملکرد سیستم‌ها با استانداردها و الزامات مشخص
- ایجاد گزارش‌های انطباق سفارشی متناسب با مقررات داخلی و الزامات آینده