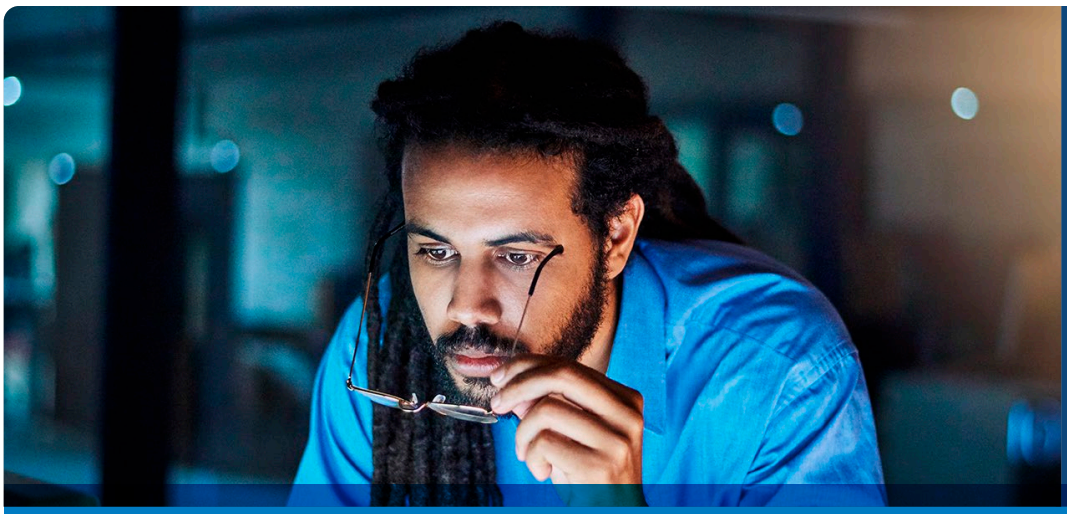
보안 제어 수단 및 정책을 검증하여 공격 벡터 차단



초기 액세스, 악의적인 파일 실행, 데이터 도난 등에 대한 공격자 기법 시뮬레이션

침투 테스트 및 공격 시뮬레이션 관리

전체 킬 체인 전반에서 보안 제어 수단 및 정책을 검증하는 Dell

조직은 엔드포인트부터 웹 및 이메일 게이트웨이에 이르기까지 수백 가지의 보안 제어 수단을 보유하고 있습니다. 제어 수단은 종종 복잡하고 관리하기 어려우며 잘못 구성하면 위험한 노출이 발생할 수 있습니다. 위협 행위자는 손상되거나 오래된 제어 수단을 악용하려고 합니다.

보안 제어 수단의 효과를 시험하고 검증하기 위해 Dell 침투 테스트 및 공격 시뮬레이션 관리는 실제 위협 행위를 면밀히 모방합니다.

이 서비스는 다음 항목을 결합합니다.

- 제어 수단이 제대로 작동하는지 확인하기 위한 월별 자동 BAS(Breach and Attack Simulation)
- 숙련된 전문가가 중요한 자산 및 데이터에 대한 방어 침해를 시도하는 연간 침투 테스트

공격 시뮬레이션 테스트 보안 제어 수단

Dell 보안 전문가는 고급 BAS 기술을 사용하여 엔드포인트에 멀웨어를 퍼뜨리려 하거나 웹 서버에서 무단 정보를 가져오려 하는 등 다양한 공격 벡터를 테스트합니다. Dell 테스터는 BAS를 적용하여 최신 공격자 TTP[2]를 포함한 위협에 대한 전체 킬 체인[1] 전반의 공격을 시뮬레이션합니다.

BAS 기술은 운영 환경에 안전하고 최신 위협 정보, 공격 및 동작을 통해 지속적으로 업데이트됩니다.

침투 테스트를 통해 고가치 타겟으로의 경로 평가

공격 시뮬레이션을 시행하더라도 일부 공격자는 환경을 탐색할 수 있는 기술을 가지고 장애물을 회피하여 중요한 데이터에 도달합니다. 바로 이때 침투 테스트가 사용됩니다.

주요 이점:

- 포괄적인 BAS(Breach and Attack Simulation)를 활용하여 악용될 수 있는 잘못 구성된 보안 제어 수단 탐지
- 월별 시뮬레이션으로 최근 새롭게 발생하는 문제 및 격차 설명
- 연간 침투 테스트로 고부가가치 자산 또는 데이터에 대한 고위험도 경로를 면밀히 검사
- 테스트 결과, 분기별 추세 및 주목할 만한 활동을 보고하여 보안 태세 개선 지원
- 임시 테스트를 통해 새로운 고위험도 위협에 대한 빠른 통찰력 획득

침투 테스트는 BAS를 보완하고 개별 제어 수단 또는 제어 수단 세트를 테스트하는 대신 환경으로 진입하는 취약한 경로 또는 고위험도 경로에 중점을 둡니다. Dell 침투 테스터는 고가치 시스템을 캡처하거나 특정 파일 세트를 도용 또는 비활성화하는 등 특정 목표에 도달하기 위한 다양한 위협 행위자 기법과 다양한 페이로드까지 에뮬레이션할 수 있습니다. 실제 공격자와 마찬가지로 숙련된 침투 테스터는 기법을 전환, 피벗 및 조정하여 타겟에 도달할 수 있습니다.

테스트 정보를 적용하여 보안 태세 개선

Dell Technologies Services는 BAS 시퀀스를 실행한 결과에 따라 수정할 보안 제어 문제에 대한 월별 보고를 제공합니다. Dell은 분기별로 다양한 공격 시뮬레이션의 추세를 검토하고 IT 환경에서 관찰되는 주목할 만한 활동을 보고하며 보안 태세 개선을 위한 권장 사항을 논의합니다.

주요 기능

BAS(Breach and Attack Simulation)

- 고객 환경에 따라 매월 자동 BAS(Breach and Attack Simulation) 실행
- 웹 게이트웨이, 이메일 게이트웨이 및 엔드포인트를 포함한 경계 및 내부 인프라스트럭처 구성 요소에 대한 보안 제어 수단 검증
- 최신 위협 정보, 공격 및 동작을 통해 BAS 툴을 지속적으로 업데이트
- 이전 시뮬레이션 및 보안 환경 요인에 따라 시뮬레이션 워크플로 변경
- 위협 인텔리전스 및 Dell의 평가에 따라 새로 검색된 보안 문제에 대한 임시 시뮬레이션 실행

침투 테스트

- 웹 게이트웨이, API, 모바일 디바이스, 외부 IP 주소, 내부 IP 주소, 클라우드 구성의 정의된 하위 집합에 대해 연간 침투 테스트 실행
- 첫 번째 테스트 결과가 결정된 후 침투 테스트를 다시 실행(선택 사항)

보고 및 검토

- 수행된 BAS(Breach and Attack Simulation)에 대한 월별 보고 제공
- 고객의 IT 환경에서 관찰된 추세 및 주목할 만한 활동에 대한 분기별 보고서 및 검토 제공
- 전반적인 보안 태세를 개선하기 위한 권장 사항 제시

온보딩

- 서비스 개시 회의 실시
- 고객이 작성한 업무 개시 전 체크리스트 검토
- 고객 IT 환경 검토
- 고객을 위해 BAS 애플리케이션 활성화
- 에이전트 롤아웃 지원 제공

지금 바로 영업 담당자에게 문의하십시오.

[1]"전체 킬 체인"에는 피싱, 웹 게이트웨이 등의 외부 위협, 손상시키는 엔드포인트, 자격 증명을 얻거나 공격, 데이터 유출 등을 확산하기 위한 내부망 움직임이 포함됩니다.
[2]"TTP" – Tactics, Techniques and Procedures

DELL Technologies