인프라 전반에서 자동화 보호

"고객이 배포 및 유지 관리를 위해 Palo Alto Networks NGFW자동화에 Red Hat Ansible Automation Platform을 사용하며 시간 절감을 비롯한 놀라운 혜택을 경험하고 있습니다. 예를 들어 한 기업은 3시간 이상 걸리던 VM 시리즈 가상 방화벽을 20분 이내에 배포하여 엔지니어링 시간을 97% 단축했습니다. 또 다른 기업은 PAN-OS 업그레이드를 일관되게 유지하기 위해 Ansible을 사용함으로써 빠듯한 유지 관리 기간에 몇 달은 커녕 2시간도 채 안 되는 시간에 고가용성(HA) 연결 NGFW 75개를 업그레이드할 수 있었습니다."

Rich Campaigna
Palo Alto Networks
제품 관리 부문

복잡한 인프라의 보안 문제 해결

기업이 클라우드로 전환하면서 팀의 생산성 향상이 요구되고 있으며, 네트워크는 점차 복잡해져가고 있습니다. 이로 인해 전체 엔터프라이즈 인프라에 대한 전체 가시성을 확보하기가 어려우며, 특히 수동 프로세스를 사용하여 다양한 네트워크 요소를 관리하고 보안 팀에서 여러 툴을 사용하여 컴플라이언스 정책을 구성하고 배포하는 경우에는 더욱 그렇습니다.

결과적으로 네트워크 운영 팀과 보안 팀은 사용자가 전 세계 어디에서나 애플리케이션과 리소스에 액세스할 수 있도록 보장하면서도 무단 사용자를 차단해 데이터가 외부로 유출되지 않도록 엔터프라이즈 아키텍처 전반에 일관된 보안 정책을 적용해야 한다는 부담을 안고 있습니다.

조직은 이러한 문제를 해결하기 위해 네트워크 인프라의 유지 및 관리를 최적화하는 NetOps 방법론을 채택하려고 합니다. 그러나 NetOps를 안전하게 구현하는 데 필요한 자동화, 오케스트레이션, 소프트웨어 정의 네트워킹 기술이 부족한 경우가 많습니다.

엔터프라이즈 전반의 보안 강화를 위한 속도, 규모, 일관성 지원

Palo Alto Networks®와 Red Hat은 협업을 통해 기업의 네트워크 인프라를 유지 관리, 업데이트, 보호하는 효율적이고 반복 가능한 NetOps 워크플로우를 생성하여 네트워크 팀이 중요한 환경을 고도로 자동화된 방식으로 보호할 수 있도록 지원합니다.

Red Hat® Ansible® Automation Platform과 결합된 Palo Alto Networks의 PAN-OS® 방화벽 시리즈를 활용하면 네트워킹 팀이 제어된 코드형 인프라(IaC) 접근 방식을 통해 해당 환경의 네트워크 장치와 변경을 관리하여 네트워크 인프라의 규모, 속도, 보안을 강화하는 NetOps 워크플로우를 생성할 수 있습니다.

이 솔루션은 인프라 전반에서 안전하게 자동화할 수 있을 뿐만 아니라 IT 팀 간의 가시성과 협업을 촉진하고 Red Hat과 Palo Alto Networks의 공동 지원을 포함합니다.

효율성과 대응력, 적응성 향상을 위한 자동화

조직은 환경, 시스템 이벤트 또는 외부 트리거의 실시간 변화를 기반으로 태스크를 자동화하는 Event-Driven Ansible을 통해 더욱 신속하고 다이나믹한 자동화를 실현할 수 있습니다.

PAN-OS용 Event-Driven Ansible 플러그인을 사용하면 Event Driven Ansible의 의사 결정 기능에서 대응이 필요한 IT 환경의 조건에 관한 인텔리전스를 수신하여 Palo Alto Networks 제품의 보안 운영을 개선할 수 있습니다. 이 플러그인은 실시간 오류 로그 스트리밍과 자동 대응을 제공하므로 자가 치유(Self-healing) 네트워크 보안을 실현할 수 있습니다.

개요:
자동화를 통해 인프라를 관리하고 보호하기 위한 반복 가능하고 일관된 운영 워크플로우를 생성하는 방법을 알아보세요.

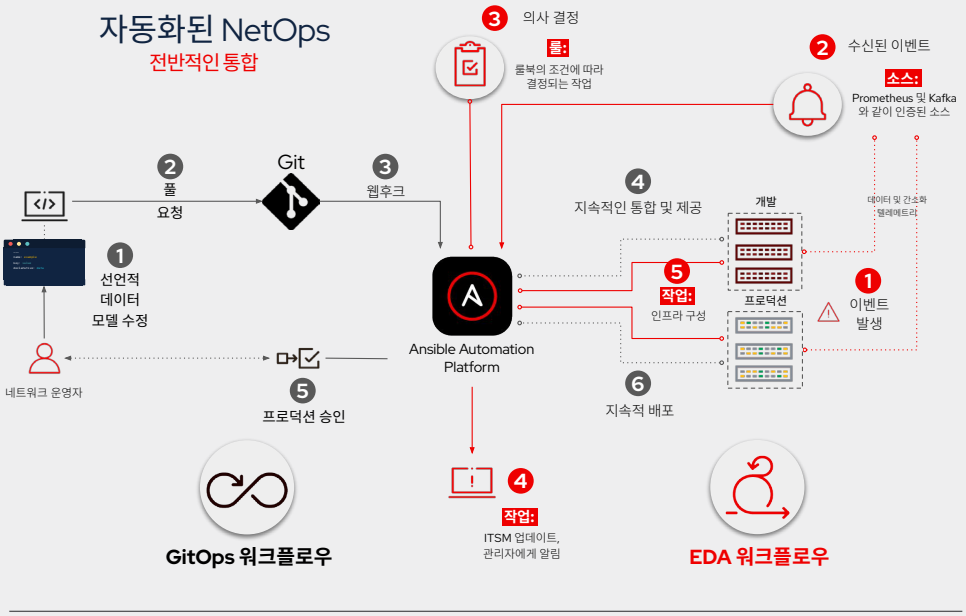

그림 1. GitOps를 위한 자동화된 NetOps 예시

Red Hat Ansible Automation Platform을 위한 Palo Alto Networks의 광범위한 인증 컬렉션은 Palo Alto NGFW(Networks Next-Generation Firewall)를 실행하는 소프트웨어인 Palo Alto Networks의 모든 PAN-OS 기반 제품의 자동화를 지원합니다. 이러한 통합 기반의 강력한 솔루션을 통해 조직은 보안을 강화하고, 운영을 간소화하고, 진화하는 위협 환경에 대응할 수 있습니다.

PAN-OS Ansible Content Collection을 사용하는 네트워크 팀과 보안 팀은 단일 자동화 플랫폼을 통해 네트워크 및 보안 구성 요소, 구성, 정책을 정의하고 관리할 수 있습니다.

고객은 애플리케이션-ID, 콘텐츠-ID, 장치-ID, 사용자-ID와 같은 PAN-OS에 내장된 핵심 기술을 통해 항상 모든 위치의 모든 사용자와 장치 전반에서 사용 중인 애플리케이션을 완벽히 파악하고 제어할 수 있습니다. 인라인 머신 러닝(ML), 애플리케이션, 위협 서명은 최신 인텔리전스로 방화벽을 다시 자동 프로그래밍하여 허용된 트래픽에 알려진 위협과 알려지지 않은 위협의 유무를 확인합니다.

개발 및 배포 가속화와 출시 기간 단축

PAN-OS Ansible Content Collection을 배포하는 고객은 다음을 수행할 수 있습니다.

- 물리 및 가상의 차세대 방화벽 배포를 자동화하고 기존 CI/CD(지속적 통합 및 지속적 배포) 파이프라인 내에 배포를 통합하여 시간을 절약하고 컴플라이언스 강화
- 변화에 빠르게 대응하여 확신을 갖고 보안 솔루션 배포
- 변경 관리 및 감사 목적으로 구성을 검사하기 위해 기록 시스템에 액세스
- 정확한 구성을 복제하고 인적 오류 제거
- 수동 프로세스를 제거하여 팀이 중요 업무에 집중할 수 있는 시간 확보

자신있게 NetOps 방법론으로 전환

Palo Alto Networks의 PAN-OS 방화벽 시리즈는 Red Hat Ansible Automation Platform과 결합되어 인프라를 자동화하고 네트워크, 보안, 컴플라이언스 운영을 안전하고 효율적으로 관리하는 데 필요한 툴을 제공하므로 IT 팀이 혁신에 집중할 수 있습니다. 자세히 알아보기:

데모 보기: Red Hat Ansible Automation Platform으로 Palo Alto Networks의 차세대 방화벽 자동화

Ansible for PAN-OS 구성 방법 알아보기

Red Hat과 Palo Alto Networks 파트너십에 대해 자세히 알아보기

한국레드햇 홈페이지 https://www.redhat.com/ko

Red Hat 소개

Red Hat은 권위 있는 어워드를 수상한 지원, 교육, 컨설팅 서비스로 고객이 여러 환경에서 표준화를 진행하고, 클라우드 네이티브 애플리케이션을 개발하고, 복잡한 환경을 통합, 자동화, 보안, 관리할 수 있도록 지원합니다.

www.facebook.com/redhatkorea
구매문의 02-6105-4390
buy-kr@redhat.com

www.redhat.com/ko
#638595_1223