자동화를 통한 특수 작전 부대의 역량 확장

확장 가능한 자동화의 필요성

수동 서버 구성 및 패치 프로세스는 시간이 많이 소요되고 오류가 발생하기 쉽습니다. 특수 작전 부대(SOF)를 포함한 전 세계 공공 부문 조직은 이러한 문제를 완화하기 위해 확장 가능한 자동화로 이전해야 합니다. 구성 및 패치를 자동화하면 수작업에 따른 오류를 방지하고, 보안을 강화하며, 신규 기능 제공 속도를 높이고, 더욱 가치가 높은 미션 중심 작업에 인력을 배치할 수 있습니다. Red Hat® Ansible® Automation Platform과 같은 포괄적인 솔루션은 모든 하드웨어 및 소프트웨어 제품의 구성과 패치를 자동화하고 기존의 벤더별 툴을 단일 통합 인터페이스로 통합할 수 있습니다.

방어 프로세스 수작업 처리 시의 비용

네트워크 업그레이드가 자동화되어 있더라도 서버, 가상 머신(VM), 클라우드 리소스를 구성 및 패치하는 과정은 여전히 수작업 방식인 경우가 많습니다. 이러한 수동 태스크는 다음을 문제를 야기하여 전략적 방위 목표를 직접적으로 저해합니다.

- 노동 집약적인 운영. 새로운 서버 100개를 프로비저닝하거나 VM 200개에 긴급 보안 패치를 적용하는 등의 반복적인 수동 태스크는 2030년까지 구현하려는 NATO의 제로 트러스트 사이버 보안 프레임워크인 다영역작전(Multi-Domain Operations, MDO) 연합과 같은 중요한 전략 이니셔티브에 인력을 효율적으로 투입할 수 없게 만듭니다.[1]
- 미션 크리티컬 오류 리스크. 업그레이드 및 패치의 매뉴얼이 여러 단계의 복잡한 지침으로 구성된 경우 인적 오류의 리스크가 커지며 이에 따라 상당한 보안 취약점이 발생하거나 시스템 전체가 실패할 수 있습니다.
- 전문성의 잘못된 배분. 반복적인 태스크에 매여 있는 관리자를 더욱 창의적인 작업에 집중하도록 재배치하면 전문성을 더 효율적으로 활용하고 사기를 진작시킬 수 있습니다.

통합되지 않은 자동화를 사용할 때의 단점

기관이 일부 수동 프로세스를 자동화했지만 자동화 전환 속도를 더 높이고 싶을 수도 있습니다. 많은 팀들이 직면한 주요 과제는 대부분의 자동화 툴이 단일 벤더의 제품에 국한되어 있다는 점입니다. IT 팀이 VM, 물리 서버, 개별 애플리케이션에 쓰이는 툴들을 모두 배우고 관리하는 것은 불가능합니다.

또 다른 장애 요인은 IT 팀들이 자체 프로세스에 대한 제어권을 유지할 수 있을지 걱정한다는 점입니다. 너무 많은 리소스가 공유되면 각 팀은 자산 보호 및 최적화된 운영을 유지하는 프로세스가 인력이나 시스템에 의해 변경될까봐 우려하게 됩니다.

1 *'NATO's NATO의 대담한 디지털 도약: 안전한 클라우드 기반 연합(Bold Digital Leap: A SECURE Cloud-Empowered Alliance).' NATO Allied Command Transformation, 2024년 12월 9일*

오픈소스 자동화 및 오케스트레이션 솔루션

하드웨어 및 소프트웨어의 구성과 패치를 자동화하면 SOF IT 팀은 한 번 변경한 후에 이 변경 사항을 전체 또는 일부 장치에 손쉽게 푸시할 수 있습니다. 변경한 대로 작동하지 않는 경우 작동하는 것이 확인된 상태로 구성을 되돌리기도 간단합니다.

Ansible Automation Platform을 통해 SOF는 모든 하드웨어 및 소프트웨어 시스템의 구성과 패치를 자동화하고 고급 워크플로우를 오케스트레이션할 수 있습니다. 모든 하드웨어 또는 소프트웨어 제품에 대해 커맨드라인 인터페이스(CLI)나 애플리케이션 프로그래밍 인터페이스(API)를 통해 실행 가능한 모든 작업을 자동화할 수 있습니다. Ansible 모듈은 다음 세 가지 방법으로 획득할 수 있습니다.

1. Red Hat Ecosystem Catalog에서 모듈을 다운로드합니다. Red Hat은 60개가 넘는 독립 벤더와 협력하여 Ansible 모듈을 검증하고 선별합니다. 이러한 모듈은 Red Hat Ecosystem Catalog에서 Ansible Content Collections로 나와 있습니다.
2. 소프트웨어 및 하드웨어 벤더로부터 모듈을 획득합니다. 일부 벤더는 자사 제품을 관리하기 위해 Ansible 모듈을 게시하거나 제공합니다.
3. 직접 제작합니다. Red Hat 또는 다른 벤더가 특정 제품의 모듈을 제공하지 않는 경우, 직접 제작할 수 있습니다.

Ansible Automation Platform은 구성 및 프로세스의 액세스 제어에 관한 IT 팀의 우려를 해결하는 데 도움을 줍니다. Ansible Automation Platform 내에서 서버 패치나 소프트웨어 업그레이드 등의 프로세스를 시작하는 관리자가 해당 자산 자체에 로그인할 수 없습니다. 대신에 Ansible Automation Platform이 해당 자산을 소유한 팀에 의해 정의된 작업을 호출합니다. 자산을 소유한 팀만 해당 자산에 로그인할 수 있으므로, 구성 드리프트 또는 권한 에스컬레이션 같은 보안 리스크를 방지합니다.

Red Hat Ansible Automation Platform의 5가지 SOF 활용 사례

기간 한정 네트워크 액세스

직원이 24시간 동안 시스템 액세스 권한이 필요한 경우 또는 머신 러닝 모델이 48시간 동안 외부 소스 데이터를 수집해야 하는 경우를 상상해 보겠습니다. 두 시나리오 모두 방화벽 포트를 개방해야 합니다. 원래대로라면 관리자는 시간 만료 후에 포트를 차단하도록 미리 알림을 설정해야 합니다. 만약 관리자가 바빠서 알림을 놓치기라도 하면 포트가 개방된 상태로 유지되어 보안 취약점이 발생합니다. Ansible Automation Platform을 사용하면 관리자는 작업을 실행할 때 작업 종료 시점을 지정할 수 있습니다.

한정된 기간 동안 리소스 프로비저닝

특정 기능을 짧은 기간 동안 향상해야 하는 경우가 있습니다. 특수 작전 부대(SOF) 임무를 지원하기 위해 기밀 클라우드 리소스를 프로비저닝하는 경우를 예로 들 수 있습니다. 미션 완료 후 관리자가 리소스를 축소하는 것을 소홀히 한다면 불필요한 비용이 수 주 또는 수개월 동안 발생할 수 있습니다. Ansible Automation Platform을 사용하면 관리자는 리소스를 프로비저닝하는 시간과 릴리스하는 시점을 모두 입력할 수 있습니다.

인시던트 대응

보안 팀은 현재 패치를 적용하거나 포트를 차단하거나 사용자를 제거하는 등의 위협 완화 조치를 장치별로 수행합니다. 이러한 수동 태스크는 노동 집약적이며 차례로 조치를 취하는 동안 대기 중인 장치는 취약한 상태로 유지됩니다. Ansible Automation Platform을 사용하면 모든 취약한 장치에 동시에 조치를 적용할 수 있습니다.

이벤트 기반 활동

Ansible Automation Platform을 다른 SOF 시스템과 통합하면 한 시스템에서 발생하는 이벤트를 감지한 후 정의된 작업을 다른 시스템에서 자동으로 호출할 수 있습니다. 예시는 다음과 같습니다.

- **VM 요청 수행.** VM을 구축하는 데는 일반적으로 10분이 걸리지 않습니다. 그러나 많은 조직에서는 요청부터 프로덕션까지 몇 주, 때로는 몇 개월이 걸릴 수도 있습니다. 한 팀이 VM을 프로비저닝하고, 다른 팀이 IP 주소를 할당합니다. 운영 체제(OS) 및 애플리케이션을 담당하는 팀도 다 다릅니다. 이러면 워크플로우 단계마다 지연이 누적됩니다. Ansible Automation Platform에서는 VM 요청이 발생하는 경우 각 팀이 정의해 둔 프로세스가 트리거되어 지정된 순서대로 실행됩니다. 하루 또는 한 시간만에 VM 요청을 수행할 수 있습니다.
- **코드형 인프라(IaC)로 서버 프로비저닝 자동화.** SOF 개발자는 서버 하드웨어, OS, 스토리지 및 다른 인프라 구성 요소를 수작업으로 프로비저닝 및 관리합니다. 하지만 국방정보시스템국(Defense Information Systems Agency, DISA) 및 고위 지침은 효율성을 향상하고 보안을 개선하기 위해 IaC로 전환할 것을 촉구합니다. VMware 또는 Amazon Web Services(AWS), Microsoft Azure 같은 상용 클라우드의 가상화 툴링과 통합되는 경우 Ansible Automation Platform은 노출된 API를 사용하는 코드를 실행하여 서버를 자동으로 프로비저닝합니다.
- **신규 팀원 온보딩.** 이벤트에 대응하여 애플리케이션 활동이 일어나도록 자동화할 수 있습니다. 예를 들어 온보딩 시스템에 신규 팀원이 감지되면 온보딩 시스템이 자동 워크플로우를 트리거하여 해당하는 하드웨어 및 소프트웨어 시스템에서 계정을 생성할 수 있습니다. 반대로 누군가 팀에서 나간 것이 감지되면 Ansible Automation Platform이 해당 계정을 자동으로 보관하거나 제거할 수 있습니다. 마찬가지로 새로운 애플리케이션 엔드포인트가 추가되면 자동 워크플로우를 트리거하여 방화벽 룰을 호출하거나, 보안 검사를 트리거하거나, 서비스 가용성을 팀에 알릴 수 있습니다.

SOF를 위한 Red Hat Ansible Automation Platform 사용의 장점

Ansible Automation Platform은 효율적이고 간편하게 도입할 수 있으며, 이는 다음과 같은 특징 때문입니다.

- **보안 인증 제공.** Red Hat Ansible Automation Platform의 오토메이션 컨트롤러에 대한 보안 기술 구현 가이드(STIG)에 관해서는 Ansible Content Collections에서 자세히 알아볼 수 있습니다.
- **필요한 교육 또는 재교육 최소화.** Ansible Automation Platform은 이미 전 세계적으로 SOF 팀이 사용 중이며 간편하게 도입할 수 있습니다.
- **벤더 독립성.** Ansible Automation Platform을 사용하여 자산 구성 및 패치를 자동화합니다. 핵심 환경부터 전술적 엣지에 이르기까지 작업 관행을 통합합니다.

- **기존 툴 보완.** Ansible Automation Platform은 기존의 제품별 자동화 툴을 대체하는 것이 아니라 동일한 인터페이스에 모두 통합하여 가치를 향상합니다. 예를 들어 IaC를 위해 Hashicorp Terraform을 사용하는 팀은 Ansible Automation Platform에서 Terraform 워크플로우를 호출할 수 있습니다. 다시 말해서, 다른 자동화 태스크에 사용하는 것과 동일한 인터페이스에서 작업하게 됩니다.

일상적인 태스크의 자동화를 통해 SOF 현대화 가속

구성 및 패치 자동화는 작업하기 간편하면서도 IT 운영에 지속적으로 효과를 미칩니다. Red Hat Ansible Automation Platform을 사용하면 SOF는 동일한 인원으로 더 많은 IT 자산을 관리하고, 리소스 요청을 더 짧은 시간 내에 수행하고, 보안 태세를 강화할 수 있으며 직원이 MDO 및 제로 트러스트 프레임워크처럼 가치가 높은 이니셔티브에 더 많은 작업 시간을 투입할 수 있습니다.

자세히 알아보기

Red Hat은 특수 작전 부대와 협력하여 미션 크리티컬 솔루션을 제공합니다. 자세한 내용을 알아보려면 Red Hatter에게 문의하세요.

한국레드햇 홈페이지 https://www.redhat.com/ko

Red Hat 소개

Red Hat은 전 세계 고객에게 높은 수준의 지원과 교육 및 컨설팅 서비스를 제공하여 권위 있는 어워드를 수상한 바 있으며 이를 통해 고객 환경 전반의 표준화, 클라우드 네이티브 애플리케이션 개발, 복잡한 환경의 통합, 자동화, 보안 및 관리를 지원합니다.

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

www.redhat.com/ko
#3134372_1225