인프라 자동화로 사이버 컴플라이언스 강화

다수 기관의 이벤트 모니터링 및 각 기관의 플레이북 사용을 통한 대응 자동화

Red Hat 솔루션

Red Hat Integration: 여러 기관의 네트워크 기기, 서버, 엣지 기기 데이터 연결

Red Hat OpenShift: Open Data Hub를 통해 악성 패턴을 인식할 수 있는 머신 러닝 모델 학습 제공

Red Hat Decision Manager: 각 기관의 룰에 따라 대응 방식에 보안 이벤트 매핑

Red Hat Ansible Automation Platform: 위협 감지 시, 각 기관의 플레이북에 따라 해당 기관의 작업을 자동으로 호출

맬웨어의 경계없는 공격

법을 집행하는 공공기관들은 범죄 기록, 수사 자료, 생체정보, 세금 신고서, 보안 카메라 영상 및 인사 기록 등 민감한 데이터를 보호해야 합니다. 민감한 정보가 노출되면 업무 운영에 차질이 생길 수 있으며 안전 위협 및 공공기관에 대한 신뢰 저하로 이어질 수 있습니다. 데이터 유출과 서비스 거부 공격(DoS) 등이 일반적인 예입니다.

법 집행 시 사이버 컴플라이언스의 장애 요인은 다음과 같습니다.

- **제한된 인력:** 보안 팀의 역량이 맬웨어에 감염된 IP 카메라와 같은 엣지 기기의 스트림을 비롯한 트래픽 볼륨 증가를 모니터링하는 데 충분하지 않을 수 있습니다. 위협 감지와 해결이 지연되면 취약성이 증가됩니다.
- **기관 전체에 대한 중앙 모니터링의 부재:** 여러 기관을 표적으로 한 공격은 정교한 경우가 많으며 주요 비즈니스 운영을 중단하고 정보를 유출시킬 위험이 매우 높습니다. 보안 이벤트가 여러 기관을 대상으로 한 공격의 일부라는 사실을 모르는 기관들은 그 심각성을 과소평가할 수 있습니다.
- **조정 중 운영 지속성:** 사법 기관은 운영 중단 없이 손상된 기기를 종료할 수 없으며, 이 때 위협 심각도에 따라 세심한 조정이 필요합니다.

솔루션: 네트워크 이벤트에 대한 종합적인 시각과 자동화된 대응

공공 데이터를 보호하려면 사법 기관은 두 가지 역량을 보완해야 합니다. 첫번째는 여러 조직의 전체 네트워크와 서버 활동을 종합적으로 파악하는 것이며, 두번째는 해당 기관의 플레이북과 위협 속성을 바탕으로 조정을 자동화하는 것입니다. 예를 들면, 금지된 네트워크 주소의 동일 목록을 여러 기관에 적용하고, 해당 주소가 나타나면 경고를 전송하고, 조사가 시작될 때까지 의심스러운 워크로드를 격리하며, 비정상적인 행동을 나타내는 가상 서버를 종료한 다음 신뢰할 수 있는 소스에서 새로운 서버를 가동하는 경우입니다.

사법 기관 내 자동화된 사이버 컴플라이언스의 이점은 다음과 같습니다.

- 더욱 신속한 인시던트 감지
- 문제 해결을 가속화하여 취약점 노출 시간 단축
- 위협 완화에 필요한 리소스 요구 사항 절감
- 사이버 보안 전문가의 일상적인 모니터링 업무를 축소하여 더 가치 있는 활동에 매진할 수 있게 되면서 직무 만족도 증가(직원 채용 및 유지에 유리)

Red Hat 솔루션의 특징과 장점

보안 강화: Red Hat 솔루션은 엄격한 정부 보안 요구 사항을 충족합니다.

파트너 에코시스템: Red Hat 파트너와 협업을 통해 데이터 조회 및 문제 해결 자동화를 위한 솔루션을 연결할 수 있습니다.

공공 기관이 검증한 기술력: 미국 사이버 보안 및 인프라 보안국(Cybersecurity Infrastructure and Security Agency, CISA)의 Red Hat OpenShift 활용 사례에서 이미 입증되었습니다.

오픈 API를 통한 유연성 확보: 새로운 기기를 추가할 때 오픈 API를 사용하면 기존 기기와 함께 모니터링할 수 있습니다.

비용 절감: Red Hat의 서브스크립션은 독점 소프트웨어 라이센스 및 지원 계약보다 비용이 적게 듭니다.

자동화된 사이버 컴플라이언스에 대한 Red Hat의 접근 방식

Red Hat은 인프라 자동화를 통해 사이버 컴플라이언스를 강화할 수 있는 종합적인 솔루션을 제공합니다.

정상적인 활동과 비정상적인 활동을 구별하도록 머신 러닝 모델 학습: Red Hat® OpenShift®에서 AI 플랫폼인 Open Data Hub를 사용하고, 위협을 시뮬레이션하여 모델을 테스트합니다. 새로 발견된 위협과 대응 효과에 관한 데이터를 입력하여 모델을 지속적으로 업데이트합니다.

다양한 유형의 위협을 문제 해결에 매핑: Red Hat Decision Manager를 사용하여 공격자의 IP 주소 차단, 위협적이지 않은 트래픽을 허용 목록에 포함, 의심스러운 워크로드 격리, 감염된 가상 서버 중단 및 새로운 서버 가동 등과 같은 구체적인 대응을 수행합니다.

여러 기관의 모니터링 및 대응 자동화: Red Hat Ansible® Automation Platform을 사용하여 여러 기관의 방화벽과 IDS, 엣지 기기, 로그 집계를 위한 Sensu 또는 운영 사례 관리를 지원하는 ServiceNow와 같은 에코시스템 제품에서 로그를 수집합니다. Ansible Automation Platform은 플레이북의 특정 작업을 자동으로 호출합니다. 해당 작업을 통해 문제가 해결되지 않으면 Ansible Automation Platform은 경고를 전송하여 ServiceNow에 케이스를 개설합니다.

기관별로 플레이북에 대한 제어 권한 부여: 특정 서비스를 종료하기 전에 얼마나 많은 리스크를 감수할 수 있는지는 개별 기관들 스스로 잘 알고 있습니다. 기관 내 사이버 보안 팀은 Ansible Automation Platform을 통해 임계값과 호스트 이름, 플레이북을 수정할 수 있는 웹 인터페이스를 사용하여 업무 요건을 충족할 수 있습니다.

자세히 알아보기: Red Hat에서 공공 부문의 IT 혁신을 지원하는 방식을 https://www.redhat.com/ko/solutions/public-sector에서 살펴보세요.

한국레드햇 홈페이지 https://www.redhat.com/ko

RED HAT 정보

Red Hat은 세계적인 엔터프라이즈 오픈소스 솔루션 공급업체로서 커뮤니티 기반 접근 방식을 통해 신뢰도 높은 고성능 Linux, 하이브리드 클라우드, 컨테이너, 쿠버네티스 기술을 제공합니다. 또한 고객으로 하여금 신규 및 기존 IT 애플리케이션을 통합하고, 클라우드 네이티브 애플리케이션을 개발하며, 업계를 선도하는 Red Hat의 운영 체제를 기반으로 표준화하는 동시에 복잡한 환경의 자동화, 보안 및 관리를 실현할 수 있도록 지원합니다. Red Hat은 전 세계 고객에게 높은 수준의 지원과 교육 및 컨설팅 서비스를 제공하여 권위있는 어워드를 다수 수상한 바 있으며, Fortune 선정 500대 기업의 신뢰를 받는 어드바이저로 인정받고 있습니다. 또한 기업, 파트너, 오픈소스 커뮤니티의 전략적인 파트너로서 고객들이 디지털 미래에 대비할 수 있도록 지원하고 있습니다.

www.facebook.com/redhatkorea
구매문의 080 708 0880
buy-kr@redhat.com

www.redhat.com/ko
#F26748_0121