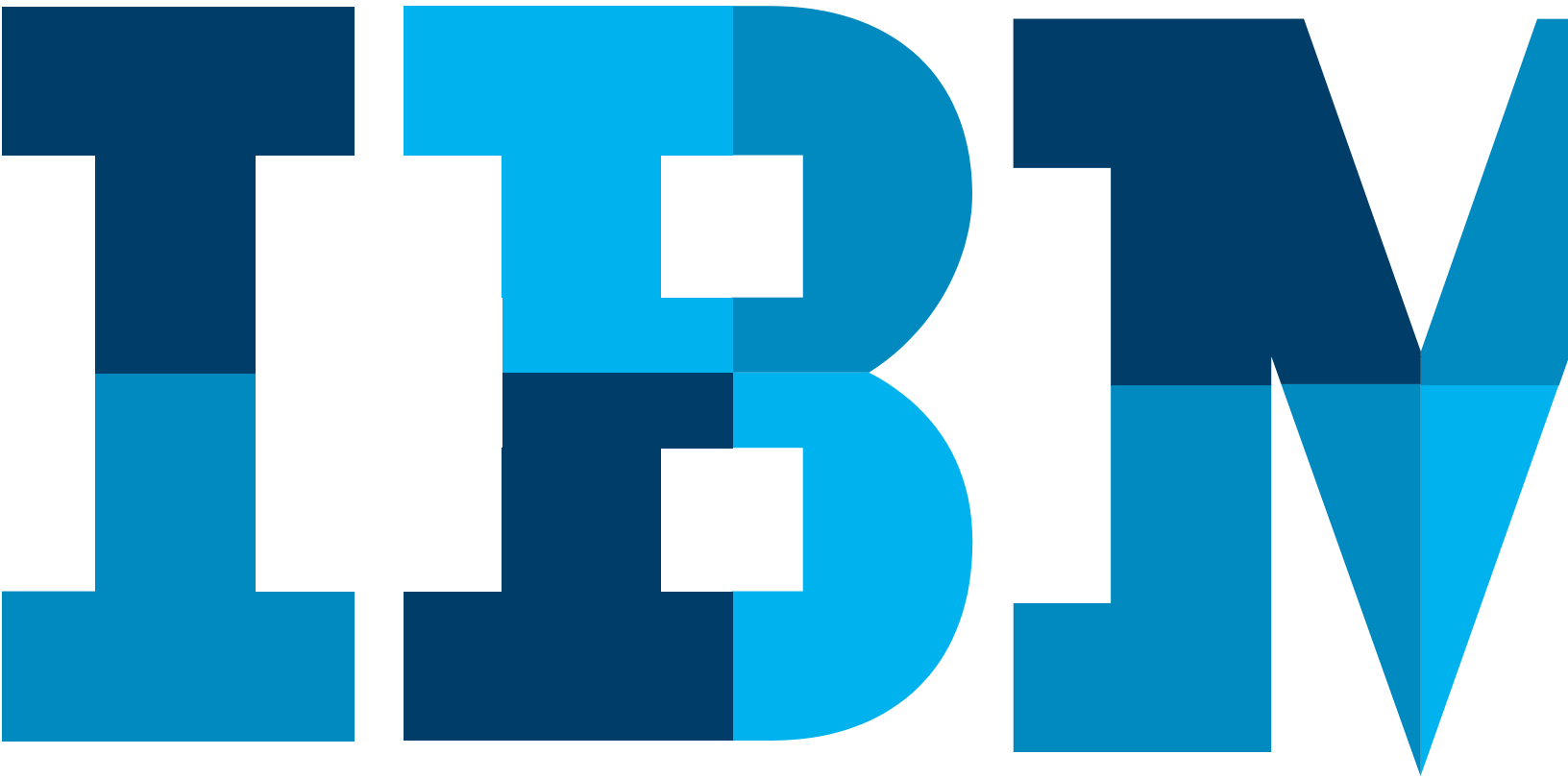
IBM Security

백서

강력한 침해사고 대응 체계를 구축하는 6단계

침해사고 대응의 과제



IBM

목차

서론: IR이 중요한 시대

전 세계의 기업들이 사이버 공격을 탐지하고 차단하는 노력만으로는 사이버 보안 위협으로부터 확실히 보호받을 수 없음을 깨닫고 있습니다. 이런 이유로, 침해사고 대응(Incident Response, IR) 프로세스를 관리, 조정, 간소화하기 위한 플랫폼을 보안팀에게 제공하고자 IBM Resilient®가 개발되었습니다.

IBM Security는 다양한 규모 및 업종의 기업들이 Resilient 솔루션을 적용하여 더 정교하고 강력한 IR 기능을 개발하도록 지원해 왔습니다. 이들은 임시용이 아닌 일관성 있고 반복 가능하며 측정 가능한 IR 프로세스를 개발하며, 전사적 차원에서 소통, 조정, 협업을 우선 과제로 여깁니다. 또한, 대응 팀이 더 빠르고 정확하게 임무를 수행하도록 뒷받침하는 기술을 활용합니다.

그러나 더 강력한 IR 프로그램을 개발하고 관리하는 데 걸림돌이 되는 문제가 있습니다. 그 중에서도 특히 중요한 3 가지는 아래와 같습니다.

1. **늘어나는 사이버 보안 침해사고** Enterprise Strategy Group에 따르면, 사이버 보안 전문가의 42%는 소속 회사에서 감당하기 어려운 양의 보안 경보가 발생하기 때문에 그중 상당수를 무시하고 있음을 지적합니다[1].
2. **인력 확보에 어려움을 겪는 보안팀** CyberSeek에 따르면, 2016년 기준으로 20,000개의 사이버 보안 관련 일자리가 충원되지 못한 상태입니다[2].
3. **효과적으로 대응하기에는 너무 복잡하고 준비되지 않은 조직** 부실한 계획과 준비 그리고 IT/비즈니스 프로세스의 복잡성이 사이버 공격 대응을 어렵게 하는 최대 장애물입니다[3].

많은 IBM Resilient 고객은 이러한 문제를 해결하기 위해 사람, 프로세스, 기술을 조정하는 데 힘쓰고 있습니다. 그러한 조정이 이루어지면 IR 분석가가 어떤 임무의 책임자, 완료해야 할 시점과 수행 방식을 파악할 수 있게 됩니다. 이 새로운 개념을 IR 오케스트레이션이라고 합니다.

IR 오케스트레이션은 보안 분석가가 IR 프로세스 및 툴을 자유자재로 구사할 수 있도록 힘을 실어 줍니다. IR 오케스트레이션 덕분에 보안 분석가는 중대한 침해사고 정보에 신속히 액세스하고 정확히 판단하며 결단력 있게 조치할 수 있습니다. 자동화를 활용하여 보안 분석가 및 기술의 생산성을 높임으로써 전문성 공백을 해소하고 보안 경보의 양을 줄입니다.

IR 오케스트레이션은 제품이 아니라 프로세스입니다. 탄탄한 기초 요소, 즉 숙련된 인력, 검증된 프로세스, 통합된 기술이 있어야 합니다. 오케스트레이션은 이러한 핵심 요건을 기반으로 하며, 어떤 조직의 오케스트레이션 실효성은 전적으로 이 기초 요소의 품질에 좌우됩니다.

IR 성숙도 평가

IBM Resilient 고객은 지난 몇 년간 성숙도 스펙트럼의 여러 단계를 거치면서 더 발전된 IR을 정립해 왔습니다. 대개 산업, 가용 자원 또는 경험의 차원에서 성숙도가 요구되지만, IBM Resilient 고객 대부분은 IR 기능을 더 발전된 단계로 끌어올릴 방법을 끊임없이 모색합니다.

이러한 고객의 성원에 힘입어 IBM Security의 Resilient 팀에서 IR 성숙도 모델을 개발했습니다.

이 모델은 임시적이고 불충분한 IR 기능부터 완벽하게 조정되고 통합되어 있으며 지속적인 개선 및 최적화가 가능한 IR 기능까지의 전 과정을 나타냅니다.

IR 오케스트레이션의 과정은 사람, 프로세스, 기술 개발에서 시작합니다. 본 가이드의 목적도 이와 일맥상통하며, 강력한 IR 기능을 구축하는 프로세스의 주요 핵심 단계를 소개하는 것입니다.

성숙도		**임시적**		**성숙 중**		**전략적**
기존 기능		**필요에 따라**	**전담 파트타임 배정**	**풀타임 배정**	**SOC/IR+**	**융합**
	사람	• 0–1	• 1–3 • 전문화	• 2-5 • 공식 역할	• ~10 • 교대제(가급적 24x7)	• 15+ • Intel, SOC, IR 팀
	프로세스	• 질서가 없고 개인의 사후 영웅적 행위에 의존 • 범용 런북(run-book) • 일부 관련자들만 아는 트라이벌 지식	• 상황별 런북, 어느 정도 일관성 있음 • 이메일 기반 프로세스	• 요구사항 및 워크플로우를 문서화하는 것이 표준 • 비즈니스 프로세스 • 차츰 얼마간 개선	• 지표를 통해 프로세스 평가 • 최소한의 위협 공유 • 교대 전환 • SLA	• 프로세스 개선 및 최적화 • 진행 중 • 광범위한 위협 공유 • 추적 팀
	기술		• SIEM • 샌드박싱	• 지속적인 모니터링 • 엔드포인트 포렌식 • 전술적 인텔리전스	• 악성코드 분석 • 추가 인텔리전스 • IT 운영	• Intel+IR 중심의 보안 프로그램 • 전략적 인텔리전스 • 물리적 보안과 연계
CMM 단계		**초기**	**반복 가능**	**정의**	**관리**	**최적화**

표 1: 침해사고 대응 성숙도 모델

1단계: 대내외 위협 인식

모든 기업은 저마다 고유한 위협 환경을 마주하게 되므로 IR 기능 구축의 첫 단계는 이 환경을 면밀하게 이해하는 것입니다.

위협 환경은 앞으로 맞설 사이버 공격의 속성을 포함하고 있습니다. 귀사가 과거에 해결한 구체적인 위협(예: 악성코드 감염, 피싱 공격)뿐만 아니라 해당 업종에 광범위하게 영향을 미치는 것으로 알려진 위협(예: 의료 기관 대상 랜섬웨어 공격, 인터넷 인프라 업체를 노리는 DDoS 공격)도 여기에 포함될 수 있습니다.

또한 강력한 위협 모델이라면 가능한 공격자 및 침해사고를 모두 고려해야 합니다. 예를 들어 최근 12개 의료 기관을 대상으로 한 설문조사에서 다수의 기관이 "부실한 위협 모델" 때문에 고전 중이며 "거의 환자 의료 기록 보호에만 몰두"하는 것으로 나타났습니다.[4] 이 조사 결과에 따르면, 의료 기관의 실무 팀은 거시적 관점에서 IT 환경 및 잠재적 위협을 모니터링하기보다는 미국 HIPAA 법 규정과 같은 협소한 범위에만 집중하고 있습니다. 의료 기기를 표적으로 하는 랜섬웨어와 같이 더 심각하지만 환자 의료 기록에 직접적으로 영향을 미치지 않는 위협도 기업의 사각지대에 숨어들었습니다.

귀사가 겪을 수 있는 사이버 침해사고는 매우 다양하며, 각각에 대한 IR 프로세스가 있기 마련입니다. 시작 단계에서 다음과 같이 질문할 수 있습니다.

- 회사가 과거에 어떤 종류의 공격 또는 사고를 겪었습니까?
- 최근에 악성코드에 감염된 적이 있습니까? 있다면 어떤 종류의 악성코드(봇넷, 데이터 유출, 랜섬웨어 등)였습니까? 침해사고는 언제 발생하여 얼마 동안 계속되었으며 어떻게 해결되었습니까?
- 직원의 인증 정보를 훔치도록 설계된 표적 피싱 이메일 사기로 피해를 입은 적이 있습니까? 그 직원은 누구입니까?
- 회사가 인기 온라인 포럼에서 또는 핵티비스트 단체나 기타 온라인 유명 인사에 의해 비판을 받은 적이 있습니까?
- 회사가 서비스 거부 공격 또는 기타 형태의 의도적 온라인 장애에서 특별히 표적이 된 적이 있습니까?

귀사가 직면할 위협을 제대로 이해하려면 경쟁사, 비즈니스 파트너, 동종 기업이 겪은 공격 유형을 살펴보십시오. 그와 유사한 공격을 본 적이 있습니까?

개인정보 유출에 대비

사이버 공격 자체가 엄청난 피해를 일으키지만, 규제 위반에 대해 부과되는 벌금도 그에 못지않은 타격을 줄 수 있습니다. 보안팀이 회사의 업종 및 표적이 될 만한 보유 데이터를 기준으로 삼아 데이터 유출 발생 시 어떤 규정이 적용될지 그리고 규제 준수를 보장하기 위해 어떻게 하면 가장 효과적으로 준비할 수 있는지를 평가하는 게 중요합니다. 다음과 같이 질문해야 합니다.

- 업계 규정, 중앙 정부/지방자치단체의 데이터 유출에 관한 법, 계약 약관 등을 포함하여 개인정보 보호를 위한 어떤 의무를 이행해야 하나요?
- 개인정보 유출이 발생하면 언제 알려야 하나요? 유출 규모, 데이터 암호화 여부 등의 요인을 다뤄야 하지만, 이는 지리적 위치 및 업종에 따라 달라질 수 있습니다.
- 고객, 법무 장관실, 기타 등 누구에게 어떻게 알려야 하나요?
- 통지 기한은 어떻게 되나요?

개인정보 보호 의무는 이미 보안 및 개인정보 보호 전문가의 주요 관심사입니다. 2018년 5월부터 EU의 GDPR(General Data Protection Regulation)이 시행되면 그 범위가 더 늘어날 것입니다.

"GDPR은 수십 년간 등장한 것 중 가장 진일보한 개인정보 보호 조치입니다. 이미 대부분 기업에서는 데이터 유출 통지 요건을 이행하는 것조차 쉽지 않습니다. 그러한 인식에 더해 GDPR로 인하여 복잡성이 가중됩니다."

— Larry Ponemon 박사, Ponemon Institute 설립자 겸 회장

GDPR은 전 세계에서 주목하는 개인정보 보호법으로서 거대하고 전면적인 변화를 수반합니다. 전 세계에서 EU 주민 또는 조직과 거래하는 모든 기업에게 적용되는 이 법은 데이터 유출이 발생하면 72시간 내에 알리도록 규정하며(미국의 기존 법 대다수보다 훨씬 더 엄격한 요건), 불이행 시 매우 무거운 벌금(2천만 유로 또는 해당 기업 연간 매출의 4%)이 부과될 수 있습니다. 각 기업은 당장 GDPR 준수를 준비하고 필요한 역할, 책임, 프로세스를 정해야 합니다.

조직 평가

또한 귀사를 둘러싼 위협 환경은 외부에서 영향을 미치는 요인과 위험뿐만 아니라 내부 과제 및 결점까지 포함합니다. 앞서 설명한 대로, 사이버 보안 전문 인력 부족은 업계가 가까운 미래에 해결해야 할 과제로 보입니다. 또한 기업은 이 문제가 당장 미치는 영향을 평가하고 해결 방안을 모색해야 합니다.

내부 전문가 부족 사태를 파악하려면, 현재 보유한 전문성 그리고 귀사가 직면하는 외부 위협에 효과적으로 맞서고 관리하는 데 필요한 전문성을 비교하여 평가하십시오. 개별 임무 완수에 소요되는 시간, 워크로드 균형 등과 같은 성과 지표를 통해 귀사가 현재 보유한 기술력 및 전문성 공백이 있는 분야를 확실히 판단할 수 있습니다. 그리고 모의 훈련 및 분석을 통해 평가 내용을 추가로 검증하여 혹시 놓쳤을 또 다른 공백을 찾아낼 수 있습니다.

마지막으로, 귀사의 위협 환경, 즉 귀사가 직면하는 공격, 준수해야 할 규정, 조직 차원의 전문가 부족 등은 끊임없이 진화하는 평가 대상입니다. 사이버 범죄 시장, 개인정보 보호법, 기타 업계 동향이 변화하므로 위협 환경도 달라질 것입니다. 반드시 정기적으로 위협 환경을 검토하고 관련 정보를 업데이트하십시오.

사례 연구:

유럽 10대 은행

한 IBM Resilient 고객은 특별한 해결 과제가 있었습니다. 전 세계에 3개의 보안팀을 두고 저마다의 프로세스를 통해 침해사고를 관리했습니다. 그로 인해 귀중한 위협 정보가 사일로화되었고, 중앙에서 관리 및 감독이 이루어지지 않았으며, IR 프로세스를 테스트하고 개선할 확실한 방법이 없었습니다.

이 회사의 보안 리더들은 전사적 범위에서 IR 계획을 표준화하고 중앙 집중식 침해사고 관리 및 감독을 활성화할 필요성을 깨달았습니다.

계획: 보안 리더들이 세 팀을 연계하여 가장 효과적이고 검증된 프로세스를 선발하고 통합함으로써 구체적인 침해사고 유형에 대한 통합 표준화 대응 계획을 함께 개발하기로 했습니다. 또한 이 회사는 세 팀을 위해 단 하나의 사고 대응 플랫폼(Incident Response Platform, IRP)을 구현했습니다.

- 중앙에서 조직 내의 모든 침해사고 처리
- 더 유의미한 컨텍스트 수집 및 협업 지원
- 더 우수한 관리 가시성 제공
- 새로운 IR 계획, 테스트, 개선 사항을 조직 전체가 공유할 수 있는 피드백 루프 생성

이 회사의 보안팀은 이와 같은 새로운 전략에 따라 전사적 차원의 경험 및 인텔리전스로부터 계속 가치를 창출할 수 있습니다.

2단계: 문서화되고 반복 가능한 표준 IR 계획 수립

부실한 계획 및 준비가 아직도 사이버 복원력의 최대 장애물이라는 사실이 설문조사를 통해 드러났습니다. 따라서 적합한 IR 계획을 갖추지 못한 기업이 대부분이라는 것도 그리 놀랍지 않습니다. Ponemon Institute의 2016년 기업의 사이버 복원력 연구에 따르면, 사이버 보안 사고 대응 계획(cyber security incident response plan, CSIRP)을 수립하고 전사적 범위에서 일관성 있게 적용하는 기업은 25%에 불과합니다. 나머지 75%는 아예 어떤 계획도 없거나, 비공식적인 임시 프로세스를 따르거나, 계획이 있더라도 기업 전체에 적용하지 못하는 상황입니다.

따라서 다수의 IR 기능이 느리고 효율성 및 실효성이 떨어집니다. 그로 인해 막대한 비용과 피해로 이어지는 사이버 공격이 발생하기 쉽고 직원의 불만 및 피로가 가중되며 보안 리더의 입지가 위태로워집니다. 그러나 표준화되고 문서화된, 반복 가능한 IR 계획이 있으면 이러한 위험이 해결되며, 보안팀은 무엇을 언제 어떻게 해야 할지 정확히 알게 됩니다. 또한 지속적인 개선을 위한 플랫폼을 제공하므로, 날로 진화하는 사이버 위협에 항상 미리 대처할 수 있습니다.

과제: 탄탄한 IR 계획을 마련하려면 상당한 시간이 필요하고 조직 전반에서 헌신적인 노력이 있어야 합니다. 이를 위해 보안 리더는 IR을 우선 과제로 삼고 추진해야 합니다. IR 계획 워크샵을 개최하면 팀의 모든 이해 관계자가 모여 일관성 있고 표준화된 대응 계획을 개발하고 문서화할 수 있습니다.

담당 팀은 경영진, 그리고 필요하다면 이사회와도 소통하면서 관련 위험에 대한 이해를 돕고, 유관 부서의 다른 리더에게도 각자 해야 할 역할이 있음을 알려야 합니다. 여기에는 마케팅, HR, 법무, IT, 기타 사업부가 포함됩니다.

이 워크샵을 진행하면서 (보안 리더의 지도 하에) 담당 팀이 모여 구체적인 사고 시나리오를 검토하고 다음 활동을 수행할 수 있습니다.

- 사고의 라이프사이클 전체를 다루기 위한 구체적인 단계 구상
- 역할과 책임 결정
- 대응 과정에서 활용할 핵심 기술 및 소통 채널 파악
- 권한 및 에스컬레이션 관련 프로세스 구현

NIST, SANS, CERT와 같은 자원을 활용하여 이러한 대화 및 계획에 적합한 프레임워크를 세울 수 있습니다. 하지만 궁극적으로 귀사에 특화된 IR 계획을 수립해야 합니다. 따라서 사내의 모든 관계자를 참여시키는 것이 중요합니다. 기존 IT 및 보안팀, 사내 주요 이해 관계자뿐만 아니라 임원, 법무 책임자, 규제 준수 책임자의 노하우 및 경험을 활용해야 합니다. 비즈니스파트너, 공급업체 등 외부 협력사도 대화에 참여할 수 있습니다.

이러한 훈련 및 대화가 마무리되면 짜임새 있고 반복 가능하며 문서화된 계획이 마련됩니다. 중앙에서 관리하고 모든 팀원이 이행하는 이 계획은 점차 꾸준히 개선할 수 있습니다.

사례 연구:

Fortune 100대 기술 기업

한 IBM Resilient 고객은 SOC에 대규모 기술 투자를 진행한 후 그에 발맞춰 사람 및 프로세스도 개발할 필요성을 느꼈습니다. 따라서 시뮬레이션을 통해 프로세스를 테스트하고 SLA 및 임원 리포트를 개발하기로 했습니다.

이 고객은 복잡하고 발생 가능성이 낮은 이벤트에 초점을 맞춘 분기별 정기 시뮬레이션을 개발했습니다. 즉 평소에 경계를 강화하여 대부분의 심각한 위협을 확실하게 차단하려 했습니다. 보안 리더는 조직 차원의 지원을 확보하고자 IR SLA를 개발했습니다. 이 지표를 침해사고 유형 및 심각도를 기준으로 분류하고, IR 팀이 지향할 표준을 마련했습니다. 또한 CISO는 이 SLA를 활용하여 이사회에 성과를 입증하고 그에 적합한 예산을 배정할 수 있었습니다. 이 고객은 지금도 매일 수백 건의 침해사고를 겪고 있으나, 숙련된 팀이 간단하고 효과적인 방식으로 해결하고 관리할 수 있습니다.

3단계: 선제적으로 IR 프로세스 테스트 및 개선

사이버 공격자는 끊임없이 새로운 우위를 확보하는 데 주력합니다. 사이버 보안팀은 항상 한발 앞서 대비하는 것을 우선 순위에 두어야 합니다.

IR 기능을 계속 발전시키는 가장 효과적인 방법 중 하나가 시뮬레이션을 실행하는 것입니다. 결과에 중점을 둔 전용 시뮬레이션의 형태여야 합니다.

IR 시뮬레이션은 "부실한 계획 및 준비"라는 장애물을 해결하는 데 유용합니다. 시뮬레이션을 통해 사람, 프로세스, 기술을 포괄하는 IR 기능의 전 범위에서 현실의 침해사고에 대비할 뿐만 아니라 더 발전시킬 기회도 모색할 수 있습니다.

보안 리더의 입장에서는 시뮬레이션의 실효성을 보장하는 게 중요하며, 담당 팀은 구체적인 단계를 통해 발전시키고 성과를 낼 수 있습니다.

먼저 보안 리더는 유의미한 시뮬레이션이 될 수 있도록 초기에 계획을 세워야 합니다. 자주 발생하는 침해사고를 시연해볼까요 아니면 뜻하지 않은 상황을 준비할까요? 두 유형 모두 살펴볼 가치가 있습니다.

또한 보안 리더는 분석가가 조사할 중요 세부 사항이 포함된 구체적이고 세세한 시뮬레이션도 개발해야 합니다. 달리 말하자면 팀에서 이 시뮬레이션을 중요하게 여기고 단순히 최소 기준 달성 여부만 확인하는 훈련에 머무르지 않게 해야 합니다.

또한 측정 가능한 시뮬레이션이 되어야 합니다. 목표를 정하고 완료까지 걸린 시간, 완성도 등의 핵심 지표를 추적하십시오. 그리고 시뮬레이션을 반복하여 개선(또는 퇴보) 효과를 측정하십시오.

마지막으로, IR 시뮬레이션은 전사적 범위에서 수행되어야 합니다. HR, 법무, 마케팅, 기타 부서를 참여시켜 실제 침해사고가 발생하면 지체 없이 각자의 역할을 해낼 수 있게 합니다. 사후 분석 결과를 조직 전체에서 공유하는 것도 중요합니다. 그러면 팀에서 정직한 소통이 가능해지며, 경영진도 어디에 어떤 자원이 필요한지 알 수 있습니다.

4단계: 위협 인텔리전스 활용

사이버 범죄자들이 손잡고 있습니다. 이들은 다크웹을 통해 협업하고 정보를 공유합니다. 보안 전문가들도 함께 대처해야 합니다.

Ponemon Institute는 2016년 기업의 사이버 복원력 연구에서 응답자 중 고성과 그룹(전년도에 사이버 복원력이 향상된 기업)과 평균 기업 그룹을 비교하여 주요 차이점을 분석했습니다. 여러 결과 중 하나를 소개하면, 고성과 그룹은 위협 공유 프로그램에 참여할 가능성이 70%로 (53%에 불과한) 평균 그룹보다 더 높습니다.

위협 인텔리전스(threat intelligence, TI) 산업이 최근 몇 년새 크게 성장했으며 그럴 만한 이유가 있습니다. 보안팀들이 각 환경에서 일어나는 활동을 더 정확히 인식하고 인사이트를 확보할 방법을 찾고 있기 때문입니다.

위협 인텔리전스 활용은 인식의 수준을 높이는 데 큰 역할을 합니다. 하지만 이를 구현하는 게 쉽지는 않습니다. 대개 보안팀은 품질이 제각각인 수많은 피드를 탐색하고 유용한 정보와 무익한 정보를 구별해야 합니다.

다행히 많은 IBM Resilient 고객이 수년간 다양한 위협 인텔리전스 피드를 구현하고 시험하면서 경험을 쌓았습니다. 그 종합적인 경험을 바탕으로 다음 3가지 핵심 전략을 통해 효과적으로 TI를 활용하면서 침해사고에 대응할 수 있습니다.

- **위협 인텔리전스를 기반으로 IR 계획 수립**
  IBM Resilient 고객인 한 대형 미디어 네트워크는 분석가들이 위협 인텔리전스 데이터를 조사하는 데 너무 많은 시간을 보낸다는 사실을 알게 되었습니다. 관련 없는 문제점을 추적하느라 자원을 허비하고 별 효과를 거두지 못했습니다.

  이 문제를 해결하기 위해 위협 인텔리전스 데이터를 기존 IR 프로세스에 접목했습니다. 분석가들은 IoC(indicator of compromise)를 침해사고로 에스컬레이션합니다. 그러면 잠재적 위협에 관한 중요 정보를 필요할 때 액세스할 수 있습니다. 현재의 상황과 관련 있는 가용 인텔리전스를 활용하는 것입니다. 그러면 훨씬 더 효과적으로 시간을 관리하고 팀 생산성을 높일 수 있습니다.

- **통합 및 상관성 분석으로 위협 인텔리전스의 실용성 강화**
  위협 인텔리전스를 SIEM 및 EDR 툴과 같은 다른 데이터 소스와 통합하면, 분석가가 더 충실하게 침해사고의 컨텍스트를 파악할 수 있습니다. 그리고 해당 정보는 더 실행 가능해집니다. 컨텍스트, 심각도, 패턴까지 고려하면서 데이터를 정제하고 범위를 한정할 수 있습니다. 그러면 분석가가 무엇을 상대하고 있으며 최상의 방법은 무엇인지 더 확실히 알 수 있게 됩니다.

- **소스 추적 및 그 유용성 평가**
  인텔리전스 피드는 무궁무진하며, 그중 하나로 다 되는(one-size-fits-all) 경우는 없습니다. 공개 소스, 폐쇄형 커뮤니티, 유료 소스 등 다양한 예가 있습니다. 게다가 위협 인텔리전스 플랫폼도 있습니다. 각 피드가 정보를 제공하는 빈도, 품질, 정보의 중요도를 기록해 두십시오. 그러면 중복된 피드 또는 어떤 식으로든 조정해야 하는 피드를 곧 알 수 있게 됩니다.

다음 섹션에서 자세히 살펴보겠지만, 사고 대응 플랫폼(incident response platform, IRP)은 사이버 침해사고를 조사하고 대처하는 수작업의 상당 부분을 자동화할 수 있습니다. 무엇보다도 IRP는 아티팩트 시각화라는 기법에서 데이터 분석 및 전문 로직을 활용합니다. 그러면 별개로 보이는 침해사고의 공통점, 이를테면 관련 IT 자산, 사용된 악성 소프트웨어, 통신한 악성 인프라 등을 찾아내 연관시킬 수 있게 됩니다.

침해사고를 식별하고 어떤 보안 위반의 스토리를 구성하는 개별 아티팩트를 포착한다면, 몇 주 또는 며칠이 걸리던 대응을 몇 시간 만에 완료할 수 있습니다. 그뿐만 아니라 사용자 액세스, 데이터 보안, 통신 등의 영역에서 현실적인 제어 기능을 구현함으로써 향후 침해사고를 예방할 수 있습니다.

"인텔리전스 공유로 조직의 보안 수준이 향상되었다는 응답 및 IR 계획의 효용 가치가 높아졌다는 응답이 각각 81%와 75%에 달합니다."

— 2016년 기업의 사이버 복원력, Ponemon Institute 조사 보고서

5단계. 침해사고 조사 및 대응의 간소화

Verizon Data Breach Investigation Report의 내용대로, Verizon이 검토한 전체 침해사고 중에서 "며칠 이내에" 탐지된 것은 1/4도 되지 않습니다. 대다수는 며칠, 몇 주 심지어 몇 개월이 지나서야 탐지되었습니다[5]. 사이버 침해사고가 몇 주 또는 몇 개월째 들키지 않고 계속되면 공격자가 감염된 네트워크에 교두보를 마련할 수 있으며, 이 경우 제거하기가 쉽지 않습니다.

그 이유 중 하나는 대부분 기업이 직원 대상의 피싱 공격과 같은 단순한 사이버 침해사고를 조사하는 데에도 임시적인 프로세스를 사용하기 때문입니다. 게다가 전문 인력이 부족하므로, 적합한 툴과 기술을 갖췄더라도 수많은 침해사고를 효율적으로 관리할 만한 인력을 찾기 어려울 수 있습니다.

통합 데이터 및 위협 인텔리전스 소스를 IR 프로세스에 추가한다면, 정교한 오케스트레이션 방식으로 대응할 가능성이 커집니다. 그 출발점은 하위 수준 작업의 자동화입니다.

자동화는 사소하고 반복적인 작업을 스트림화하여 더 빠르고 스마트한 팀 활동을 지원하는 데 유용합니다. 더 포괄적인 IR 오케스트레이션 전략(오케스트레이션에 대해서는 다음 섹션 참조)에 따라 자동화를 활용함으로써 팀의 전략적 의사결정 능력을 한층 더 강화할 수 있습니다.

예컨대 악성코드가 발견되면, 한 엔드포인트에서 탐지된 의심스러운 샘플을 자동으로 수집하고 엔드포인트 에이전트 또는 차세대 위협 탐지 플랫폼에 보내 관찰하고 분류합니다. 그 분석 결과에 따라 추가로 자동 프로세스 및 수작업 프로세스를 예약할 수 있습니다. 이를테면 네트워크에 다른 감염된 호스트가 있는지 조사하고, 이를 격리할 수 있는 권한을 요청하고, 악성코드 감염과 관련된 취약점을 규명하고, 취약한 시스템에 적용할 비상 패치를 예약하거나 요건에 따라 사내 실무자나 외부 모니터 요원에게 필수 통지를 보냅니다. 그리고 단계별로 요청, 응답, 조치 내역을 문서화하여 향후 참조할 수 있도록 합니다.

자동화를 시작하려면 먼저 간소화하기에 적합한 프로세스를 결정합니다. 대개는 분석가의 시간을 지나치게 많이 빼앗는 시간 소모적이고 사소하며 비효율적인 일이 해당되며, 이러한 프로세스는 안전하고 확실하게 자동화할 수 있습니다. 또한 보안 리더는 어떤 프로세스를 자동화할 경우 발생하는 위험 및 복잡성을 효율성 제고 효과와 비교하여 분석해야 합니다.

안전하고 확실한 자동화를 위해 프로세스의 충실도를 테스트하십시오. 여전히 사람의 의사결정 및 승인이 필요한 수작업을 스크립트화하십시오. 프로세스가 적합하고 기술이 제대로 작동하고 있음을 팀에서 확신한다면, 전면적인 자동화를 결정할 수 있습니다.

그러나 기술 기반 자동화가 시간을 절약할 수 있으나, 오로지 종합적인 IR 기능의 품질에 좌우된다는 점 그리고 IR 오케스트레이션 전략이 있어야 가장 효과적이라는 점을 기억해야 합니다.

"로마가 하루 아침에 세워지지 않았더라도 데이터가 하루 아침에 털리는 일은 비일비재합니다... 적법한 인증 정보가 있다면 순식간에 잠금을 풀고 들어와 귀중한 자산을 마음껏 가져갈 수 있습니다."

— Verizon 2016 Data Breach Investigations Report

6단계. 사람, 프로세스, 기술의 오케스트레이션

더 빠르고 자동화된 방식으로 대응한다는 IR 오케스트레이션의 비전이 업계 전반에서 많은 보안 전문가의 주의와 관심을 끌었습니다. 그러나 앞 섹션에서 언급한 대로, 성공적이고 효과적인 오케스트레이션 및 자동화가 이루어지려면 강력하고 종합적인 IR 기능이 필요합니다. 효과적인 오케스트레이션 여부는 전적으로 IR 기초 요소, 즉 사람, 프로세스, 기술의 품질에 따라 결정됩니다.

본 가이드의 전반부는 이러한 기초 요소를 세심하게 구성하고 강화하며 향후 발전이 가능한 상태로 운용하는 데 주안점을 두었습니다. 복습 차원에서 IR 기능의 효과를 평가할 때 반드시 해야 할 질문을 정리합니다.

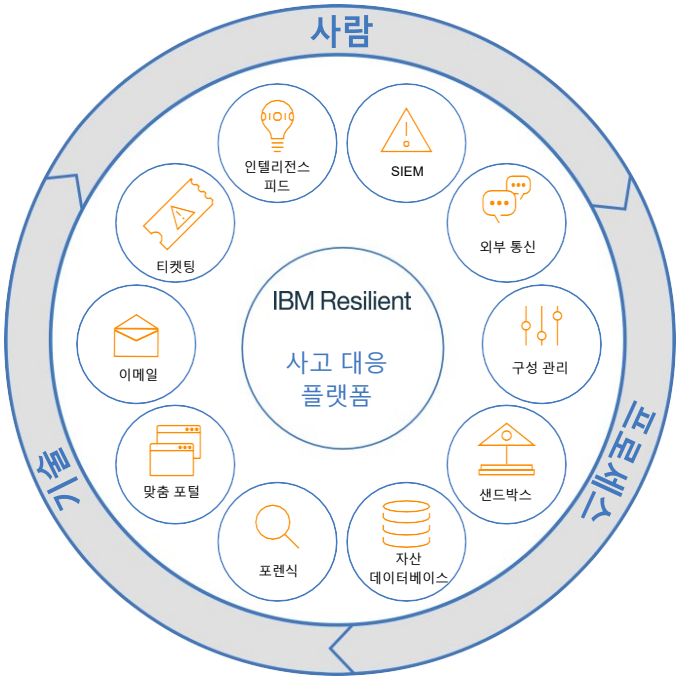


그림 1: IR 오케스트레이션에서 중앙 허브의 역할을 하는 Resilient IRP

사람: IR 팀이 제대로 조정되고 훈련된 상태인가요? 침해사고 라이프사이클의 모든 요소를 다룰 만한 기술력이 있나요? 협업 및 분석 수단이 있나요?

프로세스: 제대로 정의되고 반복 가능하며 일관성 있는 IR 계획이 있나요? 손쉽게 업데이트하고 정리할 수 있나요? 정기적으로 테스트하고 측정하고 있나요?

기술: 귀사의 기술은 적절한 방식으로 가치 있는 인사이트 및 인텔리전스를 제공하나요? 팀에서 현명한 결정을 내리고 신속하게 실행에 옮길 수 있도록 지원하나요?

이러한 질문에 답하면서 이 기본 조건을 실제 효과로 연결하는 오케스트레이션을 수행할 수 있습니다. 이러한 기반을 조성하지 않으면 오케스트레이션의 효과를 기대하기 어렵습니다.

IR 오케스트레이션의 목적은 관계자가 보안 침해사고 발생 시 해야 할 일을 정확히 인식하게 하고 빠르고 효과적이며 올바른 조치를 취하는 데 필요한 프로세스 및 툴을 갖춰 대응 팀의 역량을 강화하는 데 있습니다.

사이버 보안 전문가들 사이에서 오케스트레이션 및 자동화 모두 인기를 얻고 있으나, 오케스트레이션은 사이버 보안에서 사람 중심의 요소를 지원하고 최적화함으로써(예: 컨텍스트 인식 및 의사결정 지원) 보안 운영의 핵심 요소로 키워낸다는 점에서 다릅니다.

보안 위협은 불확실성을 가진 문제이므로 이는 중대한 의미를 갖습니다. 위협 대응이 미리 정해진 대로 진행되는 경우는 거의 없습니다. 자동화는 특정 작업을 빠르고 효과적으로 실행할 수 있어 유용합니다. 그러나 대부분 위협이 계속 진화하고 공격자도 전술의 변화를 꾀하므로 문제점 에스컬레이션, 트러블슈팅 등의 조치를 취하려면 사람의 의사 결정이 필요합니다.

자동화는 더 포괄적인 오케스트레이션 프로세스에서 효과적인 수단이지만, 오케스트레이션이 중대한 역할을 하는 데 인적 요소를 빼놓을 수 없습니다.

오케스트레이션은 조직마다 다르게 적용됩니다. 각 조직의 고유한 위협 환경, IT 및 보안 환경, 우선 과제와 연계해야 합니다. 간단한 예로, 많은 IBM 고객사에서 볼 수 있는 대표적인 오케스트레이션 방식을 소개합니다.

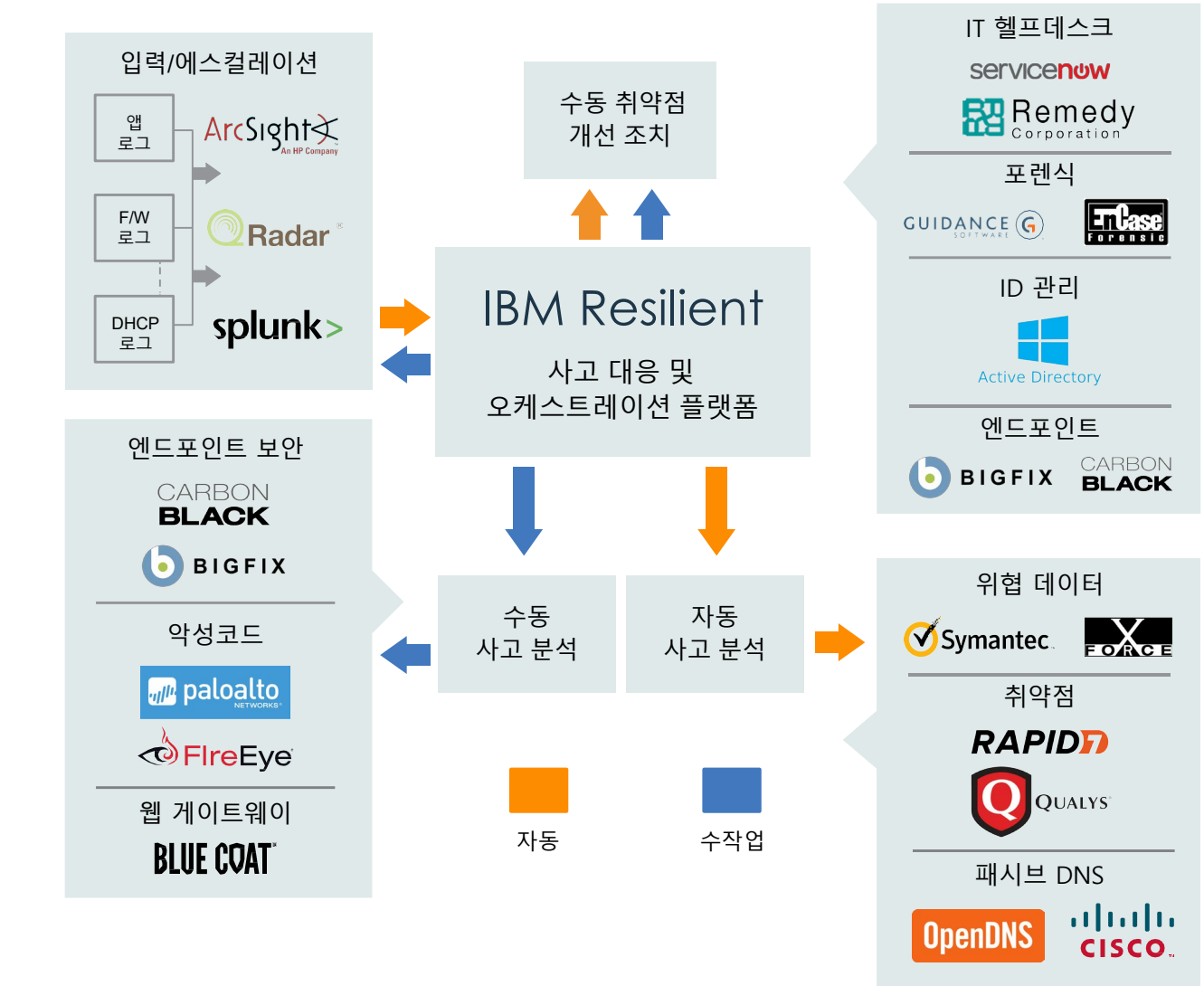


그림 2: 통합형 IRP를 사용하는 오케스트레이션 기반 대응 워크플로우의 예

그림의 왼쪽 위를 보면, SIEM 알림으로부터 침해사고가 에스컬레이션되고, 이 조직의 IRP에서 자동으로 기록이 생성됩니다. 오른쪽 맨 아래로 가면, 이 플랫폼은 내장된 위협 인텔리전스 피드 및 추가 소스로부터 귀중한 침해사고 컨텍스트를 자동으로 수집하고 전달합니다. 그 다음에는 보안 분석가가 이미 중요한 정보를 확보한 상태에서 개입하여 주도권을 갖습니다. 이 분석가는 추가 통합을 이용하여 필요한 추가 작업을 직접 수행할 수 있습니다. 이를테면 다른 보안 툴(예: 엔드포인트 보안 툴, 웹 게이트웨이)로부터 침해사고에 관한 추가 정보를 수집하거나, IT 헬프데스크에 알려 문제 해결을 시작하거나, ID 관리 팀에 사용자의 네트워크 연결을 끊도록 요청합니다.

IT 프로세스 오케스트레이션에는 다양한 방식이 있지만, 목표는 항상 같습니다. 분석가가 가장 유리한 입장에서 위협에 대응할 수 있게 하는 것입니다.

결론: 조직의 복원력 및 대응 능력 강화

기술의 발전에 힘입어 수습 사원이 푸시 버튼 하나만 누르면 침해사고에 대응할 수 있는 세상이 곧 온다고 상상하면 즐겁습니다. 그러나 IR은 현재 또한 앞으로도 복잡하고 다면적인 프로세스이므로, 뛰어난 보안 분석가의 관심과 참여가 필요합니다.

성숙한 IR은 사람, 프로세스, 기술의 조합이 연속체를 이루는 것입니다. 기술의 역할은 사람인 분석가를 대체하는 게 아니라 분석가가 더 많은 일을 해내도록, 즉 특정 위협에 대해 더 우수한 인텔리전스를 제공하고 대응 프로세스를 간소화하며 항상 준비된 상태로 대응하도록 지원하는 것입니다.

또한 성숙한 사이버 보안 IR 기능은 조직 내에서 더 거대한 문화적 변화를 가져올 수 있습니다. 즉 보안팀을 IT 운영 및 관리 팀과 더 긴밀하게 통합하여 포괄적으로 사이버 침해사고에 대응하는 프로세스를 시작하게 하는 것입니다.

IR 프로세스가 성숙한 조직은 선제적 대응 단계에 들어서게 됩니다. 즉 IR에서 얻은 정보가 조직의 전략적 자산이 됩니다. 선제적 대응 모델에서는 IR 팀의 인텔리전스를 다시 보안 및 IT 조직에 전달하여 이를 바탕으로 기술 투자 및 도입을 결정하고, 직원의 기술력을 강화하며, 위험에 대한 조직 차원의 이해를 넓혀 물리적 보안 자산 및 제공자, 위협 인텔리전스 제공자, 규제 기관 및 정부 기관 등이 포함된 더 광범위한 생태계를 수용할 수 있습니다.

이러한 수준의 성숙도에 도달한 기업이 Fortune 500 그룹에서도 소수에 불과하지만, 조만간 성숙한 IR 플랫폼으로 마이그레이션하는 기업이 늘면서 IR의 전략적 활용이 더 보편화될 것으로 기대합니다.

추가 정보

오케스트레이션 기반 대응 체제를 구축하고 보안팀이 더 빠르고 현명하게 대처하도록 지원하십시오.

아래 사이트를 방문하여 Resilient Incident Response Platform의 데모를 예약하실 수 있습니다.
http://info.resilientsystems.com/incident-response-platform-schedule-a-demo

IBM Resilient 소개

기업이 어떤 사이버 공격 또는 비즈니스 위기 상황에서도 성공을 누릴 수 있도록 지원하는 것이 IBM Security의 사명입니다. 보안팀은 Resilient 사고 대응 플랫폼(IRP)에서 더 빠르고 현명하며 효율적인 방식으로 침해사고를 분석하고 대처하며 피해를 최소화할 수 있습니다. Resilient IRP는 업계 유일의 완전한 IR 오케스트레이션/자동화 플랫폼입니다. 여기서 사람, 프로세스, 기술을 통합하고 연계하면서 단일 IR 허브를 구축할 수 있습니다. 다수의 Fortune 500대 기업 및 전세계 수백 개 파트너가 동급최강의 Resilient 보안 솔루션을 구축하기 위해 IBM을 선택했습니다.

IBM Corporation
Security Group
Route 100
Somers, NY 10589

Produced in the United States of America
2017년 12월

1 http://www.esg-global.com/blog/dealing-with-overwhelming-volume-of-security-alerts

2 http://cyberseek.org

3 http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2016_Cyber_Resilient_Organization_Executive_Summary_FINAL.pdf

4 https://securityledger.com/2016/02/focus-on-privacy-hobbles-security-at-healthcare-orgs

5 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016

재활용하세요

BUW03068KRKO-00