IBM Security

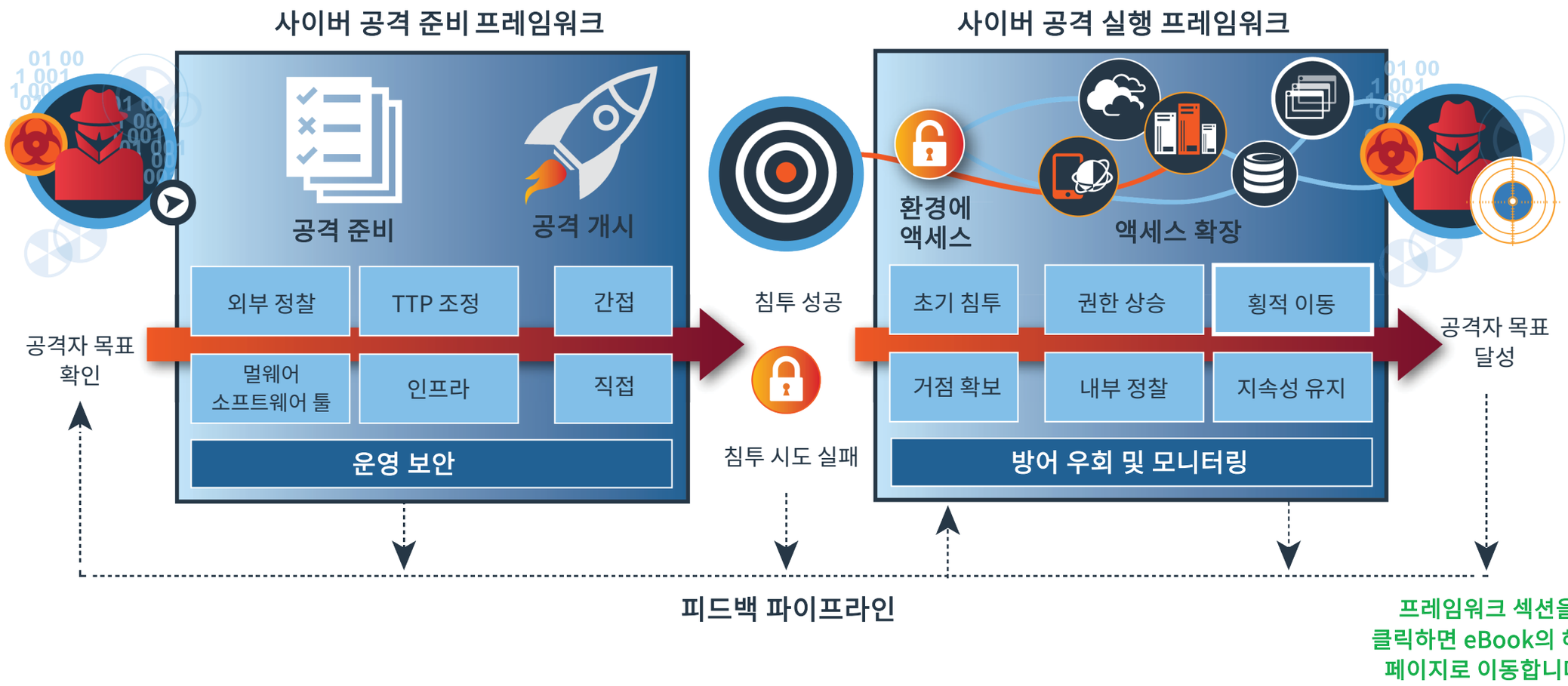
IBM

IBM SECURITY EBOOK

조직에서 점점 더 큰 리스크로 대두되고 있는 사이버 공격

IBM X-Force IRIS 사이버 공격 준비 및 실행 프레임워크로 알아본 리스크 해소 방법

사이버 공격: 준비가 가장 중요

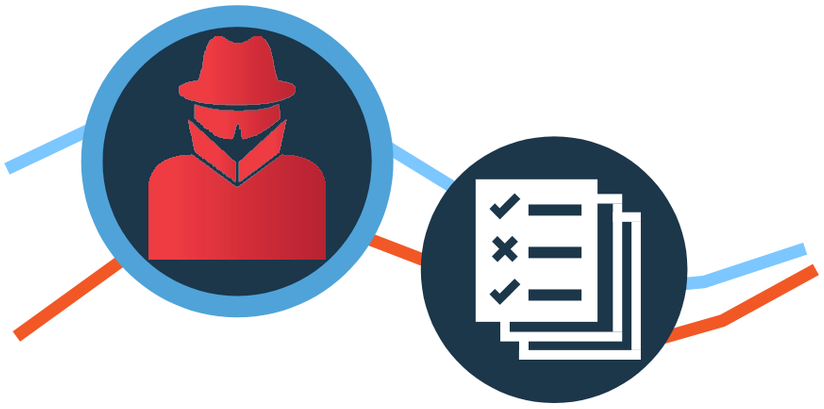


효과적인 사이버 공격 보안 전략을 수립하려면, 조직은 정확히 어떤 방식으로 사이버 공격이 발생하는지 공격자의 관점에서 철저히 파악해야 합니다. IBM® X-Force® IRIS(Incident Response and Intelligence Services) 팀의 전문가들은 공격자가 취하는 모든 조치를 다루는 포괄적인 프레임워크를 개발하였으며, 이를 통해 보안 분석가 및 위협 사냥꾼이 리스크 노출을 줄이고 지속적으로 증가하는 사이버 공격을 방지하는 데 필요한 인사이트를 제공합니다.

이 프레임워크에는 사이버 공격의 모든 단계가 포함되어 있으므로 보안 분석가는 이러한 단계를 반복적이고 포괄적인 방식으로 검토할 수 있습니다. 사이버 공격의 단계가 반드시 순차적으로 발생하는 것은 아닙니다. 전혀 발생하지 않는 단계도 있습니다. 공격이 진행되는 방식에 따라 여러 단계가 동시에 발생하거나 여러 번 반복하여 발생할 수도 있고 단계를 완전히 건너뛸 수도 있습니다.

본 eBook에서는 사이버 공격 중 발생하는 각 단계를 처음부터 끝까지 모두 설명하고 이러한 현재의 위협을 사전에 대비하는 방법에 대한 지침을 제공합니다.

공격 시작: 공격자의 공격 준비



공격을 하기 전 공격자는 신중하게 목표를 결정합니다(예: 지적 재산 절도). 공격의 첫 번째 파트는 준비 프레임워크입니다. 공격자는 공격을 준비한 후에 공격을 개시합니다.

공격 목표를 결정하고 공격을 준비하는 준비 프레임워크에서는 다음과 같이 사이버 공격자가 거쳐가는 모든 단계를 살펴봅니다.

공격자의 목표 결정. 공격자가 목표를 파악하고, 공격 요건을 확인하고, 초기 공격 계획을 세웁니다.

공격자의 공격 준비. 이 단계에는 공격자가 목표 선택부터 공격 개시까지 진행하는 데 사용하는 모든 알려진 방법이 포함되어 있습니다. 예컨대 다음과 같은 방법을 사용합니다.

외부 정찰 수행. 공격자가 목표로 설정한 조직을 조사하여 익스플로잇 공격이 가능한 액세스 지점을 찾습니다.

목표에 맞게 TTP(전술, 기법 및 절차) 조정. 공격자가 목표 조직에서 공격에 성공할 가능성이 가장 큰 TTP를 결정합니다(예: 제로 데이 익스플로잇이 포함된 이메일).

멀웨어 및 소프트웨어 툴 준비. 공격자는 공격을 준비하기 위해 네트워크 침투 및 이동에 사용할 툴 세트를 정의합니다. 공격자는 멀웨어를 사용하거나, 합법적인 용도의 소프트웨어 툴을 용도 변경하거나, 두 방법을 조합하여 사용할 수 있습니다.

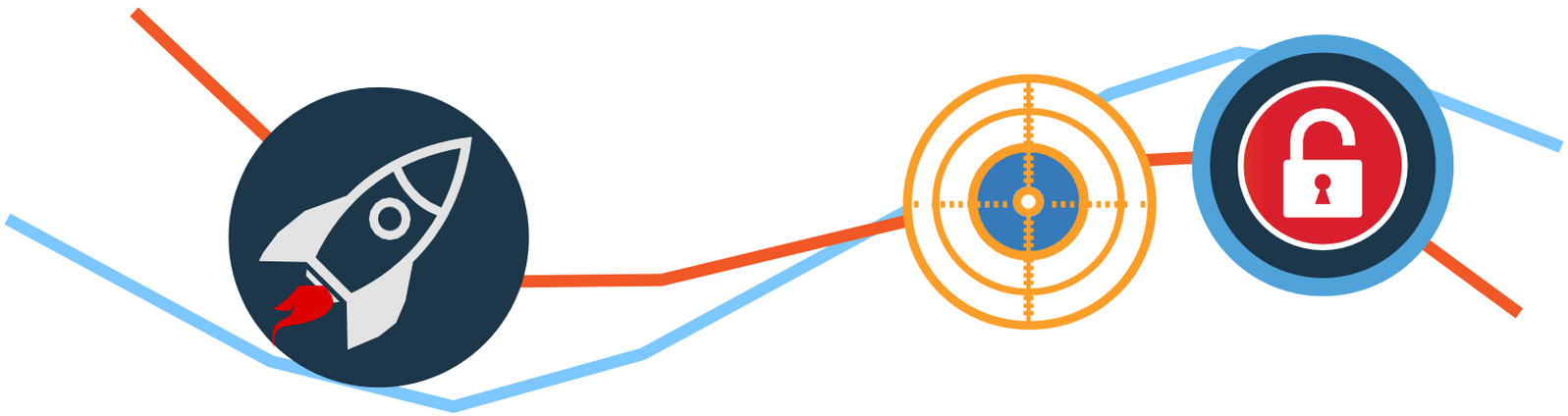
공격 인프라 준비. 공격자는 C&C(Command & Control) 네트워크를 구축하고 공격자의 시스템을 찾아가는 추적을 교란시키기 위한 절차를 개발할 수 있습니다.

방어를 위한 팁: 네트워크 보안 강화

- 회사를 공격 목표로 삼을 가능성이 있는 적대적 공격자의 위협 프로파일을 작성합니다. 프로파일이 작성되면 다음과 같이 질문해 보십시오.
  - 위협이 되는 공격자가 조직을 목표로 삼은 적이 있습니까?
  - 어떤 유형의 공격자가 조직에 관심을 가집니까?
  - 해당 위협 그룹은 어디에 있습니까?
  - 공격자의 목표는 무엇입니까?
- 가장 중요한 데이터와 같이 공격자가 목표로 삼을 가능성이 있는 자산에 대해 보호 조치를 취합니다.
- 위협이 되는 공격자가 조직과 조직의 자산, 지적 재산, 고객, 소유권이 있는 데이터 등 어디에 관심이 있는지 판별합니다.
- 의심하지 않는 공격 목표에게 합법적인 것처럼 보일 수 있는 도메인을 C&C 서버가 만들지 못하도록 회사 이름에 대한 철자 오류로 생성될 수 있는 이름의 도메인을 모두 구매하고 의심스러운 도메인 등록을 모니터링합니다.

X-Force IRIS 사이버 공격 프레임워크에 대한 팟캐스트를 들어보십시오.

공격 개시 및 실행: 침투 시작



양질의 위협 인텔리전스는 사전 예방적 위협 사냥 프로그램의 실행을 가능하게 해주는 핵심 요소입니다.[1]

공격 개시. 공격 인프라가 준비되면 공격자는 직접 또는 간접적으로 목표에 대한 공격을 개시하고 공격을 성공 또는 실패로 정의합니다.

직접 공격의 예

- 자격 증명 절도
- 악성 파일 또는 도메인이 첨부된 피싱 이메일

간접 공격의 예

- 가정용 네트워크에 연결하고 있는 동안 업무용 랩탑에 발생하는 감염
- 웹사이트 또는 온라인 광고 침투

[1] "2018 Threat Hunting Report," (2018 위협 사냥 보고서) *Crowd Research Partners,* 2018.

침투하는 데 성공하면 사이버 공격 실행 프레임워크가 시작됩니다. 침투 시도가 실패하면 공격자는 이전 단계로 돌아가 공격 전략을 재정비하고 공격을 재개할 수 있도록 실패 지점을 확인합니다.

환경에 액세스. 공격이 성공했다고 판단되면 공격자는 거점을 확보하기 위해 빠르게 작업합니다.

초기 침투 실행. 공격자가 네트워크에서 하나 이상의 호스트에 액세스하거나 사용자 계정에 로그인한 상태입니다.

거점 확보. 공격자는 네트워크 내에서 하나 이상의 호스트 또는 사용자 계정에 대한 지속적인 액세스 및 제어 권한을 확보합니다. 네트워크에 백도어를 설치하고 C&C 네트워크에 대한 아웃바운드 통신 링크를 설정하는 것으로 시작할 수 있습니다.

방어를 위한 팁: 네트워크 보안 강화

- 효율적이고 시기적절한 패치 관리와 같은 방법으로 공격에 노출되는 영역의 보안을 강화하여 대부분의 공격자가 해당 조직을 쉬운 목표로 여기지 못하도록 합니다.
- 시스템 관리 프로세스에 패치 관리 성과 지표를 포함시키고 패치 자동 확인을 사용합니다.
- 최소 권한 개념을 적용합니다. 사용자와 시스템이 정해진 역할에 해당하는 액세스 권한만 가지도록 하고 과도한 권한은 없앱니다. 사용자와 시스템이 권한 부여된 작업만 수행하도록 합니다.
- 공격하기 어렵도록 강력한 엔드포인트 감지 및 완화 전략을 구현합니다.
- 위협 사냥 프로그램을 사용하여 위협 식별 및 완화를 지원합니다.

공격 지속: 네트워크 액세스 확장

액세스 확장. 공격자가 네트워크에서 거점을 확보하면 다음 단계는 네트워크 액세스를 확장하는 것입니다. 이 단계에서는 공격자가 여러 방법을 사용하여 초기 침투에서 목표 이행까지 진행합니다.

권한 상승. 공격자가 침투한 네트워크에서 더 많은 액세스 권한을 확보합니다. 자격 증명 덤핑, 이전에 훔친 해시를 통한 비밀번호 우회, 내부 애플리케이션 또는 시스템 손상 등은 모두 네트워크 액세스 권한 상승을 위해 사용할 수 있는 전술입니다.

횡적 이동. 공격자는 훔친 자격 증명을 사용하여 원격으로 또는 다른 방법으로 네트워크에 액세스하여 해당 네트워크나 다른 연결된 네트워크의 또 다른 호스트로 이동합니다.

내부 정찰 수행. 공격자는 네트워크에 오픈 포트 쿼리, 파일에서 데이터 찾기, 특정 리소스에 대한 서비스 티켓 숙지 등의 전술을 사용하여 네트워크에 대한 추가 정보를 수집합니다.

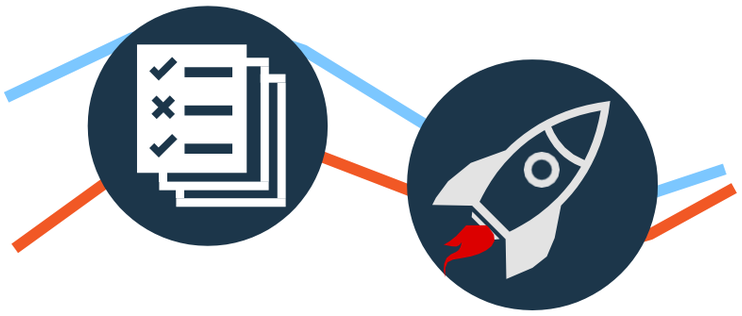
지속성 유지. 공격자는 거점을 강화하고 유지하는 조치를 통해 환경에 대한 지속적인 액세스가 보장되도록 합니다. 공격자는 초기 백도어를 레지스트리 위치에 배치함으로써 호스트가 다시 시작될 때마다 백도어가 실행되어 시스템 침투와 동시에 지속성이 확보되도록 할 수 있습니다.

방어를 위한 팁: 네트워크 보안 강화

- 위협 사냥 프로그램을 재정비합니다. 알려지지 않은 위협이 발견되면 연관된 위협 지표를 서명으로써 감지 및 보호 플랫폼으로 마이그레이션하여 자동으로 다른 모든 인스턴스를 파악합니다.
- 중앙 집중식 로깅 및 분석 플랫폼에 투자하여 자동으로 데이터의 우선순위를 지정하고 선의의 활동에서부터 악의적인 것으로 나타날 수 있는 활동에 이르기까지 여러 계층으로 데이터를 배치합니다.
- 화이트리스트를 만들고 정상 활동의 기준을 작성하며 빈도 분석을 수행합니다.
- MFA(다단계 인증)를 사용하고, 시스템에서 동일한 비밀번호 사용 기능을 제한하고, 안전한 위치에 비밀번호 해시를 저장하여 비밀번호 절도 방법에 대비하는 등 강력한 사용자 비밀번호 정책을 시행합니다.

"Proactively tackle security threats with IBM X-Force skills and expertise"
(IBM X-Force 기술 및 전문 지식을 통해 사전 예방적으로 보안 위협 해소) 솔루션 개요를 읽어보십시오.

공격 강화: 여러 단계에서 지속적으로 발생



사이버 공격의 다음과 같은 측면은 공격 라이프사이클 동안 지속적으로 존재합니다.

운영 보안. 운영 보안은 공격 준비 과정 전반에서 피해자나 사이버 보안 방어자가 공격 준비에 대해 알지 못하도록 숨기기 위해 공격자가 취하는 모든 조치를 나타냅니다.

방어 우회 및 모니터링. 실행 주기 전반에 존재하는 공격 활동의 측면으로, 공격자가 감지를 회피하기 위해 기울이는 노력이 반영된 것입니다. 해당 전술로는 데이터 마스킹과 공격의 존재를 위장하도록 설계된 악성 소프트웨어 사용이 있습니다. 로그 삭제, 악성 코드 숨기기 또는 위장 작업도 일반적으로 사용됩니다.

피드백 파이프라인. 피드백 파이프라인은 공격 준비가 시작될 때부터 실행 단계에 이르기까지 전 과정에 걸쳐 존재합니다. 네트워크 내부에 침투하고 나면 공격자는 목표와 전술을 재평가하고, 결과와 목표 임무를 비교하고, 어떤 공격 단계로든 돌아갈 수 있으며 공격 방법을 발전시킬 수 있습니다.

방어를 위한 팁: 네트워크 보안 강화

- 방어 우회 및 모니터링 전술을 방해하려면 모든 네트워크 트래픽과 엔드포인트를 분석하고 수시로 비정상 동작을 찾아봅니다.
- 공격자를 속여 액세스하도록 만드는 위장 파일 또는 시스템인, 허니팟을 설정하여 사용자 정보와 로깅된 키 입력을 비롯한 허니팟에서의 활동 세부 정보와 함께 즉각적인 경보가 보안 팀에 트리거되도록 합니다.
- 비정상적인 데이터 전송을 모니터링하거나 제한합니다. 특히 다음과 같은 활동이 필요합니다.
  - 정보를 추출하는 데 사용할 수 있는 RAR 파일 작성을 모니터링하고 검사합니다. 외부 주소로 전송되는 이메일의 급격한 증가에 대해 조사합니다.
  - 자동 전달 규칙과 새로운 이메일 위임 작성을 모니터링합니다.
  - FTP(File Transfer Protocol) 또는 DNS(Domain Name Server)를 통해 나가는 과도한 트래픽이 있는지 모니터링합니다.

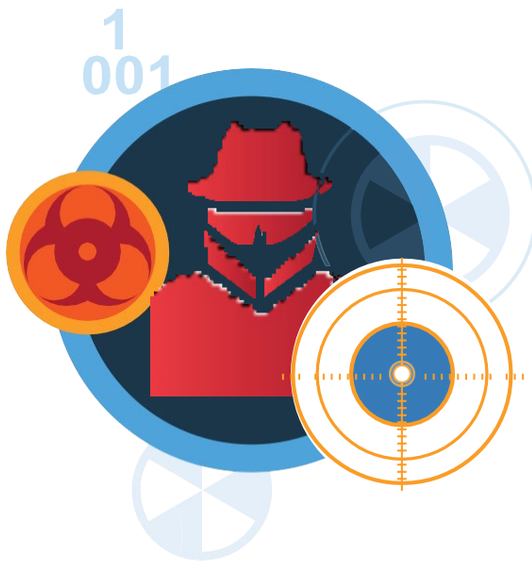
X-Force IRIS 사이버 공격 프레임워크가 이미 네트워크에 들어와 있는 공격자를 퇴치하는 데 어떻게 도움이 되는지 알아보십시오.

공격 목표 이행: 공격자 임무 완수

목표 이행. 실행 단계가 성공적으로 완료되면 공격자는 최종 목표 달성을 위한 활동을 계속합니다. 여기에는 금융 절도, 데이터 절도, 이념적 메시지 전달 또는 산업 스파이 활동으로 인한 비즈니스 중단이 포함될 수 있습니다.

사이버 공격 전략 수립

공격자가 네트워크에 진입하는 것을 효과적으로 방지하기 위해서는 공격자의 관점에서 사이버 공격 기법을 전반적으로 살펴보아야 합니다. X-Force IRIS 프레임워크는 공격 라이프사이클의 각 단계에 대한 포괄적이고 반복 가능한 분석을 제공하여 보안 분석가와 위협 사냥꾼이 악의적인 동작의 패턴을 더욱 효율적으로 파악하고 추적 및 방어할 수 있도록 지원합니다.



방어를 위한 팁: 네트워크 보안 강화

- 보안 침해 사고에 대응할 전담 팀을 구성하고 교육합니다. IBM X-Force IRIS 팀은 네트워크 포렌식 및 로그 분석에서 멀웨어 분석 및 위협 인텔리전스에 이르기까지 다양한 기술을 갖춘 보안 전문가를 지원합니다.
- 사이버 공격을 모방한 모의 훈련이나 시뮬레이션을 활용하여 관련 공격 시나리오를 연습합니다. IBM X-Force 커맨드 센터에서는 잠재적 사이버 공격에 대비하는 데 도움이 되는 현실적인 몰입형 시나리오를 제공하며 위협에 대비해 방어하는 데 필요한 전술과 툴도 지원합니다.
- 사용 가능한 포렌식 자료를 철저히 검토하여 공격에 대한 세부 정보를 파악하고, 완화 우선순위를 설정하고, 법 집행 기관에 데이터를 제공하고, 리스크 감소 전략을 수립합니다. Strategic Threat Assessment와 같은 X-Force IRIS 솔루션은 공격자 및 목표 분석에 도움이 됩니다.
- IBM X-Force IRIS Vision Retainer와 같이 신뢰할 수 있는 보안 파트너를 포함하는 침해 사고 대응 서비스를 고려해봅니다. 강력한 침해 사고 대응 계획을 수립하여 공격 전에 테스트하고 대비합니다.

보안 팀이 이 프레임워크를 사용하여 침해와 관련된 재무 손실 및 평판 하락을 최소화할 수 있는 방법에 대해 알아보십시오.

IBM Security

자세한 정보

효과적인 사이버 공격 전략 수립에 대해 자세히 알아보려면 IBM 영업대표 또는 IBM 비즈니스파트너에게 문의하거나 ibm.com/security/services/ibm-x- force-incident-response-and-intelligence 웹사이트에서 확인하십시오.

보안 침해를 겪고 있는 경우 1-888-241-9812(미국 및 캐나다) 또는 (001) 312-212-8034(미국 및 캐나다를 제외한 지역)로 연락하여 IBM X-Force 침해 사고 대응 담당자에게 문의하십시오.

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
2018년 10월

61019161-KRKO-00