IBM Security QRadar Incident Forensics

버전 7.3.0

관리 안내서

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 37 페이지의 『주의사항』의 정보를 읽으십시오.

제품 정보

본 문서는 본 문서의 업데이트된 버전에서 달리 대체되지 않는 한, IBM QRadar Security Intelligence Platform V7.3.0 및 후속 릴리스에 적용됩니다.

목차

IBM Security QRadar Incident Forensics 관리 소개

IBM® Security QRadar® Incident Forensics 관리에 대한 정보입니다.

대상 독자

관리자는 조사자라고 하는 사용자가 보안 인시던트 또는 케이스 조사 및 데이터 탐색에 초점을 맞출 수 있도록 활성 포렌식 기능을 작성, 유지보수 및 조작합니다.

기술 문서

번역된 모든 문서를 포함하여 IBM Security QRadar 제품 문서를 웹에서 찾으려면 IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)에 액세스하십시오.

QRadar 제품 라이브러리에 있는 추가 기술 문서에 액세스하는 방법에 대한 정보는 IBM 보안 문서 기술 노트 액세스(www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)를 참조하십시오.

고객 지원 문의

고객 지원 문의에 대한 정보는 지원 및 기술 노트 다운로드 (http://www.ibm.com/support/docview.wss?uid=swg21616144)를 참조하십시오.

우수 보안 관리제도에 대한 설명

IT 시스템 보안은 귀사 내/외부로부터의 부적절한 접근을 방지, 감지, 대응함으로써 시스템과 정보를 보호하는 일을 포함합니다. 부적절한 접근은 정보의 변경, 파괴 또는 유용을 초래하거나, 타 시스템에 대한 공격을 포함한 귀사 시스템에 대한 피해나 오용을 초래할 수 있습니다. 어떠한 IT 시스템이나 제품도 완벽하게 안전할 수 없으며, 단 하나의 제품이나 보안 조치만으로는 부적절한 접근을 완벽하게 방지하는 데 효과적이지 않을 수 있습니다. IBM 시스템, 제품 및 서비스는 합법적이며 종합적인 보안 접근방법의 일부로서 고안되며, 이러한 접근방법은 필연적으로 추가적인 실행절차를 수반하며 가장 효과적이기 위해서는 다른 시스템, 제품 또는 서비스가 필요할 수도 있습니다. IBM은 시스템, 제품 또는 서비스가 임의의 당사자의 악의적 또는 불법적 행위로부터 영향을 받지 않는다는 것을 보장하지는 않습니다.

참고:

본 프로그램의 사용은 개인 정보, 정보 보호, 고용, 전기 통신 및 저장과 관련된 법률 또는 규정을 포함하여 다양한 법률 또는 규정과 연관될 수 있습니다. IBM Security QRadar는 합법적인 목적과 합법적인 방법으로만 사용될 수 있습니다. 고객은 적용되는 법률, 규정 또는 정책에 의거하여 본 프로그램을 사용하고, 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다. 라이센스 사용자는 IBM Security QRadar의 합법적인 사용이 가능하게 하기 위해 필요한 모든 동의, 허가 및 라이센스를 이미 취득했거나 취득할 것임을 진술하고 보증합니다.

참고

IBM Security QRadar Incident Forensics는 회사의 보안 환경 및 데이터 개선을 돕기 위해 디자인되었습니다. 보다 구체적으로 설명하면 IBM Security QRadar Incident Forensics는 회사에서 네트워크 보안 인시턴스에 발생하는 상황을 조사하고 더 자세히 파악할 수 있도록 돕기 위해 디자인되었습니다. 이 도구를 사용하여 회사들은 캡처된 네트워크 패킷 데이터(PCAP)를 인덱싱하여 검색하고 이러한 데이터를 다시 원래 형식으로 재구성할 수 있습니다. 이 재구성 기능으로 이메일 메시지, 파일 및 그림 첨부 파일, VoIP 전화 통화, 웹 사이트를 비롯한 데이터와 파일을 재구성할 수 있습니다. 이 프로그램의 기능 및 이러한 기능의 구성 방법에 대한 추가 정보는 매뉴얼 및 이 프로그램과 함께 제공되는 다른 문서에 설명되어 있습니다. 본 프로그램의 사용은 개인 정보, 데이터 보호, 고용, 전기 통신 및 저장과 관련된 법률 또는 규정을 포함하여 다양한 법률 또는 규정과 연관될 수 있습니다. IBM Security QRadar Incident Forensics는 합법적인 목적과 합법적인 방법으로만 사용될 수 있습니다. 고객은 적용되는 법률, 규정 또는 정책에 의거하여 본 프로그램을 사용하고, 적용되는 법률, 규정 또는 정책을 준수할 모든 책임이 있다는 것에 동의합니다. 라이센스 사용자는 IBM Security QRadar Incident Forensics를 합법적으로 사용하기 위해 필요한 동의, 권한 또는 라이센스를 이미 취득했거나 취득할 것임을 진술하고 보증합니다.

제 1 장 관리자를 위한 QRadar Incident Forensics V7.3.0의 새로운 기능

IBM QRadar Network Insights V7.3.0에서는 QFlow 형식에 대한 추가 옵션을 소개합니다.

QRadar Network Insights에 사용 가능한 TLV 옵션

QFlow Collector를 사용하여 TLV(tab-length-value) 형식으로 QFlow Processor에 데이터를 내보냅니다. 새 IBM Security QRadar 설치 또는 QRadar Network Insights 어플라이언스가 배치의 일부가 아닌 QRadar 업그레이드의 경우 **QFlow 형식** 메뉴에서 TLV 형식을 선택하십시오.

 TLV 형식에 대한 자세한 정보...

제 2 장 Forensics 기능에 대한 관리 워크플로우 및 사용자 액세스

IBM Security QRadar Incident Forensics가 설치 및 구성된 후 관리자는 시스템 및 해당 조작을 문제점 해결, 유지보수 및 모니터링하고 케이스에 대한 사용자 액세스를 관리할 수 있습니다.

QRadar Incident Forensics용 관리 도구를 보려면 관리 권한이 있어야 합니다.

예제: 관리 워크플로우

다음 다이어그램에서는 QRadar Incident Forensics 관리에 대한 샘플 워크플로우를 보여줍니다.

1. 서버 관리를 사용하여 모니터링하지 않을 웹 범주와 트래픽을 필터링합니다.
2. 포렌식 사용자 권한을 사용하여 조사자에게 케이스를 지정합니다.
3. 케이스 관리를 사용하여 케이스를 작성 및 삭제하고 외부 컨텐츠를 시스템에 가져옵니다.
4. 스케줄된 조치를 사용하여 이전 문서 삭제, 데이터베이스 튜닝 및 QRadar Incident Forensics 서버 재설정 같은 유지보수를 스케줄합니다.

사용자 역할

사용자 계정을 추가하려면 먼저 사용자의 특정 액세스 요구사항을 충족하는 보안 프로파일을 작성해야 합니다. 보안 프로파일 구성에 대한 자세한 정보는 *IBM Security QRadar* 관리 안내서를 참조하십시오.

QRadar의 **관리** 탭에 있는 사용자 역할 도구에서 다음 사용자 역할을 지정할 수 있습니다.

관리 사용자가 자신에게 지정된 모든 케이스와 모든 인시던트를 볼 수 있고 자동으로 QRadar Incident Forensics 전체 액세스 권한이 제공됩니다.

포렌식

사용자는 **포렌식** 탭을 보고 이에 액세스할 수 있지만, 케이스를 만들 수 없습니다.

Incident Forensics에서 케이스 작성

사용자가 자동으로 포렌식 케이스를 만들 수 있습니다.

제 3 장 서버 관리

관리자는 IBM Security QRadar Incident Forensics 시스템 및 해당 조작을 문제점 해결, 유지보수 및 모니터링할 수 있습니다.

서버 설정을 모니터링 또는 변경하거나 시스템에 로그인한 사용자를 보려면 서버 관리 도구를 여십시오.

1. QRadar에 관리자로 로그온하십시오.
2. **관리** 탭을 클릭하십시오.
3. 기본 분할창의 **포렌식** 섹션에서 **서버 관리**를 클릭하십시오.

서버 구성 설정

IBM Security QRadar Incident Forensics 서버 관리 도구의 서버 설정을 사용하여 모든 관리 호스트에 영향을 주는 시스템 설정을 구성합니다. 설정을 변경한 후에 **관리** 탭의 **변경사항 배치** 메뉴를 사용하여 변경사항을 배치해야 합니다.

로그아웃 시 검색 히스토리 지우기

사용자가 로그아웃하면 검색 히스토리가 지워집니다. 지워진 검색은 조회 헬퍼의 조회 히스토리 목록 및 검색 및 결과 페이지의 **검색 기준 입력** 필드에 있는 마지막 사용자에 적용됩니다.

시각화할 기본 노드 수

시각화 도구가 표시하는 최대 노드 수입니다. 노드가 처음 렌더링된 후 렌더링할 노드 수를 구성할 수 있습니다. 렌더링된 노드 수를 조정하면 시각화 도구의 해당 인스턴스에만 영향을 미칩니다.

프로토콜 및 도메인 인스펙터 필터

서버 관리 도구에서 프로토콜 또는 도메인 인스펙터를 비활성화하여 특정 유형의 트래픽을 조사에서 제외할 수 있습니다. **인스펙터 필터** 옵션을 사용합니다.

프로토콜 및 도메인 조사자는 수집된 네트워크 트래픽 데이터를 처리하고 이 데이터를 의미 있는 방식으로 식별하고 인덱싱하려고 시도합니다. 해당 데이터를 식별하고 인덱싱하면 조사자가 원하는 정보를 찾는 것을 보다 잘 제어할 수 있습니다.

네트워크 트래픽 데이터가 수집되고 프로토콜이 식별되면 적합한 프로토콜 인스펙터가 데이터를 추가로 검사합니다. HTTP 프로토콜 인스펙터를 통해 식별된 네트워크 트래픽 데이터는 도메인 인스펙터를 통해 추가로 검사되고 인덱싱됩니다.

프로토콜 인스펙터

프로토콜 인스펙터는 HTTP, POP3, FTP 및 Telnet 같은 프로토콜을 식별할 수 있습니다. 프로토콜 인스펙터를 제외할 수 있습니다. 인스펙터를 제외하면 해당 인스펙터와 연관된 네트워크 트래픽 데이터는 계속 수집되지만 트래픽은 일반 레벨에서만 식별 및 인덱싱됩니다.

도메인 인스펙터

도메인 인스펙터는 특정 웹 사이트를 검사합니다. 도메인 인스펙터를 제외할 수 있습니다. 도메인 인스펙터를 제외해도 해당 인스펙터와 연관된 HTTP 네트워크 트래픽 데이터는 계속 수집됩니다. 도메인 인스펙터를 활성화하려면 HTTP 프로토콜 인스펙터도 활성화해야 합니다.

기본적으로 모든 필터는 켜져 있으며, 모든 프로토콜의 트래픽을 볼 수 있습니다. 단, SIP(Session Initiation Protocol) 트래픽만 볼 수 없습니다. 애플리케이션 계층에서 작동하는 이 호출 설정 프로토콜은 기본적으로 꺼져 있습니다.

알아두기: 인스펙터 필터의 구성을 변경하면 작성된 모든 새 케이스에 새 구성이 적용됩니다. 켜진 인스펙터는 특정 케이스에 대해 작성된 문서에 영향을 미치며, 조사자는 특정 인스펙터에 대한 검색 기능을 잃게 됩니다. 사용자는 케이스에 적용된 인스펙터를 파악할 수 없습니다.

인스펙터에 의해 처리되지 않는 프로토콜은 알 수 없음으로 분류됩니다.

웹 카테고리 필터

웹 카테고리 필터를 사용하여 인식되는 웹 페이지 및 웹 서버의 유형을 선택할 수 있습니다.

예를 들어 특정 유형의 HTTP 네트워크 트래픽을 조사에서 제외할 수 있습니다. HTTP 네트워크 트래픽 데이터가 수집되면 데이터를 분류하고 생성되는 문서를 그룹화합니다.

관리자는 데이터가 수집되지 않도록 HTTP 네트워크 트래픽 데이터를 필터링할 수 있습니다.

카테고리 또는 그룹에 대한 트래픽을 제외하거나 필터링하려면 서버 관리 도구에서 카테고리 또는 그룹을 해제해야 합니다.

웹 분류, 그룹화 및 필터링은 수집 중인 HTTP 네트워크 트래픽 데이터에 영향을 주지만, 이미 시스템에 있는 데이터에는 영향을 주지 않습니다.

그룹 필터가 데이터를 제외하도록 설정된 경우 해당 그룹에 있는 카테고리와 연관된 HTTP 네트워크 트래픽 데이터가 연관된 카테고리 필터 설정과 상관없이 사용 중에 필터링되어 제거됩니다.

예제: 웹 카테고리 필터를 사용하여 트래픽을 제외하는 경우 어떤 상황이 벌어집니까?

뉴스 또는 매거진 사이트에서 데이터를 포함하는 트래픽을 제외하려고 합니다.

1. QRadar의 **관리** 탭에서 **서버 관리**를 클릭합니다.
2. **웹 카테고리 필터**를 클릭하고 **뉴스/매거진** 필터 옆의 **꺼짐**을 클릭합니다.
3. **웹 메일/통합 메시징** 필터를 클릭하고 **켜기**를 클릭합니다.

이제 사용자가 **포렌식** 탭에서 수집된 트래픽을 조사하면 **뉴스/매거진** 데이터 모두를 포함하는 트래픽을 보며, **웹 메일/통합 메시징** 필터가 켜져 있어도 **웹 메일/통합 메시징**은 수집되지 않습니다.

지원되는 프로토콜 및 문서 유형

IBM Security QRadar Incident Forensics은 네트워크 플로우 패킷의 컨텐츠를 캡처하고 페이로드 및 메타데이터를 인덱싱 및 처리합니다.

다음 목록에서는 QRadar Incident Forensics이 처리할 수 있는 지원되는 프로토콜을 설명합니다.

- AIM
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- IMAP
- IRC
- Jabber
- Myspace
- NFS
- SIP
- NetBIOS
- Oracle
- POP3
- SMB(버전 1)
  - Lanman 2.1
  - NT 0.12

- SMTP
- SPDY
- TLS(SSL)
- SSH
- Telnet
- Yahoo Messenger
- MySQL

다음 목록에서는 QRadar Incident Forensics이 처리할 수 있는 도메인에 대한 지원 도메인(웹 사이트) 및 지원되는 언어를 설명합니다.

- AOL(Accessible, Basic, Standard)(EN)
- Charter(EN)
- Facebook(모바일, 데스크탑)(AR,CN,DE,EN,ES,FR,RU)
- Gmail(Classic, Standard)(AR,CN,DE,EN,ES,FR,RU)
- Hotmail(AR,CN,DE,EN,ES,FR,RU)
- LinkedIn(DE,EN,ES,FR,RU)
- MailCom(CN,EN,ES,FR,RU)
- MailRu(RU)
- Maktoob(AR,EN)
- Myspace(EN)
- QQMail(EN,CN)
- Twitter(EN)
- YAHOO Mail(Standard, Classic)(EN)
- YAHOO Note(EN)
- YouTube(AR,CN,DE,EN,ES,FR,RU)
- Comcast(Zimbra)(EN)

다음 목록에서는 QRadar Incident Forensics가 처리할 수 있는 지원되는 문서 형식을 설명합니다.

- HTML(HyperText Markup Language)
- XML 및 파생 형식
- Microsoft Office 문서 형식
- ODF(OpenDocument Format)
- PDF(Portable Document Format)
- EPF(Electronic Publication Format)

- 서식있는 텍스트 형식
- 압축 및 패키징 형식
- 텍스트 형식
- 오디오 형식
- 이미지 형식
- 비디오 형식
- Java™ 클래스 파일 및 아카이브
- mbox 형식

QFlow 애플리케이션 발견

QFlow 애플리케이션 발견은 다른 인스펙터에서 애플리케이션, 세션 또는 프로토콜을 발견하지 못한 경우에 사용됩니다. QFlow 애플리케이션 발견은 패킷의 첫 64 바이트에서 서명을 검사한 후 서명 및 포트로부터 애플리케이션 식별을 시도합니다. QFlow 애플리케이션 발견이 식별할 수 있는 애플리케이션, 세션 또는 프로토콜의 예에는 다음 항목이 포함되며 이에 국한되지 않습니다.

- BitTorrent
- Blubster
- CitrixICA
- Google Talk
- Gnucleuslan
- Gnutella
- GSS-SPNEGO
- NTLMMSSP
- OpenNap
- PeerEnabler
- Piolet
- UpdateDaemon
- VNC

제 4 장 케이스 관리

관리자는 케이스 관리를 사용하여 케이스 및 콜렉션을 관리할 수 있습니다. 문서 또는 패킷 캡처(pcap) 파일의 콜렉션에 대한 케이스를 만들고 외부 파일을 IBM Security QRadar Incident Forensics 시스템에 가져올 수도 있습니다.

케이스 관리 성능 조정

케이스 관리 성능을 조정하도록 **플러시** 옵션을 사용할 수 있습니다. 하나의 대형 pcap 파일을 만들기 위해 논리적으로 관련되어 있는 일련의 pcap 파일인 스트리밍 *pcap* 데이터의 경우 버퍼링된 데이터를 디스크에 강제로 쓸 수 있습니다. **플러시** 옵션은 QRadar Incident Forensics 호스트가 디스크에 종료되지 않은 플로우를 쓰도록 강제하여 해당 플로우에서 더 빠른 단계에 검색할 수 있도록 해 줍니다.

분배 그래프

케이스를 삭제할 경우 시각적으로 그래프를 사용하여 케이스의 컨텐츠를 신속하게 검토할 수 있습니다. 파일 유형, 프로토콜, 케이스에 있는 도메인을 검토할 수 있습니다.

관리 호스트에 pcap 파일 업로드

수동으로 외부 소스에서 pcap 데이터를 업로드할 수 있습니다. 처리를 위해 데이터를 업로드할 QRadar Incident Forensics 관리 호스트를 지정할 수 있습니다. 예를 들어, 세 개의 관리 호스트와 세 개의 pcap 파일이 있으면 서로 다른 관리 호스트에 각 파일을 업로드할 수 있습니다. pcap 파일이 큰 경우 FTP를 사용하십시오.

케이스 작성

케이스란 가져온 문서 및 pcap 파일로 구성된 콜렉션에 대한 논리적 컨테이너입니다. 모든 pcap 파일에 하나의 케이스를 사용하거나 케이스를 여러 개 작성할 수 있습니다. 케이스를 특정 사용자로 제한할 수 있습니다.

프로시저

1. **관리** 탭에서 **케이스 관리**를 선택하십시오.
2. **새 케이스 추가**를 클릭하십시오.
3. **케이스 이름** 필드에 고유한 이름을 입력하십시오.

제한사항: 케이스 이름에는 공백이 포함될 수 없습니다.

4. **저장**을 클릭하십시오.

결과

케이스 이름을 기반으로 하는 새로운 디렉토리가 작성됩니다(예: `/case_input/<case_name>`). 이 디렉토리는 pcap 파일을 가져오는 데 사용됩니다.

케이스에 파일 업로드

관리자는 IBM Security QRadar Incident Forensics 케이스 관리를 사용하여 스프레드시트, 텍스트 파일, 이미지 파일 같은 외부 패킷 캡처(pcap) 파일 및 문서를 업로드할 수 있습니다.

다음 파일 유형이 지원됩니다.

- HTML(HyperText Markup Language)
- XML 및 파생 형식
- Microsoft Office 문서 형식
- ODF(OpenDocument Format)
- PDF(Portable Document Format)
- EPF(Electronic Publication Format)
- 서식있는 텍스트 형식
- 압축 및 패키징 형식
- 텍스트 형식
- 오디오 형식
- 이미지 형식
- 비디오 형식
- Java 클래스 파일 및 아카이브
- mbox 형식

케이스 관리에서 사용자가 케이스에 추가할 수 있는 파일 수와 최대 파일 크기를 제한합니다.

프로시저

1. **관리** 탭의 **포렌식** 섹션에서 **케이스 관리**를 클릭하십시오.
2. 케이스를 선택하십시오.
   - 외부 파일을 기존 케이스에 추가하려면 **케이스** 목록에서 케이스를 선택하십시오.
   - 새 케이스에 파일을 추가하려면 **새 케이스 추가**를 클릭하십시오.

제한사항: 케이스 이름에는 공백이 포함될 수 없습니다.

3. **호스트에 업로드** 목록에서 파일을 처리할 관리 호스트를 선택하십시오.
4. pcap 파일 또는 다른 문서 유형을 추가하려면 다음 방법 중 하나를 선택하십시오.
   - **파일 추가**를 클릭하고 파일을 선택한 후 **업로드 시작**을 클릭하십시오.
   - 업로드 상자로 파일을 끌어오십시오.

   업로드가 완료되면 파일이 **콜렉션** 목록에 표시됩니다.

제 5 장 사용자에게 케이스 지정

관리자는 사용자에게 포렌식 데이터에 대한 액세스 권한을 부여하고, 케이스를 사용자에게 지정하며, 사용자 권한(예: FTP 액세스)을 구성합니다. 사용자에게 케이스가 지정되어야만 사용자가 데이터를 볼 수 있습니다. 사용자는 자신이 지정된 케이스의 데이터만 볼 수 있습니다.

네트워크에 대한 액세스가 제한되는 관리자가 아닌 사용자에게 케이스를 지정할 때 주의하십시오. 일반적으로 액세스 권한이 없는 IP 주소의 문서를 볼 수도 있습니다. 예를 들어 관리자가 아닌 사용자에게 재무 또는 인적 자원 정보를 포함하는 케이스를 지정하면 케이스를 조사할 때 해당 데이터를 볼 수 있습니다.

이 태스크 정보

관리자는 다음 태스크를 수행할 수 있습니다.

- 여러 사용자를 케이스에 지정할 수 있습니다.
- 사용자로부터 케이스를 제거할 수 있습니다.
- 사용자에게 지정된 모든 케이스를 보고 액세스할 수 있습니다.

사용자는 명시적으로 자신에게 지정된 케이스만 볼 수 있습니다.

프로시저

1. **관리** 탭에서 **포렌식 사용자 권한**을 클릭하십시오.
2. **사용자** 목록에서 사용자를 선택하십시오.
3. **사용 가능** 목록의 케이스 목록에서 하나 이상의 케이스를 선택하고 화살표(>)를 클릭하여 케이스를 **지정됨** 목록으로 이동하십시오.

   팁: 기본적으로 관리 권한을 가진 사용자가 모든 케이스에 지정됩니다. 왼쪽 화살표(<)와 오른쪽(>) 화살표가 표시되지 않습니다.

포렌식 케이스에 수동으로 파일 가져오기

케이스 관리 도구와 달리, 수동으로 파일을 가져올 경우 파일 크기 또는 파일 개수에 대한 제한사항이 없습니다. 수동으로 케이스를 작성하고 파일을 케이스에 복사하거나, 파일을 기존 케이스에 수동으로 복사할 수 있습니다.

예를 들어, **scp** 명령을 사용하여 다른 호스트에서 IBM Security QRadar Incident Forensics 호스트의 `/opt/ibm/forensics/case_input/case_input/` 디렉토리로 파일을 안전하게 복사할 수 있습니다.

시작하기 전에

가져온 파일의 백업 사본을 만드십시오. 파일을 가져오고 처리하면 원본 파일이 삭제됩니다.

프로시저

1. QRadar Incident Forensics에 root 사용자로 로그인하려면 SSH를 사용하십시오.
2. 케이스를 새로 작성하려면 /opt/ibm/forensics/case_input으로 이동하여 다음 명령을 입력하십시오.

   ```
   mkdir /opt/ibm/forensics/case_input/<case_name>
   ```

3. 파일을 케이스에 복사하려면 **scp** 명령 또는 다른 파일 전송 프로그램을 사용하여 파일 유형에 해당하는 디렉토리로 파일을 복사하십시오.

   다음 표에서는 가져온 파일의 디렉토리 구조를 보여줍니다.

표 *1.* 케이스 파일의 디렉토리 구조

디렉토리	설명
/opt/ibm/forensics/case_input/<*case_name*>	일련의 pcap 파일 또는 pcap 파일의 연결된 스트림을 가져오기 위해 사용되는 디렉토리입니다.
/opt/ibm/forensics/case_input/<*case_name*>/singles	개별 pcap 파일을 가져오는 데 사용되는 디렉토리입니다.
/opt/ibm/forensics/case_input/case_input/<*case_name*>/import	pcap 이외 유형(예: Microsoft Word 문서, Adobe Acrobat PDF, 텍스트 파일 및 이미지)의 단일 파일을 가져오는 데 사용되는 디렉토리입니다.

   중요사항: 파일 이름에 하이픈이 사용된 경우 파일을 가져올 때 하이픈이 밑줄로 변경됩니다.

결과

가져오기가 완료된 후 파일 이름이 작성한 케이스의 콜렉션 창에 자동으로 표시됩니다.

사용자가 pcap 파일 및 문서를 외부 시스템에서 포렌식 케이스로 FTP 전송할 수 있음

특정 케이스에 포함할 외부 데이터를 업로드하기 위해 관리자가 보안 FTP 권한을 사용자에게 부여하고 데이터가 연결되는 케이스를 관리할 수 있습니다. 사용자는 FTP 요청을 처리할 IBM Security QRadar Incident Forensics 호스트를 선택할 수 있습니다.

FTP 액세스가 사용으로 설정된 후 비밀번호를 변경하려면 FTP 액세스를 사용 안 함으로 설정하고 사용자를 저장한 후 FTP 액세스를 다시 사용으로 설정하고 새 비밀번호를 입력해야 합니다.

시작하기 전에

사용자 역할 도구의 **관리** 탭에서 포렌식 조사자의 역할을 작성하거나 지정하는지 확인하십시오.

기본적으로 /etc/vsftpd/vsftpd.conf 파일은 다섯 개 포트(55100-55104)를 열도록 구성됩니다. /etc/vsftpd/vsftpd.conf 파일을 편집하고 pasv_min_port 및 pasv_max_port 설정값을 원하는 포트 범위로 변경하여 포트 범위를 변경할 수 있습니다. **관리** 탭에서 **변경사항 배치**를 클릭하여 구성 변경사항을 배치해야 합니다.

참고: FTP 클라이언트는 TLS v1.2(vsftpd.conf 파일)를 지원해야 합니다. 다음 목록은 지원되는 최소 FTP 클라이언트 버전을 설명합니다.

- WinSCP 5.7
- FileZilla 3.9.0.6

이 태스크 정보

IBM Security QRadar Incident Forensics는 네트워크에 있는 액세스 가능한 디렉토리의 데이터를 가져올 수 있습니다. 데이터는 다음 형식을 포함하되 이에 제한하지 않은 여러 형식일 수 있습니다.

- 외부 소스의 표준 PCAP 형식 파일
- 텍스트 파일, PDF 파일, 스프레드시트 및 프리젠테이션 같은 문서
- 이미지 파일
- 애플리케이션의 스트리밍 데이터
- 외부 PCAP 소스의 스트리밍 데이터

사용자는 여러 파일을 케이스에 업로드할 수 있고, 관리자는 여러 사용자 액세스 권한을 케이스에 부여할 수 있습니다.

제한사항: 케이스 이름은 고유해야 합니다. 단일 사용자가 케이스와 연관되어 있으므로, 두 명의 사용자가 동일한 이름을 가진 케이스를 만들 수 없습니다.

프로시저

1. **관리**에서 **포렌식 사용자 권한**을 클릭하십시오.
2. **사용자** 목록에서 사용자를 선택하십시오.
3. **사용자 편집** 분할창에서 **FTP 액세스 사용** 선택란을 선택하십시오.

4. 사용자의 FTP 비밀번호를 입력하고 확인하십시오.
5. 권한에 대한 변경사항을 저장하려면 **사용자 저장**을 클릭하십시오.
6. FTP 클라이언트에서 다음 단계를 수행하십시오.
   a. TLS(Transport Layer Security)가 프로토콜로 선택되어 있는지 확인하십시오.
   b. QRadar Incident Forensics 호스트의 IP 주소를 추가하십시오.
   c. 작성된 QRadar Incident Forensics 사용자 이름 및 비밀번호를 사용하는 로그온을 작성하십시오.
7. QRadar Incident Forensics 서버에 연결하고 새 디렉토리를 만드십시오.
8. pcap 파일을 FTP 및 저장하려면 케이스에 대해 작성한 디렉토리에서 `singles`라는 디렉토리를 만들고 pcap 파일을 해당 디렉토리로 끄십시오.
9. pcap 파일이 아닌 다른 파일 유형을 FTP 및 저장하려면 케이스에 대해 작성한 디렉토리에서 `import`라는 디렉토리를 만들고 파일을 해당 디렉토리로 끄십시오.
10. FTP 서버를 다시 시작하려면 다음 명령을 입력하십시오.

    ```
    etc/init.d/vsftpd restart
    ```

11. 파일을 업로드 영역에서 QRadar Incident Forensics 디렉토리로 이동하는 서버를 다시 시작하려면 다음 명령을 입력하십시오.

    ```
    /etc/init.d/ftpmonitor restart
    ```

결과

케이스 관리에서 업로드된 데이터가 관리자에게 표시됩니다. 사용자는 **포렌식** 탭의 도구 중 하나에서 해당 케이스를 볼 수 있습니다.

QRadar Incident Forensics에서 SSL 및 TLS 트래픽 복호화

숨겨진 위협을 찾기 위해 IBM Security QRadar Incident Forensics에서 SSL 트래픽을 복호화할 수 있습니다. 서버의 개인 키와 IP 주소 또는 브라우저 세션 키와 일부 다른 세션 정보를 제공한 경우 프로토콜 인스펙터가 SSL 트래픽을 복호화할 수 있습니다.

세션 키가 외부 사이트에서 생성되거나 다른 브라우저에서 생성될 경우 프로토콜 인스펙터가 브라우저 세션의 SSL 트래픽을 복호화할 수 없습니다.

제한사항: 암호화된 트래픽이 개인 키를 통해 복호화될 경우 `Diffie Hellman` 키 교환 메커니즘이 지원되지 않습니다. 개인 키를 사용할 경우 RSA 같은 다른 키 교환 방법이 지원됩니다.

키 로그에 있는 정보로 트래픽이 복호화될 경우 Diffie Hellman 제한사항이 적용되지 않습니다.

이 태스크 정보

다음 프로토콜에 대한 복호화가 지원됩니다.

- SSL v3
- TLS v1.0
- TLS v1.1
- TLS v1.2

키 로그 파일은 SSLKEYLOGFILE 환경 변수를 사용하여 Chrome, Firefox 및 Opera 브라우저에서 생성합니다. SSLKEYLOGFILE 세션 키에 대해서는 다음 키 형식이 지원됩니다.

- RSA
- DH

프로시저

1. QRadar Incident Forensics 기본 호스트에 root 사용자로 로그인하려면 SSH를 사용하십시오.
2. /opt/qradar/forensics.conf 파일에서 키 위치를 검토하십시오.

   ```
   <sslkeys
   keydir="/opt/ibm/forensics/decapper/keys"
   keylogs="/opt/ibm/forensics/decapper/keylogs"/>
   ```

3. /opt/qradar/forensics.conf 파일에 지정된 디렉토리에 키를 복사하십시오.
   - 개인 키의 경우 키를 /opt/ibm/forensics/decapper/keys 디렉토리에 복사하십시오.

     예제:

     ```
     <keys>
      <key file=" /opt/ibm/forensics/decapper/keys/key_name">
         <address> 1.2.3.4</address>
         <range> 1.2.3.0-1.2.3.255</range>
       </key></keys>
     ```

   - 브라우저에서 생성한 키 로그 파일의 경우 키 로그 파일을 /opt/ibm/forensics/decapper/keylogs/default 디렉토리에 복사하십시오.

   /opt/ibm/forensics/decapper/keys 또는 /opt/ibm/forensics/decapper/keylogs 디렉토리에서 하위 디렉토리를 변경할 경우 decapper 서비스를 다시 시작해야 합니다.

decapper 서비스를 다시 시작하려면 다음 명령을 입력하십시오. `service decapper restart`

제 6 장 QRadar Incident Forensics의 스케줄된 조치

스케줄된 조치를 사용하여 이전 문서 삭제, 데이터베이스 튜닝 및 IBM Security QRadar Incident Forensics 서버 재설정 같은 유지보수를 스케줄할 수 있습니다.

많은 문서가 있는 경우 스케줄 조치(예: 이전 문서 삭제)를 완료하는 데 시간이 오래 걸릴 수 있습니다. 전체 케이스를 삭제할 경우 케이스 관리 도구를 사용하십시오.

문서 삭제

관리자는 문서 네트워크 시간소인을 기준으로 기한이 지난 문서를 삭제할 수 있습니다.

pcap 및 기타 파일 유형을 포함하는 문서를 케이스 또는 서버에서 삭제할 수 있습니다. 기한이 지난 문서를 삭제하면 문서 검색 시 속도를 유지하는 데 도움이 됩니다.

케이스 플러시

케이스 관리 튜닝을 돕기 위해 **케이스 플러시** 옵션을 사용할 수 있습니다. 하나의 대형 pcap 파일을 만들기 위해 논리적으로 관련되어 있는 일련의 pcap 파일인 스트리밍 *pcap* 데이터의 경우 버퍼링된 데이터를 디스크에 강제로 쓸 수 있습니다. **케이스 플러시** 옵션은 QRadar Incident Forensics 호스트가 디스크에 종료되지 않은 플로우를 쓰도록 강제하여 해당 플로우에서 더 빠른 단계에 검색할 수 있도록 해줍니다.

데이터베이스 최적화

관리자는 데이터베이스를 최적화하여 검색 엔진 인덱스를 세그먼트로 재구성하고 삭제된 문서를 제거할 수 있습니다.

데이터베이스 최적화 스케줄 조치는 **defrag** 명령과 유사합니다.

데이터베이스를 최적화하면 새 인덱스가 작성됩니다. 인덱스가 작성된 후 새 인덱스가 이전 인덱스를 대체합니다. 이전 인덱스가 대체될 때까지는 두 개의 인덱스가 존재하므로 인덱스 최적화 명령을 사용할 경우 하드 디스크 공간이 두 배로 필요합니다.

데이터베이스를 최적화하기 전에 인덱스의 크기가 하드 디스크 드라이브 사용 가능 공간의 50%를 초과하지 않는지 확인해야 합니다.

QRadar Incident Forensics 호스트에 대한 조치 스케줄링

IBM Security QRadar Incident Forensics 호스트에 대한 유지보수 태스크를 스케줄할 수 있습니다.

다음과 같은 태스크를 스케줄할 수 있습니다.

- 현재 사용 가능한 케이스에 대한 새 인덱스 빌드.
- 지정된 기간 이후 보존하지 않으려는 문서 제거(만료).
- 디스크에 데이터 쓰기 강제 실행.

프로시저

1. **관리** 탭의 **Forensics** 섹션에서 **조치 스케줄**을 클릭하십시오.
2. **새 조치 추가**를 클릭하십시오.
3. **조치 선택** 목록에서 조치를 선택하고 설정을 지정하십시오.
   - 현재 케이스에 대한 새 인덱스를 빌드하려면 **인덱스 최적화**를 선택하십시오.

     새 인덱스의 경우 기존 인덱스에 비해 두 배 정도의 공간이 필요합니다. 충분한 공간이 확보되어 있는지 확인하십시오.
   - 네트워크 시간소인이 지정된 기간보다 더 오래된 문서를 삭제하려면 **문서 만료**를 선택하십시오.

     문서를 삭제하면 인덱스도 제거됩니다.
   - 종료되지 않은 플로우를 디스크에 쓰려면 **케이스 플러시**를 선택하십시오.
4. **저장**을 클릭하십시오.
5. 조치를 실행, 편집 또는 삭제하려면 **조치** 목록에서 조치를 선택하고 **실행**, **편집** 또는 **삭제**를 클릭하십시오.

제 7 장 의심스러운 컨텐츠 관리

관리자는 의심스러운 컨텐츠 관리 기능을 사용하여 의심스러운 컨텐츠에 플래그를 지정할 수 있습니다.

Yara 룰

QRadar Incident Forensics 네트워크 트래픽에서 찾은 파일의 의심스러운 컨텐츠에 플래그를 지정하기 위해 기존 Yara 룰을 가져와서 사용함으로써 파일에서 실행되는 사용자 정의 룰을 지정할 수 있습니다.

각 Yara 룰은 키워드 룰 다음에 룰 ID를 사용하여 시작됩니다. Yara 룰은 다음과 같이 두 개의 섹션으로 구성되어 있습니다.

1. 문자열 정의: 문자열 정의 섹션에서는 룰의 일부를 구성하는 문자열을 지정합니다. 각 문자열은 달러 부호($)와 그 뒤에 오는 밑줄로 구분된 영숫자 문자의 시퀀스로 구성된 ID를 사용합니다.
2. 조건: 조건 섹션에서는 룰의 로직을 정의합니다. 이 섹션에는 파일이 룰을 충족하는 조건을 정의하는 부울 표현식이 포함되어야 합니다.

다음 예제는 단순 Yara 룰을 보여줍니다.

```
rule simple_forensics : qradar
{
    meta:
        description = "This rule will look for str1 at an offsets of 25 bytes
                       into the file."
    strings:
        $str1 = "pattern of interest"

    condition:
        $a at 25
}
```

다음 예제는 더 복잡한 Yara 룰을 보여줍니다.

```
rule ibm_forensics : qradar
{
    meta:
        description = "This rule will flag content that contains the hex
                       sequence as well as str1 at least 3 times."

    strings:
        $hex1 = {4D 2B 68 00 ?? 14 99 F9 B? 00 30 C1 8D}
        $str1 = "IBM Security!"


    condition:
        $hex1 and (#str1 > 3)
}
```

Yara 룰이 업로드된 경우 decapper는 복구 또는 PCAP 업로드에서 파일을 발견하면 지정된 룰을 사용합니다. 일치하는 컨텐츠가 발견되면 문서의 **속성** 탭 아래에 **SuspectContent** 필드가 추가됩니다. **SuspectContent** 필드는 Yara 룰 이름과 해당 룰이 식별하는 모든 태그로 채워집니다.

제한사항: 현재 Yara 모듈 구현은 사용할 수 없습니다.

Yara 룰 가져오기

기존 Yara 룰을 IBM Security QRadar Incident Forensics로 가져와서 악성 컨텐츠를 찾아 플래그 지정하기 위해 해당 룰을 사용할 수 있습니다. 가져오는 파일에 둘 이상의 Yara 룰이 존재할 수 있습니다.

프로시저

1. **관리** 탭에서 **의심스러운 컨텐츠 관리**를 선택하십시오.
2. **파일 선택**을 클릭하십시오.
3. 파일 업로드 창에서 가져올 파일을 찾은 후 **열기**를 클릭하십시오.

   중요사항: Yara 룰 이름은 고유해야 합니다.

결과

Yara 룰 가져오기가 완료되면 메시지가 표시됩니다.

다음에 수행할 작업

새로 가져온 Yara 룰은 소급 적용되지 않습니다. Yara 룰을 가져온 후 변경사항을 적용하려면 전체 배치를 수행해야 합니다.

Yara 룰 삭제

IBM Security QRadar Incident Forensics에서 기존 Yara 룰을 모두 삭제할 수 있습니다. Yara 룰을 끄려면 비어 있는 단일 룰이 포함된 파일을 업로드하십시오.

시작하기 전에

프로시저

1. 비어 있는 단일 룰이 포함된 새 파일을 작성하려면 다음 단계를 사용하십시오.
   a. 선택한 텍스트 편집기에 다음 룰을 복사하십시오.

```
rule empty
{
 condition:
           false
}
```

b. 텍스트 파일로 저장하십시오.

2. **관리** 탭에서 **의심스러운 컨텐츠 관리**를 선택하십시오.
3. **파일 선택**을 클릭하십시오.
4. 파일 업로드 창에서 1단계에서 작성한 파일을 찾은 후 **열기**를 클릭하십시오.
5. **저장**을 클릭하십시오.

결과

이 단일 룰은 항상 **false** 결과를 리턴하여 유효성 검증 프로그램을 패스하도록 해줍니다. 이 단일 룰은 기존 룰을 모두 삭제한 후 데이터베이스에 삽입됩니다. 이 단일 룰은 컨텐츠에 의심 플래그를 지정하지 않습니다.

제 8 장 QRadar Incident Forensics에서 사용자 및 시스템 사용 감사

감사 로그는 데이터 액세스와 연관된 사용자 계정을 식별하는 시간순으로 표시된 레코드입니다. 이러한 로그는 비정상적이거나 권한이 없는 액세스를 발견하고 작업 실패와 같은 문제를 식별할 수 있습니다.

다음 활동은 감사 로그 이벤트를 생성합니다.

- 케이스 작성
- 케이스 지정
- 케이스 삭제
- 콜렉션 삭제
- 모든 사용자 조회
- 문서 보기
- 문서 내보내기

제한사항: 콜렉션 이벤트 작성 로깅은 지원되지 않습니다.

프로시저

1. SSH를 사용하여 QRadar Console 또는 QRadar Incident Forensics Standalone에 관리자로 로그온하십시오.
2. `/var/log/audit` 디렉토리로 이동하십시오.
3. vi와 같은 편집기에서 `audit.log` 파일을 열어 컨텐츠를 검토하거나 **grep** 명령을 사용하여 특정 항목을 검색하십시오.

제 9 장 QRadar Network Insights를 사용하여 위협 조사

IBM QRadar Network Insights에서 네트워크 데이터를 실시간으로 분석하여 네트워크에서의 위협 동작을 조사할 수 있습니다.

QRadar Network Insights는 내부자 위협, 데이터 유출 및 멀웨어 활동을 쉽고 빠르게 발견하는 네트워크 위협 분석 솔루션입니다. 네트워크 트래픽에서의 전체 표시를 통해 필수 위협 지표가 수집되고 추적됩니다.

QRadar Network Insights를 사용하여 실시간 위협 조사

IBM QRadar Network Insights는 실시간 네트워크 데이터 분석과 고급 레벨의 위협 발견 및 분석을 제공합니다.

고급 사이버 보안 위협을 발견하고 예방하기가 점점 더 어려워지고 있습니다. 악성 활동은 종종 정상적인 사용으로 위장하여 위협이 네트워크를 통해 이동하고 통신하여 목적을 달성하게 합니다. 예를 들어 시그니처 기반 발견을 피하기 위해 멀웨어가 변하며, 피싱과 같은 사회 공학 기법은 이러한 공격의 문을 여는 데 효과적입니다.

검색 기능

QRadar Network Insights 검색 기능은 플로우 정보, 메타데이터, 추출된 컨텐츠 및 의심스러운 컨텐츠와 같은 패킷 데이터에서 중요 지표를 찾고 추출합니다. 장기 회고 분석(long-term retrospective analysis)에 추출된 컨텐츠를 사용할 수 있습니다.

IBM Security QRadar Incident Forensics와의 통합

QRadar Network Insights는 애플리케이션 활동을 기록하고, 아티팩트를 캡처하며, 네트워크 통신에 참여한 자산, 애플리케이션 및 사용자를 식별합니다. QRadar Network Insights는 사후 인시던트 조사와 위협 추적 활동을 위해 IBM Security QRadar Incident Forensics와 긴밀하게 통합됩니다. QRadar Incident Forensics 및 IBM QRadar Network Packet Capture는 전체 대화를 캡처하고, 재구성하며, 재생하지만 QRadar Network Insights는 인시던트 발견을 제공하고 대화 중에 언제든지 의심스러운 항목이나 관심 있는 주제가 논의되었는지 여부를 알려줍니다.

의심스러운 컨텐츠는 멀웨어, 비표준 포트, regex 또는 Yara 룰과 같은 여러 다양한 소스로부터 올 수 있습니다.

플로우 값

플로우는 디바이스를 네트워크에 연결할 때 자산 발견을 가능하게 하므로 네트워크 활동에 대한 표시와 함께 QRadar를 제공합니다. QRadar Network Insights를 사용하면 플로우 데이터를 이벤트 데이터와 상관시켜 로그만으로는 식별할 수 없는 위협을 발견할 수 있습니다. IBM Security QRadar QFlow Collector는 네트워크 플로우를 제공하고 계층 7 애플리케이션을 인식하기도 하며 사용자는 세션 시작을 캡처할 수 있습니다. QRadar Network Insights는 이전에 숨겨진 위협과 악성 동작을 드러나게 합니다.

관련 개념:

33 페이지의 『QRadar Network Insights 플로우 검사 레벨』
성능을 개선하려면 **플로우 검사 레벨** 설정을 구성하여 적절하게 필요한 플로우 비율을 선택해야 합니다.

QRadar Network Insights 배치

IBM QRadar Network Insights는 QRadar 콘솔에 연결되는 관리 호스트입니다.

QRadar Network Insights 배치의 경우 설치 중에 6200 어플라이언스 옵션을 선택해야 합니다. QRadar Network Insights 어플라이언스 설치에 대한 자세한 정보는 *IBM Security QRadar Incident Forensics* 설치 안내서를 참조하십시오.

QRadar Network Insights 배치의 경우 6200 어플라이언스 옵션에 라이센스 하나를 할당해야 합니다. QRadar Network Insights에서는 6200 어플라이언스에 대해 별도의 라이센스가 필요하지만 QRadar 콘솔에서 QRadar Network Insights 라이센스가 필요하지는 않습니다.

QRadar Network Insights 어플라이언스와 IBM Security QRadar Incident Forensics의 관계

IBM Security QRadar Incident Forensics Processor 배치와 별도로 QRadar Network Insights를 배치할 수 있습니다. QRadar Network Insights에서는 QRadar 콘솔에 대한 연결만 필요하고 QRadar Incident Forensics 어플라이언스에 대한 연결은 필요하지 않습니다.

QRadar Network Insights 어플라이언스

QRadar Network Insights 1920 어플라이언스는 두 개의 써드파티 네트워크 카드와 함께 제공됩니다. 네트워크 카드는 네트워크에 직접 연결되어 실시간 패킷 검사를 돕습니다.

구성 가능한 플로우 전달 기능을 사용하면 여러 어플라이언스 간에 로드 밸런싱이 가능합니다. 하드웨어 구성은 인메모리 처리를 도와 네트워크 데이터의 실시간 분석을 가능하게 합니다.

표 2. 네트워크 카드 사양

1920 어플라이언스	설명
서버	X3650 M5
CPU	2 x E5-2680 v4 14C 2.4GHz 35MB 2400MHz 120W
RAM	8 x 16GB
HDD	2 x 200GB SSD
ServeRAID	M1215
I/O 카드	Intel X520 2P 10GbE + 2 x 10G SR 2 x NT40E3 4P 40G + 2 x 10G SR + 2 x 10G LR
P/S	2 x 900W

QRadar Network Insights 구성 요구사항

IBM QRadar Network Insights를 설치하고 이를 QRadar Console에 관리 호스트로 연결한 경우 이를 사용하여 네트워크에서의 위협을 조사하려면 먼저 어플라이언스를 구성해야 합니다. QRadar Network Insights 어플라이언스는 네트워크 탭 또는 스팬 포트에서 원시 패킷을 읽은 다음 IPFIX 패킷을 생성합니다. IPFIX 패킷은 QRadar Console의 QFlow로 전송됩니다.

QFlow Collector 형식 구성

QRadar 관리 호스트 클러스터의 관리자로서 QFlow Processor로 데이터를 내보내기 위해 QFlow Collector에서 사용하는 형식인 TLV 또는 페이로드를 선택할 수 있습니다.

시작하기 전에

다음 요구사항이 충족되는지 확인하십시오.

__ • 관리 호스트로 연결된 QRadar Network Insights를 사용하여 QRadar Console을 설치하십시오.

__ • IBM QRadar Network Insights를 관리 호스트로 연결한 후 전체 배치를 수행하십시오.

프로시저

1. QRadar에 로그인하십시오. `https://IP_Address_QRadar`

   기본 사용자 이름은 `admin`입니다. 비밀번호는 root 사용자 계정의 비밀번호입니다.

2. **관리** 탭을 클릭하십시오.

3. 탐색 분할창에서 **시스템 설정**을 클릭하십시오.
4. **QFlow 설정** 메뉴에서 QFlow 형식을 선택하십시오.

표 *3. QFlow* 형식 옵션

QFlow 형식	설명
TLV	기본 QFlow 형식 설정입니다. 새 설치 또는 QRadar Network Insights 어플라이언스가 배치의 일부가 아닌 업그레이드의 경우 **TLV**(tab-length-value)를 선택하십시오.
페이로드	QRadar Network Insights 어플라이언스가 배치의 일부인 업그레이드의 경우 **페이로드**를 선택하십시오. 이는 배치가 계속해서 현 상태대로 작동할 수 있음을 의미합니다.

5. **저장**을 클릭하십시오.
6. **관리** 탭 메뉴 표시줄에서 **전체 구성 배치**를 클릭하고 변경사항을 확인하십시오.
7. 웹 브라우저를 새로 고쳐서 **포렌식** 탭을 표시하십시오.

QRadar Network Insights 관리 호스트에서 DTLS 설정

도청 및 변조를 방지하려면 QRadar Network Insights 관리 호스트에서 DTLS(Datagram Transport Layer Security)를 설정해야 합니다. 먼저 플로우 소스를 구성해야 합니다.

프로시저

1. QRadar Network Insights를 관리 호스트로 추가하십시오.
   a. **관리** 탭을 클릭하십시오.
   b. 탐색 분할창의 **시스템 구성** 섹션에서 **시스템 및 라이센스 관리**를 클릭하십시오.
   c. QRadar Network Insights 관리 호스트를 선택하십시오. 어플라이언스 유형은 6200입니다.
   d. **배치 조치** 아이콘을 클릭하고 **호스트 추가**를 선택하십시오.
   e. 프롬프트가 표시되면 QRadar Network Insights 관리 호스트의 IP 주소와 root 비밀번호를 입력하고 **추가**를 클릭하십시오.
2. 플로우 소스를 구성하려면 다음 단계를 수행하십시오.
   a. QRadar에 관리자로 로그인하십시오.
   b. **관리** 탭을 클릭하십시오.
   c. 탐색 분할창의 **플로우** 섹션에서 **플로우 소스**를 클릭하십시오.
   d. **추가** 아이콘을 클릭하십시오.
   e. 설명적인 **플로우 소스 이름**을 지정하십시오.
   f. **대상 플로우 콜렉터**를 선택하거나 제공된 값을 채택하십시오.

g. **Netflow v.1/v.5/v.7/v.9/IPFIX**를 **플로우 소스 유형**으로 선택하십시오.

h. **모니터링 포트**의 값을 입력하고 제공된 값을 채택하십시오.

i. **링크 프로토콜** 목록에서 DTLS를 선택하십시오.

j. **저장**을 클릭하십시오.

k. **관리** 탭 메뉴 표시줄에서 **전체 구성 배치**를 클릭하고 변경사항을 확인하십시오.

l. 웹 브라우저를 새로 고치십시오.

3. DTLS 통신을 구성하려면 다음 단계를 수행하십시오.

참고: 사용자 배치에서 QRadar Network Insights 관리 호스트의 플로우 소스 또는 QRadar 플로우 콜렉터를 변경하는 경우 DTLS 설치 스크립트를 다시 실행해야 합니다.

a. **배치 조치** 아이콘을 클릭하고 **호스트 연결 편집**을 선택하십시오.

b. QRadar Network Insights 수정 페이지에서 QRadar 플로우 콜렉터 및 플로우 소스를 선택하십시오.

c. **저장**을 클릭하십시오.

d. 시스템 및 라이센스 관리 페이지를 닫으십시오.

e. **관리** 탭에서 **변경사항 배치** 아이콘을 클릭하십시오.

f. **SSH**를 사용하여 QRadar Console의 root 사용자로 로그인하십시오.

g. 이 명령을 실행하여 DTLS 인증서를 설정하십시오.

```
python /opt/qradar/bin/qflow_dtls_cert_setup.py
```

h. QRadar에 관리자로 로그인하십시오.

i. **관리** 탭에서 **고급** > **전체 구성 배치**를 선택하십시오.

QRadar Network Insights 플로우 검사 레벨

성능을 개선하려면 **플로우 검사 레벨** 설정을 구성하여 적절하게 필요한 플로우 비율을 선택해야 합니다.

플로우 비율은 소스, 대상, 프로토콜 및 특정 파일 유형과 같이 사용 가능한 컨텐츠를 통한 가시성 레벨과 관련되어 있습니다.

플로우 검사 레벨은 누적되므로 각 레벨은 상위 레벨의 특성을 가집니다.

플로우

플로우는 가장 낮은 검사 레벨입니다. 플로우는 5-tuple에 의해 발견되고 각 방향에서 플로우되는 바이트 및 패킷 수가 계수됩니다. 이러한 유형의 정보는 심층

패킷 검사를 수행하지 않는 라우터나 네트워크 스위치 외부에서 가져오는 항목과 유사합니다. 이 레벨은 가장 높은 대역폭을 지원하지만 가장 적은 양의 플로우 정보를 생성합니다.

플로우 검사 레벨을 사용하여 QRadar Network Insights에서 생성하는 속성은 각 방향에서의 5-tuple 값, 플로우 ID, 패킷 및 옥텟 수와 플로우 시작 및 종료 횟수입니다.

강화 플로우

각 플로우는 프로토콜 또는 도메인 검사기 중 하나에 의해 식별되고 검사됩니다. 해당 검사에서 여러 속성을 생성할 수 있습니다.

다음 목록은 강화 플로우 검사 레벨을 사용하여 QRadar Network Insights에서 생성하는 속성을 설명합니다.

- HTTP 메타데이터 값 - URL 분류 포함
- 애플리케이션 ID 및 조치
- 파일 정보(이름, 크기, 해시)
- 원본 및 수신 사용자 이름
- 제한된 의심스러운 컨텐츠 값

컨텐츠 강화 플로우

컨텐츠 강화 플로우는 기본 설정이며 가장 높은 검사 레벨입니다. 강화 플로우 레벨의 모든 속성을 그대로 가지며 찾는 파일의 컨텐츠를 스캔하고 검사하기도 합니다. 이로 인해 컨텐츠 유형 판별이 더 정확해지며 파일 컨텐츠 검사로부터 더 많은 의심스러운 컨텐츠 값을 얻을 수 있습니다.

다음 목록은 컨텐츠 강화 플로우 검사 레벨을 사용하여 QRadar Network Insights에서 생성하는 속성을 설명합니다.

- 개인 정보
- 기밀 데이터
- 임베디드 스크립트
- 경로 재지정
- 구성 가능한 컨텐츠 기반 의심스러운 컨텐츠

표 *4.* 성능 고려사항

플로우 검사 레벨 설정	성능
플로우	10Gbps
강화 플로우	약 10Gbps. 성능은 검사 레벨 설정, 검색, 추출 기준 및 네트워크 데이터에 따라 다릅니다.

표 4. 성능 고려사항 (계속)

플로우 검사 레벨 설정	성능
컨텐츠 강화 플로우(고급)	약 3.5Gbps. 10Gbps 성능은 여러 어플라이언스에서 얻을 수 있습니다.

관련 개념:

29 페이지의 『QRadar Network Insights를 사용하여 실시간 위협 조사』
IBM QRadar Network Insights는 실시간 네트워크 데이터 분석과 고급 레벨의 위협 발견 및 분석을 제공합니다.

QRadar Network Insights 설정 구성

성능을 개선하기 위해 사용자 배치의 QRadar Network Insights 어플라이언스에서 생성하는 플로우 레벨을 구성합니다. 각 검사 레벨은 더 높은 가시성을 제공하고 더 많은 컨텐츠를 추출합니다.

프로시저

1. QRadar에 관리자로 로그인하십시오.
2. **관리** 탭을 클릭하십시오.
3. 탐색 분할창에서 **시스템 설정**을 클릭하십시오.
4. **Network Insights 설정** 메뉴를 클릭하십시오.
5. **플로우 검사 레벨**에서 필요한 플로우 비율을 선택하십시오. 다음 테이블을 사용하여 플로우 검사 레벨을 이해할 수 있습니다.

표 5. 플로우 검사 레벨

플로우 검사 레벨	설명
플로우	가장 낮은 검사 레벨입니다. 플로우는 5-tuple에 의해 발견되고 각 방향에서 플로우되는 바이트 및 패킷 수가 계수됩니다.
강화 플로우	각 플로우는 프로토콜 또는 도메인 검사기 중 하나에 의해 식별되고 검사됩니다. 해당 검사에서 여러 속성을 생성할 수 있습니다.
컨텐츠 강화 플로우	기본 설정입니다. 가장 높은 검사 레벨입니다. 강화 플로우 레벨의 모든 속성을 그대로 가지며 찾는 파일의 컨텐츠를 스캔하고 검사하기도 합니다.

6. **저장**을 클릭하십시오.
7. **관리** 탭 메뉴 표시줄에서 **전체 구성 배치**를 클릭하십시오.
8. 웹 브라우저를 새로 고치십시오.

다음에 수행할 작업

QRadar Incident Forensics Processor 관리 호스트를 배치하십시오.

QRadar Network Insights를 사용하여 위협 발견

네트워크에서의 위협 활동에 대한 실시간 표시를 위해 QRadar Network Insights를 사용하여 사이버 공격과 악성 활동의 지표를 발견할 수 있습니다.

QRadar Network Insights 컨텐츠 다운로드

IBM Security App Exchange(http://exchange.xforce.ibmcloud.com/hub/extension/522bf1095f047b0b37225d8efc5d4877)에서 QRadar Network Insights 컨텐츠(확장)를 다운로드합니다. **확장 관리** 도구를 사용하여 컨텐츠를 설치합니다.

확장 관리 도구 사용에 대한 정보는 *IBM Security QRadar* 관리 안내서를 참조하십시오.

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 라이센스까지 부여하는 것은 아닙니다. 라이센스에 대한 의문사항은 다음으로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

2바이트 문자 세트(DBCS) 정보에 관한 라이센스 문의는 한국 IBM에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 이 책을 "현상태대로" 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 변경된 사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통지 없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 언급되는 비IBM 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i) 독립적으로 작성된 프로그램과 기타 프로그램(본 프로그램 포함) 간의 정보 교환 및 (ii) 교환된 정보의 상호 이용을 목적으로 본 프로그램에 관한 정보를 얻고자 하는 라이센스 사용자는 다음 주소로 문의하십시오.

07326
서울특별시 영등포구
국제금융로 10, 3IFC
한국 아이.비.엠 주식회사
대표전화서비스: 02-3781-7114

이러한 정보는 해당 조건(예를 들면, 사용료 지불 등)하에서 사용될 수 있습니다.

이 정보에 기술된 라이센스가 부여된 프로그램 및 이 프로그램에 대해 사용 가능한 모든 라이센스가 부여된 자료는 IBM이 IBM 기본 계약, IBM 프로그램 라이센스 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

인용된 성능 데이터와 고객 예제는 예시 용도로만 제공됩니다. 실제 성능 결과는 특정 구성과 운영 조건에 따라 다를 수 있습니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 기타 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM이 제시하는 방향 또는 의도에 관한 모든 언급은 특별한 통지 없이 변경될 수 있습니다.

여기에 나오는 모든 IBM의 가격은 IBM이 제시하는 현 소매가이며 통지 없이 변경될 수 있습니다. 실제 판매가는 다를 수 있습니다.

이 정보에는 일상의 비즈니스 운영에서 사용되는 자료 및 보고서에 대한 예제가 들어 있습니다. 이들 예제에는 개념을 가능한 완벽하게 설명하기 위하여 개인, 회사, 상표 및 제품의 이름이 사용될 수 있습니다. 이들 이름은 모두 가공의 것이며 실제 인물 또는 기업의 이름과 유사하더라도 이는 전적으로 우연입니다.

상표

IBM, IBM 로고 및 ibm.com®은 전세계 여러 국가에 등록된 International Business Machines Corp.의 상표 또는 등록상표입니다. 기타 제품 및 서비스 이름은 IBM 또는 타사의 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보"(www.ibm.com/legal/copytrade.shtml)에 있습니다.

Adobe, Adobe 로고, PostScript 및 PostScript 로고는 미국 또는 기타 국가에서 사용되는 Adobe Systems Incorporated의 등록상표 또는 상표입니다.

Java 및 모든 Java 기반 상표와 로고는 Oracle 및/또는 그 계열사의 상표 또는 등록상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

제품 문서의 이용 약관

다음 이용 약관에 따라 이 책을 사용할 수 있습니다.

적용성

본 이용 약관은 IBM 웹 사이트의 모든 이용 약관에 추가됩니다.

개인적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 개인적, 비상업적 용도로 복제할 수 있습니다. 귀하는 IBM의 명시적 동의 없이 본 발행물 또는 그 일부를 배포 또는 전시하거나 2차적 저작물을 만들 수 없습니다.

상업적 사용

모든 소유권 사항을 표시하는 경우에 한하여 귀하는 이 책을 귀하 기업집단 내에서만 복제, 배포 및 전시할 수 있습니다. 귀하는 귀하의 기업집단 외에서는 IBM의 명시적 동의 없이 이 책의 2차적 저작물을 만들거나 이 책 또는 그 일부를 복제, 배포 또는 전시할 수 없습니다.

권한

본 허가에서 명시적으로 부여된 경우를 제외하고, 이 책이나 이 책에 포함된 정보, 데이터, 소프트웨어 또는 기타 지적 재산권에 대한 어떠한 허가나 라이센스 또는 권한도 명시적 또는 묵시적으로 부여되지 않습니다.

IBM은 이 책의 사용이 IBM의 이익을 해친다고 판단하거나 위에서 언급된 지시사항이 준수되지 않는다고 판단하는 경우 언제든지 부여한 허가를 철회할 수 있습니다.

귀하는 미국 수출법 및 관련 규정을 포함하여 모든 적용 가능한 법률 및 규정을 철저히 준수하는 경우에만 본 정보를 다운로드, 송신 또는 재송신할 수 있습니다.

IBM은 이 책의 내용과 관련하여 아무런 보장을 하지 않습니다. 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여 (단 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증 없이 현 상태대로 제공합니다.

IBM 온라인 개인정보 보호정책

SaaS(Software as a Service) 솔루션을 포함한 IBM 소프트웨어 제품(이하 "소프트웨어 오퍼링")은 제품 사용 정보를 수집하거나 일반 사용자의 사용 경험을 개선하거나 일반 사용자와의 상호 작용을 조정하거나 그 외의 용도로 쿠키나 기타 다른 기술을 사용할 수 있습니다. 많은 경우에 있어서, 소프트웨어 오퍼링은 개인 식별 정보를 수집하지 않습니다. IBM의 일부 소프트웨어 오퍼링은 귀하가 개인 식별 정보를 수집하도록 도울 수 있습니다. 본 소프트웨어 오퍼링이 쿠키를 사용하여 개인 식별 정보를 수집할 경우, 본 오퍼링의 쿠키 사용에 대한 특정 정보가 다음에 규정되어 있습니다.

본 소프트웨어 오퍼링은 배치된 구성에 따라 세션 관리 및 인증의 용도로 각 사용자의 세션 ID를 수집하는 세션 쿠키를 사용할 수 있습니다. 쿠키를 사용하지 못하도록 할 수 있지만 이 경우 쿠키를 통해 사용 가능한 기능도 제거됩니다.

본 소프트웨어 오퍼링에 배치된 구성이 쿠키 및 기타 기술을 통해 최종 사용자의 개인 식별 정보 수집 기능을 고객인 귀하에게 제공하는 경우, 귀하는 통지와 동의를 위한 요건을 포함하여 이러한 정보 수집과 관련된 법률 자문을 스스로 구해야 합니다.

이러한 목적의 쿠키를 포함한 다양한 기술의 사용에 대한 자세한 정보는 IBM 개인정보 보호정책(http://www.ibm.com/privacy/kr/ko), IBM 온라인 개인정보 보호정책(http://www.ibm.com/privacy/details/kr/ko), "쿠키, 웹 비콘 및 기타 기술" 및 "IBM 소프트웨어 제품 및 SaaS(Software-as-a-Service) 개인정보 보호정책"(http://www.ibm.com/software/info/product-privacy) 부분을 참조하십시오.