실 장비 기반의 AI 챗봇을 활용한 지능형 보안 관제 시스템 구축에 관한 연구

*이서하, **이혜인, ***김정윤

*원광대학교, **덕성여자대학교, ***경희대학교

*fmlf1234@wku.ac.kr, **manggae905@duksung.ac.kr, ***a321@khu.ac.kr

A Study on the Implementation of Intelligent Security Control System Based on AI and Chatbot

*Lee Seoha, **Lee Hyein, ***Kim Jungyun

*WonKwang Univ., **Duksung Women's Univ., ***Kyung Hee Univ.

요 약

본 논문에서는 고가용성 네트워크 인프라를 기반으로 생성형 AI와 챗봇을 결합한 지능형 보안 관제 시스템을 제안한다. BGP, OSPF, HSRP 등을 활용하여 중단 없는 네트워크 환경을 구축하고, 가상화 서버 위에 NTP, DHCP, TACACS+, AD, CA 등 필수 보안 서비스를 구현하여 제로 트러스트(Zero Trust) 기반의 접근 제어 체계를 마련하였다. 또한 KISA 보안 가이드를 적용하여 네트워크 장비 자체의 보안성을 강화하고 L2 구간의 취약점을 보완하였다. 특히 Gemini API를 활용하여 로그를 실시간으로 분석하고, 디스코드(Discord)를 통해 관리자에게 알림을 전송하며, 관리자의 승인을 거쳐 Netmiko 라이브러리가 자동으로 대응 명령어를 수행하는 'Human-in-the-loop' 방식의 자동화 시스템을 설계하였다.

Ⅰ. 서 론

현대의 네트워크 환경은 복잡해지고 있으며, 이에 따라 보안 위협 또한 고도화되고 있다. 안정적인 서비스 제공을 위해서는 고가용성(High Availability)이 보장된 네트워크 인프라와 효율적인 보안 관제 시스템이 필수적이다. 본 논문에서는 라우터 구간에 BGP, 그 외 구간에 OSPF를 적용하고, 방화벽의 Failover(Active/Standby) 및 백본 스위치의 HSRP 구성을 통해 게이트웨이 이중화를 구현하여 서비스 지속성을 확보하였다. 또한 AnyConnect VPN을 구축하여 원격 접속 환경을 제공하며, DMZ 구간에 웹 서버를 배치하여 외부 접근성을 확보하였다. 이러한 인프라 위에 ESXi 기반의 서버 가상화를 통해 AI, NTP, DHCP, 인증 서버 등 다양한 보안 서비스를 통합 구축하고, 생성형 AI를 활용한 자동화된 보안 대응 체계를 설계 및 구현하였다.

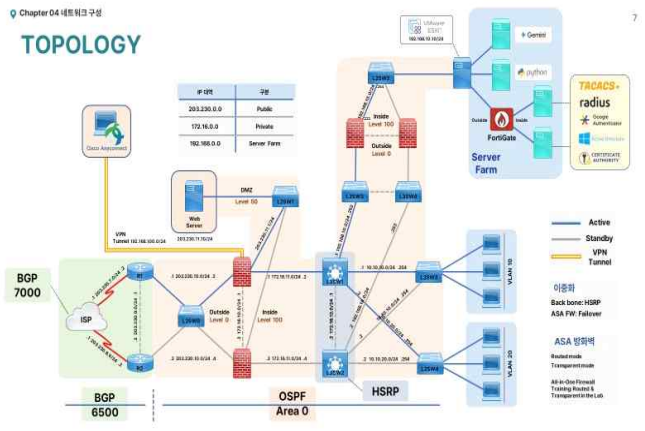

그림 2. 네트워크 토폴로지

Ⅱ. 본론

2-1. 보안 인프라 및 서비스 구축

안정적인 보안 서비스를 제공하기 위해 네트워크 및 서버 인프라를 다음과 같이 구축하였다. 첫째, 라우터 구간에는 BGP, 그 외 구간에는 OSPF를 적용하여 경로 이중화를 구성하였으며, 백본 스위치(L3)에는 HSRP를, 방화벽에는 Active/Standby Failover를 적용하여 단일 장비 장애 시에도 서비스가 지속되도록 하였다. 또한 AnyConnect VPN을 구축하고 웹 서버를 DMZ에 배치하여 내외부 접근성을 확보하였다. 둘째, KISA(한국인터넷진흥원)의 주요 정보통신기반시설 기술적 취약점 분석 가이드를 활용하여 네트워크 장비의 자체 보안을 강화하였다. 비인가자가 웹 인터페이스를 통해 장비를 장악하는 것을 방지하기 위해 ip http secure-active-session-modules exclude_webxec및 ip http active-session-modules exclude_webxec 설정을 적용하여 웹 서비스 취약점을 차단하였다. 또한 tcp/udp small서비스를 비활성화하여 불필요한 포트를 통한 DoS 공격 위협을 제거하였으며, mask-reply와 cdp를 차단하여 내부 네트워크 정보가 외부로 유출되지 않도록 조치하였다. 셋째, 다양한 엔드 디바이스가 연결되는 L2 액세스 계층의 보안 취약점을 보완하기 위해 L2 Security를 적용하였다. 사용하지 않는 포트는 'ParkingLot' VLAN 999번으로 격리하여 물리적 접근을 통한 무단 접속을 원천 차단하였으며, 포트 보안 기능을 활성화하여 인가된 디바이스만 네트워크에 접속할 수 있도록 구성하였다. 넷째, 폐쇄망 환경에서 ESXi 기반의 가상화 서버를 운용하여 리소스 효율성을 높였으며, NTP와 DHCP를 통해 모든 장비의 시간 동기화와 IP 자원 관리를 자동화하였다. 다섯째, 제로 트러스트 보안 모델을 적용하여 인

증 체계를 강화하였다. TACACS+를 통해 관리자 권한을 차등 부여(Senior/Junior)하고, 최고 관리자는 구글 OTP를 이용한 2차 인증(MFA)을 통과해야만 접근할 수 있도록 하였다[1]. 또한 Windows 및 CentOS 기반의 이중화된 CA 서버를 통해 인증서를 발급하고, VPN 및 SSH 접근 시 인증서 기반 인증을 강제하였다. 여섯째, Active Directory(AD)를 통해 중앙화된 정책 관리를 수행하였다. 특히 그룹 정책(GPO)을 활용하여 사용자의 근무 시간 외 시스템 접근을 원천 차단함으로써, 업무 시간 외 발생할 수 있는 계정 탈취 및 오남용 위협을 최소화하였다.

2-2. AI 기반 보안 관제 자동화 시스템

본 연구의 핵심인 AI 보안 관제 시스템은 Gemini API, Python 스크립트, 그리고 디스코드(Discord)를 연동하여 구축하였다. 시스템은 로그 데이터를 실시간으로 수집하는 ai_advisor.py와 관리자의 승인을 처리하는 approve.py로 구성된다. ai_advisor 모듈은 로그에서 공격 패턴을 탐지하고, 공격 횟수가 임계치(10회)를 초과할 경우 심각도를 판별하여 디스코드에 경고 알림을 전송한다. 이때, 기존 대응 명령어가 덮어씌워지는 것을 방지하는 로직을 적용하여 대응의 연속성을 보장하였다.[2] 대응 단계에서는 Netmiko 라이브러리를 활용하여 이기종 장비의 프롬프트를 인식하고 SSH 접속을 통해 명령어를 자동으로 입력한다. Netmiko는 Ansible 대비 복잡한 로직 제어와 대화형 처리에 강점이 있어, 가변적인 보안 위협 대응에 적합하다.[3] 안정성을 위해 AI가 생성한 명령어는 즉시 실행되지 않고, 관리자가 approve.py 파일을 통해 승인했을 때만 ai_advisor.sh 스크립트를 통해 방화벽 및 로컬 서버에 적용되도록 설계하였다.[4] 그림 3은 본 시스템의 핵심 모듈인 AI 자동 대응 스크립트의 실행 이력과 운영 현황을 Splunk를 통해 시각화한 결과이다. 시간의 흐름에 따라 그래프가 특정 구간에서의 단절이나 급격한 변동 없이 일정한 패턴을 유지하며 연속적으로 나타나는 것은, AI 모델과 연동된 자동화 프로세스가 프로세스 중단이나 시스템 오류 없이 지속적이고 안정적으로 수행되고 있음을 시사한다.

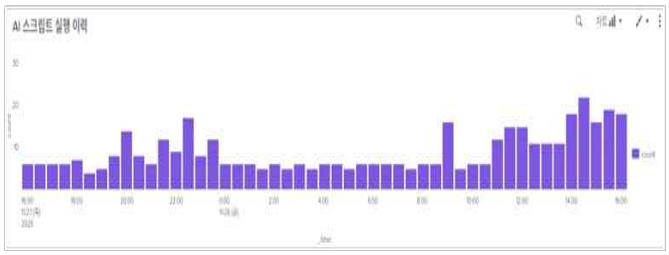

그림 3. ai 스크립트 실행이력 시각화

2-3. 시각화 및 위협 인텔리전스

Splunk를 활용하여 Brute Force 공격 시도와 장비 경고 메시지를 실시간으로 시각화하였다. 그림 4는 Brute Force 공격 시도 횟수를 시간대별 막대형 그래프(Bar Chart)로 시각화한 결과이다. 공격이 발생할 경우 해당 시간대의 막대 높이가 급격히 상승하여 평상시와 확연하게 구분되므로, 관리자가 위협의 유입 여부와 공격 강도를 직관적으로 식별할 수 있다. 이를 통해 공격이 집중되는 장비를 식별하고 보안 정책을 효율적으로 재배치할 수 있다. 또한 Spamhaus, FireHOL 등의 위협 인텔리전스를 기반으로 매일 새벽 악성 IP 리스트를 수집하고, 오전 5시 40분에 자동으로 차단 룰을 갱신하는 선제적 방어 시스템을 구축하였다.[5]

그림 4. BruteForce 공격 시도 시각화

Ⅲ. 결론

본 논문에서는 이중화된 네트워크 인프라 위에 AI와 자동화 도구를 결합한 보안 관제 시스템을 설계하고 구현하였다. 제안된 시스템은 단순한 로그 수집을 넘어, 생성형 AI를 통해 위협을 분석하고 Netmiko를 통해 대응을 자동화하되, 관리자의 최종 승인 단계를 둠으로써 자동화의 효율성과 운영의 안정성을 동시에 확보하였다. Splunk를 통한 시각화는 보안 관리자의 의사결정을 지원하며, 전체적인 네트워크 보안 수준을 향상시키는 데 기여하였다.

ACKNOWLEDGMENT

본 연구는 한국전파진흥협회에서 운영하는 시스코 보안 아카데미(K-Digital Training) 사업의 지원을 받아 수행되었음.

참 고 문 헌

[1] STAFFORD, V. Zero trust architecture. *NIST special publication*, 2020, 800.207: 800-207.

[2] GUPTA, Maanak, et al. From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. *IEEE access*, 2023, 11: 80218-80245.

[3] K. Byers, "Netmiko: Multi-vendor library to simplify Paramiko SSH connections to network devices," *GitHub Repository*, 2024. [Online]. Available: https://github.com/ktbyers/netmiko.

[4] TEAM, Gemini, et al. Gemini: a family of highly capable multimodal models. *arXiv preprint arXiv:2312.11805*, 2023.

[5] Splunk Inc., "The State of Security 2023: Race to Resilience," *Splunk Research Report*, 2023.