2019의 주요 기능

2019년 11월

2019년 11월

Firepower Threat Defense 6.5.0을 실행하는 디바이스에 대한 **CDO** 지원

이제 CDO에서 FTD 6.5.0 디바이스를 관리합니다. 다음은 CDO가 제공하는 지원 측면입니다.

- Firepower Threat Defense(FTD) 6.5.0을 실행하는 디바이스 온보딩
- Firepower 4100 및 Firepower 9300과 같은 추가 Firepower 시리즈 디바이스를 지원합니다.
- Microsoft Azure에서 가상 FTD 인스턴스를 지원합니다. 지원되는 디바이스의 전체 목록은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Firepower Threat Defense 지원 세부 사항"을 참조하십시오.
- 디바이스는 개별 FTD 또는 고가용성 쌍으로 구성된 FTD일 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Firepower 소프트웨어 업그레이드 경로"를 참조하십시오. 다음 주의 사항은 업그레이드 지원에 적용됩니다.
  - 디바이스가 관리용 데이터 인터페이스를 사용하는 경우 6.5.0을 실행하는 FTD에 대해서는 HA 쌍 업그레이드가 지원되지 않습니다.
  - Firepower 4100 및 Firepower 9300 디바이스의 업그레이드는 현재 지원되지 않습니다.

- 고객은 CDO의 업그레이드 페이지에 있는 드롭다운을 사용하여 FTD 6.5.0으로 업그레이드할 수 있습니다. 6.5 이미지 다운로드를 위해 디바이스에 제공되는 링크는 HTTP입니다. 이는 다운로드가 HTTPS를 통해 수행된 경우보다 이미지 다운로드 시간이 약간 더 길어질 수 있음을 의미합니다. 또한 FTD의 아웃바운드 HTTP 트래픽이 차단되면 이미지 다운로드가 실패합니다.

- Firepower 1010에 FTD 6.5.0이 설치되면 일반 방화벽 인터페이스 또는 레이어 2 하드웨어 스위치 포트로 실행되도록 인터페이스를 구성할 수 있습니다. 현재 CDO의 스위치 모드 지원은 읽기 전용입니다. 스위치 포트 모드에 대한 인터페이스를 생성하거나 수정하려면 FDM 콘솔을 사용합니다. CDO는 Firepower 1010s에서 스위치 포트 모드에 대한 지원을 계속 개발하고 있으며, 완전한 지원이 제공되는 경우 새로운 기능에서 발표할 예정입니다.
- 등록 토큰을 사용하여 FTD 6.5.0 디바이스를 온보딩하는 경우, 보안 이벤트 커넥터를 사용하지 않고 연결 이벤트, 파일 및 악성코드 이벤트, 침입 이벤트를 Cisco Cloud에 직접 전송할 수 있습니다. Cisco Defense Orchestrator를 사용하여 FTD 관리의 "Cisco Security Analytics 및 로깅 구현"을 참조하십시오.
- FTD 6.4.x 기능에 대한 지속적인 지원. CDO는 FTD 6.5 기능에 대한 지원을 지속적으로 개발하고 있으며 준비가 완료되는 대로 지원을 릴리스할 예정입니다.

CDO에서 지원하는 FTD 기능에 대한 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리를 참조하십시오.

사이트 간 **VPN** 연결에 대한 **IKEv1** 지원

이제 CDO에서 IKEv1(Internet Key Exchange 버전 1)을 사용하여 사이트 간 VPN 터널을 생성할 수 있습니다. 이는 IKEv2(Internet Key Exchange 버전 2)를 지원하지 않는 레거시 방화벽에서 사이트 간 VPN을 구성하는 데 도움이 됩니다. IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "사이트 간 가상 프라이빗 네트워크"를 참조하십시오.

Firepower Threat Defense 템플릿 개선

이제 CDO에서 FTD 템플릿의 일부 측면을 매개변수화하여 템플릿을 추가로 사용자 지정할 수 있습니다. 자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "FTD 템플릿 구성"을 참조하십시오.

스마트 라이선스 관리

이제 CDO 내에서 Firepower Threat Defense 디바이스용 Cisco 스마트 라이선스를 관리할 수 있습니다. 스마트 라이선싱은 워크플로우에 편리하게 내장되어 있으며 CDO 인터페이스에서 쉽게 액세스할 수 있습니다. 이제 CDO 내에서 다음 Cisco 스마트 라이선싱 작업을 수행할 수 있습니다.

- 등록 토큰을 사용하여 FTD 디바이스를 온보딩하는 동안 스마트 라이선스 적용
- 디바이스에 적용된 라이선스 보기

- Cisco Smart Software Manager로 라이선스 등록
- 디바이스에 대해 서로 다른 라이선스 유형 활성화 및 비활성화

자세한 내용은 Cisco Defense Orchestrator를 사용하여 FTD 관리의 "등록 토큰을 사용하여 Firepower Threat Defense 디바이스 온보딩" 및 "온보딩된 FTD 스마트 라이선싱"을 참조하십시오.

2019년 10월

2019년 10월

Amazon Web Services 지원

이제 CDO가 AWS VPC를 관리합니다!

AWS(Amazon Web Services) VPC(Virtual Private Cloud)는 AWS 어카운트와 연결된 가상 프라이빗 클라우드를 사용자에게 제공하는 상업용 클라우드 컴퓨팅 서비스입니다. 이 네트워크는 자체 데이터 센터에서 운영하는 기존 네트워크와 매우 유사하며 AWS의 확장 가능한 인프라를 사용한다는 이점이 있습니다.

CDO는 개체 및 규칙의 문제를 식별하고 해결 방법을 제공하여 AWS VPC를 최적화하도록 도와줍니다. CDO 사용:

- FTD 또는 ASA 디바이스와 함께 AWS VPC 환경을 관리합니다.
- AWS VPC와 연결된 모든 보안 그룹 규칙을 동시에 관리합니다.
- FTD 및 ASA 디바이스와 같이 지원되는 다른 플랫폼에서 호환되는 개체로 보안 그룹 규칙을 생성하고 맞춤화합니다.
- AWS VPC 사이트 간 VPN 연결을 봅니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리를 참조하십시오.

CDO를 사용하여 **ASA**를 **FTD** 디바이스로 마이그레이션

CDO는 ASA(Adaptive Security Appliance)를 FTD(Firepower Threat Defense) 디바이스로 마이그레이션하는 데 도움이 됩니다. CDO는 ASA에서 실행 중인 구성의 다음 요소를 FTD 템플릿으로 마이그레이션하는 데 도움이 되는 마법사를 제공합니다.

- 인터페이스
- 경로
- ACL(액세스 제어 규칙)
- NAT(네트워크 주소 변환) 규칙
- 네트워크 개체 및 네트워크 그룹 개체

- 서비스 개체 및 서비스 그룹 개체

구성을 실행하는 ASA의 이러한 요소가 FTD 템플릿으로 마이그레이션되면 CDO에서 관리하는 새 FTD 디바이스에 FTD 템플릿을 적용할 수 있습니다. FTD 디바이스는 템플릿에 정의된 구성을 채택하므로 이제 FTD가 ASA에서 실행 중인 구성의 일부 측면으로 구성됩니다.

CDO를 사용하여 ASA를 FTD로 마이그레이션하는 프로세스에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA를 FTD로 마이그레이션 워크플로우"를 참조하십시오.

Cisco, Cisco Secure Sign-on 및 **Duo Multi-Factor Authentication**을 사용하는 새로운 **SSO(Single Sign-On)** 솔루션 소개

CDO는 이 새로운 솔루션을 채택하고 고객 테넌트를 Cisco Secure Sign-on IdP(Identity Provider) 및 Duo Security 다단계 인증자로 변환합니다.

Cisco Secure Sign-On을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 강력하고 탄력적인 **ID**: AICPA SOC 2, CSA-Star 및 ISO 27001을 포함하여 가장 높은 업계 표준을 충족하는 보안입니다. 또한 고객을 위해 분리된 FedRAMP 및 HIPAA 환경을 지원합니다.
- **Duo MFA(Multi-Factor Authentication)**: Cisco Secure Sign-On과 통합된 Duo MFA는 적응형, 계층화된, 간소화된 인증을 의미합니다. 푸시 알림 한 번, 탭 한 번으로 즉시 액세스
- 원활한 워크플로우를 위한 **SSO(Single Sign-In)**: 단일 사용자 이름과 비밀번호를 입력하면 모든 디바이스에서 모든 애플리케이션에 액세스하는 동시에 워크플로우 전체에서 상황을 유지할 수 있습니다.
- 맞춤형 환경: Cisco Secure Sign-On 대시보드에서 업무용 앱을 원하는 방식으로 정렬할 수 있습니다. 탭과 검색 창을 사용하면 정리할 수 있습니다.

Note

- 자체 SSO(Single Sign-On) ID 제공자를 사용하여 CDO에 로그인하는 경우 Cisco Secure Sign-On 및 Duo로의 전환이 영향을 미치지 않습니다. 고유한 로그인 솔루션을 계속 사용합니다.
- CDO 무료 평가판을 사용 중인 경우 이 전환이 영향을 미칩니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *AWS* 관리의 "Cisco Secure Sign-On ID 제공자로 마이그레이션"을 참조하십시오.

Cisco Security Analytics and Logging(Secure Cloud Analytics와의 통합 포함)

Cisco Security Analytics and Logging은 네트워크 가시성을 개선하여 실시간으로 위협을 신속하게 탐지하고 대규모로 자신 있게 인시던트를 치료할 수 있습니다.

Cisco Security Analytics and Logging을 사용하면 모든 FTD(Firepower Threat Defense) 디바이스에서 연결, 침입, 파일, 악성코드 및 보안 인텔리전스 이벤트를 캡처하여 CDO의 한 곳에서 볼 수 있습니다.

이벤트는 Cisco Cloud에 저장되며 CDO의 Event Logging(이벤트 로깅) 페이지에서 볼 수 있습니다. 이 페이지에서 이벤트를 필터링하고 검토하여 네트워크에서 트리거되는 보안 규칙을 명확하게 파악할 수 있습니다. Logging and Troubleshooting(기록 및 문제 해결) 패키지는 이러한 기능을 제공합니다.

방화벽 분석 및 모니터링 패키지를 통해 시스템은 FTD 이벤트에 Secure Cloud Analytics 동적 엔티티 모델링을 적용하고 행동 모델링 분석을 사용하여 Secure Cloud Analytics 관찰 및 알림을 생성할 수 있습니다. 전체 네트워크 분석 및 모니터링 패키지를 구입하는 경우 시스템은 FTD 이벤트와 네트워크 트래픽 모두에 동적 엔터티 모델링을 적용하고 관찰 및 알림을 생성합니다. Cisco SSO(Single Sign-On, 단일 인증)를 사용하여 CDO에서 사용자에게 프로비저닝된 Secure Cloud Analytics 포털로 교차 실행할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "Cisco Security Analytics and Logging"을 참조하십시오.

2019년 9월

2019년 9월

등록 토큰을 사용하여 **Firepower Threat Defense** 디바이스 온보딩

이제 IP 주소, 사용자 이름 및 비밀번호를 사용하는 대신 등록 토큰을 사용하여 FTD 디바이스를 온보딩할 수 있습니다. 이는 DHCP를 사용하여 FTD에 IP 주소가 할당된 경우 특히 유용합니다. 어떤 이유로 해당 IP 주소가 변경되어도 FTD는 CDO에 연결된 상태로 유지됩니다. 또한 FTD는 로컬 영역 네트워크에 주소를 가질 수 있으며, 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.

이 온보딩 방법은 현재 FTD 6.4 릴리스 및 defenseorchestrator.cisco.com에 연결하는 고객에게 제공됩니다. defenseorchestrator.cisco.eu에 연결하는 고객은 아직 사용할 수 없습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "등록 키로 FTD 온보딩"을 참조하십시오.

2019년 8월

2019년 8월

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging은 네트워크 가시성을 개선하여 실시간으로 위협을 신속하게 탐지하고 대규모로 자신 있게 인시던트를 치료할 수 있습니다.

Firepower Threat Defense를 위한 원격 액세스 VPN 지원

RA(Remote Access) VPN을 통해 개인은 지원되는 노트북 컴퓨터, 데스크톱 및 모바일 디바이스를 사용하여 네트워크에 대한 보안 연결을 설정할 수 있습니다. CDO는 온보딩한 FTD(Firepower Threat Defense) 디바이스에서 RA VPN을 설정할 수 있는 직관적인 사용자 인터페이스를 제공합니다.

AnyConnect는 RA VPN 연결을 제공하는 엔드포인트 디바이스에서만 지원되는 클라이언트입니다.

CDO는 FTD 디바이스에서 RA VPN 기능의 다음 측면을 지원합니다.

- 프라이버시, 인증 및 데이터 무결성을 위한 TLS(Transport Layer Security) 또는 DTLS(Datagram Transport Layer Security)
- SSL 클라이언트 기반 원격 액세스
- IPv4 및 IPv6 주소 지정
- 여러 FTD 디바이스에서 공유 RA VPN 구성

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "원격 액세스 가상 사설 네트워크"를 참조하십시오.

Firepower Threat Defense 고가용성 이미지 업그레이드 지원

이제 CDO에서 FTD HA 쌍을 업그레이드할 수 있습니다. 장애 조치 쌍을 업그레이드할 때 CDO는 원하는 업그레이드 이미지를 두 디바이스에 모두 복사합니다. CDO는 기본 디바이스가 활성 모드가 아닌 경우 임시로 해당 모드를 이동한 다음 보조 디바이스를 업그레이드합니다. 보조 디바이스가 성공적으로 업그레이드되면 기본 디바이스가 업그레이드됩니다. 장애 조치 쌍은 네트워크 중단을 최소화하기 위해 디바이스를 한 번에 하나씩 업그레이드합니다.

장애 조치 쌍을 업그레이드하려면 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 고가용성 쌍 업그레이드"를 참조하십시오.

Firepower Threat Defense 디바이스를 위한 사이트 간 VPN

이제 Firepower Threat Defense 디바이스를 위한 사이트 간 VPN이 정식 출시되었습니다!

CDO를 사용하면 서로 다른 지리적 위치에 있는 두 사이트 간에 보안 연결을 설정할 수 있습니다. 이러한 피어는 IPv4와 IPv6 주소를 사용하여 내부 주소와 외부 주소를 함께 포함할 수 있습니다. Site-to-Site 터널은 IPsec(Internet Protocol Security) 프로토콜 제품군 및 인터넷 키 교환 버전 2(IKEv2)를 사용하여 구축됩니다. VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. CDO에 온보딩된 디바이스에 대해 다음 시나리오에서 사이트 간 IPsec 연결을 생성할 수 있습니다.

- 두 매니지드 디바이스 간
- 매니지드 디바이스와 다른 Cisco 피어 간
- 매니지드 디바이스와 서드파티 피어 간

Firepower Threat Defense 고가용성 지원

CDO는 Firepower Threat Defense 방화벽에 대한 고가용성(HA) 지원을 일반 공급합니다! 이제 기존 HA 쌍을 온보딩하거나 CDO에서 HA 쌍을 생성할 수 있습니다. HA 구성을 사용하면 업그레이드 기간 또는 예기치 않은 디바이스 장애와 같이 디바이스를 사용할 수 없는 시나리오에서 보안 네트워크를 유지할 수 있습니다. 장애 조치 모드에서 스탠바이 디바이스는 이미 액티브 상태가 되도록 구성되어 있습니다. 즉, HA 디바이스 중 하나를 사용할 수 없는 경우에도 다른 디바이스가 트래픽을 계속 처리합니다.

독립형 FTD 디바이스에 지원되는 대부분의 기능은 HA에 대해 구성된 디바이스도 지원합니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "FTD 고가용성"을 참조하십시오.

제공 예정... FTD HA 업그레이드 지원 현재 HA 쌍을 업그레이드해야 하는 경우에는 액티브 디바이스의 FDM 콘솔을 통해 업그레이드를 실행해야 합니다.

2019년 7월

2019년 7월

ASA 디바이스에 대한 시간 범위 개체

이제 시간 범위 개체를 사용하여 네트워크 정책의 규칙을 맞춤화할 수 있습니다. 이러한 개체를 사용하면 일회성 또는 반복 규칙을 실행하고 네트워크에서 트래픽을 처리하는 방법을 맞춤화할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 시간 범위 개체"를 참조하십시오.

Firepower Threat Defense 지원

CDO는 일반적으로 사용 가능한 Firepower Threat Defense 방화벽에 대한 지원을 제공합니다!

CDO는 Firepower Threat Defense 디바이스에 대한 간소화된 관리 인터페이스 및 클라우드 액세스를 원하는 방화벽 관리자를 위해 설계되었습니다. FDM(Firepower Device Manager) 관리자는 FDM 인터페이스와 CDO 인터페이스 간에 많은 유사성을 확인할 수 있습니다. 관리자 간에 가능한 한 일관성을 유지하기 위해 CDO를 구축했습니다.

이제 CDO는 ASA 5508-x, ASA 5515-x, ASA 5525-x, ASA 5545-x, ASA 5555-x, FTD 2100 시리즈 디바이스, FTD 1000 시리즈 디바이스 또는 가상 FTD 디바이스에 설치되었을 때 FTD 버전 6.4.0 이상을 실행하는 Firepower Threat Defense(FTD) 디바이스를 관리할 수 있습니다.

CDO를 사용하여 물리적 또는 가상 FTD(Firepower Threat Defense) 디바이스의 다음 측면을 관리합니다.

- 디바이스 관리
- 디바이스 업그레이드
- 인터페이스 관리

- 라우팅
- 보안 정책
- 정책 및 구성 일관성 승격
- 변경 추적
- 네트워크 모니터링

Firepower 1000 Series 및 Virtual FTD를 포함하여 모든 CDO FTD PID는 CCW에서 주문할 수 있습니다. PID는 플랫폼에 따라 다르지만 ASA 및 FTD에 공통적으로 적용됩니다. 자세한 내용은 Salesconnect의 주문 가이드를 참조하십시오.

지원되는 기능에 대한 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리를 참조하십시오.

Meraki MX 지원

이제 CDO에서 Meraki MX 방화벽 정책을 관리합니다!

Meraki MX는 분산형 구축을 위해 설계된 엔터프라이즈 보안 및 소프트웨어 정의 광역 네트워크(SD-WAN) 차세대 방화벽 어플라이언스입니다. 이제 Cisco Defense Orchestrator를 사용하여 Meraki MX 디바이스에서 레이어 3 네트워크 규칙을 관리할 수 있습니다.

CDO는 개체 및 정책의 문제를 식별하고 해결 방법을 제공하여 Meraki 환경을 최적화하도록 도와줍니다. 이는 디바이스 및 템플릿 모두에 연결된 정책에 적용됩니다.

CDO를 사용하여 다음을 수행합니다.

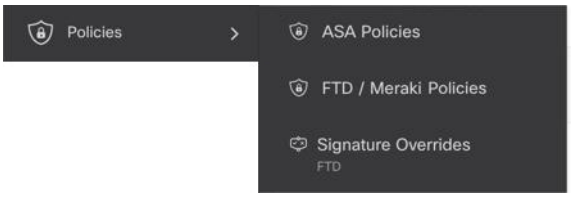
- 하나 이상의 Meraki 디바이스에서 정책을 동시에 관리합니다.
- 모든 환경에서 FTD 및 ASA 디바이스와 함께 Meraki 정책 또는 템플릿을 모니터링하고 관리합니다.
- Meraki 템플릿을 사용하여 여러 네트워크를 관리합니다.
- FTD 및 ASA 디바이스와 같이 지원되는 다른 플랫폼에서 호환되는 개체로 액세스 규칙을 맞춤화합니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *Meraki* 관리를 참조하십시오.

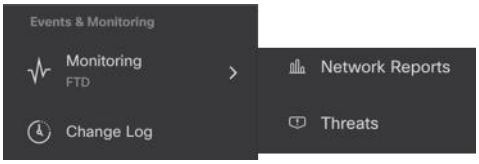
업데이트된 **GUI** 탐색

CDO의 UI 탐색이 더 쉬워졌습니다.

이제 내비게이션 바의 정책 메뉴에서 디바이스 또는 기능별로 그룹화된 정책을 안내합니다. Cisco에서는 현재 테넌트에 있는 정책에 연결하는 데 필요한 메뉴 경로만 노출합니다.



FTD의 모든 모니터링 기능은 내비게이션 바의 **Events & Monitoring(**이벤트 및 모니터링**)** 영역에서 그룹화됩니다. Monitoring(모니터링) 메뉴에는 **Network Reports(**네트워크 보고서**)** 및 **Threats(**위협**)**가 표시됩니다.



2019년 5월

2019년 5월

디바이스 연결 문제 해결

이 툴을 사용하면 SDC(Secure Device Connector)와 디바이스 간의 연결 문제를 테스트하거나 트러블슈팅할 수 있습니다. 디바이스가 온보딩에 실패하거나 온보딩 전에 CDO가 디바이스에 연결할 수 있는지 확인하려는 경우 이 연결을 테스트할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *FTD* 관리의 "SDC를 사용하여 보안 디바이스 커넥터 문제 해결"을 참조하십시오.

2019년 4월

2019년 4월

CDO 사용자 환경을 개선하는 데 도움이 될 수 있습니다.

저희는 귀하의 CDO 사용자 경험에 대해 알고자 하며, 이제 저희에게 쉽게 알려줄 수 있습니다. CDO 포털에서 나가지 않고도 피드백을 제공할 수 있도록 Help(도움말) 메뉴에 **Provide Feedback(**피드백 제공**)** 버튼을 추가했습니다. 마음에 드는 점과 개선할 점을 알려주십시오.

피드백을 남길 때 귀사에서 귀하의 역할을 알려주십시오. 네트워크 운영 센터, 보안 운영 센터에 있습니까? 아니면 모든 IT 센터에 있습니까? 완료하려는 작업을 알려주십시오. 보안 정책을 수정하거나 변경 로그에서 항목을 찾으십니까?

피드백을 남기는 방법은 다음과 같습니다.

단계 **1** CDO에 로그인합니다.

단계 **2** 테넌트 및 계정 이름 옆에 있는 help(도움말) 버튼을 클릭하고 **Provide Feedback(**피드백 제공**)**을 선택합니다.

단계 **3** 피드백을 입력하고 **Send Email(**이메일 전송**)**을 클릭합니다. 이렇게 하면 로컬 메일 서버에 수동으로 전송해야 하는 이메일이 생성됩니다.

Cisco 지원 담당자가 최대한 빨리 응답해 드리겠습니다.

2019년 2월

2019년 2월

보안 디바이스 커넥터에 영향을 주는 컨테이너 권한 에스컬레이션 취약점**: cisco-sa-20190215-runc**

Cisco PSIRT(제품 보안 사고 대응 팀)는 Docker의 심각도가 높은 취약성에 대해 설명하는 보안 자문 **cisco-sa-20190215-runc**를 게시했습니다. 취약성에 대한 전체 설명은 전체 PSIRT 팀 자문을 참조하십시오.

이 취약성은 모든 CDO 고객에게 영향을 미칩니다.

- CDO의 클라우드 구축 SDC(Secure Device Connector)를 사용하는 고객은 CDO 운영 팀에서 교정 단계를 이미 수행했으므로 아무 작업도 수행할 필요가 없습니다.
- 온프레미스에 구축된 SDC를 사용하는 고객은 최신 Docker 버전을 사용하도록 SDC 호스트를 업그레이드해야 합니다.

CDO 표준 SDC 호스트 및 맞춤형 SDC 호스트를 업데이트하는 방법에 대한 지침은 보안 디바이스 커넥터에 영향을 미치는 컨테이너 권한 에스컬레이션 취약성: cisco-sa-20190215-runc를 참조하십시오.

ASA 디바이스 대량 온보딩 시 레이블 추가

이제 ASA 디바이스를 대량 온보딩할 때 맞춤형 디바이스 레이블을 지정할 수 있습니다. 자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "ASA 대량 온보딩"을 참조하십시오.

Cisco IOS 디바이스 지원

CDO(Cisco Defense Orchestrator)를 사용하면 Cisco IOS 디바이스를 관리할 수 있습니다. 이러한 디바이스에 대해 지원되는 기능은 다음과 같습니다.

- Cisco IOS 디바이스 온보딩
- 디바이스 구성 보기
- 디바이스에서 정책 및 구성 변경 종료

- 대역 외 변경 사항 탐지
- 명령줄 인터페이스 지원
- 개별 CLI 명령 및 명령 그룹을 편집 및 재사용 가능한 매크로로 전환할 수 있습니다.
- SSH 핑거프린트 변경 사항 탐지 및 관리
- 변경 로그에서 IOS 디바이스에 대한 변경 사항 보기

자동 구축 예약

CDO를 사용하여 하나 이상의 디바이스에 대한 구성을 변경한 후에는 편리한 날짜와 시간에 해당 디바이스에 대한 구축을 예약할 수 있습니다. 예를 들어 유지 보수 기간 동안 또는 네트워크 트래픽이 적은 시간에 구축이 이루어지도록 예약할 수 있습니다.

자세한 내용은 *Cisco Defense Orchestrator*를 사용하여 *ASA* 관리의 "자동 구축 예약 옵션 활성화" 및 "자동 구축 예약"을 참조하십시오.

용어 변경: **CDO**가 관리하는 디바이스에 변경 사항 **"구축"**

디바이스 구성의 CDO 로컬 복사본에 대한 변경 사항을 디바이스 자체로 전송하는 것을 설명하는 용어를 업데이트했습니다. 이전에는 "쓰기"라는 단어를 사용하여 해당 전송을 설명했지만 이제는 "구축"이라는 단어를 사용하여 해당 전송을 설명합니다.

CDO를 사용하여 디바이스의 구성을 관리하고 변경하면 CDO는 변경 사항을 구성 파일의 자체 복사본에 저장합니다. 이러한 변경 사항은 디바이스에 "구축"될 때까지 CDO에서 "준비된" 것으로 간주됩니다. 준비된 구성 변경은 디바이스를 통해 실행되는 네트워크 트래픽에 영향을 주지 않습니다. CDO가 디바이스에 변경 사항을 "구축"한 후에야 디바이스를 통해 실행되는 트래픽에 영향을 미칩니다. CDO는 디바이스의 구성에 변경 사항을 구축할 때 변경된 구성의 요소만 덮어씁니다. 디바이스에 저장된 전체 구성 파일을 덮어쓰지 않습니다.