INNOBIZ
기술혁신형중소기업

1등급

Ientelligence SIEM & SOAR

인공지능 위협식별 및 자동대응체계 구축

QTIE

QUARRY THREAT INTELLIGENCE ECO SYSTEM

QUARRY SYSTEMS

“인공지능 위협식별 및 자동대응체계 구축을 위한 QTIE”

통합 로그 관리 및 인공지능 위협 자동대응 시스템

Quarry Threat Intelligence Eco-system

핵심 기능

▪ 로그 저장

폭주하는 다양한 장비의 로그를 수집하고 저장하며, 이기종 보안장비 로그들을 QTIE에서 한 번에 검색이 가능하며, 빠른 검색 속도 등 강력한 로그관리 기능을 제공 합니다.

▪ 위협 분석

수집된 로그를 기반으로 빠르고 정확한 다중 상관분석 및 정책을 제공하여 날로 늘어가는 보안위협에 대하여 정확하고 신속하게 위협대응을 할 수 있도록 제공 합니다. 또한 제조사 권장 탐지, 차단 정책을 제공하여 전문적인 위협판단 시스템을 제공합니다. ※ 관련 특허 4종을 보유

▪ 자동 대응

Playbook 제공을 통해 인간의 사고처럼 다중 상관 분석하고 탐지된 이벤트를 ‘자동 차단’, ‘반 자동 차단’ 기능을 통해 대응할 수 있습니다. 이러한 자동 대응 시스템은 수동 및 반복적인 업무를 자동화하여, 보안 관제팀에게 일상적인 업무보다 선제적 위협 대응을 위한 전략적인 업무에 좀 더 집중할 수 있는 능률적인 환경을 제공합니다.

▪ N-Probe

패킷 미러링을 통해 패킷기반의 네트워크 트래픽 분석을 수행합니다. 수집된 패킷내에 웹, DNS, DB통신 등 알려진 어플리케이션 프로토콜에 대한 L7레벨의 네트워크 포렌직 작업을 수행하며 이를 통해 내 외부 통신에 대한 가시성을 제공하고 실시간 통계분석과 웹에 대한 어뷰징 및 계정도용 시도 등 기존 보안장비에서 탐지 하기 어려운 위협 탐지를 수행할 수 있도록 QTIE(매니저)와 연동 구성됩니다.

보안 운영의 문제점

- 로그저장기간 6M → 1Y 변경
- 로그 저장 스토리지 부족
- 보안경고증가
- 느린 보안사고 대응
- 복잡한 보안 장비
- 많은 비용

특장점

인공지능형 위협 식별 및 자동 대응

- 보안담당자의 숙련도에 따른 보안관제 퀄리티 편차 걱정 제로
- 24 x 365 대응체계 구축
- 별도의 관제 인력 없이 자동화된 관제 및 관리체계 구축
- 특허 받은 지능형 위협 식별 및 자동대응 체계

인메모리 기반 상관분석 정책제공

- 빅데이터 기반 위협대응 Intelligence 제공
- 지능형 자동화 대응

강력한 로그관리 기능 및 로그 저장

- 전사로그 통합관리
- 벤더별 프리셋 제공

검증된 구축 사례 다량 보유

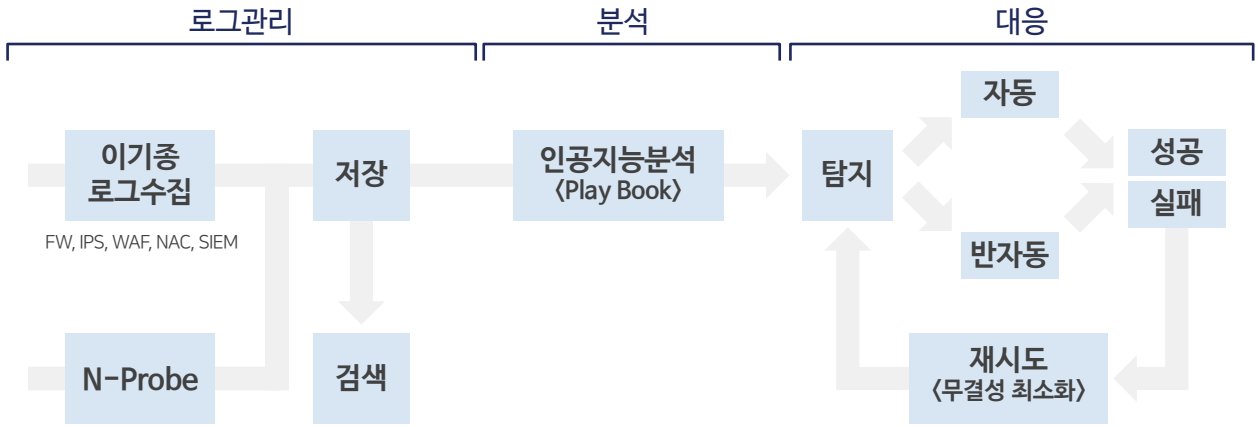
- 2014년 국내 최초 구축, 국산 FW, WAF, NAC 장비 연동 사례 보유
- API 미지원 장비 연동지원

보안관제업무 기대효과

- 사이버 위협 가시성 개선
- 대량 공격에도 자동·반자동 차단 기능으로 대응시간 단축
- TCO 절감
- 로그관리 관련 무제한 라이선스 제공

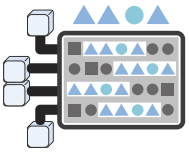
기술 개요

QTIE는 보안담당자가 이기종 보안장비의 보안로그를 수집하여 관리, 분석 및 대응하는 보안 관제 업무 프로세스를 기반으로 제작되어 업무 처리에 있어 신속하고 단순한 패턴으로 업무 효율을 증가 시킬 수 있습니다.



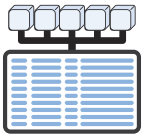
주요 기능

9가지의 주요 기능들로 QTIE는 이기종 보안 장비와의 소통이 원활합니다.



수집 및 분석

빠른 시간내에 대용량 로그를 수집하고, 수집된 로그를 검색하고 확인 할 수 있는 검색 기능 제공



로그관리 및 저장

데이터에 숨겨진 패턴을 찾고 비 정상적인 상태를 찾는 분석 기능을 제공

연계방법 API

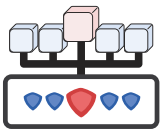
이기종 솔루션 및 고객환경에 원활하게 통합될 수 있는 개방형 API 지원

워크플로우

자동화 및 수동 워크플로우를 통해 대응 프로세스 단계를 체계화

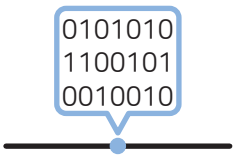
컨텍스트

네트워크, 보안, 사용자 정보를 포함한 전체 상황 정보가 통합되어 빠른 의사결정 가능



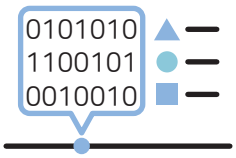
정책관리

연동된 보안장비 정책 및 상태관리



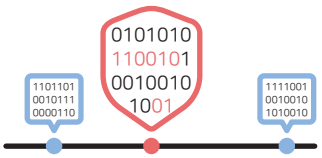
패킷기반 네트워크 분석

패킷 미러링을 통해 패킷 기반의 네트워크 트래픽 분석



네트워크 가시성

L7레벨의 네트워크 포렌식 작업을 통해 네트워크 가시성 확보



네트워크 기반 보안탐지

실시간 통계분석 및 웹 어뷰징 등 기존 보안장비에서 탐지하기 어려운 위협탐지

USE CASES

LMS 이기종 보안 장비 로그 수집, 저장, 검색

SIEM 빅 데이터 기반 보안 로그 상관 분석

SOAR 자동, 반자동 지능형 대응 시스템

N-Probe 패킷 기반 L7통신 수집 분석

대용량 로그 관리 및 실시간 통계 분석

보안 장비 로그 및 Agentless기반 웹 로그, 서버 로그 수집 검색, QPL 통한 실시간 통계 분석 기능 지원

이기종 보안 통합 SIEM

지능형 이기종 보안 로그 수집 및 상관분석

지능형 자동 위협 탐지 및 대응

지능형 이기종 보안 로그 수집 및 분석 자동 반자동 대응

패킷 기반 L7 통신 수집 분석

패킷 미러링을 통해 L7레벨의 네트워크 포렌식 작업을 수행

시스템 구성도

관련 특허 및 인증

CC 인증 | GS 인증 1등급 | 기술혁신형 중소기업 확인서 | 악성 행위 탐지 방법 및 시스템 | 부정 예매 차단 방법 및 장치 | 계정 도용 탐지 방법 및 장치 | 이기종 보안 장비와 연동하는 보안위협 자동 차단 시스템

※ 조달 등록 정보

조달청 디지털서비스몰 — 전체(규격, 업체명) ▼ QTIE

QUARRY SYSTEMS

쿼리시스템즈는 정보보호 솔루션을 중심으로 2007년부터 사이버 침해사고 대응, 관제시스템 구축, 보안 및 네트워크 분석 등의 역량을 보유한 정보보안 위협관리 전문기업입니다.

Addr. 서울특별시 송파구 백제고분로 7길 8-12, 3층 (잠실동, 승현빌딩) Tel. 02-421-8858 FAX. 02-421-8852
www.quarry.kr