솔루션 참고 사항

SOC 인사이트

AI 기반 분석을 적용하여 방대한 양의 이벤트, 네트워크, 에코시스템, DNS 인텔리전스 데이터를 실행 가능한 인사이트로 전환하여 SecOps 효율성을 높입니다.

SECOPS 효율성에 대한 장벽

오늘날 비즈니스 또는 정부 조직의 다른 기능과 마찬가지로 현대의 SOC는 사용 가능한 리소스로 더 많은 작업을 수행하는 데 어려움을 겪고 있습니다. SANS 2023 SOC Survey[1]에 따르면 SOC 기능을 최대한 활용하는 데 방해가 되는 10대 SOC 장벽 중 80%가 다음 세 가지 영역에 속합니다.

- 경고 이해 및 처리
- 도구 간 제한된 통합 또는 자동화
- 사용 가능한 직원과 기술로 주요 작업 수행

그러나 가장 비극적인 통계는 이러한 모든 장벽이 10년 넘게 SOC에 어려움이 되어 왔다는 점일 것입니다. 멀웨어 순위 및 기타 기본 필터를 기반으로 인시던트의 우선순위를 자동으로 지정하는 점진적인 개선책만으로는 SOC 분석가의 주의가 필요할 수 있는 경고 및 기타 이벤트의 증가를 따라잡을 수 없었습니다. 그래서 상황은 더 나빠졌습니다.

AI 기반 SOC INSIGHT

현대의 지속적인 공격 위협은 단일 공격에 관련된 수많은 침투 시험, 익스플로잇 공격, 암호화 및 기타 툴을 호스팅하고 배포하기 위해 유연한 공격자 인프라와 동적 C2 시스템에 의존합니다. 따라서 DNS에 대한 의존도가 매우 높으며 방어자가 이러한 위협을 탐지하고 방해하기 위해 악용할 수 있는 주요 취약점을 강조합니다.

DNS는 프로토콜, 플랫폼, OS, 애플리케이션 또는 위치에 관계없이 합법적인 활동과 악의적인 활동을 감지합니다. 이러한 고유한 가시성을 바탕으로, NSA의 사이버 보안 국장 산하 파일럿 프로그램에 따르면 DNS 보안을 통해 맬웨어 공격을 92%줄일 수 있다는 것으로 나타났습니다[2]!

사실 및 수치

- SOC 분석가의 60%가 **업무량이 증가하고 있고**, 65%는 **내년에 직장을 옮길 것 같다고** 답했습니다[4].
- 설문 조사 응답자의 55%가 **매주, 심지어 매일** 중요한 경고를 놓치는 경우가 많다고 답했습니다[5].
- 분석가의 64%는 **수동 작업에 업무 시간의 절반 이상이 소모된다고 말합니다**[6].
- 잘못된 구성은 **오류 관련 침해의 3대 요인 중 하나입니다**[3].
- 완전한 SOC 활용을 방해하는 **10대 장벽 중 8개는** 경고, 도구 통합 및 기술 부족과 관련이 있습니다.[1]
- CEO의 77%가 **핵심 기술의 가용성에 대해 걱정합니다**[7].
- **멀웨어 및 C2 활동의 92%는** 올바른 DNS 인텔리전스 및 가시성을 통해 DNS 계층에서 제어할 수 있습니다[2].

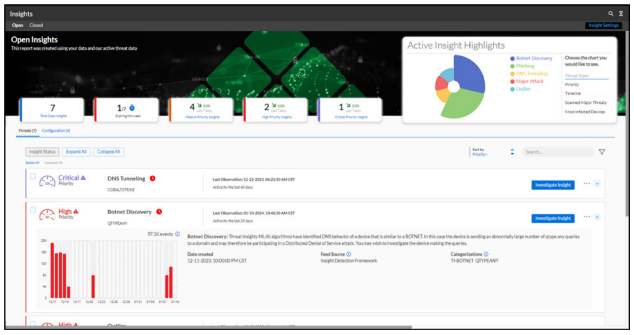

그림 *1: SOC Insight Summary* 페이지에서는 분석가에게 가장 중요한 정보에 원클릭으로 액세스할 수 있는 기능을 제공합니다.

SOC Insight는 Infoblox의 DNS(Domain Name System) 탐지 및 대응(DNSDR) 솔루션인 BloxOne Threat Defense와 함께 작동하여 다른 툴이 놓치는 알려지지 않은 위협 활동을 탐지하고 SOC 효율성을 높이며 현재 보안 투자의 전반적인 ROI를 개선하는 고유한 AI 기반 분석을 제공합니다.

다양한 인사이트를 통해 여러 문제 해결

인시던트 또는 침해 발생 후 조사 결과를 보면 잘못된 구성, 보안 도구 통합 문제 또는 단순한 경고 과부하로 인해 악의적인 활동의 초기 지표를 놓친 경우가 많습니다. SOC Insight는 방대한 양의 데이터에 AI 기반 분석을 적용하여 이러한 위험을 해결할 수 있도록 합니다.

보안 인사이트

SOC Insight용 보안 애드온은 BloxOne Threat Defense '비즈니스 클라우드' 또는 '고급'에서 사용할 수 있으며, AI를 사용하여 방대한 양의 이벤트, 네트워크, 에코시스템, DNS 가시성 및 인텔리전스를 관리 가능한 보안 인사이트 집합으로 추출합니다.

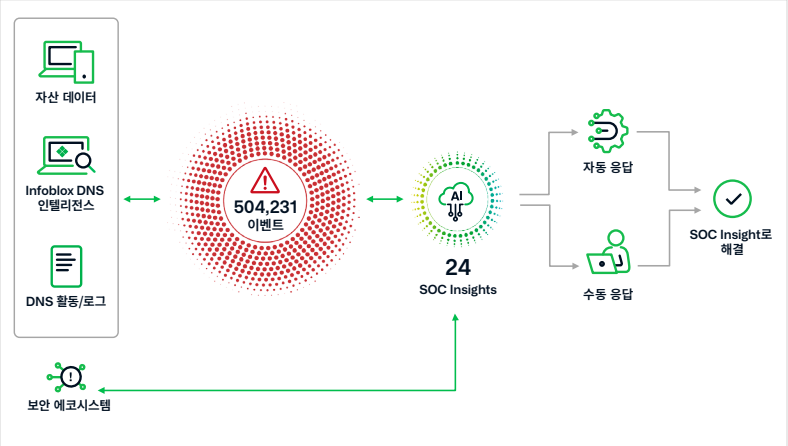

그림 2: *SOC Insight*를 사용하면 알림 과부하를 제거하여 산더미 같은 이벤트를 더욱 관리하기 쉬운 의미 있고 실행 가능한 인사이트 집합으로 추출할 수 있습니다.

- Zero Day DNS™
- 지속적인 위협
- 활성 위협 확산
- 주요 공격
- 봇넷 탐지
- 이상치 커뮤니케이션
- 피싱
- 멀웨어
- 오픈 DNS 리졸버
- DNS 터널링
- 데이터 손실 활동
- 표적 공격
- 과도한 DNS 오류
- 유사 도메인 모니터링

구성 인사이트

SOC Insight의 구성 기능은 사용자가 최신 모범 사례를 최대한 활용하고 일반적인 실수를 방지할 수 있도록 BloxOne Threat Defense '비즈니스 클라우드' 및 '고급'에 포함되어 있습니다. 동영상 및 기타 가이드를 따라 실수나 취약점을 해결하거나 허용된 예외에 대한 불필요한 경고를 비활성화하세요.

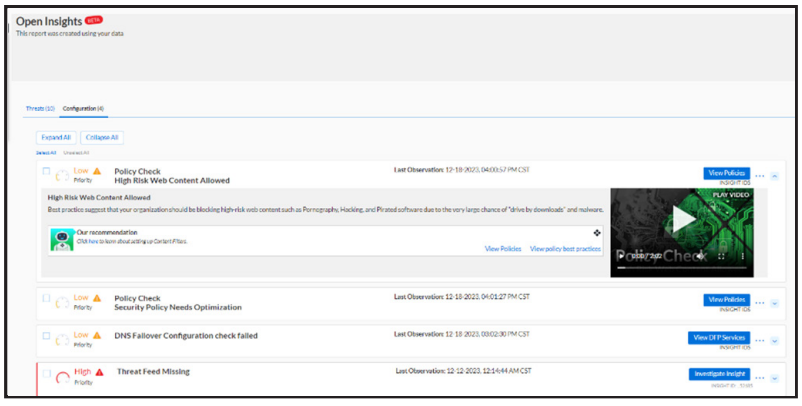

그림 3: 취약하거나 위험한 구성 오류를 사전에 식별하여 최적의 방어, 조사 및 대응 기능을 보장합니다.

- DNS 위협 피드 누락
- VirusTotal 무료 키 누락
- 보안 정책 최적화 필요
- DNS 장애 조치 확인 실패
- 피드 액션 불일치
- DFP 자산 세부 정보 숨기기
- 로깅 모드의 보안 정책
- 웹 콘텐츠 파일러 끄기
- 고위험 웹 콘텐츠 허용

재무, 운영 및 비즈니스에 긍정적인 영향

대부분의 보안 도구가 '사용 편의성'과 '침해 감소'를 약속하는 데 그치는 반면, SOC Insight는 분석가의 스트레스와 이직률을 줄이는 것부터 확장, M&A 및 기타 비즈니스 이니셔티브로 인한 많은 보안 문제를 줄이는 것까지 훨씬 더 많은 일을 해낼 수 있습니다. 예를 들어, 다음과 같은 일을 해냅니다.

- DNS의 특성상 새로운 위치나 비즈니스 파트너를 몇 달이 아닌 몇 분 만에 공통 DNS 인프라로 쉽게 통합할 수 있습니다.
- 구성 인사이트는 오류 관련 침해의 3대 요인 중 하나인 '잘못된 구성'으로 인한 침해 또는 데이터 손실을 완화할 수 있도록 하는 매우 사전 예방적인 기능입니다[3].
- '멀웨어', '피싱', '봇넷' 및 기타 '주요' 또는 '확산' 활동의 자기상관은 대응자가 한 번에 많은 위협을 해결할 수 있도록 지원하여 효율성을 높입니다.
- '이상치', 'DNS 터널링' 및 '오픈 리졸버'와 같은 인사이트 범주를 모니터링하는 기능과 BloxOne Threat Defense의 고유한 유사 기능 및 애플리케이션 가시성 기능을 통해 보다 사전 예방적 보안 태세로 전환하세요.
- 보안 에코시스템의 인텔리전스 통합은 단순한 원시 로그와 이벤트가 아닌 실행 가능한 '인사이트'를 제공하여 전체 보안 스택의 ROI를 개선합니다.
- SOC Insight는 관련 데이터를 자동으로 수집하고 분석가가 해당 데이터를 보고 피벗하여 더 빠르고 자신 있게 결론에 도달할 수 있도록 합니다. 이는 스트레스를 낮추고 숙련되고 경험이 풍부한 보안 전문가의 유지율을 높이도록 합니다.

놀라운 결과

고객들은 BloxOne Threat Defense와 함께 SOC Insight를 사용하여 다음과 같은 상당한 이점을 얻었다고 말합니다.

- EDR 및 FW 경고 50% 감소
- 월 평균 500시간의 SOC 분석가 시간 절약
- 연간 40만 달러의 생산성 절감 실현

인사이트를 통해 SIEM, SOAR 및 생태계의 기타 부분들을 향상

SecOps는 보안 에코시스템에서 원시 데이터 공유의 가치와 한계를 잘 알고 있습니다. 이로 인해 SIEM 및 SOAR 전문 지식은 대부분의 조직에서 가장 어려운 기술 중 하나가 되었습니다. SOC Insight는 이러한 다른 도구의 부담을 덜어주고 보안 스택 전체에서 결과 인사이트를 공유하여 다른 도구를 더 효과적으로 만들어 전체 SecOps 효율성을 더욱 향상할 수 있습니다.

1 'SANS 2023 SOC Survey', 2023년 6월, Chris Crowley, Barbara Filkins, John Pescatore 저

2 'NSA launches pilot program to secure defense contractors', 2020년 6월 18일, Lauren C. Williams 저, NEXTGOV/FCW

3 'Verizon 2023 DBIR Report'

4 Voice of the SOC Analyst

5 The Orca Security 2022 Cloud Security Alert Fatigue Report

6 Voice of the SOC Analyst

7 https://www.pwc.com/m1/en/publications/five-challenges-cloud-adoption-how-overcome-them.html

infoblox.

Infoblox는 네트워킹과 보안을 통합하여 비교할 수 없는 성능과 보호를 제공합니다. 포춘지 선정 100대 기업과 신생 혁신 기업에서 신뢰를 받으며, 사용자의 디바이스에 대한 실시간 가시성과 제어 기능을 제공하여 조직 내부에서 발생하는 위협을 조기에 차단할 수 있습니다.

본사
2390 Mission College Blvd, Ste.501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

버전: 20240411v2