IBM Security

지능형 오케스트레이션

차세대 사고 대응 및 보안관제 프로세스

요약

업종에 관계없이 모든 보안 책임자들은 점점 늘어가는 과제에 직면하고 있습니다. 사이버 공격이 규모, 복잡성 및 정교함 측면에서 끊임없이 진화함에 따라, 사고 대응(IR)은 시간, 기술, 리소스 측면에서 한계에 부닥치고 있습니다. 또한 보안관제센터(SOC)는 평균 75개 이상의 다양한 보안 툴을 사용하므로 완벽한 가시성 확보는 거의 불가능한데다 이러한 툴을 통합하는 것 자체가 중요한 당면 과제가 되었습니다.

이런 이유로 지난 10년 간 보안팀은 보다 빠르고 정확하며 효과적으로 사고에 대응하고 이를 해결하는 능력을 최적화하기 위한 새로운 방법을 모색했습니다.

가트너[1] 연구에 따르면 보안관제 및 대응(Security Operations and Response, SOAR) 모델에는 세 가지의 필수적인 구성요소가 있습니다.

보안 오케스트레이션 및 자동화(Security Orchestration and Automation, SOA), 보안 사고 대응 플랫폼(Security Incident Response Platforms, SIR) 및 위협 인텔리전스 플랫폼(Threat Intelligence Platforms, TIP)이 있어야 합니다. IBM은 지능형 오케스트레이션(IO) 모델이 개선된 보안관제 및 사고 대응을 주도하는 3가지 요소(사고 대응, 인간 및 머신 기반 인텔리전스, 오케스트레이션 및 자동화)를 모두 결합한 모델과 유사하다고 믿고 있습니다.

IO 모델에 있어 관건은 인간 중심이라는 점입니다. 즉, 인간이 중심에 있으며 전략적 의사결정의 핵심입니다. 지능형 오케스트레이션은 인간 지능과 머신 기반 지능을 결합함으로써 사람, 프로세스 및 기술을 완벽하게 엮어 응답 시간을 단축합니다.

SOAR = SOA + SIR + TIP

ID: 325580

출처: 가트너(2018)년 2월

IBM Security

사고 대응 기술의 발전

현재 지능형 오케스트레이션이 차세대 사고 대응 솔루션으로 부상하고 있습니다. 지능형 오케스트레이션은 지능형 위협, 사고 발생 상황 및 인공 지능을 비롯한 머신 인텔리전스와 인간 컨텍스트(human context)를 결합하므로 표준 오케스트레이션 및 자동화 활동을 훨씬 앞설 뿐만 아니라 이를 통해 더욱 빠르고 정확한 의사결정을 내릴 수 있습니다. 지능형 오케스트레이션은 이러한 인텔리전스와 조직의 지식 및 절차를 결합하므로 모든 SOC 툴을 통합하여 가이드 대응(guided response)을 제공할 수 있습니다. 가이드 대응(Guided response)은 적절한 분석가 또는 임원이 올바른 정보를 적시에 받을 수 있도록 해주며, 대응 프로세스에 중점을 두기 때문에 사이버 공격자를 앞질러서 압도할 수 있도록 해줍니다.

지능형 오케스트레이션은 대응 프로세스를 통해 분석가를 이끄는 것 외에 팀이 인간 및 기술 인텔리전스를 통해 사고를 보강하도록 지원합니다. 결과적으로 분석가들은 기대 이상의 성과를 거두고 신입 직원의 역량 강화에 필요한 시간을 단축하며 개인에 대한 의존도를 최소화할 수 있습니다.

지능형 오케스트레이션은 베테랑 보안 분석가, HR, 법무팀 및 마케팅 팀을 비롯한 조직 전체의 전문지식이 접목된 반복 가능하고 문서화된 워크플로우를 제공하며, 지속적인 개선 및 성숙을 위한 토대를 제공합니다. 다양한 경험을 갖춘 분석가의 조치를 지속적으로 구체화하고 성문화하는 것 외에 프로세스를 조정하고 자동화하기 위한 새로운 기회 발굴에 시간을 할애하면 획기적인 결과를 기대할 수 있습니다. IBM Resilient 고객은 사고 해결에 필요한 평균 시간이 1시간에서 단 몇 분으로 단축되는 것을 경험했습니다.

본 백서에서는 보안 책임자가 시작 지점에 관계없이 조직 내에서 지능형 오케스트레이션 기능을 계획, 개발 및 유지보수하는 방법을 제시합니다. 또한 새로운 기술과 플랫폼을 좀 더 큰 맥락에서 평가할 수 있도록 적절한 정보 및 지침도 제공합니다.

개요

사이버 공격에 대비하고 대응하는 것은 모든 유형 및 규모의 조직에 가장 중요한 과제입니다. 사고 대응과 관련해서는 다음 5가지 주요 당면 과제가 새롭게 부상하고 있습니다.

끝을 알 수 없을 정도로 벌어지고 있는 기술 격차

널리 알려진 대로 사이버 보안 기술의 격차는 지난 10년 동안 꾸준히 넓어졌습니다. 2015년에 Frost & Sullivan은 2022년까지 150만명에 이르는 작업자의 기술 격차를 예상했지만, 최근의 글로벌 정보 보안 인력 연구에서는 180만명으로 추정치를 수정했습니다.

민감한 데이터의 보안을 강화해야 한다는 압박을 받고 있는 조직에게 이러한 기술 격차는 심각한 문제가 되고 있습니다. 보안 예산은 지난 10년 간 서서히 증가했지만 인적 자원의 가용성은 이에 상응해 증가하지 않았습니다. Ponemon Institute의 최근 연구에 따르면 다른 보안 분야와 관련된 대응의 경우 계속해서 예산 부족에 시달리고 있는 것으로 나타났습니다. 결과적으로 이러한 현실은 분석가가 더 많은 작업을 더 빠르고 효과적으로 수행할 수 있도록 지원하는 전력 강화 기술의 필요성을 제기합니다.

급증하고 있는 사이버 공격의 규모와 복잡성

기업들은 현재의 보안 요구에 대처하기 위해 고군분투하고 있지만 위협적인 환경은 끊임없이 변화하고 있습니다. Ponemon Institute의 악성 코드 봉쇄 비용 보고서(Cost of Malware Containment report)에 따르면 보통의 SOC는 평소 1주일에 17,000개에 달하는 악성 프로그램 경고를 로깅합니다. 결과적으로 하나의 SOC에서 매년 오탐(false positive) 추적에 무려 21,000시간을 소비하고, 130만 달러에 달하는 추정 비용을 사용하고 있습니다.

그와 동시에 이러한 경고 중 하나만으로도 비즈니스 운영에 상당한 혼란을 야기할 수 있습니다. 사이버 공격의 성공으로 인한 피해를 복구하기 위해서는 며칠에서 몇 주가 걸리며, 종종 평판 손상, 데이터 유출, 벌금 부과 등 추가적인 문제가 몇 개월 동안 지속됩니다.

그 어느 때보다 복잡해진 보안 환경

점점 더 많은 조직이 사이버 보안에 투자하고 강력한 SOC를 확장함에 따라 조직에서 배포하는 보안 기술의 평균 개수가 75개까지 증가했습니다.

이러한 툴의 관리 및 유지보수는 조직에 부담이 됩니다. SOC 전반에 걸친 효과와 가치에 대한 가시성을 확보하기가 어려우며, 분석가는 대응 중에 여러 툴을 끊임없이 전환해야 하므로 상당한 시간을 소비하게 됩니다.

분석가들이 감당하기 힘든 상황이 되면서 MTTD(평균탐지시간) 및 MTTR(평균해결시간) 증대

기술 격차의 확대와 빠르게 증가하는 위협의 규모가 보안팀을 압도하는 상황이 해결해야 할 과제를 더하고 있으며, 경우에 따라서는 직원들에게 극도의 피로를 초래하기도 합니다.

평균적으로 보안 분석가는 현실적으로 대처하기에 불가능할 정도로 많은 알림을 매일 받고 있습니다. 결론적으로 보안 사고의 해결에 필요한 시간은 지리적 위치에 관계없이 모든 업계에서 일관되게 열악합니다.

Verizon의 2017 데이터 침해 조사 보고서(DBIR)에서 소스 데이터6 분석에 따르면 상황은 아주 암울합니다. 평균 사고 탐지 시간은 4시간으로 상당히 짧지만 평균 해결 시간은 4일 이상입니다. 위협 행위자에게는 이러한 제약 조건이 없습니다. 대상 네트워크에서 초기 발판만 마련하면 보통 몇 분 내에 침해 시간을 측정할 수 있습니다.

점점 복잡해지는 데이터 침해 통보 규정, 변화하는 GDPR 사고 대응 요구사항

전세계, 국가 및 지역의 개인정보 침해에 대한 요구사항은 그 어느 때보다 복잡해지고 계속해서 진화 및 변화하고 있습니다. 개인정보보호 및 법무팀은 사고 후 규제 의무 충족에 며칠을 보내지만 해당 요구사항을 이행했는지 여부에 대해 100% 확신하지 못합니다. 결과적으로 오늘날 개인정보 침해에 대한 대응은 시간이 오래 걸리고 지루하며 비용이 많이 듭니다.

아마도 가장 큰 과제는 EU GDPR(General Data Protection Regulation)의 이행일 것입니다. 이 법은 EU 회원국 국민들의 개인정보 및 정보 손실을 다루는 기업에 새로운 과제를 안겨줍니다. 또한 기업이 데이터 침해 대응에 필요한 방법을 마련하기 위한 복잡성을 야기하기도 합니다. 특히 EU 회원국 국민들의 개인정보를 수집하는 전세계 모든 기업은 소재지가 EU이건 아니건 상관없이 관계 당국에 72시간 내에 침해사고를 통보해야 합니다. 그렇지 않으면 기업은 2천만 유로 이상 또는 연간 매출의 4%에 해당하는 벌금이 부과되는 위험에 처할 수 있습니다.

차세대 지능형 대응

사이버 인재를 찾고 복잡한 SOC 환경을 관리하는 일이 어려운 것도 사실이지만, 새로운 기술의 진보는 더 빠르고 효율적인 방법으로 사이버 위협의 분류, 조사 및 해결에 필요한 기술과 인텔리전스를 팀에 제공함으로써 실질적인 혜택을 제공합니다.

지능형 오케스트레이션(IO)은 위에서 설명한 문제를 독보적으로 해결할 수 있는 강력한 보안 기능입니다. 인간 및 머신 인텔리전스를 오케스트레이션 및 자동화와 결합함으로써 IO는 사이버 공격에 대한 대응을 대폭 가속화하고 강화할 수 있습니다. 이를 위해 사람, 프로세스 및 기술 전반에서 사고 대응의 복잡성을 단순화하여 조직이 더 빠르게 가치를 창출할 수 있도록 합니다.

IO는 보안팀에 사고를 처리, 추적 및 해결할 수 있는 중앙 허브를 제공하는 사고 대응 플랫폼(IRP)을 통해 지원됩니다. 강력한 IRP는 SIEM 및 EDR과 같은 보안 기술과 완벽하게 통합되며 위협 정보를 활용하여 사고를 보강합니다. 결과적으로 보안 담당자는 탐지 및 해결에 필요한 시간을 대폭 줄이는 이점을 얻을 수 있습니다.

지능형 오케스트레이션을 통한 보안 과제 해결

사고 대응은 SOC 운영의 가장 복잡한 부분입니다. 상호 연결된 수십 가지의 다양한 기술, 복잡한 IT 및 비즈니스 프로세스뿐 아니라 조직 전체의 인력이 개입하여 최고의 성능을 내는 사전 예방적이고 대응적이며 살아 있는 프로세스입니다.

지능형 오케스트레이션을 활용하면 보안팀이 사이버 공격자보다 한 수 앞서서 압도할 수 있도록 지원할 수 있습니다.

인간 및 인공 지능의 고유한 결합으로 사이버 위협 압도

지능형 오케스트레이션은 인공 지능과 인간 컨텍스트(human context)를 결합하므로 더 빠르고 정확한 의사결정을 가능하게 해줍니다. 인간의 측면에서 지능형 오케스트레이션은 베테랑 분석가, HR, 법무팀, 마케팅 팀 등 직원의 전문성을 IR 프로세스에 접목하여 이를 성문화합니다. 따라서 초보 분석가도 전문가와 동일한 조치를 취할 수 있게 됩니다.

또한 지능형 오케스트레이션을 통해 팀은 타사 솔루션을 통합할 수 있습니다. 이를 통해 분석가가 필요로 하는 정보를 적시에 제공함으로써 더 효과적인 의사결정을 내릴 수 있게 해줍니다.

지능형 오케스트레이션은 전문가급 프로세스와 기술 인텔리전스를 제공함으로써 가이드 대응을 지원합니다. 따라서 팀은 적절한 정보를 적시에 얻을 수 있습니다.

> Resilient와 Splunk의 통합으로... 프로세스에서 부족한 부분을 파악하고 수정하여 대응에 필요한 시간을 며칠에서 평균 몇 시간 미만으로 단축할 수 있었습니다.
>
> **사고 대응 관리자**
> 펜실베니아 주립 의과대학

SOC 툴 전체에 대한 오케스트레이션 및 자동화를 통해 사이버 공격 제압

지능형 오케스트레이션을 통해 보안팀은 대응 프로세스에서 가장 효과적인 작업을 자동화할 수 있습니다. 예를 들어, 팀은 반복적이고 시간이 많이 소모되는 분류 단계를 자동화하고 보강 작업을 조정함으로써 분석가가 중요한 의사결정을 보다 신속하게 수행하는 데 집중할 수 있게 해줍니다. 그리고 최적의 행동 방침이 결정되면 분석가는 지능형 오케스트레이션을 통해 사고를 종결하는 데 필요한 조치를 신속하게 취할 수 있습니다.

결과적으로 분석가는 점점 더 증가하는 경보 및 공격의 우선순위를 더 빠르게 지정하고, 중요한 사고를 정확하게 식별하며, 공격을 완벽하고 정확하게 조사하고 중단시키기 위한 올바른 조치를 취할 수 있습니다.

Resilient를 도입함으로써 새로운 위협 대응 시간이 84분에서 2분 미만으로 줄었습니다.

글로벌 제약 회사의 사이버 보안 담당자

적응성과 민첩성을 갖춘 동적 플레이북과 가이드 대응으로 사이버 공격자 압도

보안 사고는 완전하게 형식을 갖춘 상태로 나타나는 경우가 매우 드뭅니다. 즉 사고에 대한 상세 내용이 새롭게 밝혀지면 이에 대응하는 IR 플레이북이 필요합니다. 지능형 오케스트레이션의 핵심인 동적 플레이북(Dynamic Playbooks)은 조사 과정에서 IR 플레이북을 자동으로 조정하여 분석가가 최신 정보 및 프로세스를 활용하도록 합니다.

또한 통합 위협 인텔리전스, SIEM 및 EDR 툴을 사용하여 조정된 보강 작업을 통해 분석가는 공격자의 전술, 기술 및 절차를 신속하게 파악하고 이에 대응하기 위해 즉각적인 조치를 취할 수 있습니다.

Resilient의 IRP는 최신 사고 대응 사례 구축에 도움을 줄 만큼 충분히 능력 있고 맞춤 설정 가능한 유일한 선택이었습니다. Resilient IRP를 사용하면서 발견에서 복구, 종결에 필요한 평균 시간이 크게 단축되었습니다.

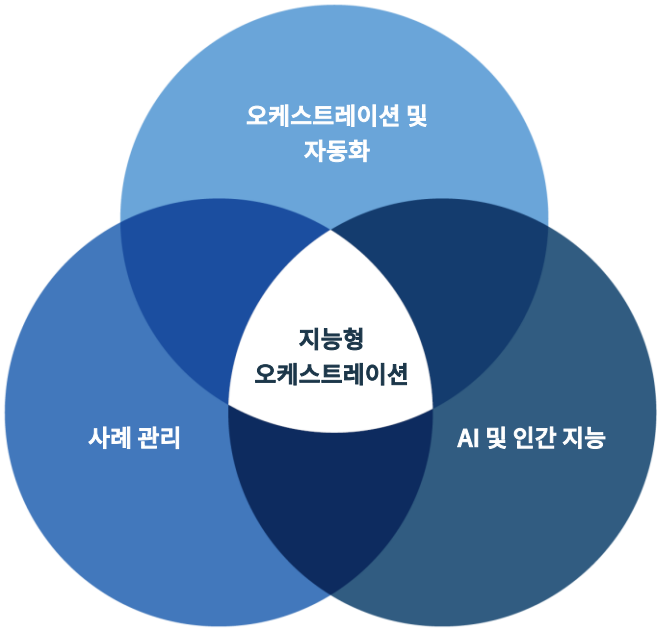
업계 선두 의료 센터 및 연구 시설의 사이버 보안 사고 대응 책임자

지능형 오케스트레이션 소개

앞에서 살펴본 것처럼 지능형 오케스트레이션(IO)은 인간 지능과 기술 인텔리전스의 조합입니다. 인간적 측면에서 지능형 오케스트레이션은 다양한 경험을 갖춘 보안 직원의 지식과 경험을 쉽게 반복할 수 있는 프로세스로 만들어 냅니다.

기술적인 측면에서 지능형 오케스트레이션은 절차 상의 막중한 부담을 머신으로 이전함으로써 분석가에게 인텔리전스를 제공하고 고부가가치 활동에 집중할 수 있는 시간을 확보할 수 있게 해줍니다.

다시 말해 IO의 목적은 대응 워크플로우를 통해 신속하고 민첩하게 분석가를 안내하는 것입니다. 또한 이러한 노력에 있어 기술 및 자동화가 중요한 역할을 하지만 사람과 프로세스에 대한 강력한 기초가 우선 마련되어야 합니다.



인텔리전스 오케스트레이션은 사고 대응 관리의 3가지 요소가 완벽하게 결합된 것입니다.

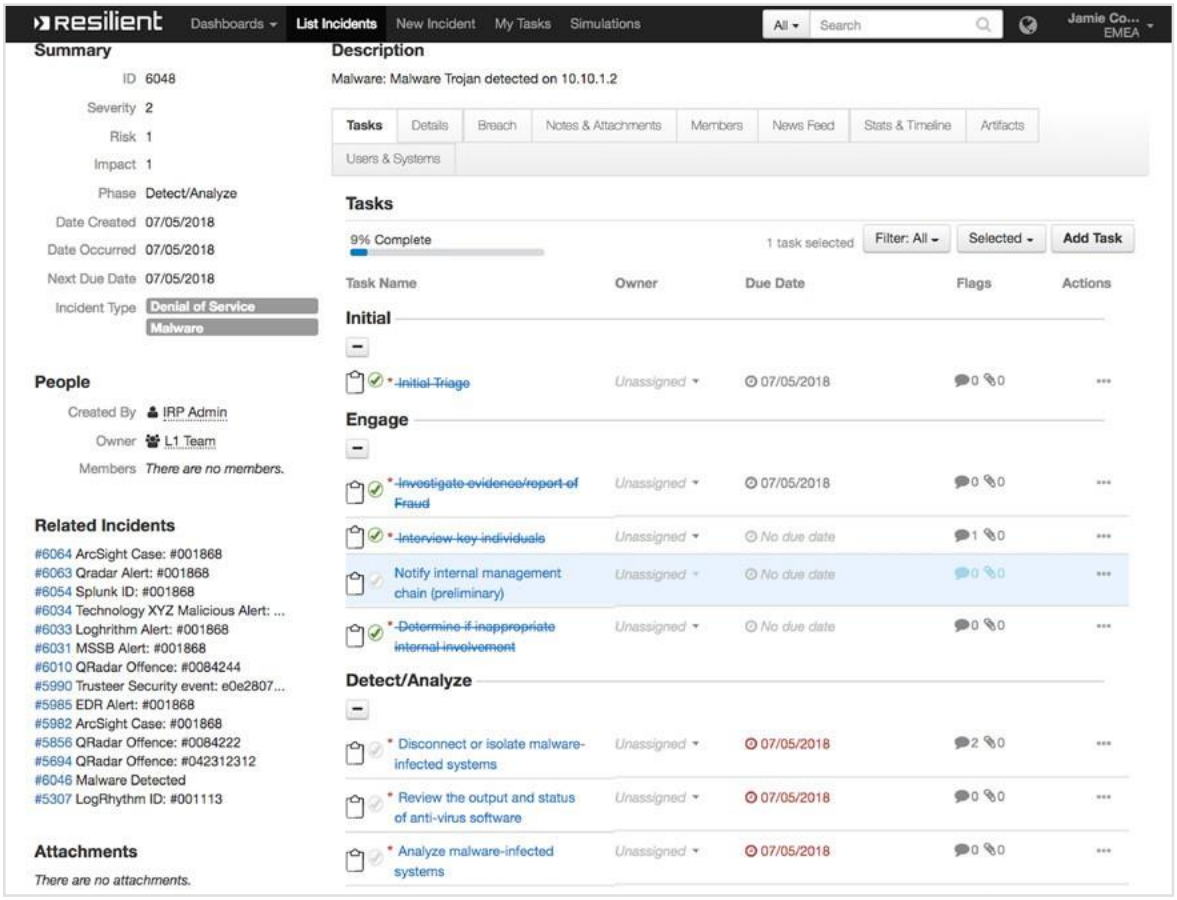
사람 → 프로세스→ 기술

사람과 프로세스

여기에서 설명하는 작업이란 문서화가 제대로 되어 있지 않고 몇몇 관계자들만 아는 지식(tribal knowledge)을 활용하여 다양한 경험을 갖춘 보안 직원의 업무를 신참 직원도 따라할 수 있도록 확실하고 반복 가능한 프로세스로 정리 및 성문화하는 것입니다. 이를 통해 조직은 개인에 대한 의존도를 낮추고 기술 과제의 측면에서 가장 중요한 새로운 분석가 교육에 필요한 시간을 단축하여 실무 처리에 대한 일관성을 높일 수 있습니다.

이와 같은 비즈니스 우선의 IR 접근 방식은 비즈니스 연속성 측면에서 큰 도움이 됩니다.

아래 그림은 Resilient IRP에서 가져온 것으로, 분석가를 위해 랜섬웨어 공격 대응 프로세스의 각 단계가 명확하게 정리되어 있습니다. 계획 단계에서 이러한 프로세스가 성문화 및 구체화되면 분석가는 사고를 즉시 철저하게 해결하기 위해 각 단계에서 취해야 할 조치를 정확하게 알게 됩니다.



지능형 오케스트레이션은 분석가에게 검증되고 반복 가능한 대응 프로세스를 통한 단계별 안내를 제공합니다.

랜섬웨어 공격 또는 보안 사고에 대응할 때에는 별도의 차별화된 조치가 필요하며, 그 중 일부는 IR 인력이 수행하고 나머지는 다른 팀에 전달되어야 합니다. 또한 일부 작업은 자동화에 적합하지만 다른 작업은 인간의 개입이 필요합니다.

IR 프로세스를 설계하고 공식화하는 과정이 필연적으로 이러한 요소를 강조하여 보여주므로 사용자는 IR 기능의 효율성을 강조할 수 있습니다.

기술: 보다 강력하고 인간 중심적인 자동화 실현을 위한 오케스트레이션의 첫 단계

IR 자동화는 엄청난 가치가 있습니다. 자동화를 통해 분석가는 반복적이고 시간이 많이 소모되는 업무 부담에서 벗어날 수 있으므로 2장에서 논의했던 3가지 주요 과제가 모두 해결됩니다.

그러나 모든 것이 자동화되는 것은 아니기 때문에 자동화는 지능형 오케스트레이션 전략의 맥락에서 가장 효과적으로 작동합니다. 그러나 일단 프로세스가 마련되면 보안팀은 전략적으로 자동화를 도입하여 중요한 단계를 간소화하고 사고 정보를 신속하게 분석가에게 제공할 수 있습니다.

SIEM, EDR, 티켓팅 시스템, 기타 IT 및 보안 툴 등의 기존 기술을 IRP와 통합함으로써 순수하게 관리에만 드는 엄청난 시간을 절약할 수 있습니다. 또한 지속적인 화면 전환이나 수동 데이터 전송 없이도 기술의 총력을 발휘할 수 있습니다.

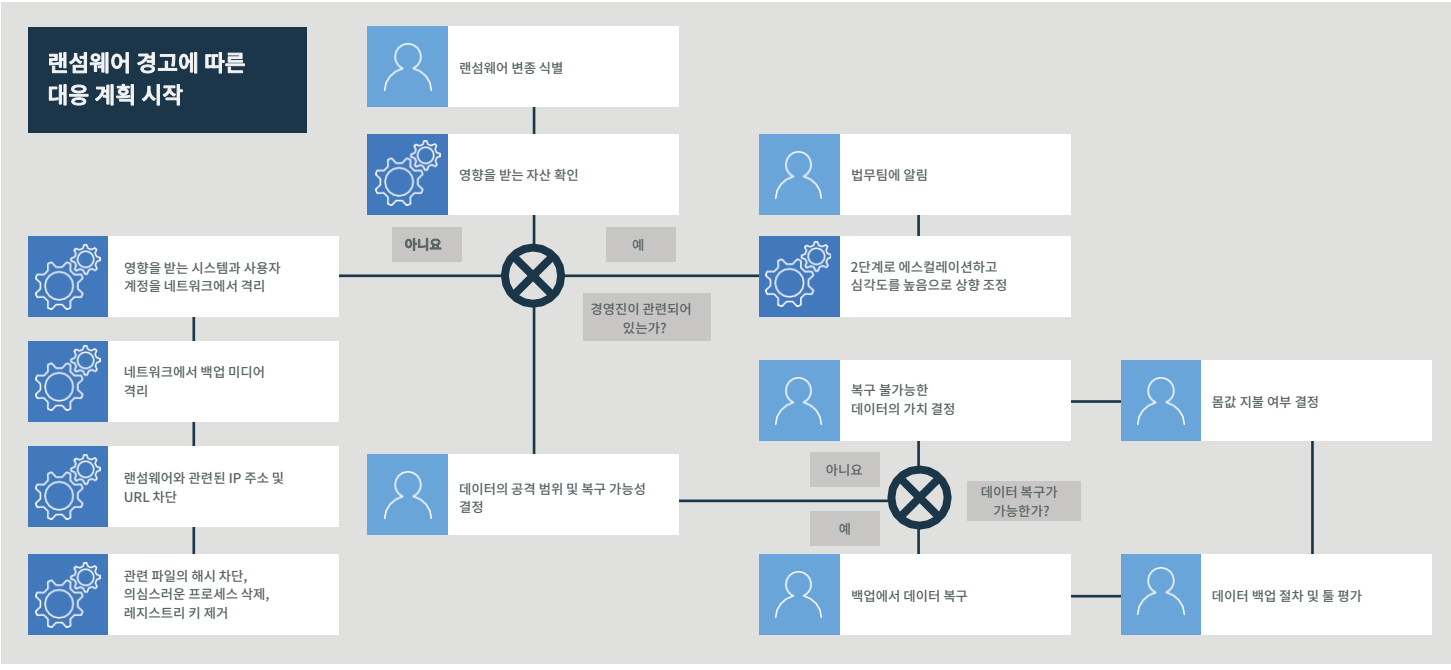
예를 들어, 시간이 가장 많이 소모되는 사고 대응 단계 중 하나는 분류이며 위협 인텔리전스 툴이 중요한 역할을 할 수 있습니다.

하지만 문제는 많은 보안팀들이 여전히 잠재적인 악성 이벤트를 수작업으로 찾은 후, 시간을 들여 위협 피드를 검색하여 의혹을 확인해야 한다는 점입니다. 이벤트당 몇 분 또는 그 이상 걸릴 수 있으므로 소중한 시간을 낭비하게 됩니다.

지능형 오케스트레이션을 사용하면 침해지표(IOC) 또는 기타 아티팩트가 탐지 제어 기술(SIEM, EDR 등)과의 통합을 통해 자동으로 IRP로 전달되고 통합된 위협 인텔리전스 피드가 자동으로 배포되므로 연결된 아티팩트 기반의 중요한 컨텍스트로 보안 사고를 보강할 수 있습니다. 이렇게 하면 보안 담당자가 더 이상 위협 피드에 수작업으로 액세스할 필요가 없으므로 상당한 시간을 절약할 수 있으며 동시에 인적 오류의 가능성이 줄어듭니다.

자동화에 적합한 작업을 파악하려면 먼저 사고 분류, 방화벽 또는 필터 규칙 업데이트, 악의적인 해시 금지 등과 같은 단순하고 반복적인 작업을 찾아야 합니다. 플레이북에는 인간의 의사결정이 필요한 지점들이 곳곳에 끼어 있으므로 자동화를 통해 이러한 지점까지, 그리고 이후 대응 작업이 진행되어야 합니다.

아래의 그림에는 랜섬웨어 공격에 대응하는 간단한 프로세스가 나와 있습니다.



지능형 오케스트레이션은 사고 정보가 밝혀짐에 따라 실시간으로 대응 계획을 조정하는 동적 플레이북을 갖추고 있습니다.

악성 프로그램 변종을 식별하고 공격 범위를 결정하는 작업에는 분석가의 상당한 개입이 필요합니다. 기술이 이러한 프로세스를 가속화하고 필요한 정보를 제공하지만 이러한 영역에서 자동화에만 의존하는 것은 매우 위험합니다.

반면, 인간이 개입하는 의사결정 지점에서 발생한 작업은 결정된 사항에 따라 자동화할 수 있는 경우가 많습니다. 일단 악성 프로그램 변종이 확인되면 버튼 클릭만으로 연결된 해시를 금지하고 IP 주소를 차단할 수 있습니다.

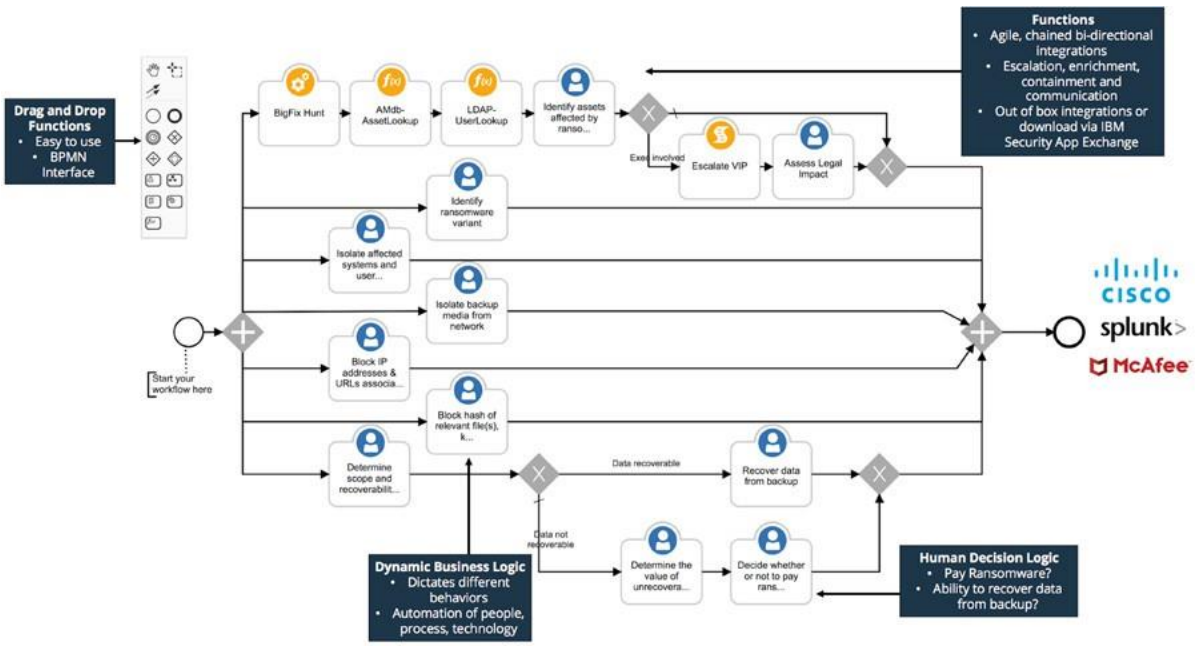
지능형 오케스트레이션의 기술은 사고에 대응하고, 인간의 개입이 필요 없는 프로세스의 측면을 처리하며, 중요한 의사 결정에 필요한 정보와 컨텍스트를 제공하는 프로세스를 통해 분석가에게 올바른 방향을 제시해야 합니다.

지능형 오케스트레이션을 통한 자동화 및 통합 가속화

지능형 오케스트레이션 기능을 포함한 IRP를 통해 코딩 및 스크립팅 작업 없이도 플레이북과 통합을 구축 및 관리할 수 있으므로, 지능형 오케스트레이션 기능을 활용하면 통합 및 자동화된 플레이북을 생성하고 유지하는 과정이 대폭 간소해집니다.

이는 지능형 오케스트레이션이 여러 플레이북에 적용하여 재사용할 수 있는 엔터프라이즈급 통합 기능에 의존하기 때문입니다. 보안팀은 업계 표준 비즈니스 프로세스 관리 표기(BPMN) 기반의 간단한 드래그 앤 드롭 방식 인터페이스로 이러한 플레이북을 설계할 수 있습니다. 또한 지능형 오케스트레이션에는 함수들을 중첩/모듈 방식으로 결합하여 구성요소화하는 기능이 포함되어 있습니다. 이러한 방식으로 조직은 구성요소들을 한 번 정의한 후 필요에 따라 구성요소들을 짜맞출 수 있습니다. 예를 들어, 보안팀에서 새로운 툴이나 개선된 표준 운영 절차를 기반으로 악성 프로그램 처리 프로세스를 업데이트해야 한다면 이러한 방식을 통해 악성 프로그램 워크플로우를 간단히 업데이트할 수 있습니다. 랜섬웨어 등에 대해 호출하는 모든 워크플로우는 새 버전을 호출하게 됩니다.

이와 같이 단순하면서도 강력한 성능의 인터페이스를 통해 보안팀은 인간의 개입이 필요한 작업과 의사결정을 기술적 통합 및 자동화와 완벽하게 결합시킨 강력한 IR 프로세스를 신속하게 구축할 수 있습니다. 이러한 강력하고 복잡한 워크플로우를 동적 플레이북(Dynamic Playbooks)이라고 합니다.



지능형 오케스트레이션을 통해 보안팀은 드래그 앤 드롭 방식의 편집기 기반으로 사람, 프로세스 및 통합을 지원하는 강력한 IR 워크플로우를 빠르고 간편하게 구축할 수 있습니다.

동적 플레이북(Dynamic Playbooks)

지능형 오케스트레이션을 통해 사람, 프로세스 및 기술을 강력한 IRP 안에서 상황에 맞춰 동적으로 적응하는 플레이북으로 코드화할 수 있습니다. 이러한 동적 플레이북은 사고를 해결하고 진행 상황을 추적하며 조직 전체의 팀 또는 개인에게 업무 할당을 용이하게 하는 프로세스를 통해 보안 분석가에게 가이드 역할을 합니다.

동적 플레이북은 코드화된 조치를 기반으로 일관된 사고 대응을 보장함으로써 대응 프로세스를 표준화하므로, 각각의 대응은 가장 숙련된 분석가가 지시한 것과 마찬가지로 취급됩니다. 또한 동적 플레이북은 보강(enrichment) 활동을 통해 드러나는 사고의 상세 내용이나 공격 변화에 실시간으로 대응하여 IR 프로세스의 단계를 추가, 제거 또는 편집합니다.

예를 들어, 악성 프로그램 사고를 조사하는 과정에서 경영진의 노트북이 감염되었다고 판단되면 대응의 본질이 변경됩니다. 이 사고를 더 높은 우선순위로 에스컬레이션해야 하고 법무팀에 민감한 정보가 위험한 상태에 있음을 알려야 합니다. 동적 플레이북을 사용하면 이러한 단계가 실시간으로 대응 플레이북에 자동으로 추가되므로 분석가는 전문가 수준의 완벽한 해결책으로 사고를 해결할 수 있습니다. 동적 플레이북은 이러한 방식으로 분석가가 빠르고 효율적으로 사고에 대응할 수 있도록 가이드 대응을 지원합니다.

실무 측면의 지능형 오케스트레이션 이점

실제 보안 환경에서 지능형 오케스트레이션이 작동하는 방식을 이해하려면 아래의 간단한 사용 사례를 살펴보시기 바랍니다.

우선, EDR이 외부 서버로의 연결을 시도하는 의심스러운 프로세스를 식별합니다. 이 사고를 수작업을 통해 직접 조사하려면 분석가는 다음을 수행해야 합니다.

- 모든 관련 이벤트를 .csv 파일로 가져오는 SIEM 쿼리를 작성하여 실행
- 의심스러운 프로세스의 MD5 해시를 식별하고 적절한 위협 인텔리전스 피드에서 조사
- 악의적인 프로세스로 확인되면 엔드포인트의 백업을 작성한 후 해당 프로세스를 네트워크의 나머지 부분과 분리시킨 다음 AV 스캔 실행
- 사고 레코드를 업데이트한 후 모든 관련 로그 파일, 메모 등을 첨부

분석가가 이 프로세스를 수행하려면 30분 이상이 소요되지만, 지능형 오케스트레이션을 사용하면 이 프로세스 중 많은 단계가 간소화되므로 분석가는 사고를 완벽하게 해결하는 데 필요한 통찰력을 신속하게 얻게 됩니다.

- EDR이 의심스러운 프로세스를 식별하고 IRP에서 사고를 자동으로 생성합니다.
- SIEM이 자동으로 쿼리되고 관련 정보가 사고에 추가됩니다.
- 이 사고의 IOC를 위협 피드와 비교하여 악의성이 있음을 확인합니다.
- 이러한 인텔리전스를 기반으로 이 사고는 악성프로그램 공격으로 분류되며 관련 동적 플레이북이 적용됩니다.
- 백업 작성부터 엔드포인트 격리, AV 스캔 실행에 이르는 표준 프로세스가 자동으로 시작됩니다.
- 모든 단계의 감사 추적 기록이 자동으로 보관됩니다.

분석가가 추가 쿼리를 수행하거나 추가 조치를 취해야 하는 경우에도 더 이상 화면 전환, 수동 기록 보관, 번거로운 수작업을 할 필요가 없습니다. 이것만으로도 사고 건당 15~30분이 절약됩니다.

> CISO를 지원하는 데 있어서 핵심은... 보안 인프라 전체에 대한 가시성을 확보하여 보안 사고 해결 과정에서 더 나은 의사결정을 내릴 수 있도록 하는 것입니다. 이러한 가시성을 기반으로 이사회, CFO 및 CEO와 보안 프로그램의 방향에 대해 보다 전략적이면서도 리스크에 기반한 대화를 나눌 수 있게 되었습니다.
>
> **Lawrence Pingree, 가트너 리서치 부문 VP**

IBM Security

사용 사례: 평균 대응 시간 97% 단축

글로벌 제약회사, 지능형 오케스트레이션으로 사고 해결 시간을 84분에서 2분 미만으로 단축

당면 과제

시장을 선도하는 세계적 제약회사가 문제 해결을 위해 IBM Resilient의 문을 두드렸습니다. 이 회사에는 전세계에 4개로 나눠진 보안팀이 있으며 각 팀은 자체 프로세스와 기술로 연간 5,000건의 사고에 대응하고 있었습니다. 사고 대응을 위한 중앙 집중식 플랫폼이 없었으며 주요 의사결정권자들이 새로운 위협에 뒤쳐지지 않도록 고군분투해야 했습니다.

이 회사의 글로벌 정보 보안 책임자는 "협업, 커뮤니케이션 및 기록 관리에 어려움을 겪었고, 팀이 보유하고 있는 기술 중 어느 것도 서로 통신이 불가능했으며, 협업이라고 해봐야 세 가지 다른 시스템에서의 조치를 문서화하는 것이어서, 결국 일을 세 번 하는 것이나 마찬가지"라고 설명했습니다.

특히 시급한 처리가 필요했던 개인정보 사고가 발생했을 때 4개의 보안팀이 동시에 대응했습니다. 각 팀은 자체 결론에 도달했고 각기 다른 제안을 제시했습니다. 결국 적절한 의사소통의 부재로 IT 팀은 상황을 악화시키기만 했던 데이터를 삭제할 것을 요청받았고 파일을 복구하는 추가 작업을 해야만 했습니다.

이러한 상황을 모두 감안할 때 이 회사에는 세 가지 주요 당면 과제가 있었습니다.

1. 높은 사고 빈도 - 연간 5,000건 이상
2. 전체적으로 일관성이 없는 대응 팀 프로세스
3. 소통, 가시성, 감사 추적의 부재

해결책

이러한 문제를 해결하기 위해서는 우선 서로 단절되어 있는 보안팀뿐만 아니라 기술 및 프로세스의 조정이 필요했습니다.

이 문제에 지능형 오케스트레이션 접근 방식을 적용하면 보안팀은 새로운 사고에 대한 조치를 신속하게 취하고 혼란과 커뮤니케이션 오류를 없애며 IR 및 관련 문서화 작업에 협업적이고 일관성 있는 접근 방식을 활용할 수 있습니다.

보안 책임자는 "우리에게 오케스트레이션은 보다 빠르고 민첩해진 상황에서도 잘 조정된 상태를 유지할 수 있게 해주는 방법"이라고 설명했으며, "우리는 역할 및 책임에서부터 데이터 기록에 이르기까지 세부 사항을 모두가 이해할 수 있도록 표준화하기 위한 방법을 모색"했다고 덧붙였습니다.

IR의 전사적 핵심 허브로 Resilient IRP를 구축하였습니다. Resilient IRP를 사용하여 이 기업은 다음을 수행할 수 있었습니다.

- 자동 생성된 감사 추적과 분석가 및 경영진을 위한 통합적인 가시성을 통해 중앙에서 대응 활동 조정
- 표준화된 IR 프로세스를 개발하고 코드화하여 보안팀이 협업을 수행하고 사고에 강력하고 일관되게 대응할 수 있도록 지원
- 조직 전체를 대상으로 개인 및 팀에 업무를 할당하여 중복 업무 제거
- 기존의 보안 기술을 대응 프로세스에 통합하는 동시에 반복적이고 시간 소모적인 수작업을 자동화

보안 책임자는 "Resilient IRP를 통해 우리 팀은 혼란과 시간 낭비를 줄이면서 톱니바퀴 같은 조직력으로 협업하고 있고, 사고 대응 시 우리는 분석가 조치의 60%를 Resilient를 통해 완료할 수 있어, 더 이상 5~6 가지 툴을 사용하면서 시간을 낭비하지 않아도 됩니다." 라고 같이 밝혔습니다.

결과

이 회사는 Resilient IRP를 도입하면서 보안팀 간의 협업에 상당한 개선 효과를 거두었습니다. 대응 프로세스에 대한 가시성이 크게 향상되어 신입이나 초보 분석가들도 상급 분석가에게 요구되는 기술을 신속하게 습득할 수 있게 되었습니다.

분석가들은 12 가지가 넘는 보안 기술과의 양방향 통합을 통해 화면 전환이나 수동 전송 없이도 필요한 거의 모든 것에 액세스할 수 있습니다.

또한 Resilient IRP를 통해 4개 보안팀 모두에 대해 IR 시뮬레이션을 실행할 수 있으므로, 팀은 이전에 문제를 야기했던 사고를 가지고 해결 과정을 훈련할 수 있습니다.

보안 책임자는 **"Resilient는 더 나은 IR을 위한 우리의 장기적인 노력에 가장 적합한 도구이며, 이 플랫폼을 통해 모의 훈련을 실시하여 직원을 교육하고 워크플로우를 훈련해 볼 수 있었습니다. 결과적으로 4개의 보안팀이 모두 효과적으로 성과를 거두고 있습니다."** 라고 강조했습니다.

궁극적으로는 가장 명백한 이점인 시간 절약이 주목을 받았습니다. 개선된 프로세스, 원활한 통합 및 자동화를 결합함으로써 일반적인 사고 해결에 걸리는 시간을 줄일 수 있었습니다. 이 회사의 글로벌 정보 보안 책임자는 "Resilient를 도입함으로써 새로운 위협에 대응하는 데 필요한 시간이 84분에서 2분 미만으로 줄었습니다." 라는 말로 인터뷰를 끝맺었습니다.

요약

보안팀이 오늘날 최고의 보안 문제에 대처하도록 지원하기 위해 지능형 오케스트레이션은 변화하는 사고 대응에 대한 획기적인 플랫폼을 제공하여 팀이 사이버 공격자보다 앞서서 압도할 수 있도록 해줍니다.

지능형 오케스트레이션의 이점은 다음과 같습니다.

- 적시에 담당자에게 올바른 정보를 제공하는 가이드 대응
- 인간의 의사결정 및 컨텍스트와 결합된 인공 지능 속도
- SOC 전반에 대한 즉각적인 가시성
- 보다 빠른 가치 실현 시간
- 민첩하고 재사용 가능한 플레이북 구성요소

지능형 오케스트레이션 플랫폼에 대한 구매자 가이드

시간이 지남에 따라 사고 대응 플랫폼 업계의 성숙도는 한층 높아졌으며, 점점 더 다양해지는 자동화 및 사례 관리 기능에 대한 솔루션을 제공하는 공급업체들도 함께 성장하고 있습니다. 많은 공급업체들이 사고 대응 범위 내에서 특정 분야를 지원하는 툴을 제공하고 있지만 사례 관리, 오케스트레이션 및 자동화, 인텔리전스의 완벽한 조합을 제공하는 업체는 거의 없습니다.

다음은 현명한 투자를 위해 공급업체를 평가할 때 확인해야 하는 9가지 질문입니다.

1. 플랫폼이 인적 측면과 프로세스 측면의 발전을 촉진하나요?

사람과 프로세스의 오케스트레이션은 성공적인 IR에 필수 요소입니다. 동적 플레이북 및 시각적 프로세스 매핑과 같은 기능은 IR 프로세스를 구체화하고 분석가의 기술을 발전시키는 데 도움이 됩니다.

2. 자동화를 통해 신속하고 효과적인 사고 대응을 지원하나요?

분석가의 압도적인 업무량은 보안 세계에서 커다란 도전 과제이지만 IR에서보다 더 절실하게 느껴지는 곳은 없습니다. 강력한 지능형 오케스트레이션 플랫폼은 통합 및 자동화를 통해 화면 전환과 같은 반복적인 업무의 부담을 줄여줍니다.

또한 IR 프로세스를 통해 하급 분석가에게도 가이드를 제시하므로 혼자 감당할 수 있는 수준을 넘어서는 새로운 업무를 맡을 수 있도록 힘을 실어줍니다.

3. IR 프로그램 효과를 추적 및 측정하는 시스템이 제공되나요?

보고와 분석은 정상 상태의 보안 기능에 필수 요소이며 ROI의 증거를 제공하고 개선이 필요한 부분을 강조하여 위험 관리 전략을 알려줍니다. 지능형 오케스트레이션 플랫폼에서는 미리 설정된 포괄적인 템플릿과 자체 템플릿 생성 옵션을 포함하여 세분화된 수준의 광범위한 보고 옵션을 즉시 사용할 수 있습니다.

4. 사고에 법무팀, HR, 마케팅 또는 임원진 개입이 필요한경우 이들에게 사고를 에스컬레이션할 수 있는 규칙 기반 시스템이있나요?

일부 사고 유형의 경우 법무팀 또는 고위 임원진의 즉각적인 개입이 필요합니다. 이러한 유형의 사고가 식별되면 플랫폼에서는 자동으로 해당 팀에 통보하고 지체없이 사건에 대한 자세한 설명을 제공해야 합니다.

5. 기존 보안 및 IT 툴과 통합되나요?

IR 기능의 가치를 극대화하려면 지능형 오케스트레이션 플랫폼은 다양한 타사 및 커뮤니티 기반 애플리케이션을 포괄할 수 있는 "오케스트레이션 에코시스템"에 적합해야 합니다.

예를 들어, IR 분석가가 직면한 가장 큰 과제 중 하나는 보안 기술 간에 데이터를 끊임없이 전환하고 전송해야 한다는 점입니다. 오케스트레이션 에코시스템과 완벽하게 통합되는 지능형 오케스트레이션 플랫폼은 이 문제를 완화하고 분석가가 전략적 활동에 시간과 노력을 집중할 수 있게 해줍니다.

시작 지점으로서 플랫폼은 EDR 및 SIEM과 같은 일반적인 보안 툴과 통합되어야 합니다. 이것 외에도 IR 기능의 특정 요구사항을 고려하여 실질적인 개발없이 기존의 모든 보안 기술과 통합되는 플랫폼을 조달해야 합니다.

6. 팀에서 인간의 개입이 필요한 업무, 통합 및 자동화를 결합한 IR 워크플로우를 구축할 수 있나요?

IR 프로세스는 끊임없이 진화하고 개선되어야 합니다. 지능형 오케스트레이션 플랫폼은 개별 작업을 자동화하거나 관련 직원에게 할당함으로써 이 프로세스를 촉진합니다.

7. 상황에 맞는 관련 위협 인텔리전스를 활용하나요?

위협 인텔리전스(threat intelligence, TI)는 IR에 가장 요긴한 것으로, 분석가가 가장 긴급한 사고에 대한 우선순위를 지정하는 데 도움을 주고 다양한 유형의 위협에 대처할 수 있는 최상의 방법에 대한 통찰력을 제공합니다. 지능형 오케스트레이션플랫폼은 TI를 직접 수집하고 자동으로 사고를 보강하기 위해이를 사용하여, 분석가가 위협 피드를 수작업으로 구문분석할때 걸리는 시간을 줄여줍니다.

8.업데이트나 커스터마이즈가 신속하고 쉽게 이루어지나요?

앞서 언급한 바와 같이 지속적인 개선은 장기적인 사고 대응 성공의 열쇠입니다. 보안팀에서 관리하고 IR 프로그램의 발전에 맞춰 업데이트되는 IRP는 이러한 개선 사항이 반영되도록 하는 데 많은 도움이 됩니다. 여기에는 역할, 책임, 소유자 업데이트, IR 플레이북, 보고 대시보드, 자동화된 워크플로가 포함됩니다.

9.조직 간 협업을 지원하나요?

IR은 폐쇄 루프 프로세스가 아닙니다. 법무팀, HR 및 마케팅 등 조직 내 다른 부서의 도움을 받는 것이 업무에 유용하며, 사고가 해결될 때까지 사고가 IR과 IT 헬프데스크 간을 오고 가는 것도 필요할 수 있습니다. 이런 이유로 헬프데스크 소프트웨어와의 통합은 매우 중요합니다.

10. 플랫폼에 개인정보 보호 규정 및 데이터 침해 통보 워크플로가 포함되어 있나요?

데이터 침해 통보 규정은 전 세계에서 지속적으로 진화하고 있으며 이러한 규정의 추적 및 준수는 그 어느 때보다도 복잡해졌습니다. 개인정보 보호 및 법무팀은 사고 후 규제 의무를 충족하는 데 수 일을 보내지만 해당 요구사항을 이행했는지 여부에 대해 100% 확신하지 못할 수 있습니다. EU GDPR(General Data Protection Regulation)의 등장으로 위험 요소와 복잡성이 전보다 훨씬 커졌습니다.

IRP는 최신 규정에 즉시 대처하는 대응 계획뿐만 아니라, 조직의 지속적인 규제 준수 상태에 대한 컨텍스트를 제공하는 새로운 규정에 대한 자동 알림 기능을 제공하여 데이터 침해 알림 요구사항을 이행하는 데 요구되는 복잡성을 줄일 수 있습니다.

11. 공급업체가 비즈니스파트너로서 가치를 제공하나요? 신뢰할 만한 실적이 있나요?

IR 소프트웨어 분야는 비교적 신생 시장이므로 의사결정을 내리기 전에 잠재적 공급업체에 대해 철저한 조사를 하는 것이 도움이 됩니다. 고려 중인 공급업체가 있다면 우려사항을 해소하기 위해 그들의 고객과 미팅을 가져보는 것도 좋은 방법입니다.

IBM Security

Resilient IRP 데모에 등록하여 IBM Resilient의 지능형 오케스트레이션을 통해 사이버 공격에 대해 사전에 대응하는 방법을 알아보세요.

대응 프로세스에 대한 오케스트레이션 기능을 통해 보안팀이 더 빠르고 지능적으로 조치를 취할 수 있도록 지원하세요.

지금 바로 Resilient 사고 대응 플랫폼(IRP)의 데모를 예약하세요
(문의: 02-3781-7332)

출처

1. Preparing Your Security Operations for Orchestration and Automation Tools. – 가트너 연구, 2018년 12월
2. Global Information Security Workforce Study - Center for Cyber Safety .... https://iamcybersafe.org/gisws/. 2018년 3월 8일 확인.
3. IT budget research 2018: Funding and spending ... - Tech Pro Research. http://www.techproresearch.com/downloads/2018-it- budgets/. 2018년 3월 8일 확인.
4. 제3차 기업의 사이버 복원력에 관한 연례 보고서 – Ponemon Institute, 2018년 3월
5. The Cost of Malware Containment - Ponemon Institute. 2016년 1월 26일, https://www.ponemon.org/blog/the-cost-of-malware-containment. 2018년 3월 27일 확인.
6. Incident discovery and containment: Average is over. | Verizon Insights. 2017년 7월 21일, http://www.verizonenterprise.com/verizon-insights-lab/VES/incident-discovery-and-containment- average-is-over-. 2018년 3월 8일 확인.
7. 가트너 보도자료: Gartner Says Detection and Response is Top Security Priority for Organizations in 2017. 2017년 3월 14일, https://www.gartner.com/newsroom/id/3638017. 2018년 3월 12일 확인

IBM Resilient 소개

IBM Resilient는 사이버 공격이나 비즈니스 위기 상황에서도 조직이 계속해서 번창할 수 있도록 지원하는 데 있어서 업계 선두주자입니다. IBM Resilient의 입증된 사고 대응 플랫폼(Resilient IRP)은 보안팀의 역량을 강화하여 사고를 보다 빠르고 지능적이며 효과적으로 분석, 대응 및 완화할 수 있도록 지원합니다. Resilient IRP는 업계 유일의 지능형 오케스트레이션 플랫폼으로, 이를 통해 보안팀은 사람, 프로세스 및 기술을 단일의 개방형 사고 대응 허브에서 통합하고 자동화할 수 있습니다. Resilient를 통해 보안팀은 동급 최강의 대응 기능을 갖출 수 있게 됩니다. IBM Resilient는 Fortune 500대 기업 중 60개 기업 및 전세계 수백 곳의 파트너를 비롯하여 300개에 이르는 글로벌 고객을 보유하고 있습니다. www.resilientsystems.com 에서 자세한 내용을 알아보십시오.