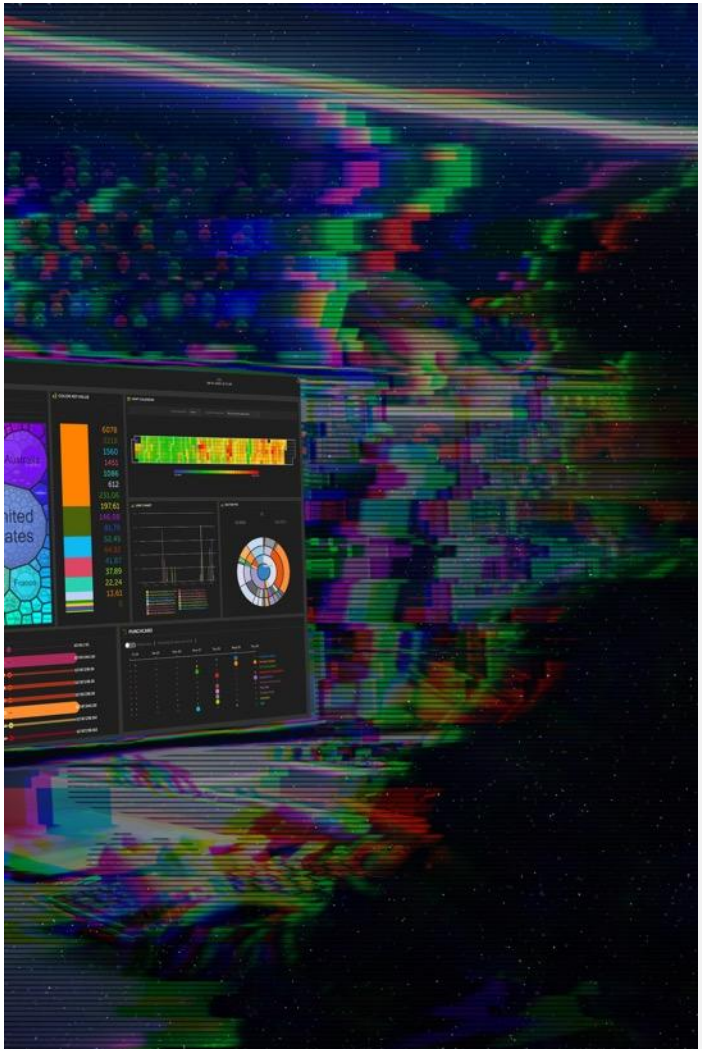


DEVO

PUTTING CLOUD-NATIVE LOGGING & ANALYTICS TO WORK FOR SECURITY

㈜한국밸런스

오늘날의 SOC에는 많은 도전 과제가 있습니다.

가시성 부족

격리된 위협 데이터 및
제한된 컨텍스트

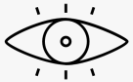
부정확한 경고

조사 지연

제한된 응답

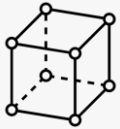
78% SOC 작업은 매우 힘들다고 합니다.

Devo는 위협을 방어하기 위한 결정적인 자신감을 제공합니다.



완전한 가시성

모든 규모의 모든 데이터:
400일간의 핫 데이터



위협 컨텍스트로 강화

내장된 위협 인텔 플랫폼
및 API 기반 통합

자동으로 위협 노출

엔터티 분석은 분석가를
안내하고 비정상적인
동작 강조 표시

간소화된 분석가 워크플로

자동화된 강화 기능은
분석가에게 정보를 제공:
단일 분류, 조사 및 헌트 UI

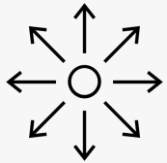
신속한 대응

단일 사고 대응 솔루션:
파트너와의 자동 응답

Devo 플랫폼 – 성공적인 SOC를 위한 기반

클라우드 네이티브 유연성

- 온프레미스 및 클라우드 소스 수집
- 멀티 클라우드 지원
- 세분화된 RBAC를 사용한 네이티브 멀티 테넌시

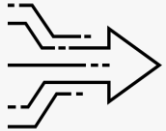


파격적인 가격, 속도 및 규모

- 단일 SaaS 라이선스
- 하루 수백 TB 데이터 규모
- 트레이드 오프 없는 낮은 TCO

데이터 손상 제로

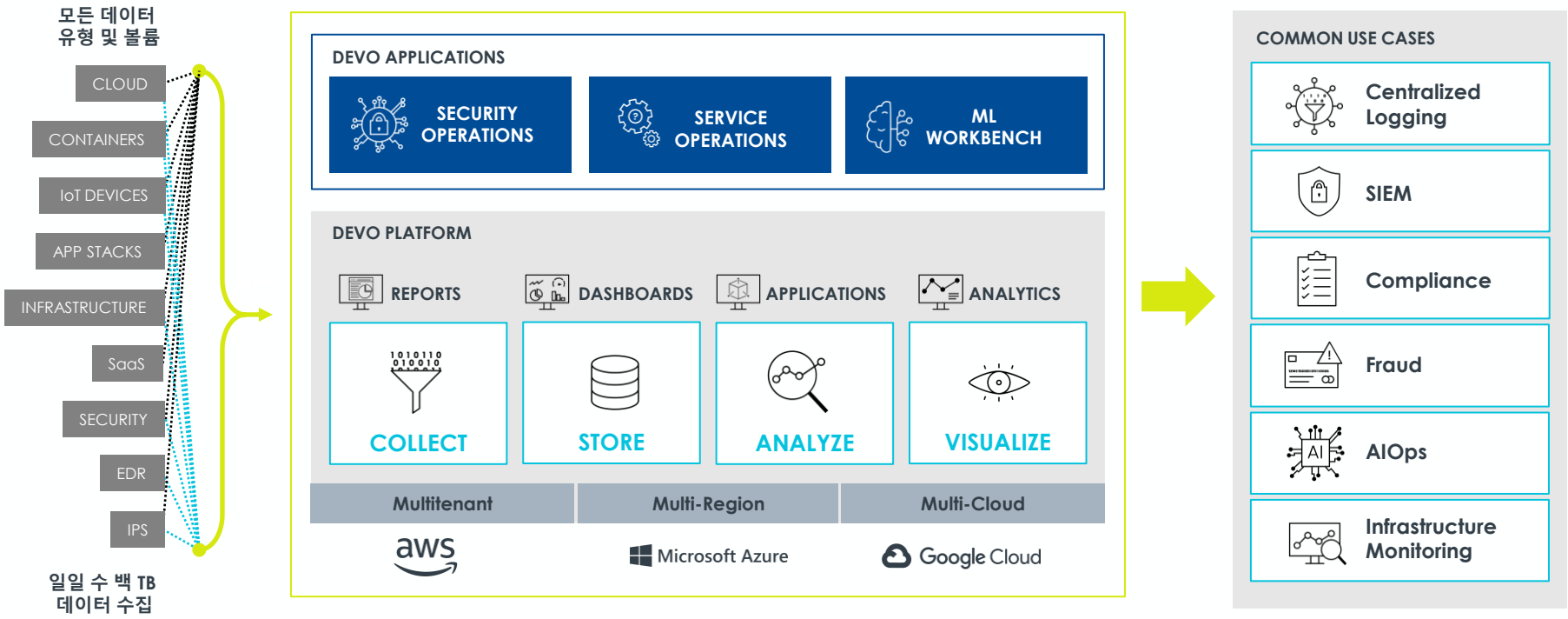
- 밀리 세컨드 레벨의 실시간 탐지
- 400일 간의 핫 데이터 보유
- 무제한 쿼리



다용도

- 다용도 사용을 위한 단일 데이터 세트
- 모든 사용자 사용 가능
- 현재의 에코 시스템에 통합

로깅 및 보안 분석을 위한 플랫폼



클라우드 전환 수행 및 데이터 제한 해결

다용도 사용

Devo 보안 운영

분석가가 중요한 사항에 집중할 수 있는 워크플로를 제공하여 SOC를 혁신합니다.

단일 솔루션에 완전한 가시성, 분석가 중심 워크플로 및 풍부한 조사를 결합한 최초의 클라우드 네이티브 차세대 SIEM입니다.

- 보안 분석
- 오케스트레이션 및 자동화
- 위협 인텔리전스
- Devo 콘텐츠 스트림
- 탐지 및 경고
- 엔터티 분석
- 조사 워크플로
- 포렌식 분석

Devo 콘텐츠 스트림

모든 기능을 포함한 간단한 라이선스

SaaS All-Inclusive License	
One license metric, data volume	✓
Unlimited queries	✓
400 days hot data	✓
Content Stream	✓
Security Operations application	✓
Service Operations application	✓
Data encryption at rest	✓
Unlimited user access	✓
24/7/365 customer support	✓
Fully managed by Devo	✓
Cloud usage costs included	✓

SOC 운영을 Devo로 전환한 대표적인 조직

News Corp

단일 멀티 테넌트 솔루션으로 지리적으로 분산된 사업부 전반에 걸쳐 가시성을 확보할 수 있는 글로벌 SOC를 구축하는 데 필요

paloalto NETWORKS

막대한 비용 증가 없이 많은 새로운 클라우드 데이터 소스를 신속하게 통합하는 데 필요합니다. SOC 자동화 및 분석가 상호 작용 감소

U.S. AIR FORCE

차세대 SIEM 솔루션을 핵심으로 하는 최신 사이버 무기 시스템을 구현하고 18분 49초 만에 위협에 대응하는 데 필요

rubrik

보안 팀이 쉽게 사용할 수 있도록 운영 환경과 분석에 대한 완전한 가시성이 필요했습니다.

News Corp

Customer Success

PROBLEM

News Corp은 전 세계 수백 개의 자회사의 다양한 인프라 문제에 직면해 있었습니다. 일부에는 자체 SOC가 있고 일부에는 SOC가 없습니다. 글로벌 CISO는 글로벌 SOC를 생성하여 사업부 전체에서 보안 및 규정 준수를 조정하는 동시에 사업부가 독립적으로 행동할 수 있도록 해야 했습니다. 이러한 문제는 GDPR과 함께 더욱 심각해졌습니다

SOLUTION

Devo는 News Corp의 글로벌 SIEM으로 Splunk를 대체했습니다. 각 사업부에는 자체 보안 운영에 대한 가시성과 제어 권한이 있는 동시에 News Corp에 단일 다중 테넌트 솔루션의 경제적, 보안 및 규정 준수 이점을 제공합니다.

"이제 모든 로그가 Devo를 사용하는 중앙 관리 도메인으로 이동하므로 경고를 한 번 만들고 모든 사업부에 적용할 수 있으므로 모든 사람이 혜택을 받을 수 있습니다. 정말 힘의 상승 효과입니다. 소규모 사업부에서는 더 큰 사업부에서 수행 중인 작업을 활용할 수 있습니다. 이제 Devo와 공유되는 공통 SaaS 로그가 있기 때문입니다."

paloalto NETWORKS

Customer success

PROBLEM

막대한 비용 증가 없이 하드웨어 판매에서 수많은 새로운 클라우드 데이터 소스를 신속하게 통합해야 하는 SaaS 소프트웨어로 비즈니스 전환. SOC 팀은 XSOAR을 계속 사용하여 SOC 자동화를 주도하고 분석가 상호 작용을 줄이기를 원했습니다.

SOLUTION

Devo는 기존 기술과 원활하게 통합되는 고성능 프로덕션 환경으로 기존의 데이터를 1/3의 비용으로 신속하게 마이그레이션했습니다.

"Devo는 우리의 SOC가 데이터를 분석하고 행동하는 방식을 변화시키는 데 있어 환상적인 파트너였습니다. 그들의 기술은 기존 제품보다 우수할 뿐만 아니라 접근하기 쉽고, 저렴하고, 확장 가능하며, 전례 없는 가치 실현 시간을 제공합니다."

U.S. AIR FORCE

Customer success

PROBLEM

제16공군 및 제33공군 사단의 주요 임무는 사이버 위협을 격리하고 치료하는 것입니다. 위협 행위자와 국가 체제 해커의 증가하는 정교함을 해결하기 위해 공군은 SOC가 18분 49초 이내에 위협에 대응할 수 있도록 해야 합니다. 또한 이 엄격한 MTTR 요구 사항은 매일 50TB 이상의 데이터를 수집하고 실시간으로 분석해야 하는 복잡한 운영 환경에서 충족되어야 합니다.

SOLUTION

Splunk, Elastic, Exabeam 등 여러 제품을 장기간 평가한 후 ArcSight에서 Devo로 글로벌 SIEM을 대체했습니다. Devo의 확장성, 워크플로 자동화, 데이터 강화 기능은 분석가가 분류 및 조사에 소요하는 20,000시간 이상을 줄이는 데 매우 중요하므로 공군이 위협을 신속하고 단호하게 감지하고 대응할 수 있습니다. Devo는 여러 가지에서 가시성, 탐지 및 대응을 위한 중앙 보안 허브 역할을 합니다

"Devo는 분류 및 조사 프로세스에서 분석가가 소비하는 시간을 20,000시간 이상 단축합니다."

rubrik

Customer Success

PROBLEM

클라우드에서 Rubrik의 SaaS 비즈니스 성장으로 인해 SOC를 유지하고 보안 태세를 강화해야 할 필요성이 생겼습니다. Rubrik의 CISO는 보안 로그 관리 솔루션이 필요했습니다. 운영 환경에 대한 완전한 가시성과 보안 팀이 보안 사용 사례를 쉽게 해결할 수 있도록 하는 분석이 핵심 동인이었습니다.

SOLUTION

Devo는 Rubrik의 멀티 클라우드 운영 환경(AWS, Azure, GCP)과 팀이 확인해야 하는 모든 추가 데이터를 제공했습니다. Rubrik은 IT 팀 및 ELK 스택과의 호환성을 유지하기 위해 Devo의 개방형 API를 많이 사용합니다.

"첫 번째 SOC를 구축하는 SaaS 회사로서 진정한 클라우드 네이티브이며 성장에 따라 쉽게 확장할 수 있는 솔루션을 찾는 것이 중요한 요구 사항이었습니다. Devo는 SOC 기술 스택을 구축하기 위한 분명한 전략적 선택이었습니다."

TOP 5 의류 소매점

Customer success

PROBLEM

Splunk Cloud 성능 및 확장성 문제는 특히 제품 출시 및 휴가 쇼핑 기간 동안 웹 스토어에 대한 실시간 통찰력을 얻을 수 있는 이 상위 5대 미국 소매업체의 능력에 영향을 미쳤습니다. 보안 팀은 데이터를 분석하는 대신 Splunk를 관리하는 데 허용할 수 없는 양의 시간을 소비하고 있었습니다.

SOLUTION

이 고객은 2018년에 Splunk를 Devo로 교체했습니다. 이제 트래픽 부하에 관계없이 전체 엔터프라이즈 및 웹 스토어에서 실시간 보안 탐지 및 대응 및 위협 헌트를 수행할 수 있습니다. Devo를 사용하면 신상품이 출시되는 동안 봇이 실시간으로 새 신발 인벤토리를 구매하는 것을 감지하고 중지할 수 있습니다.

"Splunk는 쿼리 수를 줄이고 스토리지를 줄이고 더 많은 비용을 지불할 것을 요청했습니다. 나는 그 반대를 원했습니다. 사고 대응 담당자나 분석가가 쿼리를 실행하는 데 드는 비용에 대해 걱정하는 것을 원하지 않습니다. 원하는 만큼 쿼리를 실행할 수 있어야 합니다."

TOP 5 의류 소매점

사용 사례: 클라우드 기반의 보안 분석 | 환경: **300** 사용자 | **140** 데이터 소스

SPLUNK를 사용한 때

- 불완전한 쿼리 결과
- 엄청난 라이선스 비용으로 인해 모든 데이터를 수집할 수 없음
- 라이선스 갱신 필요 보유 기간을 400일에서 90일로 줄이고 장기 약정
- 시간 및 분 단위로 측정된 경고 시간
- 필요한 동시 사용자 수를 지원할 수 없음

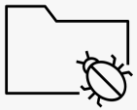
DEVO를 사용한 후

- 완전한 쿼리 충실도 달성
- 이제는 모든 데이터 수집
- 100+TB/일 수집 가능
- 쿼리 시간 최대 98% 감소
- 필요한 자원의 96% 감소
- 밀리 세컨드 단위로 측정된 경고 시간
- 모든 사용자 쿼리 실행 가능

Devo 사용 후 숫자로 나타난 결과

4.5PB 모든 핫 데이터	**3.5X** 데이터 증가	**64TB** 블랙 프라이데이에 성능 저하 없음
580 실시간 집계 작업	**50X** 쿼리 성능 향상	**18.5M** 조회 행
48TB 일일 수집, 6TB에서 증가	**80** 기계 학습 파이프라인	**3X** 출시 이후 활성 사용자

일반적인 SOC 도전 영역



더 적은 데이터 수집 및 공격 표면 노출

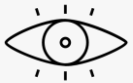
조각화된 데이터 저장소에 더 많은 데이터 덤프 조각화 가시성 추가

대규모 컨텍스트 없이 블라인드 작업으로 전체 위협 사례 놓침

데이터 및 컨텍스트에 대한 느린 액세스로 인한 분석가의 불만 및 비효율 증가

문제에 더 많은 도구와 인력을 투입

오늘은 어느 수준에 있습니까?



완전한 가시성

보안 도구를 통합하고
볼륨이나 소스에
관계없이 모든 데이터를
단일 클라우드 네이티브
솔루션으로 가져옵니다.

상황별 인사이트

위협 탐지, IP 보호,
사용자 및 엔터티의 행동
이해, 위협 인텔리전스
통합, 위협을 위험에 매핑

자동화 및 효율성

적을 찾고, 사전 예방적이며,
보안 도구를 통합하고,
자동화 및 조사 워크플로를
사용하여 팀의 역량을
강화하는 데 집중하십시오.

생산성 향상

분석가의 직무 만족도를 크게
향상시키면서 가장 중요하고
흥미로운 비즈니스 위험을
파악합니다.

[Thank You]

DEVO

More data. More clarity. More confidence.

Contact :
㈜한국밸런스
김 형덕 영업대표
Mobile : 010-7138-8889
Email : hdkim@valence.co.kr