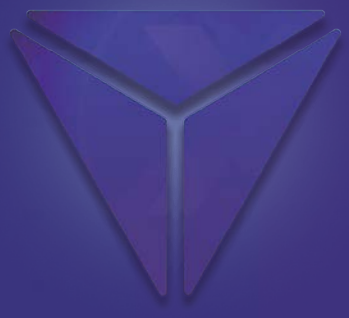

Q&A

Quaxar Launching Day

S2W

[퀘이사 연동/활용]

Q1. 유출 계정과 자산에 대한 모니터링을 효과적으로 하려면 해당 내역에 대해서 끊임없이 퀘이사와 연동해야할 것 같습니다. 내부의 자산 관리 시스템에서 이런 부분이 없는 상태라고 한다면 어떻게 해야 할까요?

유출의 경우 대체로 처음에는 대량으로 나오는 경우가 많습니다. 이런 부분은 자료 전체를 내려받거나 퀘이사에서 제공하는 API를 활용하여 내부 점검을 합니다. 첫 점검 이후에 추가로 나오는 신규 유출은 내부 시스템 연동이 없더라도 프로세스적으로 충분히 처리가 가능하신 수준이 됩니다.

유출 중에서도 심각성이 높은 악성코드 감염 (스틸러 악성코드)에 의한 것이나, 해킹으로 인한 내부 핵심 데이터베이스 유출 의심 사례로 보이는 경우, 내부 보안팀에서 충분한 조사가 어려운 경우에는 당사 Professional Service를 통해서 원인 파악 및 조치에 대한 지원을 드립니다.

내부 자산 모니터링의 경우 자산 관련 정보(e.g, 도메인) 셋업을 초기에 함께 진행합니다. 이후 모니터링 중에 발견되는 추가 자산에 대한 정보를 퀘이사를 통해 전달드립니다.

보안팀에서 알 수가 없는 자산의 추가도 생길 수 있습니다. 이런 경우에는 기업의 고유 키워드, 도메인 이름, 대역대와 같은 정보를 통해서 자동으로 탐지를 하여 알려 드리고 있습니다. 공격 표면 모니터링 (Attack Surface Monitoring) 방식이며, 이를 통해서 고객사 자산 노출을 지속적으로 탐지합니다.

즉, 내부 시스템이 있는 경우에는 이에 연동하여 관리할 수 있도록 해 드리고, 없는 경우에도 충분히 관리가 가능하도록 지원 드리고 있습니다. 효과적인 관리방안에 대한 고민이 있으시면 언제든지 문의해 주십시오.

Q2. 퀘이사에서 제공하는 정보들을 사내 시스템에 자동화하여 적용한 사례가 있나요?

API를 이용하여, SIEM, EDR, IDS, IPS 와 같은 장비에 각종 지표 연동 가능한 상태입니다. 현재 다른 고객사의 경우 REST API로 json 포맷으로 데이터를 받은 후 내부 장비에 연동하여 자동화하여 사용하고 계십니다.

Q3. 퀘이사와 타 보안 솔루션과 이중화 구성 시 중요 고려 사항은 무엇인지요? 퀘이사 자동화 관리와 이에 대한 보안 취약점 자동 스캔 및 로그 분석 등 지원이 가능한지요?

퀘이사의 경우 TI/EDR/SOAR 등과 같은 솔루션과 연동 시에 좀 더 효과적으로 사용하실 수 있습니다. 이중화 또는 통합 분석을 고려 중인 솔루션, 그리고 어떤 결과를 기대하시는지에 대해 알려 주시면, 함께 점검하여 최적의 방안을 제안 드리겠습니다.

[퀘이사 연동/활용]

Q4. 고객사 전용 게시판/RFI 게시판, RFI와 관련하여 주로 메일로 커뮤니케이션을 하고 있습니다. 별도 고객사 전용 게시판을 생성하여 케이스(티켓) 기반으로도 운영하면 추후에 히스토리 관리 측면에서 좋을 것 같은데요. 해당 기능을 제공할 계획이 있는지요?

좋은 제안이고 적극 검토하겠습니다.

Q5. 기존 자비스 엔터프라이즈 사용 고객인 경우 퀘이사로 업그레이드 되나요?

현재 사용하고 계시는 기능/정책에 맞춰서 동일한 등급의 퀘이사로 무상 업그레이드 예정입니다.

Q6. 위협인텔리전스 솔루션이 시장에 굉장히 많은데요, 이 기능만은 또는 특정 위협 정보는 퀘이사만 가능해? 라고 할 수 있는건 무엇인지? 궁금합니다.

* 국내 기업/기관을 집요하게 노리는 공격자에 대한 위협 정보 신속/정확성

* 다크웹과 암호화폐 (서드파티가 아닌) 자체적 수집 엔진 및 종합 분석력 보유

* 보안 사고 발생 시, 긴급지원 전문성과 대응력, 수사/보안 기관과 공조 역량

* RFI 기반의 신속한 지원으로 "CTI 팀이 보강된 효과"를 제공하는 것

* 다크웹, 딥웹, 텔레그램 등 다양한 채널에서 활동하는 공격자 또는 공격 그룹에 대한 분석 역량

* 보이스피싱 / 피싱 / 사칭 도메인 등에 대한 압도적인 커버리지로 우수한 정보 제공

퀘이사만의 위와 같은 강점에 더하여, 제공되는 정보의 정확도/시의성/활용성에 있어서 질적으로 우수하다고 자부하고 있습니다.

Q7. 랩서스 해킹 사례로, 모의 해킹과 직원 보안 인식 교육 중요성과 사용 컴퓨터 다단계 인증, 악성 메일 차단 등과 관련한 중요 보안 방어 요소와 더불어 Quaxar의 차별화된 지원 솔루션은 무엇인지요?

내부 접근 계정의 유출 경로는 매우 다양합니다. 또한 내부의 실수나 보안 허점으로 인해 귀중한 고객 정보나 내부 문서가 유출되기도 합니다.

누군가 우리 서비스와 유사한 형태로 피싱 사이트를 만드는 행위, 그리고 타겟팅 된 해커의 공격이나 랜섬웨어를 심기 위한 시도 등 내부 보안 강화만으로는 알기 어려운 유출 상황과 공격에 대해 한층 더 보안성을 강화할 수 있습니다.

내부 보안 인력이 충분하지 않은 경우에도, 퀘이사의 professional 서비스로 최고 전문가들의 상시 지원이 보장됩니다.

[퀘이사 연동/활용]

Q8. 퀘이사 플랫폼 자체에 대한 보호도 매우 중요할 것 같은데. 이 부분에 대해 준비가 잘 되어 있나요?

보안 점검 충분히 하여 서비스됩니다. 내부보안을 위한 운영위가 별도로 있으며, 서비스에 오픈을 위한 모의 해킹과 보안점검을 거칩니다.

Q9. 저희 회사는 한국이 아닌 다른 국가가 주 고객이라 외산 제품을 선호하는 경영진을 설득할 필요성이 있습니다. 한국이 아닌 다른 국가의 사례/이슈와 같은 정보도 한국과 같이 동일한 퀄리티로 받을 수 있나요?

S2W가 수집/분석하는 정보는 한국에만 특화되어 있지 않습니다. 예를 들어, 다크웹 관련 이슈나 랩서스, Log4shell 관련 이슈는 전 세계 공통적으로 심각도가 높은 이슈이며 이에 S2W가 가장 빠르고 풍부한 정보를 드리고 있습니다. 미디엄 블로그 등 대부분의 중요 이슈는 영문으로 작성되고, 해외 분석가들과 네트워크를 형성하여 정보를 공유하여 대응하고 있습니다. 관심 업권에서 일어나는 글로벌 동향 및 해외 이슈에 대해서도 충분히 제공해 드릴 수 있습니다.

해외의 주요 산업이나 기업의 경우, 국내보다 오히려 사례/이슈가 더 풍부한 업권도 많습니다. 현재 주요 고객사들도 글로벌 사업을 영위하고 있는 다수로, 해외 정보에 대한 커버리지에 대해서 외산 솔루션과 경쟁/비교를 거쳐서 S2W를 선택하셨습니다. 또한, 인터폴에서도 S2W의 CTI 솔루션을 도입하여 사용 중입니다. S2W에서 생산되는 정보가 전 세계적인 사이버 위협 해결에 도움이 되고 있다는 의미입니다.

[다크웹 수집/분석]

Q1. 다크웹의 테이크 다운은 어떻게 진행되나요?

상황에 따라 다르게 진행이 됩니다. 게시물 작성자를 설득하거나 자료가 올라온 호스팅 업체를 직접 컨택해 해당 게시물이 더 이상 민감 정보를 유포하지 않도록 합니다. 모든 과정은 합법적 범위 내에서 진행합니다.

문제가 발생하면 비상 서포트 TF가 가동되어 고객사 보안팀, 그리고 주요 의사 결정권자와 긴밀히 대응해 드리고 있습니다. 모니터링에서 끝나서는 안된다는 것이 퀘이사가 추구하는 Actionable Intelligence입니다. S2W의 전문성과 노하우로 수습/조사/재발방지 대응을 하는 것이 당사 professional service 지원 범위입니다.

Q2. 다크웹 주요 게시물의 자료들도 퀘이사를 통해서 다운로드 받을 수 있나요?

다크웹 내 게시판에 자료들 양이 방대하여, 모든 자료를 다운로드 해놓고 있지는 않습니다만, 대부분의 문서들과 주요 기관/기업 관련 데이터들은 확보되고 있습니다.

해킹 도구라던가, 악성코드 포함 등의 이슈가 있기 때문에 기본 브라우징은 다크웹 사이트 자체에 대한 것이 제공되고 자료의 다운로드는 별도 요청 시에 당사가 제공 드리고 있습니다. 자사 보안에 필요한 정보들은 저희가 전처리 후 제공 드리고 있습니다. 예컨대 여러 카드사의 신용카드 정보, 혹은 여러 기업 계정이 포함된 정보가 게시되는 경우, 전체에 대한 통계 및 각 고객사의 raw data를 정제해 제공 드리고 있습니다. 즉, 다운로드가 필요한 니즈가 있는 부분은 퀘이사 혹은 에스투게더를 통해서 제공이 되기 때문에 고객이 직접 다크웹의 정보를 다운로드해야 할 필요성을 느끼지 않도록 해 드리고자 합니다.

Q3. 자연어 처리 기술과 다크웹 모니터링 및 분석하는 것이 어떤 관련이 있는지요? NLP 기술이 다크웹 분석에 어떻게 활용이 되는지 궁금합니다.

NLP 기술은 핵심적인 기능으로 많이 사용하고 있습니다. 다크웹 내의 언어가 매우 다양하고 제대로 된 문법에 맞춰서 정형화된 포맷으로 기록되는 공간이 아닙니다. 전문용어나 은어도 많고 다국적 언어로 되어 있어서 다크웹만의 언어 모델링이 중요합니다.

당사의 NLP팀은 다크웹 언어분석 모델을 가장 방대한 데이터로 연구하여 국제 최고 권위 학술지(NAACL)에 등재하고, 특허도 진행 중입니다. 이런 기술들은 다크웹 사이트의 분류, 중요한 컨텐츠의 선별, 핵심 키워드 추출 등에 사용됩니다. S2W가 전 세계 어떤 기업보다도 앞서 있다고 자부하는 영역이기도 합니다.

[CTI 필요성과 구축방안]

Q1. 기업에서 CTI 도입과 CTI 조직, 인력을 구축하기 어려운 점은 무엇인지요? 기업의 경영진의 인식을 바꿀 수 있는 중요 설득 요인은 어떻게 보는지요?

내부의 보안 장비들이 해주지 못하는 영역을 논리적으로 설득하시면 좋을 것 같습니다. 예를 들어 다크웹의 배경이나 최근 사고 사례를 볼 때 공격자들의 정보, 유출내역 정보가 갖는 예방 능력과 대응력도 중요한 이유가 될 것 같습니다.

기업 내부에는, 좋은 정보를 바탕으로 신속/정확한 대응을 할 수 있는 역량을 보강하는 것은 의미가 있겠으나 그러한 정보를 직접 수집하는 시스템을 갖추거나 분석팀을 보유하는 것은 투자 효용이 매우 떨어집니다. 내부에서는 인지하기 어려운 외부 상황에 대한 인텔리전스를 확보하는 효과적인 방법으로 CTI를 고려하는 것은 효과적으로 방어력을 높이고 보안 RISK를 대폭 낮출 수 있는 투자가 된다는 점이 설득 포인트가 될 것 같습니다.

퀘이사 도입을 고려하신다면 S2W가 경영진을 함께 설득해 드리겠습니다. 최근 일련의 대형 보안 사고가 시사하는 경영상의 RISK, 관련 사건들의 원인부터 대응까지 전문적 경험이 있는 S2W가, 보안 조직 내 CTI 역량 강화와 CTI 제품 도입이 필요한 이유에 대해서 잘 설명드릴 수 있도록 하겠습니다.

Q2. CTI Strategy와 Roadmap을 작성하는 데 어려움을 겪고 있는데요. 관련하여 기업 내 CTI 운영과 관련된 컨설팅 서비스를 런칭할 계획이 있는지요?

현재 CTI 컨설팅을 별로도 하고 있지는 않습니다만, 퀘이사의 도입/활용 병행을 고려하고 계신다면 적극 지원 드리겠습니다. 외부 인텔리전스 활용과 내부 보안 조직의 CTI 역량 강화가 병행되는 것이 투자 효용에서 가장 효과적입니다. 단계별로 이런 전략을 가져가신다면 효과적이고 강력한 정보보호가 가능하리라 봅니다.

Q3. 정보보호 조직과 CTI 조직은 동일한 언어와 도구를 사용하는 건가요? 동일하다면 R&R을 통합해서 운영하면 될 것 같고, 다르다면 별도의 R&R로 분리해서 운영하는 것이 효율적일 것인데, 어떤 방안이 정답일까요?

기존 정보보호 조직의 용어(언어)와 도구에서 크게 다르지 않습니다. 다만, 기존 정보보호 조직에서 분석 업무를 하는 인원들이 충분히 내재화되어 있는지가 중요할 것 같습니다.

CTI 라이프 사이클에 맞게, 내부 자산 식별 및 영향도에 따른 이슈 모니터링, 관련 데이터 수집 및 분석이 이루어져야 하는 것을 체계화가 필요합니다. 그 기점을 시작으로, 자사의 어떤 자산을 보호하기 목적인지 여부가 정의된 상태라면, 단순 모니터링보다는 좀 더 유효성이 높은 위협 정보에 대해서 캐치 할 수 있을 것입니다.

인력의 내재화가 일정 수준 이상 된다면, 정보보호 조직 내의 별도 팀 혹은 분리된 운영을 고려할 수 있으나, 그전까지는 정보보호 조직 내부에서 긴밀하게 공조 업무를 하는 것이 더 효과적일 것이라 사료됩니다.

[CTI 필요성과 구축방안]

Q4. 현시점에서 관제 인원들을 CTI 전문 인력으로 트레이닝 하려면 어떠한 방식으로 접근해야 할까요? 또한, CTI 인력의 역량을 평가하는 기준은 무엇이 되어야 한다고 보십니까?

CTI 인력은 "외부 해커의 관점에서" 우리 기업을 볼 수 있어야 합니다.

공격 대상으로서 기업을 보려면, 공격자들이 사용하는 도구/기법에 대한 이해가 뒷받침되어야 RISK에 대해서 평가할 수 있습니다. 기본적으로 내부 보안 시스템과 대응 프로세스에 대한 관제 역량을 갖춰져 있어야 하고, 이에 더하여 최신 공격 기법, 취약점, 악성코드 이해와 같은 "공격자 관점"의 역량을 갖추고 있다면 우수한 CTI 인력이라고 할 수 있겠습니다.

분석의 경우, 단순 기술적 분석으로 그치는 것이 아닌 자사의 비즈니스 리스크에 대한 관점을 고민하면서 분석하는 실무자가 좋은 사례라고 볼 수 있습니다.

역량 평가는 정량적인 분석 내용 외에 정성적인 해당 인력의 노력과 자사 비즈니스에 대한 이해도가 반영될 수 있도록 사내에서 CTI를 위한 환경 및 정책 등의 준비를 갖춰는 것이 필요하다고 봅니다.

Q5. TI 정보를 기업 내부에서 활용할 때, 적은 것도 문제지만 너무 많은 것도 활용하기 어려울 때가 있습니다. TI 정보 활용의 Best Practice가 있다면 공유해 주십시오.

저희 고객 피드백 중에 "필요한 정보만 있어서 좋다"라는 평가를 많이 해 주고 계십니다. 소위 OSINT라고 하는 정보가 불필요하게 과도한 정보의 feeding으로 정작 시의성 있는 긴급정보의 전달이나 핵심 정보 전달에는 실패하는 경우가 많습니다. 빠르고 정확한 정보의 제공과 더불어, 불필요한 정보는 과감히 없애고, 정보 제공 수위를 고객이 조절할 수 있게 하는 것이 당사가 추구하는 TI입니다.

꼭 필요한 내용만 활용하실 수 있도록, 휘발성 정보에 대해서는 등급과 유효기간을 표기하여 제공하고, 긴급 정보는 actionable 한 대응책과 분석 리포트를 함께 제공 드리고 있습니다.

이렇게 제공받은 정보를 활용해서 내부적인 CTI 통합 상황판 등을 만드실 수도 있고, 탈취 계정의 경우, 내부 계정 관리 시스템과 연동하여 자동화된 대응도 가능합니다. 퀘이사가 best practice가 되도록 최선을 다하고 있습니다.

[기타 질의 사항]

Q1. N-DAY 분석 보고서를 만드실 때 보고서를 작성할 취약점을 고르는 기준이 있으실까요? (예. 취약점 발생한 프로그램의 tier, 취약점 severity 등)

내부 오펜시브 리서쳐들이 신규 공개되는 취약점 및 다크웹 / SNS / 중국 해킹포럼 등에서 언급되는 취약점에 대해 지속적으로 모니터링을 진행하고 있습니다. 이후 각 취약점의 영향도를 자체적으로 판단하고 있습니다.

Log4shell 케이스처럼 최종 공격을 위한 난이도는 낮고 업계 전반에 영향을 미칠 수 있는 이슈들을 최우선적으로 분석하고 고객사에 해당 내용을 전달하고 있습니다. 그다음으로는 고객사에서 요청하는 RFI입니다.

향후 좀 더 정량적인 레벨링을 도입하고 취약점에 대한 등급을 정교화하여 고객에게도 제공하고자 합니다.

Q2. 망 분리된 환경에서 퀘이사 사용을 고려할 경우, 업데이트 시 어떤 방법이 제공 가능할까요?

망 분리 환경의 경우 정보를 피딩 받으실 수 있는 중계 서버 세팅을 권장 드립니다. 유사한 환경을 구축하여 사용하고 있는 고객사의 경우, API를 통해 필요 정보를 업데이트 받고 있으며, 고객사의 인터넷존에 있는 중계기를 통해 데이터를 피딩함으로써 보안성과 독립성을 유지하는 구조로 서비스하고 있습니다.

Q3. 에스투게더를 통한 외부 정보 공유의 의미가 어떤 것인가요?

솔루션을 통한 정보의 일방적 제공과는 조금 다른 형태인 "S2W-고객사"간, 그리고 "고객사-고객사"간의 휴민트 가동이나 샘플 공유 등을 목적으로 합니다. CTI 업무를 하다 보면 상황에 따라서는 DM(개인 메세지)을 통한 데이터 제공, 정보 교류가 더 적합한 경우도 있습니다. 동향 파악 보고를 위한 정보 공유, 애로사항 공유, 노하우 공유 등의 소통도 필요합니다. 개인적 네트워크에 의지할 수도 있겠지만, 동일한 미션을 가지고 CTI 업무를 수행하는 인력들 간의 정보 공유 채널로서 기능이 필요하다고 보고 있습니다.

이런 활동이 기능하려면 신뢰 기반의 상호 호혜적인 커뮤니티가 중요합니다. 성공사례나 위급상황에 대해서 나누고 연합하고자 하는 적극적 고객사들도 많이 계십니다.

함께 만들어가야 할 부분이고 저희도 계속 고객사와 아이디어를 나누고 있는데, 공격자들은 정보를 활발히 공유하는데 반해 수비를 해야 하는 입장에서는 각개격파 당하는 부분을 궁극적으로는 해결해 보고자 합니다.

언제, 어디서
발생할지 모르는
보안 사고.

미지의 위협으로부터
기업을 보호해줄
정확한 정보, 문제 파악,
그리고 신속한 대처.

S2W가 함께하겠습니다.

S2W

S2W와 솔루션에 대해 더 알고 싶으신가요?

S2W의 문은 언제나 열려있습니다. 아래의 메일 주소로 문의주세요.

info@s2w.inc

www.s2w.inc

경기도 성남시 분당구 판교역로 192번길 12, 판교미래에셋센터 3층 | +82 07 5066 5277