COHESITY

백서

사이버 공격이 벌어지는 환경에서 사이버 레질리언스 구축

Cohesity의 파괴적 사이버 공격 레질리언스 성숙도 모델을 통해 비즈니스를 평가해 보십시오.

목차

요약

데이터는 상업 조직과 비영리 조직 모두의 생명선입니다. 이는 정보 기술에 크게 의존하게 된 프로세스 및 워크플로우의 필수 구성 요소로서, 수동의 "펜과 종이" 프로세스로 되돌리려는 시도는 조직의 제품 또는 서비스 제공 능력에 상당한 영향을 미칠 수 있는 혼란을 야기합니다.

역사적으로 이러한 중단은 홍수, 화재, 전력 손실, 구성 오류 또는 장비 고장과 같은 잘 정의된 소수의 시나리오로 인해 발생하는 비즈니스 연속성 및 재해 복구의 영역이었습니다. 오늘날 가장 일어날 가능성이 높은 혼란은 파괴적인 사이버 공격이 원인입니다.

이 백서에서는 IT 운영팀이 비즈니스 연속성 및 재해 복구 시나리오를 처리하는 데 사용한 기존 접근 방식이 이 새로운 위협을 처리하는 데 더 이상 적합하지 않은 이유를 살펴보겠습니다. 또한 보안 운영팀이 과거에 파괴적이지 않은 사이버 공격을 처리하는 데 사용한 침해 사고 대응 프로세스가 부족한 이유에 대해서도 논의할 것입니다.

마지막으로, Cohesity 파괴적 사이버 공격 레질리언스 성숙도 모델을 통해 조직이 파괴적인 사이버 공격에 대한 레질리언스를 강화하기 위해 취할 수 있는 실용적인 조치를 제공합니다. 이 모델을 사용하여 조직은 오늘날의 레질리언스 성숙도를 평가하고 시간이 지남에 따라 레질리언스를 개선하기 위한 로드맵을 개발할 수 있습니다.

새로운 위협과 기존 접근 방식의 부족

랜섬웨어는 1989년에 출시된 "AIDS 트로이 목마"로 뿌리를 거슬러 올라갈 수 있지만, 약 20년 후에 암호화폐가 등장하기 전까지는 이러한 공격이 손쉽게 수익화되어 오늘날 우리가 겪고 있는 맹공격이 이어졌습니다.

2012년에는 Flame과 Shamoon 와이퍼 악성코드가 모두 발견된 또 다른 유형의 파괴 공격이 나타났습니다. 이들은 이란 및 사우디아라비아 석유 회사의 이익과 관련된 데이터를 각각 표적으로 삼아 파기했습니다. 범죄자들이 금전적 이득을 위해 사용하는 랜섬웨어 공격과 달리, 이러한 와이퍼 공격은 다른 국가의 이익이나 경제에 해를 끼치는 국가 행위자 또는 그 지지자들의 작업입니다. 현재 지정학적 상태로 인해 최근 전 세계적으로 와이퍼 공격이 크게 증가했습니다.

정보 보안 분야의 근원부터 파괴적인 랜섬웨어 공격의 부상에 이르기까지 이 분야에서 조직이 직면한 주요 영향은 데이터 도난이었습니다. 데이터 도난은 사기 또는 물리적 상품의 도난과 달리, 조직은 여전히 데이터 사본을 보유하고 있으며, 이 데이터를 사용하여 고객에게 제품과 서비스를 계속 제공할 수 있습니다. 이러한 공격의 영향으로는 평판 손상으로 인한 2차 손실, 데이터가 도난당한 파트너 또는 데이터 주체의 잠재적 소송 또는 규제 벌금 등이 있습니다.

오늘날 랜섬웨어 및 와이퍼 공격과 같은 파괴적인 사이버 공격의 시대에 이러한 2차 손실과 함께 1차 손실, 즉 조직이 제품과 서비스를 제공할 수 없는 손실이 발생합니다. 2차 손실의 대부분은 되돌릴 수 없지만(즉, 사고 발생 전에 사고를 방지하기 위한 적절한 통제를 마련하지 않음으로써 원인이 발생함), 대응 및 복구 활동에 소요되는 매초마다 조직의 1차 손실이 증가합니다. 조직 데이터의 기밀성에 대한 공격을 통해 비효율적이고 효과적이지 못한 대응 및 복구 프로세스를 용인할 수 있었습니다. 조직에 매우 중요한 데이터의 무결성 또는 가용성에 대한 공격으로 인해 우리는 더 이상 해당 권한이 없습니다.

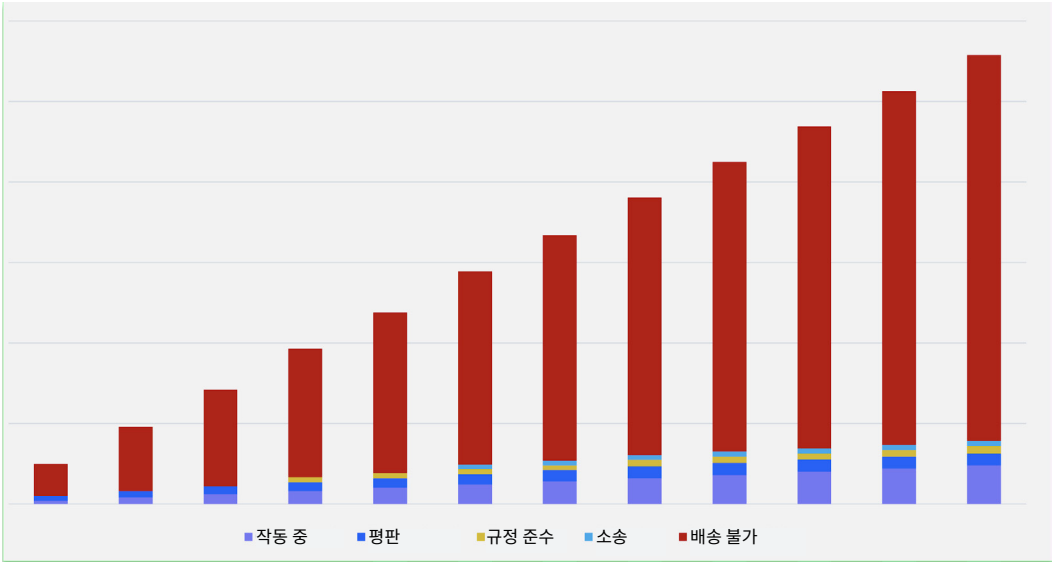

그림 1: 다양한 유형의 손실에 대한 시간의 표시 효과

서비스형 랜섬웨어(RaaS)의 최근 개발로 인해 방어자의 상황을 더 악화시킬 뿐입니다. 역사적으로 우리는 자체 인프라를 운영하고 공격을 수행한 랜섬웨어 공격자 수십 명과 집단적으로 마주했습니다. 랜섬웨어 공격자가 인프라를 운영하는 데 필요한 기술적 능력을 통합해야 할 필요성으로 인해 공격 횟수가 제한되었습니다.

이러한 많은 공격자들은 기술적 능력이 아닌 공격을 수행하는 데 필요한 인적 자원만 필요한 "계열사"가 랜섬웨어 플랫폼과 툴킷을 사용할 수 있도록 하는 것이 더 수익성이 있다는 것을 알게 되었습니다. 그 대가로 계열사는 일반적으로 몸값의 80%를 가져가고, 플랫폼 운영자는 20%를 차지합니다. 또한 RaaS를 통해 플랫폼 운영자는 플랫폼의 공격 도구를 혁신하여 다른 제공업체와 차별화하는 데 더 집중할 수 있었습니다. 한 가지 결과는 피싱을 1차 공격 벡터로 사용하는 것에서 인터넷 연결 인프라의 취약점 무기화와 같이 성공률이 높은 다른 기술로의 이동이었습니다. 이 작업은 조직이 패치를 통해 공격 표면을 폐쇄하기 훨씬 전인 며칠 내에 발생할 수 있습니다. 또 다른 증가하는 추세는 이전 공격에서 도난당한 자격 증명을 재사용하는 것입니다.

더 심각한 영향을 미치는 공격이 증가하는 문제에 직면하고 있지만, 사이버 보안에 대한 대부분의 지출은 역사적으로 기밀 유지에 대한 공격에 초점을 맞춰왔기 때문에 전통적으로 보호 및 탐지에 집중되어 왔습니다. 조직이 거의 매일 목격하는 침입 시도의 폭주에 휩쓸리는 것을 방지하도록 예방 및 탐지에 대해 비용을 지출하는 것도 중요하지만, 오늘날 파괴적인 사이버 공격의 규모와 정교함을 처리하기에는 충분하지 않았습니다. 지난 12개월 간의 헤드라인을 간단히 살펴보면 수천만 달러의 사이버 보안 예산을 가진 많은 조직이 랜섬웨어로 인해 운영에 상당한 지장을 받았음을 알 수 있습니다. 따라서 보호 및 탐지에 대한 비용 지출만으로는 충분하지 않습니다. 우리는 해자를 더 넓게 만들고 벽을 더 높게 쌓지만, 적군은 더 나은 배나 더 높은 사다리를 건설하거나 사회적으로 공학적인 방법을 통해 성문을 뚫고 들어올 뿐입니다.

NIST 사이버 보안 프레임워크 2.0과 같은 거의 모든 최신 **사이버 보안 프레임워크 EU 네트워크 및 정보 보안(NIS2) 지침 2.0** 또는 **EU 디지털 운영 레질리언스법(DORA)**같은 규정은 레질리언스 구축에 중점을 두고 있습니다. 이는 사이버 공격을 예방하고 탐지할 수 있는 능력뿐만 아니라 대응 및 복구를 통해 이를 견딜 수 있는 능력인데, 이 두 가지 기능은 기존에 투자가 부족했습니다.

평균적으로 기업에는 130개 이상의 서로 다른 사이버 보안 도구가 설치되어 있으며, 그 중 대다수는 조직이 사이버 공격의 피해자가 되는 것을 방지할 수 있을 만큼 충분히 통합되고 운영되지 못했습니다. 예방 및 탐지에 대한 추가 투자는 사이버 위험을 극히 일부만 감소시키는 반면, 사용자와의 마찰을 심화하고, 조직의 민첩성을 낮추며, 경보 피로를 높이고, 라이선스 비용을 증가하고, 관리할 보안 인프라를 더 많이 생성할 가능성이 높습니다. 반면, 대응 및 복구에 투자하면 이러한 최신 프레임워크 및 규정에서 요구하는 사이버 레질리언스와 최신 사이버 공격 위협이 요구하는 사이버 레질리언스를 확보할 수 있습니다.

사이버 레질리언스 달성을 가로막는 5가지 장벽

기존의 BC/DR 복구 접근 방식은 사이버 공격에 적합하지 않습니다

사이버 보안에서 사이버 레질리언스로의 전환에 대한 가장 큰 장벽 중 하나는 많은 조직에서 대응 기능은 최고 정보 보안 책임자(CISO)가 감독하는 팀이 담당하고, 복구 기능은 최고 정보 책임자(CIO)가 감독하는 팀이 담당한다는 것입니다. 이 두 기능은 원래 다른 위협을 처리하도록 구축되었기 때문에 대부분 서로 독립적으로 이러한 기능을 구축했습니다. 역사적으로 CISO는 데이터 도난 공격을 처리하고, CIO는 재해 복구 및 비즈니스 연속성(BC/DR)을 처리했습니다. BC/DR 전략은 홍수, 화재, 지진, 전력 손실, 장비 고장 또는 구성 오류와 같이 쉽게 이해할 수 있는 한정된 수의 위협 시나리오를 중심으로 다루어졌습니다.

막대한 사이버 보안 예산을 가지고 BC/DR 프로그램이 잘 구축된 조직이 랜섬웨어의 피해자가 되었을 때 헤드라인을 장식하는 이유는 이러한 두 가지 측면이 파괴적인 사이버 공격을 견디는 데 적합하게 적용되지 않았기 때문입니다. 막대한 비용과 엄청난 고객 혼란이 그 결과입니다.

CIO의 BC/DR 계획은 잘 정의된 소수의 근본 원인을 대처하도록 설계되었습니다. 자동화 및 오케스트레이션은 복구에서 큰 역할을 할 수 있으며, 일반적으로 시스템의 마지막 스냅샷이 복구됩니다.

이와 대조적으로 파괴적인 사이버 공격의 경우, 공격자는 백업을 적극적으로 표적으로 삼아 사용할 수 없게 함으로써 공격 성공 가능성을 높입니다. 이러한 공격자는 수백 개의 MITRE ATT&CK 기술을 원하는 순서대로 반복적으로 조합하여 취약성 악용을 통해 조직 내부로 침투할 수 있습니다. 일단 침투하면 권한을 확대하고, 백업에서 복구한 후에도 지속성을 유지하고, 조직 전체에서 측면으로 이동하고, 데이터를 훔치고, 결국 삭제하거나 암호화합니다.

파괴적인 사이버 공격으로 인한 비용이 가장 많이 드는 조직은 공격자가 백업을 사용할 수 없게 만들거나, 위협과 취약성을 제거하기 위한 적절한 복구 단계 없이 공격을 받은 시스템을 복구하여 동일한 시스템을 몇 초 또는 몇 분 이내에 재감염시키는 조직입니다.

조사가 완화에 도움이 되지 않습니다

파괴적인 사이버 공격으로부터 복구할 때 IT 운영팀은 보안 운영팀에 의존하여 재감염 및 재공격을 방지하기 위해 취해야 할 조치를 이해합니다. 보안 운영팀의 조사 결과:

- 시스템이 프로덕션으로 복귀하기 전에 IT 운영팀이 패치를 적용할 수 있도록 공격자가 악용한 취약점
- 시스템에서 제거할 악성 계정 및 인증 공급자
- 사용자의 받은 편지함에서 다시 클릭되기를 대기하는 이메일
- 변경된 구성 파일에 상주하며 제거가 필요한 지속성 메커니즘
- 공격자가 바이너리 또는 라이브러리를 악성 바이너리로 교체했는지 여부
- 레지스트리 또는 도메인 포리스트에 변경 사항이 있는지 여부

- 재발을 방지하기 위해 강화할 수 있도록 공격을 중지하거나 탐지하지 못한 통제
- 복구된 시스템에서 제거해야 하는 공격의 기타 아티팩트

또한 LOL("합법적인 시스템 도구 악용") 공격이 점점 더 보편화됨에 따라 이에 대해 환경을 관리하기 위해 사용되는 도구 자체가 사용되고 있습니다. PowerShell 또는 SSH를 사용할 수 없는 경우 복구에 어떤 영향을 줍니까?

CIO는 단독으로 행동할 때 대응 단계의 격리, 조사 및 근절 단계에 걸리는 시간과 관계없이 디스크, 파이프 및 복구 소프트웨어의 속도에 대한 단순한 요인인 복구 시간 목표(RTO)를 약속할 수 있습니다. 사고가 발생하한 후에야 조직은 예상치 못한 대응 기간을 추가해야 하는지, 추가하지 않고 계속 진행하며 복구를 여러번 반복해야 하는지, 그리고 그 때마다 RTO 기간이 추가된다는 혹독한 교훈을 배웁니다. 그렇지 않으면 거의 즉시 재감염됩니다. CIO와 CISO는 이사회 및 고위 경영진과 협력하여 대응과 복구가 모두 이루어질 수 있도록 달성 가능한 RTO에 대해 현실적인 기대치를 설정해야 합니다.

보안 통제를 이용할 수 없을 수도 있습니다

CISO는 데이터 도난 시나리오를 중심으로 많은 역량을 구축했을 수 있습니다. 해당 조직은 핵심 IT, 보안, 심지어 공격 후 기능하지 않을 수도 있는 시설 기능 구축의 가용성에 대해 가정했을 수 있습니다. 실제 사례 중 하나에서는 출입 통제 시스템을 삭제하여 대응을 시작하는 데 필요한 건물과 방에 대한 물리적 접근을 막았습니다. 또한, 음성 및 IP 및 이메일 시스템도 영향을 받아 보험사, 비즈니스 파트너, 규제 기관, 법 집행 기관 및 언론과의 소통이 불가능했습니다. (언론은 LinkedIn을 사용하여 조직의 직원에게 연락하여 무슨 일이 일어나고 있는지 확인해야 했습니다. 직원들은 스스로 아무와도 소통할 수 없었기 때문에 무슨 일이 일어나고 있는지 모르고 있다는 것을 알게 되었습니다. 이후 부정적인 언론 보도가 이어졌습니다.)

BC/DR 우선 순위는 보안과는 별도로 사업부와 협력하는 IT 운영팀에서 도출한 것이기 때문에 중요한 비즈니스 애플리케이션에 먼저 초점을 맞추는 경우가 많습니다. 그러나 IT 및 보안 운영 부서가 내부 및 외부 이해관계자와 협력하여 사고를 관리할 수 있도록 신뢰할 수 있는 최소 실행 가능한 대응 기능(MiViRC)을 복구하는 것이 중요합니다.

파괴적인 사이버 공격 후에는 보안 통제가 작동하지 않을 수 있습니다

SANS Institute의 6단계 사고 대응 라이프사이클 또는 **NIST SP800-61r2 컴퓨터 보안 사고 처리 가이드** 거의 모든 사이버 사고 대응 프레임워크에서 랜섬웨어 및 와이퍼와 같은 공격의 확산을 방지하는 데 격리 단계가 중요합니다. 문제는 조사, 근절 및 복구를 위한 엔드포인트에 대한 접근에 의존하게 되었다는 것입니다. 원격 포렌식 이미징과 엔드포인트 보안 제어**(엔드포인트 탐지 및 대응(EDR)** 및 **확장된 탐지 및 대응(XDR) 등)**는 오늘날의 안보 무기 체계에서 흔히 볼 수 있습니다.

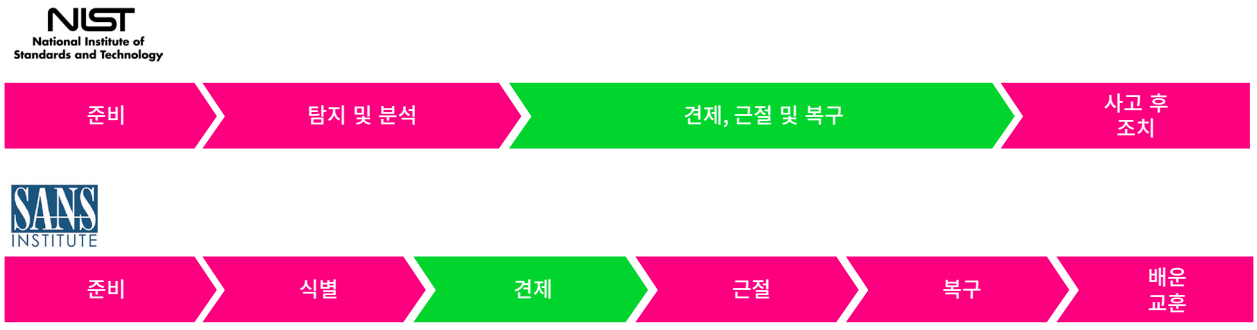

그림 2: 격리는 사고 대응 모범 사례의 일부이지만 보안 도구를 방해할 수 있음

보안 통제를 신뢰할 수 없을 수도 있습니다

사이버 공격에서 공격자의 행동을 분석하기 위한 사실상의 표준인 MITRE ATT&CK 프레임워크에는 공격자가 취하는 엔드투엔드 단계를 설명하는 14가지 전술이 있습니다. "방어 회피" 전술은 공격자가 보안 통제를 우회할 수 있는 방법을 설명합니다. ***이 특정 전술에는 다른 어떤 전술보다 많은 42 가지 기술이 있습니다.*** 백업을 보호하지 않고 엔드포인트에 있는 탐지 보안 제어에 전적으로 의존하는 것은 손상될 위험이 있습니다. 이는 결국 조직을 지속적인 랜섬웨어 및 와이퍼 공격에 가두고 복구할 수 없게 만들 수 있습니다.

요약하면, 백업 자체가 표적이 되지 않은 경우, 많은 조직에서 CIO 팀이 파괴적인 사이버 공격에 대응하여 기존의 BC/DR 프로세스와 기술을 사용하도록 할 계획입니다. CIO의 팀은 CISO 팀이 사고를 조사하고 필요한 시정 조치 또는 재감염 위험을 확립할 때까지 복구를 진행할 수 없습니다. 동시에 CISO의 팀은 이러한 공격이 대응 기능을 수행하는 능력에 미치는 영향을 고려하지 않았을 수 있으며, CIO의 팀이 대응 능력을 복구하는 데 의존할 수 있습니다.

그림 3: 방어 회피는 모든 14가지 전술 중 가장 많은 수의 ATTᴂCK 기술 보유

사이버 보안에서 사이버 레질리언스로 전환

이러한 유형의 사고를 매일 처리하는 거의 모든 사고 대응 회사는 파괴적인 사이버 공격에서 달성 가능한 RTO를 최소화하는 핵심이 격리된 대응 및 복구 환경을 구축하는 것임을 알고 있습니다. 이러한 조직은 이러한 환경을 구축하기 위해 사고 후 혼란에 처한 고객과 협력해야 하지만, 성공적인 재공격 가능성을 최소화하면서 시스템을 다시 가동하는 핵심입니다.

기존 BC/DR 시나리오를 수용한 배경을 바탕으로 일부 데이터 관리 공급업체는 IT 운영팀의 복구 요구 사항에만 초점을 맞춘 격리된 환경을 제공하여 사이버 레질리언스를 제공하는 데 필요한 대응과 복구 간의 본질적인 관계를 잊고 있습니다.

사고의 근본 원인을 처리하지 않으면 재공격 후 반복적인 복구를 수행해야 하기 때문에 시스템을 다시 프로덕션으로 가져오는 데 상당한 지연이 발생할 수 있습니다. 이렇게 반복적으로 복구를 시도하면, 각각 기업에 약속한 RTO를 초과하여 기업이 복구 계획을 수립할 때 허용 가능한 것으로 간주한 것 이상으로 가동 중단 기간이 오래 유지됩니다.

Cohesity는 보안 운영팀의 대응 요구 사항이 영향을 줄이는 데 있어 IT 운영팀의 복구 요구 사항만큼 중요하다는 견해를 가지고 있습니다. 공격의 성격을 이해하지 못하고 시스템을 복구하기 위해 서두르는 접근 방식은 공격 표면이나 아티팩트를 제거하지 못합니다. 지속적인 공격은 복구된 시스템을 몇 분 내에 재감염시킵니다. 랜섬웨어 갱단은 "더블 탭" 공격의 사용을 늘리고 있습니다. 이는 이전에 공격했던 조직이 랜섬 지불을 거부한 경우, 해당 조직을 다시 공격하는 방식입니다. 이러한 공격자는 해당 취약점이 폐쇄되지 않은 경우 처음 액세스 권한을 얻는 데 사용한 것과 동일한 취약성을 활용합니다.

Cohesity는 대응 및 복구 기능 모두의 효과성과 효율성을 개선하기 위해 두 팀에서 모두 사용할 수 있는 기능을 갖춘 단일 플랫폼을 구축했습니다.

클린룸 진입

클린룸에 대한 정의는 많지만, Cohesity에서는 클린룸을 보안 운영팀이 공격이 어떻게 발생했는지 이해하기 위해 필요한 조사 단계를 수행할 수 있는 격리된 환경으로 정의합니다. 사고의 타임라인을 구축하면 복구 단계에서 취해야 할 시정 조치의 초안을 작성하여 위협을 근절하고 재발을 방지하는 데 도움이 될 수 있습니다.

클린룸은 일반적으로 보안 운영팀이 소유합니다. 이 조사 단계에서는 시스템이 복구되지 않습니다. 이들은 격리되어 조사를 받고 있으므로 상호 의존성은 대체로 관련이 없습니다. 격리는 알려진 우수한 보안 도구를 사용하여 방어 회피(앞에서 논함)를 방지하고, 공격자가 대응 조치를 관찰하거나 방해할 수 없으며, 이미 복구된 시스템이 클린룸 내부의 시스템에 재감염될 위험이 없도록 합니다.

클린룸은 Cohesity가 몇 분 안에 설정할 수 있는 최소 실행 가능한 대응 기능(MiViRC)의 일부이며 이에 의존합니다. 신뢰할 수 있고 잘 알려진 우수한 인프라를 구축하면 대응 및 복구 프로세스의 협업, 커뮤니케이션 및 기타 워크플로우를 지원합니다. 격리된 환경에서 사용되는 알려진 양호한 상태로 보안 운영 도구를 복원하면 공격자가 사용하는 많은 회피 기술을 우회하는 데 도움이 됩니다.

Cohesity는 또한 클린룸에서 보안 운영팀의 요구를 지원하기 위한 다양한 기본 기능을 제공합니다. **Cohesity DataHawk**의 위협 헌팅 기능 덕분에 사고 대응자는 MITRE ATT&CK 프레임워크 전반에서 랜섬웨어 운영자가 사용하는 170,000개 이상의 침해 지표(IoC)를 선별하여 제공합니다. 이를 통해 조직은 공격의 전체 수명 주기에 걸쳐 공격자가 사용하는 기술을 이해할 수 있습니다.

선별된 피드는 고객의 자체 위협 인텔리전스 피드 또는 제3자가 제공하는 피드를 통해 보강할 수 있습니다. 포렌식 단계에서 고객의 보안 운영팀이 시스템에서 발견한 아티팩트는 Cohesity로 다시 전달되어 영향을 받은 추가 시스템을 찾을 수 있습니다. 그런 다음 이러한 시스템을 조사 범위로 가져올 수 있습니다.

Cohesity를 통한 위협 헌팅은 엔드포인트 에이전트에 의존하지 않기 때문에 XDR 및 EDR 시스템에 사용되는 방어 회피 기술에 취약하지 않습니다. 또한 완전히 수동적이기 때문에 공격자가 탐지하거나 방해할 수 없습니다. Cohesity를 통한 위협 헌팅은 백업을 통해 지원되므로, 조직이 격리를 위해 호스트와 네트워크를 격리한 경우에도 계속 작동합니다. 또한 많은 조직에서 백업의 보존 기간은 보안 솔루션이 일반적으로 보유하는 로그보다 더 깁니다. 이를 통해 조직은 체류 시간이 길어진 사전 배치 와이퍼 공격과 같이 저속 공격을 수행하는 국가 공격자의 활동을 감지할 수 있습니다.

전통적인 디지털 포렌식에서 조사관들은 사건 발생 후 촬영한 단일 포렌식 이미지에 의존하여 시스템이 특정 최종 상태에 어떻게 도착했는지에 대한 가설을 수립해야 했습니다. **Cohesity DataProtect**를 사용하면 이제 포렌식 조사관이 전체 사건의 타임라인을 자유롭게 시간 경과에 따라 몇 초 만에 파일 시스템 상태의 이미지를 로드할 수 있습니다. 오늘날의 조사관은 도구를 사용하여 파일 시스템을 비교하여 구성 변경 사항을 신속하게 식별하고 지속성 메커니즘 및 악성 계정을 찾을 수 있습니다. 또는 샌드박스에서 폭발을 위한 바이너리를 추출하여 DataHawk의 위협 헌팅 기능에 공급할 수 있는 더 많은 IoC를 생성할 수 있습니다.

많은 조직이 정형 데이터 저장소(예: 데이터베이스)에 보관된 데이터의 규제 영향을 잘 처리할 수 있지만, 대부분은 규제 대상 데이터 및 기타 민감한 데이터를 포함하는 수많은

비정형 데이터를 보유하고 있습니다. 이 데이터는 조직 전체에 널리 퍼져 있기 때문에 이해하기가 매우 어렵습니다. 파괴적인 사이버 공격이 발생할 경우 암호화되거나 삭제되었을 가능성이 높습니다. Cohesity DataHawk의 데이터 분류 기능은 고급 AI/ML 기반 탐지를 사용하여 백업에서 직접 규제 대상 데이터의 분산을 찾아 분류합니다. 이를 통해 기밀 데이터가 손상된 규제 기관 및 데이터 주체에게 알리는 규제 요구 사항의 준수가 용이해집니다.

Cohesity는 보안 운영팀이 사용하는 기존 도구에 조직 데이터의 맥락을 제공하기 위해 **Data Security Alliance** 설립했습니다. 클라우드, 컨테이너 및 하이퍼바이저 시대에는 인프라를 몇 초 만에 인스턴스화할 수 있어 쉽게 교체할 수 없는 데이터입니다. 또한 이러한 데이터는 준수 규정이 있는 데이터이기도 하며, 공격자가 궁극적으로 도용, 암호화 또는 삭제를 목표로 하는 데이터이기도 합니다. Palo Alto Networks, Cisco, CrowdStrike, ServiceNow, Tenable, Qualys, BigID, Okta, Securonix, CyberArk 및 Zscaler와 같은 주요 보안 공급업체와 Mandiant 및 TCS와 같은 보안 관련 전문 서비스를 제공한 경험이 있는 조직과의 관계를 구축합니다. Cohesity는 데이터 컨텍스트를 활용하여 사이버 대응 및 복구의 혁신을 주도하는 최첨단에 있으며, 조직이 기존 사이버 보안 지출에서 더 많은 가치를 얻을 수 있도록 지원합니다.

스테이징의 중요성

스테이징 룸은 일반적으로 IT 운영 부서가 소유하는 복구 환경으로, 알려진 좋은 소스에서 시스템을 신속하게 재구성하거나 복구 및 정리합니다. 보안 운영팀이 정의한 위협 완화 단계를 수행하는 곳입니다. 또한, 복구 및 완화 단계에서 프로덕션에 문제가 다시 발생하지 않았는지 확인하기 위해 복구되는 기능적 역량을 테스트하기 전에 개별 호스트 간의 상호 종속성을 충족하는 경우도 있습니다. 그런 다음 완화된 시스템이 마지막으로 한 번 백업되어, 문제가 발생할 경우를 대비하여 기준선을 제공하므로 대응 조치를 출발점에서 시작할 필요가 없습니다.

Cohesity SmartFiles는 알려진 우수한 설치 미디어를 위변조 불가 저장소에 저장할 수 있는 기능을 제공하여 공격자의 손이 닿지 않는 곳에 보관하도록 지원합니다. 그런 다음 Windows 및 Linux 시스템에 빠르게 마운트할 수 있으므로 IT 오케스트레이션 또는 스크립팅 도구를 사용하여 시스템을 다시 구축할 수 있습니다. Cohesity DataProtect로 시스템의 황금 마스터 사본을 백업하고 복제할 수 있으며, 보안 운영팀의 조사 결과에 따라 타임라인 전체의 스냅샷에서 구성 및 데이터를 복원할 수 있습니다.

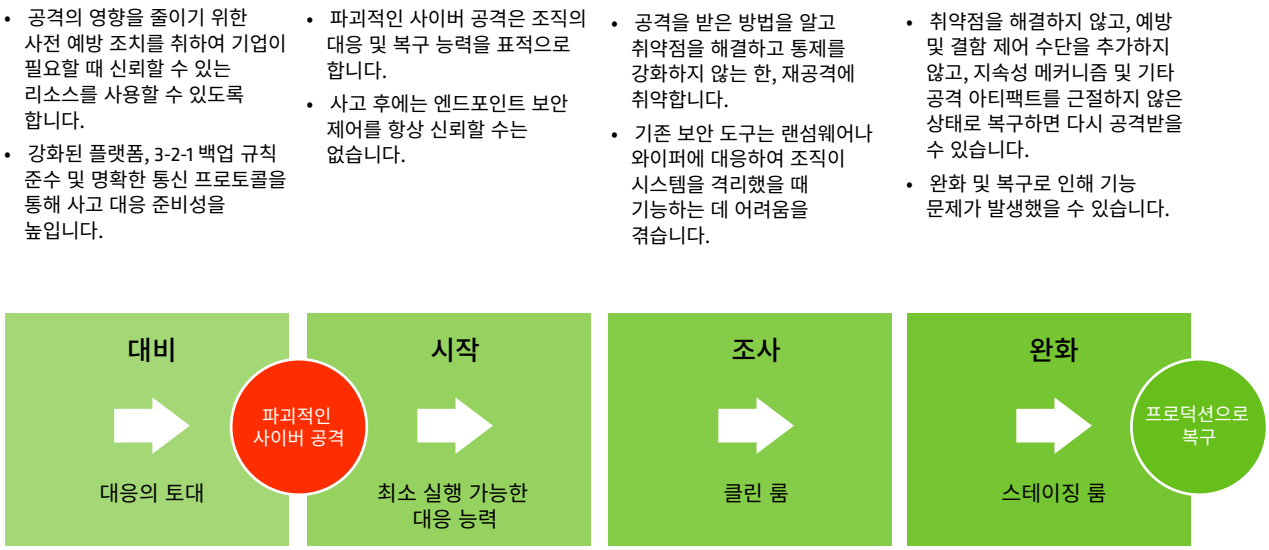

그림 4: 공격에서 복구로의 진행 상황을 보여주는 사건 타임라인

IT와 보안을 통합하여 사이버 레질리언스 제공

보안 운영팀이 사용하는 대응 워크플로우, 팀, 기술과 IT 운영팀이 사용하는 복구 워크플로우, 팀, 기술을 통합하는 것은 사이버 레질리언스를 강화하는 데 중요합니다. 이러한 기능에 개별적으로 근시적으로 집중하면 사이버 사건이 발생할 때만 영향이 증가합니다.

Cohesity는 두 팀 모두에 단일 플랫폼을 제공하는 기존 보안 도구와 통합하는 동시에 보안 운영팀의 대응 작업을 가속화합니다. 이를 통해 대응과 복구의 효율성과 효과를 개선하고 레질리언스를 강화하며 영향을 줄일 수 있습니다.

사고 대응을 위해 클린룸을 사용하는 방법

많은 조직에서는 사고를 신속하게 조사하고 데이터를 복원할 때 시스템을 재감염시키지 않는 적절한 환경이 부족합니다.

주문형 웨비나를 시청하여 추가적인 위험을 초래하지 않고 조직의 준비 및 대응 역량을 강화하는 사고 대응 전략을 수립하는 방법에 대한 실질적인 세부 정보를 확인하십시오.

웨비나 시청

Cohesity의 파괴적 사이버 공격 레질리언스 성숙도 모델 소개

이 백서에서는 사이버 레질리언스를 개선하기 위해 몇 가지 입증된 개념에 대해 논의합니다. 다음 논리적 단계는 회복력 역량을 평가하고 개선할 수 있는 방법(및 위치)을 이해하는 것입니다.

이를 위해 **Cohesity 파괴적인 사이버 공격 복원 성숙도 모델**을 제시합니다.

이 성숙도 모델은 조직이 랜섬웨어 및 와이퍼 공격과 같은 파괴적인 사이버 공격에 대한 레질리언스를 개발할 수 있도록 설계되었습니다. 이 모델은 명확한 벤치마크를 설정하고 조직이 사이버 공격에 탄력적인 효과적이고 효율적인 운영을 달성하도록 지침을 제공하는 체계적인 로드맵을 제공합니다.

Cohesity 모델은 SANS Institute의 6단계 사고 대응 프로세스, RE&CT 프레임워크, MITRE D3FEND, 및 NIST SP800-61 컴퓨터 보안 사고 처리 가이드와 같은 가장 일반적인 사이버 보안 대응 및 복구 프레임워크와 일치하므로 조직이 업계 전반의 모범 사례를 채택할 수 있도록 합니다.

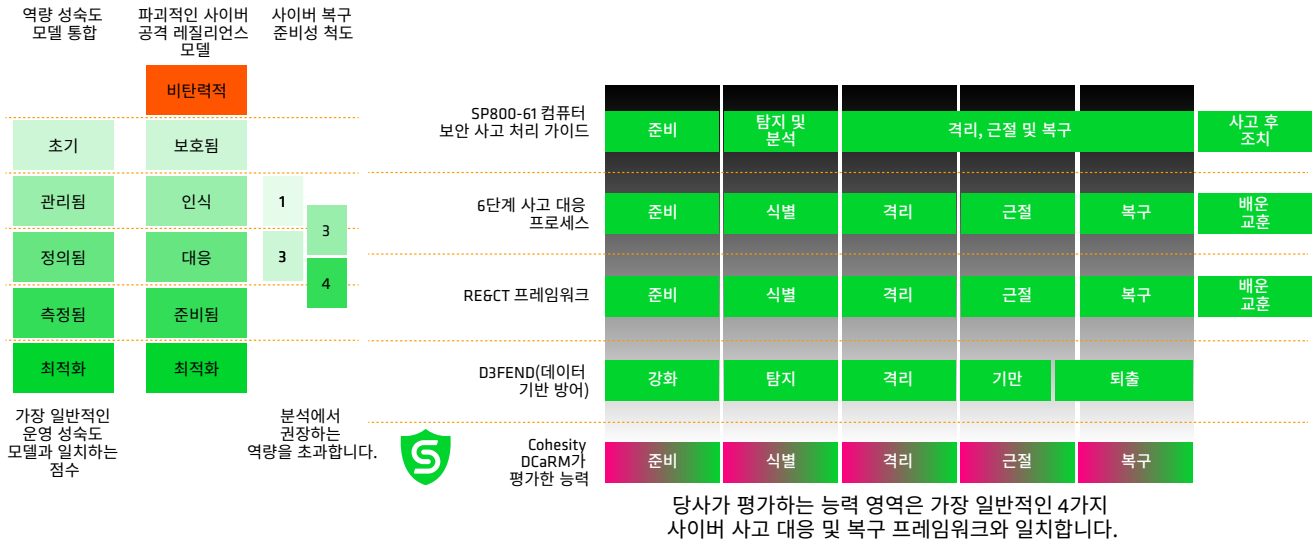

그림 5: Cohesity 파괴적 사이버 공격 레질리언스 성숙도 모델과 일반적인 대응 및 복구 프레임워크의 지표적인 정렬

성숙도 모델을 통해 조직은 사이버 레질리언스를 달성하는 데 필요한 5단계에 걸쳐 운영 역량을 평가할 수 있습니다.

1. 사건 준비
2. 공격 식별 및 조사
3. 공격의 확산 억제
4. 위협 근절 및 공격 표면 축소로 향후 공격 방지
5. 시스템을 안전한 상태로 복구

모델의 성숙도 수준은 아래 표에 나와 있습니다.

성숙도 수준	설명
비탄력적	조직은 제품 및 서비스 제공에 큰 영향을 미치지 않으면서 파괴적인 사이버 공격을 견딜 수 있는 레질리언스가 부족합니다.
복구 가능	조직은 재해 복구 및 비즈니스 연속성 역량을 구축했지만, 이는 공격자의 공격을 받을 수 있으며 재감염 또는 재공격을 방지하기 위한 적절한 조사 및 복구 단계가 부족할 수 있습니다.
강화	조직은 공격자의 공격으로부터 복구할 수 있는 능력을 보호했습니다.
인식	조직은 회피할 수 없고 침해 사고 대응의 억제 단계에 영향을 받지 않는 파괴적인 사이버 공격의 초기 단계를 탐지할 수 있습니다. 또한 사고를 처리하기 위해 IT와 보안 운영 부서 간의 공동 책임 모델도 개발되었습니다.
대응	조직은 사고 대응 및 이해관계자와의 소통을 신뢰할 수 있는 상태로 이끄는 데 필요한 도구를 복구할 수 있으며, 사고 조사, 위협 근절 및 프로덕션으로 복구하기 전에 시스템 테스트를 허용하는 격리된 환경을 갖추고 있습니다. 조직은 다양한 공격 상황에 대한 엔드투엔드 공격 훈련을 수행하고, 사고 대응자의 근육 기억을 구축하여 향후 상황을 처리하고, 프로세스를 최적화하고, 효과성과 효율성을 높이기 위한 자동화 기회를 모색함으로써 지속적인 개선을 추진합니다. 조직은 공격의 영향을 받는 경우 사건을 관리하고 대응하는 데 필요한 인프라와 리소스를 신속하게 복구할 수 있습니다.
최적화	조직은 프로세스, 인력, 기술을 지속적으로 최적화하기 위한 지표와 원격 측정법을 보유하고 있습니다. 데이터의 선제적 발견 및 분류를 통해 엔드투엔드 거버넌스 및 규제 준수를 보장합니다. 시스템을 복구할 뿐만 아니라 인프라를 신뢰할 수 있는 상태로 신속하게 재구성할 수 있는 역량이 있습니다. 사고 조사, 인프라 재구축 및 데이터 복구가 최적화되어 이러한 작업을 병렬로 수행할 수 있습니다.

그림 6: Cohesity 파괴적 사이버 공격 레질리언스 성숙도 모델의 각 성숙도 수준에 대한 주요 기여 역량의 스냅샷

Cohesity 파괴적 사이버 공격 레질리언스 성숙도 모델은 공급업체에 구애받지 않는 로드맵을 제공합니다. 이 접근 방식을 통해 사용자는 모범 사례 대응 및 복구 프레임워크를 준수하는 동시에 사이버 레질리언스를 달성하고 적절한 거버넌스, 인력 및 프로세스를 개발할 수 있습니다. 로드맵은 기술이 운영 성과를 주도하지 않고 지원하고 최적화하도록 보장합니다.

성숙도 수준을 더 자세히 살펴보겠습니다.

- **복구 가능**: 이 수준에 도달한 조직은 재해 복구 및 비즈니스 연속성이 성숙한 수준이라고 할 수 있습니다. 이들은 중요한 서비스와 이를 지원하는 인프라를 식별하기 위해 적절한 사업 영향 평가를 수행했으며, 복구 시점 및 시간 목표(RPO/RTO)를 생성했습니다. 이 조직은 공격자의 공격으로부터 보호하기 위해 데이터 관리 플랫폼에 필요한 보호 기능이 부족할 것입니다. 또한 사이버 공격의 복잡한 요소를 고려하지 않고 파괴적인 사이버 사고를 전통적인 재해 복구 및 비즈니스 연속성 시나리오로 취급합니다. 이 수준에서는 사이버 사고를 처리하기 위해 IT와 보안 운영 부서 간의 긴밀한 업무 협력 관계가 부족합니다.
- **강화**: 이 수준에서 조직은 공격자의 공격을 받을 것임을 인식하고 이러한 불가피성의 영향을 완화하기 위한 보호 조치를 마련했습니다. 최소 권한 액세스, 불변성(백업의 악의적인 변경 또는 삭제 방지), 업무 분리(악의적이거나 손상된 관리자가 피해를 입히는 변경을 방지), 볼팅(적의 손이 닿지 않는 곳에서 복구할 수 있는 기능 제공)과 같은 보안 원칙을 구현했습니다. 볼팅은 또한 조직이 3-2-1 원칙과 같은 보안 백업 규칙을 준수하는 데 도움이 됩니다.
- **인식**: 이 수준의 조직은 IT와 보안 운영 간에 잘 정의된 공동 책임 모델을 채택했습니다. 공격자가 엔드포인트 보안 시스템을 회피하더라도 위협을 탐지하고 디지털 포렌식을 수행할 수 있습니다. 또한, 조직은 호스트와 네트워크가 격리되는 동안에도 위협 헌팅을 계속할 수 있습니다. 위협 피드가 사용되지만 종종 오래된 경우가 많으며, 서비스형 랜섬웨어 플랫폼 및 취약점에서 확인된 최신 위협을 반영하기 위한 정기적인 업데이트가 포함되어 있지 않습니다. 또한 조직에는 시스템에 영향을 미치기 전에 공격의 초기 단계를 찾기 위한 심층 방어 모델도 부족합니다.

- **대응**: 이 수준에서는 조직이 동일한 공격자의 재공격 또는 재감염을 방지하기 위해 시스템이 프로덕션으로 복구되기 전에 필요한 사건 조사 및 위협 복구 조치를 취합니다. 격리 요건을 충족하기 위해 격리된 조사 및 복구 환경이 마련되어 있습니다. 또한 이러한 수준의 성숙도는 지속적인 개선과 실천을 가져와 사고에 대응하고 안전하게 복구하는 데 필요한 프로세스, 인력 및 기술을 미리 준비합니다. (SOC 분석가, 사고 대응자 및 고위 경영진이 랜섬웨어 또는 와이퍼 공격을 처음 경험할 때 데이터가 랜섬웨어에 감염되거나 회사의 모든 시스템이 삭제되는 것을 원하지 않을 것입니다. 탁상 연습은 유용하지만 실제 상황에서 필요한 엔드투엔드 워크플로우, 역량 및 기술을 테스트하지는 않습니다.)

또한 조직에서는 사이버 레질리언스에 필요한 모든 구성 요소를 준비하는 현실적인 공격 시나리오를 수행합니다. 두 개의 사고가 똑같은 경우는 없습니다. 훈련의 다양한 측면을 통해 조직은 프로세스를 최적화할 수 있습니다. 조직은 정기적으로 자동화 기회를 찾고 직원의 근육 기억을 구축합니다.

마지막으로, 이 단계에 있는 조직은 네트워크 및 보안 도구에 대한 신뢰를 신속하게 재설정할 수 있으며, 몇 분 안에 다른 리소스를 확보하여 대응 활동을 시작할 수 있습니다. 이들은 최악의 상황에서 공격을 조정하고, 소통 및 조사할 수 있는 신뢰할 수 있는 방법을 가지고 있습니다. 즉, 보안 통제가 회피되고, 출입문 접근 시스템이 중단되고, 법 집행 기관, 사이버 보험사, 언론, 규제 기관 또는 영향을 받는 데이터 주체와 이야기할 CMDB, 티켓팅 시스템, 이메일 또는 VoIP 음성이 없는 상황에 대비합니다.

- **최적화**: 이 수준은 사이버 레질리언스의 정점을 나타냅니다. 해당 조직은 조직에서 사용하는 데이터를 복구할 수 있을 뿐만 아니라 데이터 수명 주기 전반에 걸쳐 적절한 위험 관리 단계를 수행했음을 발견하고 분류하기 위해 사전 조치를 취했습니다. 워크플로우는 규정 및 영향을 받는 데이터 주체 통지 요건에 맞게 최적화되어 있으므로 벌금이 발생하지 않으며, 조직은 해당되는 경우 DORA, NIS 2, HIPAA, Prudential 규제 당국, 증권 거래 위원회를 준수할 수 있습니다. 대응형 성숙도 수준에서는 워크플로우의 자동화 기회를 모색하지만, 최적화 수준에서는 엔드투엔드 사건 대응 및 복구 프로세스 전체의 전반적인 거버넌스, 오케스트레이션 및 관리를 모색합니다. 이러한 성숙도 수준은 고위 경영진, 이사회 및 이해관계자 제3자에게 해당 조직이 사이버 레질리언스의 최전선에 있다는 확신을 줍니다.

사이버 공격에 대비하고 대처하기 위해서는 이와 같은 모델이 매우 중요합니다. 이러한 공격은 오늘날 조직이 제품과 서비스를 제공하는 데 가장 큰 위협이 됩니다. 사이버 사고 대응 및 복구 분야에서 수십 년의 경험을 가진 Cohesity 사이버 보안 전문가와 실무자가 이 모델을 설계했습니다. 이를 통해 귀사와 같은 조직이 귀사의 현재 역량을 이해하고, 업계 또는 지리적 지역의 동종 업체와 비교하여 귀사의 성숙도를 벤치마킹하며, 시간이 지남에 따라 향후 개선 및 측정할 수 있는 로드맵을 마련할 수 있도록 했습니다.

저자 소개

James Blake는 사이버 사고 대응 분야에서 30년 이상의 운영 경험을 보유하고 있으며, 30개 이상의 Fortune/FTSE 100 대 기업을 위한 엔드투엔드 보안 운영 역량을 구축했습니다. 그는 또한 여러 국가 차원의 와이퍼 공격과 수십 건의 랜섬웨어 공격을 포함한 수백 건의 대규모 사고 직후에 참여해 왔습니다. 그는 Cohesity의 글로벌 사이버 레질리언스 전략 책임자입니다.

Cohesity.com에서 자세히 알아보기

COHESITY

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

2000059-002 KO 4-2025