ANOMALI®

위협 인텔리전스 관리
플레이북

위협 인텔리전스 플랫폼(TIP) 평가,
선택, 관리 및 최적화를 위한 가이드

색인

제1장. 소개

위협 인텔리전스 플랫폼이란?

사이버 공격자의 공격 방법은 끊임없이 진화하고 발전을 거듭하고 있습니다. 기업은 사이버 공격자와 그 공격 기법, 기술 및 절차(TTP)와 관련된 조치 가능한 정보를 제공하는 위협 인텔리전스를 활용하여 사이버 공격에 대한 컨텍스트를 확보합니다. 위협 인텔리전스 플랫폼(TIP)은 위협 인텔리전스 연구의 수작업을 자동화하고 탐지 시간을 단축해주는 솔루션입니다. 또한 분석가와 기업 전체 팀 간의 협업을 지원하는 통합 환경에서 사이버 위협을 조사하고 대응할 수 있도록 지원합니다.

위협 인텔리전스를 사용하여 탐지 개선

포네몬 연구소(Ponemon Institute)는 최근 IT 전문가를 대상으로 탐지용 위협 인텔리전스 사용에 관한 설문 조사를 진행했습니다.

- **85%** 의 응답자가 포네몬 설문 조사에서 **위협 인텔리전스가 강력한 보안 체계의 필수 요건이라고** 답했으나, 단 **41%** 만이 **외부 위협을 효과적으로 탐지하고 있다고 응답했습니다**.
- **절반에 못 미치는 48%** 의 응답자가 포네몬 설문 조사에서 **전용 위협 인텔리전스 플랫폼을 보유하고 있다고 답했습니다**.
- 단 **33%** 의 응답자만이 포네몬 설문 조사에서 **위협 탐지에 충분한 예산을 보유하고 있다고 답했습니다**.

출처: 위협 인텔리전스의 가치: 포네몬 연구소(Ponemon Institute), 2019년, 북미 및 영국 기업을 대상으로 한 연례 연구

제1장. 소개

위협 인텔리전스 플랫폼과 다른 보안 솔루션의 차이점:

- ***다양한 출처에서 인텔리전스 집계*** - 보안 솔루션 대부분은 환경 내부 정보에만 초점을 맞춥니다. 진보한 위협 인텔리전스 플랫폼은 외부 및 내부 출처 데이터를 모두 사용하고 서로 연결하여 TI 분석가에게 알려진 위협이나 의심스러운 위협에 대해 한층 더 포괄적인 통찰력을 제공합니다.
- ***데이터 선별, 정규화, 강화 및 위험 점수화*** - 개별 침해지표에서 위협 인텔리전스 보고서, 게시판 및 프로필을 수동으로 생성하는 프로세스는 부담이 크고 시간이 많이 소요됩니다. 위협 인텔리전스 플랫폼은 이러한 프로세스의 대부분을 자동화하므로 분석가가 데이터를 취합하는 데 소요되는 시간을 줄이고 사전 예방적 방어 지원을 위한 충실도가 높은 인텔리전스를 제공하는 데 더 많은 시간을 할애할 수 있습니다.
- ***기존 보안 시스템과의 통합*** - 많은 보안업체가 다른 시스템을 대체하려고 합니다. TIP는 기존 솔루션과 함께 작동하여 모든 보안 솔루션의 역량을 업그레이드합니다.
- ***위협 인텔리전스의 분석 및 공유*** - 다른 분석가와 공유하지 않는다면 위협 인텔리전스 생성은 의미가 없습니다. 위협 인텔리전스를 안전하게 공유하면 보다 포괄적이고 안정적인 결과를 창출하여 더욱 신속하게 대응할 수 있습니다.

사이버 공격자는 많은 TTP와 전략을 재사용하여 유사한 조직과 인프라를 공격 대상으로 삼습니다. 악의적인 사이버 공격자에 대한 정보와 컨텍스트가 많을수록 보안 팀이 심각한 피해를 입지 않도록 한층 더 빠르고 쉽게 예방할 수 있습니다.

제1장. 소개

위협 데이터 출처를 한눈에 파악

위협 인텔리전스 플랫폼은 다양한 형식과 초점을 지닌 위협 데이터의 다양한 출처를 활용하도록 설계되어 있습니다. 보안 팀은 위협 피드를 선택하고 그중에서 해당 조직과 관련된 위협을 알리는 데 가장 적합한 항목을 결정합니다.

일반적인 데이터 출처는 다음과 같습니다.

- ***타사 프리미엄 피드*** - 보안업체는 테러 지원국 공격자 또는 딥 웹과 다크 웹 등 특정 주안점을 포함한 피드를 판매합니다. 이러한 피드는 대개 매우 포괄적이고 확보하기 어려운 정보로 이루어져 있습니다.
- ***오픈 소스 피드*** - 오픈 소스 인텔리전스는 보안 연구진, 기업 블로그, 공개적으로 제공되는 블랙리스트 또는 화이트리스트에서 제공되는 무료 정보입니다.
- ***위협 공유 단체*** - 정보 공유 및 분석 센터(ISAC)와 같은 위협 공유 단체에서 산업 관련 위협 데이터를 검증된 회원과 공유합니다.
- ***오픈 소스 분석 플랫폼*** - MISP(Malware Information Sharing Platform)는 오픈 소스 맬웨어 정보 공유 플랫폼입니다. MISP는 위협 인텔리전스 플랫폼의 전체 기능을 다 갖추고 있지는 않으나 IOC의 수집, 공유, 저장 및 상호 연결을 시작하는 사용자에게 적합합니다.
- ***커뮤니티 지식 베이스*** - 오늘날 사이버 보안과 관련된 가장 인기 있는 지식 베이스 중 하나는 MITRE ATTACK™ 프레임워크입니다. 실제 발생한 사례 관찰을 기반으로 한 공격 기법 및 기술을 담아낸 지식 베이스로 전 세계에서 쉽게 접근할 수 있습니다. 이 프레임워크는 민간 부문, 정부 기관, 사이버 보안 제품 및 서비스 커뮤니티에서 특정 위협 모델과 방법론을 개발하기 위한 기반으로도 사용됩니다.

Anomali에서 받은 데이터 및 분석 품질이 개선되어 사용자에게 유익한 정보를 전달하고 있습니다. 이를 통해 조직에 대한 내부 및 외부 위협을 한층 더 정확하게 파악하고 이러한 조사에 소요되는 시간을 더욱 효율적으로 활용할 수 있게 되었습니다.

IT 전문가 | 항공우주 및 국방 산업

제2장. 위협 인텔리전스 플랫폼이 해결해야 할 문제

위협 데이터 자동화를 통한 신속한 통찰력 확보

사이버 보안 공격 횟수와 치밀성은 하루가 다르게 상승하고 있습니다. 조직은 위협에 미리 대처하고 한층 더 효과적으로 대응할 수 있는 방법을 파악하기 위해 어떤 위협에 직면했는지 정확히 알고 있어야 합니다.

분석가들은 일반적으로 SIEM(보안 정보 및 이벤트 관리) 시스템 등 다양한 보안 솔루션의 경고를 검토하여 공격의 증거를 찾습니다. 그러나 SIEM은 조직의 모든 데이터를 처리하고 저장하도록 설계되어 있기 때문에 생성되는 대부분의 경고는 실제 위협이 아닙니다. 이러한 오탐지는 실제로 악성이 아니기 때문에 경고를 조사하는 데 필요한 귀중한 리소스의 낭비를 초래하는 경우가 많습니다.

추가 인력을 보충할 수 없는 상황이라면 보안 팀의 효율성에도 심각한 타격을 줄 수 있습니다. 위협 인텔리전스는 분석가가 경고를 필터링하고 내부 위협 마커와 함께 선별된 위협 인텔리전스를 상호 연결하여 확인할 수 있도록 도와줍니다.

위협 인텔리전스 자체에도 여러 가지 문제가 있을 수 있습니다. IOC가 수백만 개에 이를 수도 있으며 관련 정보를 파악하는 프로세스에 많은 인력이 필요할 수도 있습니다. 위협 인텔리전스 플랫폼은 입력 정보를 자동으로 상호 연결하여 사이버 위협에 대해 한층 더 빠른 통찰력을 제공합니다.

350,000건의 사이버 보안 채용 공고가 현재 진행 중이며 전 세계적으로 2021년까지 3백 5십만 개의 사이버 보안 직업이 부족할 것이라고 예측되고 있습니다.

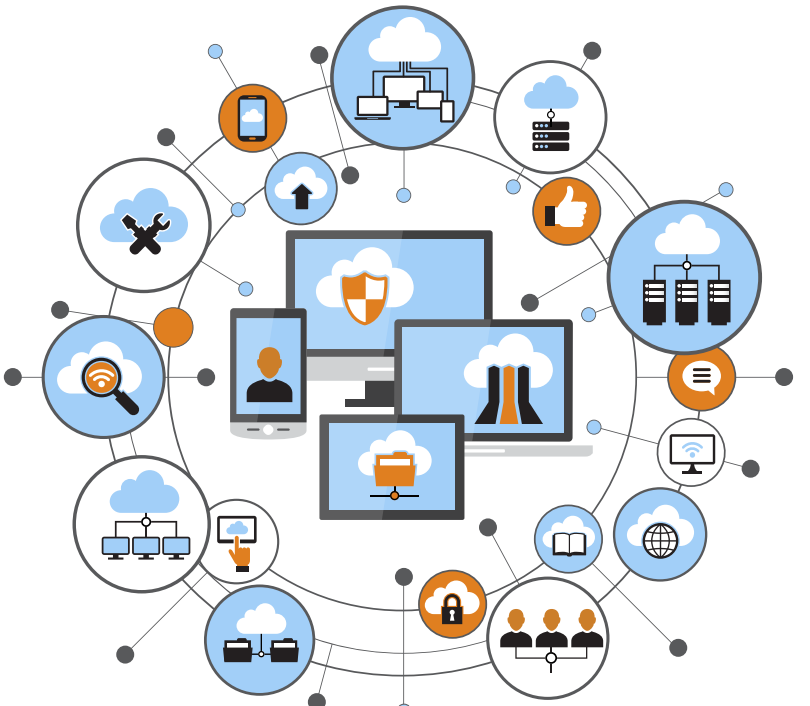
출처: Cybersecurity Ventures

제3장. 위협 인텔리전스 플랫폼의 탐지 대상

위협 인텔리전스의 주된 사용자

위협 인텔리전스 플랫폼은 정보를 수동으로 관리하는 데 쓰이는 시간을 다시 분석가에게 돌려주기 위해 설계되었습니다. 미가공 데이터가 쉽게 이해하고 바로 공유할 수 있으며 무엇보다 바로 조치를 취할 수 있는, 완성된 형태의 인텔리전스로 변환됩니다. 조직은 기존 보안 도구와의 인텔리전스, 자동화 및 통합을 통해 관련 위협을 파악할 수 있습니다. 위협 인텔리전스 플랫폼을 가장 자주 사용하는 사용자는 다음과 같습니다.

- 위협 인텔리전스 분석가
- SOC(보안 운영 센터) 분석가
- 사이버 위협 헌터
- 사고 대응(IR) 분석가
- CISO(최고 정보 보안 책임자)



제3장. 위협 인텔리전스 플랫폼의 탐지 대상

데이터 집계 및 선별

위협 인텔리전스 플랫폼은 다양한 출처에서 위협 데이터, 정보 및 인텔리전스를 자동으로 수집합니다. 보안 분석가는 사용자 지정 데이터 가져오기를 설정할 수 있는 유연성을 갖추고 있을 뿐 아니라 공급업체 또는 신뢰할 수 있는 제3자로부터 정보를 신속하게 수집할 수 있어야 합니다. 이러한 인텔리전스 리포지토리가 조사 및 기타 보안 도구로 변환됩니다.

TIP에 입력되는 많은 항목이 중복되거나, 더 이상 악성이 아니거나, 위협이 될 만한 동작이라고 보기에 충분하지 않을 수 있습니다. TIP는 사이버 위협과 관련된 다양한 요인을 기반으로 정보를 분류하고 각각의 IOC에 가중치를 적용하는 머신 러닝 알고리즘을 보유하고 있습니다. 선별된 지표는 위험 점수 및 관련 인텔리전스가 포함된 읽기 쉬운 형식으로 표시됩니다.

관계형 태그 및 IOC 유형을 기반으로 정보를 수집, 보강 및 클러스터링할 수 있는 능력이 SOC의 위협 인텔리전스 측면에서 크게 향상되었습니다. 자동 통합의 계층화를 통해 얻은 이점 역시 폭발적입니다.

SOC 관리자 | 에너지 및 유틸리티

제3장. 위협 인텔리전스 플랫폼의 탐지 대상

조사

위협 인텔리전스 분석가는 위협을 조사하고 보안 전략을 안내하는 새로운 위협 인텔리전스를 생성할 책임이 있습니다. 이러한 종류의 분석에는 일반적으로 수십여 개의 도구와 막대한 시간이 요구됩니다.

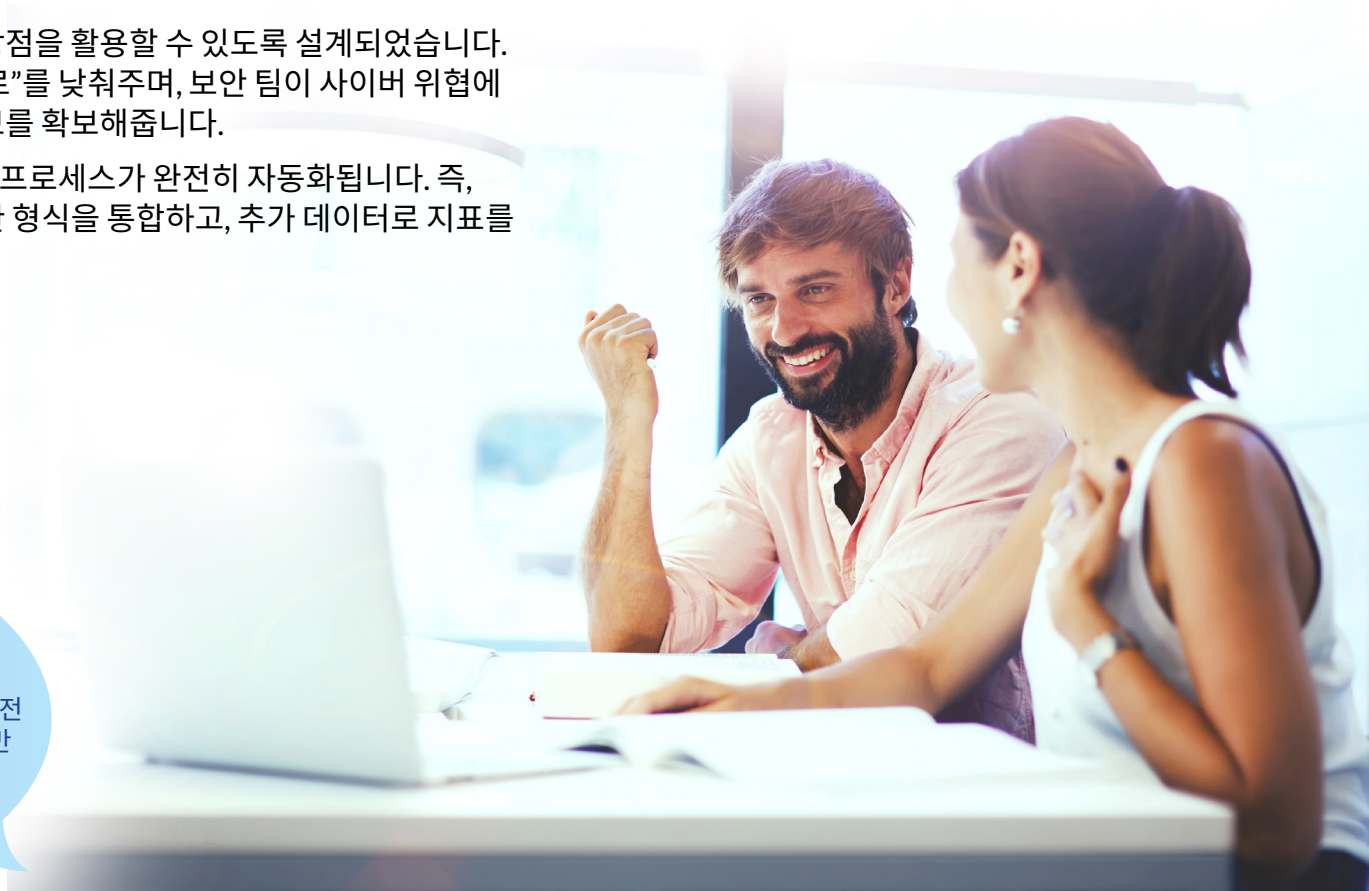
분석가는 TIP를 사용하여 자동화된 확장형 워크플로를 통해 조사를 수행하고 여러 팀과 협업할 수 있습니다. 또한 알려진 IOC와 피봇을 관리하여 알려지지 않은 위협을 조사할 수 있습니다. 동일한 조사 내에서 분석가는 지표를 인텔리전스와 연결하고, 관련 관찰 대상 및 보안 게시판을 생성하고, 사이버 공격자와 해당 TTP를 파악할 수 있습니다.

제3장. 위협 인텔리전스 플랫폼의탐지 대상

자동화

위협 인텔리전스 플랫폼은 기계 및 인적 기능의 장점을 활용할 수 있도록 설계되었습니다. 자동화는 인적 오류를 줄이고 분석가의 "경고 피로"를 낮춰주며, 보안 팀이 사이버 위협에 대한 고도의 판단을 내리는 데 필요한 시간과 정보를 확보해줍니다.

막대한 양의 데이터와 관련된 번거롭고 반복적인 프로세스가 완전히 자동화됩니다. 즉, 중복 데이터를 제거하고, 읽기 쉬운 정보로 다양한 형식을 통합하고, 추가 데이터로 지표를 강화하고, 보안 솔루션을 통합할 수 있습니다.



Anomali를 사용하면 다양한 인텔리전스 리소스에서 생성되는 대량의 데이터를 처리하고 조직과 관련된 위협을 파악할 수 있습니다. 이제 위협 데이터를 더 빠르게 가져오고, 위험과 상호 연결한 후, 사전 예방적 위협 관리 및 완화를 위해 SIEM에 필요한 지표만 내보낼 수 있습니다.

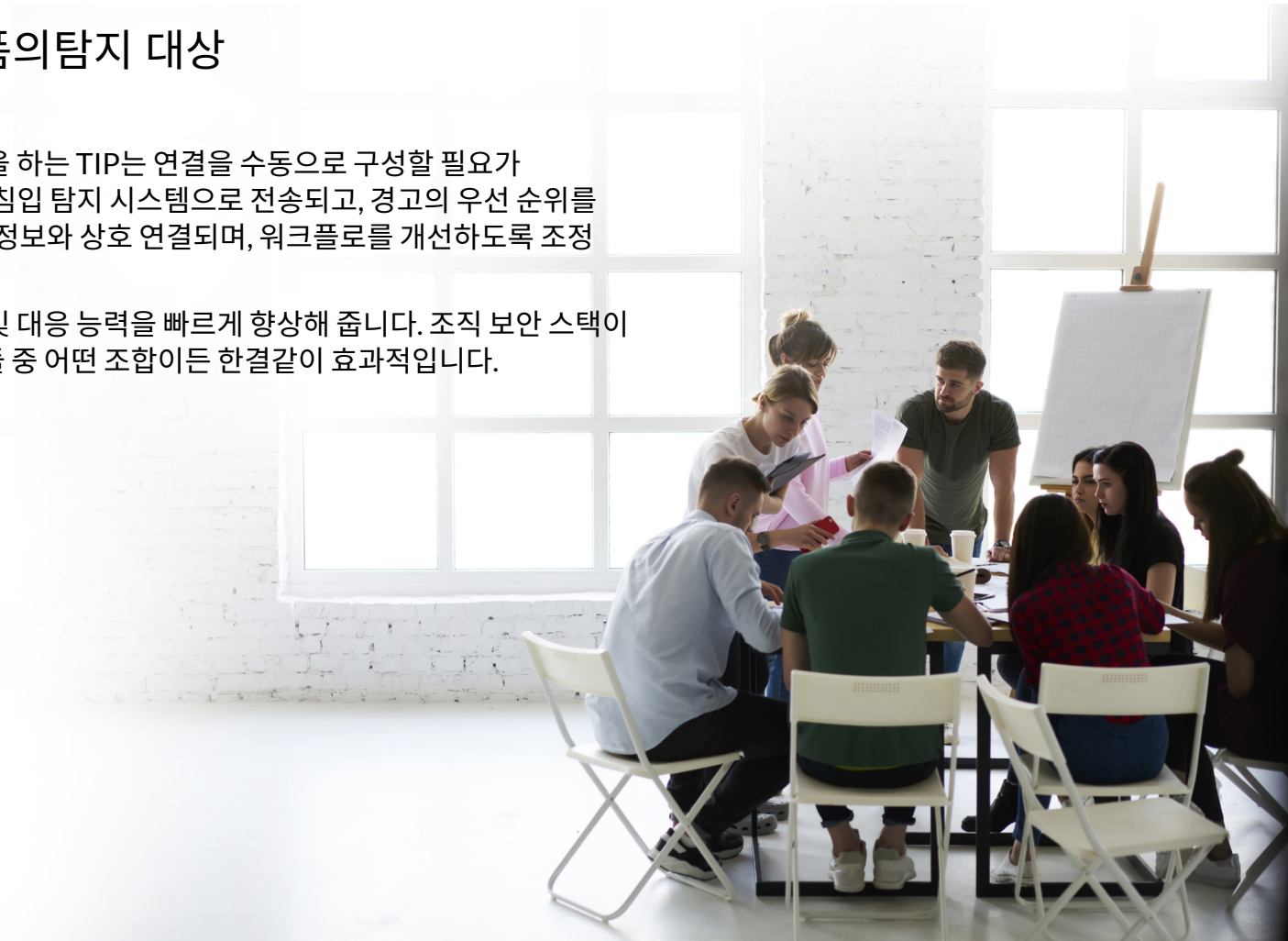
인텔리전스 분석가| FinServ

제3장. 위협 인텔리전스 플랫폼의탐지 대상

통합

정보 및 기존 보안 솔루션 사이에서 중개 역할을 하는 TIP는 연결을 수동으로 구성할 필요가 없습니다. 지표가 활성 차단을 위해 방화벽 및 침입 탐지 시스템으로 전송되고, 경고의 우선 순위를 지정하기 위해 SIEM 및 엔드포인트 솔루션의 정보와 상호 연결되며, 워크플로를 개선하도록 조정 플랫폼으로 전송됩니다.

이러한 통합의 유연성은 보안 팀의 위협 파악 및 대응 능력을 빠르게 향상해 줍니다. 조직 보안 스택이 전체적으로 클라우드 기반, 온프레미스 또는 둘 중 어떤 조합이든 한결같이 효과적입니다.



제3장. 위협 인텔리전스 플랫폼의탐지 대상

협업 및 공유

조직은 더 효과적으로 사이버 공격자의 전략을 예측하고, 악성 동작을 파악하고, 상황에 맞는 상세한 위협 인텔리전스를 통해 공격을 차단할 수 있습니다. 보안 팀은 다른 팀과 협력하여 이러한 인텔리전스를 생성하고 공유를 통해 커뮤니티를 보호함으로써 방어 체계를 강화할 수 있습니다.

TIP는 조사에 대한 협업을 촉진하고 인텔리전스의 즉각적인 양방향 공유를 가능하게 합니다. 정보 공유 및 분석 센터(ISAC)와 같은 공유 단체는 일반적으로 위협 인텔리전스 플랫폼을 활용하여 유사 산업 분야의 기업에 따라 조직이 다양한 리소스와 전문 지식을 활용할 수 있도록 지원합니다.

Anomali 자동화를 통해 악성 사이버 공격자의 정보를 빠르고 안전하게 조사하고 업계 파트너와 공유할 수 있었습니다. 또한 신뢰할 수 있는 조직으로부터 받은 인텔리전스가 경고를 위한 도구에 자동으로 채워집니다.

IT 전문가| 에너지 및 유틸리티 기업

59%의 응답자가 조직이 위협 인텔리전스를 다른 조직과 공유한다고 응답한 반면, **56%**의 응답자는 데이터 오용 가능성으로 인해 위협 인텔리전스를 공유하기 망설여진다고 답했습니다.

출처: 위협 인텔리전스의 가치: 포네몬 연구소(Ponemon Institute), 2019년, 북미 및 영국 기업을 대상으로 한 연례 연구

제4장. 보안 수명 주기에 따른 위협 관리 방법

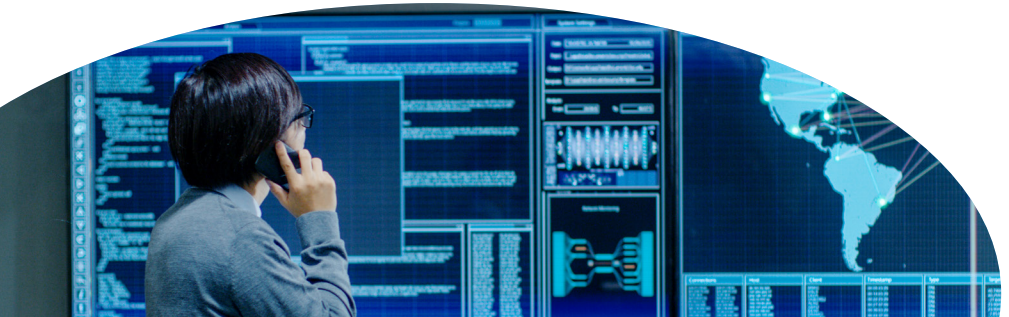
강력한 보안 체계를 구축하는 것은 반복적인 프로세스입니다. 계획, 모니터링, 탐지, 분석, 응답, 문제 해결, 피드백 등 보안 수명 주기에 이르는 모든 요소를 개선하려고 시도하는 것은 부담스러울 수 있습니다. 위협 인텔리전스는 이러한 조치를 한층 더 가속화하고 대상을 좁힐 수 있는 컨텍스트를 제공하여 각 단계를 지원합니다.

계획

보안 팀은 모든 가능성에 대비해야 합니다. 보안 팀은 조직이 생산하는 제품 또는 서비스, 지리적 위치, 정치적 동맹 등을 기준으로 어떤 위협에 직면할 가능성이 가장 높은지 평가합니다. 위협 인텔리전스를 통해 보안 팀은 이러한 이론의 옳고 그름을 입증할 수 있습니다. 분석가는 위협과의 관련성 및 사이버 공격자의 공격 방식에 대한 더 많은 가시성을 확보할 수 있습니다. 이러한 데이터, 정보 및 인텔리전스를 분석하는 것 외에도, 분석가는 TIP를 통해 예방 및 완화를 위해 가장 효과적인 도구를 선택하고 활용할 수 있습니다.

모니터링 및 탐지

악성 동작을 탐지하고 모니터링하는 방법은 다양하지만 위협 인텔리전스의 통합이야말로 이러한 위협을 사전에 방어하는 유일한 방법입니다. 사이버 공격자와 TTP에 대한 검증된 외부 컨텍스트를 사용하면 보안 분석가가 과거에 대한 조사를 실시하여 악성 공격 여부를 확인할 필요가 없습니다. 조직은 위협 인텔리전스와 기존 보안 시스템의 데이터를 상호 연결하여 이러한 악성 지표가 존재하는지 여부를 신속하게 파악할 수 있습니다. 의심스러운 것으로 파악된 모든 사항은 모니터링을 위해 통합 지점에 자동으로 전송되며, 이를 통해 위협이 네트워크에 침투하기 ***전에*** 차단할 수 있습니다.



제4장. 보안 수명 주기에 따른 위협 관리 방법

조사 및 분석

악성 개체가 발견되면 분석가는 조사를 실시하여 조직에 미치는 영향을 파악합니다. TIP는 분석가가 다양한 정보를 연결할 수 있는 증거를 조사할 수 있도록 워크벤치를 제공합니다. 분석가는 개별 IOC를 대상으로 WHOis 정보, PassiveDNS 등을 찾아 과거에 알려진 바 없는 위협을 찾아냅니다.

대응 및 해결

사이버 공격 사고가 발생했을 때 분석가는 TIP를 통해 패턴과 관련 사이버 공격자를 식별하여 한층 더 신속하게 해결 및 대응 정보를 알릴 수 있습니다. 예를 들어, 특정 공격자가 특정 도구 또는 공격 기법을 사용하는 것으로 알려져 있다면 TIP는 대상을 좁혀서 사이버 공격 조사를 수행할 수 있다는 사실을 분석가에게 알릴 수 있습니다.

Anomali를 사용하면 지표 수집 자동화를 통해 분석가가 Anomali에서 제공하는 추가 데이터를 사용하여 보안 사고를 조사하고 상황을 파악할 시간을 더 많이 확보할 수 있습니다.

인텔리전스 분석가 | FinServ

제4장. 보안 수명 주기에 따른 위협 관리 방법

피드백

피드백 단계는 현재 보안을 개선하기 위해 매우 중요한 단계입니다. 위협 인텔리전스 플랫폼은 도구와 정보 사이에 존재하기 때문에 어떤 점을 개선해야 할지 평가하는 데 유용합니다.

고려해야 할 주요 영역은 다음과 같습니다.

- 위협 식별 및 차단에 가장 유용한 정보 출처를 확인하는 ***모니터링 단계***
- 결론 도출에 걸리는 시간을 문서화하는 ***탐지 및 분석 단계***
- 올바른 정보의 수집 여부 및 대응에 걸리는 시간을 판단하기 위한 ***대응 및 해결 단계***. 예를 들어, 악성 사이버 공격자가 시스템을 감염시키는 경우 TIP 사용자는 해당 위협에 대한 정보가 이미 리포지토리에 존재하는지, 아니면 다른 출처에 해당 정보가 포함되어 있는지 확인할 수 있습니다.

제5장. Anomali®

Anomali를 통한 위협 인텔리전스 관리

Anomali는 효과적인 사이버 보안 의사 결정을 내릴 수 있도록 유도하는 위협 데이터, 정보 및 인텔리전스를 갖추고 있습니다. 조직에 대한 가장 심각한 위협의 탐지, 우선 순위 지정 및 분석을 자동화하는 플랫폼입니다. 머신 러닝, 자동화, 광범위한 파트너 에코시스템을 갖춘 Anomali는 분석가가 위협 인텔리전스를 활용하여 사이버 공격에 대한 한층 더 나은 통찰력을 갖추고 대응할 수 있도록 지원합니다.

Anomali 플랫폼은 다음 세 가지 요소로 구성되어 있습니다.

- **ThreatStream®**은 분석가가 위협 인텔리전스를 생성하고 보안 사고를 조사할 수 있도록 구축된 위협 인텔리전스 플랫폼입니다. 경고 우선순위를 정하고 보안 전략을 안내하는 머신 러닝을 통해 복잡한 대량 지표를 수집하고 상황에 맞게 조정하고, 위험 등급을 정합니다.
- **Anomali Match™**는 사용자 환경에서 탐지 시간을 자동화하고 속도를 높이기 위해 특별히 제작된 위협 탐지 엔진입니다. Anomali Match는 12개월간의 메타데이터를 활성 위협 인텔리전스와 비교하여 이전에 알려지지 않았던 위협을 조직에 알려줍니다.
- **Anomali Lens™**는 위협 및 보안 분석가가 한층 더 빠르고 정확한 의사 결정을 내릴 수 있도록 지원합니다. Anomali Lens는 모든 모바일 또는 브라우저 페이지에서 전략적 및 전술적 인텔리전스에 대한 즉각적인 액세스를 제공합니다. 모든 수준의 분석가가 실시간 점수 및 컨텍스트를 활용하여 빠르게 의사 결정을 내릴 수 있습니다. 경영진은 자신의 기기에서 위협 인텔리전스에 액세스하여 비즈니스에 대한 최신 위협과 관련된 정보를 손쉽게 확인할 수 있습니다.

Anomali의 이점

- 조직을 대상으로 삼은 위협 파악
- 위협 탐지 및 분석 자동화
- 사이버 공격자 및 행동에 대한 통찰력을 통해 대응 능력 향상
- 공격의 영향력을 최소화하여 시간과 리소스 절약
- 내부 및 외부 CTI 단체 간의 협업 허용

Anomali는 사이버 위협 인텔리전스에 필요한 모든 특성을 지속적으로 업데이트하여 새로운 차원의 보안 운영 단계로 이끌어 주었습니다. 이를 통해 새로운 위협으로부터 조직을 보호할 수 있습니다.

IT 관리자| 컴퓨터 서비스 기업

제6장. 사례 연구

콜로라도 위협 인텔리전스 공유(CTIS) 사례 연구

2017년, 콜로라도주는 Anomali와 협력하여 콜로라도 위협 인텔리전스 공유 네트워크(CTIS)를 조직했습니다. 이를 통해 주, 자치주, 연방주 및 지방자치시를 연결하여 보안 팀이 위협을 공유 및 분석하고 효과적으로 대응하도록 지원했습니다.

도전과제

콜로라도주는 지역 사회에 중요한 사이버 보안 정보를 공유할 수 있는 안전한 포털을 만들기 위해 노력하고 있었습니다. 이메일을 통해 정보를 공유하는 과거의 방법은 안전하지 않고, 비협조적이며, 긴급 상황에서 신속하게 정보를 제공할 수 없었습니다. 위협에 관한 정보를 원활하고 안전하게 공유할 수 없다면 주 정부 부서는 사이버 공격을 예방하고 차단할 수 있는 중요한 정보를 놓칠 수 있습니다.

해결책

콜로라도주는 Anomali와 협력하여 종합적인 위협 공유 및 분석 플랫폼의 제공을 통해 모든 주 정부 부서가 한 장소에서 기밀 정보를 공유할 수 있도록 했습니다. 이 포털은 현지 정부가 신뢰할 수 있는 사용자 범위 내에서 잠재적 위협에 대한 데이터를 즉시 공유할 수 있어 한층 더 확대된 가시성을 제공합니다.

주요 이점

- 콜로라도주 전역의 모든 지역, 지방자치시, 자치주 및 연방주 부서에서 원활하고 안전하게 위협 정보 공유
- Multi-State ISAC를 통한 협업 수행 및 다른 주와의 인텔리전스 공유
- 강력한 위협 조사 도구 모음과 함께 보안 분석가가 공격을 신속하게 평가 및 파악

> “콜로라도주 전역에 걸쳐 광범위한 사이버 위협 공유를 추진해야 할 중대한 필요성에 대응하기 위해 CTIS를 개발했습니다”라고 콜로라도주의 CIO 트레버 티몬스는 말했습니다. “주 내 모든 수준의 정부에서 다양한 부서와 자치주가 적극적으로 협력하여 빠르게 이를 채택하는 것을 확인했습니다. 모든 주에서 사이버 위협 공유 프로그램을 구현하여 보안 체계를 강화할 것을 강력히 권장하는 바입니다.”

백서 다운로드 »

제6장. 사례 연구

연방 시스템 통합업체 사례 연구

이 연방 시스템 통합업체(FSI)는 미국 인텔리전스 커뮤니티, 미국 국방부 및 기타 연방 기관을 위한 정보 솔루션, 엔지니어링 및 분석 분야의 검증된 공급업체입니다. FSI는 40년 이상의 경험을 바탕으로 고객의 가장 복잡한 문제를 해결할 수 있는 영향력이 큰 미션 크리티컬 서비스 및 솔루션을 설계, 개발 및 제공하고 있습니다.

도전과제

인텔리전스에 대한 민감성이 높은 클라이언트 및 보안 커뮤니티와 주로 협력하는 시스템 통합업체로서 FSI의 지적 재산(IP)에는 매우 중요하고 가치가 높은 정보가 포함되어 있습니다. 미국 정부에 반드시 필요한 이러한 지적 재산을 보호하고 보안을 유지해야 했습니다.

해결책

이 FSI는 자동화된 사이버 위협 인텔리전스 솔루션을 위해 ThreatStream을 사용했습니다. ThreatStream™ 플랫폼은 조치 가능한 인텔리전스와 기존 보안 인프라를 융합하여 사이버 공격에 대응합니다.

주요 이점

- 중복을 제거하는 동시에 여러 위협 인텔리전스 출처를 통합 및 선별
- 검증된 교차 분석 제공
- 높은 신뢰도와 함께 신속한 인텔리전스 운영

> “ThreatStream과 함께 하며 기업 자산에 대해 매일 발생하는 단순한 위협부터 첨단적인 침해 시도까지 효과적으로 방지하는 데 큰 도움을 받았습니다.” 연방 시스템 통합업체 CISO.

사례 연구 전문 읽기 »

제6장. 사례 연구

UAE 은행 연합(ISAC) 사례 연구

UAE 은행 연합(UBF)은 비영리 단체로 아랍에미리트(UAE)에서 운영되는 50개 회원국 은행 및 업계를 선도하는 UAE 은행 부문 협회를 대표합니다.

도전과제

사이버 공격의 빈도는 끊임없이 증가하고 기법은 점점 더 정교해지고 있으며, 기업과 모든 산업은 공격력이 뛰어난 사이버 공격자로부터 데이터와 시스템을 보호해야 하는 중대한 과제를 안고 있습니다. 사이버 위협 공격자와 단체가 조직을 공격하고 침투하기 위해 서로 도구, 기술 및 절차(TTP)를 공유하고 있기 때문에 기업 네트워크와 중요 인프라를 보호하는 이들도 신뢰성이 높고 안전하고 효과적인 방식으로 동료와 협력하여 대응 작업을 수행해야 합니다.

해결책

UBF Tasharuk 이니셔티브는 2017년 9월에 출시되었으며, Anomali 플래그십 제품인 ThreatStream을 기반으로 합니다. 이 플랫폼은 UAE 은행 연합 회원사가 지역 금융 기관 전반에 걸쳐 적시에 적절하고 조치 가능한 인텔리전스를 공유하는 데 사용됩니다. 정보 공유 및 분석 센터(ISAC)와 Anomali의 파트너십으로 탄생한 부가 가치 구성 요소는 이른바 "Anomali - 위협 분석 센터(A-TAC)"라고 알려진 인텔리전스 연구팀입니다.

주요 이점

- UAE 금융 부문에 대한 사이버 위협 관련 상황적 인식 제고
- 총체적인 보안 목표에 집중할 수 있는 중앙 집중식 실무자 커뮤니티
- 보안 체계 개선 및 전체 기관에 대한 사이버 공격 관련 대응 능력 향상

> "Tasharuk의 출시로 참여 은행의 사이버 범죄 방지 노력을 최소화하면서 방어 시스템 향상을 위해 잠재적 악성 위협에 대한 정보를 알릴 수 있었습니다." HE 압둘 아지즈 알 구허에어, UAE 은행 총재

블로그 살펴보기 »

제7장. 결론

사이버 범죄자, 테러 지원국 사이버 공격자, 핵티비스트는 악용을 위해 밤낮을 가리지 않고 여러 조직을 공격 대상으로 삼습니다. 이제 조직의 취약점을 파악하고, 위협에 미리 대처하며, 이벤트를 신속하게 해결하면서 그 이점을 누릴 수 있습니다.

조직에서 내부 보안 시스템과 외부 위협 피드에서 대량의 데이터를 수집할 수도 있겠지만, 이러한 모든 데이터를 수동으로 투입할 경우 엄청난 양의 리소스를 낭비하며 엄청난 수의 오탐지 및 미탐지를 일일이 가려내야 합니다. 이러한 모든 사이버 공격을 조사할 경우 사이버 보안 인재 부족으로 인해 보안 팀에 과부하가 오는 상황이 발생할 수 있습니다.

TIP은 조치 가능한 위협 인텔리전스를 제공하고 전체 보안 수명 주기를 가속화하고 단순화하는 방식으로 내부 및 외부 위협 데이터, 정보 및 인텔리전스를 취합하고 분석하는 프로세스를 자동화합니다. 관련 IOC를 식별하고 이에 대응할 준비를 하거나, 위협을 모니터링, 탐지 및 분석하고, 이벤트에 대응하거나, 보안 운영을 개선하려는 경우 TIP을 통해 위협을 한층 더 신속하고 효과적으로 방지하고 해결하는 데 필요한 컨텍스트를 확보할 수 있습니다.

Anomali는 오탐지 비율을 80%까지 줄여주므로 정규직 직원 2명을 추가 채용한 것과 같은 효과를 얻을 수 있습니다.

IT 책임자 | 의료 서비스

Anomali를 통해 위협 인텔리전스 및 관리 목표를 달성하십시오.

자세히 알아보기 | ANOMALI 주간 위협 브리핑 | 무료 STIX/TAXII: STAXX | 데모 요청

ANOMALI®

웹사이트: www.anomali.com

연락처: **+1 844-4-THREATS**(847328)
+44 8000 148096(국제 통화 요금 무료)

Anomali®는 인텔리전스 기반 사이버 보안 솔루션을 제공합니다. 조직은 Anomali 플랫폼을 사용하여 위협 데이터, 정보 및 인텔리전스를 활용하여 위험을 줄이고 방어 체계를 강화하는 효과적인 사이버 보안 결정을 내릴 수 있습니다. Anomali는 머신 러닝에 최적화된 위협 인텔리전스로 보안 팀을 강화하고, 사용자 환경을 공격 대상으로 삼는 숨겨진 위협을 파악합니다. Anomali 플랫폼은 조직이 신뢰할 수 있는 커뮤니티 간에 위협 정보를 협업 및 공유할 수 있도록 지원하며, 전 세계 ISAC 및 선도적인 기업에 의해 가장 널리 채택된 플랫폼입니다. 자세한 내용을 알아보려면 www.anomali.com을 방문하거나 트위터에서 @Anomali를 팔로우하십시오.

808 Winslow Street, Redwood City, CA 94063