COHESITY

백서

파괴적인 사이버 공격에 대한 “전시” 대응 전략을 수립하는 방법

Cohesity를 통해 랜섬웨어 및 기타 사이버 위협으로부터 안전하고 신속하게 복구

목차

요약

랜섬웨어 및 와이퍼 공격과 같은 파괴적인 사이버 공격은 기존의 비즈니스 연속성 및 재해 복구 시나리오와 비교하여 IT 운영과는 다른 접근 방식이 필요합니다. 사이버 보안 운영팀은 적절한 조사 및 위협 시정 조치를 수행하는 데 여러 가지 어려움에 직면해 있습니다. 제품 및 서비스의 배송을 가능한 한 빨리 복원하는 것만으로는 충분하지 않습니다. 또한 조직은 재감염 또는 재공격으로 인한 추가 가동 중단 시간을 방지하기 위해 복구가 안전하게 수행되도록 해야 합니다.

이 백서에서는 파괴적인 사이버 공격에 대응하기 위해 모범사례를 문서화하고, Cohesity가 이러한 운영 결과를 달성하는 데 어떻게 도움이 될 수 있는지 강조합니다.

상황 분석: 소속 조직이 "평시"와 "전시"에 다르게 운영되는 이유

"평시"는 소속 조직의 정상적인 일상 운영을 의미합니다. 보안 툴링의 경고는 일반적으로 보안 운영 센터(SOC) 또는 관리형 보안 서비스 제공업체(MSSP)의 콘솔로 전달됩니다. 이러한 경고는 우선순위 지정 및 거짓 양성의 조정을 위해 분류되며, 소속 조직의 인프라 내부 침입의 징후를 식별하기 위해 추가 증거가 수집됩니다. SOC 분석가가 적대세력이 조직을 공격하고 있다고 확신하는 경우, 사고를 선언하고 조사를 진행합니다. 이 단계에서 조직은 "전시" 모드에 있게 됩니다.

조사 중에 분석가가 조직의 시스템 및 데이터의 기밀성, 무결성 또는 가용성이 침해되었음을 발견하면 침해를 선언하고 자체 사고 대응 프로세스를 진행합니다.

적대세력이 발견되기 전에 조직 내에서 보낸 시간은 잠복 시간(dwell time)으로 정의됩니다. 적대세력은 보안 툴링 경고를 통해 발견될 수 있습니다. 하지만 아주 흔한 경우, 시스템을 사용할 수 없게 될 때만 조직은 공격을 알아차리게 됩니다. 잠복 시간은 매우 다양할 수 있습니다. 서비스형 랜섬웨어(RaaS)를 사용한 공격의 경우 4일에서 5일, 인간 중심의 랜섬웨어 공격의 경우 수백일, 또는 국가 차원의 행위자의 경우 수년이 걸릴 수 있습니다.

기밀성, 무결성 또는 가용성이 침해되는 방식의 예는 다음과 같습니다.

- **기밀유지**: 조직의 데이터가 승인되지 않은 당사자에게 공개되었습니다. 여기에는 랜섬웨어 조직에 의한 범죄 목적을 위한, 또는 와이퍼 공격을 시작하기 전 국가 행위자에 의한 스파이 활동을 위한 데이터 유출이 포함됩니다.
- **무결성**: 파괴적인 사이버 공격의 여러 단계에서 적대세력은 구성 파일, 레지스트리, ID 관리 시스템 및 잠재적으로 펌웨어를 변경하여 피해 조직 내에서 지속성을 유지합니다. 이러한 모든 변경 사항은 시스템의 무결성에 영향을 미칩니다.
- **가용성**: 파괴적인 사이버 공격은 고객에게 제품과 서비스를 제공하는 데 필요한 조직의 IT 인프라를 사용할 수 없게 만드는 것을 목표로 합니다. 랜섬웨어 공격에서 볼 수 있듯이 데이터 및/또는 시스템을 암호화하거나 와이퍼 공격에서와 같이 데이터 및/또는 시스템을 삭제하여 이러한 공격을 수행합니다.

모든 사고가 침해로 확대되는 것은 아니며, SOC는 침해가 발생하는 것을 방지하기 위해 초기 단계에서 사고를 지속적으로 탐지하고 이에 대응해야 한다는 점을 이해하는 것이 중요합니다. 일부 침해는 조직의 내부에 포함되어 있으며, 표준 사고 대응 플레이북을 사용하여 이를 관리할 수 있습니다.

그러나 특정 사고, 특히 랜섬웨어 및 와이퍼 공격은 광범위한 영향을 미칠 수 있습니다. 이러한 사고는 고객에게 제품과 서비스를 제공하는 데 필요한 시스템과 사고 관리에 필수적인 내부 IT 시스템을 사용할 수 없도록 할 수 있습니다. 여기에는 시설에 대한 물리적 접근, 규제기관 및 영향을 받는 당사자 또는 데이터 주체와의 커뮤니케이션, 또는 보험사, 법집행 기관 및 언론과의 조율에 사용되는 시스템이 포함될 수 있습니다. 이러한 경우, 조직은 사이버 **위기**를 선언하고 해당 사고를 관리할 수 있도록 다른 워크플로우를 수행할 수 있습니다.

보안 및 IT 팀이 사고, 침해 또는 위기를 처리하고, 시스템을 신뢰할 수 있는 상태로 복원하며, 재발 위협을 완화하면 조직은 "평시" 운영 상태로 돌아갈 수 있습니다.

그림 1. 파괴적인 사이버 공격에서 "전시" 및 "평시" 단계.

파괴적인 사이버 공격이 비즈니스 연속성과 다른 이유

파괴적인 사이버 공격이 발생하기 전에 홍수, 화재, 장비 또는 소프트웨어 장애, 구성 오류 또는 정전과 같은 IT 중단의 근본 원인은 몇 가지에 불과합니다. 이러한 사고에는 최소한의 조사로도 충분했으며, 표준 대응 방법은 단순히 마지막 백업 스냅샷을 복원하는 것이었습니다.

그러나 랜섬웨어는 훨씬 더 복잡합니다. 기존 바이러스 또는 웜과 달리 단일 바이너리만으로 스캔할 수 없습니다. 적대세력은 일련의 14개 단계 전반에서 공격하며, 각 단계에서 목표를 달성하기 위해 수백 가지 기술 중에서 선택합니다. 이들은 끊임없이 혁신하고 있기 때문에 어제의 보안 통제 구성은 오늘에는 효과가 없습니다.

위협이 가중되고 있는 현재 글로벌화된 지정학적 상황은 국가 차원의 행위자에 의한 와이퍼 공격의 위험을 증가시켰습니다. 탁월한 운영 능력, 자금 조달 및 동기를 가진 이러한 위협 행위자에 대응하려면, 조직은 랜섬웨어 범죄 단체가 필요로 하는 것 이상으로 사이버 복원력을 구축해야 합니다.

랜섬웨어 대비 기존 멀웨어 조사 및 시정

바이러스 및 웜과 같은 기존 멀웨어는 시스템에서 악성 바이너리를 스캔하여 탐지합니다. 일단 식별되면 보안팀은 단순히 악성 바이너리를 격리하거나 삭제할 수 있습니다. 반면 랜섬웨어 또는 와이퍼 공격에는 공격자가 취약점이 새로 공개된 후 며칠 이내에 액세스할 수 있는 일련의 이벤트가 포함됩니다. 이러한 공격은 귀사의 IT 인프라를 활용하여 "기존 자원을 악용"하고, 승인된 계정을 악용하며, 권한 승격이나 지속성 유지를 위해 설정을 변경하고, 유출을 위해 민감한 데이터를 준비하며, 운영 체제 및 애플리케이션에 내장된 기본 제공 스크립팅 및 매크로를 사용할 수 있습니다. 이 모든 과정은 탐지, 대응 및 복구 능력을 저해하는 제어를 회피하면서 이루어집니다. 기존 멀웨어와 달리 단일 바이너리만으로 스캔 및 제거할 수 없습니다.

랜섬웨어 또는 와이퍼 공격으로부터 안전하게 복구하려면 사고 발생 원인을 조사해야 합니다. 조직은 재감염 및 추가 가동 중단 시간을 방지하기 위해 발견된 위협과 취약성에 대한 시정 조치를 해야 합니다. 이는 모든 모범사례 사이버 보안 사고 대응 프레임워크의 핵심입니다.

조직은 향후 유사한 공격에 대응하고 현재 공격에서 복구된 시스템의 재감염을 방지하기 위해 다음 세 가지 중요한 영역에 대한 시정 조치를 취해야 합니다.

1. **공격 표면**: 가장 일반적인 랜섬웨어 초기 액세스 벡터는 발생률 순으로 인터넷 연결 인프라의 취약점, 재사용된 합법적인 액세스 자격 증명, 피싱 이메일과 같은 소셜 엔지니어링 전술입니다. 초기 진입 지점 또는 처음 식별된 피해자인 "환자 0"이 어떻게 침해되었는지 파악한 다음 복구된 시스템에서 위협에 대한 시정 조치를 취해야 합니다. 여기에는 취약한 시스템에 패치를 적용하고, 취약한 시스템을 웹 애플리케이션 방화벽(WAF)과 같은 일부 형태의 보호 뒤에 배치하고, 사용자의 받은메일함에서 초기 액세스를 허용한 피싱 이메일을 제거하는 것이 포함될 수 있습니다.
2. **회피 기법 또는 보안 통제의 격차**: 기밀성, 무결성 또는 가용성에 영향을 미치기 전에 조기에 보안 사고를 예방하거나 탐지하는 것은 운영 비용이 발생하지만 수익 손실, 평판 훼손, 그리고 비용이 많이 드는 잠재적인 규제 벌금 및 비즈니스 파트너 또는 영향을 받는 데이터 주체가 제기하는 소송을 방지하는 데 도움이 됩니다.

랜섬웨어 조직은 엔드포인트 탐지 및 대응(EDR)과 확장된 탐지 및 대응(XDR)을 포함한 일반적인 보안 통제를 위해 자체 RaaS 플랫폼에 회피 기술을 구축합니다. 또한 이들은 사이버 위협 인텔리전스 피드를 업데이트하고 배포하여 이들의 공격 기법을 포함시키기 전에 선제 조치를 취할 수 있는 초기 행위자의 이점도 가지고 있습니다.

프로덕션을 재개하기 전에 기존 보안 통제가 해당 공격이 IT 서비스 제공을 차단하기 전에 공격을 중지하거나 탐지하지 못한 이유를 파악해야 합니다. 그런 다음 보안 툴링이 신뢰할 수 있는 상태로 복원되고 해당 규칙이 업데이트되어 향후 공격을 조기에 방지하거나 탐지할 수 있습니다.

3. **지속성 메커니즘**: 일반적인 랜섬웨어 또는 와이퍼 공격에서 공격자는 종종 수십 개의 아티팩트를 남깁니다. 이러한 아티팩트가 거점을 만들 수 있어, 남겨진 것에 대한 완전한 이해와 그것의 제거 없이 시스템을 복구할 경우 공격자는 계속 액세스할 수 있습니다. 조직은 시스템을 복구하는 데 며칠을 소비하고도 몇 분 이내에 시스템이 감염되어 다시 다운되는 것이 일반적입니다. 다시 말하자면, 이는 지속성 메커니즘을 간과했기 때문입니다. 파괴적인 사이버 공격의 다단계 특성으로 인해, 일반적으로 위협 헌팅과 포렌식 분석을 결합하여 공격 타임라인을 구축하여 해결해야 하는 아티팩트의 포괄적인 목록을 식별해야 합니다.

침해 지표 (IOC)에 대한 오해

침해 지표(IOC)의 개념은 전술적 사이버 위협 인텔리전스의 핵심입니다. 조직이 파괴적인 사이버 공격에 대응하기 위해 수행해야 하는 전시 활동에 대해 논의하기 전에 IOC를 정의하는 것이 중요합니다.

IOC는 시스템이 ***손상되었을 수 있음***을 나타내는 단서를 제공합니다. IOC는 적대세력 행위를 찾기 위한 출발점 역할을 하지만, 최종 대상이 아니라 단서 표지판인 경우가 많습니다. 안전하게 복구하려면 조직은 해당 공격의 윤곽을 파악하고 분석하여 이전 섹션에 설명된 적절한 완화 조치를 취해야 합니다. 예를 들어, 재부팅 시 특정 코드를 다시 실행하는 변경된 구성 파일은 IOC이며, 디렉터리에 포함된 합법적인 DLL과 이름이 같은 악성 DLL도 마찬가지입니다. 마찬가지로, 합법적인 DLL 전에 이 악성 DLL을 실행하기 위해 PATH 변수를 조작하는 것도 IOC입니다. 이러한 IOC는 무언가 진행되고 있다는 것을 알려주지만 공격의 전체 윤곽을 보여주지는 못합니다.

IOC를 위협 헌팅하는 것은 사이버 보안 사고 대응에 중요하지만, 조직은 올바른 맥락에서 IOC를 적용해야 합니다. IOC에만 의존하면 부적절한 조치로 이어질 수 있습니다. 또한 심층 조사 없이 백업으로 서둘러 복원하면 재감염이 발생하거나 기타 가용성 문제가 발생할 수 있습니다.

파일을 무작정 격리하거나, IOC가 포함된 백업 스냅샷에서 이전 버전의 파일로 복원해도 근본 원인은 해결되지 않습니다. 공격자들이 애초에 이런 변경을 초래한 방법을 아직도 알 수 없으므로, 공격자들은 시스템을 반복해서 공격할 수 있는 자유로움을 계속해서 누릴 수 있습니다. 또한 이전의 호환되지 않는 구성으로 되돌리면 가용성 문제가 발생할 수 있습니다. 특히, 예를들어 공격이 시작된 이후로 바이너리가 이후 버전으로 패치된 경우 더욱 그렇습니다.

마찬가지로 백업 스냅샷에 IOC가 없다고 해서 "클린" 상태가 보장되는 것은 아닙니다. IOC는 단순히 악의적인 활동에 대한 표지판 역할을 하기 때문에 표지판을 제거해도 “대상” 은 그대로 유지됩니다. 이전 스냅샷으로 자동으로 되돌리는 경우, 이 접근 방식은 사고 대응팀이 근본 원인이 되는 공격을 인식하지 못하게 할 수 있습니다.

또한 IOC를 탐지하는 것은 사이버 위협 인텔리전스를 수집, 분석 및 배포하는 데 의존하며, 이는 진화하는 적대세력 전술보다 뒤처지는 경우가 많습니다. 즉, 적대세력이 자체 행위를 변경하는 것과 새로운 공격 기법을 인식하는 보안 툴링 사이에 지연이 있습니다. 이는 많은 사이버 보안 예산과 최신 및 최대 사이버 보안 툴링을 사용하는 팀이 있음에도 불구하고 세계 최대의 조직 중 일부가 여전히 랜섬웨어의 영향을 받는 이유를 설명합니다. 적대세력은 자체 행동 방식을 변경하여 현재의 사이버 보안 툴링이 이러한 변경 사항을 인식하기 전에 조직 내부에 탐지되지 않고 침입할 수 있습니다. 내부에 침입하면 방어 회피 기능이 엔드포인트 보안 통제를 무력하게 만듭니다. 보안 도구 공급업체가 적대세력의 새로운 행위를 인지하고 관련 위협 인텔리전스가 자체 툴링에 제공되면 이미 너무 늦습니다. 이 도구는 이미 회피되어, 탐지할 수 없을 것입니다.

이러한 문제를 완화하려면 **Cohesity DataHawk**와 같은 솔루션을 사용하여 정기적인 사전 예방적 위협 헌팅과 같은 평시 활동을 도입하는 것이 좋습니다. 이 솔루션은 기존의 보안 통제와 독립적으로 작동하며 회피를 방지할 수 없습니다. DataHawk를 사용하면 사이버 위협 인텔리전스 소스가 공격을 인식하지 못했을 때 네트워크를 통해 유입되었을 수 있는 공격을 찾을 수 있습니다.

전쟁에서의 승리: 조사, 위협 완화 및 보안 복구

가장 좋은 접근 방식은 사고 대응자를 위한 효과 증대 수단으로 올바른 기술 솔루션을 확보하고 명확한 프로세스와 운영 모델을 정의하여 모든 사람이 자신이 해야 할 일을 정확히 알 수 있도록 복원력과 준비태세를 구축하는 것입니다. 가능한 경우 자동화 및 오케스트레이션을 사용합니다. 또한 직원은 최악의 상황이 발생할 때 반응하기보다는 대응을 위한 적절한 교육을 받고 현실적인 연습에 참여해야 합니다.

사이버 복원력은 구매할 수 있는 제품이 아닙니다. 이는 사이버 사고 후 소속 조직이 올바른 일을 할 준비가 되었을 때 나타나는 창발성입니다. 사이버 복원력을 달성하려면 조직이 파괴적인 사이버 공격 후 직면하는 문제에 대해 현실적이고, 올바른 기술과 강력한 사고 대응 전략을 구축하는 데 필요한 지원을 제공하는 공급업체와 협력해야 합니다.

사이버 보안 사고 대응은 복합적인 활동입니다. 성공은 그 복합성을 무시하는 것이 아니라 인정하는 것에서 비롯됩니다. 그렇지 않고 인정하는 시늉만 내는 것은 가능한 최악의 시간, 즉 사고 중에 조직을 위기로 내몰 것입니다.

사이버 보안 디지털 포렌식 및 사고 대응 모범사례

디지털 포렌식 및 사고 대응을 위해 널리 채택된 다음의 네 가지 주요 프레임워크가 있습니다.

1. NIST SP800-61 컴퓨터 보안 사고 처리 가이드
2. SANS Institute 6단계 사고 대응 프로세스
3. RE&CT(“React”) 프레임워크
4. MITRE D3FEND(“데이터 기반 방어”)

이 백서에서는 SANS Institute 모델을 사용하는 것에 중점을 둘 것입니다. 즉, 모든 프레임워크는 사이버 공격에 대비하고 대응하기 위해 취해야 할 단계에 주로 부합합니다.

그림 2. 사이버 디지털 포렌식 및 사고 대응 모범사례.

Cohesity를 통한 운영 모범사례 달성

전시 상황에서는 모든 모범사례 사이버 보안 사고 대응 프레임워크에 격리, 조사, 위협 완화 단계와 마지막으로 복구 단계가 포함됩니다. 격리, 조사 및 완화 단계를 단축하고 복구를 서두르는 조직은 공격에 이용된 취약점을 그대로 남기게 됩니다.

공격을 탐지하거나 차단하지 않은 방어에서의 격차는 여전히 열려 있으며, 종종 지속성 메커니즘 및 기타 공격 아티팩트가 다시 발생합니다. 이로 인해 재감염 또는 재공격이 빈번하게 발생하고, 이후 가동 중단 시간이 길어지게 됩니다. 랜섬웨어 공격에 대한 대응으로 복구 중심의 접근 방식을 취하는 조직이 12회 이상 복구를 해야 하는 것을 보는 것은 드문 일이 아닙니다.

식별

식별에는 다음 두 단계가 포함됩니다.

1. **잠재적 사고가 진행 중이라는 초기 인식**: 이는 사용자 또는 제3자의 보고서 형태(유효성 및 범위를 확인하기 위해 분류 필요) 또는 일부 형태의 기술적 통제로부터 제공되는 경고일 수 있습니다.
2. **공격이 어떻게 일어났는지 이해하기**: 이를 통해 위협의 적절한 근절, 악용된 취약점 제거 및 통제 강화를 보장하여 시스템을 안전하고 복원력 있는 상태로 복구할 수 있습니다.

각 단계를 더 자세히 살펴보겠습니다.

초기 인식

초기 인식은 기술적으로 평시 활동입니다. 조직이 공격이 진행 중임을 감지할 때까지 전시를 선언할 수 없기 때문입니다. 따라서 랜섬웨어와 같은 공격을 탐지하는 메커니즘에 대해 논의하여 이것이 사고 대응 워크플로우에 어떤 영향을 미칠 수 있는지 이해하는 것이 중요합니다.

RaaS 플랫폼은 EDR 및 XDR과 같은 인기 있는 보안 도구의 회피를 상품화하여 이러한 도구가 공격에 대해 탐지하지 못하게 만들었습니다. MITRE ATT&CK 프레임워크에서, 사이버 공격이 수행되는 방법을 설명하는 가장 인기 있는 분류 체계인 방어 회피 전술은 가장 근접하는 13가지 전술보다 기법의 수가 거의 두 배입니다. 랜섬웨어 공격자가 사용하는 이러한 메커니즘은 **Cohesity DataProtect**의 이상 탐지 및 DataHawk의 위협 헌팅 기능을 회피할 수 없습니다.

DataProtect의 **AI 기반 이상 탐지**에서 제공하는 것과 같은 경고는 높은 수준의 **신뢰도**와 높은 **충실도**를 가지고 있습니다. 이러한 신뢰도는 경고가 거짓 양성이 아니라는 것을 신뢰할 수 있도록 하고, 이러한 충실도는 SOC 분석가가 경고를 검토하여 어떤 일이 일어나고 있는지에 대한 정보의 양을 의미합니다. 이를 통해 분류 및 조사 프로세스가 가속화되어 시스템을 안전하게 프로덕션으로 복구하는 데 필요한 시간이 단축됩니다.

분류 중에 사고에 대응하는 데 필요한 시스템이 영향을 받았거나 조직 전체의 시스템에 대한 암호화 또는 삭제가 미리 정의된 특정 임계값을 초과하는 것이 분명해지면, 조직은 **사이버 위기**를 선언할 수 있습니다. 사전 정의된 사이버 위기 워크플로우를 통해 조직은 침해 사고 대응자가 사이버 침해에 대해 일반적으로 수행하는 조치 이상의 특정 조치를 수행할 수 있도록 다양한 권한 승격 및 사전 규정된 권한을 설정할 수 있습니다.

사고 대응 중에 필요한 시스템이 영향을 받거나, 사용할 수 없거나, 신뢰할 수 없는 것으로 밝혀질 수 있습니다. 이러한 상황에서의 문제에는 다음이 포함될 수 있습니다.

- 임원, 규제기관, 사이버 보험 제공사, 고용된 사고 대응 회사, 공급망 파트너, 언론 등의 사고 대응 이해관계자의 연락처 목록을 이용하지 못할 수 있습니다.

- 사고 대응 워크플로우를 이용하지 못할 수 있습니다.
- 사이버 보험 증권 및 고용된 사고 대응자를 위한 계약을 이용하지 못할 수 있습니다.
- 물리적 접근 통제 시스템 또는 건물의 환경 통제를 위한 관리 서버 및 설정이 중단될 수 있습니다.
- 이해관계자에게 연락하는 데 필요한 이메일 또는 VoIP와 같은 통신 시스템이 다운되거나 신뢰할 수 없는 상태일 수 있습니다.
- 라우터 및 스위치 설정 또는 펌웨어가 신뢰할 수 없게 되어, SaaS(software as a service) 애플리케이션 또는 통신의 인터넷 연결이 도청 또는 중단될 수 있습니다.
- 보안 툴링이 회피되거나 사용할 수 없게 되었을 수 있습니다.

당연히 대부분의 조직은 먼저 가장 중요한 애플리케이션의 복원을 우선시합니다. 이는 MVC(Minimum Viable Company)라고도 하는 제품 및 서비스 제공을 재개하는 데 필수적인 것입니다. 그러나 파괴적인 사이버 공격을 당하는 조직은 사고를 효과적으로 관리하려면 계정, 애플리케이션 및 인프라의 하위 집합도 필요하다는 것을 깨닫게 됩니다. 이러한 시스템은 조직의 규제 의무를 충족하면서도 중요한 운영 시스템을 복구할 뿐만 아니라 **안전한 상태**로 복구할 수 있도록 보장합니다.

Cohesity에서는 대응 및 복구 노력을 관리하기 위한 필수 인프라 및 리소스의 이러한 하위 집합을 MVRC(Minimum Viable Response Capability)로 정의합니다. MVRC의 구성 요소가 신뢰할 수 없거나 이용할 수 없게 되었다고 가정해 보십시오. 이 경우, 조직은 이러한 리소스를 사용할 수 있도록 하고 대응 조치를 관리하기 위해 신뢰할 수 있는 툴링 세트를 재구성할 수 있는 빠른 방법이 필요합니다. **Cohesity 클린룸 솔루션**을 통해 조직은 MVRC를 신뢰할 수 있는 상태로 신속하게 재구축하고 몇 분 안에 사고를 관리하는 데 필요한 리소스를 사용할 수 있습니다.

공격이 어떻게 일어났는지 이해하기

최초 분류가 완료되고 파괴적인 사이버 공격이 진행되고 있다는 확신이 들면, 분석가는 사고를 선언하고 심층 조사를 진행합니다. 일반적으로 랜섬웨어 조직이 수행하는 마지막 작업은 서버와 엔드포인트에 암호화를 배치하는 것입니다. 이는 탐지 제어를 트리거하고 최종 사용자가 볼 수 있는 충격을 생성하는 측면에서 가장 눈에 띄는 공격의 단계이기 때문입니다.

조사 및 시정 조치를 암호화된 시스템에만 집중하면 공격의 근본 원인을 발견할 가능성이 낮습니다. 대신, 조사는 이러한 시스템 이상으로 확장되어야 합니다. 암호화되지 않은 시스템은 복구 시도 후 적대세력이 돌아와서 사용할 수 있는 지속성 메커니즘을 포함할 수 있으므로 조사자에게 요주의 대상이 되는 경우가 많습니다.

이러한 심층적인 식별 수준을 자세히 살펴보기 전에 모든 모범사례 사고 대응 프로세스의 또 다른 측면인 격리가 이 작업을 수행하는 역량에 어떻게 방해가 되는지를 이해하는 것이 중요합니다.

격리

격리는 공격의 확산을 방지하고 명령 및 제어 또는 데이터 유출 활동을 중단하므로 모든 사고 대응 프레임워크의 요구 사항입니다. 그러나 격리는 보안 운영팀에게 몇 가지 과제도 제기합니다.

- **원격 이미징은 단독으로 작동하지 않습니다**. 대부분의 조직은 물리적으로 하드 디스크 콘텐츠를 획득하는 것에서 원격 포렌식 이미징으로 전환했습니다. 그러나 감염된 호스트 또는 호스트의 네트워크를 격리하면 이 작업을 수행할 수 있는 조직의 기능이 갑자기 제거될 수 있습니다. **DataProtect**는 사용자 인터페이스 및 API를 제공하여, 사고 대응자가 마지막 스냅샷뿐만 아니라 조직의 보존 기간까지 전체 스냅샷 시계열 전반에서 파일 수준 포렌식을 수행할 수 있도록 합니다. 이를 통해 디지털 포렌식 분석가는 시간 이동의 강력한 기능을 사용하여 적대세력이 이미 삭제한 바이너리 및 기타 아티팩트를 찾고 구성 및 기타 파일에 대한 악성 델타를 신속하게 식별할 수 있습니다. 일반적으로 짧은 로그 타임라인만 유지하는 엔드포인트 보안 솔루션 및 SIEM과 달리 Cohesity를 사용하면 사고 대응자가 해당 시스템에 백업이 유지되는 전체 기간에 걸쳐 이벤트와 로그 내용을 검사할 수 있으며, 이 모든 것은 변경 불가능한 플랫폼에서 제공되므로 강력한 관리 연속성을 보장할 수 있습니다. 무엇보다도 이러한 기능은 네트워크 연결 없이 제공됩니다. DataProtect는 이 작업을 위해 파일 시스템의 오프라인 복사본을 사용하기 때문에 도청 및 중단에 영향을 받지 않습니다.

- **엔드포인트 솔루션이 격리되고 쿼리/응답이 불가능해집니다.** EDR 및 XDR과 같은 다양한 엔드포인트 솔루션의 아키텍처는 다를 수 있지만, 거의 모든 것이 엔드포인트 클라이언트에서 텔레메트리를 수신하는 중앙 관리 서버를 가지고 있습니다. 격리가 관리 서버와 엔드포인트 간의 연결을 차단하는 경우, 분석가는 이전에 관리 서버로 전송된 정보만 이용할 수 있습니다. 더 이상 엔드포인트에서 일어나는 일에 대해 실시간으로 쿼리 및 응답 방식으로 작업하여 자세히 알아볼 수 없습니다.
- 또한 격리에는 격리된 환경을 구축하는 것도 포함됩니다. 이러한 환경에서 침해 사고 대응 및 복구 기법이 발생할 수 있습니다. Cohesity 클린룸 솔루션은 이러한 환경을 조성하는 유연한 접근 방식을 제공합니다. 이것은 조직이 사고 대응 모범사례에 부합하고 보안과 IT 운영 간에 적절한 공동 책임 모델을 채택하는 데 도움이 됩니다. 이러한 접근 방식은 조직이 가동 중단 시간을 예방하고 복구 후 재감염을 방지하는 데 도움이 됩니다.

- Cohesity 클린룸 솔루션:
- 사고를 조사하고 시정 조치를 취하는 데 필수적인 MVRC 또는 영향을 받거나 회피된 인프라를 신속하게 복구할 수 있습니다.
- 보안 운영팀이 다른 보안 툴링과 함께 Cohesity Data Cloud 플랫폼의 기본 제공 보안 기능을 사용하여 엔드투엔드 공격을 이해하고 향후 공격을 방지하기 위한 적절한 시정 조치를 계획할 수 있는 격리된 조사 환경을 구축합니다.
- 보안 운영팀의 조사 결과를 통해 시정 조치에 정보를 제공하는 격리된 완화 환경을 조성합니다. 이러한 시정 조치에는 알려진 양호한 설치 이미지 및 구성에서 시스템을 신속하게 재구성, 시스템 복구, 취약점에 대한 패치 적용, 우회할 수 없도록 제어 강화, 향후 유사한 공격의 성공적인 예방 또는 탐지 등이 포함됩니다. 마지막으로, 운영 시스템으로 복원하기 전에 시스템의 기능과 성능을 테스트할 수 있습니다.

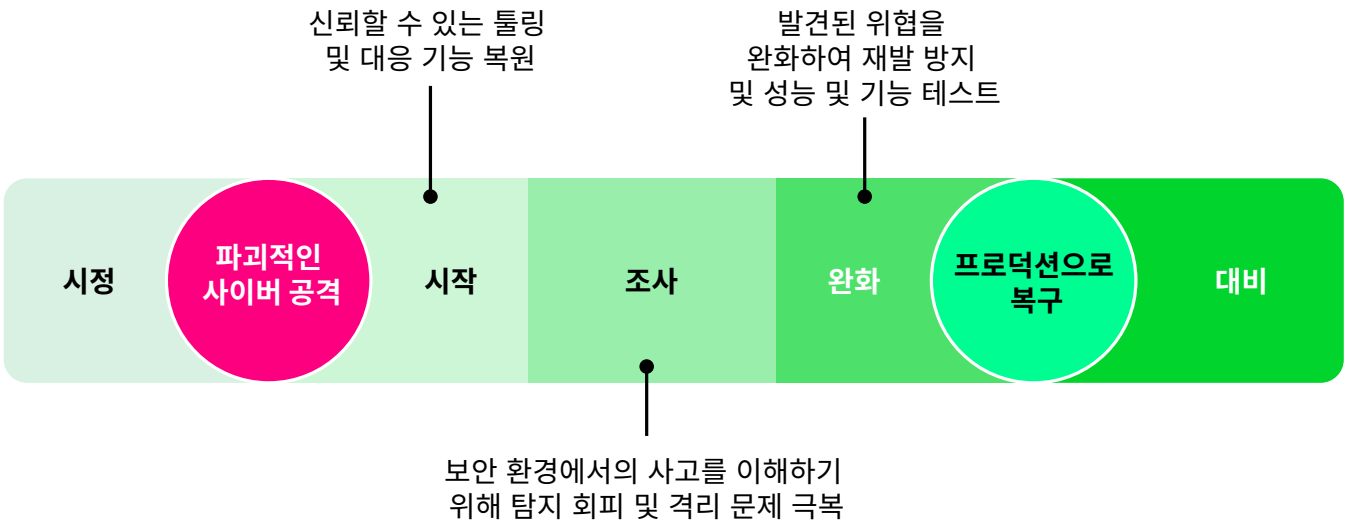

그림 3: 고객을 사이버 공격의 시정 조치로 안내하는 Cohesity 클린룸 솔루션의 4단계.

식별 단계 재검토: Cohesity 클린룸 솔루션의 지원 방법

디지털 포렌식 및 사고 대응 모범사례에 따라 조직은 이제 감염된 네트워크와 호스트를 격리했습니다. 이 단계에서 사고에 대한 조사 및 시정 조치에 필요한 영향을 받은 인프라는 신뢰할 수 있는 상태로 다시 설정됩니다. 즉, 인터넷 연결을 신뢰할 수 있어 클라우드 기반 IT, 비즈니스 및 보안 서비스를 사용할 수 있습니다. 또한 이해관계자와의 커뮤니케이션 기능이 다시 설정됩니다. 가장 중요한 것은 사고 대응 및 복구를 지원하는 데 필요한 모든 문서와 리소스를 보안팀과 IT 운영팀이 손쉽게 이용할 수 있다는 것입니다.

이제 Cohesity가 조사 중인 자산은 봉쇄를 통해 격리하는 동시에 심층적인 조사에는 어떻게 도움이 되는지 살펴보겠습니다.

공격에서 악용된 취약점 발견

랜섬웨어 조직과 와이퍼 공격을 준비하는 국가는 인터넷 연결 자산의 취약점을 통해 가장 일반적으로 초기 액세스 권한을 얻습니다. 적대세력은 취약점을 통해 초기 액세스 권한을 얻은 후 지속성 메커니즘을 설치하여 시스템 내에 잠입한 후 다른 공격자가 해당 시스템에 액세스하지 못하도록 해당 지속성 메커니즘에 패치를 적용할 수 있는 것으로 알려져 있습니다.

조직은 공격 당시 어떤 취약점이 존재했는지 어떻게 알 수 있습니까? 적대세력이 시스템을 삭제했거나 격리 조치로 인해 취약점 스캔을 위해 시스템에 액세스할 수 없는 경우 이는 더욱 더 어려워집니다.

Cohesity CyberScan은 조직이 자체 Tenable Vulnerability Management 라이선스를 사용하여 백업 스냅샷에서 취약점을 스캔할 수 있는 솔루션을 제공합니다. 이를 통해 보안팀은 시스템이 격리로 인해 이용할 수 없거나, 지워졌거나, 침입 후 적대세력에 의해 패치가 적용된 경우에도 공격 중에 취약점을 식별할 수 있습니다.

파일 시스템 포렌식 수행

파일 시스템 포렌식은 사고 대응의 핵심 분야입니다. 많은 조직에서 포렌식 이미징을 위해 원격 수집 도구를 사용합니다. 그러나 일단 격리 조치가 시행되면, 포렌식 이미징이 필요한 시스템에는 더 이상 액세스할 수 없는 경우가 많습니다.

DataProtect는 분석가가 파일 시스템의 단일 볼륨 스냅샷뿐만 아니라 전체 스냅샷 시계열에 액세스할 수 있도록 합니다. 이를 통해 포렌식 조사관은 사고 타임라인뿐만 아니라 전체 백업 보존 기간에 걸쳐 조사를 진행할 수 있습니다. 볼륨 시계열 데이터를 신속하게 마운트하고 비교하여 악성 델타를 식별할 수 있습니다. 리버스 엔지니어링, 샌드박스 내에서 실행, 또는 분석을 위해 파일 객체를 클라우드 기반 서비스로 전송하여 추출할 수 있습니다.

그림 4: 사고 대응 모범사례에 대한 Cohesity 클린룸 조정

기존의 디지털 포렌식에서 사고 대응자는 일반적으로 공격 후 시스템의 단일 이미지를 수집하고, 시스템이 어떻게 해당 최종 상태에 도달했는지에 대한 가설을 세운 뒤, 해당 이론을 입증하거나 반박할 증거를 거꾸로 수집합니다. 이와는 대조적으로, DataProtect를 사용하면 이제 사고 대응자는 훨씬 더 많은 사고 타임라인 전반에 배치된 파일 시스템 변경 사항을 확인할 수 있으며, DataProtect는 봉쇄 노력으로 감염된 호스트가 격리된 경우에도 계속 작동합니다.

위협 헌팅

IOC 위협 헌팅은 사고 대응자가 일반적으로 수행해야 하는 또 다른 작업입니다. 이러한 전시 위협 헌팅은 다음 두 가지 범주에 해당합니다.

제3자가 제공한 IOC에 대한 스캔. 이러한 제3자에는 사이버 위협 인텔리전스 공급업체, 정부 기관 또는 동료 조직이 포함될 수 있습니다. DataHawk를 사용하는 Cohesity 고객은 랜섬웨어 및 국가 행위자가 사용하는 117,000개 이상 IOC를 포함하는 자주 업데이트되는 피드를 활용할 수 있습니다. 또한 DataHawk의 위협 스캔 기능은 조직이 라이선스를 부여하고 다른 제3자로부터 YARA 형식으로 공급된 모든 IOC를 사용할 수 있는 상용 CrowdStrike 위협 인텔리전스 피드를 지원합니다.

소속 조직에서 검색한 IOC 스캔. 소속 사고 대응자는 조사 중에 아티팩트를 발견하면 이러한 IOC가 조직의 인프라 전반에 존재하는지 확인하기 위해 위협 헌팅을 하려고 합니다. 거기서부터 사고 대응의 범위에 추가 시스템을 도입해야 하는지 여부를 결정합니다.

이는 일반적으로 탐지를 허용하지만 불필요한 거짓 양성을 방지하는 방식으로 발견된 아티팩트를 설명하는 YARA 규칙을 생성하여 수행됩니다. Cohesity를 사용하면 포렌식 분석을 수행하고(이전 섹션에서 논의한 대로), 파일 시스템 아티팩트를 추출하여 Cuckoo와 같은 샌드박스에서 실행할 수 있습니다. Cuckoo는 플러그인을 통해 해당 파일과 관련된 모든 IOC에 대한 YARA 규칙을 자동으로 생성할 수 있습니다. DataHawk 위협 헌팅 기능은 엔드포인트 에이전트에 의존하지 않습니다. 이 기능은 조직이 봉쇄를 위해 격리된 시스템을 가지고 있더라도 계속 작동합니다. 이는 엔드포인트 보안 솔루션이 효과적으로 위협 헌팅을 할 수 없게 만드는 일반적인 방어 회피 기법에도 취약하지 않습니다.

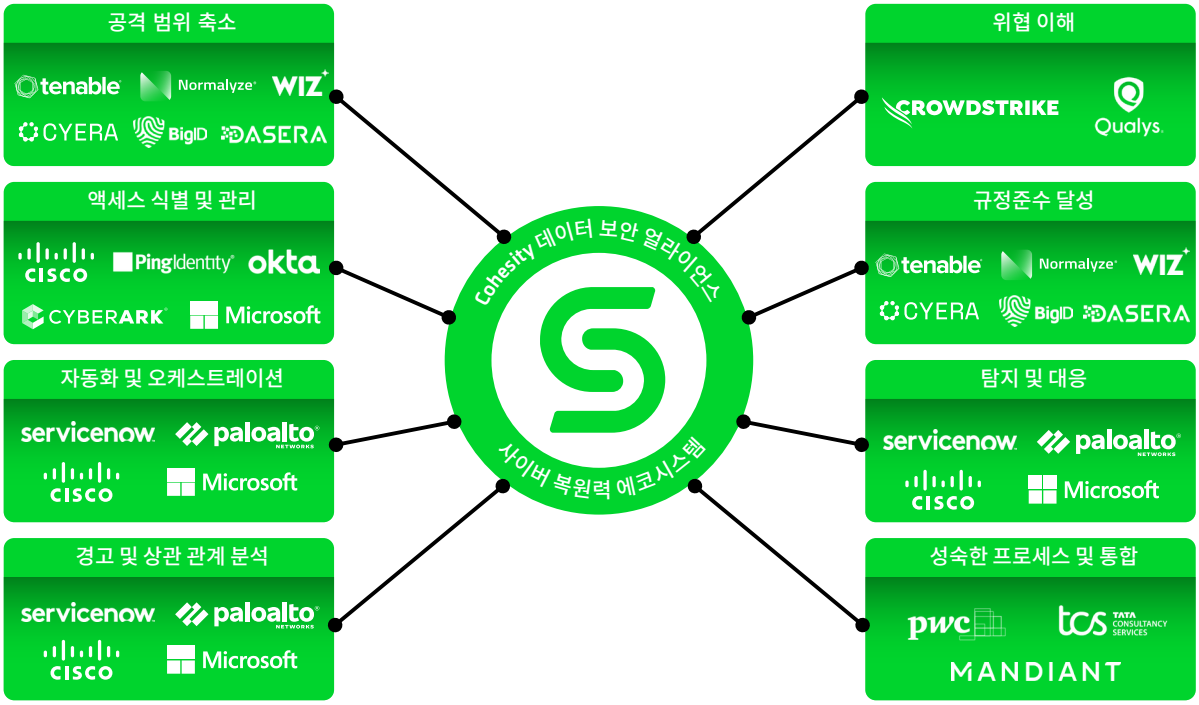

그림 5: Cohesity 데이터 보안 얼라이언스: 사이버 복원력을 위한 에코시스템.

Cohesity Global Search와 같은 기능을 통해 사고 대응자는 백업된 모든 인프라 전반에서 파일을 빠르게 위협 헌팅할 수 있으므로, 특정 아티팩트 또는 파일을 찾을 때 직접 조사 작업을 지원할 수 있습니다.

규제 준수 달성

견고한 사고 대응 프로세스를 의무화하는 것 외에도 HIPAA, DORA, NIS 2 등 최근에 업데이트된 많은 준수 규정에 따라 사이버 보안 침해가 발생할 경우 조직은 규제기관 및 영향을 받는 데이터 주체에게 해당 사실을 알려야 합니다. 침해의 성격을 이해하는 것은 그 영향을 이해하는 것과 적시 통지를 보장하는 것과 마찬가지로 식별 단계의 일부입니다.

사고가 커뮤니케이션에 영향을 미쳤다면 MVRC의 일환으로 Cohesity가 이 기능의 복원을 지원할 수 있습니다. 커뮤니케이션 템플릿은 클린룸의 기반인 **Digital Jump Bag**™에 보관할 수 있습니다. 또한 DataHawk는 백업을 스캔하여 민감한 규제 대상 데이터를 식별하여 조직이 규제 요건을 충족할 수 있도록 지원합니다. 이는 파괴적인 사이버 공격 후에 중요한 데이터 저장소가 암호화되거나 삭제될 때 특히 중요합니다.

보안 운영 툴링 통합

사이버 복원력은 팀 스포츠입니다. 단일 공급업체의 솔루션만으로는 사고 전체를 조사하고 시정 조치를 취할 수 없습니다. 이것이 바로 Cohesity가 데이터 보안 얼라이언스를 구축한 이유입니다. 이러한 협업 에코시스템을 통해 공통 거버넌스, 조사 및 복구를 위한 통합을 통해 데이터 자체와 시계열 데이터의 힘을 더 광범위한 보안 툴링 및 서비스로 가져올 수 있습니다.

자동화 및 오케스트레이션

Cohesity는 API 통합을 지원하므로 보안 오케스트레이션 및 자동 응답(SOAR) 플랫폼이 이러한 조사 작업을 주도하여 분석가 효율성을 더욱 높일 수 있습니다.

근절 및 복구

근절 및 복구 단계를 완화 단계로 통합했습니다. Cohesity와 협력하는 어떠한 조직도 해당 조직을 공격하는 적대세력이 시스템을 재감염시키거나 향후 동일한 성격의 공격이 성공하지 않도록 하는 적절한 조치 없이 파괴적인 사이버 공격으로부터 복구해서는 안 되기 때문입니다.

Cohesity 클린룸 솔루션은 신속한 볼륨 복구를 지원하므로, 위협 근절을 위해 완화 조치를 시행하기 전에 전체 파일 시스템을 복구할 수 있습니다. 이를 통해 안전한 시스템 복구를 보장하는 동시에 신뢰할 수 있는 소프트웨어 이미지와 검증된 정상 구성에서 시스템을 빠르게 재구성할 수 있습니다. 각 접근 방식마다 다음과 같은 장단점이 있습니다.

복구 및 클리닝 접근 방식	
장점:	**단점:**
사고에 앞서 미리 관리하는 것이 더 간단한 방법입니다.	조사는 심층적이고 철저하게 진행해야 합니다.
	시정 조치에 소요되는 시간은 일반적으로 재구축된 시스템에 필요한 시간보다 깁니다.
재구축 접근 방식	
장점:	**단점:**
동시에 데이터를 복구하고, 시스템을 재구축하며, 사고를 조사할 수 있는 기회를 제공하여 시스템을 안전한 상태로 가능한 가장 짧은 시간 동안 복구할 수 있습니다.	일반적으로 조사는 시스템이 신뢰할 수 있는 상태에 있으므로 심층적일 필요는 없습니다.
시정 조치가 단축되어 일반적으로 구성의 보안을 검증하고, 제어를 강화하고, 취약한 시스템에 패치를 적용하기만 하면 됩니다.	여기에는 재설치 스크립트를 구축하는 업무 능력이 필요합니다.
	설치 미디어, 라이선스 키, 구성 파일 및 스크립트는 디지털 점프백에 보관해야 합니다.

일부 Cohesity 고객은 볼륨 수준 백업과 재구축을 모두 지원하기 위해 선택합니다. 이를 통해 고객은 해당 시스템을 클리닝하는 데 수반되는 노력의 수준과 해당 클리닝이 공격 아티팩트를 남기지 않을 것이라는 확신의 정도에 따라 침해된 각 호스트에 대해 가장 적절한 보안 복구 방법을 선택할 수 있습니다.

고객은 Cohesity 클린룸 완화 환경으로 사용하기 위해 개발 환경의 용도를 변경하는 경우가 많습니다. 이 접근 방식을 통해 격리된 클린룸 완화 환경 내에서 발생하는 완화 활동과 동시에 운영 서버를 초기화할 수 있습니다. 완화 환경은 디지털 점프백에 저장된 구성을 사용하여 프로덕션 환경의 구조를 모방하도록 구성됩니다.

조사 단계에서 발견된 위협이 복구 및 클리닝 또는 신뢰할 수 있는 상태로의 재구축을 통해 완화되면 시스템을 테스트할 수 있습니다. 기능 테스트 및/또는 성능 테스트의 형태로 실시되어 시정 조치, 패치 적용 및 제어 강화가 시스템의 제공 능력에 영향을 미치지 않았음을 보장할 수 있습니다.

마지막으로 이러한 시스템의 스냅샷은 다음 두 가지 목적으로 수집됩니다.

1. 공격 아티팩트를 놓친 경우에도 처음부터 다시 시작할 필요가 없습니다. 시정 조치 후 얻은 스냅샷은 조사 및 추가 시정 조치를 위한 새로운 기준 역할을 하며 조사 단계로 전달됩니다.
2. 완화 환경이 프로덕션처럼 보이도록 구성되었기 때문에 이 스냅샷은 단순히 프로덕션 네트워크로 "리프트 앤 시프트(lifted and shifted)"될 수 있습니다.

학습한 교훈

사이버 복원력을 구축하고자 하는 조직은 지속적 개선의 원칙을 따라야 합니다. 무엇이 효과가 있었는지, 무엇이 효과가 없었는지, 무엇을 개선할 수 있는지 이해하는 것은 조직이 지속적인 가동 중단 시간을 겪지 않고 향후 사고를 보다 효과적이고 효율적으로 처리할 수 있도록 하는 데 매우 중요합니다. 격언에 따르면 "실제 교전에 그대로 적용할 수 있는 계획은 없습니다." 실제 공격을 시뮬레이션하는 것은 기술적 복구 테스트와 프로세스 개선 추진에 있어서 중요하고, 자동화 기회를 식별하며, 분석가와 사고 대응자가 경험을 축적하게 합니다.

Cohesity 클린룸 솔루션의 가장 큰 장점 중 하나는 조직이 운영 시스템에 영향을 주지 않고 전체 사고를 엔드투엔드로 시뮬레이션할 수 있다는 것입니다. DataProtect를 사용하면 운영 시스템의 복제가 가능하여, 이러한 복제에 대한 내부 레드팀 또는 외부 침투 테스트 회사의 공격을 통해 엔드투엔드 랜섬웨어 또는 와이퍼 공격을 시뮬레이션할 수 있습니다. 전체 대응 및 복구 워크플로우는 시정 조치가 적용된 시스템의 기준 스냅샷을 얻은 직후까지 수행될 수 있습니다. 이를 통해 조직은 불가피한 일이 발생하고 조직이 피해자가 될 때 파괴적인 사이버 공격의 영향을 최소화하기 위해 적절한 인력, 업무 능력, 프로세스 및 지원 기술을 마련할 수 있는 실제 시나리오를 수립할 수 있습니다.

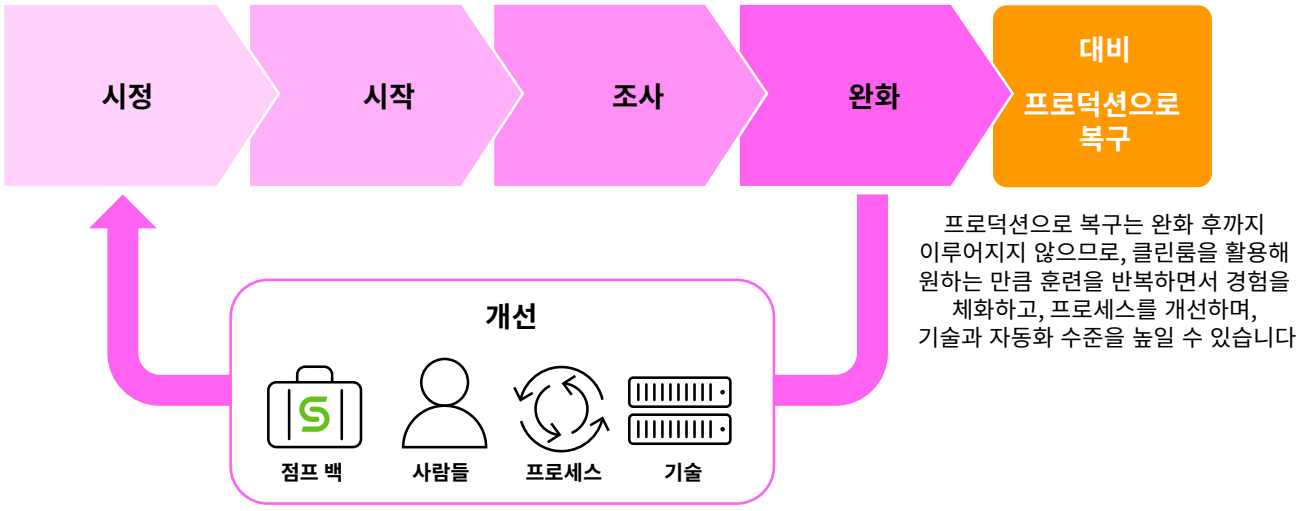

그림 6: Cohesity 클린룸 솔루션을 사용하면 실제와 같은 훈련을 통해 지속적 개선을 구현할 수 있습니다.

요약

Cohesity는 복구에 엄청난 가치를 추가로 창출할 수 있으며 디지털 포렌식뿐만 아니라 전시의 사고 대응 단계를 효과적이고 효율적으로 만들 수 있습니다. 사이버 복원력에 대한 당사의 고유한 접근 방식은 안전한 복구를 달성하는 데 걸리는 시간을 줄이고 유사한 공격으로 추가 가동 중단 시간이 발생하지 않을 것이라는 확신을 조직이 갖도록 지원합니다.

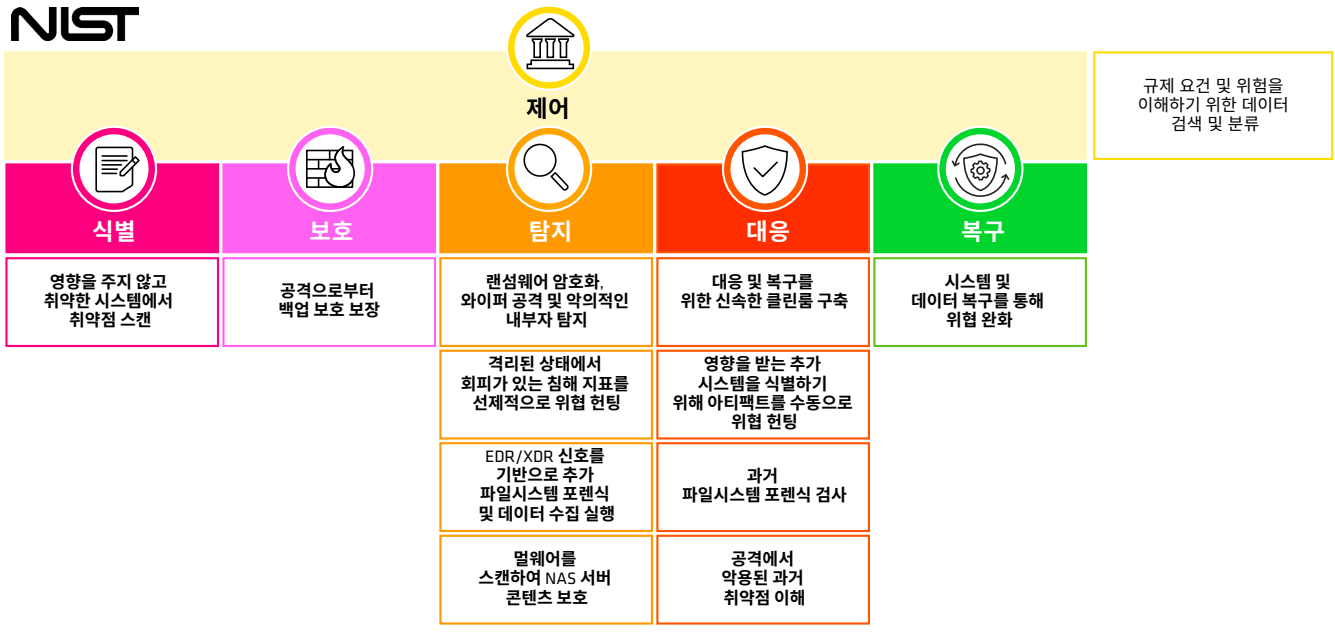

그림 7: Cohesity를 통해 사이버 사고 대응 및 NIST 사이버 보안 프레임워크 모범사례 달성

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 고객은 Cohesity를 통해 복원력을 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.

추천 자료

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

- **Digital Jump Bag™으로 사이버 복원력 향상**
- 사이버 공격이 벌어지는 환경에서 사이버 복원력 구축
- **Cohesity** 클린룸 설계 소개
- **AI** 기반 데이터 보안을 위한 현장 가이드: 혁신적인 비즈니스 성과를 제공하는 방법
- 최신 데이터 보안 및 관리에 대한 경영진 가이드
- 최신 데이터 보안 및 관리 토폴로지: **IT** 리더를 위한 가이드

Cohesity에서 자세히 알아보기

COHESITY

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

2000056-002-KO 4-2025