QTIE

지능형 위협 탐지 및 자동대응 체계 구축을 위한
통합 XDR 솔루션

QUARRY SYSTEMS

조달청 디지털 서비스몰 바로가기

QTIE
QUARRY THREAT INTELLIGENCE ECO SYSTEM

QTIE(큐티)는 지능형 위협 탐지 및 자동 대응 체계 구축을 위해 개발된 국내 최초의 SIEM, SOAR, NDR, TIP, AI 통합 XDR 솔루션 입니다.

차별화된 다중 상관분석 기능과 인공지능 기반 위협 분석 엔진, 패킷 기반 위협 탐지 엔진 (Threat Detector), KISA C-TAS, FCTI, Emerging Threat 등 국내・외 주요 TI 정보를 연동 연계하는 TI 관리 기능을 통해 위협을 보다 정밀하고 정확하게 분석하여 MTTD (위협 탐지 평균 시간)과 MTTR (위협 대응 평균 시간)을 최소화합니다.

QTIE는 국내 주요 대학, 기업, 공공에 이어 Mission Critical 한 서비스를 제공하는 금융기관에 대한 지능형 위협 자동 대응 체계 구축 사례를 보유하고 있으며, 위협을 정밀하고 정확하게 탐지할 수 있는 500여종의 제조사 권장 PLAYBOOK 제공과 지속적인 무상 업데이트 지원을 통해 1년 365일 최신화된 보안 대응 체계 구축 및 관리를 위한 기반을 제공합니다.

주요기능

Security Orchestration & 위협대응

- 3rd Party 보안 솔루션과 연동 (API / CLI)
- 보안 솔루션과 연동 분석 (VirusTotal, APT 등)
- 보안 솔루션과 연동, 위협 자동 차단 / 해제
- 관리자 수동, 승인 기반 위협 차단

Network Detection & Response

- 10만 개 이상 Signature
- 100만 개 이상 TI(Threat Intelligence) 정보
- HTTP, DNS, DB 등 주요 애플리케이션에 대한 로깅
- 파일 추출 및 통신 Packet 저장 기능

위협대응
SOAR

위협탐지
NDR

SIEM/SOAR/NDR 통합
보안 위협, 탐지 대응 자동화 XDR 솔루션

통합로그관리
LMS

위협분석
SIEM+TI+AI

통합로그 관리기능

- Agent/Agentless 기반 서버 로그(+명령어) 수집 기능
- Big Data 기반 검색 엔진 (Cluster 지원)
- QPL*을 이용한 유연한 검색과 통계 분석 기능
- 초당 1,000억 건 이상 이벤트 검색 성능

위협 탐지 및 분석 기능

- 다중 상관분석 엔진
- 3rd Party 보안 솔루션 연동 연계 기반 분석
- AI 기반 Anomaly Detection 엔진
- TI 연동, 연계

*QPL : QTIE Pipeline Language

특장점

QTIE는 국내 유일 SIEM, SOAR, NDR 통합 차세대 XDR솔루션으로 세계 최고 수준의 분석 처리 성능을 지원하며 다수 공공, 금융, 기업 고객사에서의 성공적 과업 수행을 통해 기능과 안정성이 검증된 솔루션 입니다.

CC, GS 인증 받은 솔루션

QTIE(큐티)는 CC 인증과 GS 인증을 획득한 솔루션 입니다.
보다 정밀하고 정확한 위협 탐지 분석 체계를 구축하기 위해서는 로그 및 패킷 기반의 분석과 3rd Party 보안 솔루션 및 TI 정보 연동이 필수적이며 QTIE는 로그 기반 및 패킷 기반 분석, AI 및 TI 기반 분석 기능을 제공합니다.

다수 공공, 금융, 기업사이트에서 자동대응 체계 구축

QTIE는 국내 다수의 공공, 금융, 기업, 대학 사이트에서 무인 자동 대응 체계를 구축한 실적을 보유하고 있으며, False Positive로 인한 서비스 장애 없이 99.99999999% 이상의 가용성을 보장하기 위해, 위협을 정확하게 분석하기 위한 특허 받은 관제 정책을 보유하고 있습니다.

다중 상관분석 기술

QTIE는 특허받은 기술을 활용하여 다중 상관 분석과 연계 분석을 수행할 수 있으며 이를 통해 위협을 정밀하고 정확하게 분석합니다.

AI 기반 위협 탐지

QTIE는 세계적인 Big Tech 회사인 Amazon의 OpenSearch에 적용된 AI 기반 Anomaly Detector가 내장되어 있으며 이를 활용하여 비정상 통신과 행위를 탐지하는 기능을 제공합니다.

국내 • 외 IOC정보 통합, TI 플랫폼

KISA C-TAS, 금융보안 연구원 FCTI, ABUSE.CH, EmergingThreat, Cisco, Kaspersky 등 다양한 보안 기관, 회사들의 IOC (Indicator of Compromise) 정보들을 통합 수집하여 자체 분석에 활용하거나 3rd Party 보안 솔루션으로 정보 연동 기능을 제공합니다.

주요 구축 사례

QTIE는 위협을 정밀하고 정확하게 분석할 수 있는 특허 기술이 적용된 다중 상관 분석 엔진과 NDR, TI, AI를 이용한 복합 분석 기술을 통해 위협을 정확하게 식별하여 차단할 수 있으며 공공, 금융, 기업, 대학 등 다수의 기업과 기관에 자동 대응 체계 구축 사례를 보유하고 있습니다. 위협 자동 대응 구축 체계를 통해 보안 위협을 적극적으로 대응하고, IT 보안 운영 관리 효율성을 향상할 수 있습니다.

공공기관

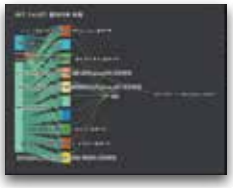
A기관의 보안센터에는 280여개의 기업 홈페이지를 보호하기 위한 DDoS 대응 시스템과 QTIE가 설치되어 있습니다. QTIE는 DDoS 탐지 차단 솔루션에서 탐지하기 어려운 Web Abusing이나 Web Macro 공격 등에 대한 위협을 탐지하며 일 평균 2,600건 이상의 자동 대응 (DDoS 장비로 악성 IP 차단 명령)을 수행하고 있습니다.

#DDoS 공격 대응 체계 강화 #20% 이상 차단 비율 향상 #100배 이상 빠른 검색 및 통계 분석

금융기관

상위기관 관제에 이어, 상주 관제 서비스를 받고 있으나 관제 대응체계 고도화를 위해 QTIE를 도입하여 PLAYBOOK 기반 자동화 관제와 관제 인력 중심의 분석 관제 서비스를 융합하여 일 대응, 분석 건수를 극대화하고 있습니다.

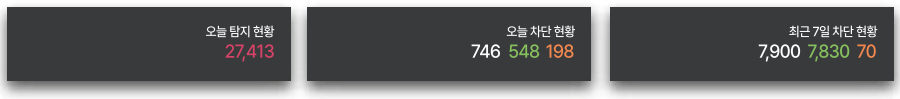
#자체 보안관제 대응 건수 향상 #분석관제 자동화 #보안 정책 고도화 여력 확보



교육기관

자체 관제 인력 없이 운영하면서 발생하는 많은 보안 위협을 보안 담당자가 전부 대응해야 했으나 QTIE를 이용한 위협 자동 대응체계 구축을 통해 기존에 미처 대응하지 못했던 다수의 위협들을 보다 적극적으로 차단 대응할 수 있게 되었으며 보안 운영 편의성이 대폭 향상되었습니다.

#자체 관제 없이 #일 평균 8,000건 위협 자동 차단 #기존 솔루션이 탐지하지 못했던 위협 탐지, 차단



민수기업

내 · 외부 위협 탐지 대응 자동화를 위해 SIEM, SOAR, TIP, AI 기능을 모두 활용하여 시스템을 구축하였으며 외부의 위협에 대해서는 방화벽과 IPS, 내부 호스트 보안을 위해 EDR과 연동 연계 구성을 하여 월 평균 3만 여건의 외부 위협을 자동 차단하고 있습니다.

#내 · 외부 위협 탐지 자동화 #월 평균 3만여건 위협 자동차단 #자료유출 탐지 #운영 인력 최소화

당신의 정보보안 전문 파트너

QUARRY SYSTEMS

Contact us

주식회사 쿼리시스템즈

Address. 서울특별시 송파구 백제고분로 7길 8-12, 3층 (잠실동, 승현빌딩)

Tel. 02-421-8858 **Email.** sales@quarry.kr

Fax. 02-421-8852 **Web.** www.quarry.kr

조달청 디지털서비스몰 전체 (규격, 업체명) ▼ QTIE