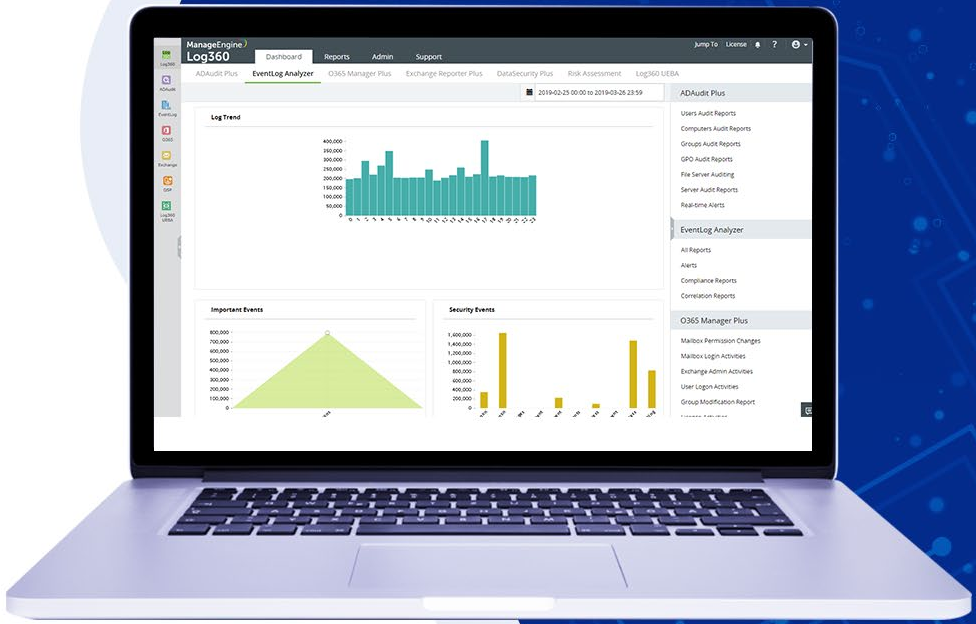
ManageEngine
Log360

통합 SIEM 솔루션



ManageEngine
Log360

Why **Log360** is a complete **SIEM solution**

Security analytics

Spots network intrusions and threats by analyzing events from network devices, servers, databases, web servers, Office 365 platforms, Exchange servers, and AD.

Intuitive dashboards and pre-built reports help you detect and respond to anomalies instantly.

Integrated compliance management

Stay compliant with PCI DSS, GDPR, FISMA, HIPAA, SOX, GLBA with audit-ready report templates. Exclusive dashboard to view the compliance state of your network.

Lets you tweak existing report templates to meet internal security policies and also allows you to build your own compliance reports easily with reusable components.

Threat intelligence

Detects attacks at their early stages with its built-in global IP threat database and STIX/TAXII threat feed processor that identifies malicious entities interacting with your network.

The real-time alerting system is tied together with the incident management system allowing you to quickly detect security incidents and resolve them.

Cloud monitoring

Detects anomalous events by monitoring activities happening in PaaS and IaaS environments such as Azure, Amazon Web Services, and SaaS applications like Salesforce.

Spots activities such as unauthorized download of customer information from Salesforce with predefined reports and alerts.

User behavior analytics (UBA)

Spots anomalies without manual intervention using sophisticated machine learning techniques.

Detect unusual volume of logons, file activity, lockouts, and more with the intuitive dashboard and exhaustive reports.

Incident management

Includes built-in incident tracking system which allows you to automatically assign owners to security alerts, track the incident resolution process, and more.

Integrates with JIRA, ServiceNow, ServiceDesk Plus, Zendesk and other help desk tools for streamlined incident tracking and resolution.

Data security

Automatically discovers personal and sensitive data in Windows infrastructure with predefined confidential data detection policies. Protect these data with the extensive file integrity monitoring capability.

Monitors file and folder creation, deletion, modification, and permission changes in Windows, NetApp, EMC file servers, and more.

보안 분석

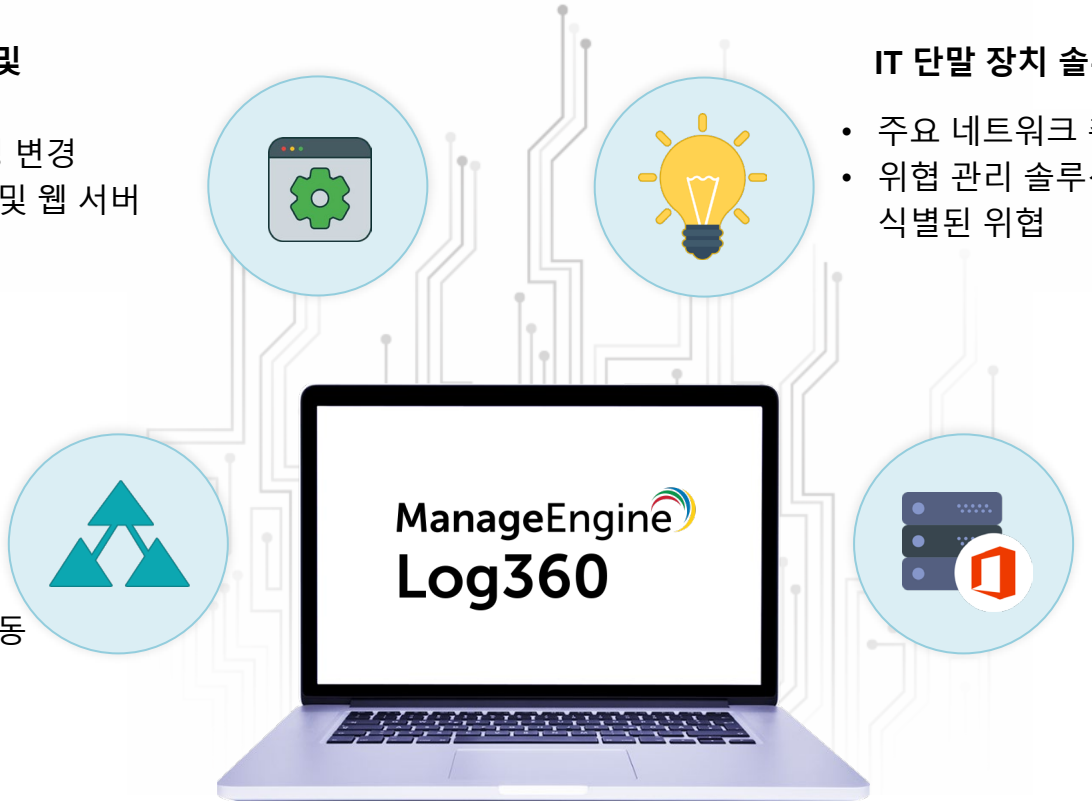
보안 정보 수집 용 통합 콘솔

네트워크 장치 및 애플리케이션

- 보안 장치 구성 변경
- 데이터베이스 및 웹 서버 활동

IT 단말 장치 솔루션

- 주요 네트워크 취약점
- 위협 관리 솔루션에 의해 식별된 위협



Active Directory

- 특수 권한 사용자 활동
- 주요 AD 변경 사항

Office 365 & Exchange Server

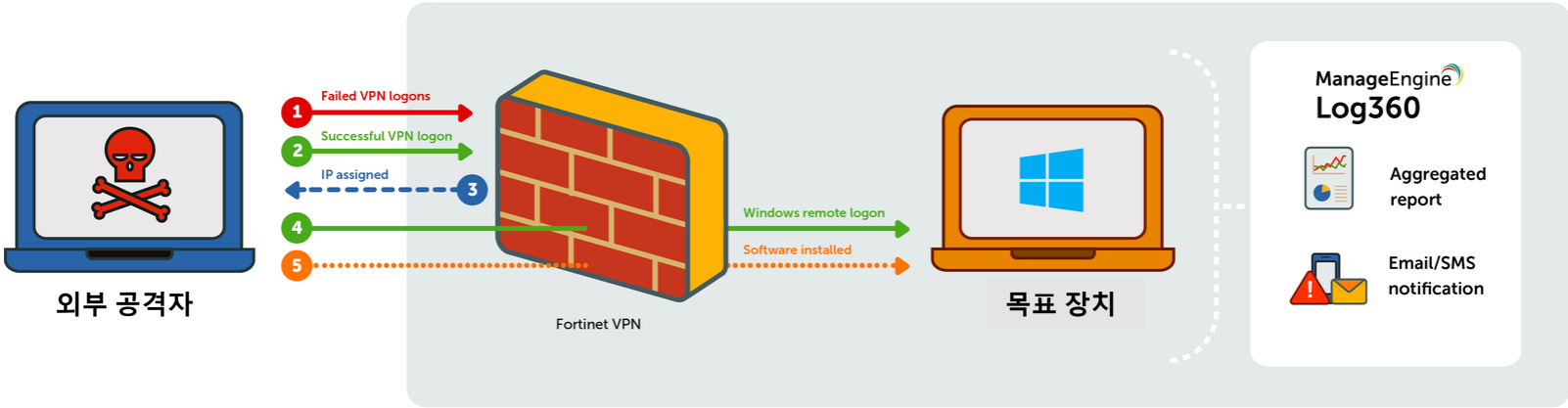
- Mailbox 트래픽 분석
- Exchange Server에 대한 콘텐츠, 권한, 트래픽 통계

고급 이벤트 상관 관계 분석

- 패턴 기반 사건/사고 탐지
- 30개 이상의 사전 정의된 규칙: 의심스러운 소프트웨어, 크립토재킹, 웜 활동 등을 탐지.
- 사건/사고 개요 대시보드
- 자세한 사건/사고 타임라인
- 고급 필드 기반 필터 기반의 사용자 정의 상관 관계 규칙 작성 도구

의심스러운 소프트웨어 설치의 탐지

의심스러운 소프트웨어 설치



1. 10 분 내에 최소 5회 VPN 로그온 실패
2. 다음 2분 내에 VPN 로그온 성공
3. 다음 2 분 내에 IP 주소가 부여됨
4. 다음 15분 내에 목표 장치에 원격 로그온 성공
5. 다음 30 분 내에 의심스러운 소프트웨어 설치

Log 포렌식 분석

- 강력한 Elasticsearch 기반 검색 엔진으로 복잡한 사고를 분석하고 몇 분 안에 근본 원인 발견 가능.
- 기본 및 고급 검색: 유연한 옵션을 사용하여 처음부터 검색 쿼리를 작성하거나 고급 쿼리 빌더 인터페이스 사용.
- 로그 아카이브를 포함하여 원시 로그 검색 및 형식이 지정된 로그 검색
- 보고서 또는 경고로 검색 저장

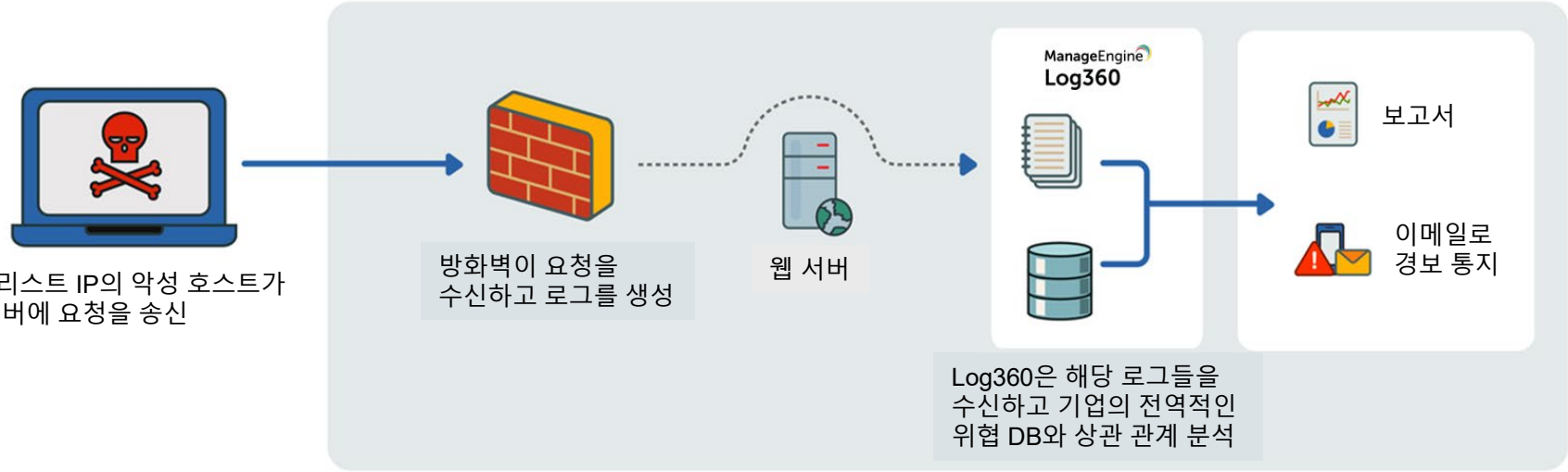
위협 인텔리전스

위협 인텔리전스

- 위협 피드 데이터로 네트워크 침입자 탐지
- 악성 URL, IP 및 도메인 이름에 대한 실시간 경고
- 맞춤형 STIX/TAXII 위협 피드 추가구성이 필요하지 않음
- 동적 및 일일 업데이트

의심스러운 소프트웨어 설치의 탐지

인바운드 악성 IP

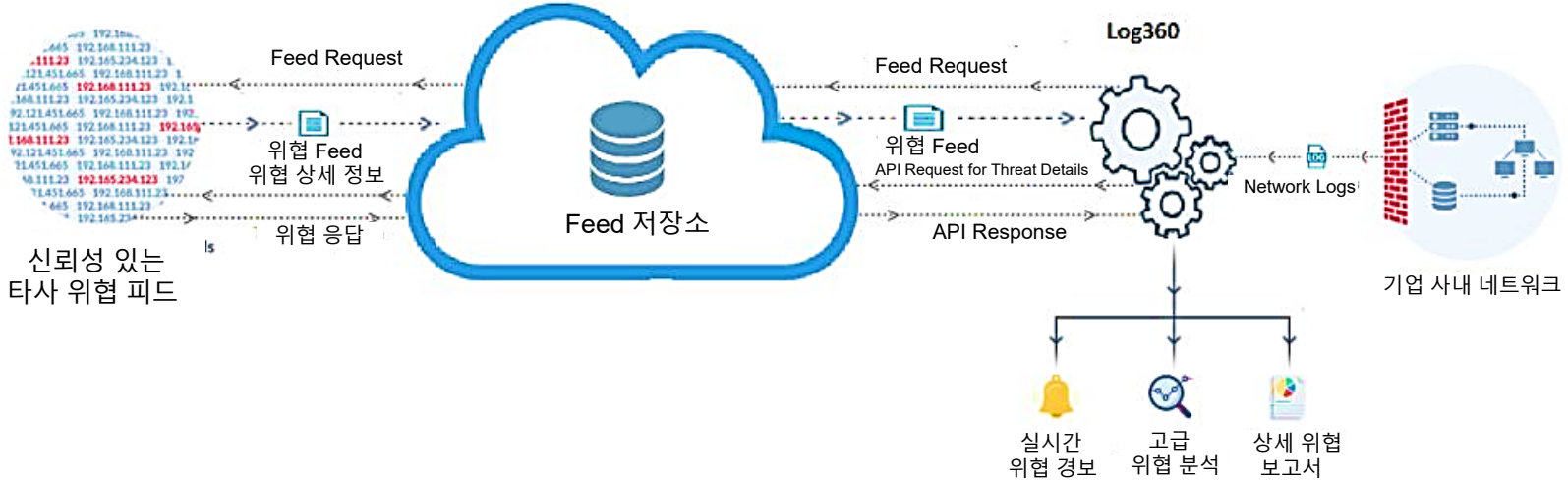


고급 위협 분석

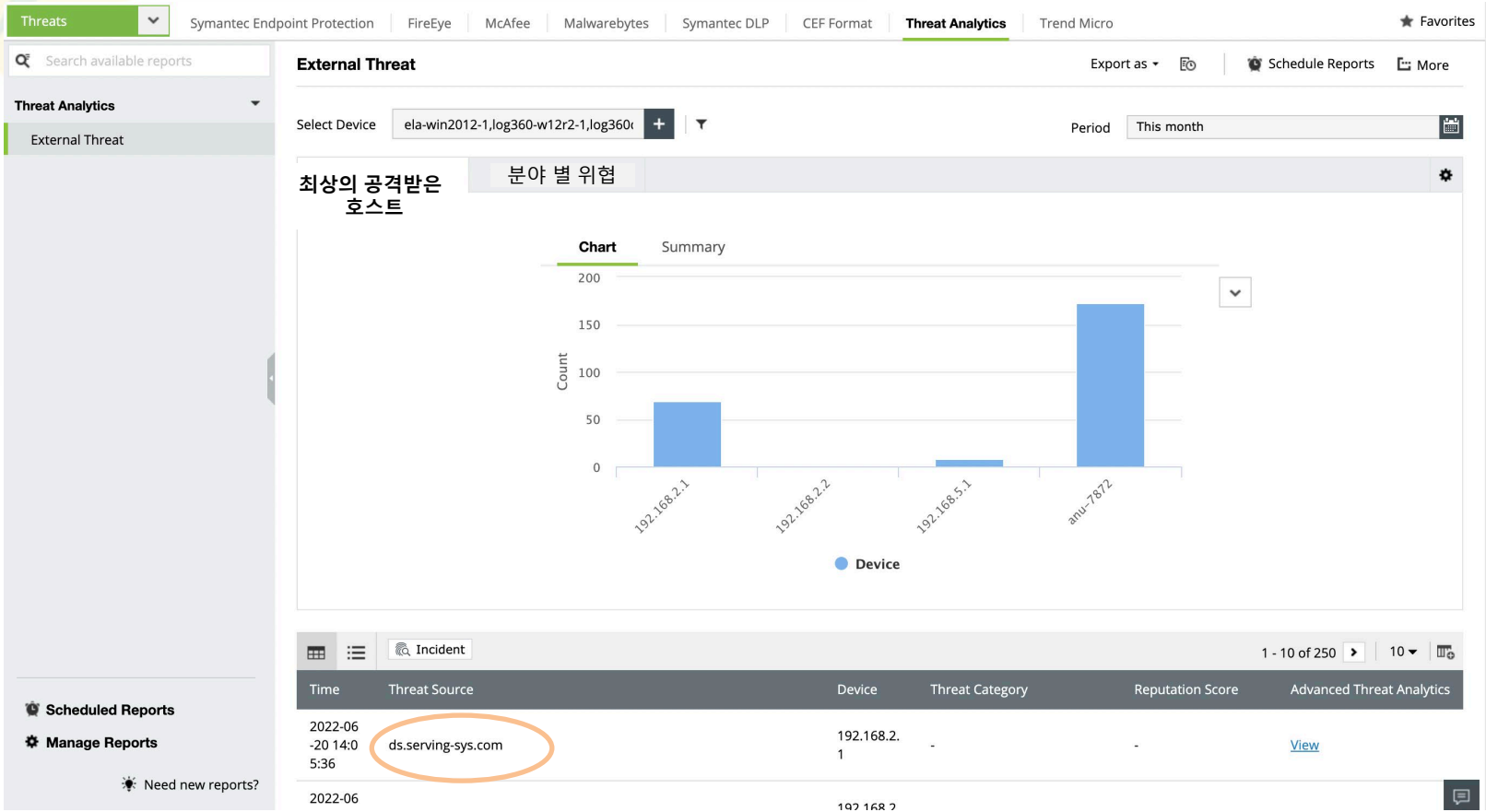
고급 위협 분석

- 신뢰할 수 있는 위협 인텔리전스 제공업체와의 통합
- 위협에 대한 심층적 자료 분석
- IP/URL 분류
- 평판 점수

통합된 위협 피드



ManageEngine
Log360



ManageEngine
Log360

고급 위협 분석

Info | Whois Info

ds.serving-sys.com
Low Risk

0 — 100
Reputation Score =**79**

Domain name	:	serving-sys.com
Domain age	:	19 Years, 2 Months
Flagged as malicious on	:	-
Last occurrence on threat list	:	-
No. of times it occurred on threat list	:	-
Category	:	Web Advertisements

Whitelist this source

Recommendation : Low Risk

Ok

사용자 및 엔터티 행동 분석

사용자 및 엔터티 행동 분석

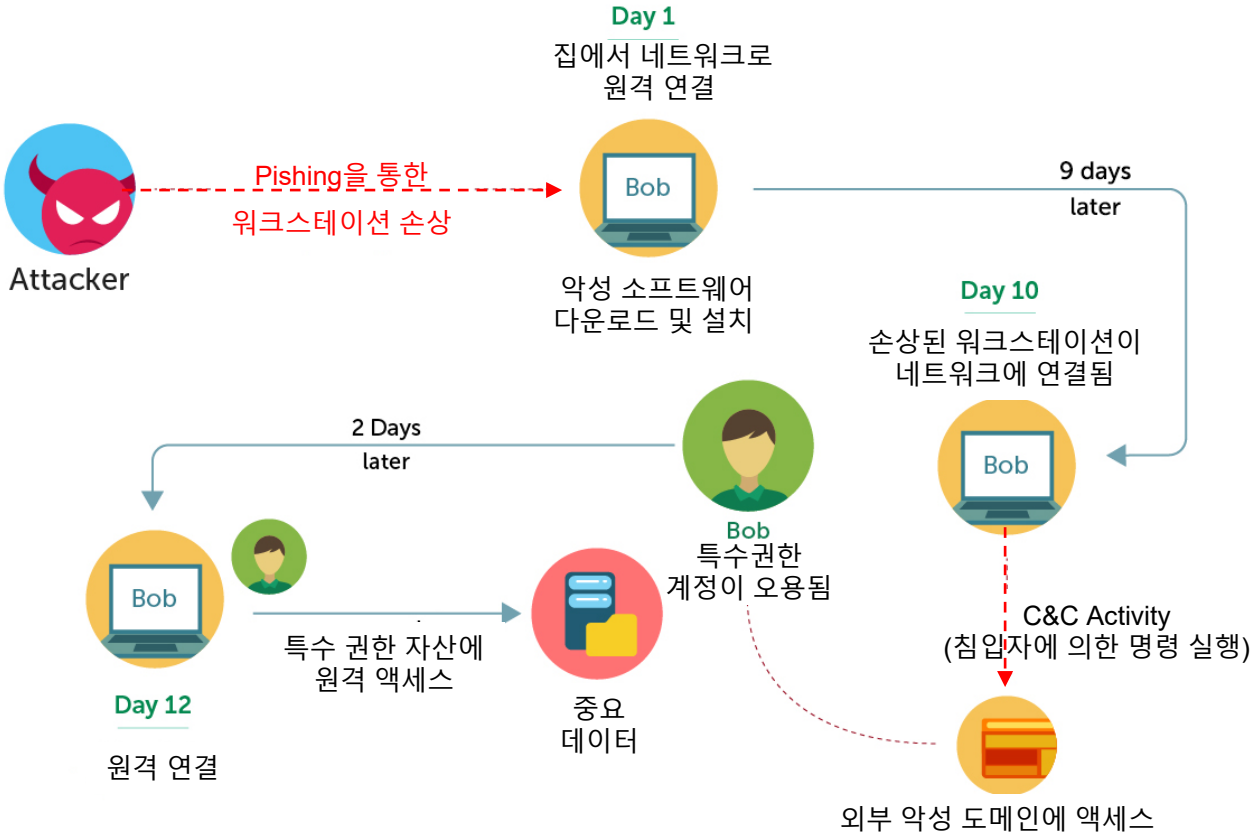
- 머신 러닝 기반 이상 탐지
- **이상 행동 탐지:** 시간, 패턴 및 횟수를 기준
- **위험 점수 기준으로 위협 우선 순위 지정:** 식별된 위협으로 인해 발생하는 위험 정도 파악
- 관심 목록에 고위험 사용자 및 엔터티 추가
- **위협 확증:** 일반적인 위협(계정 침해, 데이터 유출 등)의 지표 식별

위협 사례:

손상된 워크스테이션

및

데이터 유출 시도



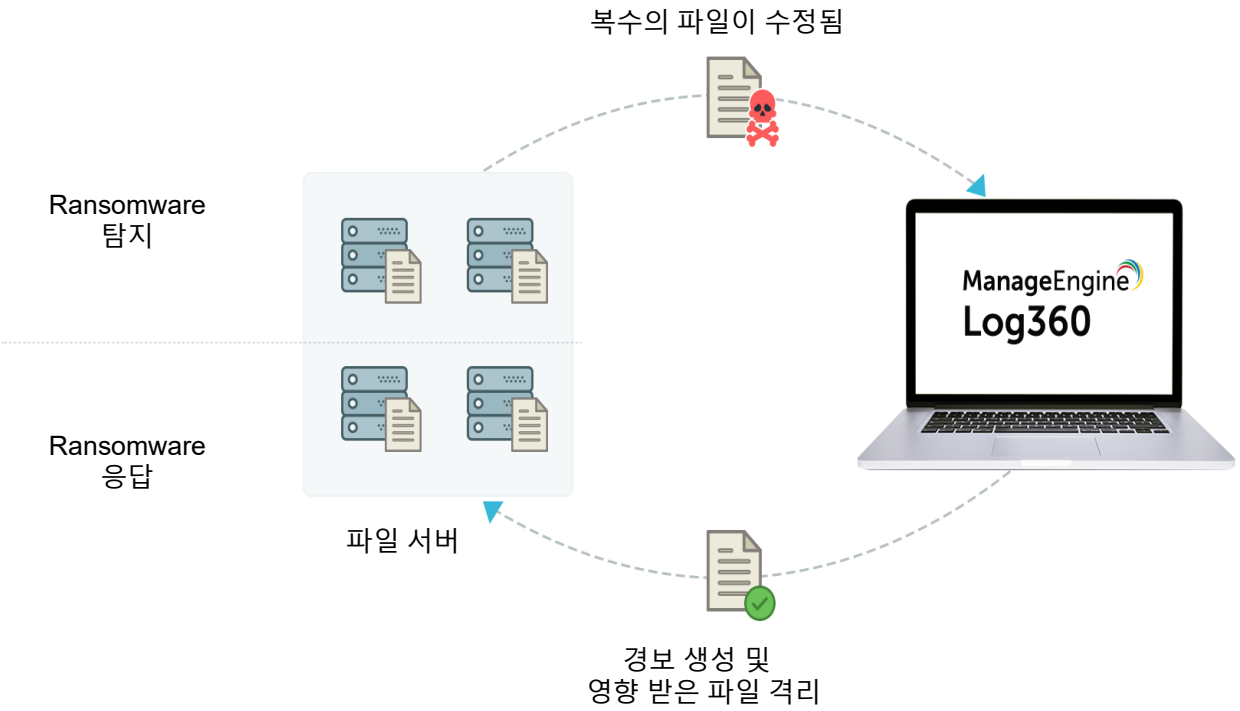
ManageEngine
Log360


데이터 보안

데이터 보안

- 사전 정의된 사용자 정의 정책을 사용하여 네트워크 전반에서 민감한 데이터(PII, PHI 등) 검색
- 파일 무결성 모니터링으로 기밀 파일 및 폴더의 무결성 보장
- 무단 파일 액세스, 권한 변경 및 수정에 대한 실시간 알림 받기

의심스러운 소프트웨어 설치 탐지



사건 관리

사건 관리

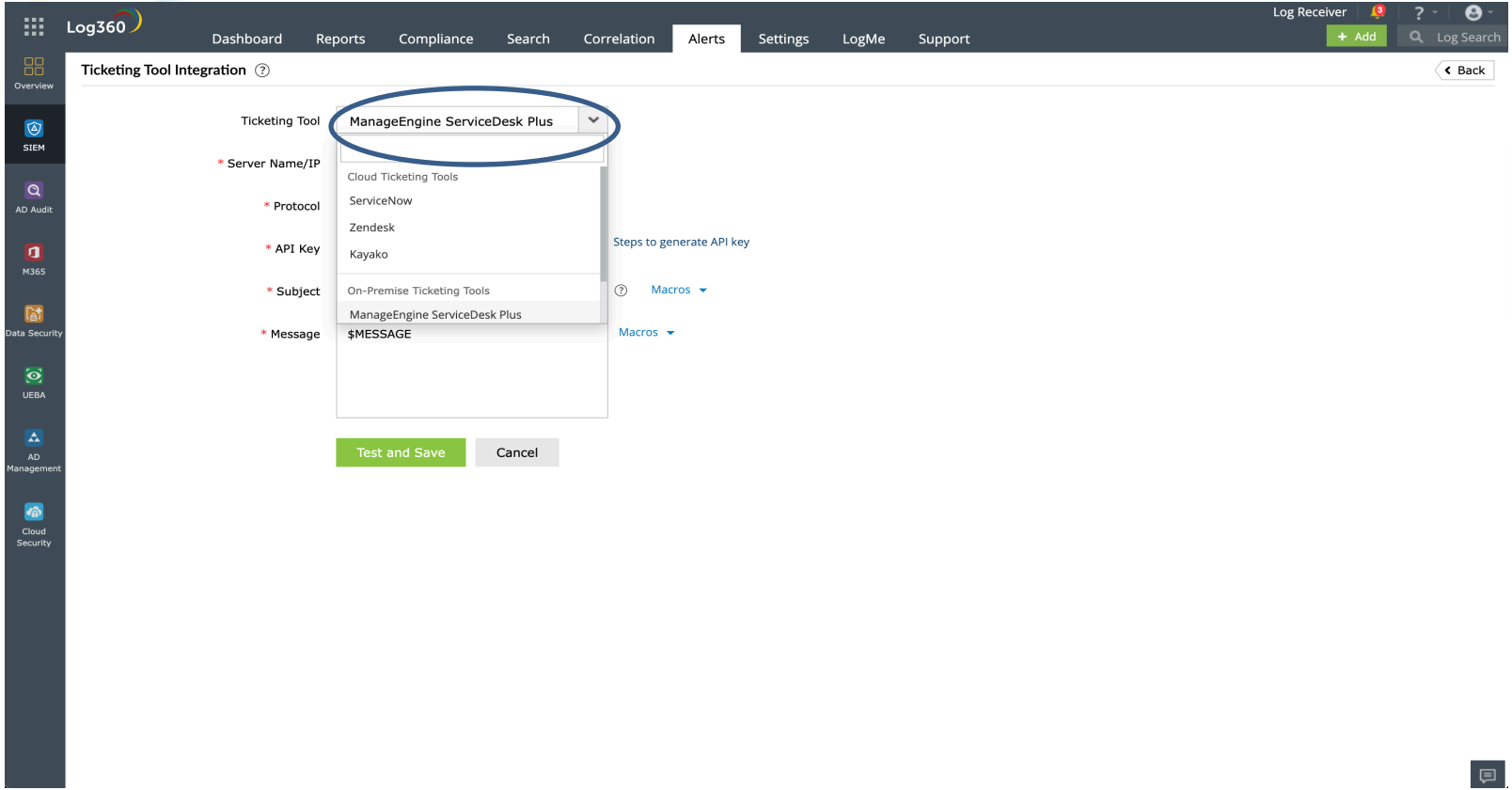
내장된 티켓팅(장애 처리 요청) 시스템:

- 자동 사건 처리 요청서 배정
- 사건 상태 추적
- 해결된 사건들에 대해 회사 내부의 침해/해결 DB 유지 관리

외부 헬프데스크에 사건 요청서 전달 기능:

- 지원되는 헬프데스크 소프트웨어: ServiceDesk Plus, ServiceNow, Jira Service Desk, ZenDesk, BMC Remedy, Kayako

헬프데스크와 통합 설정 화면



클라우드 모니터링

Cloud 환경

클라우드에서 정보 수집:

AWS:

Amazon S3, Amazon EC2,

Web Application Firewalls (WAF)

Relational Database Service (RDS),

and more

Microsoft Azure:

User activity, changes made

to network security groups,

virtual networks, DNS zones,

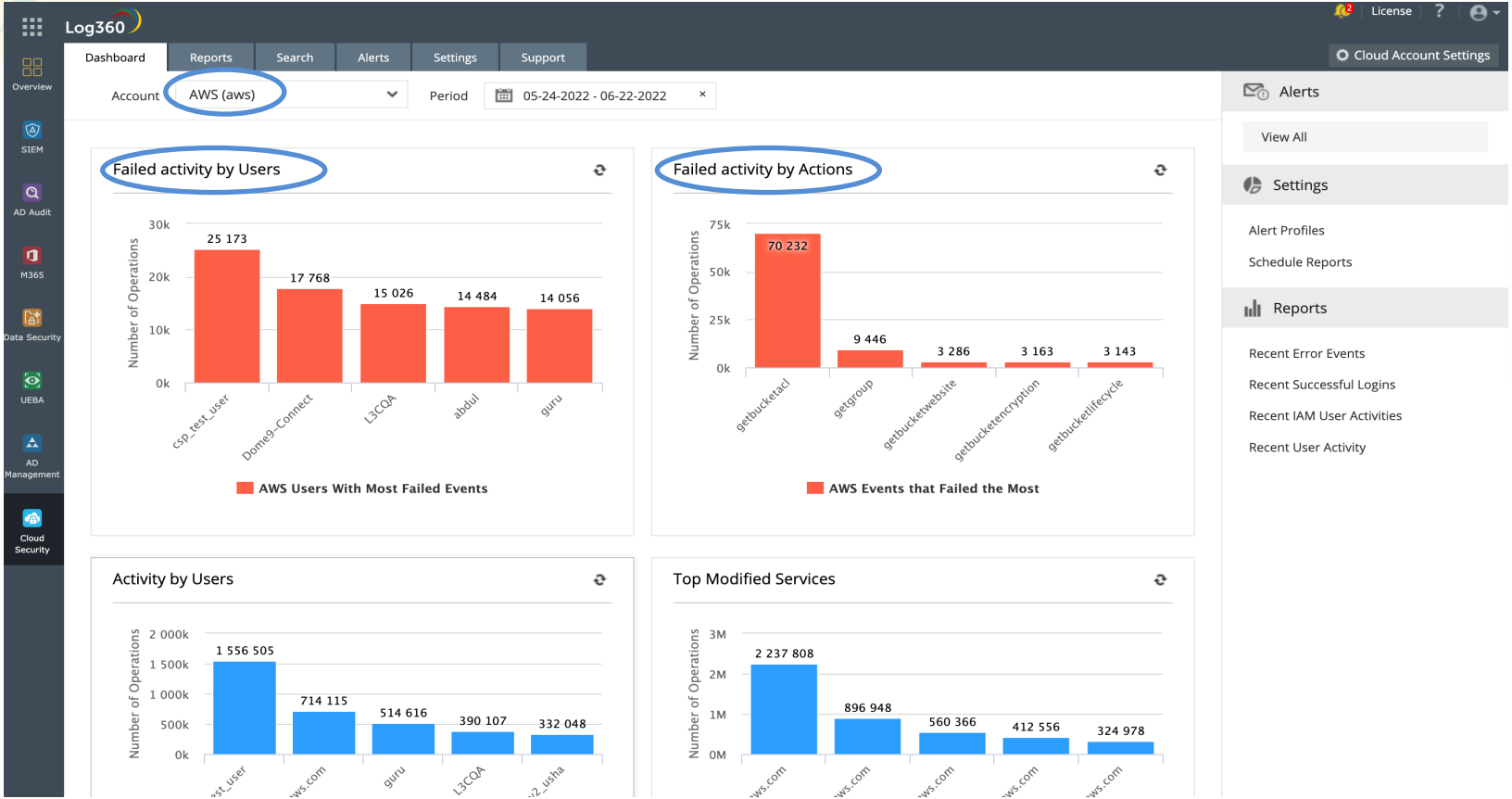
databases, and more

Salesforce:

Login, report, content,

and search activities

AWS 에서 정보 수집

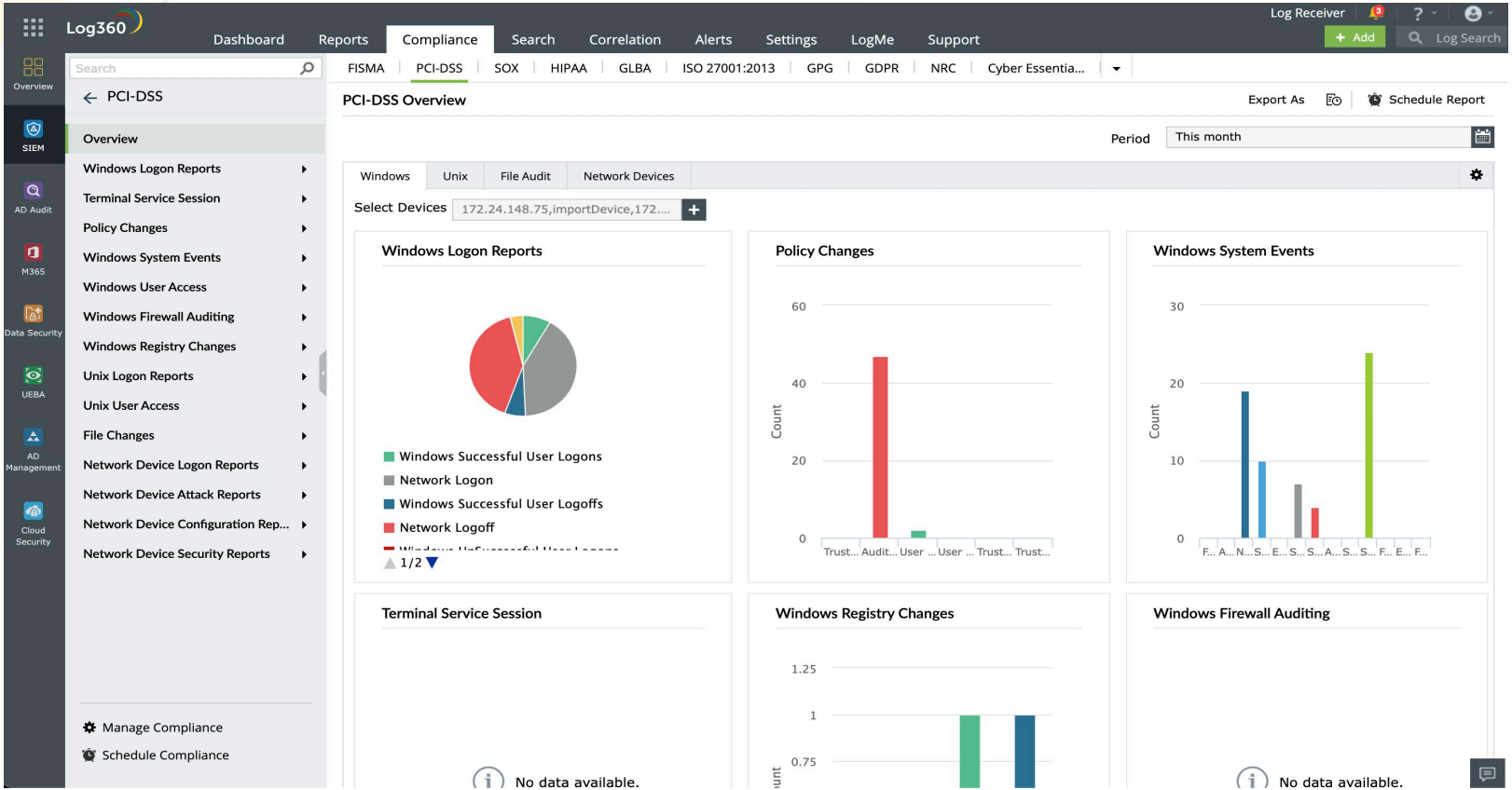

Log360
License
Dashboard
Reports
Search
Alerts
Settings
Support
Cloud Account Settings
Overview
SIEM
AD Audit
M365
Data Security
UEBA
AD Management
Cloud Security
Account
AWS (aws)
Period
05-24-2022 - 06-22-2022
Failed activity by Users
Number of Operations
30k
20k
10k
0k
25 173
17 768
15 026
14 484
14 056
csp_test_user
Dome9-Connect
L3CQA
abdul
guru
AWS Users With Most Failed Events
Failed activity by Actions
75k
50k
25k
0k
70 232
9 446
3 286
3 163
3 143
getbucketacl
getgroup
getbucketwebsite
getbucketencryption
getbucketlifecycle
AWS Events that Failed the Most
Activity by Users
2 000k
1 500k
1 000k
500k
0k
1 556 505
714 115
514 616
390 107
332 048
guru
L3CQA
Top Modified Services
3M
2M
1M
0M
2 237 808
896 948
560 366
412 556
324 978
Alerts
View All
Settings
Alert Profiles
Schedule Reports
Reports
Recent Error Events
Recent Successful Logins
Recent IAM User Activities
Recent User Activity

보안 규정 준수

규정 준수

- **내장된 규정 준수 보고서:** PCI DSS | SOX | GLBA | HIPAA | GPG | GDPR | ISO 27001 | ISLP
- 회사 내부 규정에 따른 사용자 정의 규정 준수 보고서 생성
- 규정 준수 경보 – 사전 정의 가능
- **자동 로그 보관:** 규정 준수 보관 기간에 따라 로그 장기 보관
- 변조 불가능한 안전한 보관

규정 준수보고서


Log360
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
Log Receiver
Add
Log Search
Overview
SIEM
AD Audit
M365
Data Security
UEBA
AD Management
Cloud Security
Search
PCI-DSS
Overview
Windows Logon Reports
Terminal Service Session
Policy Changes
Windows System Events
Windows User Access
Windows Firewall Auditing
Windows Registry Changes
Unix Logon Reports
Unix User Access
File Changes
Network Device Logon Reports
Network Device Attack Reports
Network Device Configuration Rep...
Network Device Security Reports
Manage Compliance
Schedule Compliance
FISMA
PCI-DSS
SOX
HIPAA
GLBA
ISO 27001:2013
GPG
GDPR
NRC
Cyber Essentia...
PCI-DSS Overview
Export As
Schedule Report
Period
This month
Windows
Unix
File Audit
Network Devices
Select Devices
172.24.148.75,importDevice,172....
Windows Logon Reports
Windows Successful User Logons
Network Logon
Windows Successful User Logoffs
Network Logoff
1/2
Policy Changes
60
40
20
0
Count
Trust...
Audit...
User ...
User ...
Trust...
Trust...
Windows System Events
30
20
10
0
Count
Terminal Service Session
No data available.
Windows Registry Changes
1.25
1
0.75
Windows Firewall Auditing
No data available.

추가 기능:

Product security

- ✓ **안전한 데이터 전송:** 보안 HTTPS 프로토콜을 통해 Log360과 브라우저 간의 모든 통신을 암호화.
- ✓ **역할 기준의 액세스 제어:** 사용자 역할을 사용하여 추가된 장치 및 제품 기능에 대한 사용자 액세스 제한
- ✓ **사용자 감사:** 모든 EventLog Analyzer 사용자 액션을 감사
- ✓ **고 가용성:** 주 서버 장애 시 인계할 보조 서버 지정

감사합니다

텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr