필수 가이드

보안 정보 및 이벤트 관리 (SIEM)

중요한 사항을 탐지하고, 포괄적 조사를 실행하며, 신속하게 대응할 수 있습니다.

splunk>

오늘날의 위협 환경은 보안팀에게 큰 과제를 안겨주었습니다. 다양한 보안 및 IT 소스에서 쏟아지는 방대한 양의 데이터 속에서 노이즈를 분석하고 하이브리드, 클라우드 및 온프레미스 환경 전반에 걸쳐 가시성을 확보하는 것은 굉장히 벅찬 일일 수 있습니다. 사소한 보안 문제를 처리하는 동시에, 주요 취약점을 확산되기 전에 우선순위 지정하는 것은 쉬운 일이 아닙니다. 대량의 원시 데이터를 바탕으로 실행 가능한 인사이트를 확보하는 것이 중요합니다.

이러한 컨텍스트의 결여는 위협 탐지를 더욱 어렵게 합니다. SANS Institute의 2023 SOC 조사에 따르면, SOC의 성공에 있어 가장 큰 걸림돌은 보안 이벤트와 관련된 컨텍스트가 현저히 부족하다는 점입니다. 분석가가 조치를 취해야 할 경보의 수가 많기 때문에, 컨텍스트 없이는 우선적으로 해결이 필요한 위협을 구분해 내는 것이 어려울 수 있습니다. 또한 분석가의 인력 부족 문제로 평균 41%의 경보가 무시되는 것으로 추정됩니다.

보안팀은 탐지, 조사 및 대응 전반에 걸쳐 업무를 수행하기 위해 25개 이상의 보안 도구를 관리해야 하는 부담까지 안고 있습니다. 그 결과 분석가들은 경보 조사에 평균 3시간을 소비하고 있습니다. 오늘날 우리가 직면한 위험은 지역에 따라 변화하는 규제를 준수하는 것뿐만 아니라, AI 기반의 정교해진 위협 캠페인을 탐지하는 것도 포함합니다.

이런 상황들 때문에 기업은 데이터에서 인사이트를 확보하고 이를 바탕으로 조치를 취하는데 어려움을 겪고 있습니다. 너무 많은 시간과 자원을 필요로 합니다. 이와 같은 어려움에 대한 해답은 보안 정보 및 이벤트 관리(SIEM) 솔루션에 있습니다. 머신러닝 기반 분석을 포함하는 SIEM 솔루션은 데이터 중심의 인사이트 확보, 위협 대응, 포괄적 리스크 완화를 가능하게 해줍니다.

본 필수 가이드에서는 SIEM 솔루션의 정의, 기능 및 여러분의 기업에 적합한 SIEM을 찾는 방법에 대해 소개하고자 합니다.

SIEM이란 무엇입니까?

SIEM 솔루션은 조종사의 레이더 시스템과 같습니다. 보안 분석가는 보안 운영 센터(SOC)를 운전하는 조종사로서 주변 상황, 전방 상황 및 사각지대에 놓인 곳까지 안전하게 탐색하기 위하여 레이더를 필요로 합니다. SIEM 솔루션은 SOC 분석가가 기업의 IT 전반을 파악하고 보호 중인 시스템 곳곳에 숨어있는 특정 보안 위협을 찾아낼 수 있도록 지원하는 보안 플랫폼입니다. 솔루션이 없다면 눈을 가린 채 비행하는 것과 같습니다.

보안 응용 프로그램, 네트워크 보안 및 시스템 소프트웨어를 통해 여러 종류의 공격 및 이상 행동을 포착하고 기록할 수는 있으나, 오늘날 가장 치명적인 위협은 분산되어 있기 때문에 이러한 도구만을 가지고는 포착할 수 없습니다. 해커는 여러 시스템을 일제히 공격하며 탐지를 피하기 위해 고도화된 회피 기법을 사용합니다. 또한 공격자는 전세계적인 전염병 사태로 원격 근무로 빠르게 전환하던 시절과 같이 문제가 발생하기 쉬운 상황을 악용하여 약점을 파고듭니다. 그 당시 SOC팀은 그간 의지해왔던 보안 도구와 프로세스를 대면으로 사용하지 않으면서도 시스템을 안전하게 유지해야만 했습니다.

바로 이러한 상황 때문에 최신식 SIEM 솔루션이 그 어느 때보다 필요합니다. 적절한 SIEM이 없다면 사이버 공격은 암세포처럼 자라나 유능한 SOC 분석가 조차도 예상치 못한 파국을 초래하는 인시던트로 이어질 수 있습니다. 그리고 랜섬웨어 공격과 같은 취약성을 발견할 때쯤이면 할 수 있는 조치는 피해를 최소화하는 것 뿐입니다.

SIEM의 기능은 무엇입니까?

Gartner의 정의에 따르면, SIEM은 '어플리케이션, 네트워크, 엔드포인트 및 클라우드 환경 전반에 배치된 모니터링, 평가, 탐지 및 대응 솔루션을 통해 생성되는 이벤트 데이터를 집계' 하는 솔루션입니다.

SIEM 솔루션은 SOC 분석가가 보다 스마트하게 일할 수 있도록 지원합니다. 이벤트 로그를 수집하고 데이터에 대한 단일 뷰를 제공함으로써 보안 태세에 대한 인사이트 및 가시성을 더 많이 확보할 수 있도록 기여합니다.

최신식 SIEM은 다음의 세 가지 주요 보안 문제를 해결할 수 있습니다.

- 데이터 노이즈 분석
- 컨텍스트를 추가한 위협 탐지 기능 부족
- 보안 및 위협의 복잡성

그렇다면 기업은 SIEM 솔루션 없이 어떻게 이러한 난제들을 해결할 수 있을까요? 그간 기업은 "전통적인" 솔루션, 다양한 포인트 솔루션, 또는 시간, 비용, 자원을 많이 필요로 하는 자체 솔루션을 사용해왔습니다.

기존 SIEM의 부족한 점

일반적으로 기존의 SIEM은 고정된 스키마를 기반으로 한 SQL 데이터베이스를 사용하는 구식의 아키텍처로 구성됩니다. 이러한 데이터베이스는 단일 장애 지점이 되거나 확장성 및 성능면에서 한계를 경험 할 수 있습니다.

통합된 가시성 부족

각종 소스에서 나오는 데이터를 원활하게 수집, 정규화 및 분석하는 기능이 없기 때문에 기존의 SIEM은 탐지, 조사 및 대응 시간에 있어 한계를 갖습니다. 더불어 데이터 수집은 매우 노동 집약적이거나 막대한 비용이 드는 일이 될 수 있습니다.

경보의 양을 줄이는 기능 부재

기존의 SIEM은 분석가가 처리하는 경보의 양을 줄이는 기능이 부재합니다. 실제로 기존 SIEM은 더 많은 경보와 오탐을 발생시키는 경우가 있으며, 이 때문에 업무량과 노이즈를 증가시켜 우선적으로 처리해야 하는 위협 식별을 더 어렵게 만듭니다.

즉시 사용 가능한 탐지 기능이 미비

보안 분석가는 보다 신속하게 위협을 탐지하고 해결할 수 있도록 SOC에 통합이 가능한 최상위 탐지 기능을 사용 할 수 있어야만 합니다.

제한적인 배포

기존의 SIEM은 온프레미스 또는 클라우드 배포로 제한되는 경우가 있습니다. 보안 실무자는 클라우드, 멀티 클라우드, 온프레미스 또는 하이브리드 환경을 유연하게 활용할 수 있어야 합니다.

워크플로우 간 통합 미비 또는 부재

분석가들은 보안 인시던트를 신속하게 처리해야 하지만, 탐지, 조사 및 대응 전반에 걸쳐 여러 가지 도구를 사용함에 따라 처리 속도가 느려지게 됩니다.

폐쇄적인 생태계

기존의 SIEM 솔루션은 대체로 다른 도구를 통합하는 능력이 부족합니다. 고객은 어쩔 수 없이 기존 SIEM에 포함된 기능을 사용하거나, 추가 비용을 지불하고 맞춤형 개발 및 전문 서비스를 이용해야 합니다.

SIEM의 5가지 필수 기능

1. 확장 가능한 실시간 보안 모니터링 및 분석 기능

SOC의 성공을 위해서는 원시 데이터를 실행 가능한 인사이트로 전환할 수 있는 플랫폼이 필요합니다. 기업의 모든 소스에서 데이터를 수집, 정규화 및 분석하는 능력을 갖추게 되면 분석가들은 가시성을 확보하여 위협이 기업에 막대한 피해를 입히기 전에 찾아낼 수 있습니다. 온프레미스, 클라우드 또는 하이브리드 중 어느 곳에 배포하든지 간에 SIEM은 보안 도구 전반에 걸쳐 지속적인 모니터링 및 상관 관계를 확장성 있게 제공해야 합니다.

2. 큐레이팅된 탐지 기능

널리 사용 중인 업계 프레임워크에 맞추어 즉시 사용 가능한 탐지 기능을 확보함으로써 분석가는 네트워크 내의 위협을 탐지하고 식별할 수 있습니다. 이를 통해 민감한 위협에 대처하는데 필요한 지원은 물론 다양한 전술, 기법 및 절차(TTP)를 관찰하여 컨텍스트를 정보를 제공합니다.

3. 경보 우선 순위 지정 기능

경보 분류에 있어 SOC 분석가가 가장 유용하게 사용하는 기능은 바로 경보 우선순위 지정입니다. 주의가 필요한 이벤트를 분석가가 신속하게 파악할 수 있도록 기여함으로써 지속되는 경보 과부하를 해결할 수 있습니다. 인시던트 심각도에 대한 컨텍스트를 통해 분석가는 오탐에 시간을 허비하는 대신 가장 문제가 되는 부분을 조사할 수 있습니다.

4. 시각화 및 대시보드 기능

전체 환경에 대한 가시성을 제공하는 직관적이고 시각적으로 강력한 대시보드를 통해 인시던트 조사 및 대응을 개선하여 기업의 보안 태세를 최신 상태로 유지할 수 있습니다. 보안 인시던트 및 심각도 수준에 대한 보다 포괄적인 가시성을 제공하여 생산성을 높이고 평균 대응 시간(MTTR)을 줄일 수 있습니다.

5. 위협 탐지, 조사 및 대응 통합 기능

탐지, 조사 및 대응 전반에 걸쳐 워크플로우를 조율함으로써 반복 가능한 자동 SOC 프로세스를 촉진하고, 방대한 양의 데이터, 경보의 수 및 수작업에 대처할 수 있습니다.

최신식 SIEM은 이벤트 검색, 모니터링 및 조사에 기여합니다. 정확한 위협 탐지 및 기업의 회복 탄력성 개선을 위해 전체 환경에 대한 가시성을 제공합니다. 보안팀은 다음과 같은 워크플로우를 통해 영향력이 강한 결과를 얻을 수 있습니다.

보안 모니터링

보안 태세에 대한 가시성을 실시간으로 확보하여 의사 결정을 향상시키고 리스크를 감소시킬 수 있습니다. 위협을 탐지, 조사 및 분석하여 보다 신속한 대응을 보장합니다.

인시던트 관리

빠르고 유연한 검색 및 보고 기능을 통해 근본 원인을 파악하고 인시던트의 증거를 쉽게 찾아낼 수 있습니다. 이를 통해 인시던트 식별, 탐지 그리고 사후 분석에 이르기까지 조사 전반에 걸쳐 분석가에게 지원을 제공합니다.

규정 준수

모든 IT/OT 리소스 및 보안 통제 전반에 대한 인사이트를 확보함으로써 의무 규정 또는 규제 프레임워크에 구애 받지 않고 최소한의 노력으로 정확한 규정 준수 및 감사 통과가 가능합니다. SOC는 모니터링, 검토 및 로그 보존 또는 감사 질문에 대한 임시 보고서 생성과 같은 기능을 사용하여 날이 갈수록 복잡해지는 규정 준수 요건 충족할 수 있습니다.

Splunk 시작하기

Splunk는 SIEM 및 보안 분석을 개선하는데 앞장서 왔습니다. 저희가 이뤄낸 혁신 덕분에 수천 명의 고객들은 경쟁자 보다 앞서는데 성공할 수 있었습니다. 업계를 선도하는 SIEM 및 보안 분석 솔루션 제공업체로서 Splunk 만이 여러 분석가로부터 업계 리더로서 인정받으며 **해트트릭(hat trick)**이라는 명성을 얻었습니다.

Splunk 엔터프라이즈 시큐리티(ES)는 전 세계 SOC가 신뢰할 만한 최적의 선택입니다. ES가 제공하는 강력한 기능을 바탕으로 포괄적인 가시성을 확보하고 컨텍스트를 통한 정확한 탐지를 실현하며 운영 효율성을 높일 수 있습니다. 확장 가능한 플랫폼 및 보조적 AI 기반 기능을 바탕으로 Splunk ES는 지속적인 보안 모니터링 및 비용 효율적인 데이터 최적화를 위한 대규모 분석을 보장합니다. 이러한 기반을 바탕으로 중요한 사항을 탐지하고, 포괄적 조사를 실행하며 신속하게 대응할 수 있습니다.

포괄적인 가시성 실현

보안팀은 하이브리드 클라우드 및 온프레미스 전반에 걸친 가시성을 확보하고 OT 환경과 IT 환경을 통합하는 가운데, 다양한 보안, IT 및 기타 비즈니스 소스로부터 쏟아지는 엄청난 양의 데이터 역시 처리해야 하는 등 힘든 상황에 놓여 있습니다. 모든 보안 문제를 찾아내는 것을 넘어 중대한 피해로 이어지기 전에 노출을 줄이고 위협을 완화하는 것을 우선과제로 삼아야 합니다. 이러한 디지털 소용돌이 속에서 보안팀은 소스에서 얻은 원시 데이터를 실행 가능한 가시성으로 전환하는데 필요한 단일 플랫폼을 가지고 있지 않습니다.

보조적 AI 기능을 갖춘 Splunk의 데이터 기반 플랫폼은 규모에 관계없이 모든 소스에서 데이터를 원활하게 수집, 정규화 및 분석하여 타의 추종을 불허하는 포괄적인 가시성을 제공합니다. 온프레미스, 클라우드 또는 하이브리드 등 배포에 관계없이 보안 도구 전반에 걸쳐 지속적인 모니터링 및 상관관계를 제공하여 공격 표면 커버리지를 극대화하는데 기여합니다. 포괄적인 검색으로 위협을 식별하고 Splunk AI 어시스턴트를 통해 검색을 SPL로 변환함으로써 시간을 절약할 수 있습니다. Splunk의 사용자 지정 경보 기능을 사용하면 신속한 조치를 간단하게 수행할 수 있습니다. 이러한 사용자 지정 경보는 다양한 조건을 기반으로 세분화 수준을 조정하여 설정할 수 있습니다. 여기에는 데이터 임계값, 트랜드에 기반한 조건, 그리고 무차별 대입(brute force) 공격과 부정 행위 시나리오와 같은 행동 패턴 인식을 포함합니다.

Splunk 엔터프라이즈 시큐리티는 보안 유즈 케이스에 결정적인 데이터만을 수집하여 비용 효율적인 데이터 최적화를 보장합니다. 사용자는 데이터 계층화를 기반으로 에지 등에서 유연하게 데이터를 저장하고 액세스할 수 있습니다. 이를 통해 포렌식 및 컴플라이언스 스토리지 비용을 줄여 추가적인 비용 절감 효과를 얻을 수 있습니다.

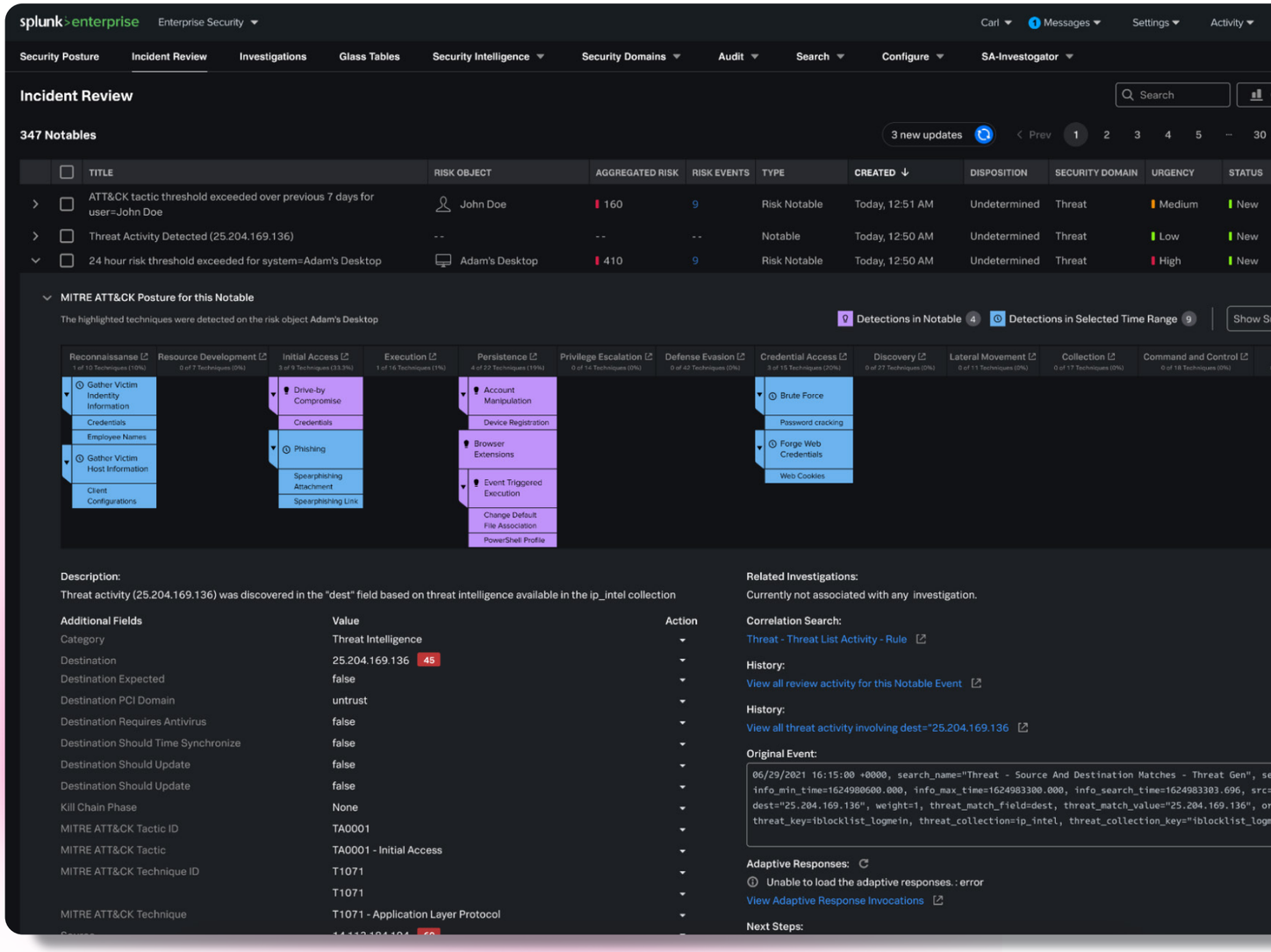
컨텍스트를 통한 정확한 탐지 가능

보안 책임자들은 컨텍스트의 결여로 막연하게 위협 탐지 활동을 할 수밖에 없는 상황에 어려움을 겪고 있습니다.

Splunk 엔터프라이즈 시큐리티의 위험 기반 경보(RBA)는 경보의 양을 90% 까지 대폭 감소시킬 수 있습니다. RBA는 Splunk 엔터프라이즈 시큐리티의 상관 관계 검색 프레임워크를 사용하여 여러 개의 리스크 이벤트를 단일 리스크 인덱스에 수집합니다. 리스크 인덱스에 수집된 이벤트들은 특정 기준을 충족해야 단일 리스크노터블(risk notable)을 생성하므로, 기존 SIEM 솔루션으로는 놓칠 수 있는 임박한 위협에 지속해서 집중할 수 있습니다. 이를 통해 생산성이 향상되고 탐지하는 위협의 정확도가 높아집니다.

Splunk 위협 연구팀(STRT)은 탐지 엔지니어링에 대한 심도 있는 연구를 바탕으로 1500개 이상의 즉시 사용 가능한 탐지 기능을 제공함으로써 위협을 신속하게 식별 및 해결하는데 기여합니다. 이러한 탐지 기능은 MITRE ATT&CK, NIST CSF 2.0 및 Cyber Kill Chain®과 같은 업계 프레임워크에 맞춰 구현되어있습니다. Splunk는 또한 머신러닝 툴킷(MLTK)을 제공하여 이상 징후 탐지를 통해 위협을 보다 원활하게 발견할 수 있도록 기여합니다.

Splunk 엔터프라이즈 시큐리티를 통해 사용자 지정 대시보드, 시각화 및 보고 기능을 활용해 보안 프로그램을 향상시킬 수 있습니다. 예를 들어 리스크 이벤트에서 관측된 전술 및 기법을 강조 표시해주는 시각화 매트릭스를 MITRE ATT&CK 프레임워크에 운용화함으로써 조사에 소요되는 시간을 절약할 수 있습니다. 또는 위협 토폴로지(Threat Topology) 시각화를 통해 인시던트의 범위를 정확하게 파악하고 대응할 수 있습니다. 향상된 리스크 분석 대시보드에서 보안 분석가는 RBA 및 행동 분석 전반에 걸친 탐지를 통해 사용자 엔티티 리스크 이벤트를 모니터링할 수 있습니다.



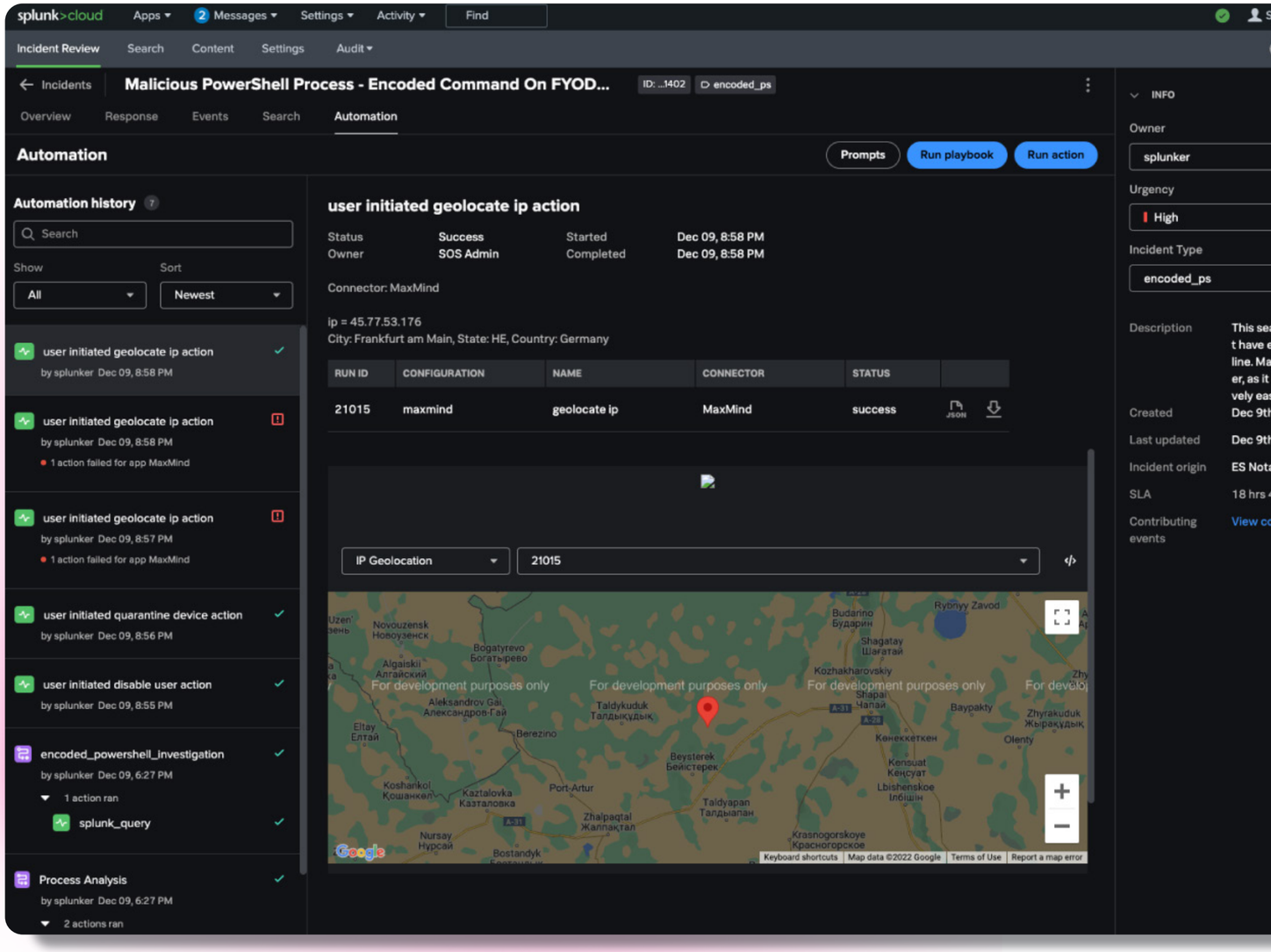
운영 효율성의 증대

방대한 양의 데이터와 경보, 수많은 도구 및 규정 준수 요건 속에서 보안팀은 AI 기반 위협 캠페인을 포함한 모든 종류의 리스크로부터 기업을 보호하는 동시에 수많은 문제를 해결해야 합니다.

미션 컨트롤(Mission Control)은 Splunk 엔터프라이즈 시큐리티의 필수 기능으로, 탐지, 조사 및 대응 전반에 걸쳐 워크플로우를 통합하는데 기여합니다. Splunk의 선도적인 SOAR 솔루션과 함께 자동화된 플레이북에 위협 인텔리전스를 탑재함으로써, SOC 프로세스를 간소화하고 수작업 및 서로 다른 도구 사이를 오가며 작업해야 하는 수고로움을 줄일 수 있습니다. 데이터 집계, 분석 및 자동화를 위한 통합 플랫폼을 통해 운영 효율성을 크게 향상시킬 수 있습니다.

또한 Splunk의 벤더 중립적 접근 방식은 이용자로 하여금 사용자 지정 앱을 구축하거나 2,200명 이상의 파트너 및 2,800개 이상의 앱으로 구성된 스플렁크베이스(Splunk)의 폭넓은 커뮤니티와 파트너 생태계를 통해 수많은 유즈 케이스를 해결할 수 있도록 기여합니다. 날이 갈수록 복잡해지는 규정 준수 요건을 준수하기 위해 데이터를 수집, 검색, 모니터링 및 분석할 수 있습니다. 또한 간소화된 로그 관리 및 PCI Compliance용 Splunk 앱과 같은 전문화된 기능을 활용하여 신속하게 작업을 수행할 수 있습니다.

위협 탐지, 조사 및 대응 통합을 통해 디지털 회복 탄력성을 강화하고 SOC를 향상시키십시오. 보안 운영 솔루션 업계의 선두주자로서 Splunk는 최신 SOC의 중추적인 역할을 하고 있으며, 효율적이고 효과적이며 확장성 있는 보안을 위해 폭넓은 기술, 커뮤니티 및 전문 지식을 제공합니다. Splunk와 함께 위협을 정확하게 탐지하고 보안 및 IT 컨텍스트를 통해 포괄적으로 조사하며 대응을 자동화하여 선제적으로 리스크를 처리하십시오.



시작하기.

업계를 정의하는 SIEM을 활용하여 SOC를 최신화하는 방법에 대해 자세히 알아볼 준비가 되셨습니까? 지금 Splunk 전문가와 상담하십시오.

splunk>

23-433250-Splunk-The Essential Guide to SIEM-EB-106