IBM Security QRadar Incident Forensics

버전 7.3.0

사용자 안내서

IBM

참고

이 정보와 이 정보가 지원하는 제품을 사용하기 전에, 45 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 사용 소개

이 안내서에는 IBM® Security QRadar® Incident Forensics을 사용하여 보안 인시던트를 조사하는 데 대한 정보가 포함되어 있습니다.

대상 독자

조사자는 포렌식 저장소에 있는 문서 및 네트워크 트래픽에서 정보를 추출할 수 있습니다. 이 정보는 보안 인시던트 조사에 사용됩니다.

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 사용자를 위한 QRadar Incident Forensics V7.3.0의 새로운 기능

IBM Security QRadar Incident Forensics V7.3.0에서는 복구를 실행하는 사용자를 위한 PCAP(Packet Capture) 디바이스 선택사항을 소개합니다.

QRadar Incident Forensics 복구에 사용 가능한 PCAP 디바이스 선택사항

QRadar Incident Forensics 복구 실행 시 사용자 배치에서 PCAP 디바이스로부터의 트래픽만 보려면 **사용자 정의 캡처 디바이스**를 선택하십시오.

 PCAP 디바이스 선택사항에 대한 자세한 정보...

제 2 장 보안 조사

IBM Security QRadar Incident Forensics를 사용하여 대두되는 위협을 발견하고, 근본 원인을 판별하며, 재발생을 방지할 수 있습니다. 포렌식 도구를 사용하여 위협을 시작한 사용자, 위협 방법, 위해를 받은 항목에 분석을 신속하게 집중할 수 있습니다.

포렌식 조사자로서 사이버 범죄의 단계별 조치를 재추적하고 보안 인시던트와 관련된 원시 네트워크 데이터를 재구성할 수 있습니다.

조직이 처음으로 위협, 잠재적인 보안 위험 또는 준수 위반을 인식한 경우 범위를 평가하고, 관련된 엔티티를 식별하며, 동기를 파악하기 위한 목표를 설정합니다.

네트워크 보안, 내부자 분석, 사기 및 오용, 증거 수집 등과 같은 다양한 유형의 조사에서 특정 시나리오의 IBM Security QRadar Incident Forensics 도구를 사용할 수 있습니다.

1. 특정 IP 주소에 대한 네트워크 세션을 복구 및 재구성하십시오.
2. 작성된 인시던트에서 증거를 수집하기 위한 속성 카테고리를 조회할 수 있습니다.

   복구를 작성하면 인시던트가 작성됩니다.
3. 관심있는 정보만 검색하려면 검색 필터를 사용하십시오.
4. 조사 유형에 따라 필요한 증거를 제공하는 포렌식 도구를 선택하십시오.

의심스러운 컨텐츠

검색을 사용하여 공격자 또는 인시던트에 대해 알고 있는 컨텍스트 요소 또는 ID를 찾을 수 있습니다. 검색에서 키워드를 사용하는 경우 의심스러운 컨텐츠가 리턴됩니다. 의심 컨텐츠 중 일부는 조사와 관련되어 있을 수 있습니다.

데이터 피벗

검색 결과에서 리턴한 컨텐츠를 핫링크로 표시하면 데이터 피벗이 가능합니다. 예를 들어, "Tom"을 검색할 경우 결과에 Tom이 작성하거나 Tom이 채팅한 이메일 등 컨텍스트 정보가 포함될 수 있습니다. 이메일을 클릭하여 조회하면 Tom이 사용한 모든 자산 또는 엔티티(예: 첨부 파일 또는 컴퓨터 ID)가 링크로 표시됩니다. 조사자는 이 링크를 사용하여 신속하게 조사할 수 있습니다.

디지털 임프레션

데이터를 조사하고 빈도를 기반으로 엔티티(예: IP 주소, 이름 및 MAC 주소) 간의 관계를 맵핑하려면 디지털 임프레션을 사용하십시오. 관계의 빈도 및 방향을 조회하기 위해 하나 이상의 결과를 선택할 수 있습니다.

설문조사자

공격을 다시 추적할 수 있도록 활동 타임라인을 확인하려면 설문조사자를 사용하십시오. 설문조사자는 시간 순으로 세션을 재구성하고 문서를 정렬할 수 있습니다.

컨텐츠 필터링

컨텐츠 카테고리의 하위세트(예: 웹 메일, 포르노)를 조회하고 검색시 잡음 또는 상관없는 항목을 제거하려면 컨텐츠 필터링을 사용하십시오.

네트워크 보안 조사

QRadar Incident Forensics을 사용하여 중요한 자산을 대상으로 한 악성 활동을 발견 및 조사할 수 있습니다. 기본 제공되는 포렌식 도구를 사용하여 네트워크 보안 위반을 해결하고 다시 발생하지 않도록 할 수 있습니다.

이벤트가 발생하는 방식을 확인하고, 이벤트의 영향을 최소화하며, 다른 위반을 방지하기 위해 할 수 있는 모든 것을 수행하려면 QRadar Incident Forensics 조사 도구를 사용하십시오.

최초 감염자: 공격의 소스 식별

이 시나리오에서는 의심스러운 위반을 조직에게 경보합니다. 최초 공격 지점을 찾아서 소스의 격리를 시도합니다. 공격이 조직의 다른 부분으로 확산되는 것을 방지하기 위해 위해를 받은 엔티티를 조직이 차단해야 합니다.

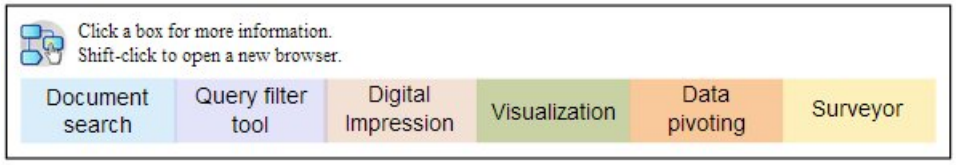
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 공격 유형을 판별합니다.
- 위협의 최초 시작점을 식별합니다.
- 악성 페이로드에 대한 상세 정보를 확보합니다.
- 악성 페이로드가 시작점을 너머 전파된 방식을 파악합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 악성 페이로드와 관련된 증상 특성을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 조사와 관련되지 않은 컨텐츠를 필터링하여 제외하려면 컨텐츠 카테고리를 사용하십시오.
3. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.
4. 악성 페이로드, 가해자 또는 대상의 확장된 관계를 탐색하려면 디지털 임프레션 및 시각화를 사용하십시오.
5. 최초 감염자를 식별하려면 데이터 피벗을 사용하고 데이터 링크를 따라가십시오.
6. 공격을 다시 추적할 수 있도록 활동 타임라인을 확인하려면 설문조사자를 사용하십시오.

위해를 받은 시스템

이 시나리오에서는 하나 이상의 시스템이 고급 사이버 공격 기술(예: 표적 공격, 피싱, 무차별 공격 또는 SQL 주입 공격)로 인한 위해를 받았음을 조직에게 경보합니다.

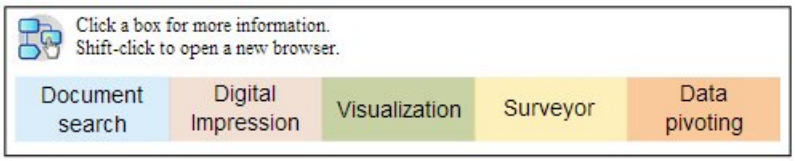
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 조직 내에서 위해의 범위를 확인합니다.
- 각 시스템에서 위해의 운영상 위험 유형을 파악합니다.
- 최초 공격에서 정리 활동 및 발견을 피하기 위해 수행한 주변 조치를 알아냅니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 악의적인 페이로드 또는 위해된 자산을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.
3. 디지털 임프레션 및 시각화를 사용하여 위해된 시스템으로 인한 엔티티 관계를 탐색하십시오.
4. 공격을 다시 추적할 수 있도록 활동 타임라인을 확인하려면 설문조사자를 사용하십시오.
5. 자유 형식의 검색, 데이터 피벗 및 컨텐츠 의심을 사용하여 데이터 카테고리에서 불일치하거나 의심스러운 상호작용을 감지하십시오.

권한없는 엔티티에 유출된 데이터

이 시나리오에서는 조직내 권한없는 엔티티 또는 외부 당사자에게 민감한 데이터가 유출되었음을 조직에게 경보합니다.

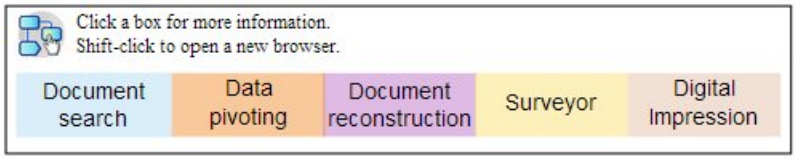
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 유출된 데이터의 특성 및 양을 판별합니다.
- 사용된 기술을 파악합니다.
- 가해자를 알아냅니다.
- 유출의 소스를 식별합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 유출된 데이터의 ID를 검색하려면 자유 형식의 검색을 사용하십시오.
2. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.

3. 데이터 재구성을 검토하여 유출된 전체 범위 또는 데이터 유출을 검토하십시오.
4. 관련된 모든 엔티티 관계를 탐색하려면 디지털 임프레션 및 시각화를 사용하십시오.
5. 공격을 다시 추적할 수 있도록 활동 타임라인을 확인하려면 설문조사자를 사용하십시오.
6. 데이터 유출의 동기를 감지하려면 자유 형식의 검색을 사용하십시오.
7. 누출된 다른 데이터에 대한 연계를 찾으려면 데이터 피벗을 사용하십시오.

내부자 분석 조사

공모, 방해 행위 및 액세스 오용을 발견하려면 QRadar Incident Forensics를 사용하십시오. 가해자, 협력자 및 위해를 받은 시스템을 식별하고 데이터 손실을 문서화하십시오.

액세스 권한의 오용

이 시나리오에서는 한 명 이상의 직원이 신임 정보를 오용하고 있거나 권한없는 활동을 위해 민감한 시스템 및 데이터에 액세스하기 위한 대리인으로 사용되고 있음을 조직에게 경보합니다.

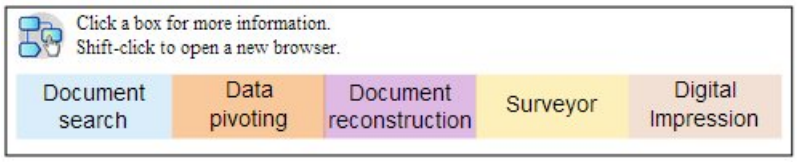
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 사용자의 ID를 판별합니다.
- 권한없는 활동에 ID를 사용하고 있는 사용자 또는 항목을 확인합니다.
- 액세스 권한의 오용 목적을 파악합니다.
- 엔티티에 오용될 수 있는 추가 ID가 있는지 평가합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 민감한 시스템 또는 데이터에 액세스하는 ID를 검색하려면 자유 형식의 검색을 사용하십시오.
2. 의심스러운 컨텐츠를 조회하거나, 자유 형식의 검색, 데이터 피벗 및 컨텐츠 필터링을 수행하여 의심스러운 액세스 시도를 확인하십시오.

3. 액세스되는 컨텐츠의 데이터 재구성을 조회하십시오.
4. 액세스의 패턴을 재추적하고 설문조사자의 빈도를 평가하십시오.
5. 단일 엔티티가 사용한 별명을 표시하려면 디지털 임프레션을 사용하십시오.

공모

이 시나리오에서는 한 명 이상의 이해 당사자가 서로 또는 외부 당사자와 공모하여 조직에 불리한 활동에 관여하고 있음을 조직에게 경보합니다.

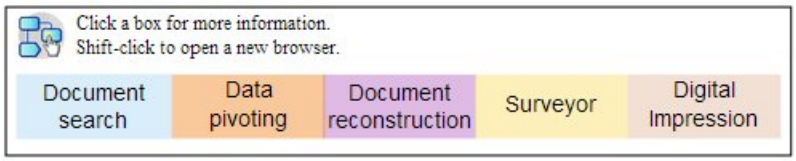
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 공모하는 엔티티를 판별합니다.
- 협력자 간의 상호작용 특성 및 패턴을 이해합니다.
- 스킴의 기저가 되는 컨텐츠를 찾아냅니다.
- 위험 범위를 이해하기 위해 스킴의 기간을 표시합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 관련된 엔티티의 ID를 검색하려면 자유 형식의 검색을 사용하십시오.
2. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.
3. 디지털 임프레션, 시각화 및 컨텐츠 필터링을 사용하여 의심스러울 수 있는 관계를 식별하십시오.
4. 설문조사자를 사용하여 관련된 엔티티의 활동을 추적함으로써 상호작용의 컨텐츠를 받으십시오.
5. 재구성된 문서를 검토하여 공모의 동기를 감지하십시오.
6. 자유 형식의 검색 및 데이터 피벗을 사용하여 공모 활동의 시작을 확인하십시오.

방해 행위

이 시나리오에서는 하나 이상의 이해 당사자가 운영을 방해하려고 시도함을 조직에게 경보합니다. 이해 당사자가 대리인으로 사용될 수도 있습니다.

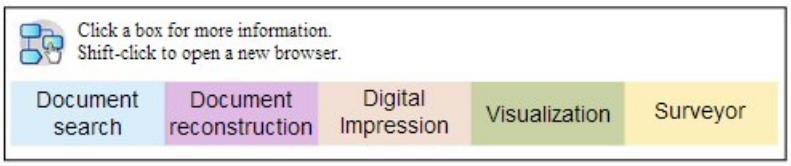
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 방해 행위를 식별합니다.
- 방해 행위에서 사용된 기술을 파악합니다.
- 방해의 영향과 범위를 평가합니다.
- 방해 행위에서 악용한 취약성을 지적합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 방해 행위의 증상을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.
3. 증상을 탐색하고 방해 행위의 ID를 발견하려면 시각적 탐색, 디지털 임프레션 및 컨텐츠 필터링을 사용하십시오.
4. 방해 행위의 활동을 추적하려면 설문조사자를 사용하십시오.
5. 방해 행위 역할 및 동기를 감지하려면 데이터 재구성을 사용하십시오.
6. 방해 행위에서 사용한 컨텐츠를 검토하려면 데이터 재구성을 사용하십시오.
7. 위해를 받은 시스템과 방해 행위가 사용된 절차를 확인하려면 자유 형식의 검색, 설문조사자 및 의심 컨텐츠를 사용하십시오.

사기 및 악용 공격 조사

권한없는 트랜잭션, 승인되지 않은 자원 할당, 프로토콜 이상 행동 및 정상적인 컨트롤 회피를 찾으려면 QRadar Incident Forensics를 사용하십시오.

권한없는 트랜잭션

이 시나리오에서는 비즈니스 운영에 부정적인 재무 영향을 미칠 수 있는 권한없는 트랜잭션에 대해 조직에게 경보합니다.

목표

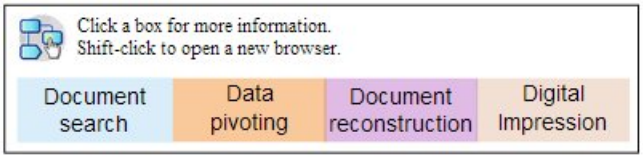
이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 권한없는 트랜잭션을 찾습니다.
- 권한없는 트랜잭션에 관련되고 이를 담당하는 엔티티를 식별합니다.

- 권한없는 트랜잭션의 빈도 및 추세를 파악합니다.
- 권한없는 트랜잭션의 위험 범위를 평가합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 일치하지 않거나 의심스러운 트랜잭션을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 해당 트랜잭션의 반복을 검색하려면 자유 형식의 검색 및 데이터 피벗을 사용하십시오.
3. 의심스러운 트랜잭션과 연관된 엔티티를 감지하려면 데이터 피벗 및 디지털 임프레션을 사용하십시오.
4. 재구성된 문서를 검토하여 수량 값을 표시하려면 트랜잭션의 컨텐츠를 알아내십시오.

자원의 승인되지 않은 할당

이 시나리오에서 조직은 비즈니스 운영에 부정적인 재무 영향을 미칠 수 있는, 자원의 승인되지 않은 할당을 의심하고 있습니다.

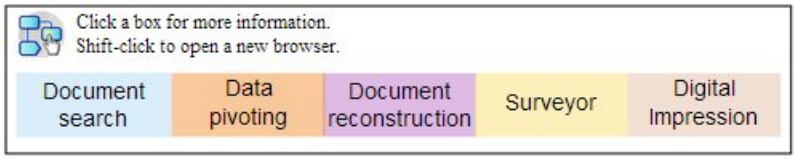
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 자원의 잘못된 할당을 찾습니다.
- 자원의 잘못된 할당에 관련되고 이를 담당하는 엔티티를 식별합니다.
- 자원의 승인되지 않은 할당에 대한 동기를 파악합니다.
- 잘못 할당된 자원의 크기와 범위를 평가합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 할당된 자원과 연관된 통신에는 자유 형식의 검색을 사용하십시오.

2. 자원의 승인되지 않은 할당을 만든 엔티티의 ID를 찾으려면 자유 형식의 검색, 데이터 피벗 및 디지털 임프레션을 사용하십시오.
3. 재구성된 문서를 검토하고 시각화를 사용하여 동기 평가와 관련된 상호작용의 컨텐츠를 처리하십시오.
4. 설문조사자를 사용하여 할당 활동을 다시 추적함으로써 잘못 할당된 자원 수량을 파악하십시오.

프로토콜 이상 행동 및 정상적인 컨트롤 회피

이 시나리오에서는 비즈니스, IT 프로토콜 및 정상적인 컨트롤을 회피하여 부정적인 재무 영향을 가져올 수 있음을 조직에게 경보합니다.

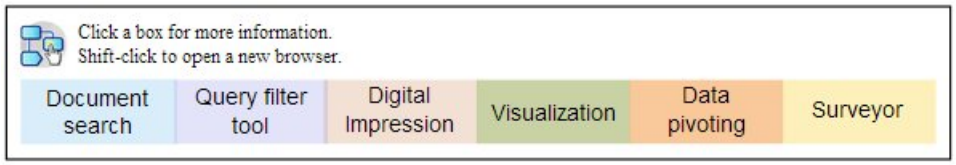
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 회피되는 프로토콜 및 정상적인 컨트롤을 평가합니다.
- 이 동작에 관련된 엔티티를 지적합니다.
- 이 엔티티의 동기를 파악합니다.
- 이상 행동의 편재성을 평가합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 프로토콜 또는 컨트롤에서 관리하는 비즈니스 프로세스를 검색하려면 자유 형식의 검색을 사용하십시오.
2. 프로토콜 및 정상적인 컨트롤을 간략하게 설명하는 문서와 상호 참조하려면 자유 형식의 검색, 데이터 피벗 및 데이터 재구성을 사용하십시오.
3. 프로토콜/컨트롤이 회피되는 특정 인스턴스를 감지하려면 컨텐츠 필터링, 자유 형식의 검색을 사용하십시오.
4. 관련된 엔티티 ID를 찾으려면 디지털 임프레션, 시각화, 데이터 피벗 및 컨텐츠 필터링을 사용하십시오.
5. 가능한 동기를 탐색하기 위해 엔티티 활동을 다시 추적하려면 설문조사자를 사용하십시오.

증거 콜렉션 조사

조직의 취약성 위험을 평가하고, 위협 또는 가해자를 식별하는 신뢰도를 정량화하고, 보안 사례를 세분화하려면 QRadar Incident Forensics를 사용하십시오.

위협 식별의 신뢰도

이 시나리오에서는 특정 위협, 악용 또는 취약성에 대해 조직에게 경보합니다. 정상적인 비즈니스 운영을 달리 대체할 수도 있는 개선 작업을 정당화하기 위해 연관된 위험에 대한 신뢰구간을 정량화하고자 합니다.

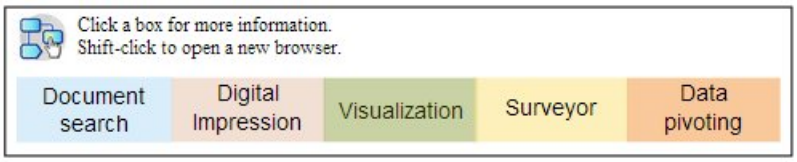
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 보안 위험에 대한 감응성을 검증합니다.
- 보안 위험의 증거가 있는지 판별합니다.
- 보안 위험의 범위와 재정적인 영향력을 평가합니다.
- 보안 위험의 특성을 파악합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 잠재적으로 시작점 대상인 엔티티를 사용하여 위협, 악용 또는 취약성을 검색하려면 자유 형식의 검색, 의심스러운 컨텐츠 및 데이터 피벗을 사용하십시오.
2. 발생 항목을 컴파일하려면 자유 형식의 검색 및 데이터 피벗을 사용하십시오..
3. 영향에 대한 참조를 제공하는 문서를 상호 참조하려면 자유 형식의 검색을 사용하십시오.
4. 영향을 받은 엔티티를 식별하려면 디지털 임프레션 및 시각화를 사용하십시오.
5. 위협 또는 가해자와 연관된 활동을 분석하려면 설문조사자를 사용하십시오.

보안 사례 세분화

새로운 동작 및 위험한 동작이 발견된 경우 조직에게 기존 보안 사례가 충분한지 평가하도록 합니다. 이 시나리오에서 조직은 당면한 위험에 대한 보안 룰의 효율성을 정량화하고자 합니다.

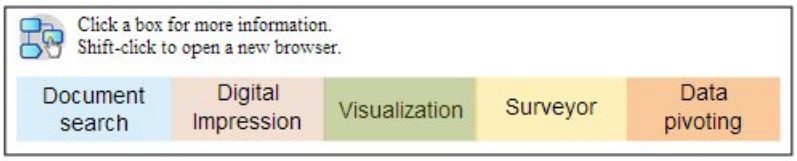
목표

이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 새로운 동작 또는 위험한 동작을 인식합니다.
- 기존 보안 룰의 효용성을 평가합니다.
- 동작인 운영 때문에 대두되는 보안 간격을 파악합니다.
- 제안된 보안 사례의 효율성을 평가합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 도메인 및 조직의 정보를 사용하여 새로운 동작 또는 위험한 동작(예: 모바일 사용자 및 클라우드 기반 서비스에 해당하는 동작)을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 의심 컨텐츠를 검사하고, 기존 보안 룰 또는 사례와 이 동작을 상호 참조하려면 설문조사자를 사용하십시오.
3. False Positive의 빈도에 대한 보안 룰의 경보를 분석하려면 자유 형식의 검색, 설문조사자, 컨텐츠 재구성 및 시각화를 사용하십시오.
4. 기존 보안 룰 또는 사례에서 발견하지 못한 잘못된 미경고를 감지하려면 자유 형식의 검색, 설문조사자, 컨텐츠 재구성, 데이터 피벗 및 시각화를 사용하십시오.

위험 평가

이 시나리오에서는 특정 취약성, 악용 또는 악성 동작을 설명하는 보안 게시판에서 조직에서 위험 평가를 수행하라고 요청합니다. 위험 평가에서 감염될 수 있는 조직과 이미 위해를 받은 조직을 판별합니다.

목표

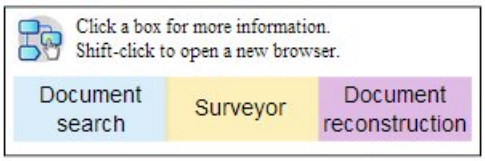
이 조사에서 문제점을 해결하기 위한 조직의 목표는 다음과 같습니다.

- 조직에서 식별된 취약성의 존재를 평가합니다.
- 외부 당사자의 악성 존재를 발견합니다.
- 위해의 증거를 알아냅니다.
- 조직이 악용의 희생자인지 판별합니다.

- 사용자의 ID를 판별합니다.

조사

포렌식 탭의 도구를 사용하면 조사하는 데 유용합니다.



1. 보안 게시판에 지정된 취약성, 악용 또는 기타 악성 동작의 특성을 검색하려면 자유 형식의 검색을 사용하십시오.
2. 표시기를 파생하는 다른 데이터 또는 조사를 상호 참조하려면 자유 형식의 검색을 사용하십시오.
3. 식별된 취약성을 악용한 상호작용을 조사하려면 설문조사자를 사용하십시오.
4. 제품에서 플래그 지정한 의심 컨텐츠를 검사하십시오.
5. 데이터 재구성을 사용하여 위험한 상호작용의 기본이 되는 컨텐츠를 검토하십시오.
6. 잠재적으로 위험한 엔티티의 활동을 다시 추적하려면 설문조사자를 사용하십시오.

제 3 장 포렌식 조사 시작하기

IBM Security QRadar Incident Forensics에서 포렌식 조사를 시작하려면 **빠른 시작** 메뉴를 사용하여 포렌식 저장소에 있는 데이터를 탐색하고 필터링합니다. 이 런치패드는 검색을 시작하거나 엔티티의 관계를 얻을 때 사용할 수 있는 사전정의된 요약 조회를 포함합니다.

시작하려면 다음 지침을 따르십시오.

1. 포렌식 복구를 시작하거나 **오펜스** 탭의 오펜스에서 검색하십시오.
   - 오펜스 또는 임의의 IP 주소를 마우스 오른쪽 단추로 클릭하고 포렌식 복구를 실행하는 경우 포렌식은 캡처 디바이스에서 지정된 시간 범위의 원시 캡처 데이터를 검색하고 문서를 추출하여 다시 빌드한 후 포렌식 저장소에 결과를 추가합니다.
   - 오펜스 또는 IP 주소를 마우스 오른쪽 단추로 클릭하고 포렌식 검색을 실행하는 경우 포렌식 저장소가 필터링되고 해당 IP 주소를 검색합니다. 이렇게 하면 **포렌식** 탭의 기본 그리드에 결과가 표시됩니다. 조회를 빌드하여 검색을 세분화할 수 있습니다.

   QRadar Incident Forensics에서 검색 요청을 수신하면 패킷 캡처 데이터를 처리하고 의도된 받는 사람에게 전송한 형식으로 다시 넣습니다. 예를 들어, Microsoft Word 문서는 Word 파일로 복구됩니다. VoIP(Voice-over-IP) 통화는 오디오 파일로 복구됩니다. 그러면 복구된 파일은 메타데이터 및 파일 컨텐츠를 사용하여 검색 가능하도록 색인화됩니다.
2. **포렌식** 탭에서 **빠른 시작**을 클릭하십시오.

   자유 양식 검색을 수행하고 고유한 조회를 빌드하는 대신, 복구 또는 검색을 실행한 후에 **포렌식** 탭의 **빠른 시작** 메뉴에서 사전정의된 조회를 사용하여 조사를 빠르게 시작할 수 있습니다. 예를 들어, **사용 불가능 컨텐츠** 카테고리를 검색하고 **엔티티 경보**와 같은 조회 중 하나를 실행할 수 있습니다. 사용 불가능 컨텐츠는 의심스러운 활동을 의미하는 컨텐츠에서 정의된 룰 세트에 기반합니다. 엔티티 경보는 보안 정책 위반과 관련된 잠재적인 악성 엔티티에 플래그를 지정합니다.

   컨텐츠 카테고리화 및 필터링 기능은 리턴되는 데이터 볼륨을 줄이는 데 도움이 됩니다.
3. **격자**에서 검색할 문서를 선택하십시오.

QRadar Incident Forensics에서는 우선순위가 지정된 검색 결과를 리턴합니다. 검색 엔진 최적화가 인터넷 검색에서 사이트의 우선순위를 지정하는 방식과 마찬가지로 목록 맨 위에 가장 빈도가 높은 항목이 나타납니다.

링크를 클릭하고 문서와 연관된 메타데이터를 검색하여 데이터 피벗을 시작할 수 있습니다. 데이터 피벗 기능은 다양한 검색 보기와 데이터 요약을 제공합니다.

4. 모든 조치 및 보안 인시던트 사이에서 관계를 조사하려면 문서 보기에서 링크를 선택하고 **관계 가져오기**를 마우스 오른쪽 단추로 클릭하십시오.

   속성을 조사한 후에 엔티티를 연결하여 수집한 정보를 필터링하십시오.

5. **디지털 임프레션**을 클릭하여 ID 트레일을 추적하고 컴파일된 연관 세트를 가져오십시오.

   디지털 임프레션은 악성 사용자 트레일을 추적하여 의심스러운 공격자 또는 내부 공격자를 식별하는 데 도움이 되는 메타데이터의 색인입니다. 이러한 관계를 빌드할 때 QRadar Incident Forensics에서는 네트워크 소스(예: IP 주소, MAC 주소, TCP 포트와 프로토콜)의 데이터를 사용합니다. 그리고 대화 ID와 같은 정보를 찾고 워드 처리 또는 스프레드시트 애플리케이션에서 작성자 ID와 같은 정보를 읽을 수 있습니다. 디지털 임프레션은 다른 사용자나 엔티티의 식별 정보에 엔티티 ID를 링크하여 연관 관계를 밝힐 수 있습니다.

QRadar Incident Forensics 검색 및 책갈피

조사자는 IBM Security QRadar Incident Forensics를 사용하여 문서 및 네트워크 트래픽에서 관련 데이터를 추출할 수 있습니다.

레코드 검색 및 책갈피 설정

직관적인 포렌식 활동을 가능하게 하기 위해 QRadar Incident Forensics는 패킷 데이터를 검색하고 다른 컨텐츠를 수집합니다. 이 기술은 보안 인시던트 조사를 지원하기 위해 검색 방식의 데이터 탐색, 세션 재구성 및 포렌식 정보를 제공합니다.

조사자는 먼저 큰 단위의 조치에 조사의 초점을 맞춘 다음 찾은 결과를 관련성이 높은 최종 결과 세트로 미세 조정합니다. 단순한 고급 방식은 먼저 수많은 레코드를 검색하여 책갈피를 설정한 다음, 책갈피가 설정된 레코드에 초점을 맞춰 최종 레코드 세트를 식별하는 것입니다. 관련된 자료를 판별하고, 항목을 포함 또는 제외하도록 조회를 변경합니다. 해당 자료를 사용하여 가설을 증명합니다.

새로운 단서를 개발할 때 다른 방법을 사용하여 이 단서를 추적할 수 있습니다. 시각화 및 분석 도구를 사용하여 관련성 결과를 수동 및 자동으로 평가할 수 있

습니다. 또한 다양한 조회를 사용하여 같은 문제의 다른 측면을 확인할 수도 있습니다.

책갈피 설정된 결과 처리

조사에 중요한 결과를 찾은 경우 나중에 보다 심층적인 조사와 최종 판별을 수행하기 위해 해당 결과에 책갈피를 설정할 수 있습니다. 필요하다고 생각되는 것보다 많이 책갈피를 설정하십시오. 의심스러운 경우 책갈피를 설정하십시오. 관련이 없는 자료는 제거하고 관련이 있는 자료에만 초점을 맞출 수도 있습니다.

관련된 결과 세트에 책갈피를 설정한 후에는 조사 내용을 미세 조정할 수 있습니다.

1. 시각화 및 분석 도구를 통해 책갈피가 설정된 각 문서를 조사하십시오.
2. 케이스 메모를 문서에 첨부하고 케이스 관련성에 대한 각 문서에 대해 최종 결정을 내리십시오.
3. 레코드가 관련되지 않은 경우 책갈피를 제거하십시오.

   조사 프로세스에서 저장소의 관련 자료를 식별했으므로 책갈피가 설정된 관련 레코드 세트는 이미 가지고 있습니다.
4. 관련 레코드를 인쇄하거나, 내보내거나, 처리하십시오.

문서 검색 및 조사

조사자는 보안 인시던트가 발생하는 방식에 대한 단서나 가설과 관련된 문서를 검색합니다.

검색

조사자는 대량의 문서(이들 문서의 대부분은 케이스와 관련이 없음)를 수동으로 정밀하게 조사하는 대신, 포렌식 저장소를 사용하여 원하는 특성을 충족하는 문서를 추출합니다. 예를 들어 특정 기간 내에 발생한 문서는 의심스러운 공격자가 전송하거나 수신한 문서 또는 관심 주제와 관련이 있습니다.

검색은 구체적일 수 있습니다. 예를 들어 "Mission Alpha"라는 정확한 문자열을 찾을 수 있습니다. 또는 검색은 일반적일 수 있습니다. 예를 들어 저장소에 있는 모든 주민등록번호를 찾을 수 있습니다.

검색은 단순하고 하나의 기준만 기반으로 할 수 있습니다. 복잡한 검색 결과는 여러 조건을 충족해야 합니다. 예를 들어, 복잡한 검색의 경우 특정 주제에 대해 의심스러운 두 공격자가 주고 받은 모든 이메일을 찾되, 첨부 파일이 포함된 이메일을 제외할 수 있습니다. 검색의 목적은 의미 있는 작업 세트로 레코드를 신속하고 정확하게 줄이기 위한 것입니다. 조사자가 더 적은 양의 문서 세트를 조사할 경우 문서가 케이스와 관련된 가능성이 더 높아집니다.

포렌식 복구

패킷 캡처 디바이스에서 원시 패킷 캡처 데이터를 검색하려면 하나 이상의 IP 주소 또는 포트에서 포렌식 복구 작업을 실행하십시오.

IP 주소 또는 포트에서 복구 실행

포렌식 복구 를 실행하여 캡처 디바이스에서 원시 캡처 데이터를 검색할 수 있습니다. 복수의 IP 주소 또는 포트에서 복구를 실행할 수 있습니다. IP 주소 또는 포트를 입력하지 않은 경우 모든 TCP 및 UDP 트래픽이 복구됩니다. 여러 IP 주소 또는 포트를 입력한 경우 쉼표를 사용하여 구분해야 합니다.

QRadar에서 IP 주소 또는 포트를 마우스 오른쪽 단추로 클릭하거나 포렌식 탭에서 **복구 실행** 아이콘  을 선택하여 포렌식 복구를 실행하십시오.

제한사항: 일반적으로 약 7개의 IPv4 주소와 7개의 포트 또는 한 번에 최대 255자를 입력할 수 있습니다. **IP 주소** 및 **포트** 필드는 다른 절과 결합하여 필터 문자열을 작성합니다. 필터 문자열은 255자를 초과할 수 없습니다.

복구 재실행

포렌식 탭의 결과 그리드에서 복구 재실행 옵션을 사용하여 이전에 작성된 복구를 실행할 수 있습니다. 예를 들어 해당 결과에서 불완전한 데이터가 리턴되는 경우 포렌식 복구를 재실행하여 다른 IP 주소를 포함시키거나 이전에 실행된 복구 작업에 지정되어 있는 시간 프레임을 변경할 수 있습니다.

이전 포렌식 복구 작업을 재실행하려면 **이 포렌식 복구 재실행**을 클릭하십시오. 복구 작업을 재실행하면 포렌식 복구 페이지에 이전에 실행된 값이 포함됩니다. 동일한 복구를 다시 실행하거나 자동으로 생성된 값을 변경할 수 있습니다.

작업이 완료된 경우에만(상태가 완료됨, 취소됨 또는 실패인 경우) 복구를 재실행할 수 있습니다.

포렌식 케이스

케이스란 가져온 문서 및 패킷 캡처 파일로 구성된 콜렉션에 대한 논리적 컨테이너입니다.

케이스는 케이스 작성 권한이 있는 관리자 또는 조사자가 작성할 수 있습니다. 관리자는 케이스를 작성하여 조사자에게 지정할 수 있습니다. 조사자는 IBM Security QRadar에서 IP 주소를 통한 패킷 캡처 데이터를 검색할 때 새 케이스를 작성할 수 있습니다.

관련 태스크:

『pcap 파일 및 문서를 외부 시스템에서 포렌식 케이스로 업로드할 수 있음』
외부 데이터를 특정 케이스에 업로드할 수 있습니다.

콜렉션

콜렉션을 사용하여 패킷 캡처(pcap) 데이터 파일, PDF 또는 네트워크 스트림 등의 특정 소스에서 관련 데이터를 그룹화할 수 있습니다.

콜렉션은 관련 데이터 그룹을 식별하고 관리하는 데 사용됩니다. 조사가 완료되면 콜렉션에 있는 그룹 데이터를 신속하게 삭제할 수 있습니다.

콜렉션은 관리자 또는 조사자가 작성할 수 있습니다. 관리자는 콜렉션을 작성하여 IBM Security QRadar Incident Forensics에 수동으로 데이터를 로드합니다. 관리자는 또한 케이스에 콜렉션을 추가할 수도 있습니다. 조사자는 IBM Security QRadar에서 IP 주소를 통한 패킷 캡처 데이터 검색을 시작할 때 새 콜렉션을 작성할 수 있습니다.

콜렉션 및 콜렉션 이름에 대해 다음과 같은 룰을 고려하십시오.

- 콜렉션 이름은 고유해야 합니다.
- 케이스에는 콜렉션이 하나 이상 포함됩니다.
- 콜렉션을 여러 케이스에 추가할 수 있습니다.
- 조사자가 같은 콜렉션이 포함된 케이스를 두 개 소유하고 있을 경우 중복된 데이터가 리턴됩니다.
- 새 pcap이 업로드될 때 콜렉션 이름이 고유하지 않을 경우 새 pcap이 업로드되기 전에 원래 콜렉션이 삭제됩니다.

pcap 파일 및 문서를 외부 시스템에서 포렌식 케이스로 업로드할 수 있음

외부 데이터를 특정 케이스에 업로드할 수 있습니다.

시작하기 전에

관리자가 외부 파일을 업로드하려는 사용자의 보안 FTP 권한을 사용 가능하게 해야 합니다.

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

여러 파일을 케이스에 업로드할 수 있습니다.

제한사항: 케이스 이름은 고유해야 합니다. 기존 케이스와 동일한 이름을 가진 케이스를 만들 수 없습니다.

프로시저

1. 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.
2. QRadar Incident Forensics 서버에 연결하고 새 디렉토리를 만드십시오.
3. pcap 파일을 FTP 및 저장하려면 케이스에 대해 작성한 디렉토리에서 `singles`라는 디렉토리를 만들고 pcap 파일을 해당 디렉토리로 끄십시오.
4. pcap 파일이 아닌 다른 파일 유형을 FTP 및 저장하려면 케이스에 대해 작성한 디렉토리에서 `import`라는 디렉토리를 만들고 파일을 해당 디렉토리로 끄십시오.
5. FTP 서버를 다시 시작하려면 다음 명령을 입력하십시오.

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

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

결과

사용자는 **포렌식** 탭의 도구 중 하나에서 해당 케이스를 볼 수 있습니다.

포렌식 저장소 조회

조사자는 포렌식 데이터베이스에서 검색할 문서의 특성을 지정할 수 있습니다. 조사할 문서 세트를 찾는 데 다중 조회가 사용됩니다.

작은 문서 세트를 수동으로 조사하고 다중 조회를 수행하는 것이 전체 저장소를 정밀하게 조사하는 것보다 낫습니다. 후속 조회 및 세분화된 조회는 대개 관련 없는 문서를 조사하는 동안에 수행됩니다.

수량이 늘어나고 조회 용어가 특수할 경우 관련성 결과 세트가 많아집니다. 목표는 원하는 결과에 대해 아는 만큼 정의하고 가능하면 매우 구체적으로 정의하는 것입니다. 조회 용어는 검색 기준에 원하는 만큼 입력할 수 있습니다. 용어는 공백 또는 부울 연산자로 구분하십시오. 공백으로만 구분된 용어는 부울 논리 연산자 OR를 의미합니다. OR 연산자는 어떤 용어를 찾더라도 동등하게 바람직함을 의미합니다. 가장 많은 검색어를 충족하는 결과가 목록의 맨 위에 배치되어 조회 용어와의 일치 정도를 나타냅니다.

하나의 검색 기준은 조회 용어라고도 합니다. 검색에는 일반적으로 둘 이상의 조회 용어가 필요합니다. 단일 검색에 대한 조회 용어 세트는 조회 문자열이라고도 합니다. 조회를 공식으로 나타내는 데는 연습이 필요하지만, 어렵지는 않습니다. 몇 개의 조회 용어를 알고 원하는 조합으로 용어를 작성하고 부정하는 방법을 학습하면 됩니다. 조회 문자열은 QRadar Incident Forensics에 저장되므로, 데이터에 대해 보다 잘 알게 될 때 검색 내용을 지속적으로 미세 조정할 수 있습니다.

관련 태스크:

33 페이지의 『관계 및 연관 시각화』
시각화 창에서는 복구된 문서에서 속성 간 관계를 검토할 수 있습니다. 예를 들어 특정 이메일 주소와 통신하는 이메일 주소를 조사할 수 있습니다.

자유 형식 조회 용어

조사자는 조회 용어를 **포렌식** 탭의 검색 기준 필드에 입력하여 정확하게 일치하는 문자열을 검색할 수 있습니다. 한 단어 또는 여러 단어 조회를 사용할 수 있습니다.

다음 표는 사용 가능한 검색 조회의 유형에 대해 설명합니다.

표 *1.* 자유 형식 조회의 유형

검색 조회의 유형	설명	예
한 단어 조회	문서에서 하나의 용어를 검색합니다.	puppies
와일드카드를 사용하는 단일 조회	조회 용어의 중간 또는 끝에서 1자 이상 일치하는 문자를 검색합니다. **제한사항:** 와일드카드 문자는 검색의 첫 글자로 사용할 수 없습니다.	te?t test* te*t
여러 단어 조회	검색 결과가 조회 용어 관련성 순서로 리턴되도록 지정합니다. 두 조회 용어를 모두 포함하는 문서가 먼저 나열되고, 조회 용어 중 하나만 포함하는 문서가 그 뒤에 나열됩니다. 조회 용어 하나만 포함하는 문서의 경우 개별 조회 용어의 발생 횟수에 따라 순위가 지정됩니다.	free puppies

표 1. 자유 형식 조회의 유형 (계속)

검색 조회의 유형	설명	예
큰따옴표를 사용하는 여러 단어 조회	정확한 문자열과 일치합니다. 두 단어를 모두 포함하지만 이 순서로 되어 있지 않은 유사한 문서는 결과로 리턴되지 않습니다. 사실상 큰따옴표는 이 두 단어를 하나의 문자열 또는 조회 용어로 전환합니다. 즉, 검색 엔진에서 별도의 두 단어로 인식되지 않습니다.	"free puppies"
AND 연산자를 사용하는 여러 단어 조회	두 조회 용어가 문서에 존재하여 일치하도록 지정합니다. 조회 용어는 어떤 순서로 되어 있든지 상관없으며, 서로 근접해 있을 필요는 없습니다.	free AND puppies

메타데이터 태그

조사자가 관련 문서에서 정확한 결과 세트를 검색할 수 있도록 공통 엔테티에 태그가 지정됩니다.

세션, 문서 또는 프로토콜의 유형에 따라 인시던트 포렌식 인덱스에 여러 메타데이터 필드를 사용할 수 있습니다.

메타데이터 태그 이름을 지정할 경우 해당 이름은 정확하고 포렌식 저장소에 존재해야 합니다.

다음 표는 메타데이터 태그 검색의 유형을 보여줍니다.

표 2. 메타데이터 태그 검색

메타데이터 태그 검색의 유형	형식	예
표준	`MetadataTag:<value>`	`ApplicationProtocol:http`
와일드카드	`MetadataTag:*`	`CreditCardNumber:*`
범위	`MetadataTag:[<start value> TO <end value>`	`Duration:[30 TO 56]`

관련 개념:

26 페이지의 『문서 어노테이션』
조사자는 문서에 책갈피를 설정하고 문서에 메모를 추가하여 케이스에 포함된 문서에 대한 아이디어와 논리적 근거를 추적할 수 있습니다.

부울 조합

단순 부울 연산자로 여러 개의 조회 용어를 연결하여 높은 표적성의 조회 문자열을 작성할 수 있습니다. 올바른 형식의 이러한 조회 문자열은 조사자가 찾고 있는 것과 정확히 일치하는 결과를 리턴할 수 있습니다.

기본 부울 연산자는 AND, OR, NOT, ()입니다. AND 연산자는 두 조회 용어가 문서에서 일치해야 함을 지정합니다. OR 연산자는 둘 중 한 조회 용어를 문서에서 찾을 수 있음을 지정합니다. NOT 연산자는 부정 처리된 조회 용어와 일치하는 결과를 부정하거나 제거합니다. () 연산자는 조회 용어와 값을 그룹화하여 명확한 구문을 위해 세트에 함수를 적용하거나 하나의 함수에 여러 값을 적용할 수 있습니다.

부울 연산자는 대문자여야 합니다.

다음 표는 조회 문자열의 부울 연산자 및 예를 보여줍니다.

표 *3.* 조회 문자열의 부울 연산자

부울 연산자	**조회 문자열 예**	**예 설명**
AND	`TcpPort:80 AND Protocol:http`	두 조회 용어는 표준 웹 트래픽을 모두 찾는 데 사용됩니다. 테스트가 포트 8080에서 발생할 경우 두 조회 용어 둘 다 true가 아니므로 일치가 아닙니다.
OR	`Collection:yahoo* OR Collection:cnn* OR Collection:msn*`	이 조회 용어는 포렌식 저장소에 있는 Yahoo, CNN 및 MSN 문서 콜렉션에서 제공하는 결과로 결과를 제한하는 데 사용됩니다.
NOT	`ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080 OR 81)`	비표준 포트를 사용하여 트래픽을 검색합니다. 첫 번째 조회 용어는 표준 HTTP 트래픽을 찾고, 두 번째 조회 용어는 허용된 HTTP 포트를 사용하고 있는 모든 트래픽을 제거합니다.

()	`(ApplicationProtocol:http AND NOT ServerTcpPort:(80 OR 8080)) OR (ApplicationProtocol:pop* AND NOT ServerTcpPort:110)`
	
	`NOT (Collection:yahoo* OR Collection:cnn* OR Collection:msn*)`
		이 조회는 괄호를 효과적으로 사용하여 복잡한 목표를 달성합니다. 괄호가 없을 경우 이 조회를 공식으로 나타내고 디버그하는 데 더 길어지고 더 복잡해집니다.

조회 빌더 도구

조회 빌더 도구를 사용하여 검색을 작성하거나 저장된 검색을 관리할 수 있습니다.

조회 빌더 도구는 조회 용어의 분류된 목록을 사용하는 강력한 검색을 작성하는 프로세스를 예제와 함께 조사자에게 안내합니다.

표 *4.* 조회 빌더 도구의 매개변수

매개변수	**설명**
카테고리 선택	**필드 선택** 목록에서 사용 가능한 메타데이터 태그 목록을 필터링합니다.

표 4. 조회 빌더 도구의 매개변수 (계속)

매개변수	설명
필드 선택	포렌식 저장소에 있는 정보에 태그를 지정하는 데 사용되는 메타데이터 태그입니다.
조회 예제	**조회 입력** 필드에 있는 조회를 실행하고 결과 수를 보고합니다.
새로 작성	**조회 삽입**을 클릭하면 기존 조회를 새 조회로 바꿉니다.
AND	**조회 삽입**을 클릭하면 새 조회를 기존 조회와 결합합니다. 문서는 두 조회 용어와 일치해야 합니다.
OR	**조회 삽입**을 클릭하면 새 조회를 기존 조회와 결합합니다. 문서가 둘 중 한 용어와 일치해야 합니다.

조사자는 파일 시스템의 폴더에 검색을 저장하고 구성하여 조사자 간에 공유할 수 있습니다. 조사자는 참조, 관리 및 이해를 위해 저장된 조회에 대해 설명 또는 이름을 사용합니다.

조회 탭의 **조회 사용** 기능은 실행을 위해 채워진 **검색 기준 입력**으로 저장된 조회를 전송하는 데 사용됩니다.

조사자는 실행하려는 조회를 선택한 다음 **조회 삽입**을 클릭하는 방법으로 이전 조회 목록을 사용하여 이전에 실행된 조회를 찾아 다시 실행할 수 있습니다.

조회 필터 도구

조회 필터 도구는 활성 데이터를 사용하여 지속적 필터를 작성할 수 있는 시각적 단서를 제공합니다.

조회 필터는 조회 문자열로 질의되는 활성 문서 세트를 줄여주는 지속적 백그라운드 필터입니다. 이 필터를 통해 사용자는 정적 조회 용어가 포함된 조회 문자열을 오버로드하지 않고도 사용 가능한 문서 세트를 줄일 수 있습니다. 따라서 사용자는 조회 문자열을 보다 잘 제어할 수 있습니다.

조회 필터는 케이스 독립적 필터 유형 목록, 동적 업데이트 및 실시간 결과 요약 기능을 제공하므로 조사 작업을 시작하기 좋은 도구입니다. 필터 유형 목록은 사용자가 사용할 수 있는 케이스 내에서 발견된 모든 값으로 채워집니다. 사용자는 자신이 소유한 케이스 내에 포함된 데이터를 신속하게 확인할 수 있습니다. 필터 유형 목록 항목을 선택하거나 지우면 자동으로 결과 요약이 업데이트됩니다. 사용자는 필터 사용 시 필터의 효율성 및 남아 있는 문서 세트의 양을 파악할 수 있습니다.

기본 조회 필터를 튜닝하는 것은 재사용하려는 조회에는 권장되지 않습니다. 보존하려는 조회의 경우 조회 필터를 새로 작성해야 합니다. 기본 조회 필터를 수

정한 경우 이후 검색 조회에서 문서가 잘못 제외되는 것을 방지하기 위해 작업이 완료된 경우 해당 필터를 재설정해야 합니다.

활성 필터의 결과

조사자는 조회 필터 도구의 결과 요약 섹션에 있는 활성 필터의 결과를 확인할 수 있습니다.

필터가 변경되면 총 문서 수와 사용 가능한 문서 수를 표시하기 위해 요약 정보가 업데이트됩니다. 총 문서 수는 필터를 적용하기 전에 조사자가 사용할 수 있는 문서 수입니다. 사용 가능한 문서 수는 필터를 적용한 후에 사용 가능한 문서 수입니다. 조사자는 이 개수를 사용하여 필터의 효율성을 판단하고 작성할 때 필터를 적절하게 조정할 수 있습니다.

조회 필터 도구의 검색 필터

조사자는 지정된 케이스에 대한 데이터를 필터링할 수 있습니다. 데이터는 필터 유형(예: IP 주소 또는 MAC 주소)에 따라 그룹으로 구분됩니다.

조사자는 로직 조치 전환을 사용하여 목록에서 선택된 항목을 포함시키거나 제외시킬 수 있습니다.

각 검색 필터 그룹에는 로직 조치 전환이 있는데, 목록에서 선택된 항목을 포함하거나 제외하도록 이 전환을 설정할 수 있습니다. 포함하도록 설정할 경우 목록에 있는 항목이 논리적 AND와 결합됩니다. 즉, 선택한 모든 항목이 사용 가능한 각 문서에 포함됩니다. 제외하도록 설정할 경우 논리적 OR가 사용됩니다. 즉, 선택한 항목이 사용 가능한 각 문서에 포함되지 않습니다.

조사자는 **UserQuery** 그룹을 사용하여 필터에 추가할 고유한 조회 문자열을 공식으로 나타낼 수 있습니다.

검색에서 리턴된 문서 수 제한

IBM Security QRadar Incident Forensics 조회에 필터를 추가하여 검색 결과 페이지에 표시되는 문서 유형이나 수를 제한할 수 있습니다.

프로시저

1. **포렌식** 탭에서 **조회 필터** 아이콘을 클릭하십시오.

   데이터는 필터 유형에 따라 그룹으로 구분됩니다.
2. 검색 필터 창에서 각 필터 유형에 대해 **포함** 또는 **제외**를 클릭하여 검색 결과에서 문서를 포함할지 여부를 선택하십시오.
3. 필터 그룹에서 항목을 찾으려면 다음 단계를 수행하십시오.
   a. **필터 유형** 컬럼에서 필터 그룹을 확장하십시오.
   b. 검색 창에서 기준을 선택하고 **찾기**를 클릭하십시오.

웹 카테고리 필터 그룹에서 레코드를 검색하면 일치하는 모든 카테고리 필드가 표시됩니다. 예를 들어, **웹 카테고리 같음 대화**를 검색하면 **대화** 및 관련 카테고리(예: **인스턴트 메시징**, **웹 메일/통합 메시징**, **검색 엔진/웹 카탈로그/포털**, **클라우드**)가 표시됩니다.

문서 어노테이션

조사자는 문서에 책갈피를 설정하고 문서에 메모를 추가하여 케이스에 포함된 문서에 대한 아이디어와 논리적 근거를 추적할 수 있습니다.

상호작용 중 교환되는 문서의 순서를 시간순으로 표시하는 그리드의 설문조사자 도구 및 기본 결과 화면에서 문서에 책갈피를 설정할 수 있습니다. 조회와 조사는 복잡할 수 있으므로 조사자는 관심이 덜한 문서를 비롯한 모든 레코드에 책갈피를 설정합니다. 책갈피를 사용하면 복잡한 조회와 조사를 다시 작성할 필요가 없습니다. 레코드에 책갈피를 설정한 후에는 어노테이션을 작성할 수 있습니다.

조사 중 둘 이상의 경로를 따라가야 하는 경우가 있습니다. 브라우저 기능을 사용하면 현재 있는 탭을 복제할 수 있습니다. 탭을 복제할 경우 되돌아와서 추가 경로를 따라가거나 분기점에 도달하는 방법을 기억할 필요가 없습니다. 현재 탭을 필요한 횟수만큼 복제할 수 있습니다. 다른 탭에 있는 다른 경로를 따라가서 관련 문서에 책갈피를 설정하십시오. 책갈피가 설정된 각 문서에 도달하는 경로를 지정하는 메모를 추가할 수 있습니다.

메모는 조사 중 생각을 기록하는 한 방법이며, 관리자만 제거할 수 있습니다. 조사자의 사용자 ID 및 입장한 시간소인으로 메모에 태그가 지정됩니다. 문서를 내보낼 경우 메모는 재구성된 문서와 해당 속성이 포함된 출력입니다.

관련 개념:

22 페이지의 『메타데이터 태그』
조사자가 관련 문서에서 정확한 결과 세트를 검색할 수 있도록 공통 엔테티에 태그가 지정됩니다.

제 4 장 조사 도구

조사자는 설문조사자, 디지털 임프레션, 내보내기 및 시각화 도구를 사용하여 데이터를 여러 가지 방식으로 관리할 수 있습니다.

검색 결과 페이지는 **포렌식** 탭의 기본 페이지입니다. 검색 결과는 **그리드** 탭에 제공됩니다. 조사자는 그리드의 검색 결과를 사용하여 문서를 신속하게 검색하고 액세스할 수 있습니다. **그리드** 탭에서 설문조사자, 디지털 임프레션, 내보내기 및 시각화 도구를 사용하여 추가로 조사할 수 있습니다.

행 표시기

행 표시기는 지정된 결과 세트에 리턴되는 각 문서에 대한 고유 ID를 제공합니다. 행 표시기를 사용하여 문서 및 필요한 모든 관련 문서를 재구성된 보기 시각화 도구로 전송할 수 있습니다.

행 정렬

그리드에 표시되는 행을 정렬할 수 있습니다. 총 결과 수는 그리드에 표시되는 결과 수보다 클 수 있으므로 전체 결과 세트를 정렬할 수 없습니다.

본 문서 표시기

본 문서 표시기는 조사자가 문서를 봤는지 여부를 나타내기 위해 빨간색과 녹색으로 번갈아 표시되는 작은 원입니다.

문서 선택

조사자는 표시된 문서 선택자를 사용하여 결과 그리드에 표시될 문서 수를 선택할 수 있습니다. SELECT ALL을 사용하여 문서를 후속 기능으로 전송할 수 있고 처리 또는 시각화를 위해 많은 수의 문서를 전송할 수 있습니다. 표시된 문서 선택자를 사용하여 문서를 선택할 경우 그리드에 있는 문서가 아닌 전체 문서가 선택됩니다.

네트워크 및 문서 시각화

조사자는 시각화 도구를 사용하여 패턴을 발견하고, 지정된 기간 동안 네트워크 트래픽 및 문서 정체가 가장 많이 발생하는 위치를 파악하며, 의심스러운 컨텐츠를 확인할 수 있습니다. 예를 들어 조사자는 업무 시간 후에 액세스되는 서버와 같은 네트워크 트래픽 패턴을 시각화할 수 있습니다.

VGrid 도구는 시간 블록으로 구분됩니다. 네트워크 트래픽 또는 문서와 같이 의심스러운 컨텐츠는 그리드에서 빨간색 사각형으로 표시됩니다. 녹색 사각형은 정상적인 컨텐츠를 나타냅니다. 밝은 색상의 블록은 트래픽이 많음을 나타냅니다. 색상의 채도가 높을수록 트래픽 양이 많은 것입니다. 시간 블록의 밝기는 VGrid 도구에 표시되는 현재 데이터와 관련이 있습니다. 예를 들어 다른 시간 블록이 더 많은 데이터를 포함하여 로드될 경우 밝은 색상의 시간 블록이 어두워집니다.

조사자는 컨텐츠가 포함된 시간 블록별로 네트워크 트래픽의 유형과 문서 수를 확인할 수 있습니다.

시간 블록에서 네트워크 트래픽 및 문서 검사

조사자는 특정 시간 블록 내에서 개별 문서, 탐색한 웹 사이트 또는 전송된 이메일을 검사할 수 있습니다.

프로시저

1. **포렌식** 탭에서 **VGrid** 탭을 선택하십시오.
2. 다음 옵션 중 하나를 사용하여 시간 블록의 컨텐츠를 검사하십시오.
   - 네트워크 트래픽의 유형과 문서 수를 확인하려면 시간 블록 위로 마우스를 이동하십시오.
   - 시간 블록의 컨텐츠를 검색하려면 시간 블록을 하나 이상 선택하십시오. 마우스 오른쪽 단추를 클릭하고 **선택한 시간 블록 검색**을 선택하십시오.
   - 이벤트 시퀀스를 확인하려면 시간 블록을 선택한 다음 **설문조사자**를 선택하십시오.
   - 컨텐츠를 시각화하려면 시간 블록을 선택한 다음 **시각화**를 선택하십시오.

설문조사자 도구

설문조사자 도구를 사용하여 이벤트가 발생하는 경우 보안 인시던트에서 이벤트 시퀀스를 시각화할 수 있습니다.

조사자는 이 도구를 사용하여 의심스러운 공격자가 본 내용과 그들의 조치를 확인할 수 있습니다. 설문조사자 도구는 영화처럼 표시되는 Visualizer에서 보안 인시던트의 활동을 시간순으로 표시합니다. 설문조사자는 시간 지향적이므로 결과 화면에서 한 개의 문서를 선택할 경우 많은 내용이 표시되지 않습니다. 너무 적은 문서가 선택된 경우, **속성** 탭에서 선택된 문서의 시간 범위를 확장하십시오. **컨텍스트 표시** 링크를 클릭하여 시간을 확장하십시오.

속성 탭을 사용하여 인증서 정보 및 메타데이터를 표시하십시오. 이벤트, 플로우 및 자산별로 필터링하려면 IP 주소 또는 포트를 마우스 오른쪽 단추로 클릭하고, 이벤트 및 자산별로 필터링하려면 MAC 주소를 마우스 오른쪽 단추로 클릭하십시오.

케이스 시간, 프로토콜 및 IP 주소별로 해당 조회를 필터링할 수 있습니다.

목록 탭을 사용하여 시간순으로 표시되는 송수신된 문서 목록을 확인할 수 있습니다.

녹색 문서 ID 번호는 조사자가 문서를 검토했음을 나타내고, 빨간색 ID 번호의 문서는 검토하지 않았음을 나타냅니다.

재구성된 문서 보기

보기 탭에는 목록 보기에서 화면 왼쪽에 선택된 문서의 재구성된 보기가 표시됩니다.

왼쪽의 시퀀싱과 오른쪽의 재구성이라는 강력한 조합을 통해 의심스러운 공격자가 본 내용과 네트워크에서 수행한 조치를 확인할 수 있습니다. 설문조사자는 네트워크를 횡단한 표시되는 문서 이외에도 발생한 인증서 교환 및 은밀한 컴퓨터 간 핸드쉐이크도 표시합니다.

관련 태스크:

41 페이지의 제 5 장 『트래픽IP 주소에 대한 네트워크 트래픽 조사』
보안 인시던트 중 발생한 대화에서 관련 컨텐츠를 표시하려면 IP 주소와 연관된 네트워크 트래픽을 복구하고 재구성할 수 있습니다. 또한 IP 주소와 관련된 기존 케이스를 통해 검색할 수도 있습니다.

추출된 문서 컨텐츠

텍스트 탭에는 문서에서 추출된 컨텐츠가 표시됩니다. 문서 컨텐츠에는 서식이 지정되어 있지 않습니다.

이 텍스트는 검색 엔진 인덱서에서 추출됩니다.

QRadar Incident Forensics에서 문서 내보내기

IBM Security QRadar Incident Forensics에서 내보낸 모든 문서(내보낸 pcap 문서 제외)는 재구성된 문서, 문서의 원시 텍스트, 속성, 문서에 첨부된 참고를 포함합니다.

pcap 문서를 내보내는 경우 재구성은 수행하지 않습니다. 예를 들어, 웹 페이지를 내보내는 경우 기본 연결 중 다운로드된 브라우저가 다운로드됩니다. 일반적으로 대부분의 텍스트 컨텐츠는 기본 연결 중에 다운로드됩니다. 그러나 최신 브라우저는 내보내기에 포함되지 않은 추가 항목(예: 스타일시트 및 이미지)을 다운로드하기 위해 다중 연결을 사용합니다. 내보내는 경우 pcap 컨텐츠는 먼저 재구성되지 않습니다.

또 다른 예제로, 기본 명령 및 제어 연결과 별도의 데이터 연결이 존재하는 복잡한 프로토콜(예: FTP 및 VOIP)이 있습니다. VOIP 호출 또는 FTP 다운로드에 대한 pcap 파일을 내보내는 경우 데이터가 재구성되지 않으며, 예상치 못한 결과가 발생할 수 있습니다.

pcap 파일로 문서 내보내기

여러 IBM Security QRadar Incident Forensics 및 IBM Security QRadar Packet Capture 어플라이언스에서 pcap 파일로 문서를 내보낼 수 있습니다.

제한사항: pcap 형식으로 내보낸 컨텐츠는 재구성되지 않습니다.

프로시저

1. 선택한 문서에서 데이터를 내보내려면 **포린식** 탭의 복구 그리드에서 문서 옆에 있는 선택란을 선택한 후 **내보내기**를 클릭하십시오.

   최대 25개의 문서를 pcap 형식으로 내보내도록 선택할 수 있습니다.
2. **내보내기 유형 선택** 목록에서 **PCAP**를 클릭하십시오.
3. QRadar Incident Forensics 호스트에 대한 모든 문서를 내보낸 후 **다운로드**를 클릭할 수 있습니다.
4. 문서 내보내기에 실패한 경우 **실패** 메시지를 클릭하여 문서를 다시 내보내십시오.

결과

단일 pcap 파일을 내보내는 경우 pcap 파일이 다운로드됩니다. 둘 이상의 pcap 파일을 내보낸 경우 pcap 파일은 압축 파일(.zip)로 구성되고 압축 파일은 다운로드됩니다.

각 문서는 QRadar Incident Forensics 호스트의 IP 주소 및 원래 문서의 출처인 QRadar Packet Capture 디바이스의 IP 주소를 저장합니다. QRadar Incident Forensics 호스트를 제거하거나 QRadar Packet Capture를 이동하는 경우 내보낼 수 없습니다.

디지털 임프레션

디지털 임프레션이란 ID 트레일을 식별하는 컴파일된 연관 및 관계 세트입니다. 디지털 임프레션은 공격 엔티티의 ID, 통신 방식 및 통신 내용을 표시할 수 있도록 네트워크 관계를 재구성합니다.

디지털 임프레션 도구를 사용하여 다음과 같은 중요한 질문에 신속하게 답변할 수 있습니다.

- 의심스러운 공격자, 컴퓨터 또는 IP 주소에 대해 알려진 내용은 무엇입니까?

- 의심스러운 공격자가 말을 건 대상은 누구입니까?
- 연락 네트워크에 있는 사람은 누구입니까?
- 의심스러운 공격자가 자신의 ID를 위장하려고 시도합니까?

온라인 ID

이메일 주소, Skype 주소, MAC 주소, 채팅 ID, 소셜 미디어 ID, 트위터 ID 등의 온라인 ID는 엔티티 또는 사람을 식별하는 데 사용됩니다. 네트워크 트래픽과 문서에서 발견된 알려진 엔티티 또는 사람에는 자동으로 태그가 지정됩니다.

IBM Security QRadar Incident Forensics는 서로 상호작용하는 태그가 지정된 ID를 상호 연관지어 디지털 임프레션을 생성합니다.

디지털 임프레션 보고서의 콜렉션 관계는 연속적으로 수집된 전자적 존재를 나타내는데, 이는 공격자, 네트워크 관련 엔티티 또는 디지털 임프레션 메타데이터 용어와 연관됩니다. 조사자는 문서와 연관된 태그가 지정된 디지털 임프레션 ID를 클릭할 수 있습니다. 생성되는 디지털 임프레션 보고서는 표 형식으로 나열되며, ID 유형별로 구성됩니다.

관계 정보 가져오기

디지털 임프레션 보고서에는 중심 *ID*와 다른 모든 ID 간의 상호작용이 표시됩니다. 중심 *ID*는 보안 인시던트의 관심 출처인 온라인 ID입니다.

여러 카테고리에서 최고의 ID는 보통 해당 ID 유형 또는 카테고리에 있는 중심 ID의 ID입니다. 예를 들어 ID가 MAC 주소일 경우, 상호작용이 가장 많은 이메일 주소는 컴퓨터를 소유하고 있는 의심스러운 공격자에게 속할 수 있습니다. 그러나 IP 주소가 동적으로 지정될 경우 시간 범위 동안에 지정된 IP 주소도 조사해야 합니다.

다른 카테고리와 중심 ID 간의 상관 관계는 일반적으로 덜 강력합니다. 디지털 임프레션을 기반으로 작업 수행을 결정하기 전에 독립된 소스로 데이터의 유효성을 검증하십시오. 디지털 임프레션 도구를 사용하면 의심스러운 공격자와 엔티티로 조사 범위를 확장할 수 있습니다.

관계 조사를 통한 ID 트레일 추적

디지털 임프레션은 공격 엔티티 및 이와 통신하는 다른 엔티티를 식별할 수 있도록 네트워크 관계를 재구성합니다.

디지털 임프레션 도구는 상관 이벤트의 빈도 분포를 표시합니다. 이 도구는 엔티티 간의 관계를 표시하고 상관을 계수합니다. 개수가 높을수록 관계가 더 강력합니다. 예를 들어, 이메일 주소와 다른 엔티티 간의 관계를 조회할 경우 누가 누

구와 통신하는지 확인할 수 있습니다. 이메일 주소와 연관된 IP 주소, 의심 대상이 방문한 IP 주소 및 이메일 주소와 연관된 다른 이름을 확인할 수 있습니다.

분산 배치의 경우 조직 내의 한 노드에 대한 관계를 표시하도록 선택할 수 있습니다.

프로시저

1. 복구 그리드의 문서 목록에서 결과를 선택하고 **디지털 임프레션** 탭을 선택하십시오.
2. 목록에서 탐색할 항목을 선택하십시오.

   기본적으로 디지털 임프레션 보고서는 표 형식으로 나열되며, ID 유형별로 구성됩니다. 중심 ID와 상호작용하는 모든 ID가 표시됩니다. 상호작용하는 ID는 ID 유형별로 구성되며, 상호작용 빈도를 기준으로 정렬됩니다.
3. 원하는 ID가 표시되는 경우 선택하십시오.

   ID는 하이퍼링크이므로 다른 보고서의 중심 ID로 사용할 수 있습니다. 다른 탭이 작성되고 새 중심 ID가 표시됩니다. 의심스러운 공격자가 상호작용하는 사람과 이 공격자의 상호작용과 상호작용하는 사람을 확인할 수 있습니다. 의심스러운 공격자와 이 공격자와 상호작용하는 엔티티로 조사 범위를 확장할 수 있습니다.
4. 다른 호스트를 살펴보려면 **원격 호스트 선택** 목록에서 IP 주소를 선택하십시오.

   분산 설치의 경우 QRadar Incident Forensics 호스트를 선택한 다음 디지털 임프레션을 표시할 수 있습니다. 기본 보기는 기본 호스트지만, QRadar Incident Forensics 호스트와 연관된 보조 호스트를 선택할 수 있습니다.
5. 중심 ID와 다른 ID 간 상호작용의 연관과 관계에 대한 시각화를 표시하려면 **데이터 시각화** 탭을 클릭하십시오.

시각화 도구

여러 속성과 데이터 카테고리 간의 연관과 관계를 시각적으로 탐색할 수 있습니다.

시각화 창에서는 한 개, 두 개 또는 많은 수의 문서 선택에 대한 메타데이터 관계 맵을 검토할 수 있습니다. 많은 수의 문서 선택을 사용할 경우 조사자가 메타데이터 관계 및 상대적 빈도에 대한 종합 보기를 표시할 수 있습니다. 그런 다음 이러한 경로를 따라 보안 인시던트를 추가로 조사할 수 있습니다.

하나의 관계 또는 두 관계를 모두 변경하여 서로 다른 관계를 갖도록 선택한 문서의 시각화를 쉽게 재작성할 수 있습니다.

시각화는 선택한 문서 내에 포함된 모든 관계 및 관계 빈도를 표시합니다. 각 노드는 선택한 문서와 관련된 메타데이터의 개별 조각을 나타냅니다. 크기는 다른 노드와 비교한 상대적 빈도를 제공합니다. 링크는 메타데이터의 개별 조각 간에 발견된 연결을 표시하며, 크기를 통한 빈도를 제공합니다. 조사자는 노드를 사용하여 추가 탐색을 위한 가능한 경로를 식별할 수 있습니다.

관계 및 연관 시각화

시각화 창에서는 복구된 문서에서 속성 간 관계를 검토할 수 있습니다. 예를 들어 특정 이메일 주소와 통신하는 이메일 주소를 조사할 수 있습니다.

프로시저

1. 복구 그리드에서 조사하려는 문서에 해당하는 선택란을 클릭한 다음 **시각화**를 클릭하십시오.
2. 레이아웃, 표시할 문서 수 및 표시하려는 속성 간 관계를 선택한 다음 새로 고침을 클릭하십시오.
3. 확대/축소 컨트롤을 사용하여 이미지를 확대 또는 축소하십시오.
4. 새 검색을 수행하거나 활성 필터를 수정하려면 노드를 마우스 오른쪽 단추로 클릭하십시오.

   컨텍스트 메뉴에서 해당 메타데이터를 다시 가져와서 검색을 새로 수행할 수 있습니다. 메타데이터를 포함하거나 제외하도록 활성 필터를 수정할 수도 있습니다.

   제한사항: 시각화 창에서 최대 9999개의 문서를 한 번에 볼 수 있습니다.

의심스러운 컨텐츠 또는 악성 컨텐츠에 대한 아티팩트 분석

보안 분석가는 재구성된 아티팩트(예: 파일 및 이미지)를 분석하여 발견을 회피하는 위협을 검색할 수 있습니다. 또한 협업자와 아티팩트 간의 연결에 대해 파악하기 위해 해당 파일 및 이미지에 대한 링크를 조사할 수 있습니다.

예제 - 아티팩트 분석을 사용하여 공격의 소스(최초 감염자) 찾기

John은 Replay Industries의 보안 분석가입니다. 정상적으로 수행되는 모든 보안 조치에도 불구하고 일부 시스템이 감염되었습니다. 해당 시스템을 식별하고 격리한 후 John은 해당 시스템을 감염시킨 방법과 다른 자산이 유사한 방식으로 위험에 노출되어 있는지 여부를 파악해야 합니다.

특정 IP 주소에서 패킷 복구

John은 연관된 IP 주소 및 대략의 시간 프레임으로부터 QRadar Incident Forensics를 사용하여 관련 패킷 데이터를 복구할 수 있습니다.

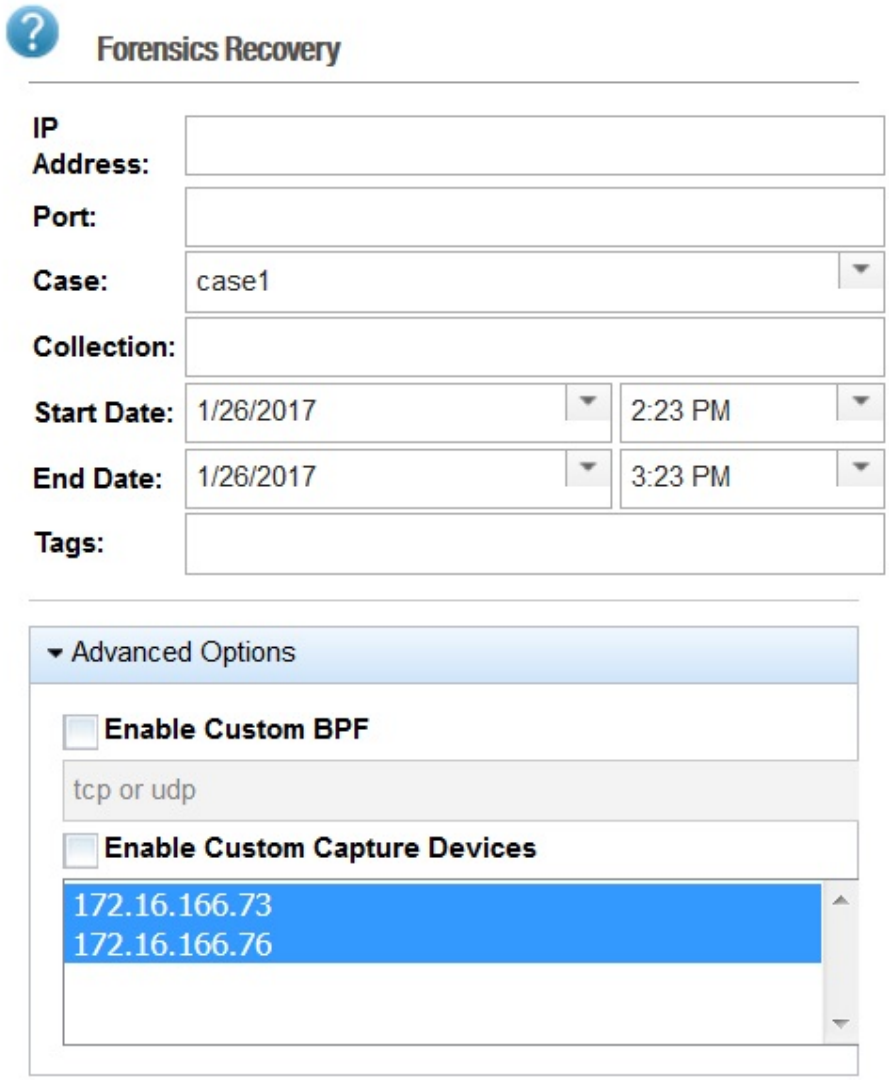


그림 *1.* 특정 *IP* 주소에서 복구

파일 분석

John은 QRadar Incident Forensics 내에 포함된 파일 분석 기능을 사용하여 실행 가능한 컨텐츠 검색을 시작합니다. 이제 모든 파일의 목록, 해당 파일이 전송된 빈도, 임베드된 파일 또는 스크립트가 포함되어 있는지 여부 및 엔트로피 점수를 확인할 수 있습니다. John은 신속하게 QRadar Incident Forensics에서 의심스러운 컨텐츠 및 임베드된 스크립트가 포함된 것으로 플래그 지정한 이미지

파일을 확인합니다.

Doc #	File Name	Extension	Description	Protocol	Frequency	Suspect Content	Embedded Script	Embedded Files	File Size (Bytes)	File Hash (SHA-256)	Entropy
1	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	1916	70c6e673cd0150b1ffa89e	4.93731
2	index.php	php	CSS File	http	1	No Suspect Content	No Embedded Script	0	163060	dbbb35dcf2e494f068b9d1	5.74523
3	index.php	php	JavaScript	http	1	No Suspect Content	No Embedded Script	0	164112	909a0b9fa48182b58dd85	5.38451

그림 2. 파일 분석 속성

데이터의 무작위도를 측정하고 암호화된 악성 프로그램을 찾기 위해 사용되는 파일 엔트로피 점수와 엔트로피 분포는 파일이 정상에서 벗어난 정도를 명확하게 보여줍니다. 추가적인 분석을 통해 이 파일에 기존 보안 조치에서 발견되지 않고 빠져나갔으며 감염된 시스템에 대한 책임이 있는 새로운 유형의 악성 프로그램이 포함되어 있음이 확인되었습니다.

다음 다이어그램에서 엔트로피는 바이트당 비트의 가변성에 대한 지표로 사용됩니다. 데이터 단위의 각 문자는 1바이트로 구성되어 있기 때문에 엔트로피 값은 문자의 가변성 및 데이터 단위의 압축성을 나타냅니다. 파일에서 엔트로피 값의 가변성은 파일에 의심스러운 컨텐츠가 숨겨져 있음을 나타낼 수 있습니다. 예를 들어 높은 엔트로피 값은 데이터가 암호화 및 압축되어 저장됨을 나타낼 수 있으며, 낮은 값은 런타임 시 페이로드가 복호화되어 다른 섹션에 저장됨을 나타낼 수 있습니다.

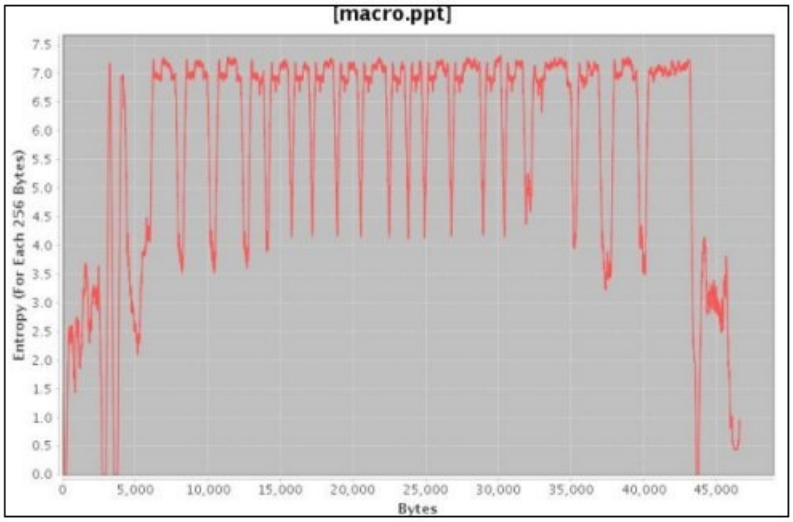


그림 3. 임베드된 스크립트를 표시하는 파일 엔트로피 그래프 예제

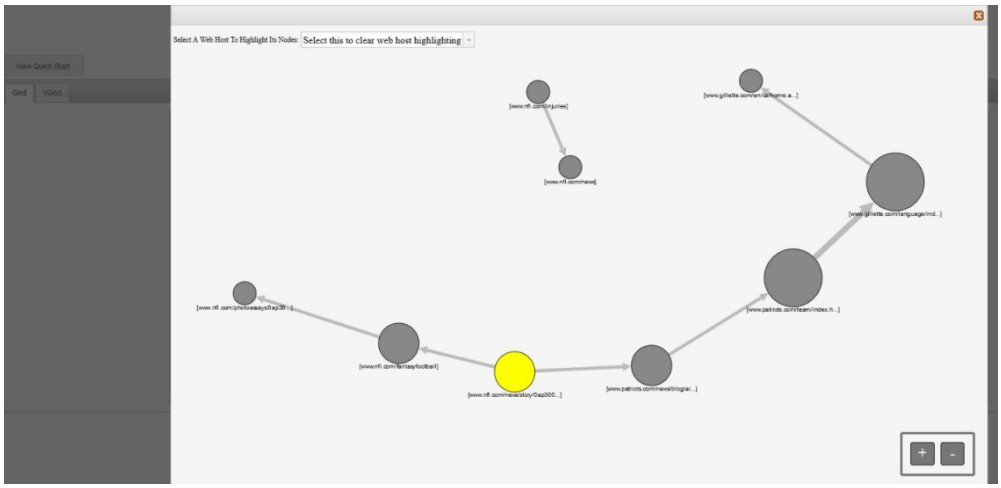
이제 John은 이 파일의 출처 및 이 파일을 보유하고 있을 가능성이 있는 다른 잠재적 사용자를 파악해야 합니다. John은 QRadar Incident Forensics를 사용하여 신속하게 감염된 이미지 파일을 제공한 웹 서버를 찾습니다. 문제의 웹 페이지는 모든 사용자가 좋아하는 NFL 팀의 최신 뉴스를 방송하는 것으로 유명하며 위험에 노출되어 있습니다. 해당 웹 사이트에 많은 이미지가 포함되어 있음에

도 불구하고 이전에 John이 파일 분석을 통해 찾은 임베드된 악성 프로그램이 포함된 이미지는 한 장 뿐입니다.

웹 사이트 통신을 시각화하는 링크 분석

다른 시스템이 감염되었는지 여부를 판별하기 위해 John은 링크 분석을 사용하여 신속하게 사용자가 본 모든 웹 사이트를 시각화하며, Replay와 거래하는 회사의 웹 사이트 간에 대량의 트래픽이 존재함에도 불구하고 소량의 액세스 서브세트만 명확하게 감염된 웹 호스트인 것으로 판명되었습니다. John은 해당 링크를 분석하여 이 웹 호스트에 액세스하기 위해 네트워크에서 사용된 다른 서버를 확인합니다.

이 조사에서 John은 웹 페이지 간의 관계 또는 트랜잭션을 나타내는 노드 간 화살표 및 웹 페이지를 표시하는 그래프의 노드를 사용하여 신속하게 트래픽 패턴을 평가하고 문서를 방문한 방법을 확인합니다. 노드가 클수록 문서의 해당 경로에 더 많은 링크가 포함된 것이며, 링크 화살표가 클수록 해당 링크가 더 자주 사용된 것입니다.



유명한 NFL 뉴스 사이트라는 점을 감안할 때 수많은 다른 서버가 해당 웹 호스트에 접속하여 잠재적으로 감염된 것으로 확인된 것이 그리 놀라운 일은 아닙니다.

이미지 분석

John은 악성 이미지 파일을 다운로드한 서버의 범위를 좁히기 위해 이미지 분석으로 전환하여 신속하게 송수신된 모든 이미지 파일을 확인합니다.

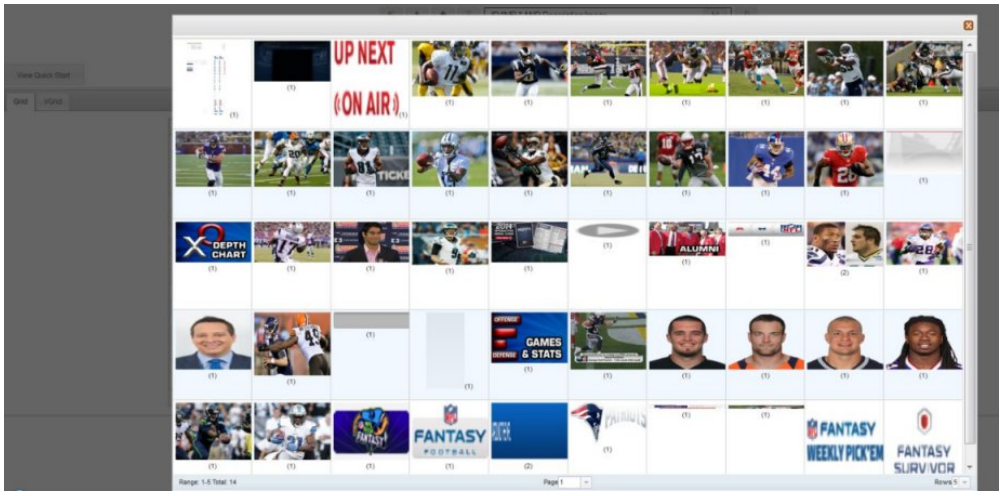


그림 *4.* 이미지 분석 및 이미지 배포 예제

John은 신속하게 감염된 서버 및 확신할 수 없는 2대의 서버가 모두 위험에 노출된 이미지 파일에 액세스했음을 확인합니다.

또한 John은 동일한 웹 사이트에 액세스한 다른 서버 중 일부는 감염된 파일을 다운로드하지 않았음을 확인합니다. 이제 John은 2대의 서버를 추가로 격리하고 Replay Industries가 IBM X-Force® Exchange에 업로드하여 다른 사용자와 공유할 수 있는 감염된 파일에 대한 새 파일 해시를 작성해야 한다는 정보를 파악했습니다.

임베드된 컨텐츠 및 악성 활동에 대한 파일 분석

파일에서 숨겨진 위협을 조사하기 위해 파일 엔트로피 값을 보고, 추가 분석을 위해 임베드된 파일 및 스크립트를 다운로드하고, 문서 및 해당 속성을 확인할 수 있습니다.

불법 침입자가 컨테이너 파일 내의 2진 파일 컨텐츠를 난독 처리할 수 있기 때문에 IBM Security QRadar Incident Forensics의 파일 분석을 사용하여 파일에 임베드된 스크립트 또는 기타 2진 컨텐츠가 포함되어 있는지 여부를 조사할 수 있습니다.

파일 엔트로피는 파일에서 데이터의 무작위도를 측정하며, 파일에 숨겨진 데이터 또는 의심스러운 스크립트가 포함되어 있는지 여부를 판별하기 위해 사용됩니다. 무작위도의 범위는 무작위가 아님을 나타내는 0부터 완전히 무작위임을 나타내는 8(예: 암호화된 파일)까지입니다. 단위를 더 많이 압축할 수 있는 경우 엔트로피 값이 낮아지고, 단위를 더 적게 압축할 수 있는 경우 엔트로피 값이 높아집니다.

다음 다이어그램에서 엔트로피는 바이트당 비트의 가변성에 대한 지표로 사용됩니다. 데이터 단위의 각 문자는 1바이트로 구성되어 있기 때문에 엔트로피 값은 문자의 가변성 및 데이터 단위의 압축성을 나타냅니다. 파일에서 엔트로피 값의

가변성은 파일에 의심스러운 컨텐츠가 숨겨져 있음을 나타낼 수 있습니다. 예를 들어 높은 엔트로피 값은 데이터가 암호화 및 압축되어 저장됨을 나타낼 수 있으며, 낮은 값은 런타임 시 페이로드가 복호화되어 다른 섹션에 저장됨을 나타낼 수 있습니다.

프로시저

1. **포렌식** 탭의 **그리드** 보기에서 하나 이상의 복구된 파일을 선택하십시오.
2. 그리드의 맨 위에 있는 조사 도구 메뉴에서 **파일 분석**을 클릭하십시오.

   결과적으로 각 그리드 행에는 문서에 대한 분석 데이터가 포함됩니다(예: 파일 이름, 설명, 의심스러운 컨텐츠 발견 여부 및 엔트로피 값).
3. 특정 속성(예: 엔트로피)별로 파일을 정렬하려면 연관된 컬럼 표제를 클릭하십시오.
4. 추가 조사가 필요한 경우 파일 목록에서 파일을 마우스 오른쪽 단추로 클릭하십시오.
   - 문서 및 해당 속성을 검토하려면 **문서 표시**를 클릭하십시오.
   - 엔트로피 그래프를 검토하고 임베드된 파일 또는 스크립트에 악성 프로그램이 포함되어 있는지 확인하려면 **엔트로피 표시**를 클릭하십시오.

     엔트로피 값은 파일에 악성 컨텐츠가 포함되어 있는지 여부를 나타내는 지표로 사용할 수 있습니다. 예를 들어 ASCII 텍스트 파일은 일반적으로 높은 수준의 압축이 가능하며 엔트로피 값이 낮습니다. 암호화된 데이터는 일반적으로 압축이 불가능하며 엔트로피 값이 높습니다. 악성 프로그램은 파일 및 이미지 모두에 압축되어 숨겨져 있는 경우도 있습니다.
   - 임베드된 파일을 다운로드하려면 **임베드된 파일 추출**을 클릭한 후 다운로드할 파일을 선택하십시오.

     이 옵션은 임베드된 파일 또는 스크립트가 포함된 문서에서만 사용 가능합니다. 파일은 웹 브라우저의 다운로드 위치에 다운로드됩니다. 보호되지 않은 환경에서 잠재적으로 손상을 입힐 수 있는 스크립트를 열지 않도록 주의하십시오.

숨겨진 위협 또는 의심스러운 활동에 대한 이미지 분석

사용자가 본 이미지는 크기 및 관련성별로 정렬되며 소괄호 안에 빈도 수가 표시됩니다. 이 분석은 직원이 회사 자원을 사용하여 부적절하거나 제한 또는 금지된 이미지를 보는 경우에 유용할 수 있습니다. 예를 들면 보안 위반 대상인 항공기, 특정 빌딩 또는 위치와 관련된 이미지입니다.

이미지 분석을 사용하면 각 문서를 열어 이미지를 보지 않고, 하나 이상의 패킷 캡처 파일에 있는 하나 이상의 문서에서 가장 관련성이 높은 이미지를 하나의 디스플레이에 표시할 수 있습니다.

프로시저

1. **포렌식** 탭의 **그리드** 보기에서 설명에 이미지가 포함된 문서를 하나 이상 선택하십시오.
2. 그리드의 맨 위에 있는 조사 도구 메뉴에서 **이미지 분석**을 클릭하십시오.

   결과로 문서 내에 포함되어 있는 모든 이미지의 축소판 버전이 관련성 순서에 따라 표시됩니다. 이미지 옆에 있는 소괄호 내의 숫자는 문서에 있는 이미지의 인스턴스 수를 나타냅니다. 축소판 이미지 위로 커서를 움직이면 이미지가 커집니다.
3. 추가 조사가 필요한 경우 이미지를 마우스 오른쪽 단추로 클릭하십시오.
   - 이미지 및 해당 속성을 검토하려면 **문서 표시**를 클릭하십시오.
   - 엔트로피 그래프를 검토하고 이미지에 악성 프로그램이 포함되어 있는지 확인하려면 **엔트로피 표시**를 클릭하십시오.

     엔트로피 값은 파일에 악성 컨텐츠가 포함되어 있는지 여부를 나타내는 지표로 사용할 수 있습니다. 예를 들어 비트맵 이미지 파일 및 ASCII 텍스트 파일은 일반적으로 높은 수준의 압축이 가능하며 엔트로피 값이 낮습니다. 암호화된 데이터는 일반적으로 압축이 불가능하며 엔트로피 값이 높습니다. 악성 프로그램은 파일 및 이미지 모두에 압축되어 숨겨져 있는 경우도 있습니다.

연결 및 관계에 대한 링크 분석

링크 분석에서 링크는 사용자가 본 웹 사이트 간의 공통성을 보여줍니다. 보안 인시던트 조사 중에 신속하게 겹침이 있는 위치 및 사용자가 통신하는 방법을 확인할 수 있습니다.

예를 들어 가해자 그룹이 협력하고 있는 것으로 판단되지만 그 방법이 확실치 않은 경우 여러 사용자의 문서 세트를 보고 링크 분석을 사용하여 공통 웹 페이지를 표시할 수 있습니다. 그런 다음 특정 웹 사이트를 조사할 수 있습니다.

프로시저

1. **포렌식** 탭의 **그리드** 보기에서 하나 이상의 웹 페이지를 선택하십시오.
2. 그리드의 맨 위에 있는 조사 도구 메뉴에서 **링크 분석**을 클릭하십시오.

   웹 사이트 간에 관계가 있는 경우 Cytoscape 차트에 웹 페이지가 원형(노드)으로 표시되고 웹 페이지에 대한 링크가 화살표로 표시됩니다. 노드가 클수

록 문서의 해당 경로에 더 많은 링크가 포함된 것이며, 링크 화살표가 클수록 해당 링크가 더 자주 사용된 것입니다. 선택한 노드는 노란색으로 표시됩니다.

3. 특정 웹 호스트로부터의 통신을 조사하려면 **웹 호스트 선택** 목록에서 웹 호스트를 선택하십시오.

   선택한 웹 호스트의 웹 페이지를 표시하는 노드는 진한 회색 원형으로 강조표시됩니다.

4. 원형(노드) 및 화살표의 크기를 늘리거나 줄이려면 확대(+) 또는 축소(-) 제어를 사용하십시오.

   마우스 휠을 스크롤하여 노드 및 화살표의 크기를 늘리거나 줄일 수도 있습니다.

5. 하나 이상의 노드를 이동하려면 노드를 클릭한 후 끌어서 놓으십시오.

   백그라운드의 임의 위치를 클릭한 다음 누른 상태로 끌어서 전체 그래프를 이동할 수 있습니다.

문서의 속성 페이지에서 복구 실행

문서의 **속성** 탭을 볼 때 IP 주소 또는 포트에 대한 복구를 실행할 수 있습니다.

프로시저

1. **포렌식** 탭의 검색 페이지에서 검색을 수행하십시오.
2. 리턴한 문서의 목록에서 문서를 열려면 하나를 클릭하십시오.
3. **속성** 탭을 클릭하십시오.
4. IP 주소 또는 포트를 클릭하십시오.
5. 메뉴에서 **다음의 복구 실행**을 클릭하십시오.

제 5 장 트래픽IP 주소에 대한 네트워크 트래픽 조사

보안 인시던트 중 발생한 대화에서 관련 컨텐츠를 표시하려면 IP 주소와 연관된 네트워크 트래픽을 복구하고 재구성할 수 있습니다. 또한 IP 주소와 관련된 기존 케이스를 통해 검색할 수도 있습니다.

네트워크 트래픽이 IP 주소에서 재구성된 경우 인시던트가 작성됩니다. 조사자는 보안 인시던트의 이벤트 시퀀스를 시각화하거나 인시던트의 문서를 볼 수 있습니다.

IBM Security QRadar Incident Forensics에서는 복구된 각 파일에 있는 사용 가능한 네트워크 데이터, 파일 데이터, 메타데이터 및 텍스트 문자를 모두 인덱싱합니다.

분산 배치의 경우, 여러 개의 캡처 디바이스와 QRadar Incident Forensics 호스트가 데이터를 캡처하고 처리합니다. 집계된 인시던트 복구 결과를 보거나 호스트 및 캡처 디바이스별 결과를 볼 수 있습니다.

프로시저

1. 케이스를 작성하고 패킷 캡처 디바이스의 데이터를 가져오려면 QRadar에서 IP 주소를 마우스 오른쪽 단추로 클릭한 후 **포렌식 복구 실행**을 선택하거나

   포렌식 복구 아이콘  을 클릭하십시오.

   a. 다음 정보를 사용하여 포렌식 복구 매개변수를 설정하십시오.

표 *5.* 포렌식 복구 매개변수

매개변수	설명
IP 주소	복수의 IP 주소를 구분하려면 쉼표를 사용하십시오. IP 주소 또는 포트가 입력되지 않을 경우 기본 TCP 또는 UDP가 사용됩니다.
포트	복수의 포트를 구분하려면 쉼표를 사용하십시오.
케이스	케이스 이름은 고유해야 합니다.
콜렉션	복구된 데이터는 콜렉션으로 그룹화되고 케이스와 연관됩니다. 콜렉션 이름은 고유해야 합니다. 케이스에 해당 콜렉션 이름이 존재하는 경우 원래 콜렉션이 삭제됩니다.
태그	선택사항입니다. 관련 문서에서 신속하게 정확한 결과 세트를 검색하기 위해 사용됩니다. 복수의 태그를 구분하려면 쉼표를 사용하십시오. 영숫자 문자만 사용하십시오. 특수 문자는 허용되지 않습니다.
사용자 정의 BPF(Berkeley Packet Filter) 사용	관리자가 사용할 수 있습니다. 이 선택란을 선택하면 IP 주소와 포트를 지정하는 BPF 입력 필드가 활성화됩니다.

표 5. 포렌식 복구 매개변수 (계속)

매개변수	설명
사용자 정의 캡처 디바이스 사용	관리자가 사용할 수 있습니다. 이 선택란을 선택하면 사용자 배치에 PCAP 디바이스 목록을 생성합니다. 디바이스를 하나 이상 선택하여 해당 디바이스로부터의 트래픽만 볼 수 있습니다.

b. **확인**을 클릭한 다음 포렌식 탭을 클릭하십시오.

문제점 해결: 데이터를 복구할 수 있는 권한이 없다는 메시지가 표시되면 보안 프로파일에 IP 주소에 액세스할 수 있는 권한이 있는지 확인하십시오. **태그** 필드에서 # 문자를 사용한 경우에도 해당 메시지가 표시될 수 있습니다.

c. 인시던트를 확인하려면 인시던트 아이콘  을 클릭하십시오. 계층 구조를 통해 탐색하는 경우 컨텐츠를 펼치거나 접으십시오.

d. 인시던트의 문서를 보려면 **검색 페이지 결과로 이동**을 클릭하십시오.

e. 인시던트에 대한 이벤트 시퀀스를 시각화하려면 **설문조사자 페이지 결과로 이동**을 클릭하십시오.

f. 특정 인시던트를 제거 또는 취소하려면 **이 인시던트 삭제 또는 취소**를 클릭하십시오.

g. 이전 포렌식 복구 작업을 재실행하려면 **이 포렌식 복구 재실행**을 클릭하십시오. 예를 들어 해당 결과에서 불완전한 데이터가 리턴되는 경우 포렌식 복구를 재실행하여 다른 IP 주소를 포함시키거나 이전에 실행된 복구 작업에 지정되어 있는 시간 프레임을 변경할 수 있습니다.

2. QRadar에서 기존 케이스를 검색하려면 IP 주소를 마우스 오른쪽 단추로 클릭한 후 **포렌식 검색 실행**을 클릭하십시오.

a. **포렌식** 탭에서 인시던트 아이콘을 클릭하십시오.

b. 인시던트와 연관된 활동 집합을 조사하려면 케이스 위로 마우스를 이동하여 케이스를 강조표시한 후 검색 아이콘을 클릭하십시오.

c. 분산 배치의 QRadar Incident Forensics 호스트 및 캡처 디바이스별로 활동을 조사하려면 **케이스** 항목을 펼친 다음 **콜렉션** 항목을 펼치십시오.

d. 인시던트의 상호작용에 대해 시간순으로 표시된 목록을 보려면 콜렉션 위로 마우스를 이동하여 콜렉션을 강조표시한 후 설문조사자 아이콘을 클릭하십시오.

관련 개념:

29 페이지의 『재구성된 문서 보기』

보기 탭에는 목록 보기에서 화면 왼쪽에 선택된 문서의 재구성된 보기가 표시됩니다.

사용자 정의 BPF

포렌식 복구를 실행할 때 특정 유형의 트래픽만 표시하기 위해 사용자 정의 BPF(Berkeley Packet Filter)를 작성하도록 선택할 수 있습니다.

포렌식 복구에서 선택란을 선택하면 네트워크 트래픽을 필터링할 BPF 필터를 지정하는 BPF 입력 필드가 활성화됩니다.

BPF 구문을 사용하여 BPF 필터를 지정할 수 있습니다. 표현식은 하나 이상의 기초로 구성됩니다. 기초는 네트워크 프로토콜 헤더에 있는 하나 이상의 필드에 대한 참조입니다. 예를 들어 호스트, 포트, TCP 포트는 모두 기초입니다. AND, OR 및 NOT 연산자를 사용하여 복잡한 필터 표현식을 빌드할 수 있습니다.

다음은 필터 예제입니다.

```
host 10.0.0.1
port 80
tcp port 80 and host 10.0.0.1
host 10.0.0.1 or host 10.0.0.2 or port 80 or port 443
```

사용자 정의 BPF를 작성하려면 Admin 사용자 역할에 대한 액세스 권한이 있어야 합니다. Admin이 아닌 사용자에게는 BPF 텍스트 필드에 대한 읽기 전용 액세스 권한이 있습니다. Admin 사용자는 임의의 BPF 표현식을 입력할 수 있습니다.

제한사항: 포렌식 복구는 제공된 BPF 입력을 적용합니다. 복구의 결과가 예상치 못한 결과인 경우 복구 입력 및 BPF를 검사하여 기준이 올바른지 확인하십시오.

사용자 정의 BPF에서 사용하지 않더라도 BPF 필드에는 항상 **IP 주소** 또는 **포트** 필드의 컨텐츠가 포함되어 있습니다. IP 주소 또는 포트가 입력되지 않은 경우 사용자 정의 BPF는 기본 TCP 또는 UDP를 사용합니다.

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.

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.

용어집

이 용어집은 IBM Security QRadar Incident Forensics 소프트웨어 및 제품에 대한 용어와 정의를 제공합니다.

이 용어집에 사용되는 상호 참조는 다음과 같습니다.

- 참조하십시오*(See)*는 비선호 용어에서부터 선호 용어까지 또는 약어에서 완전한 형태까지를 참조하도록 합니다.
- 도 참조하십시오*(See also)*는 관련 용어 또는 대조되는 용어를 참조하도록 합니다.

기타 용어 및 정의는 IBM Terminology 웹 사이트(새 창에서 열림)를 참조하십시오.

『가』 『다』 『마』 50 페이지의 『바』 50 페이지의 『사』 50 페이지의 『아』 50 페이지의 『자』 50 페이지의 『차』 51 페이지의 『카』 51 페이지의 『타』 51 페이지의 『파』 51 페이지의 『I』

가

가설(hypothesis)

케이스에서 수집된 사용 가능한 증거를 기준으로 한 인시던트에 대한 제안된 설명입니다. 가설은 테스트 및 반증이 가능해야 합니다.

공격자(attacker)

정보 시스템에 피해를 주거나 일반 액세스용이 아닌 정보를 액세스하려는 사용자(사람 또는 컴퓨터 프로그램)입니다. 공격(attack)도 참조하십시오.

공격(attack)

권한이 없는 사용자가 소프트웨어 프로그램이나 네트워크 시스템의 조작을 방해하려고 시도하는 행위입니다. 공격자(attacker)도 참조하십시오.

다

도메인 인스펙터(domain inspector)

Facebook 또는 Gmail 같은 특정한 도메인 웹 사이트에서 포렌식 데이터를 해체 및 추출하도록 설계된 특별한 인스펙터입니다.

디지털 임프레션 관계(digital impression relationship)

케이스와 관련된 태그 지정된 ID 간의 관계입니다.

디지털 임프레션(digital impression)

개별 케이스내에서 서로 간에 연결된 태그 지정된 ID로 구성된 보고서입니다.

디캡핑(decapping)

패킷 캡처 데이터가 디컴파일되어 모든 수집된 데이터가 결과 보고서로 생성되는 프로세스입니다.

마

메타 데이터(metadata)

데이터의 특성에 대해 설명하는 데이터 즉, 설명적 데이터입니다.

메타데이터 관계 맵(metadata relational map)

케이스 문서에서 관련된 메타데이터를 표시하는 맵입니다.

바

보안 인시던트(security incident)

정상적인 네트워크 작업에 위반, 위해 또는 공격이 발생하는 이벤트입니다.

복구 작업(recovery job)

검색한 캡처 데이터를 복구하고 이를 decapper 디바이스로 전달하여 수집하는 프로세스입니다.

부울 연산자(Boolean operator)

작업 세트를 평가할 때 AND, OR 또는 NOT의 논리 연산을 지정하는 기본 제공되는 기능입니다. 부울 연산자는 &&, || 및 !입니다.

비정상(anomaly)

예상되는 네트워크 작동과 다른 이상 작동입니다.

사

설문조사자 도구(surveyor tool)

Visualizer에서 보안 인시던트의 활동을 시간순으로 표시하는 도구입니다.

수집된 네트워크 트래픽(ingested network traffic)

포렌식 디캡핑 프로세스에서 처리한 캡처된 네트워크 트래픽입니다.

수퍼플로우(superflow)

스토리지 제한조건을 줄여 처리 용량을 늘리기 위해 유사한 특성을 가진 여러 플로우로 구성된 단일 플로우입니다.

아

암호화(encryption)

컴퓨터 보안에서, 원본 데이터를 획득하지 못하도록 하거나 복호화 프로세스를 사용해서만 획득할 수 있도록 데이터를 난해한 양식으로 변환하는 프로세스입니다.

연속적으로 수집된 전자적 존재(continuously collected electronic presence)

링크된 디지털 임프레션 콜렉션인 공격자의 온라인 ID입니다.

오펜스(offense)

모니터되는 조건에 대한 응답으로 전송된 메시지 또는 생성된 이벤트입니다. 예를 들어, 오펜스는 정책이 위반되었는지 또는 네트워크가 공격받고 있는지에 대한 정보를 제공합니다.

이동 경로(breadcrumb)

사이트 내에서 사용자 위치를 표시하는 웹 인터페이스 요소입니다. 대개 페이지 맨 위 또는 맨 아래에 표시되는 일련의 하이퍼링크입니다. 이 링크는 조회한 페이지를 표시하므로 사용자가 시작 위치로 다시 이동할 수 있게 해줍니다.

인시던트(Incident)

보안 인시던트(security incident)를 참조하십시오.

자

중심 ID(centering identifier)

다른 모든 ID가 상호 작용하는 카테고리 항목입니다. 중심 ID는 조사의 중심 항목입니다.

차

추적(trail)

케이스에 포함된 개인을 케이스 외부의 개인에게 연결하는 디지털 임프레션입니다.

취약성(Vulnerability)

운영 체제, 시스템 소프트웨어 또는 애플리케이션 소프트웨어 구성요소에서 보안 위험이 노출된 부분입니다.

카

카테고리(category)

특정 설명 또는 분류에 따라 그룹화된 항목 세트입니다. 카테고리는 차원내 다른 레벨의 정보일 수 있습니다.

캡처 디바이스(capture device)

패킷 캡처 어플라이언스(packet capture appliance)를 참조하십시오.

케이스(case)

특정 조사와 관련된 데이터베이스 내에 포함된 정보입니다.

콜렉션(collection)

케이스와 연관되고 명확하게 이름 지정된 데이터 세트입니다. 예를 들어, 캡처된 네트워크 패킷의 정렬된 세트입니다.

타

통신(conversation)

둘 이상의 네트워크 엔드포인트 간에 포렌식하게 재구성된 데이터 플로우입니다. 예를 들어, 소셜 네트워크 통신입니다.

트래픽(traffic)

데이터 통신에서 경로의 특정 지점을 통과하여 전송된 데이터 수량입니다.

파

패킷 캡처 어플라이언스(packet capture appliance)

트래픽 데이터를 인터셉트 및 로그하는 독립형 어플라이언스입니다.

패킷 캡처 정보(packet capture information)

캡처 디바이스가 수집하는 트래픽 데이터 정보입니다.

포렌식 조사자(forensic investigator)

포렌식 저장소의 네트워크 트래픽 및 문서에서 관련 데이터를 추출하는 사용자입니다.

프로토콜 인스펙터(protocol inspector)

HTTP 또는 FTP 같은 네트워크 프로토콜에서 포렌식 데이터를 추출하도록 설계된 특별한 인스펙터입니다.

플로우 레코드(flow record)

두 개의 호스트 간의 통신 레코드입니다.

I

ID(identity)

사용자, 조직, 위치 또는 항목을 나타내는 데이터 소스의 속성 콜렉션입니다.

색인

[가]

[다]

[마]

[사]

[아]

[자]

[파]

I