TI Use Case

S2W

Active Threat and Vulnerability Management

Attack Surface Monitoring*

고객사 비공개 자산의 외부 노출을 탐지하여 즉시 대응한 사례

기업의 비공개 자산 정보의
외부 노출을 탐지

내부 테스트 서버의 취약점으로
인해 외부에 노출됨을 발견

신속하게 고객사 알림 후
긴급 대응 완료

Challenge

기업의 정보는 여러 경로를 통해 외부로 노출될 수 있습니다. 협력사의 실수, 임직원 개인 계정 유출 등의 이유로 기업 자산 정보가 노출될 경우 내부 보안 시스템에서의 탐지가 어렵습니다.

만약 노출된 정보가 기업의 비공개 정보, 주요 자산 정보 등를 포함하고 있다면 사이버 위협의 타겟이 될 수 있습니다. 이는 기업의 막대한 재정적 피해나 브랜드 이미지 하락으로 이어질 수 있기 때문에 적시에 문제를 파악하고 신속하게 해결하는 것이 중요합니다.

Action

이 케이스는 Quaxar가 고객사의 기업 자산 정보가 외부로 노출된 정황을 탐지한 사례입니다. 정보 노출 경로 추적을 통해 기업 내부에서만 접속되어야 할 테스트 서버가 외부에서 IP 형태로 접근 가능함을 파악했습니다. S2W는 이 사실을 즉시 고객사에 알리고 문제의 테스트 서버를 닫아 기업 자산의 노출을 차단하도록 안내했습니다. 그 결과 고객사는 즉시 해당 정보를 이용한 비정상적 외부 접근이 없었는지 확인할 수 있었습니다.

더 나아가 추후 테스트 서버 사용시엔 최신 보안 패치까지 적용된 버전 사용을 권고하는 등 유사 사고 방지를 위한 컨설팅을 제공했습니다. 이는 취약점을 최소화하고 잠재적 위협을 미연에 방지하기 위한 조치였습니다. 만약 최신 보안 패치가 되지 않은 구 버전의 서버 사용 시 매우 높은 확률로 테스트 서버가 다시 외부로 노출될 수 있기 때문입니다.

Key Benefit

고객사는 Quaxar를 통해 기업의 기밀정보와 내부 서버의 외부 노출 상황을 빠르게 인지하고 문제점을 파악할 수 있었습니다. 문제를 파악한 후에는 S2W로부터 즉시 행동 가능한 대응책을 안내받아 신속하게 상황을 수습하여 안전하게 기업의 정보와 자산을 보호할 수 있었습니다.

이를 통해 고객사는 내부 보안 시스템만으로는 탐지가 어려운 외부 위협의 위험성에 대해 인지하고 기존의 보안 시스템의 취약점들을 보완할 수 있는 기회가 되었습니다.

Attack Surface Monitoring*

외부 인터넷에 공개되어 누구나 조직의 자산에 쉽게 접근할 수 있는 부분을 탐지하는 서비스입니다. 여기에는 소스코드, 개발서버 등 민감한 내부 자산들을 포함하며, 이 자산들이 내부 직원 혹은 파트너사 등을 통해 외부에 노출되지 않도록 면밀히 모니터링합니다.

TI Use Case

S2W

Data Breach Detection:

Corporate Data Leakage Detection

| 다크웹에 유출된 대량 데이터베이스 속 개인 계정 정보를 탐지한 사례

다크웹 고객 지정 키워드 모니터링 중 위협 데이터 유출 정황 포착

분석과 대조를 통해 고객사 계정 정보 유출 탐지

신속한 고객사 알림 및 즉시 적용 가능한 인텔리전스 제공

Challenge

다크웹 포럼은 개인 정보 거래의 장으로 유명한 플랫폼 중 하나입니다. 일반적으로 이렇게 외부에서 발생하는 사이버 위협은 내부 보암 시스템을 이용해 탐지하기 어렵습니다.

이 케이스는 Quaxar가 다크웹에 유출된 고객사 계정 정보를 탐지한 사례입니다. 단순히 대량의 개인 정보를 해킹해 데이터베이스를 디지털 플랫폼이나 웹사이트에 판매하는 사이버 공격은 외부 침투 등의 예측 불가한 사이버 공격을 초래합니다. 그리고 이는 기업 기밀 유출과 같은 치명적인 피해로 이어질 수 있습니다.

Action

Quaxar는 고객사 지정 키워드 위주의 다크웹 모니터링 중 러시안 다크웹 포럼에 게재된 대량의 데이터베이스 판매 포스팅을 포착하고 그것의 높은 위험성을 탐지했습니다. S2W는 분석을 통해 해당 데이터베이스가 고개사 임직원의 계정 정보를 포함하고 있다는 사실을 확인했습니다. 임직원 계정 정보 유출은 기업 서버의 취약점으로 이어져 외부 침투 공격의 표적이 될 가능성이 있기 때문에 신속한 대응이 필요한 상황이었습니다.

S2W는 즉시 고객사에 계정 유출 사실을 알리고 상황에 맞는 대응 방법을 안내했습니다. 그리고 추가 피해 확산을 방지하기 위해 기업 계정의 해킹 현황과 유출 경로를 분석했습니다. 고객사는 유출된 정보를 이용한 비정상적 서버 접근 시도가 없었는지 신속하게 확인할 수 있었습니다. 더 나아가 계정 비밀번호 강화 등 S2W가 제공한 행동 인텔리전스를 통해 잠재적 위협에 선제적으로 대응했습니다.

Key Benefit

고객사는 Quaxar를 통해 불특정 다수 대상 해킹 공격으로 인한 임직원 계정 유출 사고를 적시에 파악할 수 있었습니다. 또한, S2W로부터 제공받은 대응 방법을 따라 빠르게 외부 침투 가능성을 차단해 피해 확산을 막았습니다.

해당 사고는 고객사 사이버 보안을 강화하는 계기가 되었습니다. 그 결과 자칫하면 심각한 기업의 핵심 자산 유출로 이어질 수 있었던 상황을 미연에 방지하고 더 견고한 보안 시스템을 갖추게 되었습니다.