사이버 위협 인텔리전스 솔루션

quaxar

quaxar

외부 위협 대응을 위한 CTI 솔루션

Quaxar는 내부 보안 시스템으로 탐지가 어려운 외부 위협을 모니터링하고 관리해 조직의 사이버 보안을 강화하는 CTI 솔루션입니다. 딥,다크웹을 비롯한 다양한 채널에서 방대한 양의 데이터를 수집하고, 수집한 데이터를 정제, 연결해 위협 인텔리전스(TI)를 도출합니다. 추출된 TI를 활용해 다양한 외부 위협을 선제적으로 예방하고, 예상치 못한 사이버 공격이나 탐지된 잠재적 위협에 신속하게 대응할 수 있는 실행 가능한 인텔리전스를 제공합니다.

Quaxar 핵심 서비스

디지털 리스크 프로텍션 (DRP)

기업의 브랜드 가치를 보호하고 고객 신뢰도를 향상시킵니다.

- 브랜드 어뷰징 사이트 탐지
- 피싱 사이트 탐지
- 비정상 모바일 앱 탐지
- 어뷰징 사이트/앱 테이크 다운 서비스

능동적 위협 및 취약성 관리

다양한 외부 위협 관련 유의미한 인텔리전스를 신속하게 제공합니다.

- 표면 공격 모니터링 (ASM)
- 랜섬웨어 활동 모니터링
- 최신 취약점 및 IoC 정보 제공
- 위협 행위자 프로파일링

데이터 침해 탐지

딥/다크웹 및 기타 채널에서 기업 핵심 자산 유출을 감지합니다.

- 개인 정보 유출 탐지
- 기업 정보 유출 탐지
- 금융 정보 유출 탐지

추가 서비스

신속한 보고서

고객 요청시 특정 주제에 대한 분석 보고서를 신속하게 제공합니다.

예) 악성코드, 위협 그룹, 암호화폐 등

사고 대응

침해사고의 경우 전문가가 사고 조사를 지원합니다.

테이크다운 서비스

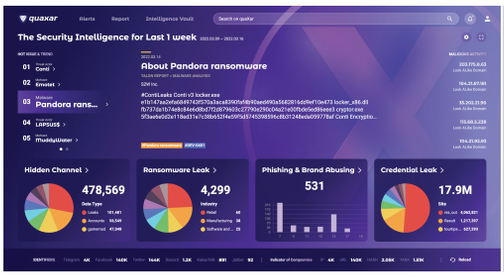
브랜드를 오용하는 악의적 콘텐츠 및 웹 사이트를 제거 및 문제 해결을 수행합니다.

S2W

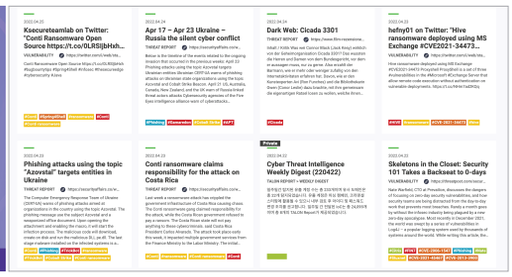
Quaxar 주요 기능

대시보드

- 사이버 보안 관련 핫 이슈 및 동향
- 위협 인텔리전스 현황
- 최신 사이버 위협 관련 콘텐츠



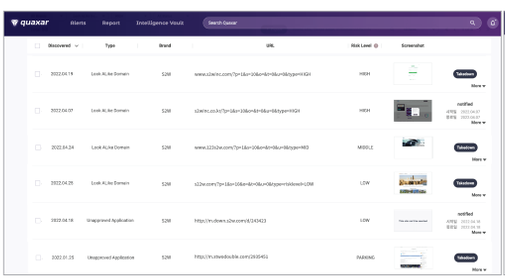
▲ 메인 대시보드



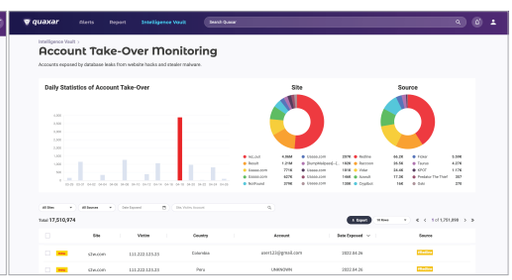
▲ 최신 사이버 위협 관련 콘텐츠

디지털 리스크 프로텍션

- 브랜드 어뷰징 사이트/앱 모니터링
- 계정 탈취 모니터링
- 랜섬웨어 활동 모니터링



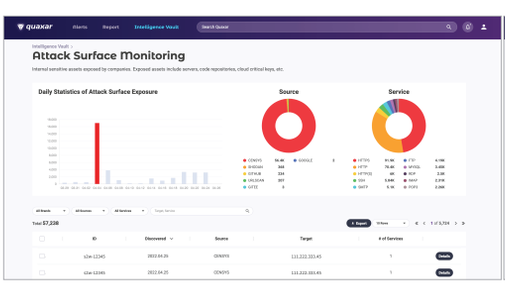
▲ 브랜드 어뷰징 사이트/앱 모니터링



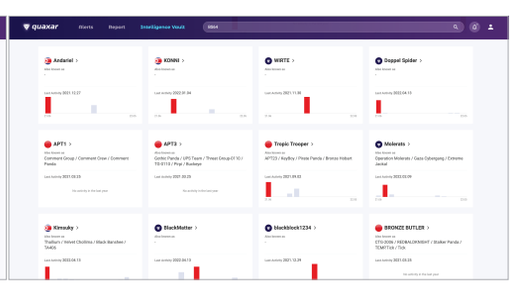
▲ 계정 탈취 모니터링

위협 인텔리전스

- 공격 표면 모니터링 (ASM)
- IoC(침해지표) 네비게이터
- 탐지룰 정보
- 위협 행위자 프로파일링



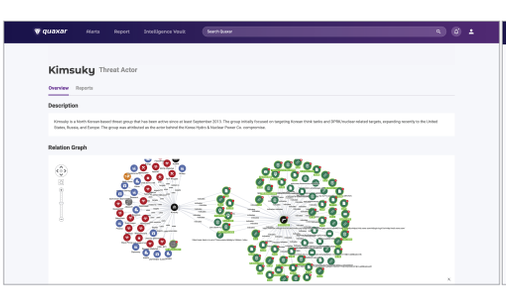
▲ 표면 공격 모니터링 (ASM)



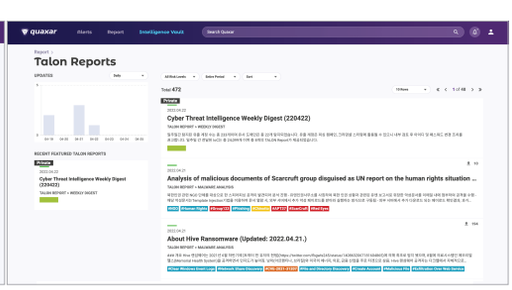
▲ 위협 행위자 프로파일링

보고서

- Talon 보고서
- 보안 뉴스
- 취약점
- OSINT IoC



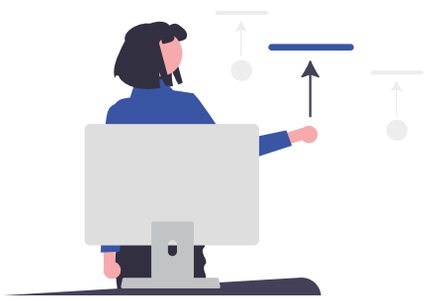
▲ 인텔리전스 관계 그래프



▲ Talon 분석 보고서

S2W

고객사 후기



글로벌 오토모티브 기업 | 매니저

Quaxar를 사용하면서 가장 좋은 점 중 하나는 S2W가 위협 행위자의 정보를 선제적으로 제공한다는 것이었어요. LAPSUS$ 사건에서도 S2W 덕분에 사전에 공격을 준비하고 예방할 수 있었어요. S2W는 LAPSUS$가 우리를 공격하려고 시도하기 훨씬 전에 LAPSUS$의 공격 기법에 대해 알려주었어요.

S2W의 정보가 없었다면, 우리는 큰 보안 사고를 겪을 수도 있었어요. 이번 사건을 통해 선제적 외부 위협 방어가 얼마나 중요한지 깨닫게 되었습니다.

글로벌 이커머스 기업 | 선임 매니저

국내 주요 대기업들은 해외를 근거지로 둔 국가지원 해킹그룹에 지속적으로 노출되고 있다고 들었어요.

Quaxar는 특정 위협 그룹이 만든 악성코드가 퍼지고 있음을 가장 먼저 감지해서 알려주었어요. 국내 대기업의 기밀 정보를 노리는 것으로 유명한 그룹인 만큼 신속한 대응이 필요했어요. S2W는 주요 위협 그룹과 악성 코드에 대한 풍부한 IoC를 보유하고 있어서 신규 위협을 빠르게 탐지해주었어요. 그 덕분에 악성코드 유포 사실을 인지한 당일에 근거지를 파악하고 차단해 위협에 대응할 수 있었네요.

이커머스
C 기업

" 아직 활성화되지 않은 피싱 사이트에 대한 도메인 정보를 받고 있습니다. "

처음 받아보는 정보들을 제공해주고 있는데요, 그것들이 보안사고 예방에 큰 도움을 줍니다.

텔레콤
S 기업

" 내부 주요 자산과 개인 정보 유출 탐지율과 정확도와 탐지율이 굉장히 높아요. "

S2W의 정확한 유출 원인 분석 덕분에 위협 대응이 한결 수월해졌어요.

오토모티브
H 기업

" S2W는 최신 위협 그룹 및 공격 지표에 대한 정보를 누구보다 먼저 파악해서 알려줘요. "

신속한 정보 전달 덕분에 위협에 대비하고 사고를 예방할 수 있었어요.

S2W

S2W는 사이버 위협, 브랜드/디지털 어뷰징 및 가상 자산을 위한 인텔리전스 솔루션을 제공합니다.

데이터 중심의 초연결 사회에서 최적의 문제 해결 방법을 도출하고, 외부 위협으로부터 조직을 보호하고 기업 브랜드 가치 향상을 위한 맞춤형 솔루션을 제안합니다.

S2W는 빅 데이터 분석, 머신 러닝, 딥 러닝 등 다양한 기술을 활용해 위협 인텔리전스, 디지털 어뷰징 인텔리전스, 가상 자산 인텔리전스 솔루션을 제공합니다.

발표

Cybercriminal Minds
An investigative study of cryptocurrency abuses in the Dark Web (NDSS 2019)

Doppelgangers on the Dark Web
A large-scale Assessment on phishing Hidden Web Services (WWW 2019)

OPERATION NEWTON
HI KIMSUKY? DID AN APPLE(SEED) REALLY FALL ON NEWTON'S HEAD? (Virus Bulletin 2021)

Shedding New Light on the Language of the Dark Web
(NAACL 2022)

특허권

암호화폐 거래 분석 방법 및 시스템

지식 그래프를 활용한 사이버 보안 제공 방법과 장치 그리고 프로그램

암호화폐 거래 분석 방법과 장치

다중 도메인에서 데이터를 수집하는 방법과 장치

S2W

info@s2w.inc | +82 70 5066 5277 | www.s2w.inc

quaxar

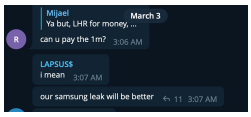
활용 사례

Quaxar는 내부 보안 시스템으로 탐지하기 어려운 외부 위협을 모니터링하고 관리해 조직의 자산과 가치를 보호하는 CTI 솔루션입니다. S2W의 많은 고객들은 Quaxar를 통해 사이버 보안을 강화하고 있습니다.

사이버 공격 그룹의 움직임을 사전에 감지하여 피해를 방지한 사례

글로벌 오토모티브 기업 H사

2022.03.03
LAPSUS$ 채널에서 S사 데이터 도난에 대한 언급 포착



2022.03.05
LAPSUS$ 채널에 업로드 된 S사 유출 데이터 토렌트 파일을 탐지

2022.03.06
고객들에게 LAPSUS$의 침투 방법에 대한 정보 제공

2022.03.08
고객들에게 LAPSUS$에 대한 상세 보고서를 제공

2022.03.09
고객에게 최신 주요 IoC를 제공

2022.03.15
LAPSUS$가 L사로부터 훔친 데이터를 언급

2022.03.22
텔레그램에 다음과 같이 게시

1. L사의 유출 데이터
2. 마이크로소프트의 유출 데이터

2022.03.23
텔레그램에 해킹 사고 관련 옥타의 공식 진술에 대한 반박 글을 게시

국내 S사 LAPSUS$ 데이터 유출 사건 발생 당시 S2W의 대응

Challenge

LAPSUS$는 세계의 많은 주요 기업들과 조직들을 타겟하는 사이버 위협 그룹입니다. 그들은 단기간에 마이크로소프트, 엔비디아, 삼성 등 대형 기술 기업의 정보를 탈취하고 피해를 입힌 랜섬웨어 그룹으로 악명 높았습니다. 처음 그들이 활동을 시작했을 때는 그들에 대해 알려진 정보가 거의 없어 공격 수법을 분석하고 대책을 세우는 것이 어려웠습니다. 이로 인해 공격에 대한 대응이 늦어졌고, 그들은 기회를 놓치지 않고 빠른 속도로 공격을 이어갔습니다.

이 사건의 가장 큰 어려움은 정보의 부재였습니다. 피해 확산을 인지하고 추가 사고를 예방하기 위해서는 신속한 사고 대응에 필요한 정확한 정보 확보와 의미 있는 인텔리전스 도출이 중요했습니다.

Action

S2W는 LAPSUS$의 비공개 채팅 채널에서 주요 글로벌 기업 데이터 유출 정황을 처음 포착했습니다. 곧이어 Quaxar 실시간 모니터링 시스템을 통해 유명 다크웹 포럼에 해당 기업의 데이터가 담긴 파일이 첨부된 게시물을 탐지했습니다. S2W는 적발 즉시 정보 유출 사고 경위와 판매자에 대한 조사에 착수했습니다.

S2W는 Quaxar를 통해 딥/다크 웹을 포함한 다양한 채널에서 LAPSUS$의 흔적을 추적하고 가능한 많은 데이터를 수집해 분석했습니다. 이 과정에서 그들이 기업 서버 침투에 사용한 초기 계정 정보를 입수했습니다. 이 정보는 사건 분석과 사고 확산 방지에 중요한 역할을 했습니다.

S2W의 전문 분석가들은 자체적으로 분석한 내용을 토대로 LAPSUS$ 침투 기술에 대한 분석 보고서를 작성하고 추후 발생 가능한 잠재 공격에 대한 대응책을 세웠습니다. S2W는 선제적 대응에 필요한 보고서와 공격 대비에 즉시 적용 가능한 핵심 인텔리전스인 IoC를 고객들에게 신속하게 제공했습니다.

Results

S2W 고객들은 제공된 인텔리전스를 사용해 LAPSUS$ 공격을 막을 수 있었습니다. 실제로 한 고객사는 S2W가 제공한 IoC를 내부 보안 시스템에 적용한 후 LAPSUS$의 침투 시도를 포착했습니다. 신속한 사전 대응으로 사이버 공격으로부터 기업 자산과 브랜드 가치를 보호할 수 있었습니다.

이와 같이 Quaxar는 특정 상황에서 필요한 핵심 정보를 신속하게 파악하여 제공합니다. Quaxar에서 제공하는 독점적인 인텔리전스를 갖춘 선제적 대응으로, S2W의 고객들은 잠재적인 위협을 방지하고 기업 자산을 보호할 수 있었습니다.

S2W

피싱/어뷰징 사이트 탐지 및 테이크다운 서비스를 통한 브랜드 보호

글로벌 이커머스 기업 C사

Challenge

디지털 쇼핑 플랫폼과 이용자가 늘면서 이들을 겨냥한 사이버 범죄도 같이 증가했습니다. 이 케이스의 고객은 그러한 위협으로 고통받고 있었습니다. 사기범들에 의해 브랜드 사칭 웹사이트와 앱은 지속적으로 생성되었고, 그 수와 속도는 내부 담당자가 처리할 수 있는 한계를 넘어선 상황이었습니다.

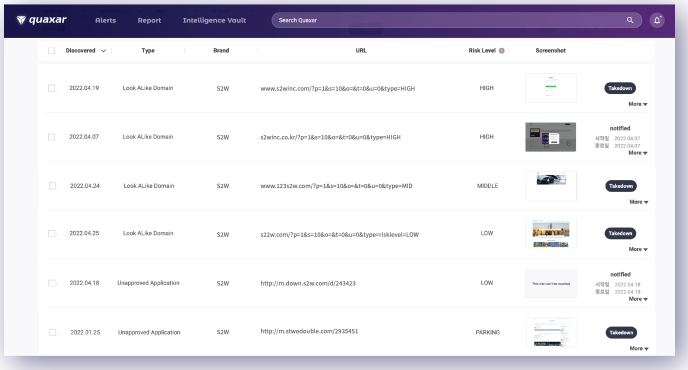
사칭 사이트와 앱으로 연결되는 접속 경로가 다양하고 숨겨져 있는 경우가 많아 내부 보안시스템으로는 감당하기 어려운 부분도 있었습니다. 상황이 지속됨에 따라 고객사는 재정적인 피해뿐만 아니라 브랜드 가치의 하락을 겪게되었습니다. 그들은 피해 확산을 막기 위해 외부 위협 대응과 브랜드 가치 보호 솔루션을 찾고있었습니다.

Action

S2W는 Quaxar의 브랜드 어뷰징 모니터링 서비스를 제공해 고객사 브랜드 사칭 웹 사이트와 앱 등의 어뷰징 정보를 비롯해 관련 위협 정보를 확인할 수 있게 도와주었습니다. Quaxar는 그들에게 활성화 상태의 피싱 사이트부터 아직 비활성화 상태인 look-a-like 도메인까지 다양하고 많은 브랜드 어뷰징 관련 정보를 제공했습니다.

또한 국가, 위협 행위자 정보 등 세부적인 인텔리전스를 이용해 위협 상태를 모니터링할 수 있도록 했습니다. 이처럼 Quaxar는 숨겨진 정보를 제공함으로써 잠재 위협 방지에 도움을 주었습니다. 한가지 예로, Quaxar는 고객이 한 번도 진출한 적 없는 외국 불법 앱스토어에서 고객을 사칭한 피싱앱을 적발했습니다. Quaxar는 이와 같은 위협 정황 포착시 담당자에게 이메일을 통해 즉시 알림을 보냈습니다.

또한 고객 요청 시 테이크다운 서비스를 제공합니다. 테이크다운 서비스는 S2W의 전문 위협 인텔리전스 분석팀이 위협 요소를 제거해주거나 또는 유사한 수준의 해결 방법을 고안해 처리해주는 서비스로, 고객의 브랜드 가치 및 지적 재산 보호를 위한 서비스입니다.



Results

Quaxar의 브랜드 보호 서비스를 통해 고객사는 브랜드 어뷰징 위협 및 관련 사이버 범죄를 효과적으로 관리할 수 있게되었습니다. 브랜드 어뷰징으로 인한 사기 범죄가 줄어들면서 고객들의 금전적 피해 사례도 감소했습니다. 또한, 그들은 고객들의 신뢰와 브랜드 평판을 되찾았습니다.

그들은 특히 Quaxar가 제공하는 독보적인 인텔리전스에 높은 만족도를 표했습니다. 특히 그들이 전에 사용했던 다른 CTI 솔루션이나 서비스로부터 얻을 수 없었던 종류의 데이터를 많이 얻게되었습니다. Quaxar의 잠재 위협 정보와 같은 데이터가가 그 예인데, 그것들이 사고 예방에 효과적인 역할을 하고있다 전했습니다. 또한 즉각적인 테이크다운 서비스를 통해 사이버 보안 관리 효율성을 향상시킬 수 있게되었습니다.

신속한 취약점 정보 공유를 통한 피해 방지

전 고객

Challenge

Log4J 취약성은 세계적으로 화제가 되었던 제로데이 취약점이었습니다. Log4J는 대부분의 Java 기반 프로젝트에서 사용되는 오픈 소스 자바 로깅 라이브러리로 알려져있습니다. 그렇기에 Log4J의 취약점 발견은 전 세계의 많은 소프트웨어에 영향을 주는 심각한 문제로 떠올랐습니다.

Log4J 취약점은 공격자가 특정 메시지 명령을 입력만으로 대상 컴퓨터의 전체 데이터를 해킹하거나 삭제할 수 있고 악성 프로그램까지 삽입할 수 있을 정도로 치명적인 취약점이었습니다.

발견된 적이 없는 취약점이기 때문에 그에 대한 정보나 관련 공격에 대한 대책도 없었습니다. 그리고 그것은 Log4J를 사용하는 모든 소프트웨어가 잠재적인 사이버 위협에 노출된 상태이고, 언제든 사이버 공격의 대상이 될 수 있다는 것을 의미했습니다.

Action

Quaxar는 광범위한 채널 모니터링을 통해 각종 취약점에 대한 정보를 지속적으로 수집하고 식별합니다. 수집한 정보에서 자사 고객사들과 관련된 취약점을 분류합니다. 그리고 고객사들이 사용중인 소프트웨어 목록을 기준으로 취약점의 관련도와 위험도를 판단합니다.

S2W는 Log4J 취약점을 인지한 시점부터 관련 정보를 수집하고 분석해 2차 공격에 대한 대응책을 마련해 고객사들에게 제공했습니다. 그 결과, Log4J가 보안 문제로 큰 화제가 되기 전에 그에 대한 대응 방법을 고안하고 고객사들을 잠재 위협으로부터 보호할 수 있었습니다.

S2W는 자체 탐지 기술을 이용해 log4shell의 실제 공격 코드를 획득했고, 사전 대응의 일환으로 고객사들에게 해당 코드를 탐지할 수 있는 스노트 룰을 제공했습니다.

Results

Quaxar는 Log4J의 취약성을 사태 초기에 인지했는데, 이는 대부분의 기업에 매우 영향력 있는 프로그램이었기 때문에 매우 이른 단계에서 고객사들에 알릴 수 있었습니다.

S2W의 취약점 연구진은 외부에서는 찾을 수 없는 취약점 POC 코드를 생성해 고객사들에게 제공하는데, 이는 특정 취약점이 내부 자산에 얼마나 큰 영향을 미치는지 훨씬 쉽게 분석할 수 있게 합니다.

S2W에서 제공하는 신속한 대응 가이드와 인텔리전스를 통해 고객사들은 중요한 취약점을 인식하고 대비할 수 있었습니다. 결과적으로 S2W의 고객사들 중 그 누구도 Log4J 취약성으로 인해 공격받거나 피해를 입지 않았습니다.

S2W

www.s2w.inc | info@s2w.inc | +82 70 5066 5277
경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층