DELL Technologies

사이버 공격으로부터의 신속한 복구를 위한 전문 지식 및 리소스

운영 중단 없는 사이버 인시던트 대응에 잘 대비되어 있다는 확신을 얻을 수 있음

Dell Incident Recovery Retainer Service

사이버 공격의 위험과 비용은 계속 증가하고 있습니다. 비즈니스 운영 능력을 상실하면 재무 성과, 고객 관계, 규정 준수 및 회사 평판에 피해를 볼 수 있습니다.

공격이 발생할 경우 성공적으로 복구하려면 대응 속도가 가장 중요합니다. 하지만 정상 운영으로 돌아가려는 노력은 대단히 어려울 수 있습니다. 인시던트를 억제하는 것 외에도 지연 시간을 최소화하면서 중요한 애플리케이션을 다시 온라인 상태로 되돌리려면 IT 환경과 방대한 양의 데이터를 복원해야 합니다.

75%
2025년까지 1회 이상의 공격이 발생할 조직의 비율[1]

97%
사이버 이벤트를 경험한 고객에 대한 Dell의 운영 회복 지원 성공률[2]

16일
랜섬웨어 공격을 받은 후 평균 다운타임[3]

많은 IT 팀이 사이버 공격으로부터 복구하는 데 필요한 충분한 역량이나 기술 조합을 갖추고 있지 않습니다. Dell Incident Recovery Retainer Service를 사용하면 업계 인증을 받은 사이버 보안 및 인프라스트럭처 전문가 팀의 지원을 받아 환경을 복원할 수 있습니다. 본 서비스에는 120시간 또는 240시간의 복구 지원이 포함됩니다. 즉, 주문 승인을 기다릴 필요 없이 즉시 Dell의 팀이 복구에 투입됩니다.

복구 준비 상태 평가. 서비스를 시작할 때 조직의 현재 복구 및 복원 전략을 이해하는 것이 중요하다고 생각합니다. Dell의 숙련된 팀이 기존 복구 계획, 네트워크 및 인프라스트럭처, 백업 프로세스 등을 검토합니다. 팀은 인시던트 준비 상태와 복구 태세를 강화하기 위한 로드맵을 제공하는 평가 및 계획 요약 보고서를 준비합니다.

주요 이점

- 인시던트 발생 시:
  - 고도의 기술을 갖춘 숙련된 Dell 사이버 보안 전문가의 신속한 응답을 받습니다.
  - Dell EMC 팀은 고객의 상황을 신속하게 진단하고 비즈니스 중단을 최소화하기 위한 최선의 조치를 결정합니다.
  - 위협이 근절되고 악용된 취약성이 차단됩니다.[4]
- 리테이너 모델은 연간 120시간 또는 240시간의 복구 지원을 제공합니다.
- Dell Technologies 사이버 보안 팀은 각 고객 상황에 다양한 경험, 기술 및 툴을 제공합니다.
- 개선 우선 순위를 안내하는 요약 보고서를 포함하는 기존 복구 역량 및 범위에 대한 초기 복구 준비 상태 평가
- Dell 팀이 초기 평가를 수행하여 고객의 환경을 파악했으므로 복구 프로세스의 효율성이 향상됩니다.

주요 기능

인시던트 복구 활동에 연간 120시간 또는 240시간

- 원격으로 제공(일부 지역에서는 현장 서비스 이용이 가능하며 추가 요금이 부과됨)
- 프로젝트 관리자가 활동을 감독
- 인시던트 및 상황 평가
- 리소스 할당 및 배포
- 포렌식 분석 - 디지털, 멀웨어, 데이터
- 위협 근절
- 데이터 완전 파기, 복구, 보존
- 환경 및 애플리케이션 재설정

인시던트 복구 역량 평가

- 업무 시작 시 수행
- 사이버 보안 인시던트 발생 시 대응을 준비하기 위해 클라이언트 네트워크, 인프라스트럭처 및 시설 검색
- 인시던트 복구 계획, 데이터 백업 및 복원 역량 검토
- Dell은 준비 상태 및 복구 태세 강화를 위한 권장 사항을 포함한 요약 보고서를 준비합니다.

서비스 수준:

- 고객의 초기 요청 후 2시간 이내에 고객과의 서비스 개시 회의를 예약합니다(평균 대응 시간).
- 서비스 개시 회의 후 6시간 이내에 원격 응답이 시작됩니다(평균 응답 시간).
- 현장 응답에 합의한 경우 서비스 개시 회의 후 24시간 이내에 현장 응답이 시작됩니다(평균 응답 시간).

사용된 시간과 남은 시간은 분기마다 고객과 함께 검토됩니다.

- 복구 및 복원 시간이 완전히 사용되지 않은 경우 인시던트 복구 계획, 사이버 보안 개선 및 관련 영역에 대한 전문가 지원에 남은 시간이 적용될 수 있습니다.

충격으로 인한 손상 방지

조직이 심각한 사이버 인시던트의 발생 시기를 정확히 알 수 있는 방법은 없습니다. Dell Incident Recovery Retainer Service로 대비하십시오. 고도의 기술을 갖춘 숙련된 사이버 보안 전문가가 위협을 제거하고 중요한 운영을 재확립하기 위해 노력하며 지체 없이 상황에 투입될 것임을 알고 안심할 수 있습니다.

지금 바로 영업 담당자에게 문의하십시오.

[1] Detect, Protect, Recover: How modern backup applications can protect you from ransomware, Nik Simpson, Gartner, 2021년 1월 6일, Gartner 문서 ID G00733304 https://www.gartner.com/en/documents/3995229

[2] 2019년 6월부터 2021년 7월까지 북미 지역의 서비스 요청에 대한 Dell 분석 기준

[3] Why Ransomware Costs Businesses Much More than Money, Forbes, 2021년 4월 30일, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6

[4] 포함된 연간 120시간 또는 240시간 이상의 복구 작업이 필요한 경우 추가 시간을 구매할 수 있습니다.

DELL Technologies