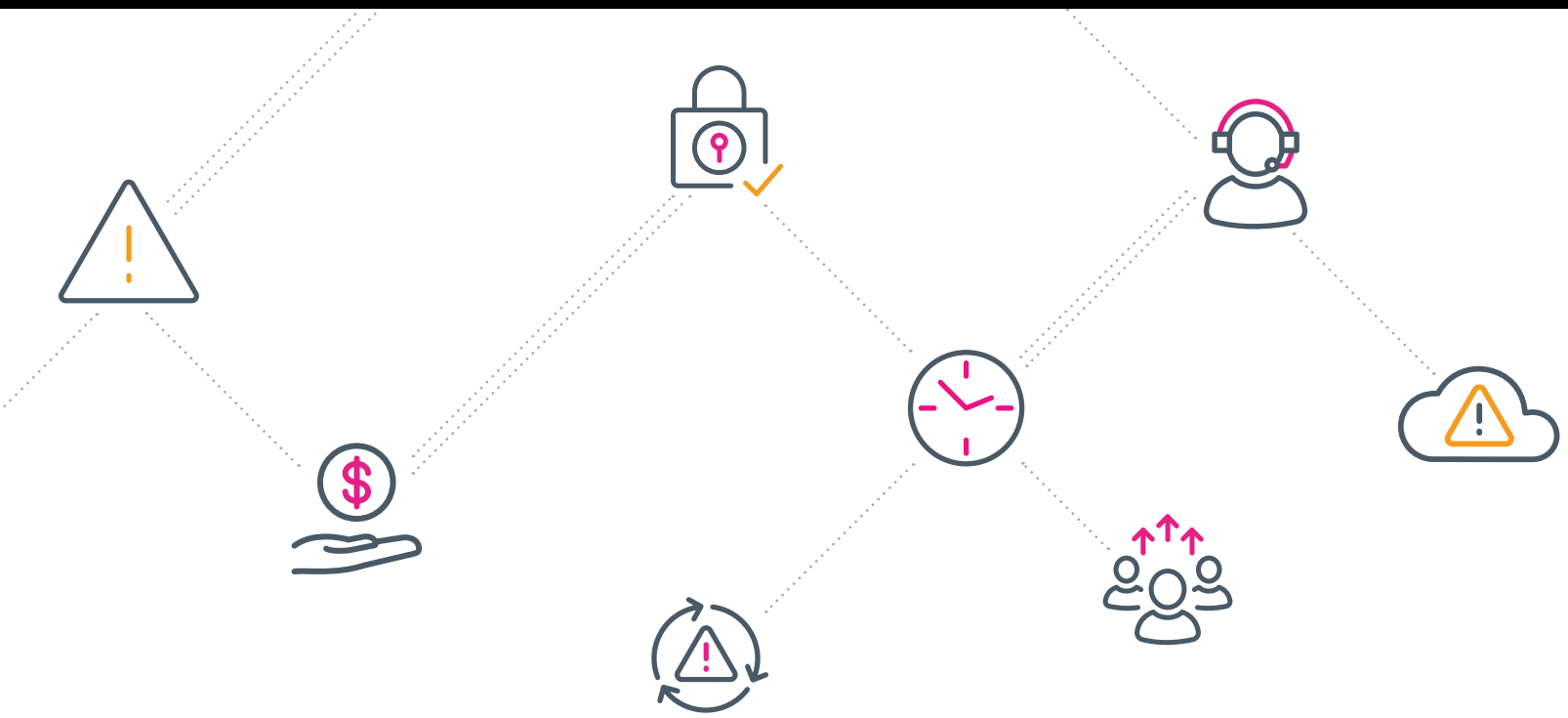
2022 SIEM 구매자 가이드

분석 기반 보안 솔루션의 구매자, 구매 대상, 구매 장소, 구매 시점 및 구매 이유

splunk>
turn data into doing™

목차



1. SIEM 개요

SIEM(Security Information Event Management) 솔루션은 마치 파일럿과 항공 교통 관제사들이 사용하는 레이더 시스템과 같습니다. SIEM이 없다면, 대규모 조직의 IT는 마치 앞을 볼 수 없는 채로 운항하는 것과 같습니다. 보안 어플라이언스 및 시스템 소프트웨어는 고립된 환경에 대한 공격과 비정상적인 작동을 포착하고 기록하는 데는 뛰어나지만, 오늘날 대부분의 심각한 위협들은 여러 시스템 분산되어 동시에 실행되며, 첨단 기법을 활용해 탐지를 회피합니다. 따라서 SIEM이 없다면 공격이 발생하고 치명적 사고로 발전할 수 있습니다.

더욱이 클라우드 서비스 사용이 증가하면서 공격이 더욱 교묘해지고 취약점 노출이 확대되고 있기에, 많은 기업들에게 SIEM의 중요성은 더욱 커지고 있습니다.

본 구매 가이드는 SIEM의 개요, 허와 실, 발전 과정, 주요 기능, 각 기업을 위한 최적의 보안 솔루션 결정 방법 등을 설명하는데 그 목적을 두고 있습니다

그렇다면, SIEM이란 무엇일까요?

가트너의 **SIEM 정의**에 따르면 "다양한 이벤트 및 컨텍스트 데이터 소스에서 보안 이벤트의 실시간 수집 및 과거 내역 분석을 통해 위협 탐지와 보안 사고 대응을 지원하는 기술" 입니다.

그 의미를 보다 쉽게 이해할 수 있을까요?

간단히 설명해 SIEM은 이벤트 로그를 수집하고 이 데이터에 대한 단일 뷰와 추가적인 인사이트를 제공하는 보안 플랫폼입니다.

SIEM의 진화

이벤트 로그의 장기 저장과 실시간 모니터링을 결합하여 보안 태세의 현재 상태를 전체적으로 이해하는 것은 매우 중요합니다. 이러한 IT팀의 요구를 충족하기 위해 SEIM은 성장해 왔습니다. 그러나 레거시 SIEM은 복잡하고 확장하기 어려운 과거의 기술로 구성되어 있습니다. 따라서 IT 전문가가 보안 공격을 신속하게 식별하고 이해하는 것이 힘들었던 것이 사실입니다. 결국 레거시 SIEM은 더 큰 유연성과 사용 편의성을 위해 강력한 분석 기반 도구로 진화할 필요성이 있었습니다. SIEM의 핵심 기능은 지난 10년간 확장세를 보였으며, 규정 준수 보고, 방화벽과 같은 엔드포인트 제품의 로그 집계, 위협 모니터링, 이벤트 상관 관계 설정, 분석 및 사고 대응이 포함되어 있습니다.

세상이 디지털 시대로 접어들면서 기업들은 클라우드 솔루션을 탐색하고 구현하기 시작했습니다. 그 결과 최신 분석 기반 SIEM 솔루션은 클라우드 기반 솔루션에 대응이 가능하지만, 레거시 SIEM은 그렇지 못합니다. 본 가이드에서는 레거시 SIEM과 최신 분석 기반 SIEM 간의 차이점과 유즈 케이스를 살펴볼 것이고, 이를 통해 독자 여러분 환경에서 SIEM 구현 준비도를 살펴봅니다.

과거에 발목 잡힌 레거시 SIEM

보안 전용 데이터를 수집, 저장 및 분석하기 위한 수많은 소프트웨어 옵션이 시장에 나와 있지만 이 데이터를 실행 가능한 인텔리전스로 전환할 수 있는 소프트웨어는 거의 없습니다.

애석하게도 SIEM 플랫폼에 투자한 많은 엔터프라이즈 IT 조직들은 이와 같은 근본적인 진실을 뼈아픈 경험을 통해 알게 되었습니다. 보안 이벤트의 기록에 막대한 시간과 비용을 지출했지만, 모든 데이터를 수집하는 데 긴 시간이 걸렸고, SIEM을 구축하는 데 사용된 기본 데이터 시스템은 정적인 경향이 있기 때문이었습니다.

더 큰 문제는 분석에 이용할 수 있는 데이터가 보안 이벤트만을 기반으로 한다는 것입니다. 이는 보안 이벤트와 나머지 IT 환경 전반에서 실제로 발생하는 일들을 상호 연관시키는 것을 어렵게 만듭니다. 보안 이벤트 조사가 필요한 경우, 대부분의 IT 조직은 소중한 시간을 낭비할 여유가 없습니다. 또한, 레거시 SIEM 솔루션으로는 조사가 필요한 보안 이벤트의 속도를 따라잡을 수 없습니다. 여기에 더해 많은 기업들이 클라우드 서비스를 채택하면서 위협 벡터가 확대되고 있습니다. 따라서 사용자 활동, 행동 및 어플리케이션 접근이 어떻게 이뤄지는지 다양한 클라우드, 핵심 SaaS 및 온프레미스 서비스를 모니터링하고 잠재적인 위협과 공격을 전체적으로 판단할 수 있어야 합니다.

레거시 SIEM - 문제점과 특징

문제	이슈
필요한 데이터 사용 불가	제한적 탐지, 조사, 대응
유지 및 운영의 어려움	복잡성 및 숙련된 직원
높은 오탐률	SecOps에 부담
불안정	시스템 중단
유연하지 않은 데이터	크리티컬 케이스에 적응 불가
정적 워크플로우	제한적/한정적
신종 위협 탐지 불가	비즈니스 리스크

대안: 분석 기반 SIEM

엔터프라이즈 IT조직은 모든 보안 관련 데이터 전반에서 정보의 상관 관계를 파악할 수 있는 간단한 방법을 필요로 합니다. 즉, IT조직이 손쉽게 자체 보안 태세를 관리할 수 있는 솔루션이 필요합니다. 단순히 이벤트가 발생한 후 관찰하는 것이 아니라, IT 조직은
이벤트 발생을 예측하고 취약성을 제한하기 위한 조치를 실시간으로 구현할 수 있어야 합니다. 이를 위해서는 분석 기반 SIEM 플랫폼이 필요합니다.

이 지점에서 레거시 SIEM과 현대화된 솔루션 간의 차이가 명확하게 드러납니다. 가트너는 "**현대화된 SIEM은 데이터를 로깅하는 것 이상의 기능을 수행하며 데이터 분석을 위해 단순한 상관 관계 규칙 이상을 적용**"한다고 지적했습니다.

지금부터는 특정 요건을 갖춘 최신 SIEM(분석 중심 SIEM 솔루션)에 대해 설명하고자 합니다. 현대적 SIEM 솔루션을 통해 IT조직은 실시간 으로 위협을 모니터링하고 사고에 신속하게 대응하여 피해를 방지 하거나 제한할 수 있습니다.

하지만 모든 공격이 외부에서 이루어지는 것은 아닙니다. 따라서 IT조직은 사용자 활동을 모니터링함으로써 내부자 위협 또는 우발적인 공격의 위험을 최소화할 수 있는 방법이 필요합니다. 위협 인텔리전스는 광범위 한 위협 환경의 특성을 이해하고 이러한 위협을 사용자 환경의 맥락에 맞게 적용하는 과정에서 핵심적 역할을 합니다.

분석 기반 SIEM은 탁월한 보안 분석 기능을 제공해야 하며 IT 팀이 정교한 정량적 방법론을 활용해서 인사이트를 확보하고 업무에 대한 우선 순위를 설정할 수 있도록 해야 합니다. 마지막으로 최신 SIEM은 핵심 플랫폼의 일부로서 첨단 위협 대응에 필요한 전문적 도구를 포함해야 합니다.

분석 기반 SIEM과 레거시 SIEM의 또 다른 주요 차이점은 현대화된 솔루션은 유연한 배포 특성을 활용해 온프레미스, 클라우드 또는 하이브리드 환경에 구축이 가능하다는 점입니다.
아래 그래프는 레거시 SIEM이 아닌 분석 기반 SIEM 솔루션을 선택해야 하는 가장 중요한 7가지 이유를 설명합니다.

레거시 SIEM을 교체해야 하는 7가지 이유

많은 조직들이 전통적인 SIEM의 구형 아키텍쳐에 묶여 있는 경우가 있습니다. 이 경우 일반적으로 SQL 데이터베이스를 사용하고 고정된 스키마를 사용합니다. 하지만 이러한 데이터베이스는 모든 문제의 원천이 될 수 있으며, 확장성 및 성능에 한계가 있습니다.

1. 제한된 보안 유형	수집된 데이터 유형이 제한되기 때문에 탐지, 조사 및 응답 시간에 한계가 있습니다.
2. 효율적인 데이터 수집 불가능	레거시 SIEM에서는 데이터 수집이 매우 어렵거나 많은 비용이 소요되는 프로세스가 될 수 있습니다.
3. 느린 조사	레거시 SIEM에서는 원시 로그 검색과 같은 기본적인 작업도 상당한 시간이 걸릴 수 있으며 완료하는 데 며칠, 몇 시간이 걸리기도 합니다.
4. 설치 용이성 및 확장성	SQL 기반 데이터베이스의 규모가 커질수록 안정성은 떨어집니다. 이벤트 급증으로 인해 서버가 다운되면서, 고객 입장에서는 성능이 빈번하게 저하되거나 서비스 중단이 발생하기도 합니다.
5. 단종 또는 불확실한 로드맵	레거시 SIEM 벤더의 인수합병 등으로 소유권이 변경되면서 R&D 속도가 느려집니다. 지속적인 투자와 혁신이 이루어지지 않는다면, 보안 솔루션은 증가하는 위협 환경을 따라잡지 못하게 됩니다.
6. 폐쇄된 에코시스템	레거시 SIEM 벤더들은 시중에 나와있는 다른 툴들을 통합할 수 없는 경우가 많습니다. 고객들은 SIEM에 포함된 기능들을 이용하거나 커스텀 개발 및 전문 서비스를 위한 추가 비용을 지출해야 합니다.
7. 온프레미스로 제한	레거시 SIEM은 대개 온프레미스 구축으로 제한됩니다. 하지만 보안 실무자들은 클라우드, 온프레미스 및 하이브리드 워크로드를 사용할 수 있어야 합니다.

SIEM의 클라우드 전환

클라우드에서, 또는 SaaS로서 SIEM을 실행하는 것은 많은 기업들이 보안 인텔리전스와 관련하여 겪고 있는 문제를 해결하는 데 도움이 될 수 있지만 많은 IT 리더들은 여전히 클라우드 보안 및 신뢰성에 대해 확신하지 못하고 있습니다. 하지만 클라우드 기반 SIEM 솔루션을 배제하기 전에 대부분의 대규모 클라우드 서비스의 보안 절차와 기술은 일반 기업들보다 훨씬 엄격하다는 사실을 알아야 합니다.

SaaS는 이미 CRM, HR, ERP 및 비즈니스 분석 등 중요한 업무 시스템에서 널리 사용되고 있습니다. 또한 SaaS가 엔터프라이즈 어플리케이션에 적합한 이유—빠르고 편리한 배포, 적은 운영 부담, 자동 업데이트, 사용량 기반 과금 및 확장성, 강력한 인프라—때문에 SIEM에는 클라우드 환경이 적합합니다.

클라우드 기반 솔루션은 온프레미스 및 클라우드의 다양한 데이터 세트를 활용할 수 있는 유연성을 제공 합니다. 많은 엔터프라이즈 워크로드가 IaaS, PaaS, SaaS로 이동하고 있으며 제3자 시스템과 손쉬운 통합이 손쉽다는 점을 감안하면, 클라우드 상의 SIEM은 더욱 적절한 옵션이 됩니다. SIEM을 클라우드로 전환함에 따른 주요 이점으로는 하이브리드 아키텍처의 유연성, 자동 소프트웨어 업데이트, 단순한 구성, 즉각적이며 확장 가능한 인프라, 강력한 통제력 및 고가용성 등을 들 수 있습니다.

엔터프라이즈를 위한 SIEM 유즈 케이스

지금까지 SIEM의 발전과 현대화된 분석 기반 SIEM 솔루션이 레거시 SIEM과 차별화되는 특성에 대해 살펴봤습니다. 이제 어떤 보안 유즈 케이스를 현대적 SIEM을 통해 구현할 수 있는지 설명하도록 하겠습니다.

첨단 위협을 완화하기 위한 조기 탐지, 신속한 대응 및 협업은 오늘날 엔터프라이즈 보안 팀에 상당한 부담을 안겨주고 있습니다. 더 이상 리포팅 및 모니터링 로그와 보안 이벤트로는 충분하지 않습니다. 보안 실무자들은 IT, 현업 부서 및 클라우드에 이르기까지 조직 전반에서 대규모로 생성된 모든 데이터 소스에 기반한 폭 넓은 인사이트를 필요로 합니다. 외부 공격과 악의적인 내부자에 맞서기 위해서는 탐지, 사고 조사 및 CSIRT 위반 시나리오 조정 등을 빠르게 수행할 수 있는 첨단 보안 솔루션이 필요합니다. 또한 기업들은 알려진/알려지지 않은 위협, 신종 위협을 탐지하고 대응할 수 있어야 합니다.

엔터프라이즈 보안팀은 일반적 보안 유즈 케이스는 물론, 고급 유즈 케이스도 해결하는 SIEM 솔루션을 이용해야 합니다. 또한 다이내믹한 위협 환경에 대응하기 위해 현대화된 SIEM은 다음과 같은 기능을 제공할 수 있어야 합니다.

- 소스에서 생성되는 모든 보안 관련 이벤트의 중앙 집중화 및 집계
- syslog, 파일 전송, 파일 수집 등을 포함한 다양한 수신, 수집 방식 지원
- 보안 이벤트에 컨텍스트(context) 및 위협 인텔리전스 추가
- 다양한 데이터 간의 상관 관계 및 경보
- 신종 및 알려지지 않은 위협 탐지
- 조직 전반의 활동 프로파일링
- 모든 데이터(사용자, 어플리케이션)를 수집해 모니터링, 경보, 조사,
- 애드혹(ad hoc) 검색 등의 용도로 사용할 수 있도록 함
- 고급 침해 분석을 위해 데이터의 애드 혹 검색 및 리포팅 기능 제공
- 사고 조사 및 상세 사고 분석을 위한 포렌식 조사 실행
- 규제 준수 상태 평가 및 보고
- 보안 상태에 대한 분석 및 리포팅 사용
- 간소화된 애드혹 분석 및 이벤트 시퀀싱을 통한 공격자의활동 추적

SIEM 데이터는 주로 서버 및 네트워크 디바이스 로그에서 수집되지만, 엔드포인트 보안, 네트워크 보안 디바이스, 어플리케이션, 클라우드 서비스, 인증 및 권한 부여 시스템, 기존 취약점 및 위협의 온라인 데이터 베이스 등을 통해서도 제공됩니다.

하지만 데이터 집계는 전체 과정의 절반에 불과합니다. 그 다음, SIEM 소프트웨어는 최종 리포지터리를 상호 연관시켜 비정상적인 작동, 시스템 이상 징후 및 기타 보안 사고의 지표를 확인합니다. 이 정보는 실시간 이벤트 알림뿐만 아니라, 규제 준수 감사 및 보고, 성능 대시보드, 과거 동향 분석 및 사후 사고 포렌식 등에도 사용됩니다.

보안 위협의 수가 지속적으로 증가하고 더욱 교묘해지고 있는 데다 모든 조직이 보유한 디지털 자산의 가치가 높아지고 있다는 점을 감안하면, 전반적인 IT 보안 생태계에서 분석 기반 SIEM 솔루션의 채택이 지속적으로 증가하는 것은 당연한 것입니다.

SIEM이 정말 필요한가?

지금까지 SIEM의 용도에 대해 살펴봤습니다. 이제 주제를 넓혀 보겠습니다. 여러분은 실제로 SIEM 솔루션을 필요로 합니까? 아니면 다른 것을 필요로 합니까?

아직 고급 보안 유즈 케이스에 대한 준비가 되어 있지 않다면, 단순히 CLM(Central Log Management)과 같은 머신 데이터에 대한 인사이트를 제공하는 솔루션을 필요로 할 수도 있습니다. 참조: **보안 및 로그 관리를 위한 Splunk Enterprise**를 확인해 보십시오.

그렇다면, CLM(Central Log Management) 솔루션이란 무엇일까요? CLM은 로그 데이터에 대한 중앙 집중식 뷰를 제공하는 솔루션으로 간단히 정의가 가능합니다.

자세하게 살펴보기 위해 다음과 같은 질문을 해보도록 하겠습니다. 로그 데이터란 무엇일까요? 로그 데이터는 컴퓨터에서 생성된 로그 메시지로서 모든 기업, 조직 또는 기관에서 일어나는 일들의 최종적인 기록입니다. 하지만 광범위한 비즈니스 목표의 지원과 문제 해결에는 아직 활용되지 않고 있습니다.

다시 CLM으로 돌아가겠습니다. 로그 관리의 목적은 컴퓨터에서 생성된 로그를 수집하고 검색 및 보고를 위해 접근할 수 있도록 만드는 것입니다. 즉, 보안 측면에서 CLM이 사고 조사와 경보 분류와 같은 작업을 지원할 수 있다는 것을 의미합니다.

로그 관리는 SIEM의 태동 시점부터 SIEM의 핵심 기능이었습니다. 하지만, 로그 데이터에 대한 인사이트만을 필요로 한다면, 분석 기반 SIEM 솔루션이 최적의 툴이 될 수 있을까요? **저명한 SIEM 애널 리스트인 Anton Chuvakin**에게 해답을 구해 보겠습니다.

요약하면, 로그 집계를 위해 SIEM 솔루션을 사용한다는 것은 필요 이상의 과도한 지출입니다. 여기에서 핵심은 SIEM을 이용해 기본적인 유즈 케이스와 고급 유즈 케이스 모두를 해결할 수 있다는 것입니다.

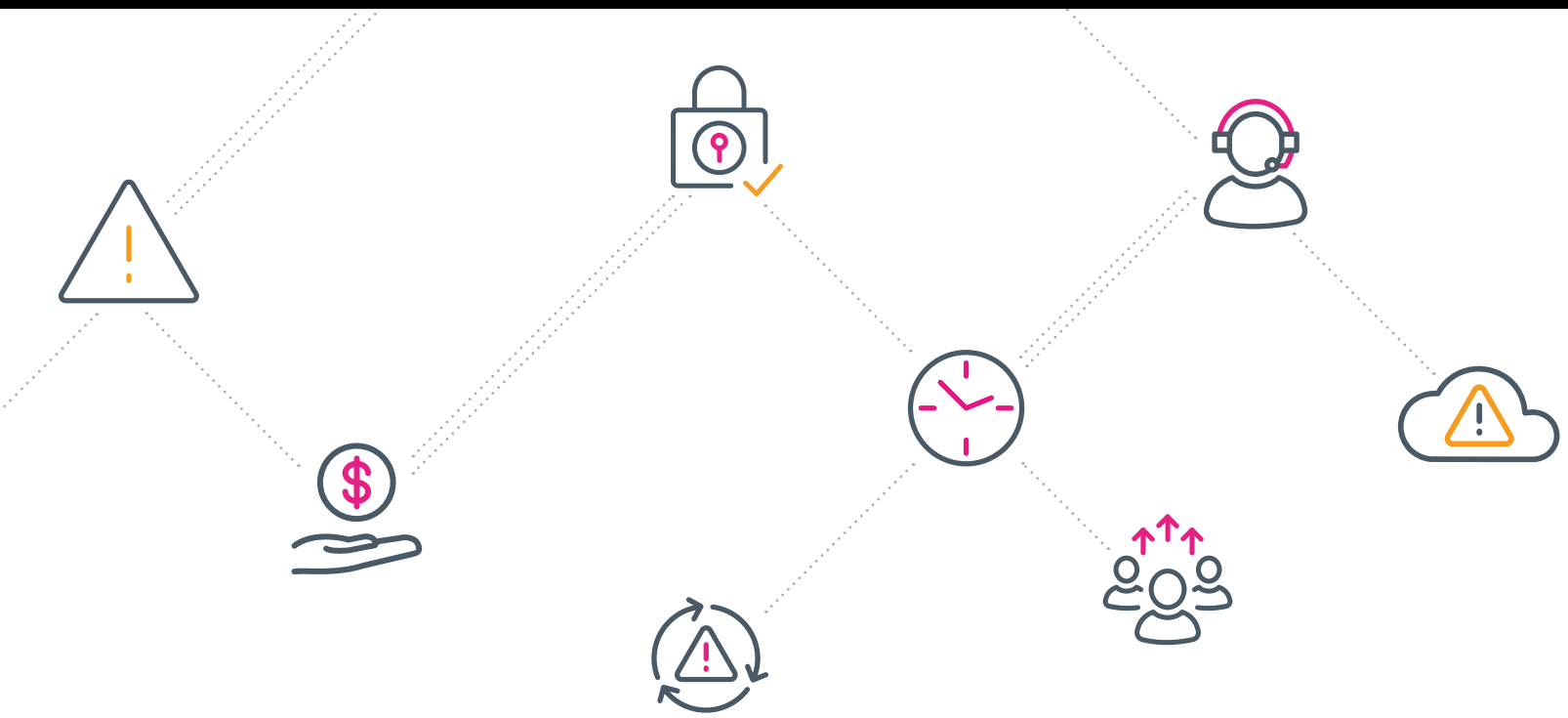
성숙 단계의 끝에는 **가트너 용어**로 UEBA(User and Entity Behavior Analytics)가 있습니다. 동일한 영역을 일컫는 또 다른 명칭으로는 **Forrester 가 선호하는 용어**인 보안 사용자 행동 분석과, **Splunk가 선호하는 용어인 UBA(User Behavior Analytics)**등이 있으며 본 보고서에서는 후자를 사용할 것입니다. 모두 근본적으로 동일한 기술을 일컫는 명칭들입니다.

UBA는 내부 및 외부 위협을 탐지하고 해결하는 데 사용됩니다. 예를 들어, UBA는 사용자의 정상적인 습관을 학습하고 기준을 설정한 다음, 정상에서 벗어나면 경보를 보내는 기능 등을 제공하기 때문에 보다 고급 보안 유즈 케이스로 인식되고 있습니다.
예를 들어 기준을 설정하기 위해서는 UBA 솔루션은 다음과 같은 활동의 패턴을 추적할 것입니다.

- 사용자가 일반적으로 로그인하는 위치
- 사용자에게 허용된 권한
- 사용자가 액세스할 수 있는 파일, 서버 및 어플리케이션
- 사용자가 정상적으로 로그인할 때 이용하는 디바이스

현재 몇몇 UBA 벤더들이 SIEM 시장에서 경쟁하기 위해 시도하고 있습니다. 이들은 SIEM 시장의 신규 진입 업체들입니다. UBA는 유용한 솔루션이지만, UBA 솔루션만으로 SIEM 솔루션을 대체할 수는 없습니다. 즉, UBA는 SIEM의 새로운 카테고리가 아니며 UBA 자체가 별도의 보안 기술입니다. 하지만 이상적인 경우라면, UBA 솔루션을 분석 기반 SIEM 솔루션과 함께 실행할 수 있어야 합니다.

보다 분명하게 설명하자면, CLM 솔루션은 SIEM이 아니며 UBA 솔루션만으로 SIEM을 구성할 수도 없습니다. 이제 Chuvakin 박사가 그 해답에 대한 **트윗을 보내주시기**만 하면 좋을 텐데요.



2. SIEM 기본 정보

이제 분석 기반 SIEM 솔루션의 구성 요소에 대해 살펴보겠습니다. 분석 기반 SIEM은 6가지 핵심 기능을 제공합니다.

실시간 모니터링	위협은 빠르게 이동할 수 있으며 IT는 실시간으로 위협을 모니터링하고 이벤트 상관관계 분석을 진행하여 위협을 찾아내고 멈출 수 있어야 합니다.
사고 대응	IT는 손상을 최소화하고 복구 시간과 비용을 줄이기 위해 잠재적인 침해는 물론 보안 위반 또는 공격의 여파를 처리 및 관리하는 체계적인 방법이 필요합니다.
사용자 모니터링	컨텍스트에 따라 사용자 활동을 모니터링하는 것은 위반을 찾아내고 사용자 권한 오용을 발견하는 데 매우 중요합니다. 최상위 권한 사용자(privileged user) 모니터링은 규제 준수 보고의 공통적인 요구 사항입니다.
위협 인텔리전스	위협 인텔리전스는 IT가 비정상적인 활동을 인식하고 기업에 대한 위험을 평가하며 대응 우선 순위를 지정하는 데 유용합니다.
고급 분석	분석은 방대한 데이터에서 인사이트를 도출하는 데 중요하며 머신 러닝은 이와 같은 분석을 자동화하여 숨겨진 위협을 식별할 수 있습니다.
고급 위협 탐지	보안 담당자들은 킬 체인(kill chain) 전반에서 위협을 모니터링, 분석 및 탐지하는 전문 툴을 필요로 합니다.
유즈 케이스 라이브러리	실시간으로 위협을 이해하고 대응하는 것은 리스크 경감을 위해 필수적입니다.

이 기능들을 통해 기업들은 SIEM을 다양한 보안 유즈 케이스는 물론 규제 준수를 위해 활용할 수 있습니다. 이러한 다양한 유즈 케이스 지원 여부가 현대화된 SIEM을 규정하는 요소이기도 합니다. 이제 분석 기반 SIEM을 구성하는 필수적 기능에 대해 자세하게 살펴보도록 하겠습니다.

실시간 모니터링

위협을 발견하는 데 소요되는 시간이 길어질수록 더 큰 피해를 입을 수 있습니다. IT 조직은 온프레미스 또는 클라우드 등 어디에 저장되어 있건 관계없이 모든 데이터 세트에 실시간으로 적용할 수 있는 모니터링 기능을 포함한 SIEM을 필요로 합니다. 또한, 이와 같은 모니터링 기능은 자산 데이터, 아이덴터티 데이터와 같은 컨텍스트 데이터 피드(contextual data feed)는 물론, 경보를 생성하는 데 사용될 수 있는 위협 인텔리전스 피드(threat intelligence feed)를 모두 검색 및 추출할 수 있어야 합니다.

분석 기반 SIEM은 사용자, 디바이스 및 어플리케이션은 물론 IT 환경 내 모든 엔티티를 식별할 수 있어야 하며, 특정 ID와 연관되지 않은 모든 활동 을 식별할 수 있어야 합니다. SIEM은 이 데이터를 실시간으로 사용해 다양한 유형과 종류의 이상 행동을 식별할 수 있어야 합니다. 식별이 완료 되면 해당정보는 이상 행동으로 발생할 수 있는 사업적 리스크를 평가하기 위해 설정된 워크플로우로 쉽게 입력이 가능해야 합니다.

또한 커스터마이제이션이 가능하고 사전에 정의된 상관 관계 규칙 라이브러리, 실시간으로 보안 사고를 표시하는 이벤트 콘솔이 있어야 하며, 보안 사고 및 이벤트에 대한 상황을 실시간으로 보여주는 대시 보드가 필요합니다. 마지막으로 실시간으로 혹은 특정 시점에 정기적으로 실행되도록 예약이 가능한 상관 관계 검색이 기본적으로 제공되어야 합니다. 또한, IT 관리자가 검색을 위한 별도의 언어를 익힐 필요가 없도록 직관적인 사용자 인터페이스가 제공되어야 합니다.

마지막으로 분석 기반 SIEM은 검색 데이터 액세스가 생성하는 네트워크 트래픽의 양을 줄일 수 있도록 실시간 및 과거 데이터를 로컬하게 검색할 수 있는 기능을 제공해야 합니다.

Autodesk, AWS에서 Splunk를 활용해 시간 및 투자 지출(capex) 절감

최근 발표된 아카데미 시각 효과상의 20개 수상자를 포함해 제조, 설계, 건설, 건축, 언론 및 엔터테인먼트 산업 전반의 고객들은 Autodesk 소프트웨어를 이용해 자체 아이디어를 디자인, 시각화 및 시뮬레이션하고 있습니다. 전 세계 각지에 진출한 Autodesk는 그룹 전반에서 전 세계적인 사업, 운영 및 보안 인사이트를 확보하고 운영 인텔리전스 소프트웨어를 구축하는 최적의 인프라를 선택해야 한다는 과제에 직면했습니다. 그리고 Splunk 플랫폼을 도입한 이후, Autodesk는 다음과 같은 이익을 거두었습니다.

- 수십 만 달러 절감
- 주요 운영 및 보안 관련 인사이트
- 제품 성능에 대한 실시간 가시성

왜 인가?

Splunk는 2007년 운영 문제 해결을 위해 머신 데이터를 활용하는 방법으로서 Autodesk에 도입되었습니다. 현재는 3개 사업부 전반의 실시간 모니터링, 자세한 보안 인사이트, 임원 관련 다양한 비즈니스 분석 등을 포함하도록 확장되었습니다.

- EIS(Enterprise Information Services) — 정보 보안 및 정보 관리를 포함한 글로벌 기업 IT 관리 부문
- ACG(Autodesk Consumer Group) — Autodesk의 모든 소비자용 제품 부문
- IPG(Information Modeling & Platform Products) — 모든 산업군의 디자이너 엔지니어 등이 사용하는 상용 소프트웨어 부분

Autodesk는 Splunk Enterprise Security (Splunk ES)를 이용해 보안 이슈를 식별하고 해결하는 시간을 단축하고 있습니다. Splunk App for AWS도 활용해 Splunk Enterprise 및 기타 주요 어플리케이션을 위해 유연한 리소스를 제공하고 관리합니다.

데이터 기반 의사 결정 역량 강화

Splunk Enterprise, Splunk App for AWS, Splunk Enterprise Security 및 기타 Splunk 솔루션을 통해 Autodesk는 운영, 보안 및 제품 성능에 대한 중요한 실시간 인사이트를 얻을 수 있었습니다. Splunk의 유연한 데이터 기반 분석 및 AWS 기반 플랫폼은 Autodesk의 시간 절약, 설비투자 절감, 중요한 의사 결정의 범위와 깊이 향상에 도움이 되었 습니다. **자세한 내용.**

사고 대응

효과적인 사고 대응 전략의 핵심은 명확한 사고를 식별하는 것은 물론, 사고를 추적 및 업무를 재배정하고 주석을 추가할 수 있는 SIEM 플랫폼의 강력한 기능을 활용하는 것입니다.

IT는 조직 내 다른 구성원들의 직무에 따라 다양한 수준의 액세스를 제공할 수 있어야 합니다. 또한 수동 및 자동 이벤트 집계 기능, 타사 시스템의 정보를 pull/push하는 데 사용할 수 있는 API(Application Programming Interfaces) 지원, 합법적으로 허용된 포렌식 증거 수집 기능, 특정 유형의 사고에 대응하는 방법을 안내하는 플레이북 등의 기능도 중요합니다.

가장 중요한 것은 분석 기반 SIEM이 진행 중인 사이버 공격을 중단시킬 수 있는 자동 대응 기능을 포함해야 한다는 것입니다.

SIEM 플랫폼은 사고 관리를 위한 사용자 지정형 워크플로우가 개발될 수 있는 허브가 되어야 합니다. 물론, 모든 사고가 동일한 긴급성을 지닌 것은 아닙니다. 분석 기반 SIEM은 대시보드를 통해 잠재 위협의 심각도를 항목화할 수 있는 수단을 제공하며, 이를 통해서 노터블 이벤트를 평가하고, 분석가에게 이벤트 검토를 할당하며, 조사를 위한 정보 획득을 위해 노터블 이벤트를 상세 검토할 수 있어야 합니다. 또한, 분석 기반 SIEM으로 IT 조직은 모든 이벤트에 대한 적절한 대응을 위해 필요한 상황 별 인사이트를 확보할 수 있어야 합니다.

이러한 대응 기능에는 중요한 이벤트와 그 상태를 식별하고 이벤트의 심각도를 표시, 해결 프로세스를 시작하는 것은 물론, 해당 사고와 관련한 전체 프로세스에 대한 감사가 포함되어야 합니다.

마지막으로, IT 팀은 조사 중 단 몇 번의 마우스 클릭으로 모든 필드에 필터를 직관적으로 적용하여 분석 범위를 확장 또는 축소할 수 있는 대시보드가 있어야 합니다. 최종 목표는 바로 모든 보안 팀 구성원들이 이벤트, 조치 및 주석을 타임라인에 추가함으로써 팀 내 다른 구성원들이 현재 어떤 일이 일어나고 있는지를 쉽게 이해할 수 있도록 하는 것입니다. 그 다음, 이러한 타임라인은 저널(journal)에 포함되어 쉽게 공격을 검토하고, 특정 유형의 이벤트에 대응하기 위한 킬 체인 방법론을 반복적으로 적용하는데 도움을 줄 수 있어야 합니다.

PagerDuty, Splunk Cloud 및 Amazon Web Service로 엔드 투 엔드 가시성 보장

엔터프라이즈급 사고 대응 서비스를 제공하는 PagerDuty는 고객사의 신속하고 효율적 IT 사고 관리 및 해결을 지원합니다. 클라우드 네이티브 기업인 PagerDuty는 운영 분석 및 분류 요구를 충족하는 솔루션이 필요했으며 AWS에서 실행되는 Splunk Cloud를 선택했습니다. 이후 PagerDuty는 자체 서비스의 고가용성을 보장하고 고객의 요구에 맞춰 확장을 제공할 수 있었으며, Splunk Cloud를 도입한 이후, 다음과 같은 이익을 거두었습니다.

- 고객 만족도 및 고가용성 클라우드 서비스 보장
- 이전 서비스보다 30%의 비용 절감
- IT 및 보안 사고 해결 시간을 몇 십 분에서 몇 분 또는 초 단위로 단축

왜 Splunk인가?

Arup Chakrabarti는 PagerDuty의 인프라 엔지니어링 담당 디렉터로서 사이트 신뢰성, 내부 플랫폼 및 보안 엔지니어링을 담당하고 있습니다 Arup의 팀에서는 전사적 엔지니어링 조직에서 생산성과 효율성을 증진하는 것을 목표로 하고 있습니다.

여기서 엔지니어링 조직이란, 회사의 상품 개발 조직에 속한 다양한 엔지니어링 팀을 모두 포괄합니다.

Splunk Cloud를 도입하기 전에 PagerDuty는 로깅 솔루션을 사용했는데, 매일 수백 기가바이트의 로그를 인덱싱하기 시작하면서 해당 솔루션의 확장성 한계를 느낍니다. 뿐만 아니라, 이 팀은 자체 데이터에서 실행 가능한 정보를 도출, 신속하게 의사 결정 및 문제 해결이 어렵다는 사실을 깨달았습니다. 이전에 사용하던 서비스와 Splunk Cloud를 비교하여 실행한 후, Splunk Cloud가 문제를 신속하게 해결하고 고객에게 고가용성을 보장하는 데 필요한 우수한 속도를 제공한다고 판단했습니다. 그리고 며칠 내에 엔지니어들은 Splunk Cloud로 마이그레이션을 완료했습니다 Chakrabarti는 **"이전 솔루션에서는 일부 쿼리가 데이터를 크런치하고 필요한 정보를 제공하는 데 최대 30분이 걸렸는데 이는 도저히 받아들일 수 없는 일이었습니다. 하지만 Splunk Cloud 도입으로 고객 영향 측면에서, 해결 시간을 몇 십 분에서 몇 분 또는 몇 초 단위로 단축할 수 있었습니다."**라고 설명했습니다

Chakrabarti는 비용이 Splunk Cloud를 선택한 가장 큰 요인은 아니었지만, **"최적의 솔루션을 도입하기로 했으며, 현재 이용하고 있는 솔루션보다 30% 저렴하다고 회계 팀에 말하자 그 반응은 열광적 이었습니다."** 라고 밝혔습니다. **자세한 내용**.

사용자 모니터링

사용자 활동 모니터링은 액세스 및 인증 데이터를 분석하고, 사용자 컨텍스트를 설정하며 의심스러운 활동과 회사 및 규제 정책 위반과 관련한 경보를 전달할 수 있는 기능을 기본적으로 포함해야 합니다.

가장 자주 공격 대상이 되고, 또한 공격을 당하면 가장 큰 피해로 연결되는 최상위 권한 사용자(privileged user)까지 사용자에 대한 모니터링을 확장하는 것이 중요합니다.

실제로 이와 같은 위험 때문에 최상위 권한 사용자 모니터링은 대부분의 규제가 강한 산업에서는 규제 준수 보고를 위한 공통적인 요건입니다.

이러한 목표를 달성하기 위해서는 모든 타사 어플리케이션 및 서비스를 포함하도록 확장이 가능한 다양한 아이덴터티 메커니즘을 활용하는 실시간 뷰와 리포팅 기능이 필요합니다.

Travis Perkins PLC, 하이브리드 클라우드 전환을 위해 분석 기반 SIEM 채택

Travis Perkins PLC는 영국의 건설 자재 및 주택 수리 용품 소매 유통 업체로서 2천여 개 매장과 2만8천여 명의 직원을 보유하고 있습니다. 2014년 이 업체는 "클라우드 우선" 여정에 착수했지만, 기존 보안 정보 및 이벤트 관리 솔루션은 하이브리드 환경 전반에서 필요한 보안 인사이트를 제공할 수 없었습니다.

Travis Perkins PLC는 여러 대안들을 검토했으며 Splunk Cloud, Splunk Enterprise 및 Splunk Enterprise Security (ES)를 SIEM으로 선택했습니다. Splunk 플랫폼을 도입한 이후, Travis Perkins PLC는 다음과 같은 이익을 거두었습니다.

- 하이브리드 인프라 전반의 가시성 향상
- 복잡한 사이버 위협 탐지 및 대응 능력 확보
- 보다 효율적인 리소스 활용을 통한 IT 비용 절감

왜 Splunk인가?

경기 침체로 어려운 시장 상황에 직면해 Travis Perkins PLC는 기술 투자를 우선 순위에서 제외했습니다. 하지만 최근 경기가 회복되면서 모든 기술 인프라에 대한 전략적 검토를 실시했으며 비용을 줄이고 유연성을 높이기 위해 클라우드 우선 접근 방식을 채택했습니다.

Travis Perkins PLC가 Google Cloud의 G Suite, Amazon Web Services 및 Infor CloudSuite 등을 비롯해 많은 클라우드 서비스를 실행하면서, 기존 SIEM이 복잡한 하이브리드 환경 전반에서 보안 이벤트에 대한 필요한 인사이트를 제공할 수 없다는 것이 분명해졌습니다. HP, IBM, LogRhythm 등의 대안들을 검토한 결과, Travis Perkins PLC는 보안 관련 환경에 대한 단일 뷰를 제공하기 위해 Splunk Cloud, Splunk Enterprise 및 Splunk ES 등을 선택했습니다.

처음부터 보안에 중점을 두고 개발

Travis Perkins PLC는 Splunk ES 구현을 통해 보안 팀에만 초점을 맞추는 것이 아니라 IT 부서 내 모든 구성원의 보안 인식을 향상시켰습니다. 이제 IT 운영 팀의 구성원은 특정 대시보드 및 경보에 액세스하여 잠재적 위협에 대한 초동 조치를 취할 수 있으며 전담 보안팀으로 에스컬레이션하기 전에 필요에 따라 즉각적인 조치를 실시하는 것이 가능합니다. 그 결과, Travis Perkins PLC는 일반적으로 요구되는 막대한 리소스 투자 없이 매우 효과적 이고 능률적인 SOC를 구축했습니다.

위협 방어 자동화

영국 전역에서 근무하는 2만4천 명의 직원들이 다양한 디바이스를 이용해 회사 데이터에 액세스하고 있었기 때문에 Travis Perkins PLC는 사이버 보안의 상당 부분을 자동화하는 것이 중요했습니다. Travis Perkins PLC는 이전의 상관 관계 데이터 혹은 기존 보안 솔루션에서 보내온 경보에 기반하여 다양한 위협 활동에 대하여 위험 점수를 Splunk ES를 활용하여 계산하고 있습니다. 피싱 이메일과 관련한 특정한 문제의 경우, Splunk 플랫폼에서 상관 관계 검색을 통해 감염된 클라이언트가 식별되면, 자동 경보를 생성합니다. 그러면, 해당 팀들은 사전 설정된 플레이북을 이용해 대처합니다. Splunk ES의 스윔레인(swimlane)은 자산 또는 사용자에 대한 종합적인 뷰를 제공하며 보안 사고의 조사 및 해결 시간을 크게 단축합니다. **자세한 내용**.

위협 인텔리전스

분석 기반 SIEM은 2개 차별화된 유형의 위협 인텔리전스를 제공해야 합니다. 먼저 위협 인텔리전스 사용에 있어 핵심은 침해, 공격 전술, 기법, 절차 등에 대한 현재 상황 정보와 함께 다양한 사고 및 활동 유형에 대한 맥락 정보를 제공할 수 있어야 한다는 것입니다. 이러한 인텔리전스를 통해 이미 활성화된 C&C(Command-and-Control) 서버로 알려진 외부 IP 주소에 대한 아웃바운드 연결을 식별하는 등 비정상적인 활동을 쉽게 확인할 수 있습니다. 이러한 위협 인텔리전스를 통해 분석가들은 적절한 대응 우선 순위 지정에 필수적인 공격의 위험 평가에 필요한 영향도 및 목적 등의 정보를 확보하게 됩니다.

두 번째 형태의 인텔리전스는 자산 중요도, 사용량, 연결 상태, 소유권 그리고 사용자의 역할과 책임 및 고용상태를 평가해야 합니다. 이러한 추가적인 맥락 정보는 위험과 사고의 잠재적 영향의 평가 및 분석에 있어 매우 중요합니다. 예를 들어, 분석 기반 SIEM은 사원증 정보를 수집한 다음, 해당 데이터를 VPN 인증 로그와 상관 관계 분석을 실행하고, 기업 네트워크상의 직원 위치에 대한 컨텍스트를 제공해야 합니다. 더 깊은 수준의 분석 및 운영 인텔리전스를 제공하기 위해 SIEM은 관계형 데이터베이스의 정형 데이터와 머신 데이터를 결합할 수 있어야 합니다.

위협 인텔리전스 데이터는 다양한 유형의 IT 인프라 및 어플리케이션에 의해 생성된 머신 데이터와 통합되어 초기 침입 탐지 성공률을 높이는 방식으로 감시 사항 목록(watch list), 상관 관계 규칙 및 쿼리를 생성할 수 있어야 합니다. 이 정보는 자동으로 이벤트 데이터와 상관 관계를 형성하고 대시보드 뷰 및 리포트에 추가되거나 방화벽, IPS(Intrusion Prevention System) 등과 같은 디바이스에 전달되어 취약점을 해결할 수 있어야 합니다.

SIEM에서 제공하는 대시보드는 IT 환경에 배포된 취약성 탐지 제품군에 대한 상태 및 활동을 추적할 수 있어야 합니다. 구체적으로는 스캐닝 시스템에 대한 상태를 제공하고, 취약성 검토를 위한 스캐닝을 더 이상 하지 않는 시스템을 식별할 수 있어야 합니다.

요컨대, 포괄적인 위협 인텔리전스 계층을 통해 모든 위협 목록에 대한 지원을 제공하고, 중복 인텔리전스를 자동으로 식별하고, 여러 위협 목록에 공통적으로 나열된 위협을 식별 및 우선 순위를 지정하고, 다양한 위협에 가중치를 할당하여, 비지니스에 영향을 줄 수 있는 실제 위험을 식별할 수 있어야 합니다.

로스앤젤레스 시, 실시간 보안 인텔리전스 통합해 40개 이상의 산하 기관 전반에서 공유

로스앤젤레스 시는 디지털 인프라를 보호하기 위해 자체 보안상태에 대한 상황을 인식하고 각 부서와 관계 당사자들을 위한 위협 인텔리전스를 확보해야 했습니다. 과거, 로스앤젤레스 시의 40 여 개 산하 기관들은 별도의 보안 장치를 사용하고 있었기 때문에 데이터를 통합하고 분석하는 것이 복잡했습니다. 로스앤젤레스는 위협을 식별해 우선 순위를 부여하고 위험을 완화하며, 의심스러운 활동에 대한 가시성을 확보하고 도시 전체의 위험을 평가하기 위해 확장 가능한 SaaS 보안 정보 및 이벤트 관리 솔루션이 필요했습니다. Splunk Cloud 및 Splunk Enterprise Security를 구축함으로써 로스앤젤레스는 다음과 같은 이점을 거두었습니다.

- 도시 전체를 위한 SCO 구축
- 실시간 위협 인텔리전스
- 운영 비용 절감

실시간 상황 인식

Splunk Cloud는 로스앤젤레스 시의 보안 상태에 대한 REST API를 활용하여 워크플로우 작업 또는 스크립트를 찾아서, 이를 시스템에 적용하는 것은 물론, 종합적인 뷰를 제공합니다. Splunk 포워더는 로스앤젤레스 시의 미가공 로그 및 기타 데이터를 Splunk Cloud로 보내고, 여기에서 데이터를 정규화하여 통합 SOC로 전송하고, 그 다음 Splunk 대시보드에서 분석 및 시각화가 이뤄집니다.

Splunk ES에는 사전 개발된 커스터마이제이션이 용이한 대시보드를 제공하고 있기에, 고위급 직원 및 분석가들은 도시의 네트워킹 인프라 전반의 보안 이벤트에 대해 항상 실시간으로 상황을 인식할 수 있었습니다. 모든 보안 데이터가 지속적으로 업데이트되는 하나의 데이터베이스에 저장되며, Lee의 팀은 다양한 로그와 정형 및 비정형 데이터 및 모든 머신 데이터를 보고 비교하여, 포괄적이고 실행 가능한 보안 인텔리전스를 도출할 수 있었습니다.

신속하게 최신 위협 인텔리전스 제공

시의 통합 SOC는 정보 수집 이상의 역할을 합니다. 정보 제공을 위해 Splunk Cloud의 데이터를 시기적절한 위협 인텔리전스로 변환합니다. 로스앤젤레스는 FBI, 국토 안보부, 비밀 서비스 등 법집행 기관과 같은 외부 이해 관계자와 함께 발견 사항을 공유합니다. 이 정보를 사용하여 로스앤젤레스는 연방 정부와 협력하여 위험을 식별하는 전략을 개발하고 네트워크 침입을 방지하기 위한 전략을 수립합니다.

Lee는 "상황 인식을 통해 스스로를 알고, 위협 인텔리전스로 적을 이해하고 있습니다. 우리는 통합 위협 인텔리전스 프로그램을 운영하고 있으며, Splunk SIEM은 우리의 통합 SOC에 적용한 중앙화된 정보 관리 플랫폼의 핵심 솔루션입니다."라고 말했습니다. **자세한 내용**.

고급 분석

분석 기반 SIEM은 통계, 설명적 및 예측적 데이터 마이닝, 머신 러닝, 시뮬레이션 및 최적화 등과 같은 정교한 정량적 방식을 사용한 고급 분석을 적용함으로써 추가적인 주요 인사이트를 제공합니다. 주요 고급 분석 방식에는 이상 징후 탐지, 피어(peer) 그룹 프로파일링, 엔터티 관계 모델링 등이 포함됩니다.

또한, 분석 기반 SIEM은 분류된 이벤트를 킬 체인에 매핑하거나 히트맵을 작성하여 보다 효과적으로 사고 조사를 지원하는 등 데이터를 시각화하고 상관 관계를 파악할 수 있는 툴을 제공하는 것이 중요합니다.

이 모든 것을 가능하게 하기 위해서는 스스로 정상적인 활동과 실제 이상 징후를 학습할 수 있는 머신 러닝 알고리즘을 사용하는 SIEM 플랫폼에 액세스할 수 있어야 합니다.

이 정도 수준의 활동 분석이 이뤄지면, 예측 모델을 개발, 검증 및 배포가 가능합니다. 또한, SIEM 플랫폼에서 타사 툴을 사용해 개발된 모델도 적용할 수 있어야 합니다.

혁신적인 클라우드 기반 SIEM 구축으로 Equinix에 실행 가능한 보안 인텔리전스 제공

Equinix, Inc.는 5개 대륙 33개 시장에서 세계적인 기업들이 자신들의 고객, 직원 및 파트너들과 연결되도록 돕고 있습니다. 전세계 수천 여 개 기업들이 Equinix 데이터 센터 및 상호 접속 서비스에 의존하고 있기 때문에 Equinix에서 보안은 무엇보다도 중요합니다. 보안 인프라 전반에서 통합 뷰를 확보하기 위해 Equinix는 중앙 집중식 가시성 확보가 가능하며, 운영 부담 없이 쉽고 신속하게 구현할 수 있는 SIEM 기능을 갖춘 클라우드 솔루션이 필요했습니다. Splunk Cloud 및 Splunk Enterprise Security(ES)를 구축함으로써 Equinix는 다음과 같은 이점을 거두었습니다.

- 완벽한 운영 가시성
- 보안 태세 강화
- 시간 및 비용 절감

Splunk Cloud 및 Splunk Enterprise Security로 인프라에 대한 완벽한 가시성 확보

Splunk Cloud를 도입하기 전까지, Equinix는 매달 생성되는 300억 건 이상의 원시 보안 이벤트 처리에 어려움을 겪고 있었습니다. 하지만 Splunk ES 및 Splunk Cloud를 이용해 보안팀은 이제 300억 건의 원시 보안 이벤트를 약 1만2천 개의 상관 관계된 이벤트로 줄이고, 20개의 실행 가능한 경보로 다시 한번 줄일 수 있었습니다. 이러한 작업을 통해 실행 가능한 보안 인텔리전스와 전담 SOC를 위한 토대를 제공할 수 있었습니다. Splunk 플랫폼 내에 통합된 모든 데이터를 통해 보안 팀은 시스템들 간에 데이터를 상호 참조함으로써 사고 연구, 조사 및 대응 속도가 이전보다 30% 빨라졌습니다.

Equinix의 CISO인 George Do는 "궁극적인 목표는 고객, 직원 및 데이터를 보호하는 것입니다. ES와 Splunk Cloud는 SIEM 플랫폼으로서 우리가 원하는 정보를 항상 쉽게 이용할 수 있도록 합니다."라고 밝혔습니다.

"사고 조사가 필요하면, 관련 데이터가 Splunk 대시보드에 표시되기 때문에 보안팀의 모든 구성원과 최고 경영자들이 액세스할 수 있습니다. 이를 통해 전통적인 온프레미스 기반 SIEM을 구축하는 것과 비교해 총소유비용(TCO)을 50% 절감하는 등 막대한 시간 및 작업 부담을 절감하고 있습니다."

Splunk ES를 통해 Equinix는 이제 포괄적인 보안 분석 역량을 갖추게 되었습니다. 예를 들어, 한 현지 사용자 계정에 다른 대륙에서 로그인을 하는 의심스러운 활동 신호가 나타나면, 높은 우선 순위의 경보가 즉시 실행되고 보안 팀에 전달됩니다.

Splunk Cloud와 ES를 활용함으로써 Equinix는 민감한 기업 정보의 유출을 막을 수 있게 되었습니다. 특히 관리자는 상관 관계 분석을 통해 퇴사 예정인 직원이 기밀 데이터를 훔칠 가능성이 있는지 파악할 수 있게 되었습니다. **자세한 내용**.

고급 위협 탐지

보안 위협은 지속적으로 증가하고 있습니다. 분석 기반 SIEM은 네트워크 보안 모니터링, 엔드포인트 탐지 및 대응형 샌드박스, 행동 분석 등을 함께 구현하여 교묘한 신종 위협에 대응하고 있으며, 새로운 잠재적인 위협을 식별하고 격리시킬 수 있습니다. 대부분의 방화벽 및 IPS들은 자체적으로 이와 같은 기능들을 제공하지 못합니다.

보안에 있어 위협을 탐지하는 것은 물론, 특정한 신종 위협의 최초 탐지 후 어디를 공격하고 있는지 파악하고, 위협을 억제하는 방법, 정보 공유 방법 등을 규명함으로써 해당 위협의 범위를 파악할 수 있어야 합니다.

유즈 케이스 라이브러리

보안 이벤트는 끊임없이 진화하고 있기에 분석가 역시 위협을 실시간으로 탐지하고 대응할 수 있어야 합니다. 분석 기반 SIEM 솔루션은 즉시 사용 가능하고 사용자와 관련이 높은 콘텐츠를 활용하여 보안 태세를 강화하 수 있습니다. 유즈 케이스 라이브러리는 수집된 데이터를 기반으로 분석가가 새로운 유즈 케이스를 자동으로 발견하고 사용자의 환경 내에서 어떠한 유즈 케이스를 사용하는 것이 적합한지 결정하는데 도움이 될 수 있습니다. 이를 통해 신규 및 진행 중인 위협에 대해 더 빠른 탐지 및 사고 대응이 가능하며, 궁극적으로 리스크를 경감시킬 수 있다는 장점이 있습니다.

SAIC 가시성 및 위협 탐지확보

SAIC(Science Applications International Corp.)는 기술 엔지니어링 및 엔터프라이즈 정보 시장 분야에 주력하는 업계를 선도하는 기술 통합 업체입니다.

이공계 연구, 프로그램 관리 및 IT 서비스 등에 대한 전문성을 보유한 SAIC는 미국 정부가 주력 고객입니다. 따라서 SAIC는 강력한 SOC(Security Operations Center)와 CIRT(Computer Incident Response Team)를 구축하여 사이버 공격을 방어해야 했습니다. Splunk 플랫폼을 도입한 이후, SAIC는 다음과 같은 이익을 거두었습니다.

- 보안 태세 강화 및 운영 수준 향상
- 사고 탐지 및 해결 시간 80% 이상 단축
- 엔터프라이즈 환경 전반에서 포괄적인 가시성 확보

왜 Splunk인가?

2013년 이해 상충을 피하기 위해 원래의 SAIC가 2개 회사로 분할된 이후, SAIC는 새로운 보안 프로그램의 일환으로 SOC를 구축해야 했습니다. 필요한 보안 도구는 거의 다 가지고 있었지만, 방어 체계의 기반을 형성하는 보안 정보 및 이벤트 관리 솔루션은 없었습니다. 분할 전 보안 조사를 위한 핵심 툴로서 사용하던 전통적인 SIEM은 한계가 있었습니다. 이에 SAIC는 Splunk Enterprise로 SIEM을 보완했으며, 해당 플랫폼을 사용하여 상관 관계 검색을 통해 사고 탐지는 물론 사고 조사까지 처리하고 있습니다.

SAIC의 IT 운영 인력들은 이제 네트워크 모니터링, 성능 관리, 어플리케이션 분석 및 리포팅을 위해 Splunk 솔루션을 이용하고 있습니다.

SAIC는 새로운 SOC 구축에 착수한 후, 지속적인 모니터링, 경보 및 분석을 위한 사고 탐지, 조사 및 리포팅 등을 포함한 모든 SIEM 관련 요건을 충족하기 위한 단일 보안 인텔리전스 플랫폼으로서 Splunk를 활용하기로 결정했습니다.

환경 전반의 완벽한 가시성과 위협 탐지

SAIC는 현재 Splunk 소프트웨어를 활용하여 모든 위협에 대해서 자체 환경을 모니터링하고 있습니다. SOC에서 분석가들은 맞춤형 Splunk 대시보드에서 이상 및 승인되지 않은 활동에 대한 경보 및 징후를 모니터링합니다. 그 결과 분석가들은 시그니처 기반 위협(IDS 또는 멀웨어에 의해 로깅한 위협 등)과 알려지지 않은 위협(비정상적인 활동을 하는 최상위 권한 계정)을 즉시 인식하는 것이 가능합니다.

전통적인 SIEM들은 일반적으로 사전 개발된 경직된 검색 기능을 사용해 검색하기 때문에, 교묘한 신종 위협을 포착하지 못하고 많은 허위 경보를 발생시킵니다. 하지만 Splunk 플랫폼을 통해 SAIC 분석가들은 매우 정확하고 새로운 상관 관계 분석을 구현하여, SAIC를 겨냥한 위협과 침해지표(IOC)를 탐지하여 매우 높은 수준으로 위험을 측정하고 관리하고 있습니다. CISO를 포함한 임원들은 위협 활동에 대한 트랜드, 소스 위치 집계 정보, 및 새롭게 발견된 침해지표 등 다양한 KPI를 확인할 수 있습니다. **자세한 내용**.

아키텍처

최신 위협에 대응하기 위해서는 유연하고 확장 가능한 솔루션이 필요합니다. 분석 기반 SIEM 솔루션은 온프레미스, 클라우드 또는 하이브리드 환경에 배포가 가능해야 합니다.

현대적인 SIEM은 모든 규모의 조직에서 사용할 수 있어야 하며, 조직의 성장과 보안 요구 사항 성숙도에 맞춰 확장할 수 있을 만큼 충분히 유연해야 합니다.

Aflac, 분석 기반 보안을 위해 Splunk 플랫폼 채택

Aflac은 미국의 유명 보험사입니다. 보안 위협의 규모와 속도가 증가함에 따라 Aflac은 고객, 10,000명에 가까운 직원 및 브랜드 평판을 보호하기 위해 새로운 분석 기반 보안 접근이 필요했습니다. Aflac은 내부 위협 인텔리전스 시스템(TIS)의 핵심적 기능 수행을 위해 Splunk의 플랫폼을 사용하고 있습니다. Splunk Enterprise Security(ES) 및 Splunk UBA(사용자 행동 분석)를 배포한 이후 Aflac은 다음과 같은 이점을 얻을 수 있었습니다.

- 2주 만에 엔터프라이즈급 솔루션 구현
- 6개월 동안 200만 개 이상의 보안 위협 차단
- 수동 데이터 수집 및 보고를 솔루션으로 대체하여 매월 40시간을 절약, 팀원들이 사전 예방적 보안 모니터링 및 분석에 집중

왜 Splunk인가?

Aflac이 새로운 시장과 새로운 서비스를 제공함에 따라 스피어피싱부터 악성코드 확산까지 빠르게 변화하는 위협 환경에 적응할 필요가 있었습니다. 하지만 Splunk 플랫폼을 채택하기 전에는 전통적 SIEM 솔루션만 사용했으며, 공격을 적절히 탐지하고 대응하기 위해서는 보다 강력한 위협 인텔리전스 플랫폼이 필요하다는 점을 인식하게 됩니다.

Aflac의 보안 운영 및 위협 관리 이사 D.J. Goldsworth는 "이전의 SIEM에서는 조치를 취하기 전에 데이터를 매우 잘 알고 있어야 했지만 Splunk는 데이터를 매우 빠르게 알 수 있도록 도와줍니다. 또한 Splunk 덕분에 팀이 더욱 빠르게 움직일 수 있어, 모든 이해당사자들에게 더 빠르게 솔루션의 가치를 보여줄 수 있었습니다."라고 말합니다.

Aflac은 처음에는 위협 헌팅을 위해서 Splunk ES를 사용하기 시작했습니다. Goldsworth는 "처음 POC는 위협 헌팅 유즈 케이스에 Splunk ES를 사용하는 것이었지만, 우리의 기대보다 훨씬 더 빨리 많은 가치를 제공해 주었습니다. 매우 짧은 시간에 지능형 위협을 탐지하는 놀라운 성과를 달성할 수 있었으며, 그 결과 다양한 보안 유즈 케이스에 Splunk ES 및 UBA를 사용하기 위해 더 많은 투자를 결정하게 되었습니다."라고 밝혔습니다.

즉각적인 투자 효과

Goldsworth에 따르면 Splunk 플랫폼을 구현하고 엔터프라이즈급으로 전환이 2주 정도의 매우 짧은 시간 안에 가능했습니다.

Goldworth는 "데이터 소스의 양과 구현하고자 하는 유즈 케이스의 수를 고려할 때 이는 매우 놀라운 일이었습니다. 또한, Splunk를 통해 즉각적인 투자 수익을 얻을 수 있었습니다." 라고 설명했습니다.

Aflac은 Splunk ES를 사용하여 SOC에서 일하는 수많은 정규직 직원의 시간을 절약할 수 있었습니다. Goldsworth는 "이전에는 수동으로 작성하던 보고서를 이제는 완전히 자동화하여 한 달에 40시간 이상을 절약할 수 있었습니다."라고 말했습니다. "Splunk를 사용하면 다양한 소스에서 데이터를 수집하여, 이사회나 경영진 등 이해 관계자에게 의미 있는 방식으로 데이터를 제공할 수 있습니다." 라고 설명했습니다.

현재는 6개 팀의 약 40명의 직원이 Splunk 플랫폼을 사용하여 위협 헌팅, 위협 인텔리전스, 보안 운영, 사고 대응, 어플리케이션 보안, 보안 관리 및 부정사용 등 광범위한 보안 유즈 케이스를 관리하고 있습니다.

Goldworth는 "Splunk를 구현하여 위협 인텔리전스를 먼저 실시하고 그 다음 보안 운영으로 사용 영역을 확대했습니다. 이 과정에서 Splunk 솔루션의 능력을 확실히 알 수 있었고 자연스럽게 부정사용으로 적용 영역을 확장했습니다."라고 말했습니다.

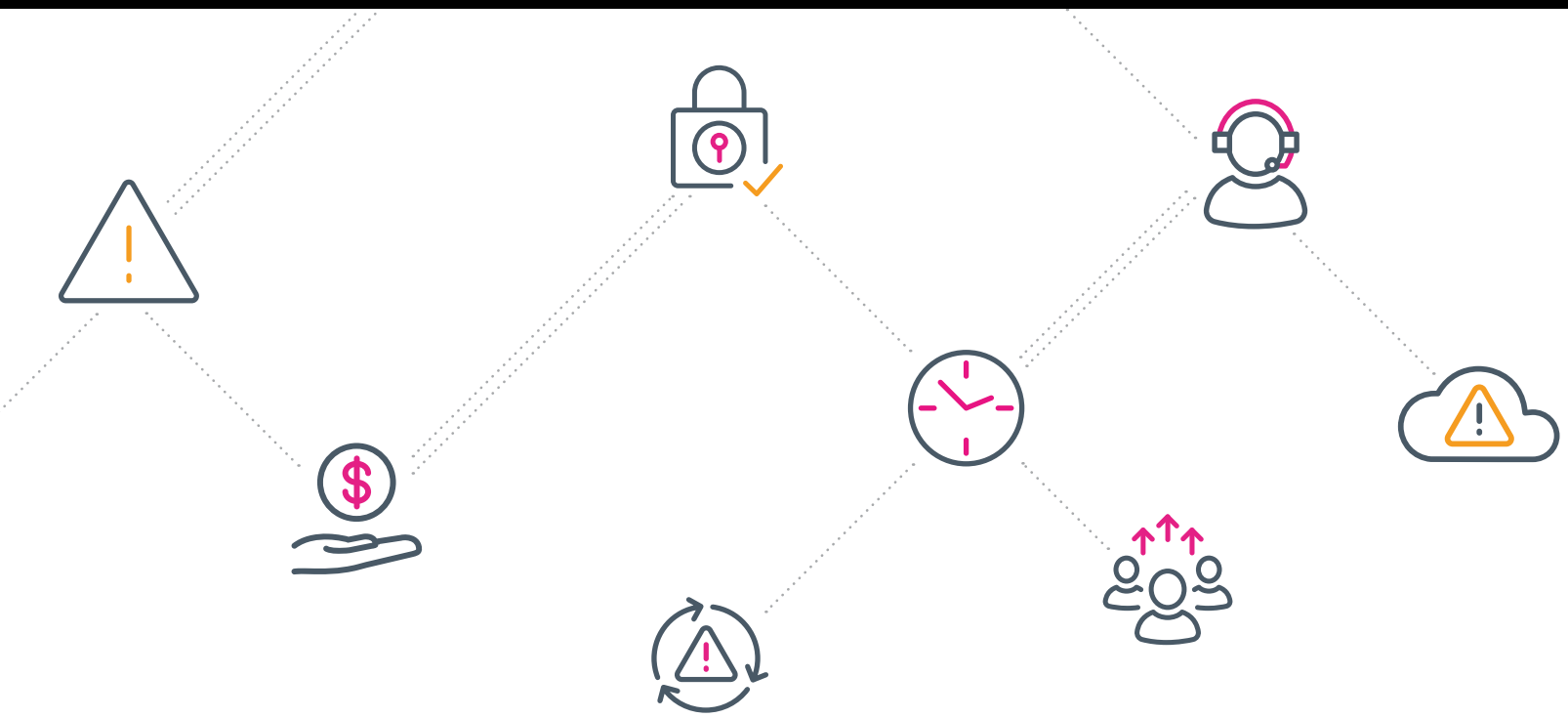
배포, 운영 및 지원

SIEM 솔루션은 시작 및 실행이 어려울 수 있으며, 일단 운영을 시작하면 지속적 유지 관리가 필요하다고 알려져 있습니다. 따라서 분석 기반 SIEM은 SIEM 지식을 갖춘 엔지니어가 부족할 수 있음을 감안하여, 사전 정의된 기능과 대시보드를 제공하고, 공급업체는 프로페셔널 서비스 등을 통해 발생 가능성이 있는 문제를 해결할 수 있어야 합니다.

로그 및 데이터 관리

로그 데이터는 모든 기업, 조직 또는 기관에서 일어나는 일들의 최종적인 기록이며 보다 광범위한 비즈니스 목표의 지원과 문제 해결 과정에서 제대로 활용되지 못하는 경우가 많습니다.

그리고 공격이 어디에서나 발생할 수 있는 오늘날의 위협 환경에서 모든 데이터는 보안과 관련이 있습니다. 이벤트 로그는 위협 탐지를 수행하고 규정 준수를 자동화하며 지능형 위협보다 앞서기 위한 시작점이 될 수 있습니다. 그리고 SIEM 솔루션은 비정형 원시 데이터를 저장할 장소가 필요하며, 이러한 데이터는 위협 헌팅, 고급 분석 및 사고 조사와 같은 작업을 수행하기 위한 데이터 보강에 유용하게 작용합니다.



3. 현대화된 SIEM의 9가지 기술적 기능

이제 분석 기반 SIEM의 6가지 핵심 기능에 대해 알아보기 위해, 분석 기반 SIEM 솔루션을 구성하는 기술에 대해 깊이 살펴보도록 하겠습니다. 이를 통해 레거시 SIEM, 오픈소스 SIEM 그리고 UBA 벤더들과 같은 신규 SIEM 시장 진입 업체 등과 현대화된 SIEM을 분명하게 구분해 보겠습니다.

SIEM 시장에 주목하는 모든 분들에게 가트너의 연례 매직 쿼드런트 보안 정보 및 이벤트 관리 보고서를 읽어 볼 것을 권합니다. 해당 보고서는 오픈소스 SIEM 벤더와 UEBA 벤더 등과 같은 신기술들을 포함하는 형태로 변화해 왔습니다.

또한, 가트너는 추가 SIEM 보고서를 제공하는 별도의 연구 조사를 진행했으며, 현대화된 SIEM을 차별화하는 9개 기술적 기능에 대해 집중적으로 다루며, Splunk 와 같은 기업들이 어떻게 기여할 수 있는지를 설명하고 있습니다.

광의의 SIEM에 속하는 여타 솔루션과 현대화된 SIEM 솔루션을 구분하는 9가지 기술적 기능들은 다음과 같습니다.

	SPLUNK	레거시 SIEM	오픈소스	신규 업체
1. 로그 및 이벤트 수집	예	예	예	예
2. 실시간 상관 관계(correlation) 규칙 활용	예	예	DIY	예
3. 고급 분석 및 머신 러닝의 실시간 활용	예	제한적	DIY	예
4. 장기적인 과거 내역 분석 및 머신 러닝	예	제한적	DIY	제한적
5. 장기적인 이벤트 저장	예	제한적	예	제한적
6. 정규화 데이터(normalized data)에 대한 검색 및 리포팅	예	예	예	예
7. 원시 데이터(raw data)에 대한 검색 및 리포팅	예	복잡	예	복잡
8. 추가 상관 관계 및 분석을 위한 컨텍스트 데이터의 수집	예	제한적	예	제한적
9. 보안 분야 외 유즈 케이스 해결	예	아니오	DIY	아니오

1. 로그 및 이벤트 수집

분석 기반 SIEM 솔루션은 모든 이벤트 로그를 수집, 사용 및 분석하고 실시간으로 통합 뷰를 제공할 수 있어야 합니다. 이를 통해 IT 및 보안 팀은 하나의 중앙화된 장소에서 이벤트 로그를 관리하고, 여러 시스템 또는 여러 일자에 대해 서로 다른 이벤트의 상관 관계를 정의하고, 레지스트리 변경 및 ISA 프록시 로그와 같은 다른 데이터 소스를 연계하여 전반적인 상황 파악이 가능합니다. 보안 실무자들은 단일 위치에서 모든 이벤트 로그에 대한 감사 또는 리포팅을 실행할 수 있어야 합니다.

2. 실시간 상관관계 규칙 활용 이벤트

상관관계란 다양한 보안 이벤트를 개괄적으로 파악한 이후 실제로 문제가 되는 요소를 파악하기 위해 다양한 이벤트를 연계하여 인사이트를 확보하는 것을 의미합니다.

3. 고급 분석 및 머신 러닝의 실시간 활용과(4.) 장기적인 과거 내역 분석 및 머신 러닝

기본적인 분석을 사용하면 데이터에 대한 패턴을 찾고 인사이트를 SIEM의 사용 맥락에 맞춰 제공하는 것이 가능합니다. 이러한 인사이트에 기반하여 보안 분석가는 더 심도있는 조사를 실행하고, 위협이 발생하기 전에 탐지하거나 사건에 대한 포렌식을 수행할 수 있습니다.

최근 실시된 **Forrester 조사**에 따르면 74%의 "글로벌 엔터프라이즈 보안 기술 의사 결정자들이 보안 모니터링 향상을 높은 또는 최우선 우선순위로 평가"했으며 "벤더들은 보안 분석 기능을 기존 솔루션에 추가하고 있으며 신규 벤더들은 레거시 솔루션으로 인한 부담 없이 최신 기술들을 활용하는 (보안 분석)솔루션을 개발"하고 있는 것으로 확인되었습니다.

또한 머신 러닝은 데이터 분석을 한층 발전시킵니다. 분석 기반 SIEM 솔루션에 머신러닝을 적용하면 과거 데이터를 토대로 더욱 지능화된 예측 분석을 할 수 있으며, 보안 실무자들은 이를 이용해 사고를 탐지하고 공격을 예측 또는 차단할 수 있습니다.

5. 장기적인 이벤트 저장

분석 기반 SIEM 솔루션은 장기적으로 과거 로그 데이터를 저장할 수 있습니다. 이를 통해 시간 경과에 따른 데이터의 상관관계 분석을 실행하고 규제 준수 요건을 준수에 도움을 줍니다.

이 기능이 특히 보안 측면에서 중요한 이유는 무엇일까요? 장기적인 머신 러닝 데이터 보관을 통해 보안 분석가들은 보안 포렌식 등을 실시하고, 네트워크 침해의 공격 경로를 역추적할 수 있습니다.

6. 정규화 데이터에 대한 검색 및 리포팅

SIEM의 관점에서 검색 및 리포팅은 사용자들이 데이터를 검색하고 데이터 모델과 피봇(pivot)을 개발하며 검색과 피봇을 보고서로서 저장하는 것은 물론, 경보를 설정하고. 공유가 가능한 대시보드를 만들 수 있도록 도움을 줍니다.

7. 원시 데이터(raw data)에 대한 검색 및 리포팅

SIEM의 측면에서 원시 데이터의 검색 및 리포팅이란, 다양한 소스 전반에 대한 데이터 컬렉션이며 분석 기반 SIEM 솔루션에 의한 중앙 집중화를 의미합니다. 분석 기반 SIEM 솔루션은 레거시 시스템과 달리 거의 모든 소스에서 원시 데이터를 수집할 수 있습니다. 이후 해당 데이터는 실행 가능한 인텔리전스로 전환될 수 있으며, 나아가 이해하기 쉬운 보고서로 전환될 수 있으며, SIEM 플랫폼에서 적절한 당사자에게 직접 배포가 가능합니다.

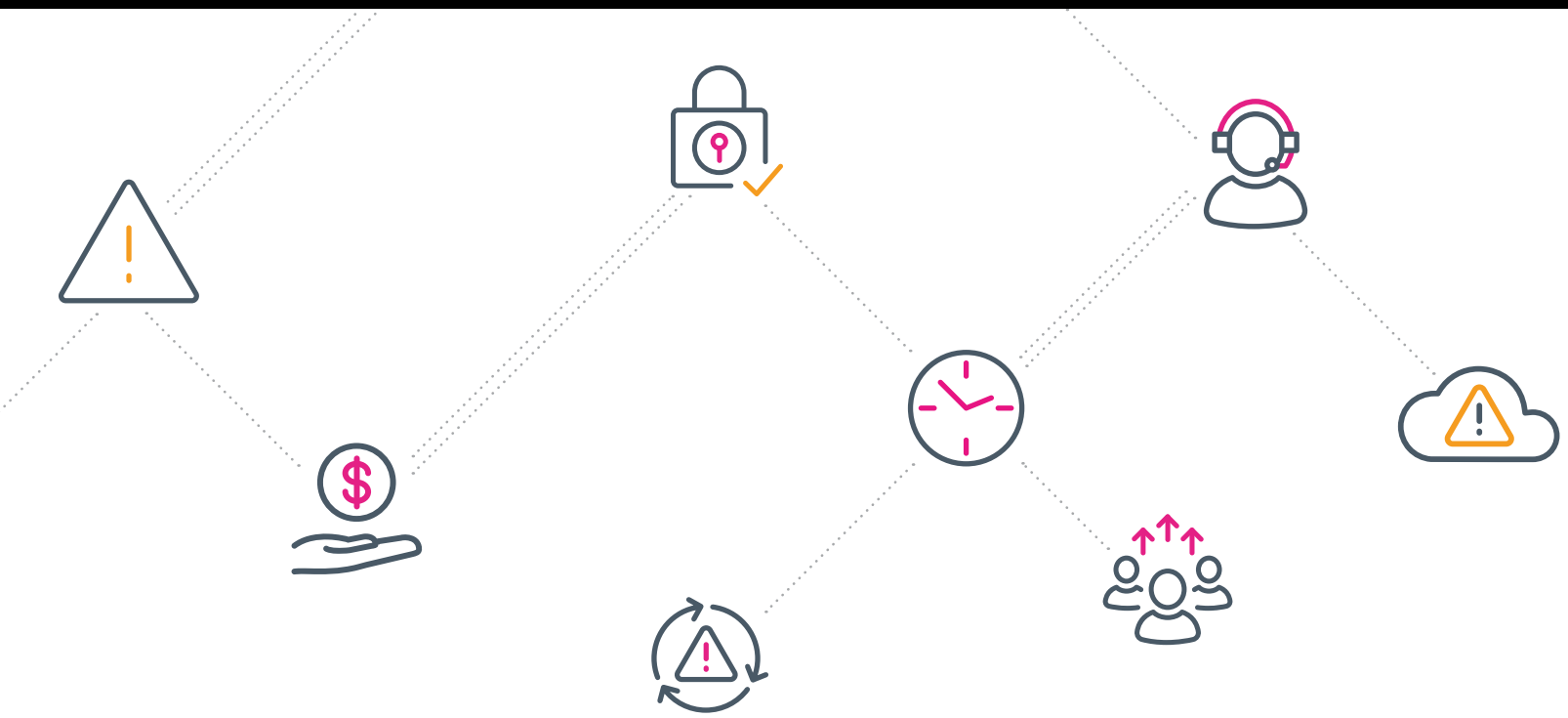
8. 추가 상관 관계 및 분석을 위한 컨텍스트 데이터의 수집

분석 기반 SIEM 솔루션이 데이터를 수집한 다음, 사용자가 해당 데이터를 이용해 업무를 수행하고, 그 의미가 무엇인지 파악하기 위해서는 컨텍스트 정보가 추가적으로 필요로 합니다. 실제 위협과 오탐을 구분하고, 실제 위협을 효과적으로 탐지하며 대응하는 데 있어 컨텍스트 정보는 매우 중요합니다.

분석 기반 SIEM 솔루션은 외부 위협 인텔리전스, 내부 IT 운영 및 이벤트 패턴에 컨텍스트를 추가할 수 있습니다. 이를 통해 사용자는 상세하게 조사가 가능하며, 실시간으로 위협에 대응할 수 있습니다.

9. 보안 분야 외 유즈 케이스 해결

분석 기반 SIEM 솔루션과 레거시 SIEM 솔루션 간의 또 다른 차이점은 IT Ops와 같은 보안 이외의 분야에 대한 여러 유즈 케이스에 사용이 가능한가 여부입니다.



4. Splunk 활용하기

데이터는 끊임없이 변화하는 세상의 중심에 있으며 도전과 기회를 동시에 제공합니다. 하지만 COVID-19로 인한 근무 방식의 변화, 클라우드 마이그레이션으로 인한 복잡성 증대, 4G에서 5G로의 네트워크 전환, 800억 개에 이르는 네트워크에 연결될 장치, 그리고 자동화가 우리의 삶의 일환이 되어버린 새로운 디지털 시대에는 데이터로 인한 도전 과제는 더욱 복잡해질 것입니다.

이러한 문제를 해결하기 위해 활용할 수 있는 가장 중요한 수단 중 하나는 데이터입니다. 본인들이 생성하는 데이터의 힘을 활용할 수 있는 기업은 더 효율적이고, 수익성이 높으며, 혁신적이며, 보안성도 더 높을 것입니다.

이러한 문제 해결을 위해 Splunk는 Data-to-Everything 플랫폼을 구현했으며, 전 세계 최초로 데이터를 행동으로 전환하는데 있어 장벽을 제거하고 있습니다. 이를 통해 모든 질문, 의사 결정 및 행동에 데이터를 활용할 수 있도록 지원하고 있습니다.

Splunk Enterprise는 모든 소스의 머신 데이터를 모니터링하고 분석하여 운영 인텔리전스를 제공함으로써 기업의 IT, 보안 및 비즈니스 성과를 최적화합니다. 직관적인 분석 기능, 머신 러닝, 패키지 어플리케이션 및 오픈 API를 지원하는 Splunk Enterprise는 세밀하고 심도 있는 유즈 케이스에서부터 전사적인 분석의 근간으로까지 확장이 가능한 유연한 플랫폼입니다.

- 모든 소스에서 로그/머신 데이터의 수집 및 인덱싱 가능
- 강력한 검색, 분석 및 시각화 기능으로 조직 전반의 역량 강화
- 방대한 Splunkbase 앱 에코시스템에서 보안, IT 운영, 비즈니스 분석 등을 위한 솔루션 제공
- 온프레미스 소프트웨어 또는 클라우드 서비스로서 이용 가능

Splunk의 SIEM 솔루션

Splunk 보안 솔루션은 현대적 SIEM의 새로운 기준을 충족할 뿐만 아니라, 컨텍스트와 시각적 인사이트를 제공하여 보안팀이 분석 결과에 기반하여 보다 신속하고 현명한 보안 의사 결정을 내릴 수 있도록 도움을 줍니다.

Splunk는 자체 SIEM을 구축하거나 레거시 SIEM에서 마이그레이션하기를 원하는 기업들에게 다양한 옵션 및 온프레미스, 클라우드 또는 하이브리드 등 다양한 배포 옵션을 제공합니다.

고객은 Splunk Enterprise 또는 SplunkCloud를 사용하여 기본 SIEM 유즈 케이스를 구현할 수 있습니다.

SplunkEnterprise 및 SplunkCloud는 Splunk 플랫폼의 핵심으로서 데이터 수집, 인덱싱, 검색 및 보고 기능 또는 CLM을 제공합니다. 많은 Splunk 보안 고객이 Splunk Enterprise 또는 Splunk Cloud를 사용하여 자체 실시간 상관 관계 검색 및 대시보드 등을 구축하여 SIEM의 기본적인 기능을 활용하고 있습니다. Splunk는 바로 사용할 수 있는 대시보드, 상관 관계 검색 및 보고서를 통해 고급 유즈 케이스를 지원하는 프리미엄 솔루션인 Splunk Enterprise Security(ES)를 제공합니다. Splunk ES는 Splunk Enterprise, Splunk Cloud 또는 둘 다에서 실행됩니다. 사전 구축된 상관 관계 규칙 및 경보 외에도 Splunk ES에는 조사에 도움이 되는 사고 검토, 워크플로우 기능 및 타사 위협 인텔리전스 피드가 포함되어 있습니다. 또한 Splunkbase에는 다른 보안 벤더를 위해 사전 구축된 검색, 보고서 및 시각화가 포함된 300개 이상의 다른 보안 관련 앱이 있습니다. 바로 사용할 수 있는 이러한 앱, 유틸리티 및 추가 기능은 보안 모니터링, 차세대 방화벽, 고급 위협 관리 등 다양한 기능을 제공합니다. 즉시 사용 가능한 풍부한 콘텐츠를 통해 유즈 케이스를 구현할 수 있을 뿐만 아니라 Splunk 보안 연구팀에서 제공하는 전문적인 정보를 활용하여 새로운 지능형 위협을 해결할 수 있습니다. Splunk, 파트너 및 타사에서 제공하는 이러한 모든 리소스와 서비스는 보안 활동 범위를 확장하는데 도움을 줍니다.

Splunk ES는 또한 규제 준수, 어플리케이션 보안, 사고 관리, 신종 위협 탐지, 실시간 모니터링 등 다양한 보안 유즈 케이스를 지원하기 위해 독립적으로 활용할 수 있는 5개의 프레임워크로 구성된 분석 기반 SIEM 입니다 분석 기반 SIEM 플랫폼은 단일 보안 분석 솔루션 내에 머신 러닝, 이상 징후 탐지 및 기준 기반 상관 관계 기능을 모두 결합하고 있습니다. Splunk ES는 시간 경과에 따라 시각적으로 이벤트 상관 관계를 찾고 다단계 공격에 대한 세부 사항 확인이 가능합니다.

Splunk ES는 모든 보안 관련 데이터 전반에서 비즈니스 컨텍스트에 따라 실시간으로 위협, 공격 및 기타 이상 활동을 발견, 모니터링 및 리포팅할 수 있도록 합니다. 이러한 고급 분석을 통해 고객들은 보다 빠른 위협 탐지 및 보안 에코시스템 전반에 걸친 신속한 사고 대응을 실현할 수 있습니다. Splunk Mission Control은 광범위한 보안 포트폴리오의 일부로서 Splunk ES의 강력한 기능을 개선 및 강화하는 새로운 솔루션입니다. 미래 지향적인 클라우드 기반 SaaS로서 공통 작업 영역에서 전체 이벤트 수명 주기에 대한 위협 및 우선 순위가 높은 보안 문제를 탐지, 관리, 조사, 헌팅, 격리 및 해결이 가능합니다.

분석 기반 SIEM의 핵심 기능을 업계 최초의 공통 작업 공간에 표시했으며, Splunk ES와 Splunk Mission Control은 SOC의 관리성 강화, 효율적 조사 수행, 프로세스 간소화 등 핵심적 요소를 지원하기 때문에 보안 위협을 더 빠르게 탐지, 조사, 대응할 수 있습니다.

SplunkES는 Splunk Enterprise 또는 Splunk Cloud(코어 데이터 플랫폼), Splunk User Behavior Analytics(고급 UBA 기능), Splunk Phantom(보안 오케스트레이션, 자동화 및 대응 [SOAR]), Splunk Mission Control(탐지, 조사 및 대응을 위한 공통 작업 공간)등을 아우르는 광범위한 보안 포트폴리오의 일부입니다.

Splunk, 왜 SIEM으로서 운영이 가능한가?

- Splunk 소프트웨어는 모든 규모(대, 중, 소)의 SOC 운영에 사용이 가능
- 보안 태세 평가, 모니터링, 경보 및 사고 처리, CSIRT, 침해 분석 및 대응, 이벤트 상관 관계 분석 등 광범위한 정보 보안 운영을 지원
- SIEM 및 보안 유즈 케이스에 대한 즉각적인 지원
- 알려진/알려지지 않은 위험 탐지, 위협 조사, 규제 준수 확인, 상세한 인사이트를 위한 고급 보안 분석 사용
- 검증된 통합형 빅 데이터 기반 보안 인텔리전스 플랫폼
- 고급 침해 분석을 위한 애드 혹 검색 활용
- 온 프레미스, 클라우드 및 하이브리드 온 프레미스/클라우드 배포 옵션
- 주요 클라우드 제공업체를 위한 탐지 및 조사 콘텐츠 사전 구축

하나의 SIEM으로 모든 것을 관리하다

사용자 환경 전체의 보안이 성숙해짐 따라 올바른 SIEM 솔루션의 선택은 미래의 비지니스 성공에 기여할 수 있습니다. Splunk ES는 전체 SOC를 재편하고 미래 지향적 전략을 수립하는 기반 역할을 할 수 있습니다.

Splunk ES는 Splunk Security Operations Suite의 핵심으로서, 차세대 SOC를 지원하기 위해 단일 플랫폼에 최고의 SIEM, UEBA 및 SOAR 기술을 결합이 가능합니다.

Splunk는 상기 기능을 기본적으로 지원할 뿐만 아니라 다음과 같은 유즈 케이스도 지원합니다.

- **모니터링:** Splunk Enterprise, Splunk Cloud, 또는 Splunk Enterprise Security
- **조사:** Splunk Enterprise, Splunk Cloud, 또는 Splunk Enterprise Security
- **자동화 및 오케스트레이션:** Splunk Phantom
- **지능형 위협 및 내부 위협 탐지:** Splunk UBA 및 Splunk Enterprise Security
- **사고 대응:** Splunk Phantom 또는 Splunk Enterprise Security
- **규정 준수:** Splunk Enterprise, Splunk Cloud, 또는 Splunk Enterprise Security

InfoTeK과 Splunk, 공공 부문을 위한 보안 인텔리전스 플랫폼 제공

많은 조직들이 SIEM 소프트웨어를 이용해 보안 위협을 모니터링, 조사 및 대응하고 있습니다. 하지만, 한 미국 정부 기관에서는 HP ArcSigh의 레거시 SIEM 소프트웨어가 예상대로 실행되지 않았으며, 업무 수행에 차질이 생겼습니다. 이 정부 기관은 세계적인 사이버 보안, 소프트웨어 및 시스템 엔지니어링 업체인 InfoTeK에 의뢰해 자사의 SIEM 툴을 교체했습니다. Splunk Enterprise 와 Splunk ES를 도입한 이후, 이 고객은 다음과 같은 이익을 거두었습니다.

- 주말 동안 설치하고 다음 날부터 공격 차단
- SIEM 지원 비용 75% 절감 달성
- 로그 어그리게이터 및 엔드포인트 솔루션 등 필요한 툴 수 감소

이 정부 기관은 Splunk Enterprise 및 Splunk ES를 통해 IT팀에 합리적인 비용으로 실행 가능한 보안 인텔리전스를 제공이 가능한 분석 기반 SIEM을 구축했습니다. InfoTeK은 이 고객을 위해 주말 동안 Splunk 소프트웨어를 구축했습니다. 그리고 구축 다음 날부터 소프트웨어의 가치가 발휘되었습니다. IT팀은 보안 이벤트를 검색하고 즉시 공격 벡터를 차단할 수 있었습니다.

InfoTeK의 수석 사고 처리 책임자겸 보안 엔지니어인 Jonathan Fair는 **"다른 제품에서는 여러 툴을 이동하면서 사용해야 몇 시간, 며칠, 심지어 몇 주가 걸리는 작업을 Splunk를 통해 몇 초, 몇 분 또는 몇 시간 내에 완료될 수 있었습니다. 이 고객은 네트워크를 완전히 재구축해야 하는 수준의 위협을 성공적으로 차단이 가능했으며, 심지어 제품 구매를 완료하기도 전에 ROI를 실현할 수 있었습니다."**라고 설명했습니다.

자세한 내용.

여기를 클릭해 InfoTek이 어떻게 SIEM 비용을 75% 절감했는지 확인해 보십시오.

모니터 리포트	탐지 경보	분석 조사	대응 협업	
사전 정의된 뷰 및 규칙	상관 관계 규칙, 임계 값	분석 조사 및 컨텍스트 보강	전사적 조율 및 대응	**SIEM** Security Ops 관리 경보 및 사고 관리, 정책 기반 규칙, 즉시 사용 가능한 보안 규칙 및 분석

미국 정부 내각급 부처

레거시 소프트웨어 유지보수 비용 900,000 달러 절감. 시민들은 정부 기관이 세금을 현명하게 지출하는 것은 물론, 효과적으로 서비스를 제공하기 위한 탄력적인 운영에 최선을 다하기를 기대합니다. 미국의 한 정부 부처는 정보 및 이벤트 관리 툴로서 HP ArcSight를 보유하고 있었는데, 해당 부처의 요건을 지원하지 못하고 고가에 속도도 느렸습니다. 이에 보안과 규제 준수를 위해 ArcSight를 Splunk Enterprise로 교체했으며, 해당 부처는 다음과 같은 이점을 거두었습니다.

- 소프트웨어 유지보수에 지출되는 연간 90만 달러 절감
- 보안 탐지, 대응 및 해결 역량 향상
- 보안 조사 시간을 몇 시간에서 몇 분으로 단축

사전 예방적 보안 접근 방식

Margulies와 그의 팀은 Splunk Enterprise를 사용하여 보안 문제를 조사하는 40명의 분석가를 보유한 이 부처의 SOC를 지원하고 있습니다. 또한 장애 해결 및 리포팅을 위해 Splunk Enterprise를 활용하는 전사 IT 팀도 지원하고 있습니다. 그 이외에도 부처의 보안 규정 준수를 관리하는 직원들도 지원하고 있습니다.

Heartland Automotive, Splunk 플랫폼으로 브랜드 평판 및 데이터 보호

오일 교환으로 잘 알려진 Heartland Automotive 서비스의 Jiffy Lube는 미국 내 최대 윤활유 소매 서비스 매장 프랜차이즈입니다. Heartland Automotive는 브랜드와 가장 중요한 리소스인 데이터를 보호하기 위해 사이버 보안 플랫폼이 필요했습니다. Splunk ES 와 Splunk UBA를 통합한 SIEM 플랫폼을 구축함으로써 Heartland Automotive는 다음과 같은 이점을 거두었습니다.

SIEM 및 내부자 위협 차단 솔루션 구현 3주 만에 가치 실현 성공

- 25% 적은 TCO로 새로운 플랫폼을 확보 혁신적 업무 주도
- 실시간 보안 조사 및 내부자 위협 차단 체계 확립

대규모 조직들이 많은 데이터 소스를 보유하고 있기 때문에 SIEM 구현이 종종 복잡하며 경보를 설정하는 데 몇 주가 필요할 수도 있습니다. Alams은 Splunk 프로페셔널 서비스 팀이 회사의 데이터 소스를 파악하고, SIEM 디자인을 상세하게 구현, 경보 설정 과정 등 전체 프로세스를 원활하게 구축했다고 밝혔습니다.

Heartland Automotive 서비스의 IT 및 정보 보안 총괄 임원인 Chidi Alams는 "신속한 가치 구현이 무엇보다 중요했습니다. 일반적으로 3개월이 걸렸던 SIEM 및 내부자 위협 탐지 솔루션을 3주 만에 구현할 수 있었습니다. CFO를 비롯한 임원진은 단 하루만에 솔루션의 가치를 볼 수 있었고, 그 다음 날 거의 구현이 완료되었다는 데 깊은 인상을 받았으며 빠른 시간 내에 구현을 완료할 수 있다는 확신을 갖게 됐습니다."라고 밝혔습니다. **자세한 내용.**

여기를 클릭해 Heartland Automotive가 Splunk를 이용하여 TCO는 25% 낮추고, 혁신적 업무를 실행하고 있는 방안을 확인해 보십시오.

Splunk ROI 개요

분석 기반 SIEM 솔루션은 막대한 투자를 요구한다는 비판을 받기도 합니다. 하지만, 현실은 비용이 보는 사람의 눈에 따라 달라진다는 것입니다.

만약 기업이 내부 공격자의 희생양이 된 후, 분석 기반 보안 솔루션은 얼마나 비싸게 생각될까요? 아니면, 언론의 1면을 장식하는 랜섬웨어 공격을 당한 후에는 어떨까요?

따라서, 내부자 및 외부의 악의적인 해커 모두로부터 기업을 사전 예방적으로 보호하고 침해 당하지 않는 데 따른 즉각적인 투자 수익(ROI)을 고려해야 하는 것입니다.

하지만, SIEM을 통한 투자 수익은 여기서 끝나지 않습니다.

분석 기반 SIEM 솔루션은 규제 준수, 사기, 도용 및 오용 탐지, IT 운영, 서비스 인텔리전스, 어플리케이션 딜리버리 및 비즈니스 분석 등 일반적인 IT 유즈 케이스를 지원합니다.

보안팀은 다른 IT팀과 함께 협력하고 있기 때문에 다른 유즈 케이스에 대한 가시성을 토대로 조직 전반에 대한 중앙 집중식 뷰를 확보하고 부서 간 협업을 활성화하며 보다 강력한 ROI를 달성할 수 있습니다.

분석 기반 SIEM 솔루션의 실제 ROI를 이해하는 최적의 방법은 이미 구축한 고객으로부터 직접 들어 보는 것입니다.

하나의 플랫폼에서 이뤄지는 SIEM, UBA 및 SOAR의 미래

본 구매자 가이드에서 강조한 것처럼 모든 SIEM이 다 동일한 것은 아닙니다. 분석 기반 SIEM 솔루션은 실시간 모니터링, 사고 대응, 사용자 모니터링, 고급 분석 등 강력한 기능을 통해 미래를 안전하게 보장할 수 있는 근간이 될 수 있습니다.
그리고 단일 플랫폼에서 분석 기반 SIEM과 UBA(고급 위협 탐지) 및 SOAR 기술을 결합한다면 조직을 보호할 수 있는 SOC의 능력은 한층 강화됩니다.

보안 위협은 계속해서 발전할 것이며 우리는 신속하게 대응할 준비가 되어 있어야 합니다. 데이터, 분석 및 운영 솔루션을 최적화하고 현대화하여 조직을 보호하고 사이버 방어 태세를 강화하십시오. 사이버 공격을 신속하게 억제하고 교정하기 위해서는 공통 작업 공간에서 전체 이벤트 수명 주기에 걸쳐 보안 이벤트를 관리할 수 있는 미래형 보안 운영 플랫폼이 필수적입니다.

Splunk의 분석 기반 SIEM 솔루션과 이 솔루션이 귀사의 보안 태세를 향상시킬 수 있는 방법에 대해 자세히 알고 싶습니까?
지금 Splunk 전문가와 만나 보십시오.