프록시 디바이스 업로드

프록시 디바이스 업로드

Cisco Secure Web Appliance(구 Web Security Appliance 또는 WSA)와 Blue Coat ProxySG 같은 프록시 디바이스의 로그 파일에 있는 텔레메트리 데이터를 분석을 위해 전역 위협 알림 시스템에 업로드합니다.

단계 **1** 페이지 오른쪽 상단에 있는 톱니바퀴 아이콘을 클릭하고 **Device Accounts(**디바이스 계정**)**를 선택하여 설정 마법사를 엽니다.

참고 기존 디바이스 계정이 이미 하나 이상 있다면 설정을 건너뛰고 Device Accounts(디바이스 계정) 페이지가 표시됩니다.

단계 **2** 설정 마법사를 시작하여 디바이스 계정을 추가할 준비가 되면 **Let's Get Started(**시작하기**)**를 클릭합니다.

단계 **3** 드롭다운에서 자동 또는 수동 업로드를 선택하여 텔레메트리 데이터를 디바이스에서 업로드하는 방법을 선택합니다. 전역 위협 알림 시스템은 한 번에 하나의 업로드 방법만 지원합니다. 업로드 방법을 결합할 수는 없습니다.

참고 자동 업로드에서 수동 업로드로 전환하려면 먼저 모든 프록시 디바이스를 자동 업로드 구성에서 제거해야 합니다.

단계 **4** 자동 업로드 방법을 선택했다면, 로그 파일을 전송하는 데 사용할 프로토콜로 **SCP** 또는 **HTTPS**를 선택합니다.

a) 이 디바이스의 이름을 입력하고 **Add Account(**계정 추가**)**를 클릭합니다.

b) SCP를 선택한 경우:

- 정보(호스트, 포트, 디렉터리, 사용자 이름)를 복사하여 Cisco WSA 컨피그레이션에 붙여넣습니다. 보안 유지를 위해 정보는 한 번만 표시됩니다.
- Cisco WSA를 구성하는 자세한 방법은 로그 파일을 Cisco 전역 위협 알림에 업로드하도록 Cisco Secure Web Appliance 구성을 참고하십시오.
- Cisco WSA Management Console에서 공개 SSH 키를 반환하면, 공개 SSH 키를 복사하여 디바이스 계정에 붙여넣습니다.

프록시 디바이스 업로드

- 마침을 클릭합니다.
- 원한다면 Device Accounts(디바이스 계정) 페이지로 이동하고 디바이스를 클릭하여 나중에 공개 SSH 키를 입력해도 됩니다.

c) HTTPS를 선택한 경우:

- 정보(호스트, 포트, 경로, 사용자 이름, 비밀번호)를 복사하여 Blue Coat ProxySG 컨피그레이션에 붙여넣습니다.
- Blue Coat ProxySG를 구성하는 자세한 방법은 로그 파일을 Cisco 전역 위협 알림에 업로드하도록 Blue Coat ProxySG 구성을 참고하십시오.
- 마침을 클릭합니다.

단계 **5** 수동 업로드 방법을 선택한 경우:

a) 로그 파일의 형식을 검증합니다. 다음 준비 지침을 따릅니다.

- Cisco WSA 및 Blue Coat 프록시에서 생성한 W3C 로그 파일이 지원됩니다.
- 모든 로그 파일은 GZip(*.gz) 형식으로 압축해야 합니다.
- 각 로그 파일은 1GB보다 작아야 합니다. 1GB보다 큰 로그 파일은 복수의 작은 파일로 분할해야 합니다. 개별 시간 간격이 중복되지 않으며 모든 파일에 동일한 올바른 헤더가 포함되어 있는지 확인합니다.
- 로그 파일이 적용되는 총 시간 간격은 2일을 초과해야 합니다.
- 각 로그 파일은 중복되지 않는 특정 시간 간격을 대상으로 해야 합니다.
- 각 로그 파일은 로그 항목을 시간 오름차순으로 포함해야 합니다. 즉 이전 항목이 새 항목 앞에 와야 합니다.
- 로그 파일은 알파벳순/숫자순으로 정렬하고 시간 순으로 업로드해야 합니다. 즉 이전 파일을 새 파일보다 먼저 업로드해야 합니다. 단일 업로드에서 업로드 구성 요소가 파일을 자동으로 정렬합니다. 여러 번 업로드한다면, 항상 최신 데이터를 업로드해야 합니다. 프록시 로그 파일에서 기본적으로 사용하는 명명 규칙이 유지된다면, 파일 이름이 이미 올바르게 정렬되었다는 뜻입니다.
- 이전에 업로드한 데이터보다 오래된 데이터는 처리되지 않습니다.
- 업로드할 수 있으려면 로그 파일의 콘텐츠가 특정 기준을 충족해야 합니다.
  - 업로드하기 전에 로그 파일을 확인할 수 있는 Log Validation Tool이 제공됩니다.
  - 로그 파일의 처음 20개 행을 복사하고 Log Validation Tool에 붙여넣어 오류를 확인합니다.
  - 모든 오류가 표시되며, 사용자가 오류를 수정하는 동안 툴이 자동으로 오류를 계속 확인합니다.

b) **Add files(**파일 추가**)**를 클릭하여 업로드할 로그 파일을 선택하거나 로그 파일을 업로드 상자에 끌어다 놓습니다.

참고 업로드 상자에 추가된 모든 파일을 지우려면 **Clear files(**파일 지우기**)**를 클릭합니다.

c) **Start upload(**업로드 시작**)**를 클릭하면 선택된 로그 파일이 분석을 위해 전역 위협 알림 시스템에 업로드됩니다. 전역 위협 알림 시스템에 결과가 표시될 때까지 기다립니다.

참고 데이터 삭제 위험을 최소화하기 위해 전역 위협 알림 시스템은 5시간이 지나야 업로드된 데이터 처리를 시작합니다. 따라서 처리를 시작하기 전에 모든 업로드를 완료하고 모든 요소가 올바른지 확인할 수 있습니다.

주의 수동에서 자동으로 전환하면 모든 업로드가 즉시 중단되고 업로드된 데이터의 처리가 중단됩니다. 업로드된 데이터가 모두 삭제됩니다.

참고 페이지를 닫거나 다른 페이지로 이동하면 현재 파일 업로드가 모두 중단됩니다.

참고 자동 업로드를 사용하려면 먼저 모든 수동 업로드를 중단해야 합니다. 모든 데이터가 처리되기 전에 전환하면 전환에서 일부 분석 데이터가 손실될 수 있습니다. 시스템에서 데이터를 삭제하지 않도록, 마지막 수동 업로드로부터 24시간이 지난 후에 전환을 수행하십시오.

다음에 수행할 작업

Device Accounts(디바이스 계정) 페이지에 프록시 디바이스와 관련 정보가 나열됩니다. Status(상태) 열에는 각 디바이스의 상태가 표시됩니다.

- New(신규) - SCP에 대한 컨피그레이션이 완료되지 않았습니다. 공개 SSH 키가 누락되었을 수 있습니다.
- Provisioning(프로비저닝) - 계정을 프로비저닝하는 중이며, 아직 준비되지 않았습니다.
- Ready(준비) - 계정이 생성되었습니다.
- Error(오류) - 상태 위에 커서를 올리면 오류를 설명하는 팝업 메시지가 표시됩니다.

이 개요 페이지에서는 다른 디바이스 계정을 추가하거나, 임의의 디바이스를 클릭하여 제거하거나, 공개 SSH 키를 입력하거나, 문제를 해결할 수 있습니다.

여러 디바이스 또는 업로드 프로세스 간에 계정을 공유할 수 있지만, 파일 이름 충돌 가능성을 최소화하고 업로드 문제 해결을 간소화할 수 있도록 각 디바이스에 별도의 계정을 사용하는 것이 좋습니다.

디바이스 계정이 준비되면 **Confirmed(**확인됨**)** 또는 **Detected(**탐지됨**)** 페이지를 클릭하여 네트워크 상의 의심스러운 활동에 관한 정보를 확인합니다.

참고 데이터는 일반적으로 프로비저닝이 완료된 후 2~3일 이내에 사용할 수 있습니다.

프록시 디바이스 업로드