사이버 보안 생존 가이드:

최신 사이버 위협에 대응하는 방법

디지털 세계는 클릭하고 다운로드하고 로그인할 때마다 숨겨진 사이버 트랩이 작동할 수 있는 위험한 황야가 되었습니다.

오늘날의 사이버 환경은 랜섬웨어, DDoS 공격, 피싱 사기, 백업 침투와 같은 위협이 점점 더 고도화되면서 그 어느 때보다 위험해지고 있습니다. 해커들은 이제 AI를 활용하여 기존 방어 체계를 교묘히 무력화하고 있으며, 한때 기회주의적 공격이었던 것을 광범위한 피해를 유발할 수 있는 계산적이고 지속적인 위협으로 변모시키고 있습니다.

Dell 고객들은 해커가 소셜 미디어 데이터를 스크래핑하여 사이버 보안에 가장 정통한 직원마저도 속일 수 있는 설득력 있는 메시지를 작성하는 AI 기반 공격에 대한 우려를 표명했습니다.

이러한 사례들은 공격자가 첨단 기술을 악용하여 전례 없는 정확도로 조직을 조종하고, 속이고, 침투하고 있음을 여실히 보여줍니다.

이 같은 적대적인 환경을 헤쳐나가기 위해 조직에는 최첨단 툴, 사전 예방적 전략, 그리고 경계하는 문화를 결합한 생존 키트인 포괄적인 사이버 보안 전략이 필요합니다. 이 가이드에서는 이러한 전략의 구성 요소를 살펴보고, 조직이 오늘날 가장 시급한

조직 보호를 위한 맵: 제로 트러스트 프레임워크

오늘날의 AI 기반 위협 환경에서 제로 트러스트 프레임워크 도입은 더 이상 선택 사항이 아닙니다. 공격자는 AI를 사용하여 정찰을 자동화하고, 자격 증명을 탈취하고, 공격 기법을 빠르게 적응시켜 기존 방어 체계의 효과를 떨어뜨리고 있습니다. 제로 트러스트는 "침해 가정" 사고방식으로 작동하며, 모든 접근 요청을 지속적으로 검증하고 엄격한 인증 프로세스를 구현하여 위험을 최소화합니다.

제로 트러스트는 사용자, 디바이스 및 애플리케이션을 사전 예방적으로 모니터링하여 무단 액세스 및 데이터 침해 가능성을 줄입니다. 이는 ID 관리에 대한 현대적이고 통합된 접근 방식입니다.

캠프장 안전 유지: 공격 노출 지점 축소

AI 기반 위협으로부터 방어하려면 공격 노출 지점을 줄이는 것이 필수적이며, 공격자는 엔드포인트, API 및 공급망 취약성을 자주 악용합니다. 엔드포인트와 API는 네트워크의 진입점 역할을 하며, 멀웨어를 배포하거나 기밀 데이터를 훔치기 위한 표적이 되는 경우가 많습니다.

이러한 영역을 보호하려면 강력한 인증, 전송 중인 암호화된 데이터, 정기적인 취약성 테스트, EDR(Endpoint Detection and Response) 툴, 패치 관리, 디바이스 강화 등 계층화된 방어 전략이 필요합니다. 엔드포인트 모니터링 솔루션과 지속적인 위협 탐지는 악의적인 활동을 실시간으로 식별하고 차단하는 데 도움이 됩니다.

조직은 소프트웨어 공급망 및 개발 수명주기를 보호하기 위한 사전 예방적인 전략을 채택해야 합니다. 최소 권한 액세스를 적용하면 권한이 부여된 사용자 및 애플리케이션만 중요 시스템과 상호 작용할 수 있으며, 자동화된 위협 탐지 및 대응을 통해 취약성이 발견되면 신속하게 해결할 수 있습니다.

노련한 사이버 위협 추적자 따르기: 사전 예방적인 위협 탐지 및 대응

AI 기반 공격은 취약성을 악용하고, 합법적인 행동을 모방하며, 보안 조치를 우회하기 위해 동적으로 적응하기 때문에 탐지가 어렵습니다. 이러한 정교한 위협에 대처하기 위해 조직에서 사후 대응적 조치만으로는 부족하며, 신속한 대응 기능을 갖춘 지능형 공격 탐지 시스템이 필요합니다. AI와 머신 러닝을 활용하여 보안 팀은 행동 패턴을 분석하고, 이상 징후를 탐지하고, 위협에 실시간으로 대응하여 심각한 피해가 발생하기 전에 문제를 해결할 수 있습니다.

효과적인 탐지 및 대응 시스템은 위험을 발견하고 자동화된 대응을 시작할 수 있도록 방대한 양의 운영 데이터를 수용해야 합니다. 또한 이 위협 인텔리전스는 자체적으로 구축되므로 시스템을 더욱 스마트하게 만들고 새로운 공격 전술을 사전 예방적으로 식별하여 대응할 수 있게 해줍니다.

폭풍 전 대피소 구축 연습: 인시던트 대응 및 복구

공격을 예방하는 것이 첫 번째 단계이지만, 조직은 공격이 불가피한 것처럼 운영해야 합니다. 최소한의 피해로 공격에서 생존하는 것이 목표이며, 효과적인 전략은 다음 두 가지 요소를 포함합니다.

- 확고한 IRR(Incident Response and Recovery) 계획
- 중요 데이터 및 애플리케이션 백업을 중심으로 한 기술적 조치

인시던트 복구 계획은 포괄적이어야 합니다. 강력한 공격은 회사 운영의 대부분, 아니면 전부를 마비시킬 가능성이 높으므로, 계획에는 사이버 인시던트 발생 시 회사의 모든 부서가 어떻게 대처해야 하는지가 포함되어야 합니다. 또한 계획에는 조직이 내외부적으로 어떻게 커뮤니케이션할 것인지, 그리고 미리 작성된 커뮤니케이션 템플릿을 활용할 수 있는 방안도 포함되어야 합니다. 계획은 정기적으로 업데이트하고 유지 관리해야 합니다. 마지막으로, 계획의 효과는 얼마나 자주 실행하는지에 달려 있습니다. 공격이 발생하면 모든 구성원이 본능적으로 대응할 준비가 되어 있어야 합니다.

기술 관점에서 볼 때, 조직은 **MVC(Minimum Viable Company)**의 운영이 어떤 모습인지 결정하는 것부터 시작해야 합니다. 종이와 연필만 가지고 운영을 하더라도 계속 작동해야 하는 시스템은 무엇일까요? 영업은 계속 운영되는 것이 중요할까요? 고객 서비스는 어떨까요?

이러한 결정이 내려지면 이를 중심으로 백업 및 복구 메커니즘을 구축해야 합니다. 알려진 정상 데이터로 복구할 수 있는 역량을 갖추면 조직이 신속하게 운영을 재개할 수 있을 뿐만 아니라, 데이터를 볼모로 잡으려 하는 악의적인 행위자의 영향력을 약화시킬 수 있습니다. 또한, 현대적인 IR 전략은 기존 접근 방식을 넘어 챗봇이나 가상 에이전트와 같은 AI/LLM 시스템을 결제 시스템이나 고객 데이터와 동일한 복구 우선순위를 가진 계층 1 자산으로 취급해야 합니다.

지능형 위협에 대처하기 위해 IR 계획은 자동화와 수동 점검의 균형을 맞춰야 합니다. 전체 시스템 운영 중단 시 조직이 어떻게 기능할지 아는 것이 중요합니다. 펜과 종이로만 업무를 처리해야 한다면 어떻게 될까요?

모두의 참여 필요: 직원 인식 제고

직원들은 마치 황야에서 위험을 헤쳐나가는 생존 팀과 같이 사이버 위협에 맞서는 1차 방어선입니다. 모든 구성원은 위험을 식별하고 리소스를 보호하는 데 중요한 역할을 합니다. 이러한 방어력을 강화하기 위해 조직은 지능형 피싱 및 딥페이크와 같은 AI 기반 위협을 포함하는 공격 시뮬레이션과 같은 강력한 인식 제고 프로그램이 필요합니다.

최고의 프로그램은 지속적인 교육, 개방적인 커뮤니케이션, 실제 시뮬레이션 및 공동 책임 문화를 결합합니다. 일선 직원부터 임원까지 모든 구성원이 기존 위협과 AI 기반 위협을 모두 이해하면 조직은 경계를 늦추지 않고 정보에 정통한 조직이 됩니다. 팀워크와 준비를 강화함으로써 조직은 진화하는 사이버 위험에 미리 대비하고 잠재적 공격에 대한 회복탄력성이 뛰어난 방어 체계를 구축할 수 있습니다.

AI 기반 공격에 대한 회복탄력성을 유지하기 위한 모범 사례

AI 기반 공격에 대한 회복탄력성을 유지하기 위해 조직은 사전 예방적이고 전략적인 접근 방식을 채택해야 합니다**.** 다음은 **10**가지 모범 사례입니다**.**

제로 트러스트 아키텍처

액세스 권한 부여 전에 모든 사용자와 디바이스가 인증을 받도록 지속적인 검증, 엄격한 액세스 제어 및 네트워크 세분화를 요구합니다. 이는 빠르게 움직이는 AI 기반 공격을 차단하고 억제하는 데 도움이 됩니다.

엄격한 취약성 및 패치 관리**:**

OS, 펌웨어, 앱, API 및 타사 소프트웨어에 대한 스캐닝 및 신속한 패치 적용을 자동화합니다.

ID 및 액세스 관리 강화**:**

강력한 인증(MFA, RBAC)을 구축하고 강력한 자격 증명 정책을 시행하여 피싱 및 자격 증명 자동 공격의 성공 가능성을 줄입니다.

AI 기반 위협 탐지 및 모니터링**:**

AI/ML 기반의 동작 및 이상 징후 탐지를 활용하여 미묘하거나 자동화된 위협을 실시간으로 포착합니다.

자동화된 자산 검색 및 인벤토리**:**

클라우드, IoT, 섀도우 IT 등 모든 자산을 지속적으로 검색하고 모니터링하여 숨겨진 노출을 방지합니다.

자동화된 인시던트 대응**:**

자동화된 플레이북을 사용하여 위협을 신속하게 격리, 억제 및 해결하고 공격자 체류 시간을 최소화합니다.

마이크로 세분화 및 네트워크 액세스 제어**:**

네트워크와 워크로드를 세분화하고 격리하여 공격자의 측면 이동을 방지하고 위협을 억제합니다.

정기적인 현실적 시뮬레이션 및 지속적인 개선**:**

모의 연습, 레드 팀 구성 및 피싱 시뮬레이션을 실시하고, 결과에 따라 IR 계획 및 탐지 모델을 업데이트합니다.

엔드포인트 및 **API** 강화**:**

고급 엔드포인트 보호(EDR/XDR)를 활용하고 API 게이트웨이를 보호하십시오. 강력한 인증, 속도 제한, 입력 검증 및 암호화를 지원합니다.

변경 불가능한 에어 갭 백업 및 복구**:**

위변조 방지 백업을 유지하여(에어 갭 처리되고 정기적으로 테스트되면 가장 좋음) 깔끔하고 신속한 복구를 보장합니다.

DELL Technologies

Dell Technologies: 미지의 영역을 탐험하는 고객을 위한 가이드

지능형 사이버 위협으로부터 조직을 보호하려면 진화하는 위험에 미리 대비할 수 있는 적절한 툴과 전문 지식이 필요합니다. 오늘날의 복잡한 사이버 보안 환경에서 데이터, 시스템 및 평판을 보호하기 위한 강력한 전략은 필수적입니다. Dell Technologies는 규모에 관계없이 모든 조직의 요구 사항을 충족하도록 맞춤화된 포괄적인 솔루션 제품군을 제공하여 이러한 문제를 해결합니다.

안전한 공급망, 지능형 공격 탐지 및 엔드포인트 보호부터 안전한 데이터 관리까지 Dell은 최신 사이버 공격으로부터 방어하는 데 필요한 기술을 비즈니스에 제공합니다. 업계를 선도하는 전문성을 바탕으로 Dell 팀은 고객과 긴밀히 협력하여 맞춤형 보안 전략을 개발합니다. 실시간 모니터링, 자동화된 위협 대응, 제로 트러스트 아키텍처와 같은 기능을 통해 Dell은 조직이 사전 예방적이고 회복탄력성이 뛰어난 상태를 유지할 수 있도록 지원합니다.

랜섬웨어, 피싱 공격 또는 규정 준수 등 어떤 작업을 수행하든 Dell Technologies는 오늘날의 위협 환경을 자신 있게 헤쳐나갈 수 있도록 지원합니다. Dell Technologies와 협력하여 비즈니스를 보호하고 디지털 시대에 성공을 거둬, 운영이 안전하고 효율적이며 앞으로 어떤 일이 일어나든 대비할 수 있도록 보장하십시오.

> "공격이 발생하는 동안 시스템에 액세스하지 못할 수 있으므로 인시던트 대응 계획을 종이에 인쇄해 두어야 합니다."
>
> ***Rachel Tyler***
> 사이버 보안 자문 컨설턴트, *Dell Services*

도움이 될 수 있는 Dell 제품 및 솔루션

주요 **Dell** 솔루션	설명
Dell Trusted Infrastructure	혁신을 위한 현대적이고 안전하며 회복탄력성이 뛰어난 기반을 더불어 구축하는 Dell 서버, 네트워킹, 스토리지 및 사이버 회복탄력성 솔루션의 조합입니다.
사이버 회복탄력성	데이터를 보호하고 안전한 복구를 보장하도록 설계된 포괄적인 솔루션 포트폴리오입니다. 어플라이언스, 소프트웨어 및 as-a-Service가 포함됩니다.
사이버 보안 서비스	워크로드 전반에 걸쳐 포괄적인 보안 전략을 개발하고 구현하는 데 도움이 되는 서비스 제품군입니다. 오퍼링에는 자문 서비스, vCISO, Managed Detection and Response, 침투 및 취약성 테스트, 인시던트 대응 및 복구가 포함됩니다.
Dell Trusted Workspace(엔드포인트 보안)	PC를 보호하도록 설계된 기본 제공 기능과 선택 사항인 추가 기능의 조합입니다. 안전한 공급망 관리 방식을 기반으로 구축된 기본 제공 기능으로는 SafeBIOS, SafeID with TPM이 있습니다. 선택 사항인 추가 기능으로는 Secured Component Verification, SafeID with ControlVault, 그리고 작업 공간 보안을 극대화하는 파트너 소프트웨어인 CrowdStrike 및 Absolute가 있습니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.