Context Explorer 사용

다음 주제에서는 Firepower System에서 Context Explorer(상황 탐색기)를 사용하는 방법을 설명합니다.

Context Explorer(상황 탐색기) 정보

Firepower System Context Explorer(상황 탐색기)는 애플리케이션에 대한 데이터, 애플리케이션 통계, 연결, 지리위치, IOC, 침입 이벤트, 호스트, 서버, 보안 인텔리전스, 사용자, 파일(악성코드 파일 포함), 관련 URL 등 모니터링 중인 네트워크의 상태에 대한 자세한 인터랙티브 그래픽 정보를 콘텍스트에 맞게 표시합니다. 개별 섹션은 이 데이터를 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 표시합니다. 첫 번째 섹션인 시간 경과에 따른 트래픽 및 이벤트 카운트의 선 그래프는 네트워크 활동의 최신 추세를 한눈에 볼 수 있는 그림을 제공합니다.

간편하게 맞춤형 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며, 그래프 영역을 클릭하거나 커서를 올려놓기만 하면 데이터 섹션을 자세히 확인할 수 있습니다. 또한 탐색기의 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수도 있습니다. Administrator(관리자), Security Analyst(보안 분석가) 또는 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 사용자 역할이 있는 사용자만 Context Explorer(상황 탐색기)에 액세스할 수 있습니다.

Firepower System 대시보드는 세부적으로 맞춤화 및 구획화할 수 있으며 실시간으로 업데이트됩니다. 반면 Context Explorer(상황 탐색기)는 수동으로 업데이트되고, 데이터에 대한 더 넓은 범위의 콘텍스트를 제공하도록 설계되었으며, 활성 사용자 탐색에 편리하도록 일관된 단일 레이아웃을 제공합니다.

특정 요구에 맞게 네트워크 및 어플라이언스에서 실시간 활동을 모니터링하려면 대시보드를 사용합니다. 반대로, 매우 세분화되고 분명한 상황에서 사전 정의된 최신 데이터 세트를 조사하려면 Context

Explorer(상황 탐색기)를 사용합니다. 예를 들어 네트워크의 호스트 중 15%만 Linux를 사용하지만 여기에서 거의 모든 YouTube 트래픽이 생성되는 경우 필터를 신속하게 적용하여 Linux 호스트 또는 YouTube 관련 애플리케이션 데이터만 보거나 두 가지 데이터를 모두 볼 수 있습니다. 간결하고 매우 집중적인 대시보드 위젯과는 달리 Context Explorer(상황 탐색기) 섹션은 시스템 활동을 Firepower System의 전문가는 물론 일반 사용자도 알기 쉬운 유용한 형식으로 시각적으로 표시하도록 설계되었습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다. 필터를 적용해 모든 Context Explorer(상황 탐색기) 섹션에 표시되는 데이터를 제한할 수도 있습니다.

다중 도메인 구축의 경우, Context Explorer(상황 탐색기)는 사용자가 상위 도메인에서 데이터를 확인할 때 모든 하위 도메인에서 집계된 데이터를 표시합니다. 리프 도메인의 경우에는 해당 도메인과 관련된 데이터만 확인할 수 있습니다.

대시보드 및 **Context Explorer** 간 차이

다음 표에는 대시보드와 Context Explorer(상황 탐색기)의 주요 차이점이 요약되어 있습니다.

표 ***1:*** 비교*:* 대시보드 및 ***Context Explorer(***상황 탐색기***)***

기능	대시보드	**Context Explorer(**상황 탐색기**)**
표시 가능한 데이터	Firepower System이 모니터링하는 모든 데이터	애플리케이션, 애플리케이션 통계, 지리 위치, 침해 지표, 침입 이벤트, 파일(악성 코드 파일 포함), 호스트, Security Intelligence(보안 인텔리전스) 이벤트, 서버, 사용자, URL
맞춤형 가능	• 대시보드를 맞춤형할 수 있는 위젯 선택 • 개별 위젯은 다양한 수준으로 맞춤형할 수 있음	• 기본 레이아웃은 변경 불가 • 적용된 필터는 탐색기 URL에 나타나며 나중에 사용하도록 북마크 처리 가능
데이터 업데이트 빈도	자동(기본값): 사용자가 구성함	수동
데이터 필터링	일부 위젯에 대해 가능(위젯 환경설정을 수정해야 함)	(탐색기의 모든 부분에 대해 가능하며 다중 필터 지원
그래픽 콘텍스트	일부 위젯(특히 Custom Analysis)은 데이터를 그래픽 형식으로 표시 가능	매우 자세한 도넛 그래프를 포함하여 폭넓은 그래픽 콘텍스트로 모든 데이터 표시 가능
관련 웹 인터페이스 페이지에 대한 링크	일부 위젯에서	모든 섹션에서
표시된 데이터의 시간 범위	사용자가 구성함	사용자가 구성함

관련 항목

대시보드 정보

트래픽 및 침입 이벤트 횟수 시간 그래프

Context Explorer(상황 탐색기) 상단에는 시간 경과에 따른 트래픽 및 침입 이벤트의 선 그래프가 있습니다. X축은 시간 간격을 나타냅니다(선택한 시간 창에 따라 5분에서 1개월까지). Y축은 킬로바이트 단위의 트래픽(파란색 선) 및 침입 이벤트 카운트(빨간색 선)를 나타냅니다.

X축의 최소 간격은 5분입니다. 이를 위해 시스템에서는 선택한 기간의 시작 지점과 종료 지점을 가장 가까운 5분 간격으로 반올림합니다.

기본적으로 이 섹션에는 선택한 기간의 모든 네트워크 트래픽 및 생성된 모든 침입 이벤트가 표시됩니다. 필터를 적용하면 필터에 지정된 기준과 관련이 있는 트래픽 및 침입 이벤트만 표시하도록 차트가 변경됩니다. 예를 들어 `Windows`의 **OS Name**으로 필터링하면 시간 그래프에는 Windows 운영체제를 사용하는 호스트와 관련된 트래픽 및 이벤트만 표시됩니다.

침입 이벤트 데이터로 Context Explorer(상황 탐색기)를 필터링하면(예: **Priority**가 `High`) 침입 이벤트에 더 집중할 수 있도록 파란색 트래픽 선이 숨겨집니다.

트래픽 및 이벤트 카운트에 대한 정확한 정보를 보려면 포인터를 그래프 선의 특정 지점에 올려놓을 수 있습니다. 색이 있는 선 중 하나로 포인터를 가져가면 해당 선이 그래프 앞으로 이동하므로 콘텍스트를 더 자세히 볼 수 있습니다.

이 섹션에서는 주로 Intrusion Events(침입 이벤트) 및 Connection Events(연결 이벤트) 테이블의 데이터를 보여줍니다.

보안 침해 지표 섹션

Context Explorer의 IOC(Indications of Compromise, 보안 침해 지표) 섹션에는 모니터링되는 네트워크에서 감염 가능성이 있는 호스트를 전체적으로 보여주는 두 개의 인터랙티브 섹션이 있습니다. 이 둘은 각각 트리거된 가장 일반적인 IOC 유형의 비례 보기 및 트리거된 지표 수 기준의 호스트 보기입니다.

IOC에 관한 자세한 내용은 보안 침해 지표 데이터 섹션을 참조하십시오.

지표별 호스트 그래프

도넛 형식의 Hosts by Indication 그래프는 모니터링되는 네트워크에서 호스트별로 트리거된 IOC의 비례 보기를 제공합니다. 내부 원에는 카테고리(예: `CnC Connected` 또는 `Malware Detected`)로 구분된 내용이 표시되며, 외부 원에는 특정 이벤트 유형(예: `Impact 2 Intrusion Event - attempted-admin` 또는 `Threat Detected in File Transfer`)별로 그러한 데이터가 더 자세히 구분되어 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

호스트별 지표 그래프

막대 형식의 Indications by Host 그래프에는 모니터링되는 네트워크에서 IOC가 가장 높은 호스트 15개에 의해 트리거된 고유한 보안 침해 지표(IOC)의 개수가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

네트워크 정보 섹션

Context Explorer(상황 탐색기)의 Network Information(네트워크 정보) 섹션에는 소스, 목적지, 사용자, 트래픽과 관련된 보안 영역, 네트워크의 호스트에서 사용하는 운영체제 구분, Firepower System이 네트워크에서 수행한 액세스 컨트롤 작업의 비례 보기 등 모니터링되는 네트워크의 연결 트래픽을 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

운영 체제 그래프

도넛 형식의 Operating Systems 그래프는 모니터링하는 네트워크의 호스트에서 탐지한 운영체제의 비율을 표시합니다. 내부 원에는 OS 이름(예: `Windows` 또는 `Linux`)으로 구분된 내용이 표시되며, 외부 원에는 특정 운영체제 버전(예: `Windows Server 2008` 또는 `Linux 11.x`)별 데이터가 더 자세히 구분되어 표시됩니다. 일부 긴밀하게 연결된 운영체제(예: Windows 2000, Windows XP 및 Windows Server 2003)는 그룹화됩니다. 매우 드물거나 인식되지 않는 운영체제는 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 테이블의 데이터를 주로 보여줍니다.

소스 **IP**별 트래픽 그래프

막대 형식의 Traffic by Source IP 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 사용자별 트래픽 그래프

막대 형식의 Traffic by Source User 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 사용자 15명에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

액세스 제어 작업별 연결 그래프

원 형식의 Connections by Access Control Action 그래프는 Firepower System이 모니터링되는 트래픽에서 수행한 액세스 컨트롤 작업(예: `Block(차단)` 또는 `Allow(허용)`)의 비례 보기를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Source User 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 IP별 트래픽 그래프

막대 형식의 Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 가장 활발한 목적지 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 목적지 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

인그레스/이그레스 보안 영역별 트래픽 그래프

막대 형식의 Traffic by Ingress/Egress Security Zone 그래프는 모니터링되는 네트워크에 구성된 각 보안 영역에 대한 들어오는 또는 나가는 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카

운트를 보여줍니다. 필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

나열된 각 보안 영역에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Ingress/Egress Security Zone 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 정보 섹션

Context Explorer(상황 탐색기)의 Application Information(애플리케이션 정보) 섹션에는 모니터링되는 네트워크에서 전반적인 애플리케이션 활동 내용을 보여주는 인터랙티브 그래프 3개 및 테이블 형식의 목록 1개가 있습니다. 트래픽, 침입 이벤트, 애플리케이션과 관련된 호스트 등은 각 애플리케이션에 할당된 비즈니스 연관성 또는 추정 위험 단위로 더 세부적으로 구성됩니다. Application Details List(애플리케이션 상세정보 목록)는 위험, 비즈니스 연관성, 카테고리 및 호스트 카운트의 인터랙티브 목록을 제공합니다.

이 섹션의 모든 "애플리케이션" 인스턴스에서 기본적으로 애플리케이션 정보 그래프 집합은 특별히 애플리케이션 프로토콜(예: DNS 또는 SSH)을 검사합니다. 특별히 클라이언트 애플리케이션(예: PuTTY 또는 Firefox) 또는 웹 애플리케이션(예: Facebook 또는 Pandora)을 검사하도록 Application Information(애플리케이션 정보) 섹션을 설정할 수도 있습니다.

애플리케이션 정보 섹션 초점

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Application Protocol Information(**애플리케이션 프로토콜 정보**)** 섹션으로 포인터를 이동합니다.

참고 동일한 Context Explorer(상황 탐색기) 세션에서 전에 이 설정을 변경한 경우에는 섹션 제목이 **Client Application Information(**클라이언트 애플리케이션 정보**)** 또는 **Web Application Information(**웹 애플리케이션 정보**)**으로 표시될 수 있습니다.

단계 **3** **Application Protocol(**애플리케이션 프로토콜**)**, **Client Application(**클라이언트 애플리케이션**)** 또는 **Web Application(**웹 애플리케이션**)**을 클릭합니다.

위험/비즈니스 관련성 및 애플리케이션별 트래픽 그래프

도넛 형식의 Traffic by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크에서 탐지되는 애플리케이션 트래픽의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 그래프는 변경되지 않습니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by Risk/Business Relevance and Application 그래프는 표시되지 않습니다.

이 그래프에서는 Connection Events(연결 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 침입 이벤트의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 침입 이벤트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 및 Application Statistics(애플리케이션 통계) 테이블의 데이터를 주로 보여줍니다.

위험/비즈니스 관련성 및 애플리케이션별 호스트 그래프

도넛 형식의 Hosts by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 호스트의 비례 표시를 관련 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`) 별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other(**기타**)**로 그룹화됩니다.

자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance(**비즈니스 연관성**)**를 클릭합니다. 기본 보기로 돌아가려면 **Risk(**위험**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

애플리케이션 상세정보 목록

Application Information(애플리케이션 정보) 섹션 아래쪽에는 Application Details List(애플리케이션 상세정보 목록)가 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 애플리케이션에 대한 예상 위험, 예상 비즈니스 연관성, 카테고리 및 호스트 카운트 정보를 제공하는 테이블입니다. 애플리케이션은 관련 호스트 카운트의 내림차순으로 나열됩니다.

Application Details List(애플리케이션 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다. 이 테이블에서는 Applications(애플리케이션) 테이블의 데이터를 주로 보여줍니다.

이 목록은 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. 탐색기 시간 범위가 변경되어도 목록은 변경되지 않습니다.

보안 인텔리전스 섹션

상황 탐색기의 Security Intelligence(보안 인텔리전스) 섹션에는 보안 인텔리전스에서 모니터링하거나 차단한 모니터링되는 네트워크의 트래픽을 전체적으로 보여주는 세 개의 인터랙티브 막대 그래프가 있습니다. 그래프에서 그러한 트래픽은 카테고리, 소스 IP 주소, 대상 IP 주소로 각각 정렬됩니다. 트래픽의 양(초당 킬로바이트 단위) 및 해당 연결 수가 모두 나타납니다.

카테고리별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Category 그래프는 모니터링되는 네트워크에서 상위 보안 인텔리전스 카테고리에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Category 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

소스 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Source IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 소스 IP 주소에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Source IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

대상 IP별 보안 인텔리전스 트래픽 그래프

막대 형식의 Security Intelligence Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 목적지 IP 주소에 대한 네트워크 트래픽(초당 킬로바이

트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Security Intelligence Traffic by Destination IP 그래프는 표시되지 않습니다.

이 그래프에서는 Security Intelligence Events(보안 인텔리전스 이벤트) 테이블의 데이터를 주로 보여줍니다.

침입 정보 섹션

Context Explorer(상황 탐색기)의 Intrusion Information(침입 정보) 섹션에는 모니터링되는 네트워크의 침입 이벤트를 전체적으로 보여주는 인터랙티브 그래프 6개와 테이블 형식의 목록 1개가 있습니다. 여기에는 영향 레벨, 공격 소스, 대상 목적지, 사용자, 우선순위 레벨, 침입 이벤트와 관련된 보안 영역과 더불어 침입 이벤트 분류, 우선순위 및 카운트의 자세한 목록이 포함됩니다.

영향별 침입 이벤트 그래프

원 형식의 Intrusion Events by Impact 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 영향 레벨(0~4)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS 통계) 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 공격자 그래프

막대 형식의 Top Attackers 그래프는 모니터링되는 네트워크에서 상위 공격 호스트 IP 주소(이벤트를 일으키는)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 사용자 그래프

막대 형식의 Top Users 그래프는 최고 침입 이벤트 카운트와 관련된 모니터링되는 네트워크의 사용자를 이벤트 카운트 단위로 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프는 침입 탐지(IDS) 사용자 통계 및 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다. 신뢰할 수 있는 사용자 데이터를 표시합니다.

우선 순위별 침입 이벤트 그래프

원 형식의 Intrusion Events by Priority 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 우선순위 레벨(예: `High`, `Medium` 또는 `Low`)로 그룹화하여 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 대상 그래프

막대 형식의 Top Targets 그래프는 모니터링되는 네트워크에서 상위 대상 호스트 IP 주소(이벤트를 일으키는 연결의 대상)에 대한 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 인그레스/이그레스 보안 영역 그래프

막대 형식의 Top Ingress/Egress Security Zones 그래프는 모니터링되는 네트워크에 설정된 각 보안 영역(그래프 설정에 따라 Ingress 또는 Egress)과 관련된 침입 이벤트의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

침입 이벤트 상세정보 목록

Intrusion Information(침입 섹션 아래쪽에는 Intrusion Event Details List(침입 이벤트 상세정보 목록)이 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 침입 이벤트에 대한 분류, 예상 우선순위 및 이벤트 카운트 정보를 제공하는 테이블입니다. 이벤트는 이벤트 카운트의 내림차순으로 나열됩니다.

Intrusion Event Details List(침입 이벤트 상세정보 목록) 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 이 테이블에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

파일 정보 섹션

Context Explorer의 Files Information(파일 정보) 섹션에는 모니터링되는 네트워크의 파일 및 악성코드 이벤트를 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

6개 중 5개 그래프에는 AMP for Networks (구 AMP for Firepower) 관련 데이터, 즉 네트워크 트래픽에서 탐지되는 파일의 악성코드 속성, 파일 형식, 파일 이름과 이러한 파일을 보내는(업로드) 호스트 및 받는(다운로드) 호스트가 표시됩니다. 마지막 그래프에는 AMP for Networks 또는 AMP for Endpoints가 조직에서 탐지한 모든 악성코드 위협이 표시됩니다.

참고 침입 정보에 대해 필터링하는 경우 전체 Files Information(파일 정보) 섹션은 표시되지 않습니다.

상위 파일 유형 그래프

도넛 형식의 Top File Types 그래프는 네트워크 트래픽에서 탐지되는 파일 형식(외부 원)의 비례 보기를 파일 카테고리(내부 원)로 그룹화하여 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 파일 이름 그래프

막대 형식의 Top File Names 그래프는 네트워크 트래픽에서 탐지되는 고유한 상위 파일 이름의 카운트를 보여줍니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

성향별 파일 그래프

원 형식의 Top File Types 그래프는 AMP for Networks 기능(구 AMP for Firepower)으로 탐지한 악성코드 성향의 비율을 표시합니다. 성향은 Firepower Management Center이(가) 악성코드 클라우드 조회를 수행한 파일에만 있습니다. 클라우드 조회를 트리거하지 않은 파일은 `N/A` 성향을 갖습니다. `Unavailable` 성향은 Firepower Management Center에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 전송 파일 그래프

막대 형식의 Top Hosts Sending Files 그래프는 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 전송 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 호스트 수신 파일 그래프

막대 형식의 Top Hosts Receiving Files 그래프는 상위 파일 수신 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 수신 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware(**악성코드**)**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files(**파일**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 파일 보기로 돌아갑니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

상위 악성코드 탐지 그래프

막대 형식의 op Malware Detections 그래프에는 AMP for Networks 또는 AMP for Endpoints가 조직에서 탐지한 상위 악성코드 위협 숫자가 표시됩니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프가 AMP for Networks 데이터를 표시하려면 Malware(악성코드) 라이선스가 있어야 합니다.

이 그래프에서는 File Events(파일 이벤트) 및 Malware Events(악성코드 이벤트) 테이블의 데이터를 주로 보여줍니다.

지리위치 정보 섹션

Context Explorer(상황 탐색기)의 Geolocation Information(지리위치 정보) 섹션에는 모니터링되는 네트워크의 호스트가 데이터를 교환하는 국가를 전체적으로 보여주는 3개의 인터랙티브 도넛 그래프가 있습니다. 이러한 그래프는 각각 이니시에이터 또는 응답자 국가 단위의 고유한 연결, 소스 또는 대상 국가 단위의 침입 이벤트, 수신 또는 송신 국가 단위의 파일 이벤트에 대한 것입니다.

이니시에이터/응답자 국가별 연결 그래프

도넛 형식의 Connections by Initiator/Responder Country 그래프는 이니시에이터(기본값) 또는 응답자로서 네트워크의 연결과 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 응답자 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Responder(**응답자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Initiator(**이니시에이터**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Initiator 보기로 돌아갑니다.

이 그래프에서는 Connection Summary Data(연결 요약 데이터) 테이블의 데이터를 주로 보여줍니다.

소스/목적지 국가별 침입 이벤트 그래프

도넛 형식의 Intrusion Events by Source/Destination Country 그래프는 이벤트의 소스(기본값) 또는 목적지로서 네트워크의 침입 이벤트와 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 침입 이벤트의 목적지 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Destination(**목적지**)**을 클릭합니다. 기본 보기로 돌아가려면 **Source(**소스**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Source 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events(침입 이벤트) 테이블의 데이터를 주로 보여줍니다.

전송/수신 국가별 파일 이벤트 그래프

도넛 형식의 File Events by Sending/Receiving Country 그래프는 네트워크의 파일 이벤트에서 파일을 전송하거나(기본값) 수신하는 것으로 탐지되는 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 파일 수신 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Receiver(**수신자**)**를 클릭합니다. 기본 보기로 돌아가려면 **Sender(**발신자**)**를 클릭합니다. Context Explorer(상황 탐색기)에서 빠져나가도 기본 Sender 보기로 돌아갑니다.

이 그래프에서는 File Events(파일 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 정보 섹션

Context Explorer의 URL Information 섹션에는 모니터링되는 사용자 네트워크의 호스트가 데이터를 교환하는 URL을 전체적으로 보여주는 3개의 인터랙티브 막대 그래프가 있습니다. 여기에는 URL과 연결된 트래픽 및 고유한 연결이 포함되며 개별 URL, URL 카테고리 및 URL 평판 단위로 정렬됩니다. URL 정보에 대해서는 필터링할 수 없습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 전체 URL Information(URL 정보) 섹션은 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

URL별 트래픽 그래프

막대 형식의 Traffic by URL 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 카테고리별 트래픽 그래프

막대 형식의 Traffic by URL Category 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 카테고리(예: `Search Engines(검색 엔진)` 또는 `Streaming Media(스트리밍 미디어)`)에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Category 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

URL 평판별 트래픽 그래프

막대 형식의 Traffic by URL Reputation(URL 평판별 트래픽) 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 평판 그룹(예: , Trusted(신뢰할 수 있는), 또는 , Neutral(보통))에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL 평판에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.

자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하는 경우 Traffic by URL Reputation 그래프는 표시되지 않습니다.

이 그래프가 URL 카테고리 및 평판 데이터를 포함하려면 URL Filtering(URL 필터링) 라이선스가 있어야 합니다.

이 그래프에서는 URL Statistics(URL 통계) 및 Connection Events(연결 이벤트) 테이블의 데이터를 주로 보여줍니다.

Context Explorer 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 보안 분석가

Context Explorer(상황 탐색기) 새로 고침

Context Explorer(상황 탐색기)는 표시되는 정보를 자동으로 업데이트하지 않습니다. 새로운 데이터를 표시하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기) 자체를 다시 고치면(브라우저 프로그램을 새로 고치거나 Context Explorer(상황 탐색기)에서 나간 후 다시 돌아오는 방법 사용) 표시되는 모든 정보를 새로 고칠 수 있지만, 섹션 설정에 대해 변경한 내용(예: Ingress/Egress 그래프 및 애플리케이션 정보 섹션)이 유지되지 않으며 로딩에 지연이 발생할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 오른쪽 위에 있는 **Reload(**다시 로드**)**를 클릭합니다.

새로 고침이 완료되기 전까지 **Reload(**다시 로드**)**는 흐리게 표시됩니다.

Context Explorer(상황 탐색기) 시간 범위 설정

Context Explorer(상황 탐색기)의 시간 범위를 마지막 시간 단위(기본값)로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경해도 변경 사항을 반영하여 Context Explorer(상황 탐색기)가 자동으로 업데이트되지는 않습니다. 새로운 시간 범위를 적용하려면 탐색기를 수동으로 새로 고쳐야 합니다.

Context Explorer(상황 탐색기)에서 빠져나가거나 로그인 세션을 종료해도 시간 범위에 대한 변경 사항은 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Show the last(**마지막 선택 표시**)** 드롭다운 목록에서 시간 범위를 선택합니다.

단계 **3** 선택적으로, 새 시간 범위의 데이터를 보려면 **Reload(**다시 로드**)**를 클릭합니다.

팁 **Apply Filters(**필터 적용**)**를 클릭해도 시간 범위 업데이트가 적용됩니다.

Context Explorer(상황 탐색기) 섹션 최소화 및 최대화

하나 이상의 Context Explorer(상황 탐색기) 섹션을 최소화할 수 있습니다. 이는 특정 섹션에만 집중하거나 더 간단한 보기를 원하는 경우 유용합니다. Traffic and Intrusion Event Counts Time 그래프는 최소화할 수 없습니다.

페이지를 새로 고치거나 어플라이언스에서 로그아웃해도 최소화 또는 최대화 구성 상태는 Context Explorer(상황 탐색기) 섹션에서 그대로 유지됩니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 섹션을 최소화하려는 경우에는 섹션 제목 표시줄의 최소화(−)를 클릭합니다.

단계 **3** 섹션을 최대화하려면 최소화된 섹션에서 제목 표시줄의 최대화(최대화(□))를 클릭합니다.

Context Explorer(상황 탐색기) 데이터에 대해 드릴다운

Context Explorer(상황 탐색기)에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. (Traffic and Intrusion Events over Time 그래프에서는 드릴다운할 수 없습니다.) 예를 들어 Traffic by Source IP 그래프에서 IP 주소를 드릴다운하면 Connection Events(연결 이벤트) 테이블의 Connections with Application Details(애플리케이션 상세정보 연결) 보기가 표시되며, 선택한 소스 IP 주소와 연결된 데이터만 포함됩니다.

검사하는 데이터 유형에 따라 콘텍스트 메뉴에 추가 옵션이 표시될 수 있습니다. 특정 IP 주소와 관련된 데이터 포인트는 선택하는 IP 주소에서 호스트 또는 whois 정보를 볼 수 있는 옵션을 제공합니다. 특정 애플리케이션과 관련된 데이터 포인트는 선택하는 애플리케이션에 대한 애플리케이션 정보를 볼 수 있는 옵션을 제공합니다. 특정 사용자와 관련된 데이터 포인트는 해당 사용자의 사용자 프로파일 페이지를 볼 수 있는 옵션을 제공합니다. 침입 이벤트 메시지와 관련된 데이터 포인트는 해당 이

벤트와 관련된 침입 규칙에 대한 규칙 문서를 볼 수 있는 옵션을 제공하며, 특정 IP 주소와 관련된 데이터 포인트는 해당 주소를 차단 또는 차단 금지 목록에 추가할 수 있는 옵션을 제공합니다. 이 목록에 대한 자세한 내용은 글로벌 및 도메인 보안 인텔리전스 목록와 그 하위 항목을 참조하십시오.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** **Traffic and Intrusion Events over Time**을 제외한 임의의 섹션에서 조사하려는 데이터 포인트를 클릭합니다.

단계 **3** 선택한 데이터 포인트에 따라 여러 가지 옵션이 표시됩니다.

- 테이블 보기에서 이 데이터를 더 자세히 살펴보려면 **Drill into Analysis(**분석을 위해 드릴다운**)**를 선택합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 관련 호스트에 대해 자세히 알아보려면 **View Host Information(**호스트 정보 보기**)**을 선택합니다.
- 특정 IP 주소의 데이터 포인트를 선택했으며 해당 주소에서 whois 검색을 수행하려면 **Whois**를 선택합니다.
- 특정 애플리케이션과 관련된 데이터 포인트를 선택했으며 해당 애플리케이션에 대해 자세히 알아보려면 **View Application Information(**애플리케이션 정보 보기**)**을 선택합니다.
- 특정 사용자와 관련된 데이터 포인트를 선택했으며 해당 사용자에 대해 자세히 알아보려면 **View User Information(**사용자 정보 보기**)**을 선택합니다.
- 특징 침입 이벤트 사용자와 관련된 데이터 포인트를 선택했으며 관련된 침입 규칙에 대해 자세히 알아보려면 **View Rule Documentation(**규칙 문서 보기**)**을 선택합니다. 원한다면 **Rule Documentation(**규칙 문서**)**을 클릭해 더 구체적인 규칙 상세정보를 확인합니다.
- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 해당 IP 주소를 보안 인텔리전스 전역 차단 및 차단 금지 목록에 추가하려면 적절한 옵션을 선택합니다.

Context Explorer의 필터

Context Explorer(상황 탐색기)에 처음 표시되는 기본적인 광범위한 데이터를 이용해 네트워크의 활동에 대해 좀 더 세부적인 콘텍스트를 얻기 위해 이러한 데이터를 필터링할 수 있는 옵션이 제공됩니다. 필터는 모든 유형의 Firepower System 데이터(URL 정보 제외)를 포괄하며, 포함과 제외를 지원하고, Context Explorer(상황 탐색기) 그래프 데이터 포인트에서 클릭하여 빠르게 적용될 수 있으며, 전체 Explorer에 영향을 미칩니다. 한 번에 최대 20개의 필터를 적용할 수 있습니다.

Context Explorer(상황 탐색기) 데이터에 여러 방법으로 필터를 추가할 수 있습니다.

- Add Filter(필터 추가) 대화 상자에서
- 탐색기에서 데이터 포인트를 선택한 경우 콘텍스트 메뉴에서

- 특정 상세정보 보기 페이지(Application Detail, Host Profile, Rule Detail 및 User Profile)에 나타나는 텍스트 링크에서 이러한 링크를 클릭하면 상세정보 보기 페이지의 관련 데이터에 따라 Context Explorer(상황 탐색기)가 자동으로 열리고 필터링이 수행됩니다. 예를 들어 사용자 `jenkins`에 대한 사용자 상세정보 페이지에서 Context Explorer(상황 탐색기) 링크를 클릭하면 해당 사용자와 관련된 데이터만 표시하도록 탐색기가 제한됩니다.

일부 필터 유형은 다른 유형과 호환되지 않습니다. 예를 들어 침입 이벤트(예: **Device** 및 **Inline Result**)와 관련된 필터는 연결 이벤트와 관련된 필터(예: **Access Control Action**)와 동시에 적용할 수 없습니다. 시스템에서 연결 이벤트 데이터와 침입 이벤트 데이터를 정렬할 수 없기 때문입니다. 시스템에서는 호환되지 않는 필터가 동시에 적용되는 것을 방지합니다. 한 필터 유형이 좀 더 최근에 활성화되었으면, 비호환성이 존재하는 한 호환되지 않는 유형의 필터는 표시되지 않습니다.

여러 필터가 활성화된 경우 동일한 데이터 유형에 대한 값은 OR 검색 기준으로 취급되므로, 적어도 하나의 값과 일치하는 모든 데이터가 표시됩니다. 서로 다른 데이터 유형에 대한 값은 AND 검색 기준으로 취급되므로, 데이터는 필터링하는 각 데이터 유형에 대해 적어도 하나의 값과 일치해야 합니다. 예를 들어 `Application: 2channel`, `Application: Reddit` 및 `User: edickinson` 필터 집합에 대해 나타나는 데이터는 사용자 `edickinson` 및**(AND)** 애플리케이션 `2channel` 또는**(OR)** 애플리케이션 `Reddit`과 관련이 있어야 합니다.

다중 도메인 구축의 경우 상위 도메인에서 Context Explorer(상황 탐색기)를 볼 때 여러 하위 도메인을 필터링할 수 있습니다. 이 경우 **IP Address(IP** 주소**)** 필터를 추가할 때 주의해야 합니다. 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 리터럴 IP 주소를 사용하여 이 설정을 제한하면 예기치 않은 결과가 발생할 수 있습니다.

표시되는 데이터는 매니지드 디바이스 허가 및 구축 방법, 데이터를 제공하는 기능 설정 여부 등의 요소에 따라 달라집니다.

참고 필터는 필요한 정확한 Firepower 데이터 콘텍스트를 특정 시간에 얻기 위한 간단하고 민첩한 툴 역할을 합니다. 필터의 목적은 영구적인 설정 설정이 아니며, Context Explorer(상황 탐색기)에서 빠져나가거나 세션을 종료하면 필터도 사라집니다. 나중에 사용하기 위해 필터 설정을 보존하려면 필터링된 Context Explorer(상황 탐색기) 보기 저장, 24 페이지 섹션을 참조하십시오.

데이터 유형 필드 옵션

다음 표에는 필터로 이용할 수 있는 데이터 유형과 각 유형에 대한 예제 및 간단한 정의가 나열되어 있습니다.

표 *2:* 필터 데이터 유형

유형	값 예	정의
액세스 컨트롤 작업	`Allow(허용)`, `Block(차단)`	트래픽을 허용 또는 차단하기 위해 액세스 컨트롤 정책에서 수행하는 작업입니다.

유형	값 예	정의
애플리케이션 범주	web browser(웹 브라우저), email(이메일)	애플리케이션의 가장 핵심적인 기능에 대한 일반 분류입니다.
애플리케이션 이름	Facebook, HTTP	애플리케이션의 이름입니다.
애플리케이션 위험성	Very High(매우 높음), Medium(중간)	애플리케이션의 예상 보안 위험입니다.
애플리케이션 태그	encrypts communications(통신 암호화), sends mail(메일 전송)	애플리케이션에 대한 추가 정보(애플리케이션에는 0부터 원하는 수만큼의 태그 포함 가능)입니다.
애플리케이션 유형	Client(클라이언트), Web Application(웹 애플리케이션)	애플리케이션 유형(application protocol, client 또는 web application)입니다.
사업 타당성	Very Low(매우 낮음), High(높음)	비즈니스 활동에 대한 애플리케이션의 예상 연관성(레크리에이션과 반대)입니다.
대륙	North America(북미), Asia(아시아)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 대륙입니다.
Country	Canada(캐나다), Japan(일본)	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 국가입니다.
디바이스	device1.example.com, 192.168.1.3	모니터링되는 네트워크에 있는 디바이스의 이름 또는 IP 주소입니다.
도메인	Asia Division(아시아 부서), Europe Division(유럽 부서)	네트워크 활동을 그래프로 작성할 디바이스의 도메인입니다. 이 데이터 유형은 다중 도메인 구축에서만 표시됩니다.
이벤트 분류	Potential Corporate Policy Violation(잠재적 기업 정책 위반), Attempted Denial of Service(시도된 서비스 거부)	침입 이벤트에 대한 설명으로, 침입 이벤트를 트리거한 규칙, 디코더 또는 전처리기의 분류에 의해 결정됩니다.
이벤트 메시지	dns response(dns 응답), P2P	이벤트에 의해 생성되는 메시지로, 이벤트를 트리거한 규칙, 디코더 또는 전처리기에 의해 결정됩니다.
파일 속성	Malware(악성코드), Clean(클린)	Firepower Management Center가 악성코드 클라우드 조회를 수행한 파일의 성향입니다.
파일 이름	Packages.bz2	네트워크 트래픽에서 탐지되는 파일의 이름입니다.

유형	값 예	정의
파일 SHA256	임의의 32비트 문자열	Firepower Management Center에서 악성 코드 클라우드 조회를 수행한 파일의 SHA-256 해시 값입니다.
File Type(파일 유형)	GZ, SWF, MOV	네트워크 트래픽에서 탐지되는 파일 형식입니다.
파일 유형 카테고리	Archive(아카이브), Multimedia(멀티미디어), Executables(실행파일)	네트워크 트래픽에서 탐지되는 파일 형식의 일반 카테고리입니다.
IP 주소	192.168.1.3, 2001:0db8:85a3::0000/24	IPv4 또는 IPv6 주소, 주소 범위 또는 주소 블록입니다. IP 주소를 검색하면 이벤트가 반환되는데, 여기서 해당 주소는 이벤트의 소스 또는 대상입니다.
영향 레벨	Impact Level 1(영향 레벨 1), Impact Level 2(영향 레벨 2)	모니터링되는 네트워크에서 이벤트의 예상 영향입니다.
인라인 결과	dropped(삭제됨), would have dropped(삭제된 것으로 추정됨)	트래픽이 삭제되었는지, 삭제된 것으로 추정되는지 또는 시스템에 의해 작동되지 않았는지의 여부입니다.
IOC 카테고리	High Impact Attack(강력한 공격), Malware Detected(악성코드 탐지)	트리거된 IOC(Indications of Compromise) 이벤트에 대한 카테고리입니다.
IOC 이벤트 유형	exploit-kit, malware-backdoor	특정 IOC(Indications of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킵니다.
악성코드 위협 이름	W32.Trojan.a6b1	악성코드 위협의 이름입니다.
OS Name	Windows, Linux	운영체제의 이름입니다.
OS Version(OS 버전)	XP, 2.6	운영체제의 특정 버전입니다.
Priority(우선순위)	high(높음), low(낮음)	이벤트의 예상 긴급도입니다.
보안 인텔리전스 카테고리	Malware(악성코드), Spam(스팸)	보안 인텔리전스로 확인된 위험 트래픽의 카테고리입니다.
보안 영역	My Security Zone(내 보안 영역), Security Zone X(보안 영역 X)	트래픽이 분석되고 통과되는(인라인 구축의 경우) 인터페이스 집합입니다.
SSL	yes, no	SSL 또는 TLS 암호화 트래픽입니다.

유형	값 예	정의
User	`wsmith`, `mtwain`	모니터링되는 네트워크의 호스트에 로그인하는 사용자의 ID입니다.

추가 필터 창에서 필터 생성

이 절차를 사용하면 Add Filter(필터 추가) 창에서 필터를 처음부터 만들 수 있습니다. (콘텍스트 메뉴를 사용하여 빠른 필터를 만들 수도 있습니다.)

Context Explorer(상황 탐색기) 왼쪽 위의 **Filters(**필터**)** 아래에 있는 더하기(+)를 클릭하여 액세스할 수 있는 Add Filter(필터 추가) 창에는 필터가 2개만 있습니다.

- **Data Type(**데이터 유형**)** 드롭다운 목록에는 Context Explorer(상황 탐색기)를 제한하는 데 사용할 수 있는 많은 유형의 Firepower System 데이터가 포함되어 있습니다. 데이터 유형을 선택한 다음 **Filter(**필터**)** 필드에서 해당 유형에 대한 특정 값(예: **Continent** 유형에 대해 `Asia` 값)을 입력합니다. 사용자에게 도움이 되도록 선택 가능한 데이터 유형에 대한 몇 가지 예제 값이 Filter(필터) 필드에 회색으로 표시됩니다. (필드에 데이터를 입력하면 이러한 값이 지워집니다.)
- 필터 필드 `*` 같은 특수 한 검색 파라미터 입력과 `!` 이벤트의 수를 기본적으로 검색 합니다. 필터 파라미터 앞에 `!` 기호를 추가하면 제외하는 필터를 만들 수 있습니다.

참고 추가하는 필터는 자동으로 적용되지 않습니다. Context Explorer(상황 탐색기)에서 필터를 보려면 **Apply Filters(**필터 적용**)**를 클릭해야 합니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 더하기(+)를 클릭합니다.

단계 **3** **Data Type(**데이터 유형**)** 드롭다운 목록에서 필터링할 데이터 유형을 선택합니다.

단계 **4** **Filter(**필터**)** 필드에 필터링할 데이터 유형 값을 입력합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** 선택적으로, 원하는 필터 집합이 구성될 때까지 이전 단계를 반복하여 필터를 더 추가합니다.

단계 **7** **Apply Filters(**필터 적용**)**을 클릭합니다.

관련 항목

데이터 유형 필드 옵션, 20 페이지

검색 제약 조건

콘텍스트 메뉴에서 빠른 필터 생성

Context Explorer(상황 탐색기) 그래프 및 목록 데이터를 탐색할 때 데이터 포인트를 클릭한 다음 콘텍스트 메뉴를 사용하여 해당 데이터를 기반으로 빠르게 필터를 만들 수 있습니다(포함 또는 제외). 콘텍스트 메뉴를 사용하여 데이터 유형(애플리케이션, 사용자, 침입 이벤트 메시지, 개별 호스트 등)의 정보에 대해 필터링하면 필터 위젯에는 해당 데이터 유형에 대한 관련 세부 사항 페이지(예: 애플리케이션 데이터의 경우 Application Detail(애플리케이션 세부 사항))로 연결되는 위젯 정보가 포함됩니다. URL 데이터에 대해서는 필터링할 수 없습니다.

특정 그래프나 목록 데이터를 좀 더 자세히 조사하려는 경우에도 콘텍스트 메뉴를 사용할 수 있습니다.

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**을(를) 선택합니다.

단계 **2** Traffic and Intrusion Events over Time을 제외한 탐색기 섹션 또는 URL 데이터가 포함된 섹션에서 필터링할 데이터 포인트를 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 이 데이터에 대한 필터를 추가하려면 **Add Filter(**필터 추가**)**를 클릭합니다.
- 이 데이터에 대한 제외 필터를 추가하려면 **Add Exclude Filter(**제외 필터 추가**)**를 클릭합니다. 필터를 적용하면 제외된 값과 관련된 데이터 외의 모든 데이터가 표시됩니다. 제외 필터는 필터 값 앞에 느낌표(!)를 표시합니다.

필터링된 **Context Explorer(**상황 탐색기**)** 보기 저장

Context Explorer(상황 탐색기)에서 나오거나 세션 종료 후 필터 설정을 Context Explorer(상황 탐색기)에 저장하려면, 원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다. 적용된 필터는 Context Explorer(상황 탐색기) 페이지 URL에 통합되므로 해당 페이지의 즐겨찾기를 로드하면 해당 필터도 로드됩니다.

프로시저

원하는 필터가 적용된 Context Explorer(상황 탐색기)의 브라우저 즐겨찾기를 생성합니다.

필터 데이터 보기

다중 도메인 구축 시 현재 도메인 및 하위 도메인의 데이터를 볼 수 있습니다. 더 높은 수준 또는 동기 도메인의 데이터는 볼 수 없습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 해당 필터 위젯에서 **Information(**정보**)**을 클릭합니다.

필터 삭제

프로시저

단계 **1** **Analysis(**분석**)** > **Context Explorer(**상황 탐색기**)**를 선택합니다.

단계 **2** 왼쪽 위의 **Filters(**필터**)** 아래에서 아무 필터 위젯의 지우기(✕)을 클릭합니다.

팁 모든 필터를 동시에 삭제하려면 **Clear(**지우기**)** 버튼을 클릭합니다.

필터 삭제