

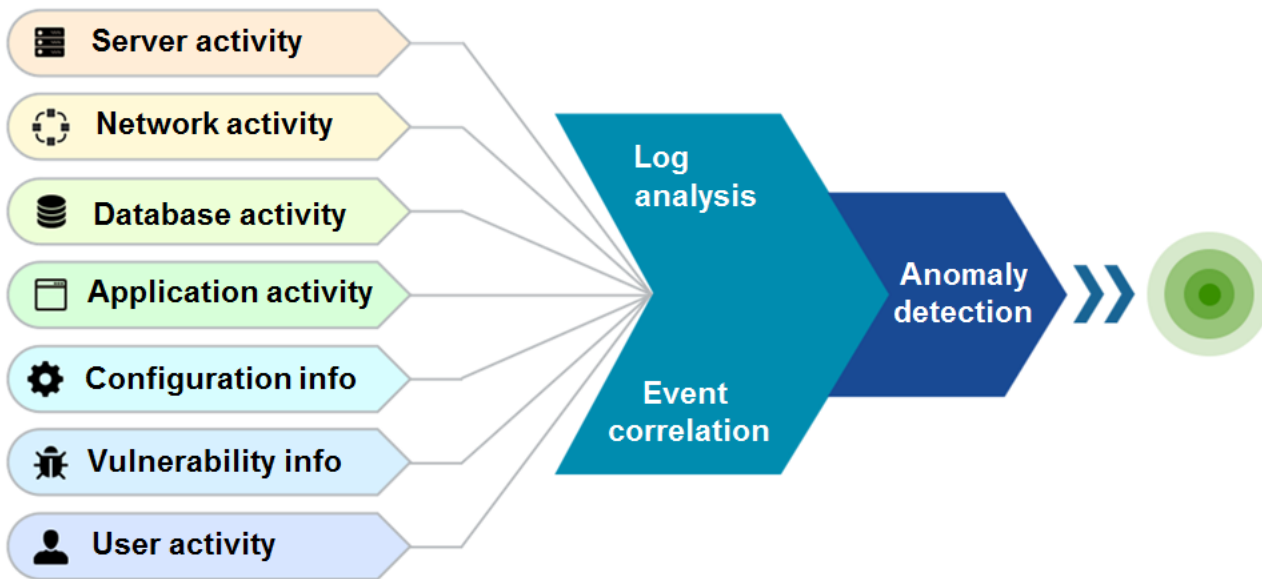


ManageEngine   
EventLog Analyzer

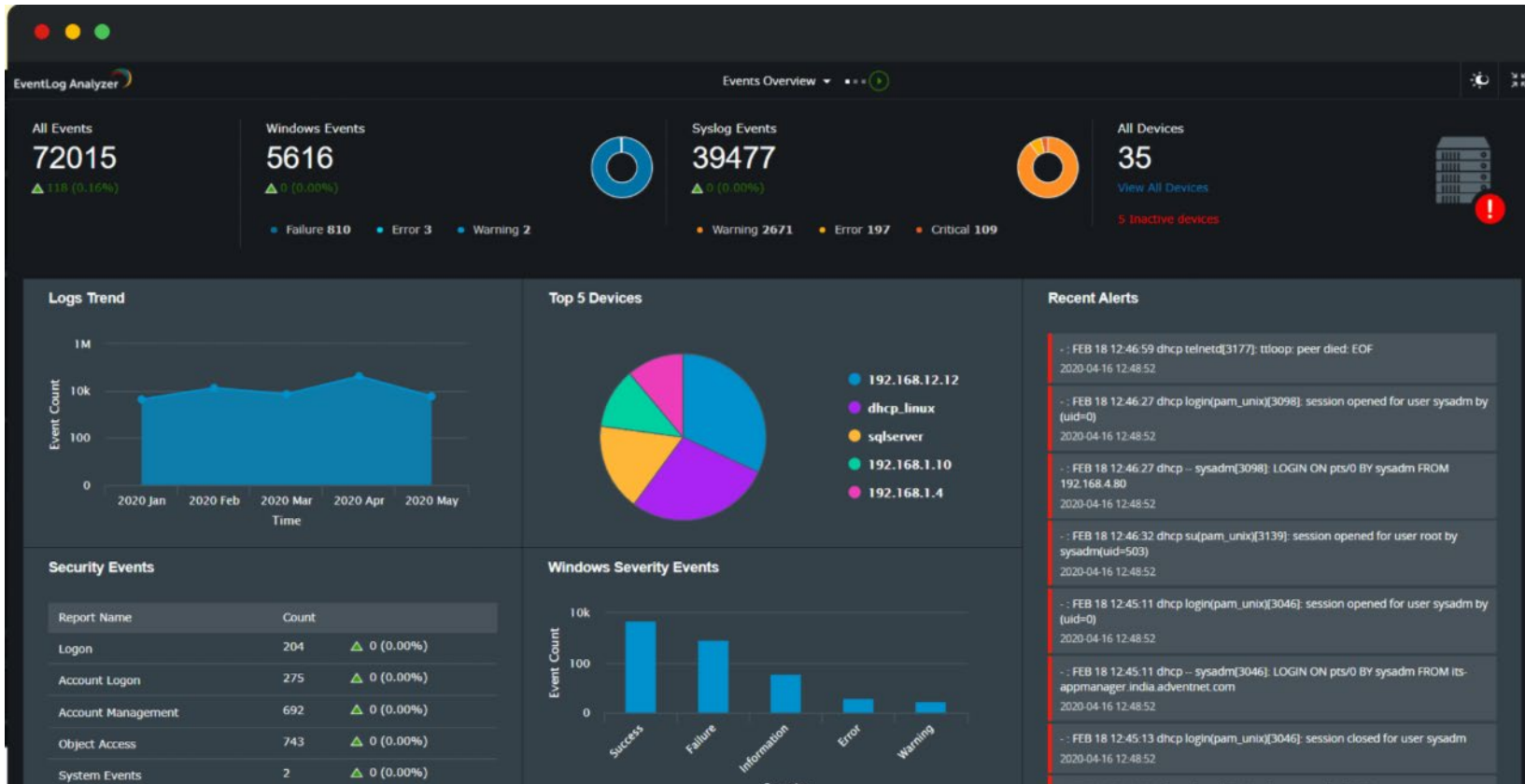
**종합  
로그 관리 솔루션**

[www.eventloganalyzer.com](http://www.eventloganalyzer.com)

# EventLog Analyzer의 기능



# Dashboard (1)



# Dashboard (2)



# 목 차

---

## 1. 로그 관리

- 로그 수집
- 로그 분석
- 로그 상관 관계 분석
- 로그 장기 보관

## 2. 종합 감사

- 네트워크 장치 감사
- 애플리케이션 감사

## 3. 위협 인텔리전스 (Threat intelligence)

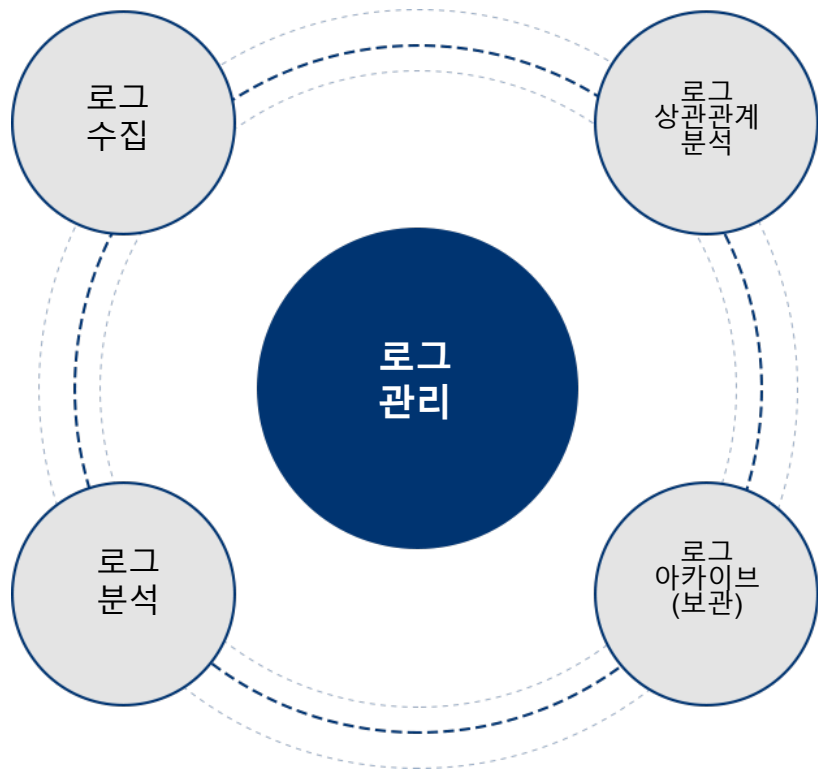
- 위협 피드 알림
- 사건 관리

## 4. 통합 규정 준수 관리 시스템

## 5. 제품 차별화 요소

# 로그 관리

---



# 로그 수집

---

- 에이전트 기반 및 에이전트 없는 로그 수집 방법을 모두 지원.
- 600개 이상의 로그 소스를 지원.
  - 네트워크 장치: 라우터, 스위치, IDS/IPS 및 방화벽
  - Windows 및 Linux/Unix 서버, IBM AS400
  - Oracle 및 Microsoft SQL Server
  - Apache 및 IIS 서버
  - 취약점 스캐너, 위협 인텔리전스 솔루션 등
- 사용자 지정 장치, 사내 응용 프로그램 등이 발생하는 사람이 읽을 수 있는 모든 로그 형식을 구문 분석 가능.

# 지원되는 Log Source (1)

---



## Database Platforms

- [Microsoft SQL Servers](#)
- [Oracle On-premises Databases](#)



## Routers and Switches

- [Cisco](#)
- [Hewlett-Packard](#)



## Vulnerability Scanners

- [Nessus](#)
- [Nmap](#)
- [Nexpose](#)
- [OpenVAS](#)
- [Qualys](#)



## Web Servers

- [Apache HTTP Server](#)
- [Microsoft IIS](#)



## Hypervisors

- [Microsoft Hyper-V](#)
- [VMware](#)



## Linux and Unix Systems

- [Linux](#)
- [IBM AIX](#)
- [HP UX](#)
- [Solaris](#)



# 지원되는 Log Source (2)

---



## Firewalls, NGFWs, IDS, and IPS

- [Barracuda](#)
- [Check Point](#)
- [Cisco](#)
- [Cisco Meraki](#)
- [Cyberoam](#)
- [Fortinet](#)
- [Huawei](#)
- [Juniper](#)
- [Juniper NetScreen](#)
- [Palo Alto](#)
- [pfSense](#)
- [SonicWall](#)
- [Sophos](#)
- [Watchguard](#)
- [F5 firewall](#)



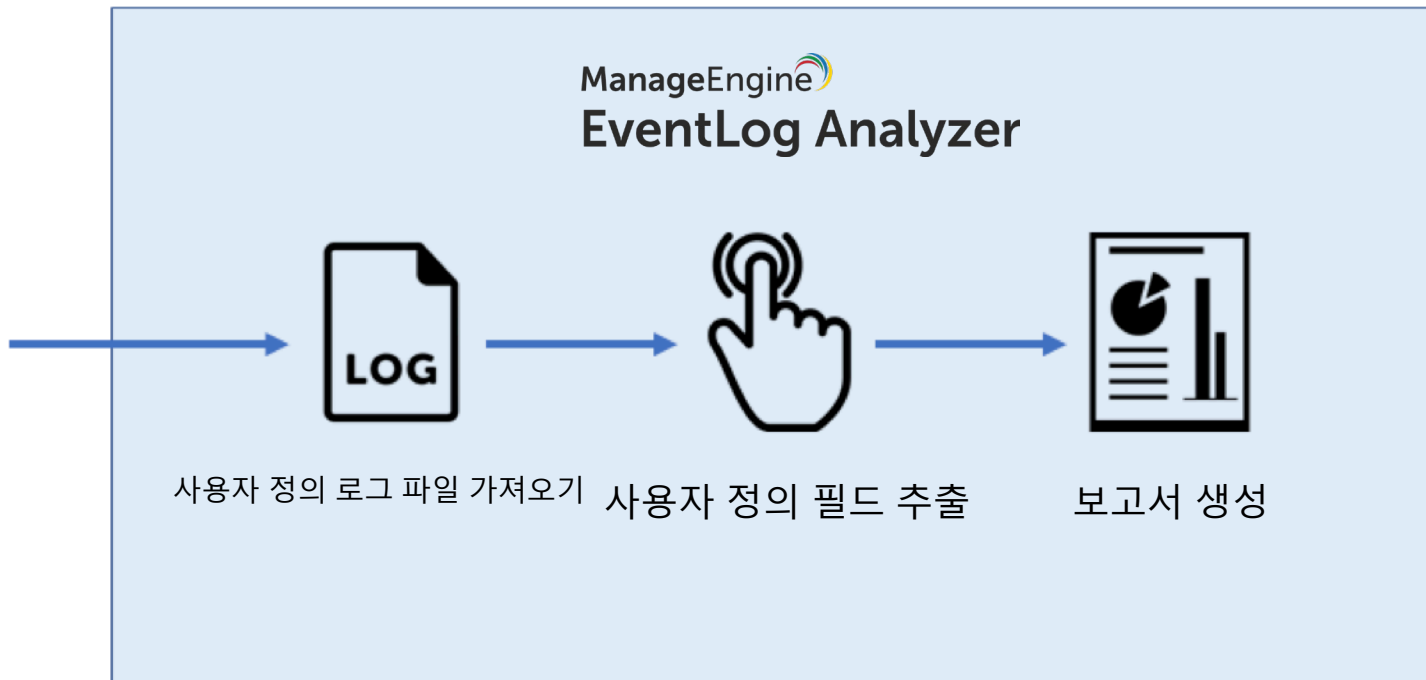
## Endpoint Security Solutions

- ESET Antivirus
- Kaspersky Antivirus
- Microsoft Antimalware
- Norton Antivirus
- Sophos Antivirus
- [FireEye](#)
- Malwarebytes
- [McAfee](#)
- [Symantec Endpoint Protection](#)

# 로그 수집: 사용자 정의 로그 구문 분석



관리자



# 로그 수집: 사용자 정의 로그 구문 분석

The screenshot displays a log analysis application interface. At the top, it shows 'Log Type : admp-app2-cogserv...' and 'Logs from the file - cogserver.log'. Below this, there are sections for 'Default Fields' and a list of log messages. A dialog box titled 'Extract Additional Fields' is open, showing a list of log messages with a search filter '7652'. The dialog also displays a 'Matched Log Messages (23)' section with a list of messages. A 'Details for field value : 7652' section shows a 'Field Name \* Port\_number' and a 'Field Value' field. At the bottom of the dialog, there is a 'Generated Pattern' section with a pattern '(?sm)(?:(?<Port\_number>.+)?)s+'. The dialog has 'Save Pattern', 'Cancel', and 'Ask Support' buttons.

Log Type : admp-app2-cogserv... Logs from the file - cogserver.log Showing: 1 - 20 of : 24

Default Fields

All Message : 10.38.12.85:9300 7652 2010-03-03 17:37:45.010 -5 EDEA0CACED8602F1C883EAF558AA3E8EAAA19E90 dv2ws92MIs42qMssMq22wwhdG4vC9hsG2MhGyll 687 Thread-2707 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute

IPAddress (23)

URI (

URI1

URI2

URI3

URI4

URI5

Port

MAC

Email

Usage

Execu

Execu

Execu

Execu

Extract Additional Fields

Log Type : admp-app2-cogserver.log Matched Log Messages (23) | Unmatched Log Messages (1) | X

Select & click the field value to be extracted

10.38.12.85:9300 7652 2010-03-03 17:37:47.838 Message : 10.38.12.85:9300 7652 2010-03-03 17:37:45.010 -5 EDEA0CACED8602F1C883EAF558AA3E8EAAA19E90 dv2ws92Ms42qMssMq22wwhdG4vC9hsG2MhGyll 687 Thread-2707 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute

Field Name(s) should only be alphanumeric. i.e [a-zA-Z0-9\_@.-]

Details for field value : 7652

Field Name \* Port\_number Field Value

Generated Pattern : Validate this pattern (or) Choose and generate a pattern

(?sm)(?:(?<Port\_number>.+)?)s+

Save Pattern Cancel Ask Support

Message : 10.38.12.85:9300 7652 2010-03-03 17:37:46.010 -5 B64467B4285B805FDC916314C3964A71F2B14A04 jy2Mshj8 GMC4sqh9Ch2MG4y8C2vC99GqMjGMlvd 42178 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

Message : 10.38.12.85:9300 7652 2010-03-03 17:37:47.838 -5 B64467B4285B805FDC916314C3964A71F2B14A04 sG2v8lM w8lG9sy9vG9j8sqll22vsq2sG84wq9ll 42180 Thread-26316 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

Message : 10.38.12.85:9300 7652 2010-03-03 17:37:47.978 -5 B64467B4285B805FDC916314C3964A71F2B14A04 ylsyq9lw2 dv8w8q2jv8vlls4ww44d4qj2hlvj 42182 Thread-10906 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/contentManagerService/1

Message : 10.38.12.85:9300 7652 2010-03-03 17:37:52.088 -5 86446784285B805FDC916314C3964A71F2B14A04 w4vqY8C4Cs2q8qq29h282GsGICv9lvj9Cq 3 Thread-6574 DISP 732 4 Audit.Other.dispatcher.DISP.com.cognos.pogo.handlers.engine.ServiceLookupHandler http://developer.cognos.com/schemas/reportService/1.absolute

760 -5 EDEA0CACED8602F1C883EAF558AA3E8EAAA19E90 hc44j2qww44Cy8jG89ys9hg45wh92C9vd8Gww8 39172 Thread-146 DISP 732 4

# 로그 분석

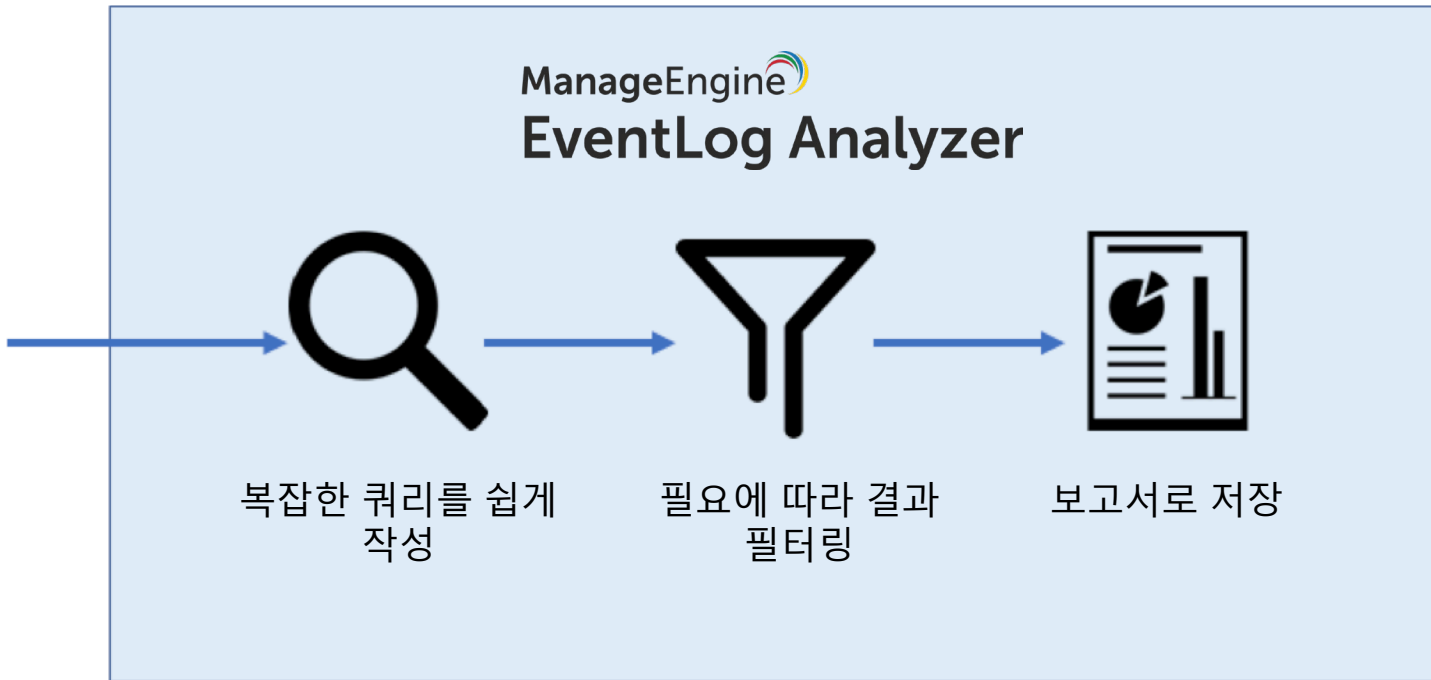
---

- 보안, 감사 및 규정 준수 요구 사항을 충족하는 1000개 이상의 즉시 사용 가능한 보고서 및 경고 프로필 제공
- 특정 요구 사항을 충족하는 사용자 지정 보고서 및 경고 프로필 제작 도구 제공.
- 빠르고 사용하기 쉬운 검색 엔진으로 심층 로그 포렌식을 수행하고 수백만 개의 로그를 검색.
  - **20,000 syslog / 초**
  - 2,000 Windows 이벤트 로그 / 초

# 로그 분석: 로그 포렌식



관리자



# 로그 분석: 로그 포렌식

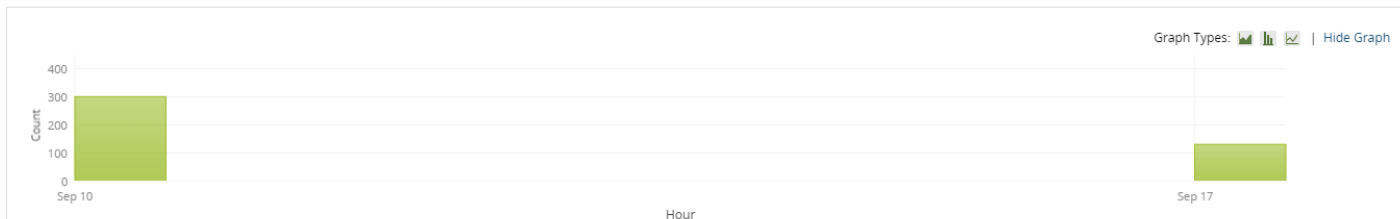
192.168.218.136 Pick Device All Log Types

Basic | Advanced

USERNAME = "administrator"

Go Save Search Save as Alert

Clear Search



How to extract fields? Showing: 1 - 10 of 431 View per page: 10 Add/Remove Fields

Message : Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Product Version: 5.2.2. Product Language: 1033. Manufacturer: Oracle Corporation. Installation success or error status: 0. 126244

Profile Value : - Target User : - Accesses : - GUID : - Source Port : 514 Process Name : - Group Domain : - Chantype Details : - Rule Name : - Target Ip : - Source : Ms  
iInstaller Previous Value : - Session Type : - Member Group SID : - Share Path : - SID Filtering : - Severity : information Service Type : - Packet Discarded : - Domain : -  
Fault Module : - Object Name : - Top And Least Values for field - SEVERITY X  
Service Name : Oracle VM Virtual  
:- Security Id : - Passwd  
Type : - Machine Name : -  
- Version : 5.2.2 Max Pa  
- Update Name : - Lock  
- New Filename : - Encr  
17:59:30 Username : admin

| Value       | Count | Percentage |
|-------------|-------|------------|
| failure     | 215   | 49.88%     |
| success     | 129   | 29.93%     |
| information | 87    | 20.19%     |

| Value       | Count | Percentage |
|-------------|-------|------------|
| information | 87    | 20.19%     |
| success     | 129   | 29.93%     |
| failure     | 215   | 49.88%     |

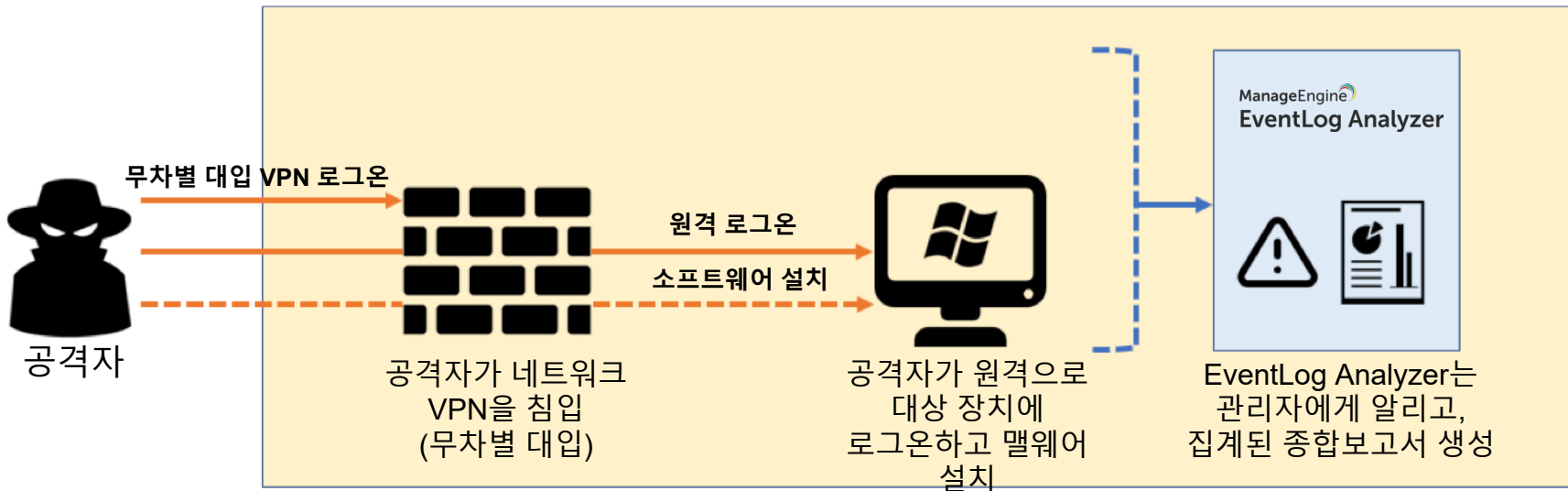
Malware Name  
pires : - File  
Object type :  
Privilege :  
Intelligence :  
Sep 2017,

# 로그 상관 관계 분석

---

- 30개 이상의 사전 정의된 상관 관계 규칙을 통해 장치 전반의 공격 패턴을 탐지.
- 의심스러운 소프트웨어 설치, 웹 활동과 같은 공격 등의 이상 징후를 탐지.
- 타임라인 형식으로 로그 추적을 표시하는 집계 보고서 제공.
- 비즈니스 환경에 특정한 공격 패턴을 생성하고 탐지하는 맞춤형 상관 관계 규칙 제작 도구 지원

# 로그 상관 관계 분석: 예





# 로그 상관 관계 분석: 상관 이벤트

The screenshot displays the EventLog Analyzer interface. A central window titled "Event history" is open, showing a list of events. The events are as follows:

| Time     | Date        | Event Description  | Details                 |
|----------|-------------|--|-------------------------|
| 13:50:52 | 05 Jan 2018 | A software is installed on Windows.<br>Windows Installer installed the product. Product Name: Oracle VM VirtualBox 5.2.2. Pr...                        | <a href="#">Details</a> |
| 13:44:58 | 05 Jan 2018 | A windows account successfully logs on using remote logon.<br>An account was successfully logged on. Subject: Security ID: 5-1-0-0 Account Name: - ... | <a href="#">Details</a> |
| 13:42:40 | 05 Jan 2018 | A user successfully logged on to the network using Fortinet VPN.<br>date=2018-01-05 time=13:42:40 devname=FortiGate-VM devid=FGVMEV0000000000 L...     | <a href="#">Details</a> |
| 13:42:13 | 05 Jan 2018 | A user failed to log on to the network using Fortinet VPN.<br>date=2018-01-05 time=13:42:13 devname=FortiGate-VM devid=FGVMEV0000000000 L...           | <a href="#">Details</a> |
| 13:42:09 | 05 Jan 2018 | A user failed to log on to the network using Fortinet VPN  | <a href="#">Details</a> |
| 13:42:09 | 05 Jan 2018 | A user failed to log on to the network using Fortinet VPN.<br>date=2018-01-05 time=13:42:09 devname=FortiGate-VM devid=FGVMEV0000000000 L...           | <a href="#">Details</a> |

At the bottom of the event history window, there is a "Close" button. Below the window, a table shows the event details in a grid format:

| Time                 | Date | IP          | User  | Device                     |
|----------------------|------|-------------|-------|----------------------------|
| 05 Jan 2018 13:46:16 |      | 192.168.2.2 | james | 172.21.202.130             |
|                      |      |             |       | Oracle VM VirtualBox 5.2.2 |

The background interface shows a sidebar with various threat categories like "System/server threats", "Web server threats", etc., and a main area with a search bar and a "History" section.

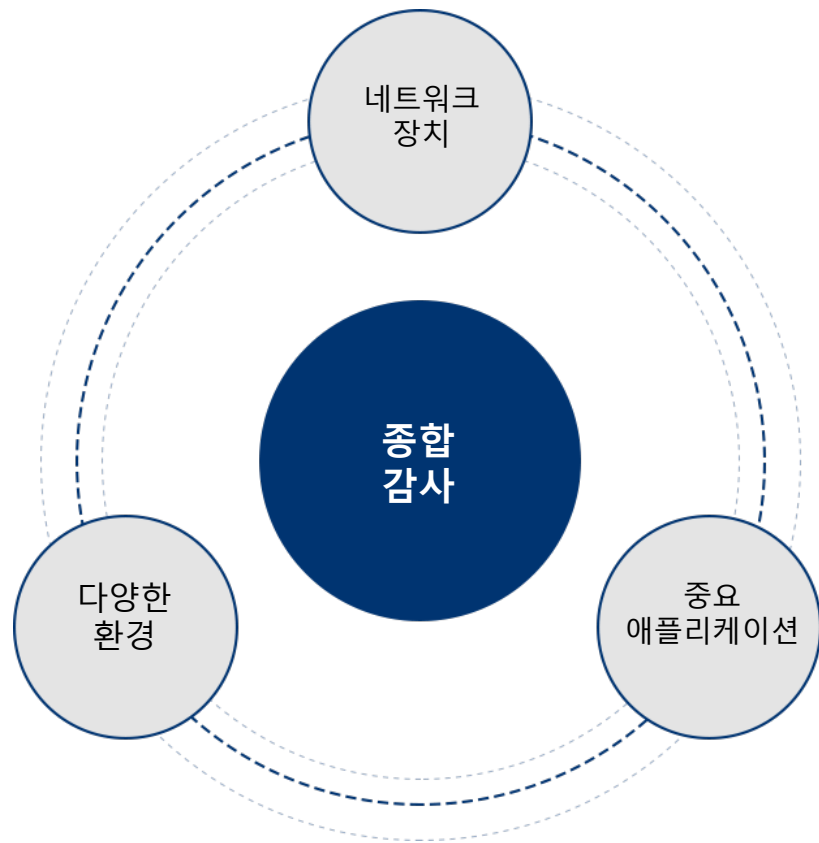
# 로그 장기 보관

---

- 로그 파일은 향후 포렌식 분석, 규정 준수 및 내부 감사를 위해 로그 데이터가 보호되도록 암호화 지원
- 기본적으로 수신된 모든 원시 로그가 포함된 로그 아카이브 파일은 24시간마다 생성됨. 그런 다음 이러한 파일은 하드 디스크 공간을 절약하기 위해 7일마다 압축됨.
- 언제든지, 원하는 파일을 EventLog Analyzer 데이터베이스에 로드할 수 있으며, 보관된 이벤트 데이터에 대한 보고서를 생성 가능

# 종합 감사

---

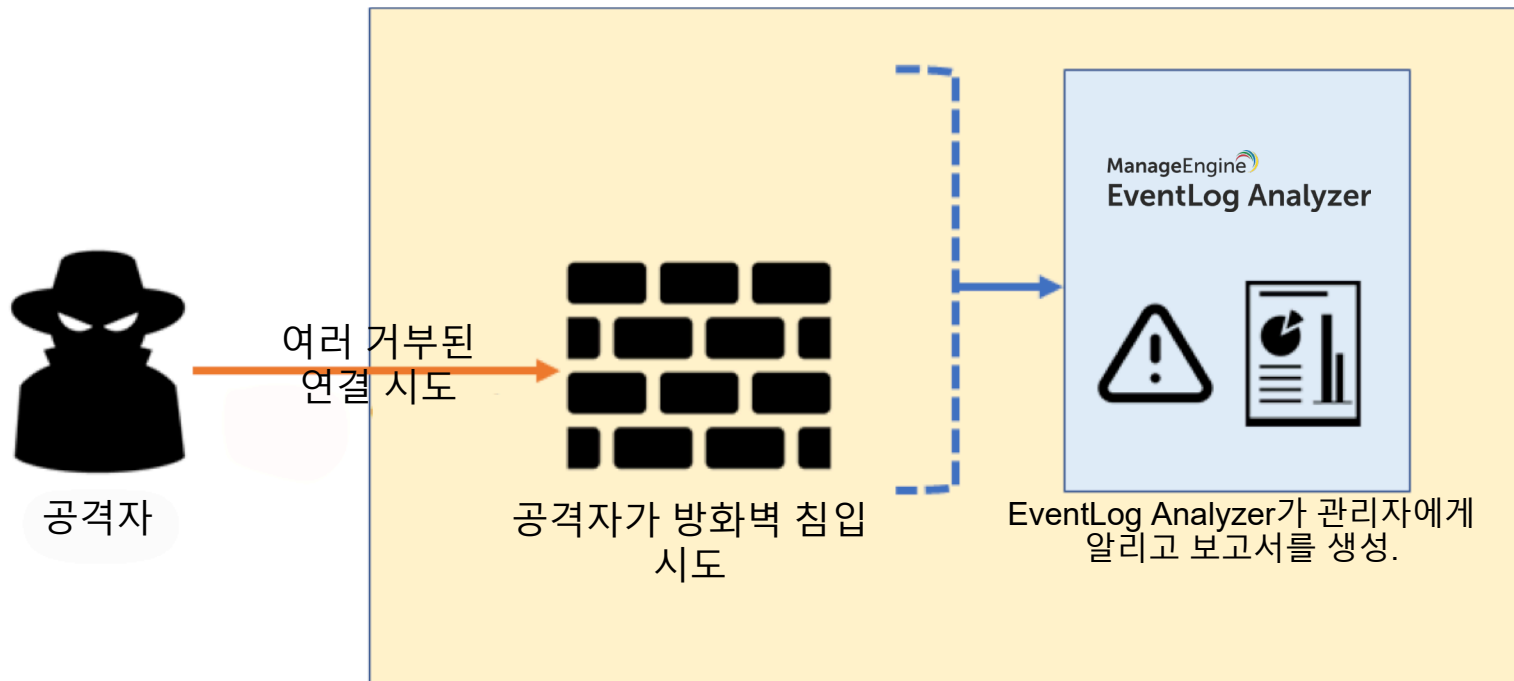


# 네트워크 장치 감사

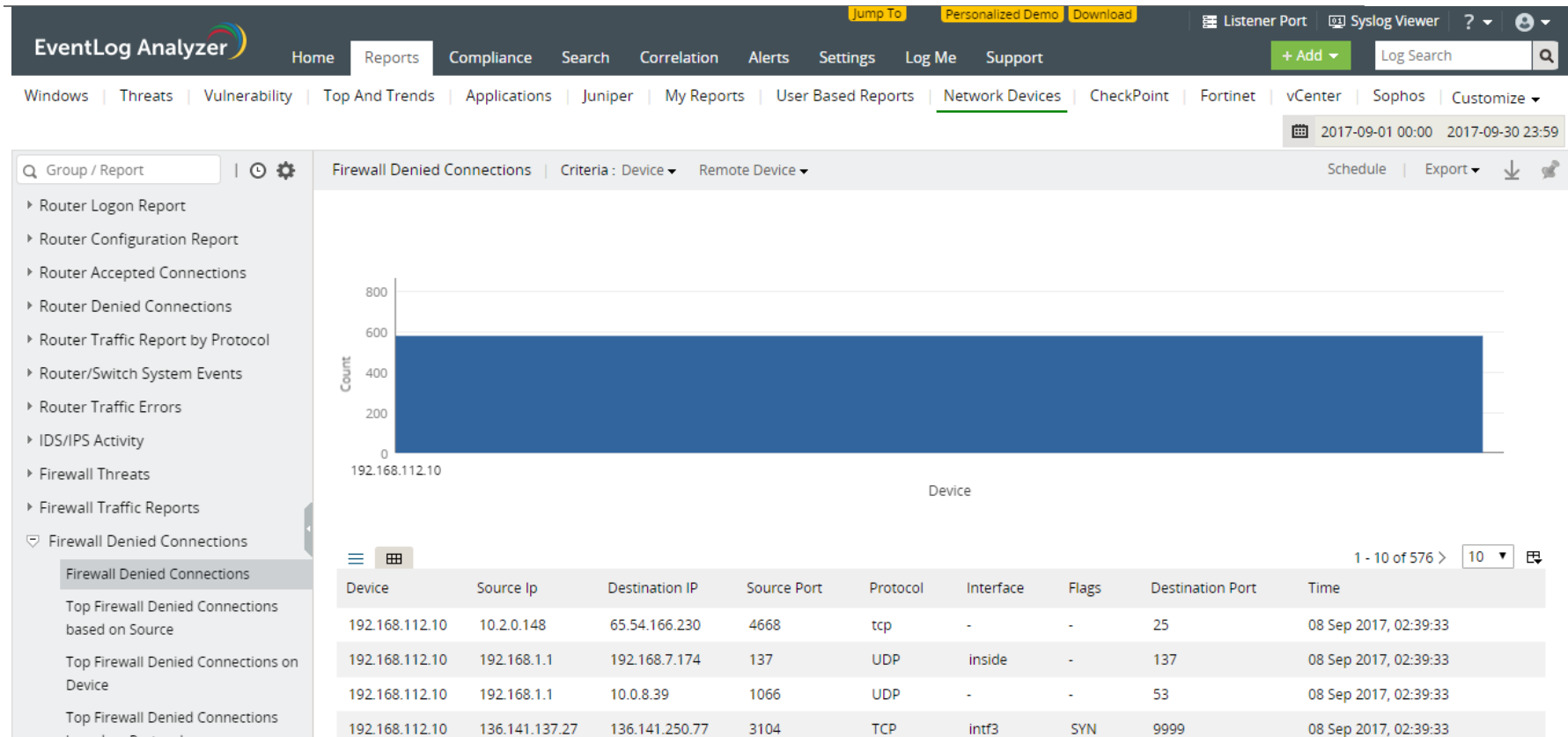
---

- 방화벽 구성 및 규칙 변경을 모니터링.
- 경계 장치에 대한 무단 액세스 시도 및 권한 상승을 식별.
- 라우터, 스위치, 방화벽 및 IDS/IPS 장치에서 거부된 연결, 위협 및 기타 비정상적인 사건을 감지.

# 네트워크 장치 감사: 방화벽 침해 시도



# 네트워크 장치 감사: 방화벽 침해 시도

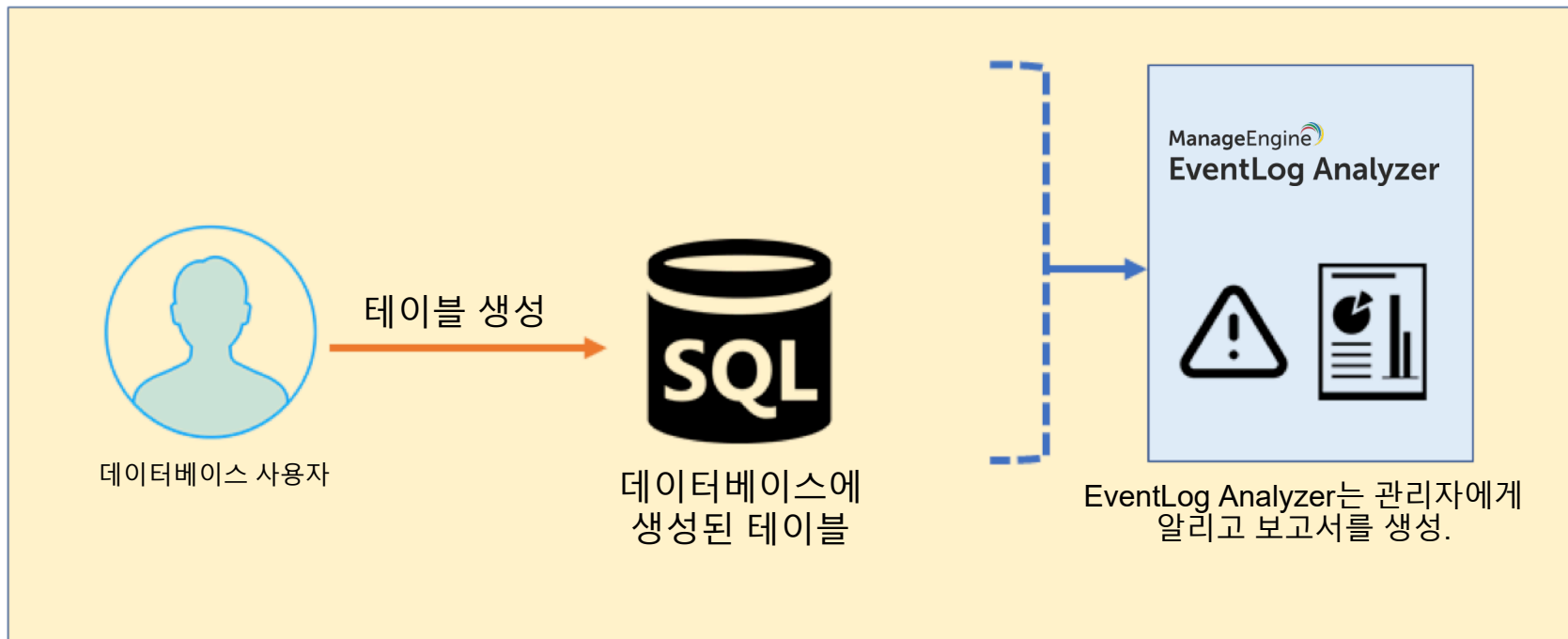


# 애플리케이션 감사

---

- 애플리케이션 로그 데이터 가져오기 자동화: 가져온 로그에서 보안 보고서를 추출하고, 사용자 지정 로그 파서를 사용하여 사내의 애플리케이션 로그를 분석.
- IIS 및 Apache 웹 서버 보안: 오류 이벤트, 로그인 시도 실패, 서버 공격과 같은 비정상적인 활동을 실시간으로 식별.
- Microsoft SQL Server 및 Oracle 데이터베이스 감사: 사용자 작업, DML 및 DDL 쿼리, 데이터베이스 변경 사항, 서버 계정 변경 사항을 추적.
- 취약점 스캐너 및 위협 인텔리전스 솔루션 감사: 가장 취약한 포트, 호스트, 감염, 데이터 도난, 잠재적 보안 위험 등에 대한 자세한 자료 제공.

# 애플리케이션 감사: 특정 사용자가 생성한 테이블





# 애플리케이션 감사: 특정 사용자가 생성한 테이블

Windows | Threats | Vulnerability | Top And Trends | Applications | Juniper | My Reports | User Based Reports | Network Devices | CheckPoint | Fortinet | vCenter | Sophos | Customize ▾

📅 2017-09-01 00:00 2017-09-30 23:59

🔍 Group / Report



Created Tables | Criteria : Device ▾ | User ▾ | Remote Device ▾

Schedule | Export ▾



Dropped clusters

Altered Clusters

Created Tables

Dropped Tables

Altered Tables

Selected Tables

Inserted Tables

Updated Tables

Deleted Tables

Created functions

Dropped functions

Altered functions

Created Schemas

Created procedures

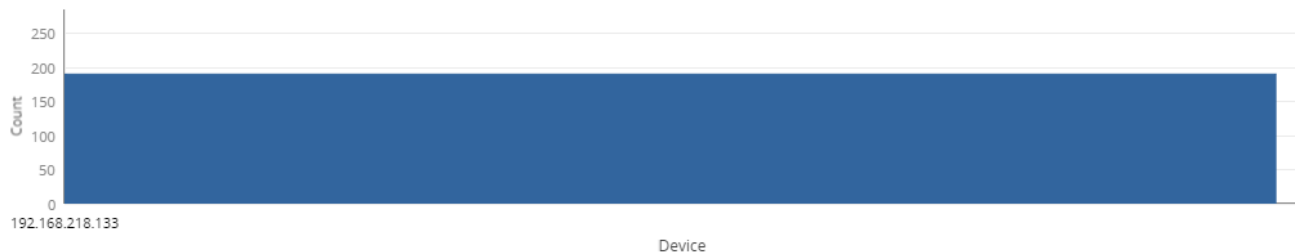
Dropped procedures

Altered procedures

Executed procedures

Created triggers

Dropped triggers

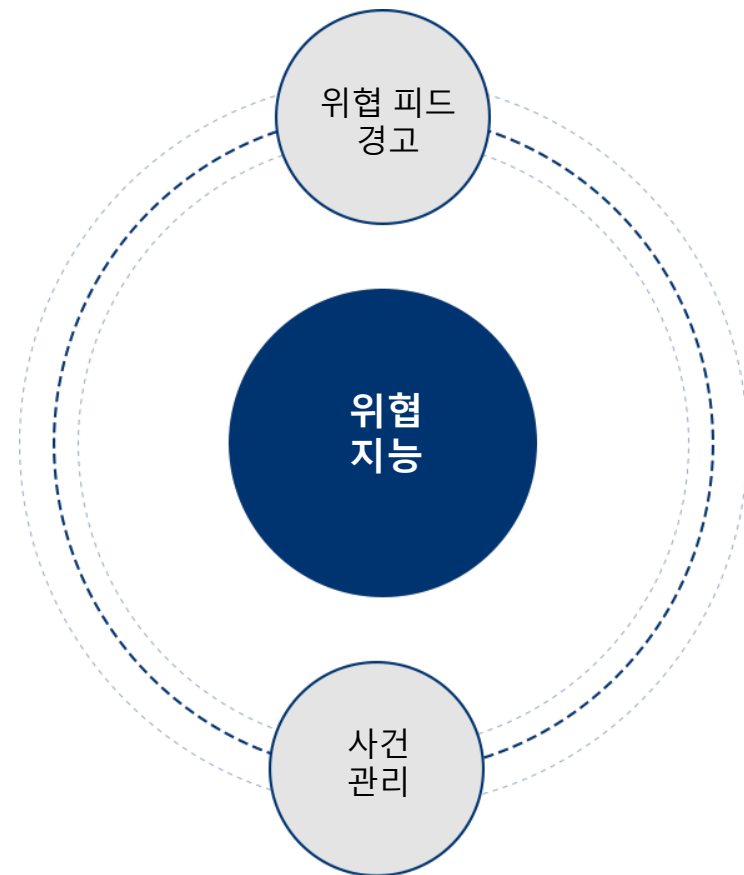


1 - 10 of 190 > 10 ▾

| Device             | Username | User Device  | Terminal | Object Creator | Object Name | Comment Text | Time                  |
|--------------------|----------|--------------|----------|----------------|-------------|--------------|-----------------------|
| Username = SCOTT X |          |              |          |                |             |              |                       |
| 192.168.218.133    | SCOTT    | ELA-RHEL6-64 | pts/2    | SCOTT          | VIVEK       | -            | 09 Sep 2017, 02:56:25 |
| 192.168.218.133    | SCOTT    | ELA-RHEL6-64 | pts/2    | SCOTT          | VIVEK       | -            | 09 Sep 2017, 02:56:25 |
| 192.168.218.133    | SCOTT    | ELA-RHEL6-64 | pts/2    | SCOTT          | DEPT_10     | -            | 09 Sep 2017, 02:56:25 |
| 192.168.218.133    | SCOTT    | vishnu-2268  | unknown  | SCOTT          | NEW_PRODUCT | -            | 09 Sep 2017, 02:56:25 |
| 192.168.218.133    | SCOTT    | vishnu-2268  | unknown  | SCOTT          | NEW_PRODUCT | -            | 09 Sep 2017, 02:56:25 |

# 위협 인텔리전스 (Threat intelligence)

---



# 위협 피드 경고

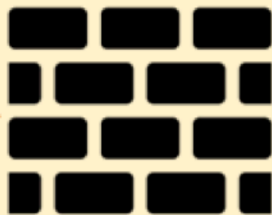
---

- EventLog Analyzer는 여러 오픈 소스 및 STIX/TAXII 기반 위협 피드를 처리.
- 동적으로 업데이트되는 6억 개 이상의 악성 IP, URL 및 도메인 데이터베이스.
- 의심스러운 IP, URL 및 도메인에서 트래픽이 감지되면 실시간 알림을 제공.
- 이 기능을 설정하는 데 사전 구성이 필요 없음.

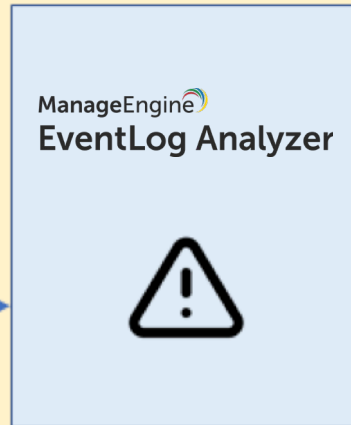
# 위협 피드 경고: 예



공격자



알려진 악성 IP가  
네트워크에 접속을 시도.



EventLog Analyzer는  
실시간으로 관리자에게 알림.

# 위협 피드 경고: 예

2016-10-16 00:00 2016-10-16 16:35

Alert Profiles [List] + Add Alert Profile Export to: Showing 1 - 50 of 1965 > > 50 ▾

| Time Generated        | Host      | Severity | Message                            |
|-----------------------|-----------|----------|------------------------------------|
| Oct 16, 2016 14:13:59 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:57 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:45 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:45 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:42 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:38 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:34 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:32 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:30 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:30 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |
| Oct 16, 2016 14:13:23 | 10.0.0.10 | High     | Malicious IP found - 222.186.56.42 |

# 사건 관리

---

- 내장된 사건 관리 콘솔을 사용하여 보안 사건을 관리.
- 운영자에게 사고 티켓을 자동으로 할당.
- 사건 티켓을 추적하고 여러 보기를 사용하여 티켓을 필터링하는 등의 작업을 수행.
- 또는 사건 티켓을 ServiceDesk Plus 등의 ITSM 또는 헬프데스크로 전달.

# 사건 관리 – 담당자 배정

The screenshot displays the 'Update Alert' dialog box in the EventLog Analyzer interface. The dialog contains the following fields:

- \*Assign To:** A dropdown menu with 'operator' selected.
- Notes:** A text input field containing 'admin'.
- \*Status:** A dropdown menu with 'Open' selected.

At the bottom of the dialog are 'Save' and 'Cancel' buttons. The background shows a table of alerts with the following columns: Time Generated, Device, Severity, Owner Name, Status, and Message.

| Time Generated       | Device                | Severity | Owner Name | Status | Message                                       |
|----------------------|-----------------------|----------|------------|--------|---|
| 22 Sep 2017 17:59:00 | Based on correlati... | High     | -          | Open   | Correlation:Logon Success by Source Host rule |
| 22 Sep 2017 17:59:00 | Based on correlati... | High     | -          | Open   | Correlation:Logon Success by Source Host rule |
| 22 Sep 2017 17:59:00 | Based on correlati... | High     | -          | Open   | Correlation:Logon Success by Source Host rule |
| 22 Sep 2017 17:59:00 | Based on correlati... | High     | -          | Open   | Correlation:Logon Success by Source Host rule |

# 자동화된 워크플로

---

- 사건 대응 관리를 자동화하여 공격을 억제하거나 영향을 최소화.
- 사전 정의된 워크플로를 경고 프로필과 연결하여 감지된 보안 사고를 자동으로 수정.
- 보안 경고가 트리거될 때 자동으로 실행되는 사건 워크플로를 만들고 관리.
- EventLog Analyzer의 기본 제공 워크플로를 사용하거나 유연한 워크플로 빌더를 사용하여 요구 사항에 따라 워크플로 규칙을 사용자 지정.



# 자동화된 워크플로

EventLog Analyzer Purchase now Jump To Log Receiver ? + Log Search

Home Reports Compliance Search Correlation Alerts Settings LogMe Support + Add

Search

All Alerts  
My Alerts  
Assigned Alerts  
Unassigned Alerts  
Critical Alerts  
Profile Based Alerts  
Correlation Alert Profiles  
Alert Configurations  
Manage Workflows

### Manage Workflow

Workflow Credentials + Create Workflow

| Actions | Workflow Name            | Description   | Associated Alert Profiles | Workflow History             |
|---------|--------------------------|---|---------------------------|------------------------------|
|         | Block USB                | This workflow blocks the USB port on a potentia...  | 0                         | <a href="#">View History</a> |
|         | Delete User              | This workflow deletes a potentially compromise...   | 0                         | <a href="#">View History</a> |
|         | Disable Computer         | This workflow disables a potentially compromis...   | 0                         | <a href="#">View History</a> |
|         | Kill Process             | This workflow kills a process on a potentially c... | 0                         | <a href="#">View History</a> |
|         | Log Off and Disable User | This workflow logs off and disables a potential...  | 0                         | <a href="#">View History</a> |
|         | Popup Alert              | This workflow displays a popup alert on the affe... | 0                         | <a href="#">View History</a> |
|         | Stop Service             | This workflow stops a service on a potentially c... | 0                         | <a href="#">View History</a> |

1-7 of 7 10

ManageEngine

# 통합 규정 준수 관리 시스템

---

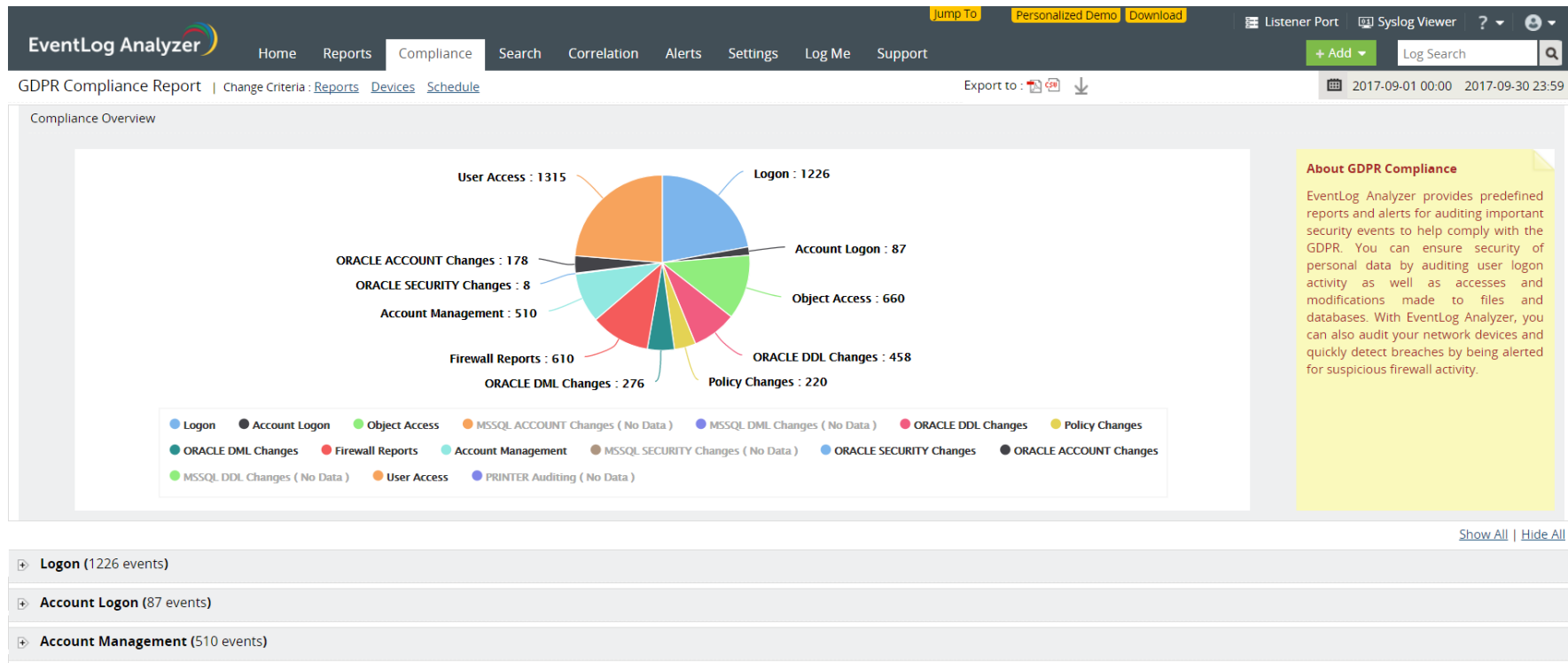


# 통합 규정 준수 관리 시스템

---

- 즉시 사용 가능한 규정 준수 보고서 (국제 산업계 표준):
  - PCI DSS
  - GDPR
  - FISMA
  - HIPAA
  - GLBA
  - SOX
  - ISO 27001
- 내부 보안 정책을 충족하기 위해 기존 보고서를 수정하거나 새 규정 준수 보고서 작성 가능.
- 강력한 검색 기능과 보안 로그 보관 기능으로 대부분의 규정 준수 정책에 대한 포렌식 분석 및 로그 보관 요구 사항을 충족

# 통합 규정 준수 관리 시스템



# EventLog Analyzer: 제품 차별화 요소

---

- 배포 및 사용이 간편합니다.
- 다양한 로그 소스를 지원합니다.
- 추가 기능이 필요 없습니다!
- SIEM 솔루션과 쉽게 통합할 수 있습니다.
- 간단한 라이선스 모델 - 대상 장비 수량 기준

# Edition 비교

| Features                               | Premium Edition | Distributed Edition |
|--|-----------------|---------------------|
| Log collection and archival            | ✓               | ✓                   |
| Universal Log Parsing and indexing     | ✓               | ✓                   |
| File Integrity Monitoring              | ✓               | ✓                   |
| Real-time event correlation and alerts | ✓               | ✓                   |
| Compliance reporting                   | ✓               | ✓                   |
| Log forensics                          | ✓               | ✓                   |
| Scalable architecture                  | ✗               | ✓                   |
| Multi-geographical location monitoring | ✗               | ✓                   |
| Server specific reports                | ✗               | ✓                   |
| Rebranding and client specific views   | ✗               | ✓                   |

# 전세계 10,000 이상의 고객이 사용 중

## 10,000+

organizations trust **EventLog Analyzer** with their Active Directory security.

**SIEMENS**

**Deloitte.**

AmericanBank

Apollo  
HOSPITALS

**accenture**  
High performance. Delivered.

UNIVERSITY OF  
OXFORD

HARVARD  
UNIVERSITY

**SANYO**

Mitsubishi  
Corporation

**Infosys**<sup>®</sup>

**Panasonic**

**IBM**<sup>®</sup>

**ERNST & YOUNG**  
Quality In Everything We Do

# 감사합니다

---

텔리맨트 주식회사

<https://www.tmn.co.kr>

02) 588-7350

기술 질문: [inforeq@tmn.co.kr](mailto:inforeq@tmn.co.kr)

견적 요청: [sales-info@tmn.co.kr](mailto:sales-info@tmn.co.kr)