aws re/start

예방: 시스템 강화

Security Fundamentals

보안 수명 주기: 예방 - 시스템 강화를 시작하겠습니다.

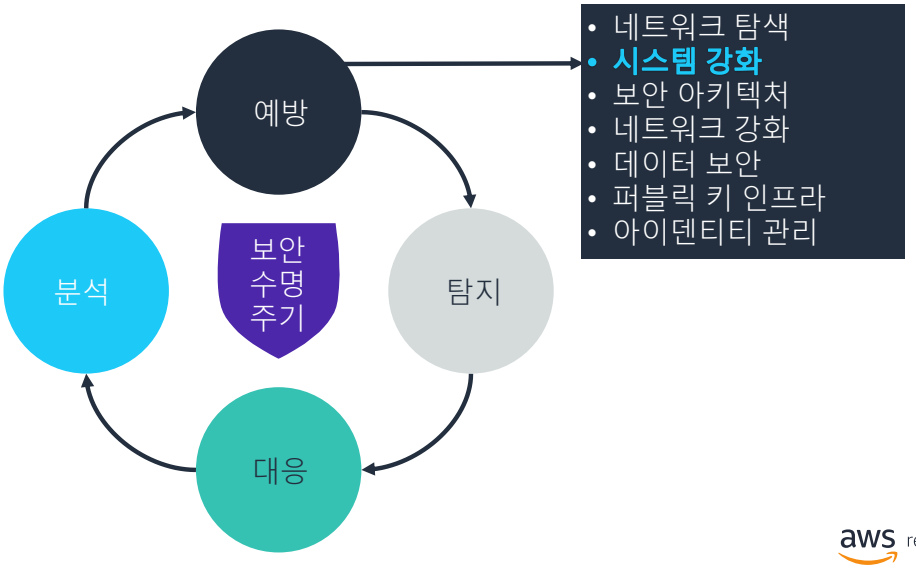
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 시스템 강화의 원칙을 설명하고 이 원칙이 컴퓨터 보안에 어떻게 적용되는지 설명합니다.
- 기준과 그 중요성을 설명합니다.
- 다양한 시스템을 강화하는 방법과 사용되는 기법을 설명합니다.
- 탐지에 사용되는 도구를 알아보고 일반적인 보안 구성 문제를 보여 줍니다.

보안 수명 주기: 예방



aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 위협을 탐지했을 때 어떤 조치를 취할지 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 예방 조치를 구현하면서 수명 주기가 완료됩니다.

이 강의에서는 예방 단계의 일부로 **시스템 강화**의 개념을 배웁니다.

강화란?

- 시스템에서 실행되는 서비스의 수를 줄입니다.
- 시스템 강화를 달성하는 도구를 사용합니다.

보안과 사용성의 균형

aws re/start

공격자가 권한을 확대하거나 루트 사용자 액세스를 얻지 못하도록 취약점을 줄이려면 시스템을 보호해야 합니다. 강화 프로세스에는 시스템에서 실행되는 서비스의 수를 줄이는 것이 포함됩니다. 실행되는 서비스의 수가 적어지면 보안 이벤트의 잠재력도 줄어듭니다.

이 강화와 시스템의 사용성 사이에서 균형을 맞추십시오. 시스템을 보호하려면 기본 구성을 자주 변경해야 합니다. 그러나 시스템을 너무 자주 변경하면 사용성의 심각한 제한 때문에 시스템이 제대로 작동하지 않을 수 있습니다.

강화할 수 있는 시스템의 유형


데스크톱


서버


애플리케이션


스위치


라우터


무선 액세스 포인트


스팸 백신 솔루션


원격 게이트웨이

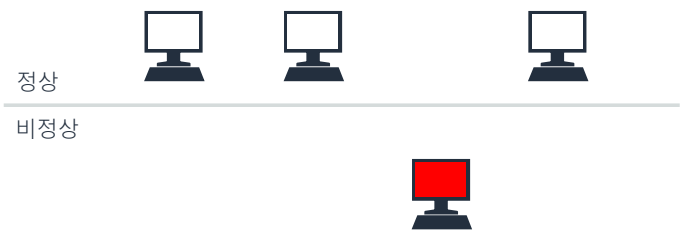

리버스 프록시


휴대폰

보안을 위해 모든 종류의 시스템을 강화할 수 있습니다. 시스템의 예에는 컴퓨터나 서버가 아닌, 자주 간과되는 디바이스가 포함됩니다.

보안 기준

- 기준은 네트워크의 **정상적인** 조건을 정의합니다.
  - **무엇을 어떻게** 보호할지 결정하는 출발점을 제공함
  - 시스템에 적용되는 변경 사항을 반영하도록 업데이트됨
  - 개선 조치를 포함함
  - 시스템에 관해 업데이트된 문서에 의존함



예를 들어, 매장에서 컴퓨터가 진열된 복도를 걸어가는데 컴퓨터 네 대 중 한 대의 화면이 다른 컴퓨터와 다릅니다. 세 대의 화면은 환영 페이지인데, 네 번째 컴퓨터의 화면은 오류 페이지가 떠 있는 것입니다.

여러분은 환영 페이지를 사용하여 정상의 기준을 세울 수 있습니다. 이 기준(환영 페이지)을 세우면 정상이 아닌 것으로 간주되는(오류 페이지) 열외를 결정할 수 있습니다. 마찬가지로, 컴퓨터와 컴퓨터 네트워크에도 비정상을 빠르게 탐지할 수 있도록 정상 작동이 무엇인지 결정합니다.

적은 수의 기준을 세우도록 하면 제대로 강화되지 않은 디바이스 한 개를 탐지하기가 더 쉽습니다. 그러나 기준이 없으면 보안 일탈을 식별할 방법이 없기 때문에 의심스러운 이벤트가 발생했는지 판단할 수 없습니다. 문서화가 가능하고 정확하게 유지 관리했다면 시스템 문서로부터 기준을 도출할 수 있습니다.

시스템 강화 방법

시스템을 강화하는 일반적인 방법

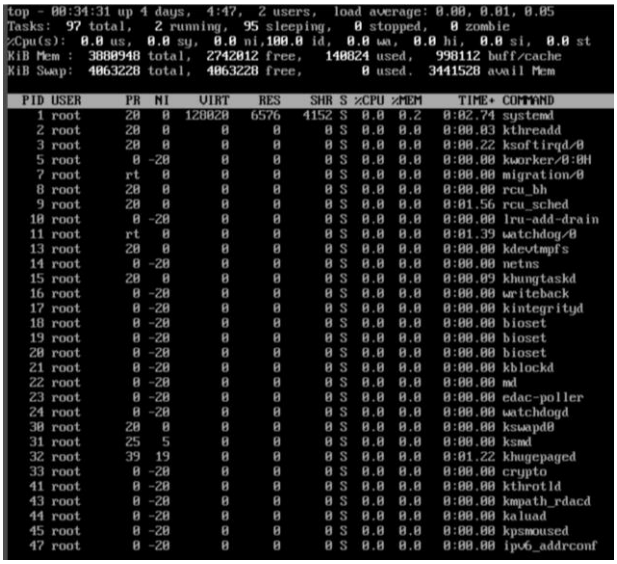
- 불필요한 서비스를 끕니다.
- 그룹 정책으로 컴퓨터 운영을 제어합니다.
- 주기적으로 패치와 업데이트를 적용합니다.

시스템을 강화하는 방법은 다음과 같습니다.

- 사용하지 않는 서비스를 끕니다.
- 기업 정책과 제한을 구현합니다.
- 주기적으로 보안 업데이트와 패치를 적용합니다.

Linux 프로세스

- 시스템이 기본적으로 사전 강화되어 있지 않습니다.
  - 포그라운드 또는 백그라운드에서 프로세스 실행
  - 사용하지 않는 서비스 비활성화 또는 시스템 시작 시 자동으로 시작되지 않도록 예방



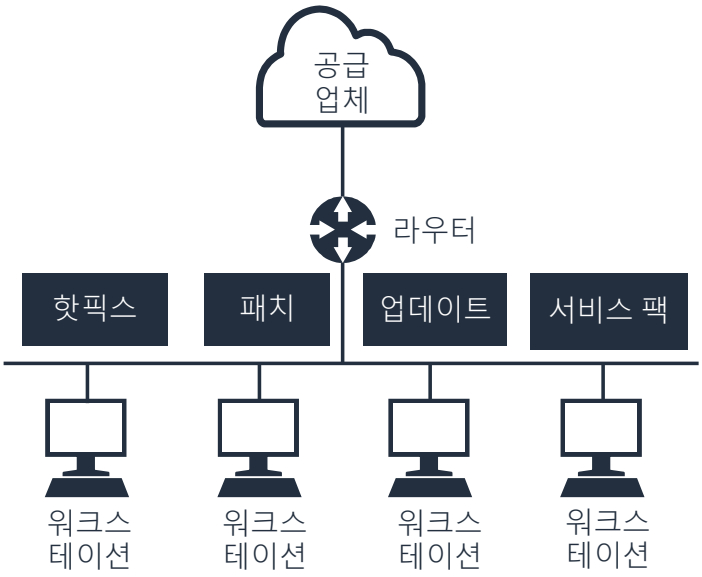
aws re/start

Linux 서비스는 백그라운드에서 실행되고 사용자에게 보이지 않는다는 점에서 애플리케이션과 다릅니다. 많은 서비스가 시스템에서 실행되고 있을 수 있습니다. 따라서 시스템을 강화하는 한 가지 방법은 사용하지 않는 서비스를 비활성화하거나 최소한 시스템이 시작될 때 자동으로 시작되지 않도록 하는 것입니다.

패치

패치:

- 시스템에서 취약점이 발견된 위치에 적용됩니다.
- 성능 또는 기능 문제를 해결합니다.
- 시스템에 침입할 수 있는 수단의 종류를 줄입니다.
- 시스템을 더 신뢰할 수 있고 안전하게 만듭니다.
- 소프트웨어 업데이트로 진행되거나 업데이트의 집합(서비스 팩) 중 일부로 진행됩니다.



aws re/start

또 다른 시스템 강화 방법은 중앙화된 프로세스로 주기적으로 패치를 적용하는 것입니다. 패치는 펌웨어, 운영 체제, 애플리케이션, 기타 소프트웨어에 영향을 미칠 수 있습니다.

소프트웨어 개발 보안 가이드라인

이것은 애플리케이션 개발과 관련한 위험을 최소화하기 위해 따라야 할 일반적인 보안 원칙입니다.

역할별 시스템 강화

클라이언트	서버
• 바이러스 백신 및 방화벽을 켭니다. • 실행되는 애플리케이션의 수를 줄입니다. • 업데이트가 출시되면 적용합니다. • 제거 가능한 미디어를 제한합니다. • 다운로드를 제어합니다. • 터미널 서비스를 제한합니다. • 환경을 모니터링합니다.	• 물리적 액세스를 제한합니다. • 전담 역할을 사용합니다. • 파일 시스템을 보호합니다. • 암호화와 PKI를 사용합니다. • 알림을 사용합니다. • 업데이트가 출시되면 적용합니다. • 관리 액세스를 제한합니다.

디바이스를 강화하는 단계는 디바이스의 역할에 따라 다를 수 있습니다. 예를 들어, DNS 서버에서는 웹 서버와 같은 서비스를 실행할 필요가 없습니다.

이 테이블에는 클라이언트 디바이스, 서버 디바이스, 웹 서버, 데이터베이스 서버별로 강화 가이드라인이 나와 있습니다.

역할별 시스템 강화(계속)

웹 서버	데이터베이스 서버
• 경계 영역을 검토하고 경계 영역에서 강화합니다. • 맬웨어, 조작, 기타 부정 이용이 없는지 면밀히 모니터링합니다.	• 운영 체제(OS)를 강화합니다. • 데이터베이스를 암호화합니다. • 해싱을 활성화합니다. • 데이터베이스 권한을 사용합니다. • 요청을 필터링합니다.

디바이스를 강화하는 단계는 디바이스의 역할에 따라 다를 수 있습니다. 예를 들어, DNS 서버에서는 웹 서버와 같은 서비스를 실행할 필요가 없습니다.

이 테이블에는 클라이언트 디바이스, 서버 디바이스, 웹 서버, 데이터베이스 서버별로 강화 가이드라인이 나와 있습니다.

역할별 시스템 강화(계속)

FTP 서버	디렉터리 서비스 서버
• 익명 모드를 비활성화합니다. • 평문을 사용하지 않습니다. • IP 필터링을 사용합니다. • 폴더를 격리합니다. • 할당량을 유지 관리합니다. • 폴더 권한을 적용합니다.	• 관리적, 물리적, 기술적 제어를 넘어 환경의 깊은 곳에 위치시킵니다. • 강력한 인증을 구현합니다. • 이벤트를 모니터링합니다. • 권한 제한을 활성화합니다. • 트래픽을 암호화합니다.

이 테이블에는 파일 전송 프로토콜(FTP) 서버, 디렉터리 서비스 서버, 동적 호스트 구성 프로토콜(DHCP) 서버, 도메인 이름 시스템(DNS) 서버별로 강화 가이드라인이 나와 있습니다.

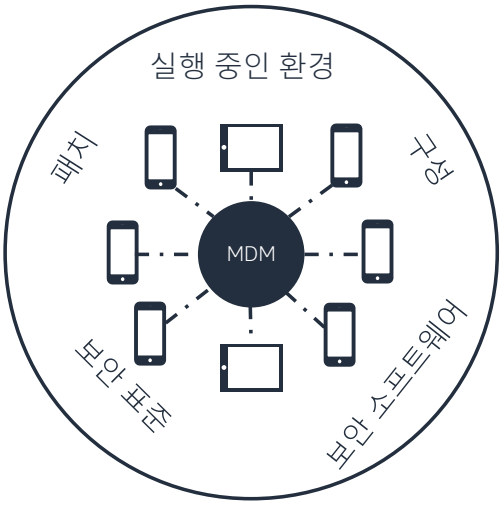
역할별 시스템 강화(계속)

DHCP 서버	DNS 서버
• 포트 보안을 활성화합니다. • 모니터링합니다. • 역할을 격리합니다.	• Microsoft Active Directory Domain Services 영역을 사용합니다. • 신뢰할 수 있는 서버에 Domain Name System Security Extensions(DNSSEC)를 사용합니다. • 파밍 이벤트를 예방하기 위해 쓰기 가능한 캐시 문제를 해결합니다.

이 테이블에는 파일 전송 프로토콜(FTP) 서버, 디렉터리 서비스 서버, 동적 호스트 구성 프로토콜(DHCP) 서버, 도메인 이름 시스템(DNS) 서버별로 강화 가이드라인이 나와 있습니다.

모바일 디바이스 관리(MDM)

MDM 솔루션을 사용하여 디바이스를 보호하고 제어합니다.

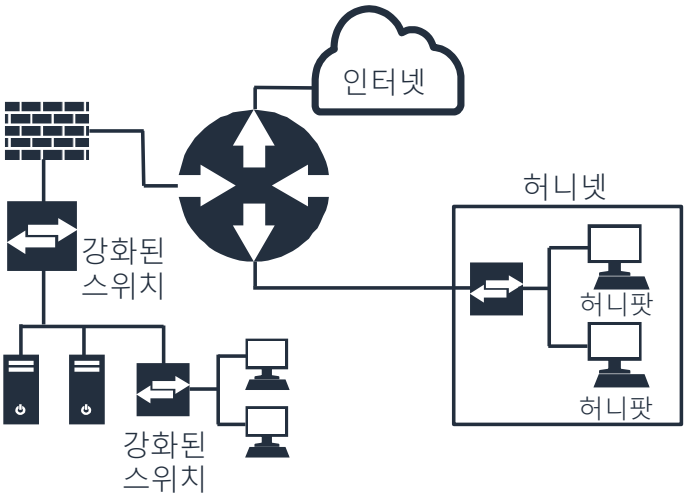


aws re/start

모바일 디바이스 보호를 위해서는 모바일 디바이스 관리(MDM) 솔루션을 사용합니다. MDM을 사용하여 디바이스 사용과 관련한 기업 정책 및 보안 정책을 시행하십시오. 개인 디바이스 사용(BYOD)을 허용하는 기업은 MDM을 구현해야 합니다.

네트워크 강화

- 다음을 예방하기 위해 예방 기법을 구현합니다.
  - 중간자 공격(MITM) 이벤트
  - 세션 하이재킹
  - 보안 인증 정보 스니핑
  - 원격 연결 맬웨어
- 예방 기법의 예는 다음과 같습니다.
  - 스위치 구성 및 포트 제한 (하드웨어)
  - 디코이 네트워크(허니팟 및 허니넷)
  - 방화벽(모든 유형)



aws re/start

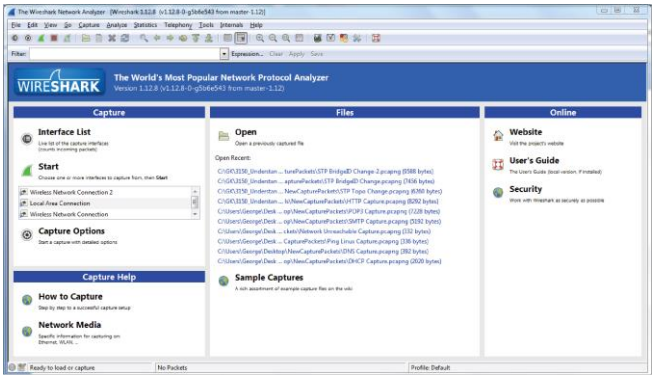
일반적인 네트워크 이벤트를 막기 위해 다양한 하드웨어와 소프트웨어 구성 요소를 사용합니다. 예:

- 세그먼트화에는 스위치를 사용합니다.
- 전환에는 허니팟과 허니넷을 사용합니다. 허니팟은 사이버 공격자를 유인하기 위한 디코이 컴퓨터입니다. 공격을 피하고 공격자에 관한 정보를 얻는 데 사용할 수 있습니다. 허니팟 네트워크, 즉 '허니넷'을 설정하여 네트워크를 강화할 수 있습니다.
- 트래픽 제어에는 방화벽과 액세스 제어 목록(ACL)을 사용합니다.

시스템 강화 도구

분석 도구

- 무료:
  - Wireshark
- 상업용:
  - Nessus Vulnerability Scanner
  - Nexpose
  - Acunetix Vulnerability Scanner
  - IBM Security AppScan
  - Colasoft Capsa Network Analyzer



aws re/start

시스템 강화를 수행하는 데 도움을 주는 분석 도구는 다음과 같습니다.

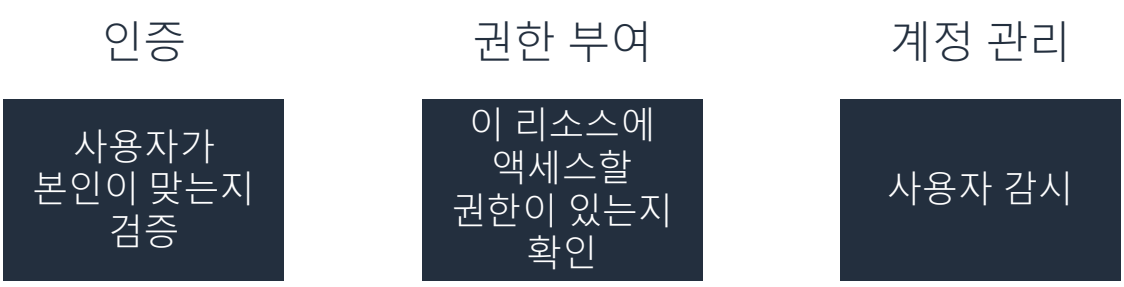
- **Wireshark** - 네트워크 스니퍼(프로토콜 분석기). 이 도구는 네트워크의 트래픽을 보는 데 사용합니다. 어떤 트랜잭션이 발생하는지, 어떤 IP 및 MAC 주소가 트래픽을 발생시키는지, 어떤 프로토콜이 있는지를 볼 수 있습니다. 암호화되지 않은 통신이나 악의적인 통신 또는 기준을 벗어난 활동을 식별하는 데 이 도구를 사용하십시오.

- **Nessus Vulnerability Scanner, Nexpose, Acunetix Vulnerability Scanner** - 수동적인 취약점 스캐너입니다. 시스템 또는 전체 네트워크에 이 도구를 실행할 수 있습니다. 이 도구는 시스템과 취약점 및 노출 데이터베이스를 비교합니다. 해결할 필요가 있는 잠재적인 결점이 포함된 보고서가 생성됩니다.

- **IBM Security AppScan, Colasoft Capsa Network Analyzer** - Wireshark와 용례가 비슷한 상업용 스니퍼입니다.

기업에서는 규모와 필요에 따라 분석 도구를 선택합니다. **소규모 자영업(SOHO)**에서 사용하도록 개발된 무료 도구는 지사가 수백 개인 대규모 글로벌 기업에는 적절하지 않거나 효율적이지 않을 것입니다.

인증, 권한 부여, 계정 관리

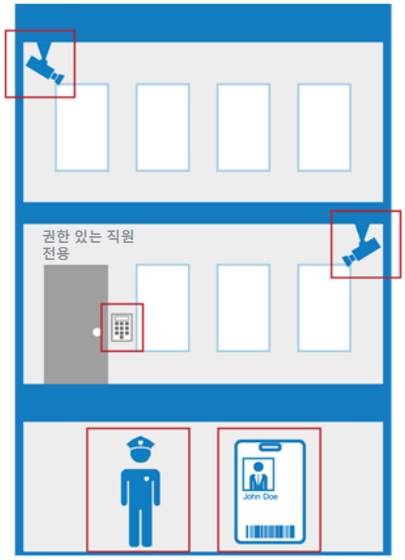


시스템 강화를 위한 포괄적인 솔루션을 결정하려면 다음과 같은 세 가지 보안 측면을 고려해야 합니다.

- **인증** - 사용자가 본인이 맞는지 검증
- **권한 부여** - 사용자가 요청된 리소스에 액세스할 권한이 있는지 확인
- **계정 관리** - 감사 또는 선택적으로 결제에 사용되는 사용량 및 기타 정보 수집

물리적 보안

- 시설에 대한 물리적인 액세스를 제한합니다.
- 자연재해 또는 인재를 예방하도록 건물을 설계합니다.
- 물리적 보안을 다른 모든 보안 원칙의 기준으로 삼습니다.



aws re/start

물리적 보안 또한 시스템 강화에 기여합니다. 취약점은 대부분 사람으로부터 발생합니다.

핵심 사항

- 시스템 강화의 목적은 보안 위험을 최소화하기 위해 시스템으로 인해 노출되는 취약점의 수를 줄이는 것입니다.
- 효과적인 시스템 강화 기법에는 보안 기준 수립, 불필요한 서비스 끄기, 주기적인 패치 적용이 있습니다.
- 시스템을 강화할 때는 시스템의 사용성과 제한 사이에서 균형을 맞춰야 합니다.
- 프로토콜 분석기와 같은 분석 도구가 시스템 강화에 도움이 됩니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 시스템 강화의 목적은 보안 위험을 최소화하기 위해 시스템으로 인해 노출되는 취약점의 수를 줄이는 것입니다.
- 효과적인 시스템 강화 기법에는 보안 기준 수립, 불필요한 서비스 끄기, 주기적인 패치 적용이 있습니다.
- 시스템을 강화할 때는 시스템의 사용성과 제한 사이에서 균형을 맞춰야 합니다.
- 프로토콜 분석기와 같은 분석 도구가 시스템 강화에 도움이 됩니다.