COHESITY

백서

랜섬웨어 복원력 확보를 위한 로드맵

목차

사이버 복원력 대 데이터 복원력

대부분의 기업에서는 업무 연속성 및 재해 복구(Business Continuity and Disaster Recovery, BC/DR)의 형태로 데이터 복원력 전략이 마련되어 있지만, **데이터** 복원력을 위해 설계된 기술과 프로세스가 랜섬웨어 시대에 항상 진정한 **사이버** 복원력으로 이어지는 것은 아닙니다.

사이버 복원력이 뛰어난 회사를 만들려면 커뮤니케이션, 협업, 보안 도구, 인증 시스템, 백업 플랫폼 및 기타 여러 시스템의 호스트가 다음을 위해 필요합니다.

- 공격 발생 방식 조사
- 영향을 받는 데이터 주체, 규제 기관 및 법 집행 기관과 소통
- 재발 위협 완화
- 프로덕션으로 복구

와이퍼 공격이라고도 하는 파괴적인 사이버 공격은 조사 워크플로를 시작하기도 전에 대응 및 통신 기능을 복구해야 하므로 기존의 탐지-대응-복구 흐름을 더 반복적으로 변경합니다. 이러한 경우, 백업 및 복구 플랫폼은 사고 대응자를 위한 신뢰할 수 있는 포렌식 소스 역할을 하는 데 매우 중요합니다.

사이버 복원력을 달성하고 최신 사이버 공격을 견디기 위해 기업은 성공의 기반이 되는 두 가지 영역을 고려해야 합니다.

1. 복구 기능은 공격자가 도달할 수 없는 곳에 있어야 합니다.
2. 대응 계획에서는 프로덕션 시스템뿐만 아니라 사고에 효과적이고 효율적으로 대응하는 데 필요한 보안, 인증 및 통신 플랫폼의 신속한 복구를 위한 대비 조치를 갖추어야 합니다.

랜섬웨어 및 와이퍼 공격에서 복구-대응-복구의 반복적인 특성으로 인해 보안팀과 IT 운영팀은 이러한 공격의 영향을 최소화하기 위해 긴밀하게 협력해야 합니다.

사이버 복원력 프로그램 만들기

홍수, 화재 및 자연 재해와 같은 전통적인 BC/DR 시나리오에서 사고의 근본 원인을 신속하게 확인할 수 있습니다. 랜섬웨어 공격의 경우, 공격자는 몸값 지불만이 피해자의 유일한 옵션이 되도록 복구를 중지하기 위해 적극적으로 방해하고 있습니다.

이러한 공격자는 표적의 방어 체계에 지속적으로 적응하므로 공격의 성격을 확립하고 복구할 올바른 프로세스를 이해하는 데 있어 규범적인 조사 및 대응 프로그램이 매우 중요합니다. 또한 이 조사를 통해 조직에서는 공격이 성공할 수 있게 해준 취약점에 대한 가시성을 확보하고 향후 사고를 방지하기 위한 방어 체계를 강화할 수 있습니다. 이는 대응이 거의 즉각적으로 이루어질 수 있는 전통적인 재해와 대조됩니다.

사이버 공격에 맞서 복원력을 갖추거나 생존하려면 단순히 기술을 사용하는 계획 그 이상의 것이 필요합니다. IT 및 보안 팀은 공격자와 이들이 시도하는 공격의 유형을 이해해야 합니다. 이러한 유형의 인텔리전스를 통해 표적 방어 체계를 구축하여 공격을 차단하거나 조기에 탐지할 수 있는 가능성이 커집니다. MITRE ATT&CK와 같은 프레임워크를 통해 조직은 표준화된 방식으로 위협을 정량화하고 복구 방법을 전달할 수 있습니다.

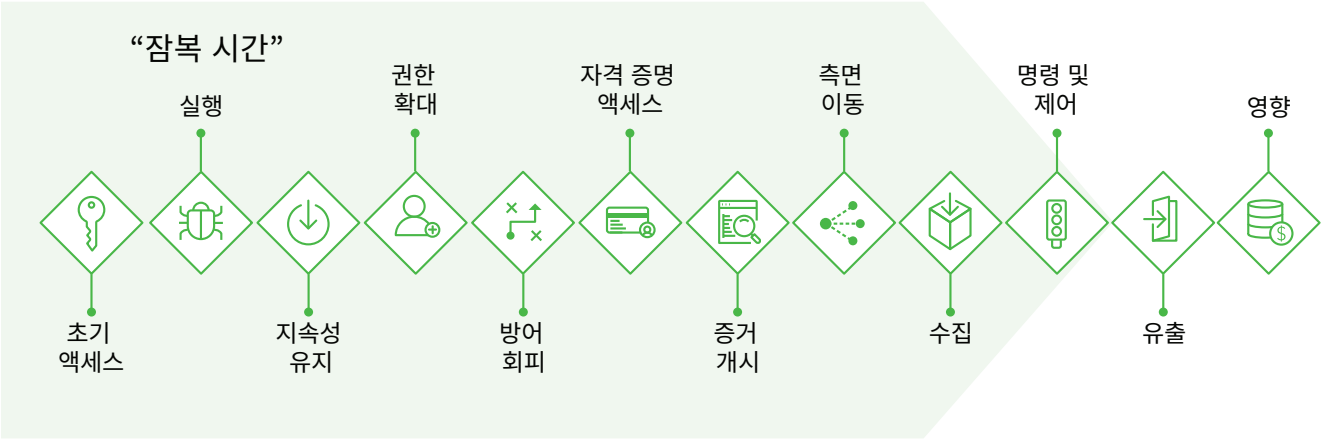
예를 들어, 아래 다이어그램은 랜섬웨어가 활성화되기 전에 공격자가 해당 환경에 머무르면서 무엇을 할 수 있는지 보여줍니다. 어떤 경우에는 랜섬웨어 페이로드가 성공하는 데 필요한 조치가 될 수 있는 반면, 어떤 경우에는 공격자가 네트워크에서 끈질기게 머물러 향후 공격을 시작하는 데 도움이 될 수 있습니다. "잠복 시간"은 수일에서 수개월이 될 수 있습니다. 공격자가 해당 환경에서 어떻게 작동하는지 알면 보안팀이 공격 지표를 선제적으로 찾을 수 있습니다.

> 잠복 시간은 공격이 탐지되기 전에 악의적인 공격자가 침해된 시스템에 액세스하는 시간을 말합니다. 잠복 시간이 길어지면 공격자가 피해를 입히거나 민감한 정보를 훔칠 기회가 더 많아집니다.

다이어그램의 각 작업을 공격의 단계로 간주해 보십시오. 심지어 페이로드가 활성화되기도 전에 12단계 중 10단계가 실행된다는 점은 놀랍습니다. 랜섬웨어 공격의 경우, 암호화 또는 데이터 유출이 시작되기 전에 시스템이 완전히 침해됩니다. 네트워크에 이러한 기반을 둔 공격자는 복구 작업을 방해하고 새로운 공격을 시작하여 여러 건의 몸값을 갈취할 수 있습니다. 이를 '더블 버블' 또는 '더블 탭' 랜섬웨어라고 하며, 공격자가 꾸준한 수익원을 창출하는 데 점점 많이 사용되는 방법입니다.

단 한 번의 공격만으로도 상품 및 서비스 제공에 방해될 수 있으므로 피해자에게 치명적일 수 있습니다. 그러나 여러 번의 공격에 노출되면 다음을 비롯한 2차 손실 가능성이 커집니다.

- 평판 손상
- 데이터 주체 및 파트너의 소송
- 데이터 주체의 정보를 적절히 보호하지 않는 것에 대한 규제 벌금



더욱 복잡한 문제는 공격자가 네트워크에 더 오래 머무를수록 공격의 아티팩트가 백업에 저장될 가능성이 커진다는 점입니다. 이러한 아티팩트가 식별 및 제거되지 않고 복구되면 공격이 다시 시작될 수 있습니다. 이와 같은 시나리오는 랜섬웨어 공격에서 복구된 조직이 깨끗한 데이터를 복구하지 못할 때 자주 발생합니다.

조직은 디지털 포렌식 및 사고 대응(Digital Forensics & Incident Response, DFIR) 프로세스를 따라 보안 운영 센터 내에서 깨끗한 데이터를 복구해야 합니다. 역사적으로 DFIR은 다음에 의존해 왔습니다.

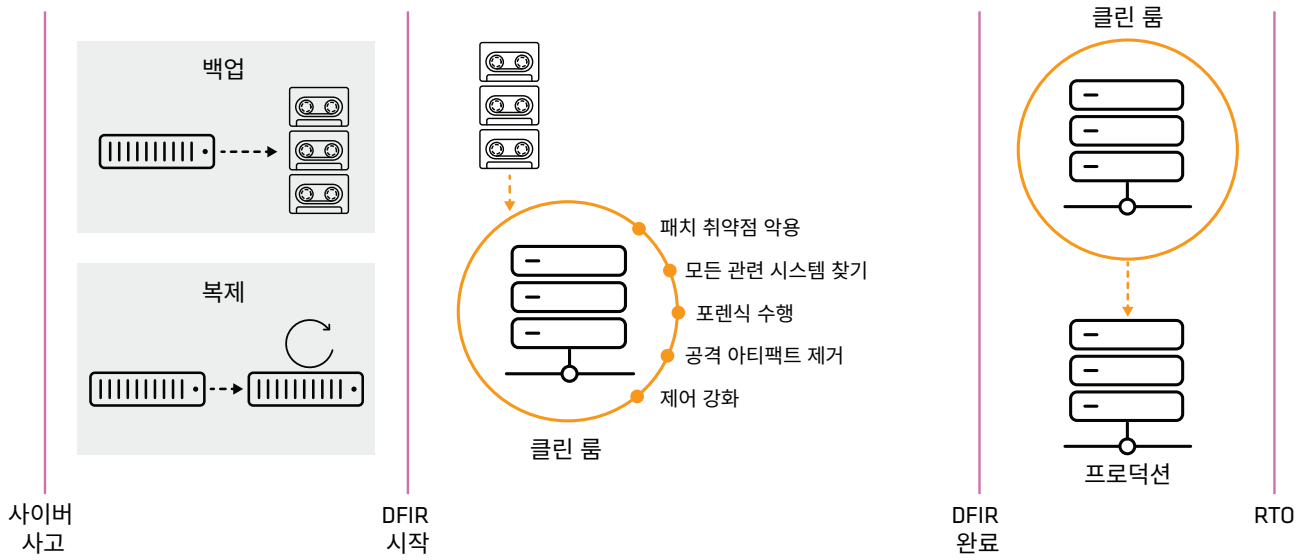
- 침해된 호스트의 포렌식 이미징
- 조사 프로세스 및 도구를 적용하여 사고 타임라인 식별
- 공격에 사용되는 바이너리 아티팩트 찾기 및 분석
- 사용된 권한 확대 및 지속성 방법 파악
- 사고 범위를 확장하기 위해 다른 침해된 시스템 찾기
- 플랫폼이 다시 프로덕션 단계로 들어가기 전에 해결할 취약점 스캔
- 예방 및 탐지 제어로 공격을 멈추거나 탐지하지 못한 이유 파악

일반적으로 이러한 작업은 격리된 복구 환경(Isolated Recovery Environment, IRE) 또는 "클린 룸" 환경에서 수행됩니다.

물론 삭제되거나 암호화된 시스템을 포렌식으로 이미징해도 의미 있는 증거를 얻을 수 없으므로 사고 대응자는 조사를 위해 백업 저장소에 의존하기 시작했습니다. 백업 데이터를 사용하면 시간에 따른 변경 사항을 확인하고 공격의 수명 주기를 추적할 수 있습니다.

Cohesity는 DFIR 프로세스를 시작할 수 있는 변경 불가능하고 포렌식 측면에서 타당한 플랫폼을 제공합니다. 조사관은 API를 통해 신속하게 인스턴스화 및 오케스트레이션할 수 있는 과거 파일 시스템 스냅샷에 액세스할 수 있으므로, 영향을 받는 시스템의 컨텍스트뿐만 아니라 전체 사고 타임라인 동안 파일 시스템에 대한 인사이트도 제공합니다. 이는 분석가에게 시간 여행의 초능력을 부여하는 것과 같습니다. 분석가는 시간이 지남에 따라 파일 시스템을 비교하여 지속성을 유지하기 위한 구성 파일 변경, 악성 복사본으로 합법적인 바이너리 및 라이브러리 덮어쓰기 또는 공격에 사용되는 기타 악성 아티팩트 식별과 같은 적대적인 기술을 식별할 수 있습니다.

> 복구 시간 목표(RTO)는 예기치 않은 중단 후 네트워크 또는 애플리케이션을 복원하고 데이터에 다시 액세스할 수 있을 때까지 허용되는 최대 시간입니다.



DFIR 프로세스에 백업 인프라를 포함하면 데이터를 프로덕션에 다시 투입하기 전에 조사를 완료할 수 있습니다. 여기서의 과제: 이 문제는 조직에서 설정한 복구 시간 목표(Recovery Time Objective, RTO)에 부정적인 영향을 미칠 수 있습니다. 결국, 대부분의 RTO는 사이버 공격 중에 필요한 조사를 고려하도록 계산되지 않았습니다.

백업을 활용하여 클린 룸 환경을 조성하면 전체 가동 중단 시간을 줄이고 복원된 데이터가 깨끗한지 확인하여 재감염 시 프로세스를 다시 거칠 필요가 없습니다. 이를 통해 조직이 RTO를 충족하고 지속적인 가동 중단 시간을 피할 수 있도록 지원합니다.

계획에서 실행까지의 사이버 복원력

철저한 대비

모든 이해관계자와 협력하여 기능 간 랜섬웨어 복원력 팀을 구성합니다.

랜섬웨어 사고는 기타 사이버 공격과 다릅니다. 이는 조직 전체와 고객에게 제품과 서비스를 제공하는 능력에 영향을 미칩니다. 대응과 회복에 걸리는 매 순간이 1차 손실입니다. 직원은 소통할 수 없고 업무를 수행할 수 없습니다. 언론은 사건을 보도하려고 적극적인 관심을 보일 것입니다. 그리고 고객은 좌절할 것입니다. 사이버 공격 발생 시 조직의 모든 사람이 자신의 역할을 아는 것이 중요합니다.

여기에는 다음을 결정하는 것이 포함됩니다.

- 이메일과 같은 주요 방법이 작동하지 않을 경우 소통이 이루어지는 방식
- 각 기능 및 대응 단계를 주도할 사람
- 팀원이 부재 중일 경우 따라야 할 프로세스 및 2차 연락 담당자

대응 및 복구에 직접 관여하지 않는 직원들도 자신에게 기대되는 사항을 알아야 합니다. 이유가 무엇일까요? 신뢰할 수 있는 정보가 없으면 소문과 추측이 대응을 방해하고 회복을 늦출 수 있기 때문입니다.

모든 이해관계자와 함께 사실적인 가상 랜섬웨어 시뮬레이션을 수행합니다.

조직을 하나로 모으는 가장 좋은 방법 중 하나는 조직의 특성에 초점을 맞춘 사실적인 가상 랜섬웨어 시뮬레이션입니다. 실제 랜섬웨어 공격 중에 직면할 가능성이 높은 랜섬웨어 대응에 대한 몇 가지 위협과 과제에 대한 인사이트를 얻을 수 있습니다.

랜섬웨어 위험 계산 시 모든 영향을 고려하십시오. 영향은 다음과 같습니다.

- 1차 영향:
  - 조직이 제품과 서비스를 제공할 수 없는 경우.
- 2차 영향:
  - 전문 서비스 및 랜섬웨어 운영자에게 지불하는 비용을 포함하여 사고 조사 및 대응에 드는 운영 비용
  - 조직에 대한 평판 훼손
  - 랜섬웨어 사건과 관련된 규제 벌금 또는 제재 대상 기관에 대한 지급
  - 지적 자본 손실
  - 데이터 침해와 관련된 파트너 또는 고객의 소송

랜섬웨어 위험을 기업 위험 관리에 통합합니다.

명백해 보이지만, 많은 기업들이 랜섬웨어가 미치는 영향을 중대한 운영 위험으로 간주하지 않습니다. 조직의 기업 위험 관리에 랜섬웨어 위험을 통합하면 사이버 보안 정책에 대한 적절한 지원을 얻기 위해 적절한 수준의 거버넌스를 수립하고 적절한 수준의 위험 관리를 유지하는 데 도움이 됩니다.

전사적 랜섬웨어 정책을 만듭니다. 다음을 수행해야 합니다.

- **랜섬웨어 공격으로 선언할 사고에 대한 명확한 기준을 제시합니다.** 랜섬웨어에 대응하고 랜섬웨어로부터 복구하는 워크플로는 기존 악성 코드 및 데이터 유출을 처리하는 워크플로와 다릅니다. 사고를 신고할 수 있는 권한을 SOC 분석가에게 부여하는 기준을 수립하여 적절한 조사, 억제 및 근절 조치를 취할 수 있도록 해야 합니다. 이러한 명확성 없이는 SOC가 이러한 조치를 취할 수 있는 권한을 요청하는 동안 랜섬웨어 공격이 조직 내에 확산될 수 있습니다.

- **사이버 백업 전략을 정의합니다.** 사이버 복원력 시나리오에 대한 백업 전략은 기존 재해 복구 및 비즈니스 연속성 사건에 대한 데이터 복원력 전략과 다를 수 있습니다. 이는 대응 및 복구 능력의 구조와 성숙도에 따라 결정됩니다.
  - 백업 데이터만 해당: 사고를 조사하고 베어메탈에서 인프라를 다시 구축하는 데 필요한 서버를 가져온 다음 데이터를 복구합니다. 이 정책은 취약점 및 구성 오류 스캔을 포함하여 복구에 사용되는 Golden Master 이미지가 유지되는 방법을 설정해야 합니다.
  - 백업 인프라: 전체 인프라를 복구한 다음, 사고 대응에 따라 다양한 부분을 다양한 지점으로 복원하여 이를 정리합니다.
- **운영 복원력 범주를 정의합니다.** 이러한 범주는 이미 수립된 데이터 복원력 비즈니스 영향 분석을 기반으로 하며, 클린 룸 내에서 대응 도구를 도입할 수 있는 기능과 사이버 복원력 백업 전략을 포함합니다.
  - **사고에 대응하고 복구하는 데 필요한 통신 및 보안 인프라를 복구하는 기능을 포함합니다.** 고려 사항:
    - 물리적 액세스 제어
    - 도메인 이름 서비스
    - 음성 통신
    - 이메일
    - 대응을 조정하는 데 사용되는 협업 플랫폼
    - 사례 관리
    - 포렌식 및 사고 대응 도구
    - 취약점 스캔 및 관리
    - ID 및 액세스 관리
- **조직이 몸값 지불을 고려할 조건을 정의합니다.**
  - 조직은 몸값을 지불하기 위해 어떻게 자금을 확보합니까?
  - 조직의 보험 증권에 몸값 지불이 포함되어 있습니까?
  - 보험사는 게릴라식 랜섬웨어 공격자의 행동을 전투원으로 간주합니까?
  - 보험사가 제재 대상 법인에 대한 지급을 보장합니까?
  - 랜섬웨어 운영자와의 협상에 대한 조직의 접근 방식은 무엇입니까?
  - 예를 들어, 지급을 받는 그룹이 제재를 받는 경우 평판, 규제 및 형사상 영향은 무엇입니까?
  - 귀사는 몸값을 지불하기 위해 어떻게 암호화폐를 얻습니까? KYC(Know Your Customer) 타임라인을 확인하는 데 걸리는 시간을 고려하십시오.
- **랜섬웨어 정책이 주기적으로 업데이트되었는지 확인합니다.** 이렇게 하면 랜섬웨어 공격의 변화하는 특성을 더 잘 반영할 수 있습니다.

미리 대비

- **랜섬웨어 운영자와 그들의 도구, 기술 및 절차(TTP)를 이해합니다**.
  - 랜섬웨어 갱단, 캠페인 및 기술에 대한 정부, 상업 또는 오픈 소스 인텔리전스를 확보합니다.
  - 수직 시장 또는 지역에서 랜섬웨어 운영자와 운영 관련 와이퍼 공격을 수행하는 공격자에 대한 인텔리전스 수집 및 분석을 최우선으로 합니다.
  - MITRE ATT&CK 프레임워크에 대해 사용하는 기술을 매핑합니다.
  - 랜섬웨어 갱단이 사용하는 최신 기술을 통합하여 정기적인 피싱 테스트를 계획합니다.

  - 랜섬웨어 운영자가 악용하는 취약점에 대한 패치가 취약점 관리 프로그램에서 우선적으로 적용되는지 확인합니다.
  - 랜섬웨어 운영자가 타사와 관리형 서비스 제공업체 간의 관계를 악용하여 귀사와 유사한 조직을 표적으로 삼는 방법을 이해합니다. 제3자 위험 평가 및 통제에서 이 점을 고려하십시오.
- **연락처 정보를 문서화하고 유지합니다.** 가능하면 랜섬웨어 사고가 영향을 미치지 않는 대역 외 통신 채널을 통해 대응팀의 모든 구성원과 백업 구성원, 주요 직원 및 주요 이해관계자를 포함하십시오.
- **보고 채널을 생성합니다.** 랜섬웨어 사고를 보고하도록 고객, 동료 조직 및 공급망 파트너와 같은 제3자를 포함합니다.
- **내부 사용자가 랜섬웨어와 유사한 행동을 보고할 수 있는 보고 채널을 생성합니다.** 캡처:
  - 보고자의 이름 및 역할
  - 발생 시기
  - 보고자가 인지한 사항
  - 랜섬웨어라고 생각한 이유
  - 당시 하고 있던 작업
  - 보고자의 물리적 위치 및 연결된 네트워크
  - 사용하고 있던 계정
  - 사용하고 있던 시스템(운영 체제, 호스트 이름, IP 주소)
  - 로그인한 계정
  - 연락한 대상 및 알려준 내용
  - 보고자가 담당 역할에서 일반적으로 액세스하는 항목
- **조직과 관련된 랜섬웨어 또는 와이퍼 사고를 법 집행 기관 및 사이버 보안 기관에 보고할 수 있는 보고 채널을 만듭니다.**
- **사이버 위기 대응 팀을 구성합니다.** 포함:
  - 비즈니스 리더
  - IT(복구 및 취약점 관리 포함)
  - OT(관련된 경우)
  - 보안 운영(사고 대응 관리자, 디지털 포렌식, 그리고 조직이 보유하고 있는 경우 악성 코드 리버스 엔지니어링, 헌팅 팀, 위협 인텔리전스 포함)
  - 법률 고문
  - PR
  - 인사
- **필요한 경우, 사고 대응 조직의 서비스를 유지합니다.**
  - 사고 대응 조직과 계약을 맺기 위해 사전 승인을 받습니다.
  - 사고 대응을 위해 보험사에 의존하는 경우, 보험에 가입했을 때 작성된 증명서를 통제하고 실제 랜섬웨어 사고를 처리하기 위해 규정 미준수의 증거를 찾을 수도 있습니다.
- **보류 진술 및 위반 발표 템플릿의 초안을 작성합니다.** 명세서 초안을 대부분 작성해 놓으면 나중에 세부 정보를 추가해야 할 경우에도 신속하게 대응하고 추측을 피하기가 더 쉬워집니다.
  - 미디어 교육을 받고 침해 대응 행동 기록에 대해 교육을 받은 조직의 대변인과 백업 담당자를 지명합니다.
  - 브리핑 및 미디어 인터뷰를 위한 커뮤니케이션 채널(사고의 영향을 받지 않는 채널)을 준비합니다.
- **법 집행 기관 및 국내 컴퓨터 비상 대응 팀과의 관계를 사전에 수립합니다.**
- **법률 고문이 법 집행 기관과의 계약을 검토하도록 합니다.**
- **법률 고문이 제안된 대응 계획 및 진술, 민사, 규제 및 형사 책임의 가능성을 검토하도록 합니다.**

공격 범위 축소

- **랜섬웨어 갱단에 의해 종종 악용되는 취약점이 있는 시스템에 대한 패치 적용의 우선순위를 정합니다.** 중요한 자산 취약점을 식별하고 패치를 적용합니다.
- **시스템을 강화합니다.** 위협 인텔리전스를 통해 발견된 랜섬웨어 갱단이 사용하는 중요한 시스템과 공격 벡터의 우선순위를 정합니다. 포트 및 프로토콜을 사용하여 장치를 올바르게 구성하고 업무 목적으로 사용되지 않는 장치를 비활성화합니다. 랜섬웨어 운영자는 합법적인 도구를 사용하여 'Living off the Land(LOTO)' 공격을 하므로 이러한 도구에 대한 액세스를 제한하면 공격 가능성이 줄어듭니다.
- **원격 데스크톱 프로토콜 및 기타 원격 데스크톱 서비스 사용에 대한 모범 사례를 따릅니다.** 원격 액세스 서비스는 랜섬웨어 운영자의 기본 초기 액세스 벡터입니다. 지정된 시도 횟수 이후 계정 잠금, 다단계 인증, 모든 원격 데스크톱 로그인 시도 기록을 적용합니다. 원격 데스크톱 서비스에 대한 유효한 비즈니스 이유로 원격 액세스가 정당화되는지 확인합니다. 원격 데스크톱 서비스의 무단 사용에 대해 네트워크를 감사합니다.
- **파일 공유 프로토콜을 비활성화하거나 차단합니다.** 여기에는 서버 메시지 블록(Server Message Block, SMB) 프로토콜 아웃바운드 및 오래된 버전의 파일 공유 프로토콜 제거 또는 비활성화가 포함됩니다. 위협 행위자는 파일 공유 프로토콜을 사용하여 조직 전체에 악성 코드를 전파합니다.
- **모든 시스템에 대한 자격 증명 및 액세스 권한이 최소 권한에 따라 관리되는지 확인하고 특권 계정 수를 제한합니다.**
- **특권 계정이 일상적인 활동에 사용되지 않도록 합니다.**
- **네트워크 세분화를 구현합니다.** 네트워크 세분화는 랜섬웨어의 확산을 제한하고 내부망 이동을 탐지할 가능성을 높이는 가장 효과적인 방법 중 하나입니다.
- **기준 구성 및 구현 변경 제어를 사용합니다.** 기본 구성과 변경에 대한 지식을 사용하면 조사 중에 백업 이미지를 알려진 적합한 이미지와 비교할 수 있습니다.
- **조직 내에서 보안이 취약한 데이터 저장소를 식별합니다.** Cohesity DataHawk 데이터 분류는 백업 전반에서 스캔하여 프로덕션 시스템에 영향을 주지 않고 민감한 데이터를 식별합니다. 조직에서는 민감한 데이터가 어디에 있는지 종합적으로 파악하여 해당 데이터의 위험을 평가할 수 있습니다.

백업 보호

- **백업 시스템에 에어 갭이 충분히 적용되었는지 확인합니다.** 이렇게 하면 공격자가 삭제하거나 손상시키지 못합니다. Cohesity FortKnox는 가상 에어 갭을 통해 Cohesity 관리형 클라우드 볼트에서 변경 불가능한 데이터 복사본으로 사이버 복원력을 개선합니다.
- **공격자가 백업 시스템을 손상시키거나 삭제하지 못하게 하는 변경 불가능한 데이터 저장소를 사용하도록 합니다.** 예를 들어, Cohesity Data Cloud는 데이터 잠금 기능이 있는 변경 불가능한 스토리지 플랫폼을 기반으로 구축되어 권한이 확대된 사용자도 백업을 삭제하지 못하도록 합니다.
- **백업 관리자 계정에서 다단계 인증을 사용합니다.** 기본 ID 및 액세스 관리 서버가 랜섬웨어의 영향을 받는 경우에 대비하여 여러 옵션을 구현합니다. Cohesity는 SSO 및 TOTP 다단계 접근 방식을 모두 지원합니다.
- **역할 기반 액세스 제어(Role-Based Access Control, RBAC)를 사용하여 최소 권한을 할당합니다.** 백업 시스템 사용자에게는 역할과 관련된 작업 수행에 필요한 최소 권한만 할당해야 합니다. Cohesity에는 최소 권한을 지원하는 세분화된 RBAC가 있습니다.
- **침해된 관리자 계정이 악의적인 변경을 하지 못하도록 백업 시스템에 업무 분리가 이루어지도록 합니다.** Cohesity의 쿼럼 기능을 통해 조직은 백업 및 복구와 관련된 작업에 대한 여러 계층의 권한 부여를 정의할 수 있습니다.
- **3-2-1 백업 전략을 채택합니다.** 2개의 서로 다른 매체에 3개의 데이터 복사본을 보관하고, 그중 1개 이상의 복사본을 외부에 보관합니다.
- **정기적으로 백업을 테스트합니다.** 백업 테스트를 정기적으로 수행하고 자동화해야 합니다. 필요한 경우 시정 조치를 취할 수 있도록 테스트 결과를 보고합니다. Cohesity DataProtect는 자동화된 테스트를 지원합니다.

- **중요 시스템의 완료/실패/테스트된 백업 범위에 대한 지표를 수집하고 보고합니다.**
- **성장을 위해 백업 인프라에 적절한 용량을 확보합니다.**
- **백업 시스템이 랜섬웨어 사고에 대응하는 데 필요한 사이버 보안 기능을 지원할 수 있는지 확인합니다.** 사고 발생 시 보안 팀은 암호화되어 있으므로 피해자 시스템을 포렌식으로 이미지화할 수 없습니다. 보안 팀은 백업 시스템에 의존하여 사고를 조사할 수 있어야 합니다. Cohesity는 데이터 분류, 위협 인텔리전스 피드 및 헌팅과 같은 대응 기능을 데이터 관리 플랫폼 자체에 구축했습니다. 또한 데이터 보안 연합(Data Security Alliance)을 통해 Splunk, Cisco, Palo Alto, Tenable, Qualys, Crowdstrike 및 ServiceNow와 같은 주요 보안 공급업체와 사전 통합된 솔루션을 제공합니다.
- **사고 후 재구축 속도를 높이기 위해 중요한 시스템의 골든 마스터를 구축하고 유지 관리합니다.** 클린 룸 내에서 시스템을 재구축하기 위해 신속하게 배포할 수 있는 사전 구성된 운영 체제 및 관련 애플리케이션 소프트웨어가 포함된 이미지 템플릿을 유지합니다.

랜섬웨어 보호 강화

- **랜섬웨어 갱단이 사용하는 ATT&CK 기술에 대한 기존 예방 및 탐지 제어 범위의 격차를 식별합니다.** 이를 지속적으로 수행하여 공격자가 행동을 조정할 때 예방 또는 탐지 가능성을 극대화합니다.
  - 예방, 탐지 및 대응 단계에서 사용할 수 있는 일반적인 침해 지표(IOC)는 다음과 같습니다.
    - 비정상적인 파일 트랜잭션(암호화 및 삭제 볼륨 편차)
    - 서비스 및 애플리케이션의 의심스러운 부팅 시간
    - 알 수 없고 예기치 않은 서비스 및 애플리케이션이 있음
    - 무단 원격 액세스/VPN 소프트웨어의 존재
    - 시스템 성능 저하(CPU/RAM 사용률 증가)
    - 저하/비활성화된 호스트 보안 계측 성능, 보안 에이전트 비활성화됨
    - 알 수 없는/예기치 않은 도메인 이름 및 IP 주소 연결
    - 프로토콜 불일치
    - 알려진 잘못된 파일 해시
    - 구성 파일에 대한 의심스러운 변경
    - 비정상적인 인바운드 및 아웃바운드 트래픽 또는 소스/대상
    - 메모리 덤프의 의심스러운 프로세스 및 텍스트
    - 로그인한 사용자의 의심스러운 계정(과거 및 현재)
    - 의심스러운 네트워크 공유 및 마운트된 네트워크 공유
    - 의심스러운 사용자 계정
    - 의심스러운 인증서 설치
    - ARP 및 DNS 캐시의 의심스러운 항목
    - 시스템 또는 로그 파일 또는 NTP 서버의 날짜/시간 이상
    - DHCP 로그의 의심스러운 항목 또는 임대
    - 비정상적인 사용자 에이전트 문자열
    - 비표준 애플리케이션 비컨 및 업데이트
    - 전체 패킷 캡처 내부의 바이너리
- **예방적이고 탐지적인 콘텐츠를 테스트합니다.** 랜섬웨어 IOC에 대해 생성된 규칙을 테스트합니다.
- **파일 암호화 또는 삭제와 같은 랜섬웨어 및 와이퍼 공격에 해당하는 엔드포인트 파일 시스템 이상 탐지를 구현합니다.** Cohesity는 머신 러닝을 사용하여 이러한 패턴을 식별합니다.
- **이메일 게이트웨이 필터를 구현하여 알려진 악성 지표가 있는 이메일을 차단합니다.**
- **사용자의 받은 편지함에서 랜섬웨어 관련 콘텐츠를 담고 있는 것으로 식별된 이메일을 제거하는 메커니즘을 구현합니다.**

- **도메인 기반 메시지 인증, 보고 및 적합성(Domain-based Message Authentication Reporting and Conformance, DMARC) 정책 및 검증을 구현합니다.** 유효한 도메인에서 위조되거나 변조된 이메일을 받을 가능성이 줄어듭니다.
- **특정 비즈니스 요구 사항이 없는 한 이메일을 통해 전송되는 Microsoft Office 파일의 매크로를 비활성화합니다.**
- **중요한 자산에 대한 목록/화이트리스팅을 허용하는 애플리케이션을 사용하여 승인된 소프트웨어만 실행할 수 있도록 합니다.** Windows 플랫폼에서는 Microsoft 소프트웨어 제한 정책 또는 AppLocker를 사용합니다. 가능한 모든 애플리케이션을 나열하는 것보다는 디렉토리 허용 목록을 사용하십시오. 많은 랜섬웨어 공격 벡터의 실행을 제한하는 기본값을 사용하면 애플리케이션을 PROGRAMFILES, PROGRAMFILES(X86) 및 SYSTEM32에서 실행할 수 있지만, 'Living off the Land(LOTO)' 공격을 막지는 못합니다. 특정 애플리케이션에 예외가 허용되지 않는 한 다른 모든 위치를 허용하지 않습니다.
- **공급망의 위험 관리 및 사이버 위생 관행, 제3자 파트너, 관리형 서비스 제공업체(MSP)를 이해합니다.** 많은 랜섬웨어 공격은 제3자를 통해 이루어집니다.
  - 사이버 위험 관리 및 통제에서 회사와 파트너의 역할을 이해합니다. 역할과 책임이 명확하게 정의되고 측정되며, 시정 조치를 위한 메커니즘이 계약서에 포함되도록 합니다.
- **특히 원격 액세스 및 특권 계정의 경우 가능한 한 많은 서비스에서 다단계 인증을 사용합니다.**
- **논리적 또는 물리적 네트워크 세분화를 구현하여 사업부 또는 IT 리소스의 범주 및 모든 운영 기술(OT) 환경을 분리합니다.** 이렇게 하면 공격 발생 시 랜섬웨어 확산이 제한됩니다.
- **Living off the Land(LOTO) 공격에 PowerShell이 사용될 기회를 줄입니다.**
  - 사례별로 PowerShell 사용을 특정 사용자로 제한
  - PowerShell을 버전 5.0 이상으로 업데이트하고 이전 PowerShell 버전 모두 제거
  - 모듈, 스크립트 블록 및 전사 로깅이 활성화되어 있는지 확인
  - PowerShell이 활성화된 시스템에서 "PowerShell" Windows 이벤트 로그 및 "PowerShell Operational" 로그의 보존 기간이 180일 이상인지 확인
- **비정상적인 동서 및 남북 트래픽 패턴에 대한 과거 네트워크 트래픽을 분석합니다.** 네트워크 트래픽 메타데이터(NetFlow/sFlow)를 사용하거나, 가능한 경우 전체 패킷 캡처 또는 네트워크 침입 탐지/예방 시스템을 사용합니다.
- **도메인 컨트롤러를 보호합니다.**
  - **데이터 관리 및 보안 에이전트 외에 도메인 컨트롤러에 추가 소프트웨어가 설치되지 않았는지 확인합니다.** 도메인 컨트롤러에 대한 액세스는 관리자 그룹으로 제한해야 합니다. 이 그룹 내의 모든 사용자는 일상적인 활동에 별도의 제한된 계정을 사용해야 합니다.
  - **도메인 컨트롤러에서 호스트 방화벽을 구성하여 인터넷에 대한 액세스를 방지합니다.**
  - **가능한 경우 인증에 Kerberos를 사용하도록 활성화하고 NTLM 감사를 활성화하여 네트워크를 통해 NTLM v2 응답만 전송되도록 합니다.**
  - **로컬 보안 인증 보호가 활성화된 경우 LSASS.EXE를 감사하여 어떤 애플리케이션이 영향을 받는지 파악합니다.** 이렇게 하면 코드 삽입으로 자격 증명을 획득하지 못하게 되고 그 영향이 수용 가능한 경우 이러한 보호 기능을 활성화할 수 있습니다.
  - **호스트와 도메인 컨트롤러 간에 SMB 서명이 필요한지 확인합니다.** 이렇게 하면 네트워크에서 재생 공격을 사용할 수 없습니다.

랜섬웨어 탐지 강화

- **과거 데이터를 사용하여 침해를 사전에 찾아냅니다.** 예방 또는 탐지 규칙이 없는 랜섬웨어 갱단과 관련된 새로운 위협 인텔리전스 및 IOC를 사용합니다. Cohesity에는 랜섬웨어 갱단이 사용하는 110,000개 이상의 IOC를 제공하고 백업에 대한 존재를 추적할 수 있는 기능을 제공하는 통합 위협 인텔리전스 피드가 포함되어 있습니다. 공격자는 라이브 시스템이 아닌 백업을 수동적으로 추적함으로써 이 활동을 탐지할 수 없으므로 공격자가 엔드포인트 솔루션에 사용하는 방어 회피 기술의 대상이 아닙니다. 또한 백업의 보존 기간은 보안 솔루션보다 길어 탐지의 범위를 확장할 수 있는 경향이 있습니다.
- **CPU 및 디스크 사용률의 비정상적인 변경에 대한 메커니즘을 구현합니다.** 이러한 지표는 일반적으로 IT 운영 플랫폼에서 수집하지만, 탐지 기능을 개선하기 위한 추가 신호로 보안 팀에 추가로 전달될 수 있습니다.
- **비정상적인 네트워크 프로토콜을 식별합니다.** 여기에는 랜섬웨어 갱단이 사용하는 것으로 알려진 I2P 또는 TOR이 포함됩니다.
- **랜섬웨어 및 와이퍼 명령과 제어에 사용되는 알려진 포트 또는 대상을 사용하여 네트워크 연결을 식별합니다.**

사고에 대응

- **영향을 받는 자산과 관련된 유사한 알림을 식별하고 그룹화합니다.**
- **다음을 포함하여 사고의 초기 손실 예상(폭발 반경)을 작성합니다.**
  - 암호화/삭제된 엔드포인트의 추정 개수
  - 암호화/삭제된 시스템의 영향을 받는 비즈니스 가치 사슬
  - 영향을 받는 데이터의 규제 의무(레코드 수, 데이터 유형)
  - 유출의 증거

Cohesity는 영향을 받는 시스템의 백업을 자동으로 검색하여 랜섬웨어 사고의 잠재적인 규제 영향을 식별합니다. 백업되는 시스템은 사고 발생 전 또는 대응 중에 요구에 따라 백업되는 방식으로 분류할 수도 있습니다.

- **데이터 유출에 사용되는 스테이징 환경을 찾습니다.** 예기치 않게 많은 데이터가 증가하거나 해당 호스트에서 찾을 수 없을 것으로 예상되는 다른 유형의 데이터가 있는 네트워크의 시스템을 식별합니다. Cohesity는 영향을 받는 시스템의 백업을 자동으로 검색하여 랜섬웨어 사고의 잠재적인 규제 영향을 식별합니다.
- **유선 및 무선 네트워크 모두에서 감염된 호스트를 격리합니다.**
- **랜섬웨어의 변종이 알려져 있고 자체적으로 확산되는 경우, 알려진 통신 및 감염 채널(호스트 또는 네트워크 방화벽, 이메일 게이트웨이, 네트워크 액세스 제어)을 차단합니다.**
- **클린 룸을 활성화합니다.** 보안 도구, 통신, 협업 또는 액세스 제어 시스템에 영향을 미치는 경우, 알려진 양호한 인스턴스를 신속하게 인스턴스화하여 대응 활동을 시작할 수 있습니다.
- **영향을 받은 시스템의 마지막 백업을 클린 룸 환경으로 복원합니다.** 이는 조사를 시작하기 위한 포렌식 이미지 역할을 합니다. 다른 시점의 시스템 상태는 과거 추세를 파악하고 시간 경과에 따른 파일 시스템 변경 사항을 식별하는 데 도움이 될 수 있습니다.
- **신뢰할 수 있는 탐지/대응/포렌식 도구를 클린 룸 내부의 시스템에 다시 배포합니다.** 공격자는 탐지를 회피할 수 있도록 엔드포인트 도구를 표적으로 삼습니다. 따라서 엔드포인트 도구가 올바르게 작동하고 있다는 확신이 줄어듭니다. 엔드포인트 도구를 다시 설치하면 적절한 기능을 보장하고 도구가 올바르게 보고하고 있다는 신뢰를 구축할 수 있습니다.

- **랜섬웨어 변종이 알려지지 않은 경우 다음을 수행하여 판단합니다.**
  - 몸값 요구 메시지(암호화 후 자동으로 열릴 수 있는 그래픽 팝업, 텍스트 또는 HTML 파일, 연락처 이메일이 포함된 감염된 시스템의 배경 화면과 같은 이미지 파일, 몸값을 요구하는 사운드 파일) 수집
  - 랜섬웨어 갱단 및 변종(랜섬웨어 이름, 사용된 언어, 구문, 구조, 문구, 아트워크, 연락처 이메일 주소, 사용자 이름, 랜섬 요구 결제 유형[예: 암호화폐 유형, 기프트 카드], 암호화폐의 경우 결제 주소, 지원 채팅 주소 또는 지원 URL)을 식별하기 위해 랜섬 메시지 분석
  - 암호화된 파일 및 기타 생성된 아티팩트(암호화된 파일 이름 변경 체계 및 확장자, 대상 파일 유형, 대상 파일 위치, 파일 소유권 및 영향을 받는 파일 그룹, 파일 생성/수정 시간에 대한 대량 변경과 같은 파일 메타데이터 변경, 엔트로피 및 바이트 플롯 시각화, 암호화된 파일에 사용되는 아이콘, 파일 플래그, 암호화된 파일 또는 키 자료의 매니페스트가 포함된 파일, 기타 데이터 파일) 분석
  - 필요한 경우 보다 심도 있게 감염 벡터 조사
  - 인스턴스화된 파일 시스템에서 의심스러운 바이너리를 추출하여 알려진 변형이 아닌 경우 리버스 엔지니어링 수행
  - 수집된 아티팩트를 확인하여 다음과 같은 사이트에 대한 랜섬웨어 갱단 및 변종 식별:
    - 랜섬웨어 인구 조사(https://goo.gl/b9R8DE)
    - CryptoSheriff(https://www.nomoreransom.org/crypto-sheriff.php)
    - ID 랜섬웨어( )
- **지속성의 증거를 찾습니다.** Cohesity에서 생성한 과거 스냅샷을 인스턴스화하여 분석가가 파일 시스템을 검사하고 지속성의 증거를 찾을 수 있습니다. 이를테면 다음과 같습니다.
  - 로그 계정을 통한 외부 시스템에 대한 인증된 액세스, 경계 시스템의 백도어, 경계 시스템의 취약점 악용을 포함할 수 있는 "외부에서 내부로 전달되는" 지속성 메커니즘
  - 내부 시스템에 악성 코드를 이식하거나 다양한 Living-off-the-Land(LOTO) 스타일 수정(Cobalt Strike와 같은 상용 침투 테스트 프레임워크 배포, PsTools, 특히 PsExec를 사용하여 악성 코드를 원격으로 설치 및 제어하고 정보 수집, PowerShell 스크립트 사용 등)을 포함할 수 있는 "내부에서 외부로 전달되는" 지속성
- **메모리 내용의 이미지를 캡처하여 의심스러운 프로세스 또는 텍스트 아티팩트를 감지합니다.**
- **변경된 레지스트리 키를 식별합니다.**
- **최근에 생성된 압축 파일을 식별합니다.**
- **예약된 프로세스 및 작업을 검사합니다.**
- **작동해야 하는 네트워크 서비스와 비교하여 활성/실행 중인 네트워크 서비스를 감사합니다.**
- **스테이징 또는 유출의 증거가 있는 경우 데이터 손실 플레이북을 실행합니다.** Cohesity DataHawk는 공격 당시 해당 시스템에 어떤 데이터가 있는지 식별할 수 있으므로 사고 대응자가 규정 준수 의무를 파악하고 데이터 주체 및 규제 기관에 알릴 수 있습니다.
- **공격에서 악용된 시스템의 취약점을 식별합니다.** Cohesity CyberScan을 사용하면 사고 대응자가 공격 지점 근처의 스냅샷에 대해 Tenable Nessus 취약점 스캐너를 실행할 수 있으므로 시스템이 프로덕션으로 복귀하기 전에 적용할 패치의 매니페스트와 마지막으로 예약된 취약점 스캔 이후 공격자가 악용했을 수 있는 취약점을 만들 수 있습니다.
- **승인되지 않은 자산에 대한 지적 재산, 금융 정보 또는 개인 식별 정보를 스캔하여 스테이징에 사용되는 자산을 식별합니다.** Cohesity DataHawk 데이터 분류를 사용하여 스테이징 환경에서 민감한 데이터를 식별할 수 있습니다.
- **과거 인스턴스화된 파일 시스템에서 의심스러운 바이너리를 추출합니다.** 이를 분석, 리버스 엔지니어링 또는 VirusTotal과 같은 서비스에 업로드합니다. ServiceNow Security Incident Response, Splunk Phantom, Palo Alto XSOAR과 같은 보안 오케스트레이션 및 자동화된 대응(Security Orchestration & Automated Response, SOAR) 도구를 사용하면 Cohesity에서 과거 파일 시스템의 인스턴스화를 조율할 수 있습니다.

- **인스턴스화된 파일 시스템에서 의심스러운 바이너리를 추출하고 악성 코드 분석 샌드박스에서 폭발시킵니다.**
- **조직 내 유사한 시스템에 감염이 있는지 확인합니다.** 유사한 사용자 및 그룹으로 호스트를 조사합니다. 시스템이 암호화되지 않은 경우 이러한 호스트의 인스턴스를 감염된 시스템과 비교하여 잠재적 영향을 식별합니다. Cohesity는 조직의 백업 인프라를 신속하게 쿼리할 수 있는 인덱싱 및 검색 기능을 갖추고 있습니다.
- **로컬 계정, ID 및 액세스 관리 도구, 디렉터리 서비스에서 새 계정 또는 권한/액세스 권한 변경을 확인합니다.**
- **랜섬웨어 명령 및 제어에 연결하려는 다른 시스템을 식별합니다.**
- **MITRE ATT&CK를 사용하여 조사 과정을 계속 따라가며 최초 감염자, 초기 감염 벡터 및 감염된 각각의 최종 사용자 장치를 찾습니다.**
- **회피된 예방 또는 탐지 통제 수단과 사용된 메커니즘을 식별합니다.** 이를 완화 계획에 추가하여 프로덕션으로 복귀하기 전에 통제를 강화합니다.

커뮤니케이션

- **언론과 소통합니다.** 해로운 추측을 예방하기 위해 언론에 최신 소식을 지속적으로 알립니다.
- **영향을 받는 데이터 주체와 소통합니다.** 모든 알림이 규제 및 법적 의무를 준수하는지 확인합니다.
- **내부 이해관계자와 소통합니다.** 특히 언론이 LinkedIn과 같은 플랫폼을 사용하여 직원을 식별하고 직접 연락할 수 있으므로 내부 직원에게 상황과 상황에 대한 기대치를 지속적으로 알립니다.
- **보고에 대한 규제 준수 의무를 충족하기 위해 규제 당국에 알립니다.**
- **보험사에 알립니다.**
- **법 집행 기관 및 국가/산업 CERT에 알립니다.**

사고로부터의 복구

최상의 시나리오는 IMR(즉시 대량 복구)과 같은 도구를 사용하여 감염을 찾아 제거하고 시스템을 프로덕션으로 복구하는 것입니다. 실제로, 복구된 시스템과 베어메탈로 재구성된 시스템이 결합될 수 있습니다. 베어메탈 복구를 수행하려면 테스트된 최신 패치로 안전하고 유지 관리되는 중요한 시스템의 '골드 이미지'에 액세스해야 합니다. 이러한 템플릿을 신속하게 배포하여 복구가 불가능한 시스템을 재구축할 수 있습니다. 또한 Cohesity Data Cloud에 있는 도구를 사용하여 보안을 유지할 수 있으므로 사이버 공격 중에 손상되지 않습니다. 그런 다음 기본 운영 체제 및 애플리케이션과 다른 백업의 관련 데이터를 복원할 수 있습니다. 이를 통해 RTO를 최적화하는 동시에 영향을 받은 시스템의 과거 백업을 포렌식용으로 생성합니다.

데이터 및 애플리케이션을 복구하는 동안 사고를 문서화하고 재발을 방지하기 위한 조치를 취해야 합니다.

조직에서는 다음을 수행해야 합니다.

- 초기 감염 벡터, 취약점 악용 및 지속성 메커니즘에 대한 지식을 통해 복구 계획을 업데이트하여 향후 공격으로부터 보호하고 각 구성 요소를 안전하고 안정적인 상태로 되돌릴 수 있도록 합니다.
- 나머지 시스템을 다시 클린 룸으로 복구하고 위의 단계를 반복하여 손상 지표를 격리합니다.
- 발견한 취약점 패치
- 영향을 받는 모든 시스템과 계정에 대해 암호 재설정 실행
- 제거된 이메일 받은 편지함에서 악용 아티팩트가 포함된 이전 이메일 제거
- 이전에 감염된 시스템에 대한 집중 모니터링 증가

핵심 요점 및 후속 조치 수립

랜섬웨어 공격을 경험한 후, 다음 질문을 통해 학습한 교훈을 얻으십시오.

- 어떤 제품과 서비스가 영향을 받았습니까?
- 비즈니스에 어떤 영향을 미쳤습니까?
- 영향을 받은 이해관계자는 누구입니까?
- 이 사고에 관련된 위협 행위자는 누구였습니까?
- 대응 과정에서 무엇이 잘못되었습니까?
- 대응 과정에서 무엇이 제대로 진행되었습니까?
- 언제 공격을 탐지했습니까?
  - 최초 감염과 탐지 사이에 시간이 얼마나 걸렸습니까?
  - 왜 더 빨리 탐지되지 않았습니까?
  - 어떤 통제가 이를 감지/방지하지 못했습니까?
- 어떤 통제가 어떻게 우회되었습니까?
- 향후 사고를 방지하기 위해 기업 운영 내에서 조정해야 할 사항은 무엇입니까?
- 향후 이를 어떻게 피할 수 있습니까?
- 필요한 RTO/RPO 내에 프로덕션으로 복구할 수 있었습니까?

새로 발견된 IOC를 승인된 파트너와 공급업체에 보냅니다.

- 문서 및 플레이북을 업데이트합니다.
- 최종 사고 보고서와 배운 교훈을 이해관계자와 규제 기관에 전달합니다.

Cohesity 소개

Cohesity는 AI 기반 데이터 보안의 리더입니다. Fortune 100대 기업 중 85개 이상과 글로벌 500대 기업 중 약 70%를 포함한 13,600개 이상의 기업 고객사는 Cohesity를 통해 레질리언스를 강화하는 동시에 방대한 양의 데이터에 대한 Gen AI 인사이트를 제공합니다. Cohesity와 Veritas의 엔터프라이즈 데이터 보호 부문의 결합으로 구축된 이 회사의 솔루션은 온프레미스, 클라우드 및 엣지에서 데이터를 안전하게 보호합니다. NVIDIA, IBM, HPE, Cisco, AWS, Google Cloud 등의 지원을 받고 있는 Cohesity는 캘리포니아주 산타클라라에 본사를 두고 있으며 전 세계에 지사를 두고 있습니다. 자세한 내용을 알아보려면 **LinkedIn**, **X**, **Facebook**에서 Cohesity를 팔로우하세요.

https://www.cohesity.com/ko-kr/에서 자세히 알아보기

COHESITY

https://www.cohesity.com/ko-kr/
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000059-002 KO 4-2025