COHESITY

백서

Digital Jump Bag™ 으로 사이버 레질리언스 향상

최소 실행 가능한 대응 역량을 신속하게 복원하고 사고 대응을 강화하는 방법

목차

앞으로

James Blake
사이버 레질리언스
전략 부사장

저는 30년 넘게 파괴적인 사이버 공격과 데이터 도난에 대한 사이버 대응의 최전선에 있었습니다. 제 경험은 국가 차원의 와이퍼 공격에 대한 사고 대응 실행부터 세계 최대 은행의 사이버 위험 관리를 주도하는 것에 이르기까지 다양합니다.

이 기간 동안 저는 "점프 백"의 가치를 배웠습니다. 이 용어는 원래 공격을 당한 물리적 장소로 이동하는 데 필요한 필수 하드웨어 및 소프트웨어를 보유한 물리적 컨테이너를 지칭했습니다. 이 점프 백은 사건을 신속하게 조사하고, 증거를 수집하고, 위협을 완화하는 데 필수적이었습니다.

하드웨어 및 소프트웨어뿐만 아니라 조직 내 주요 이해관계자와 제3자의 연락처 목록 인쇄물, 위기 관리 계획, 내가 대응해야 할 사고 유형에 대한 워크플로우, 휴대폰과 같은 항목이 포함되어 있습니다. 이 아이디어는 즉시 대응할 준비가 되어 있어야 했습니다. 사고의 압박을 받는 상황에서 필요한 모든 것을 찾으려고 너무 서두르게 되면 귀중한 시간을 낭비하고 필수적인 것을 잊어버릴 수 있습니다. 점프 백에는 도구, 공정의 세부 사항 및 통신을 허용하는 방법이 들어 있습니다.

오늘날 우리는 원격 수집, 엔드포인트 및 확장형 탐지 및 대응(EDR/XDR), 가상 머신 및 클라우드 인스턴스의 세계에 살고 있습니다. 점프 백은 여전히 현장에 가져가는 물리적 컨테이너가 될 수 있습니다. 그러나 이제는 Digital Jump Bag™을 준비할 때 가장 큰 유용성을 찾을 수 있습니다. 보호되고 신뢰할 수 있는 이 저장소는 원격 수집 및 분석에 필요한 도구뿐만 아니라 사고 대응 및 복구 중에 긍정적인 결과를 얻는 데 필요한 기타 디지털 자산에 대한 신속한 액세스를 제공합니다.

요약

Digital Jump Bag™은 클린룸의 기반입니다. 클린룸은 보안 운영팀이 공격이 어떻게 발생했는지 이해하기 위해 필요한 조사 단계를 수행할 수 있는 안전하고 격리된 환경입니다. 또한, 클린룸을 사용하여 복구 전에 시정 조치를 취하여 위협을 근절하고 재발을 방지합니다. 디지털 점프 백에 들어가는 것은 조직의 성숙도, 구조, 프로세스 및 도구에 따라 달라집니다.

본질적으로 디지털 점프 백은 최소 실행 가능한 대응 역량(MVRC)을 신속하게 복구하도록 합니다. 이 역량은 조직이 사이버 공격에 효과적으로 대응하는 데 필요한 필수 도구, 문서 및 프로세스의 간소화된 집합입니다. MVRC는 조직이 사이버 사고 발생 시 신속하게 침해를 억제하고, 중요한 비즈니스 운영을 복원하며, 가동 중단 시간을 최소화할 수 있도록 보장합니다.

Cohesity 클린룸 솔루션은 조직이 파괴적인 사이버 공격에 맞서 싸울 수 있도록 지원하는 현대적인 접근 방식을 지원합니다. 다양한 요구 사항에 적응할 수 있는 유연성을 제공하고 시간이 지남에 따라 운영상의 사이버 레질리언스 기능의 지속적인 개선을 지원합니다.

이 백서에서는 조직이 보다 강력하고 민첩한 사고 대응 전략을 구축할 때 디지털 점프 백에 포함시킬 항목으로 고려해 보아야 할 것을 추천해 드립니다.

사이버 레질리언스에서 일반적으로 해결되지 않은 문제

파괴적인 사이버 공격은 종종 피해자 조직 내에서 사용되는 보안 도구의 회피와 관련이 있으며, EDR/XDR 회피 기능은 오늘날 우리가 본 랜섬웨어 공격의 대부분을 담당하는 일반적인 서비스형 랜섬웨어(RaaS) 플랫폼에 내장되어 있습니다. 본질적으로 EDR/XDR 솔루션은 엔드포인트에 위치하며, 이를 회피하지 않으면 프로세스, 네트워크 연결 및 파일 시스템에 대한 탁월한 가시성을 제공합니다.

SANS Institute의 6단계 사고 대응 수명 주기, NIST SP800-61 컴퓨터 보안 사고 처리 가이드, RE&CT 프레임워크 및 MITRE D3FEND와 같은 사고 대응 모범 사례는 감염된 네트워크 및 호스트의 격리를 통해 사고의 확산 억제를 옹호합니다. 엔드포인트 제어의 세계에서는 기껏해야 조직이 사고를 조사하기 위해 이미 수집한 정보만 남게 됩니다.

하지만 끊임없이 변화하는 공격자와 마주할 때, 공격을 미리 이해하기 위해 어떤 정보를 수집해야 할지 항상 알 수는 없습니다. 조사 및 대응 역량이 이제 접근할 수 없는 상황이 되었다는 사실에 너무 집중한 나머지 다른 중요한 진실을 보지 못하게 될 수 있습니다. 마찬가지로, 연결을 차단하면 영향을 받는 호스트의 볼륨에 대한 원격 포렌식 이미징이 불가능합니다.

보안 도구 외에도 다른 많은 시스템이 사고 대응의 조사, 완화 및 복구 단계에 관여합니다. 이는 랜섬웨어 및 와이퍼와 같은 파괴적인 사이버 공격의 영향을 받을 수 있지만, 많은 비즈니스 영향 분석에서 중요한 요소로 간과되는 경우가 많습니다. 저는 물리적 액세스 통제가 영향을 받아 사고 대응자가 건물 안에 들어갈 수 없었던 사고에 연루된 적이 있습니다. 많은 조직에서는 음성 인터넷 프로토콜(voice-over-IP, VoIP) 및 이메일 서버가 공격당하여 언론, 규제 기관, 법 집행 기관, 사이버 보험사 또는 영향을 받는 데이터 주체와 소통할 수 없었습니다. 조직에서 수행하는 많은 탁상 랜섬웨어 연습은 공격자의 표적 기술에 의해 발생하는 이러한 영향을 충분히 포착하지 못합니다. 결국, 공격자들은 조직이 침해 사고에 대응하고 복구하는 데 어려움을 겪게 만들고 싶어합니다.

RaaS 플랫폼은 최근 패치된 취약점을 단 5일 만에 악용할 수 있으므로, 시스템에서 이를 식별하고 패치한 후 시스템을 프로덕션으로 복귀해야 합니다. 그렇지 않으면 동일한 공격자 또는 동일한 RaaS 플랫폼을 사용하는 다른 계열사가 롤백됩니다.

또한 영향을 받은 첫 번째 시스템인 소위 "최초 감염자"를 제공하는 초기 액세스 벡터를 식별한 다음 사고를 처리해야 합니다. 공격자가 지속성을 유지하는 방법을 이해하고, 권한을 확대하고, 공격의 다른 아티팩트를 찾아 복구가 안전한 상태로 유지되도록 해야 합니다. 또한, 대응팀은 통지에 대한 규제 의무를 준수하기 위해 손상되었을 수 있는 데이터의 성격을 이해해야 합니다.

암호화된 시스템의 분석만으로는 충분하지 않습니다. 일반적으로 랜섬웨어 갱단은 공격 주기가 끝날 무렵 암호화 도구를 배포합니다. 인프라 내부에 며칠에서 수백 일까지 잠복할 수 있는 공격의 마지막 몇 분 또는 몇 시간 동안 말입니다. 암호화에는 노이즈가 매우 많으며 보안 제어 및 사용자 감지를 트리거할 가능성이 높습니다. 이때가 되면

너무 늦은 것입니다. 속도를 염두에 두고 구축해야 한다는 필요성으로 인해 암호화 도구가 무결성을 염두에 두고 구축되지 않는 경우가 많아 암호 해독 키에 대한 몸값을 지불하는 사람은 많은 양의 데이터를 잃게 됩니다. 공격자가 네트워크 내부에 어떻게 들어왔고 계속 머무르는지 파악하지 않고 암호화된 시스템에만 범위를 제한하는 것은 재해의 원인이 됩니다.

이러한 접근 방식을 취하는 조직은 수십 번이나 회복한 후에도 반복해서 재감염되는 경우가 많습니다. 이러한 " 악순환" 주기는 사고를 적절히 조사하고 얻은 통찰력을 활용하여 위협으로부터 수습함으로써 해결됩니다.

스스로에게 한번 물어보십시오. 만약 전화나 이메일이 없고, 열쇠가 없어 건물에 들어갈 수 없고, 이벤트가 시작될 때 ID 및 액세스 관리 시스템에 액세스할 수 없었다면 마지막 비상 대응 훈련 결과가 어떻게 달랐을까요?

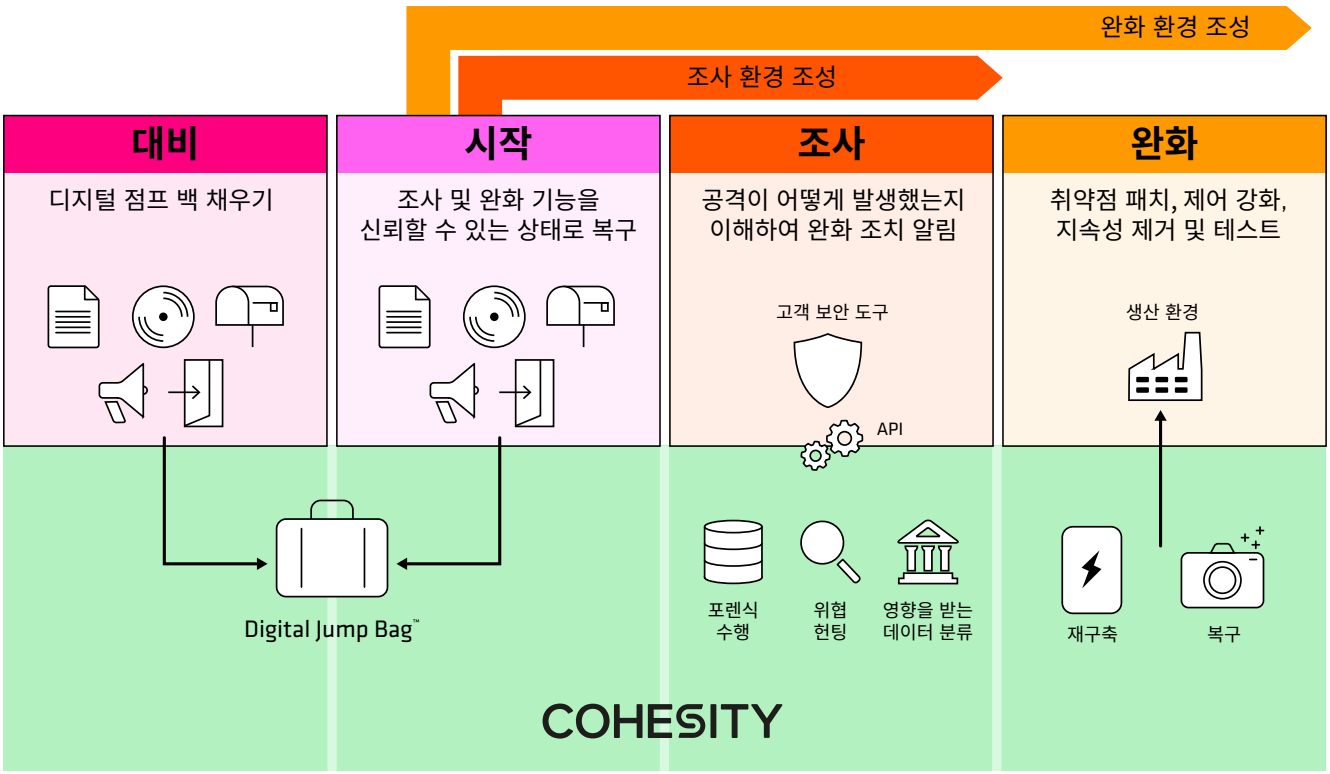
디지털 점프 백이 Cohesity 클린룸 솔루션에 적합한 이유

디지털 점프 백은 Cohesity 클린룸 솔루션 전체의 기반이며, 조직이 깨끗한 데이터를 다시 프로덕션으로 복원할 수 있도록 사고 대응 및 복구의 중요한 단계를 지원합니다(아래 참조).

각 단계에서 무슨 일이 일어나고 있는지 살펴보겠습니다.

대비

이 단계에서는 완화 환경에서 복원될 상호 의존적 시스템 계층을 지원하는 네트워크 또는 하이퍼바이저 구성과 같이 디지털 점프 백에 들어갈 항목을 선택합니다. 후속 단계를 활성화하기 위한 제안 사항은 "디지털 점프 백의 잠재적 구성 요소는 무엇입니까?" 섹션을 참조하십시오.



시작

이 단계에서는 커뮤니케이션, 협업 및 사고 조사에 필요한 도구가 포함된 MVRC를 디지털 점프 백에서 복구하여 격리된 클린룸 환경 내부의 신뢰할 수 있는 상태로 복구합니다. 또한 디지털 점프 백은 조사 및 완화 환경을 구축합니다.

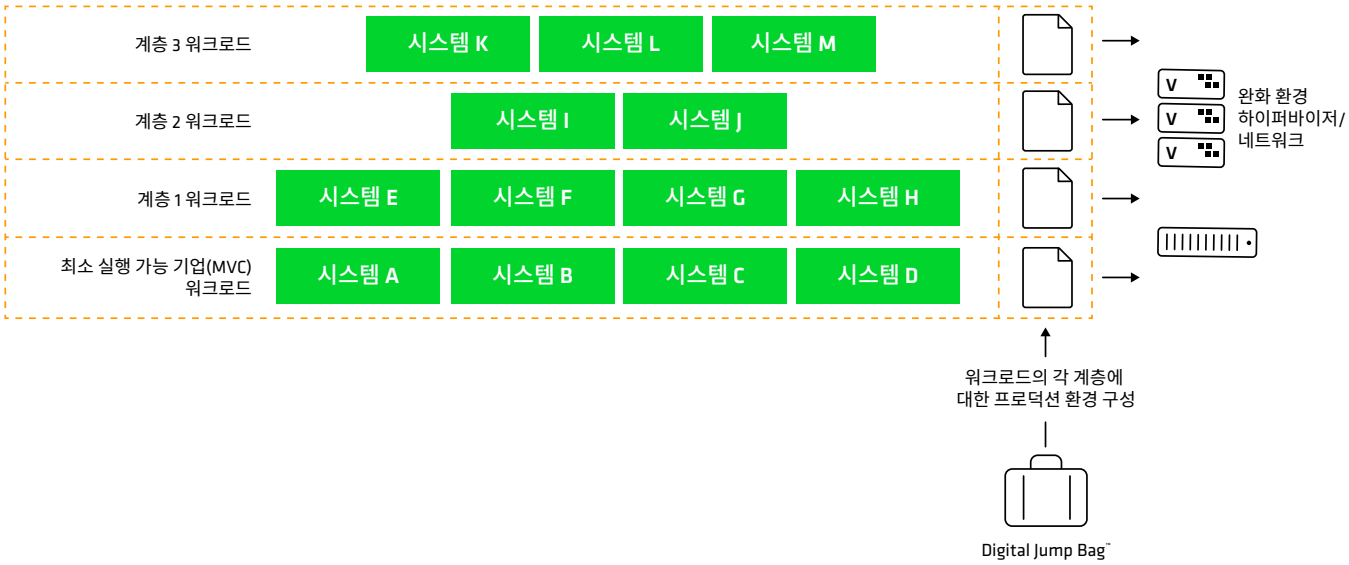
조사

보안 운영에서는 데이터 분류, 위협 헌팅 및 파일 시스템 포렌식에 대한 기본 Cohesity 기능과 함께 격리된 클린룸 내에서 신뢰할 수 있는 상태로 복구된 보안 도구를 사용하여 전체 엔드투엔드 사고 타임라인을 이해합니다. 보안 도구가 클린룸 내부의 신뢰할 수 있는 상태로 복구되고 Cohesity 의 보안 기능이 엔드포인트 제어에 사용되는 방어 회피 기술의 대상이 되지 않기 때문에 격리로 인한 회피 및 격리의 문제가 극복됩니다. Cohesity의 데이터 보안 연합은 Cohesity 솔루션과 함께 작동하도록 사전 구성된 보안 운영 센터에 존재하는 다양한 보안 공급업체 도구를 제공합니다.

완화

IT 운영팀은 보안 운영팀이 사고에 대해 발견한 내용을 사용하여 복구한 다음 정리하거나 시스템을 신뢰할 수 있는 상태로 다시 구축합니다. 조사 단계에는 상호 종속성이 있는 시스템이 완전히 복구되지 않지만, 완화 단계에서는 복구됩니다.

고객은 종종 사고 복구 기간 동안 개발 환경을 완화 환경으로 재사용합니다. 상호 의존적인 시스템은 프로덕션 환경에 맞는 네트워크 구성을 통해 완화 환경에서 도입됩니다. 이러한 네트워크 또는 하이퍼바이저 구성은 디지털 점프 백에 있는 상호 의존적 시스템의 각 계층에 대해 저장됩니다. 이는 아래에 나와 있습니다.



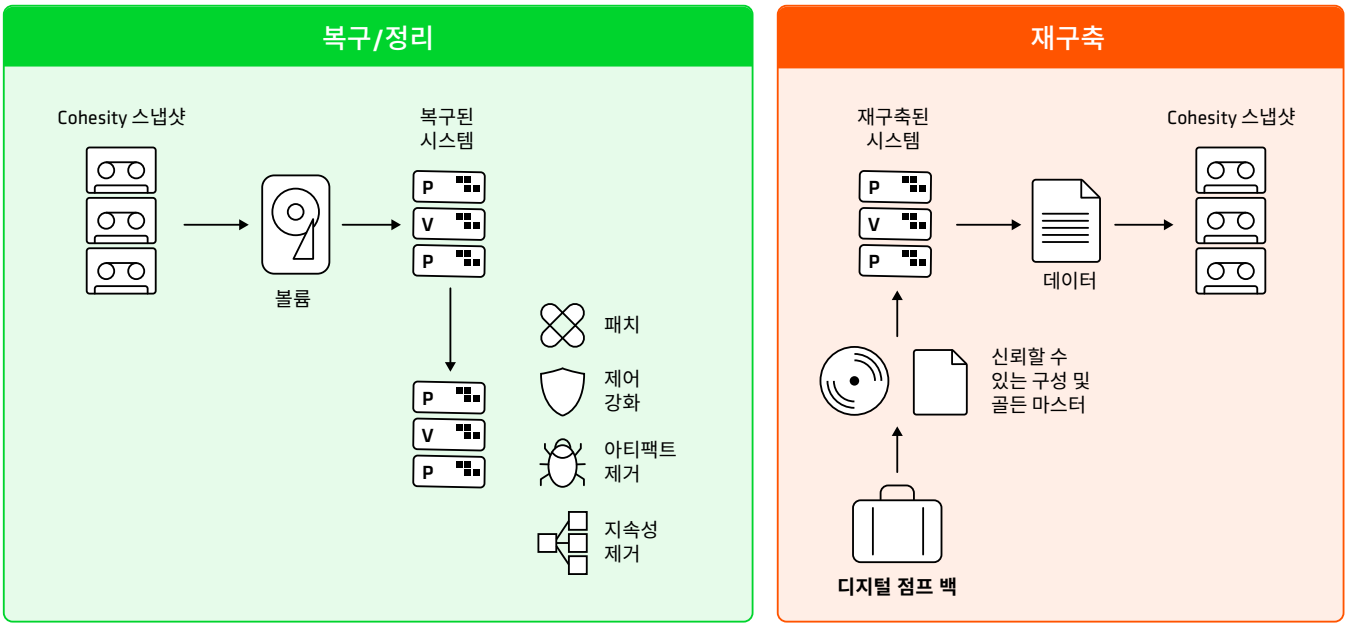
사고 대응 모범사례에 대한 Cohesity 클린룸 조정.

Cohesity 클린룸 솔루션을 사용하면 "복구 및 정리" 또는 " 신뢰할 수 있는 상태로 재구축"할지의 전략을 보편적으로 적용하거나, 사고 발생 시 복구 노력 수준과 위협의 잔여 위험에 따라 시스템별로 선택할 수 있습니다. 각 옵션에 대한 간략한 설명을 살펴보겠습니다.

- **복구 및 정리**: 시스템은 스냅샷에서 복구되며, 조사 단계에서 보안 운영팀이 설명한 완화 단계가 수행됩니다. 데이터는 일반적으로 악의적인 페이로드를 전송하는 데 사용되지 않기 때문에 데이터 복구는 시스템 재구축과 동시에 발생하는 경우가 많아 궁극적인 복구 시간을 단축할 수 있습니다.
- **시스템을 신뢰할 수 있는 상태로 재구축**: 디지털 점프 백에는 잘 알려진 양호한 구성, 설치 스크립트 및 골든 마스터 설치 이미지가 포함됩니다. 시스템이 재구축되면 재구축된 시스템의 스냅샷에서 데이터가 복구됩니다.

"점프 백을 사용하여 최소 실행 가능한 대응 역량 확립" 섹션에서는 각 접근 방식의 비교 내용을 자세히 설명합니다.

보안 운영팀의 조사 요구 사항을 충족하는 환경과 IT 운영팀이 완화 조치를 적용하여 복구가 안전한 상태로 이루어지도록 하는 환경을 갖추면 조직이 사이버 레질리언스에 대한 효과적이고 적절한 공동 책임 모델을 달성하는 데 도움이 됩니다. 이 접근 방식은 IT 및 보안 운영 자산을 최대한 활용할 수 있도록 보장하여 보안 복구 속도를 최적화합니다.



Cohesity 클린룸은 고객에게 워크로드를 복구 및 정리하거나 신뢰할 수 있는 상태로 신속하게 재구축할 수 있는 옵션을 제공합니다.

시스템이 다시 구축되거나 복구되면 해당 워크로드 계층에서 기능 및 성능 테스트를 수행할 수 있습니다. 스냅샷을 만든 다음, 전체 상호 의존적 워크로드가 프로덕션 환경으로 복원됩니다. 즉, 사고의 전체 범위를 조사하고, 위협을 완화하고, 성능 및 기능을 복원한다는 것을 알 수 있습니다.

이러한 테스트 사례는 상호 의존적 워크로드의 각 복구 계층에 대해 디지털 점프 백에 저장할 수 있습니다. 조사 및 완화 조치가 누락된 경우 완화 단계 종료 시 촬영한 스냅샷을 추가 조사 및 완화의 기반으로 사용할 수 있으므로 출발점으로 돌아갈 필요가 없습니다.

Cohesity 클린룸이 사고 대응 모범사례에 맞추어 조정하는 과정

Cohesity 디지털 점프 백과 최소 실행 가능한 대응 역량은 SANS Institute의 6단계 사고 대응 수명 주기, NIST SP800-61 컴퓨터 보안 사고 처리 가이드, RE&CT 프레임워크 및 MITRE D3FEND에 설명된 사이버 사고 대응 모범 사례에 부합합니다. 이러한 접근 방식을 통해 이미 이러한 방법론을 따르고 있는 조직은 Cohesity 클린룸 솔루션을 기존 워크플로우에 쉽게 통합할 수 있습니다. 사고 대응 및 복구 성숙도를 개선하고자 하는 고객은 Cohesity 클린룸 솔루션을 도입하여 이러한 모범 사례를 구현할 수 있습니다.

사고 대응 모범사례에 대한 Cohesity 클린룸 조정

보안 및 IT 운영을 통합하여 레질리언스 제공

사이버 레질리언스는 팀 스포츠입니다. IT 운영이나 보안 운영만으로는 달성할 수 없습니다. 두 팀 모두 통합 프로세스와 보완적인 도구가 필요합니다. 마찬가지로, 누구도 사이버 레질리언스를 제공할 수 없습니다. Cohesity 클린룸 솔루션은 보안 운영팀이 조사 환경을 활용하고 소유할 수 있도록 설계되었으며, IT 운영은 완화 환경을 소유하고 활용할 수 있도록 설계되었습니다. 팀 간의 이러한 주인의식과 이관은 명확한 공동 책임 모델을 보장하여, 활동이 누락될 가능성을 최소화하는 데 도움이 됩니다.

공격의 일부 측면이 초기 조사 및 완화에서 누락된 경우, 처음부터 다시 시작할 필요 없이 이전에 완화된 스냅샷을 조사 단계로 반복적으로 되돌릴 수 있는 기능을 통해 조사 시간과 최종 복구 시간을 단축할 수 있습니다.

보안 운영팀이 조사 환경에서 워크로드 조사를 마치면 즉시 IT 운영팀과 완화 환경으로 이관하여 재구축, 복구 및 정리할 수 있습니다. 이를 통해 IT 및 보안 운영 리소스를 가장 효율적으로 사용할 수 있습니다.

더 빠르게 대응하고 더 스마트하게 복구: Cohesity CERT(사이버사고대응팀)

많은 조직은 효과적인 사이버 사고 대응을 위한 전문 지식이나 리소스가 부족합니다. 영향을 최소화하기 위해 전용 CERT(사이버사고대응팀) 서비스로 세계적 수준의 데이터 보안 솔루션을 개선했습니다.

Cohesity CERT는 사이버 공격으로부터 전문가 주도의 빠른 복구를 제공하며, 가동 중단 시간을 최소화하여 데이터를 복원하여 운영을 재개할 수 있도록 보장합니다.

Cohesity CERT는 Cohesity 구독의 일부로 모든 고객이 사용할 수 있습니다.

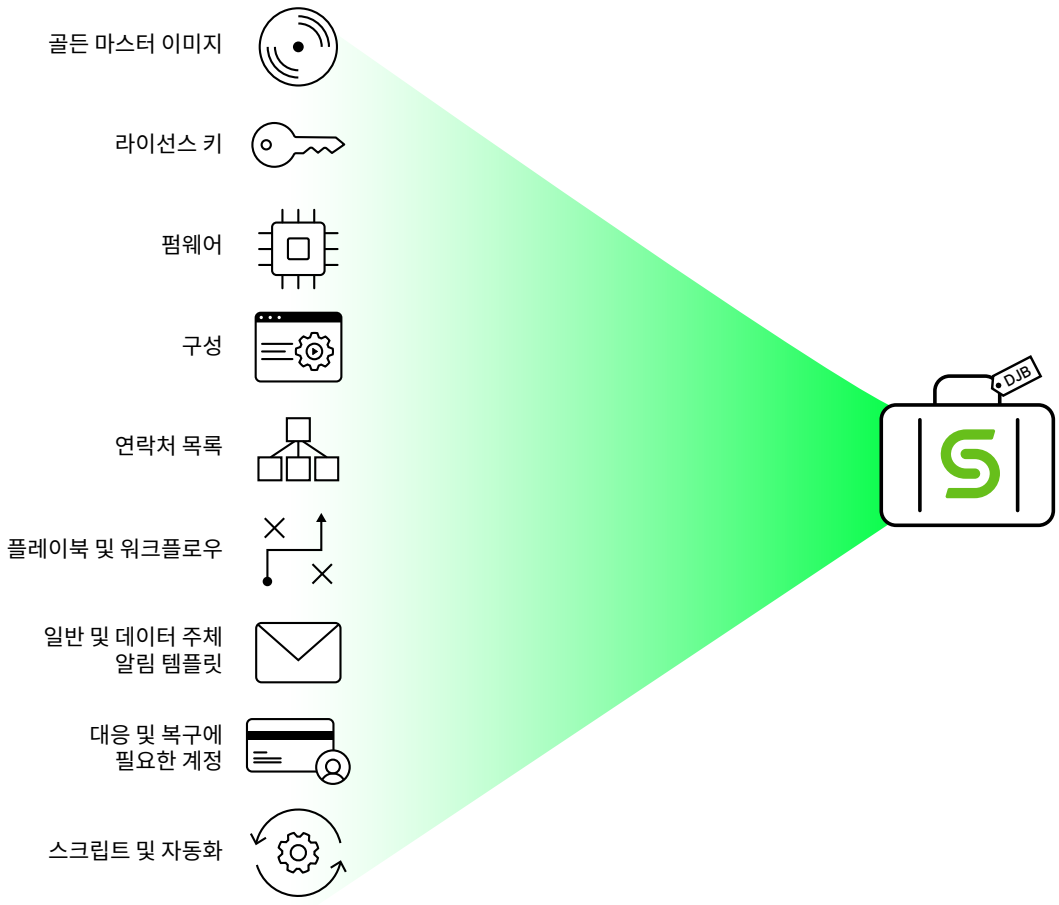
디지털 점프 백의 잠재적 구성 요소는 무엇입니까?

디지털 점프 백의 내용은 개별 분류, 조사 및 완화 프로세스와 이를 달성하는 데 사용하는 도구에 따라 다릅니다.

보통 고객의 디지털 점프 백에 일반적으로 포함되는 항목은 다음과 같습니다.

문서

- 내부 이해관계자 및 법 집행 기관, 정보 공유 및 분석 센터, 보험 회사, 고용된 사고 대응자 및 규제 기관과 같은 외부 기관을 포함한 연락처 목록.
- 네트워크 다이어그램.
- 조직의 구성 관리 데이터베이스의 백업 또는 덤프 가능성.
- 사고 대응 런북/워크플로우 사본.
- 유지된 사고 대응 서비스 및 사이버 보험사 관련 계약 및 정책 문서.
- 애플리케이션 및 도구에 대한 사용자 매뉴얼.



시작 단계를 위한 리소스: 협업 및 커뮤니케이션

- 내부 이해관계자 및 법 집행 기관, 정보 공유 및 분석 센터, 보험 회사, 고용된 사고 대응자, 규제 기관, 언론 및 영향을 받는 데이터 주체와 같은 외부 제3자와의 커뮤니케이션이 필요할 가능성이 높습니다. 이 기능을 구축하려면 디지털 점프 백에 다음이 포함될 수 있습니다.
  - 안전한 연결을 위해 잘 알려진 양호한 라우터와 스위치 펌웨어 및 구성. 또는 신뢰할 수 있는 대기 장비를 유지할 수도 있습니다.
  - 대응 및 복구에 필요한 리소스로만(Cohesity Helios에 대한 액세스 포함) 유입 및 유출을 제한하는 방화벽 소프트웨어 및 구성.
  - 조사 및 완화 환경의 시스템을 포함하여 다른 시스템을 재구축하기 위한 기반으로 사용되는 기본 운영 체제 설치 미디어 및 라이선스 키.
  - 자동화 및 오케스트레이션 스크립트는 무인 설치를 위한 Windows Answerfiles부터 Ansible 플레이북, 코드 기반의 인프라 Terraform에 이르기까지 다양.
  - 음성 인터넷 프로토콜 관리(VoIP) 서버 소프트웨어 및 구성. 이것이 전체 프로덕션 VoIP 환경이 아니라는 것을 깨닫는 것이 중요합니다. 대응 및 복구 활동과 관련된 내용만 있습니다. 프로덕션 VoIP 구성은 조사 후 온라인으로 반환되며 발견된 모든 위협이 완화되었습니다.
  - 이메일 서버 소프트웨어 및 구성. VoIP 서버와 마찬가지로 이것은 프로덕션 기능이 아닙니다. 이는 대응 및 복구 활동에 관련된 리소스 간의 커뮤니케이션만 허용합니다.
  - 티켓팅, 컨퍼런스 등 조직에서 사용하는 기타 협업 도구는 점프 백에 포함될 수 있습니다.
  - 규제 기관 및 영향을 받는 데이터 주체 통지용 템플릿

조사 단계 환경을 위한 리소스

보안 운영팀은 일반적으로 조사 단계에서 사용되는 환경을 소유합니다. 엔드투엔드 공격 타임라인을 이해하여 조직이 재감염 및 재공격으로부터 보호하면서 생산 능력 복구에 대한 정보에 입각한 결정을 내릴 수 있도록 하는 데 중점을 두고 있습니다. Cohesity의 기본 보안 운영 기능을 사용하여 데이터 분류, 위협 헌팅, 파일 시스템 포렌식과 같은 작업을 수행하고 Cohesity가 다른 보안 운영 도구를 지원하는 방식을 혼합하여 조직 내부의 시스템을 조사합니다. Cohesity를 사용한 위협 헌팅은 사고 억제의 영향을 받지 않습니다. 수동적이므로 공격자에게 보이지 않으며 엔드포인트 보안 솔루션에 흔한 회피 기법의 대상이 아닙니다. 조사 단계 환경에서 시스템은 일반적으로 격리된 상태로 조사됩니다.

- 보안 소프트웨어용 설치 미디어 및 구성. 이렇게 하면 격리된 클린룸 환경 내에서 신뢰할 수 있는 상태로 도구를 재설치할 수 있으므로 도구 및 대응 활동이 회피되거나 중단되지 않는다는 확신을 가질 수 있습니다.
- 보안 도구는 클린룸 내부의 신뢰할 수 있는 상태로 다시 설치할 수 있습니다. 이 도구는 보안 사고 대응 팀의 선호도에 따라 크게 달라지지만 일반적으로 다음 중 적어도 일부를 포함합니다.
  - 엔드포인트 탐지 및 대응(EDR) 및 확장된 탐지 및 대응(XDR) 도구(Palo Alto Networks, Cisco XDR 및 CrowdStrike 포함)
  - 포렌식 캡처 및 분석 도구(예: Dissect, Flare, Redline, Sleuth Kit, Autopsy, CyLR 및 UAC(Unix-like Artifacts Collector))
  - 침해 지표 및 증거 공유 도구(예: Cortex, Kuiper 및 MISP)
  - 이벤트 로그 분석기(예: 이벤트 로그 탐색기, 이벤트 로그 관찰자, Hayabusa, LogonTracer 또는 WELA(Windows 이벤트 로그 분석기))
  - 취약성 스캐너(예: Qualys, Rapid7 neXpose, Tenable Nessus 또는 OpenVAS)

- 패킷 캡처 및 분석 소프트웨어(예: Wireshark)
- Netflow/SFlow 분석기
- 메모리 캡처 및 분석기(예: Volatility, Memoryze, Orochi, Rekall 및 WindowsSCOPE).
- 샌드박스, 악성코드 리버스 엔지니어링 및 분석 도구(예: Cuckoo, CAPA, CAPE, Ghidra, Joe Sandbox, Mastiff, Radare 2 및 Valkyrie Comodo).
- 웹 브라우저 기록 포렌식 도구(예: 인터넷 기록 포렌식)
- 위의 도구 중 상당수는 Kali Linux 및 SANS Institute SIFT Workstation과 같은 보안 소프트웨어 배포판 내에서 사용할 수 있습니다. 각 도구를 설치하지 않고 디지털 점프 백 안에 보관할 수 있습니다.

완화 단계 환경을 위한 리소스

IT 운영팀은 일반적으로 완화 환경을 소유합니다. 완화 환경에서 시스템 운영 체제 및 애플리케이션은 디지털 점프 백에 포함된 신뢰할 수 있는 설치 미디어 및 구성을 통해 재구축되거나 백업 스냅샷에서 복구되고 조사 단계 동안 보안 작업에서 얻은 정보를 사용하여 정리됩니다. 취약점 패치, 향후 동시 공격을 방지하거나 탐지하기 위한 누락된 제어 또는 규칙 적용, 지속성 메커니즘, 악성 계정 또는 기타 공격 아티팩트 제거와 같은 위협을 완화하기 위한 시정 조치를 취합니다. 완화 환경에서는 제품 또는 서비스를 제공하기 위한 상호 의존적 시스템을 통합하고 재구축하거나 완화합니다. 마지막으로 백업 스냅샷에서 데이터를 복원하여 성능과 기능을 테스트할 수 있습니다. 이 시점에서 스냅샷이 생성되고 시스템이 프로덕션 환경으로 복구됩니다.

- 조직이 "복구 및 정리" 접근 방식이 아닌 "재구축" 방식을 취하는 경우, 디지털 점프 백에는 애플리케이션 스택에 필요한 설치 미디어 및 구성이 포함됩니다.
- 현재 상호 의존적 워크로드에 필요한 네트워크 또는 하이퍼바이저 구성. 이를 통해 완화 환경은 궁극적으로 워크로드를 복구할 수 있는 프로덕션 환경을 복제할 수 있습니다.
- 워크로드에 대한 테스트 사례.

점프 백을 사용하여 최소 실행 가능한 대응 역량 확립

MVRC 내에서 디지털 점프 백을 사용하여 시스템을 구축할 때 고객은 두 가지 선택권을 갖습니다. 사전 구축된 시스템을 복구하거나 신뢰할 수 있는 소스에서 다시 구축합니다.

- **최소 실행 가능한 대응 역량 유지:** MVRC에 필요한 시스템을 구축하고 디지털 점프 백에 저장되는 볼륨 수준의 백업을 수행합니다. 대응 및 복구 또는 보안 도구 회피에 필요한 시스템에 영향을 미치는 사이버 보안 사고가 의심되는 경우, 스냅샷을 복구하여 최소 실행 가능한 대응 역량을 확립합니다.
- **디지털 점프 백의 리소스에서 재구축**: 여기에서 MVRC에 필요한 시스템에 대한 신뢰할 수 있는 구성과 골든 마스터 이미지를 디지털 점프 백에 보관합니다. 대응 및 복구에 필요한 시스템에 영향을 미치는 사이버 보안 사고가 발생하거나 보안 도구 회피가 의심되는 경우, 디지털 점프 백을 장착합니다. 이러한 시스템은 스크립트 또는 오케스트레이션 도구를 사용하여 다시 구축됩니다.

각 전략에는 아래 표에 요약된 장단점이 있습니다.

최소 실행 가능한 대응 역량을 유지하고 백업한 후 사고 후 스냅샷을 복원합니다.	
장점:	**단점:**
대응 중 기능 시스템에 빠르게 접근	패치 및 업데이트에는 추가 단계(재구축, 업데이트/패치, 백업)가 필요하며, 이에 따라 지속적인 리소스가 필요합니다. 이러한 단계에서는 대응 및 복구에 영향을 미치는 오류가 발생할 수 있습니다. 조직이 IT 시스템을 안전하게 유지하지 못하고 사고로 인한 영향을 받았다고 가정합니다. 구축 및 백업된 최소 실행 가능한 대응 역량 시스템에 동일한 문제가 발생하지 않는다는 보장은 무엇입니까?
필요한 구성 요소만 복원할 수 있는 기능	디지털 점프 백에서 기하급수적으로 더 많은 공간을 차지하여 라이선스 비용 발생
	대응 중 업데이트 및 패치가 필요할 수 있어 지연 발생
	인프라 종속성 도입 가능
요구 사항:	
디지털 점프 백에서 성공적인 MVRC 구축 테스트 수행	
MVRC 백업 수행, 증거 보전 조치를 활성화하여 법적 목적을 위해 보존, 복제 및 오프사이트 보관	

사고 후 신뢰할 수 있는 소스에서 최소 실행 가능한 대응 역량 재구축	
장점:	**단점:**
운영 체제, 애플리케이션 또는 구성의 새 버전이 있을 때 점프 백으로 내보내기만 하면 되어 소스를 비교적 쉽게 유지 관리할 수 있습니다.	인프라를 재구축하는 데 시간 필요
복제 및 아카이브를 통한 휴대성	
하드웨어 및 플랫폼 변경에 대한 적응성 향상	
디지털 점프 백의 백업 설치 공간이 상당히 작습니다(즉, 하나의 Windows Server 2025 이미지는 약 3.6GB이며 여러 시스템 간에 공유될 수 있는 반면, 해당 이미지를 사용하는 최소 실행 가능한 응답 역량의 각 서버에는 약 35GB가 필요합니다).	
요구 사항:	
디지털 점프 백 채우기 및 업데이트 프로세스 확립	
콘텐츠 사용에 대한 다양한 시나리오 연습	
필요한 하드웨어를 준비해 두거나 기존 하드웨어를 안전하게 지우는 프로세스 정의	

결론

점점 더 정교해지고 파괴적인 사이버 공격에 직면하여 조직은 사후 대응적 복구에서 전략적 레질리언스로 전환해야 합니다. 여기에는 사이버 공격에 신속하게 대응할 수 있는 더 나은 입지를 확보하기 위해 포괄적인 디지털 점프 백을 사고 대응 전략에 통합하는 것이 포함됩니다. 잘 준비된 디지털 점프 백은 MVRC를 가능하게 하고 클린룸의 기반 역할을 합니다. 보안팀은 사고를 조사하고, 위협을 억제하고, 중단을 최소화하면서 운영을 복원하는 데 필요한 필수 도구, 프로세스 및 문서를 갖추게 됩니다.

Cohesity 클린룸 솔루션은 2차 공격의 위험을 최소화하면서 사고 대응 속도를 높이고 조사를 지원하는 신뢰할 수 있는 환경을 제공합니다.

모듈식 설계 덕분에 Cohesity는 격리된 환경을 신속하게 구축하여 대응 및 복구 프로세스를 지원하고 팀이 협업하여 위협을 더 빠르게 완화할 수 있습니다.

Cohesity 소개

Cohesity는 AI 기반 데이터 보안의 리더입니다. Fortune 100대 기업 중 85개가 넘는 기업과 글로벌 500대 기업 중 약 70%를 포함한 12,000개 이상의 기업 고객은 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 새너제이에 본사를 두고 있으며 전 세계에 지사를 두고 있습니다. 자세한 내용을 알아보려면 LinkedIn, X, Facebook에서 Cohesity를 팔로우하세요.

www.cohesity.com에서 Cohesity가 최신 데이터 보안으로의 여정을 가속화하는 방법을 알아보십시오.

추천 자료

다음의 백서, 가이드 및 블로그에서 자세한 정보를 확인할 수 있습니다.

- 사이버 공격이 벌어지는 환경에서 사이버 레질리언스 구축
- 최신 데이터 보안 및 관리 토폴로지: IT 리더를 위한 가이드
- Cohesity 클린룸 설계 소개
- AI 기반 데이터 보안을 위한 현장 가이드: 혁신적인 비즈니스 성과를 제공하는 방법
- 최신 데이터 보안 및 관리에 대한 경영진 가이드

Cohesity에서 자세히 알아보기

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000056-002-KO 4-2025