2024
-08

네트워크 보안장비 도입제안서

대표이사: 선영주

한라 KPC 漢拏

목차

1 SIEM 솔루션 제안

1.1. 도입 배경

오늘날 네트워크 보안의 중요성은 점점 커지고 있다. 각종 사이버 공격으로부터 네트워크를 보호하기 위해, 공공기관에서 신뢰할 수 있는 SIEM 솔루션의 도입이 필수적이다. 이 제안서는 여러 SIEM 솔루션을 비교하고, 최적의 솔루션을 도입하기 위한 방향성을 제시한다.

1.2. 주요 SIEM 솔루션 비교

솔루션	주요 특징	장점	단점
IBM QRader	AI와 머신러닝 기반 위협 탐지 및 분석 기능	지능형 보안 분석 기능 제공, 온프레미스 및 클라우드 환경 지원, 높은 자동화 기능	비용이 비교적 높음
RSA NetWitness	이벤트 볼륨, 지리적 확산, 아키텍처 복잡성을 고려한 대규모 환경에 최적화	광범위한 확장성, 비즈니스 컨텍스트 통합으로 위협 우선순위 지정 가능	복잡한 환경 설정과 운영, 초기 설정 비용이 높음
Splunk ES	강력한 데이터 분석 능력을 바탕으로 한 위협 탐지 및 로그 분석	성숙한 데이터 분석 및 시각화 기능, 클라우드 및 온프레미스 환경 모두에서 사용 가능	높은 라이선스 비용, 복잡한 초기 설정

[표 1] SIEM 솔루션 특징과 장단점

1.3. 솔루션별 상세 분석

- **IBM QRadar**

  IBM의 QRadar는 인공지능과 머신러닝을 활용하여 위협을 탐지하고 분석하는 데 강력한 성능을 지닌다. QRadar는 IBM의 보안 플랫폼 Watson과 통합하여 이상 징후를 신속하게 감지하고, 자동화된 대응을 가능하게 한다. 특히, 대규모

공공기관에서도 자주 사용되는 신뢰성 높은 솔루션이다.

- **RSA NetWitness**
  RSA는 대기업과 정부 기관을 보호하는 보안 솔루션으로 잘 알려져 있다. RSA NetWitness는 이벤트 볼륨이 크고, 지리적 분산이 넓은 환경에서도 효과적으로 작동하도록 설계되었다. 이 솔루션은 비즈니스의 중요도를 고려하여 위협에 대한 대응 우선순위를 설정하는 데 탁월하다.
- **Splunk ES**
  Splunk는 로그 파일 분석에 강점을 지닌 SIEM 솔루션이다. Splunk ES는 뛰어난 데이터 분석과 시각화 기능을 통해 복잡한 환경에서의 로그 분석 및 위협 탐지에 탁월한 성능을 발휘한다. 이 솔루션은 클라우드 및 온프레미스 환경 모두에서 활용할 수 있으며, 글로벌 시장에서도 높은 점유율을 차지하고 있다.

1.4. 결론 및 권고 사항

- **도입 우선순위**: 도입 환경의 복잡성과 규모, 그리고 예산에 따라 최적의 솔루션을 선택하는 것이 중요하다. 예산이 충분하고 글로벌 표준을 충족해야 하며, 신뢰성 높은 보안 솔루션을 필요로 하는 경우, IBM QRadar를 추천한다. QRadar는 AI와 머신러닝을 기반으로 한 지능형 보안 분석 기능을 제공하며, 온프레미스 및 클라우드 환경 모두에서 탁월한 성능을 발휘한다. 특히, 자동화된 위협 탐지 및 대응 기능을 통해 보안 사고를 신속하게 처리할 수 있어, 공공기관에 적합한 솔루션이다.
- **추가 고려 사항**: 도입 후 운영의 효율성, 확장 가능성, 기술 지원의 용이성을 함께 고려해야 한다. IBM QRadar는 이러한 측면에서도 우수한 지원을 제공하여, 장기적인 운영 효율성을 높일 수 있는 최적의 선택이다.

2 WAF 솔루션 제안

2.1. 도입 배경

오늘날의 디지털 환경에서 웹 애플리케이션은 비즈니스의 핵심 역할을 하고 있으며, 이러한 웹 애플리케이션을 보호하는 것은 기업과 공공기관에 있어 필수적이다. 특히

ROADo의 DMZ에 위치한 공개 웹 서버는 항상 개방된 상태로 해커의 공격에 노출되어 있으며, 웹 애플리케이션 해킹을 통해 중요한 데이터베이스 정보가 유출될 가능성도 크다. 따라서, ROADo의 웹 서버를 효율적으로 보안하기 위해 웹 애플리케이션 방화벽(WAF)을 도입하여 웹 서버로 유입되는 트래픽을 검사하고 다양한 웹 공격으로부터 서버를 보호하는 것이 중요하다. 이를 통해 개인정보보호법, HIPAA, PCI-DSS 등의 IT 컴플라이언스를 준수하고, 보안 사고로 인한 경제적 손실 및 회사 평판 손상을 예방할 수 있다.

2.2. 주요 WAF 솔루션 비교

솔루션	주요 내용	장점	단점
AI WAF	포괄적인 웹 공격 탐지, Machine Learning & Threat Intelligence, 트래픽 디코딩	- 다양한 웹 공격에 대한 포괄적인 탐지 - 머신러닝 기반 미지의 공격 대응 - 네트워크 투명 프록시 모드 제공	- 높은 성능 요구 - 복잡한 초기 설정이 필요할 수 있음
펜타시큐리티 WAPPLES	로직 기반 웹 방화벽, OWASP Top 10 위협 방어, 손쉬운 정책 관리	- 로직 기반 탐지로 오탐률이 낮음 - 다양한 공공기관 및 기업에 검증된 신뢰성	- 맞춤형 공격에 대한 대응이 제한적일 수 있음 - 추가 비용 발생 가능
가비아 WAF	클라우드 및 온프레미스 지원, 가볍고 빠른 설치, 중소규모 환경에 적합	- 간편한 설치와 관리 - 저렴한 비용으로 기본적인 보안 제공	- 고급 위협에 대한 대응이 제한적 - 대규모 환경에서 성능 한계

[표 2] WAF 솔루션 특징과 장단점

2.3. 솔루션별 상세 분석

- **AIWAF (Application Insight Web Application Firewall)**

  AIWAF는 포괄적인 웹 공격 탐지와 머신러닝 및 위협 인텔리전스를 통한 미지의 공격 대응 기능을 제공한다. SQL/LDAP Injection, XSS, CSRF, Web Shell, Overflow 등 다양한 공격을 탐지하며, 트래픽의 더블 및 멀티 인코딩을 디코딩하여 공격을 차단한다. 관리의 용이성을 위해 네트워크에 영향을 주지 않는 Full Transparent Proxy 모드를 제공하며, 고가용성을 위한 HA(active-standby 및 active-active) 지원, 그리고 통합 대시보드를 통해 웹 사이트 현황을 한눈에 파악할 수 있다. AIWAF는 다양한 네트워크 구성 모드(In-line, Out-of-path, Mirroring)를 지원하며, 머신러닝을 통해 알려지지 않은 공격을 탐지하고, Brute Force, Scraping 등 악성 봇 트래픽도 효과적으로 탐지한다.

- **펜타시큐리티 - WAPPLES**

  WAPPLES는 로직 기반의 웹 방화벽으로, 특허받은 로직을 사용하여 OWASP Top 10 위협을 포함한 다양한 웹 공격을 방어한다. 로직 기반 탐지 방식으로 인해 오탐률이 낮으며, 복잡한 규칙 설정 없이도 손쉬운 정책 관리와 설정이 가능하다. 이미 다양한 공공기관과 기업에서 검증된 신뢰성 높은 제품으로, 신뢰성이 보장된다. 그러나, 고도화된 맞춤형 공격에 대한 대응이 제한적일 수 있으며, 추가 기능 확장을 위해서는 비용이 발생할 수 있다.

- **가비아 – WAF**

  가비아의 WAF는 클라우드와 온프레미스 환경을 모두 지원하며, 가볍고 빠른 설치가 가능한 웹 방화벽 솔루션이다. 중소규모 환경에 적합하며, 기본적인 웹 애플리케이션 보호 기능을 제공하면서도 다양한 보안 옵션을 유연하게 설정할 수 있다. 간편한 설치와 관리가 가능하며, 비교적 저렴한 비용으로 기본적인 보안을 제공한다. 다만, 고급 위협에 대한 대응이 제한적일 수 있으며, 대규모 환경에서는 성능의 한계가 있을 수 있다.

2.4. 결론 및 권고 사항

- **도입 우선순위**

  WAF 솔루션의 도입은 기업의 규모와 보안 요구사항에 따라 달라진다. 대규모 공공기관이나 높은 보안 수준이 요구되는 기업의 경우, AIWAF를 고려하는 것이 좋다. 강력한 웹 공격 탐지 기능과 신뢰성 있는 성능을 제공하며, 다양한 공격

시나리오에 효과적으로 대응할 수 있다.

- **추가 고려 사항**

  도입 후 운영의 효율성, 확장 가능성, 기술 지원의 용이성도 고려해야 한다. 특히, AIWAF는 다양한 네트워크 구성 모드와 머신러닝 기반의 공격 탐지 기능을 제공하여 높은 유연성과 보안성을 보장한다.