사이버 공격으로부터 복구

인시던트 발생 후 효과적이고 효율적으로 운영을 복원합니다.

포괄적인 보안 복구 전략의 절차

공격의 영향 완화 → 손상된 서비스 및 디바이스 재구축 → 운영 환경 복원 → 인시던트 분석 및 학습

사이버 보안 성숙도 향상을 위한 단계

1. **인시던트 억제**
   영향을 받는 시스템을 네트워크에서 분리하고 침해된 계정을 비활성화하여 추가 피해를 방지합니다.
2. **시스템/디바이스 복원**
   침해된 시스템을 재구축하고, 소프트웨어를 다시 설치하고, 보안 패치 및 업데이트를 적용합니다.
3. **데이터 복구**
   백업에서 데이터를 복원하거나 전문적인 데이터 복구 기법을 사용하여 손실 또는 암호화된 파일을 가져옵니다.
4. **포렌식 분석**
   공격 메커니즘과 악용된 취약성을 조사하여 향후 인시던트를 방지합니다.
5. **인시던트 대응 평가**
   복구를 마친 후 프로세스를 평가하여 개선할 부분을 파악합니다.
6. **AI/ML 활용**
   영향을 받은 시스템과 데이터를 신속하게 식별하고 백업에서 복원 프로세스를 자동화하여 복구 속도를 높입니다.

사이버 복구에는 팀 전체의 노력이 필요합니다.

전문 서비스 및 파트너십
사이버 보안 파트너가 귀중한 전문 지식과 리소스를 제공합니다.

- 포렌식 분석
- 침해 원인 파악
- 향후 인시던트를 방지하기 위한 조치

포괄적인 사이버 보안 전략을 구현하는 방법에 대해 자세히 알아보세요.

eBook 보기 →

DELL Technologies