클라우드 가시성 보고서

보고서는 네트워크 및 전반적인 상태에 대한 통찰력과 그에 따른 의사 결정에 활용할 수 있는 귀중한 통계 정보를 제공합니다. 멀티 클라우드 방어에서는 다음 유형의 보고서를 생성할 수 있습니다.

Discovery

DNS 쿼리 및 VPC 플로우 로그에서 대역 외 트래픽 정보를 가져오고 데이터를 위협 인텔리전스 및 클라우드 인벤토리 정보와 상호 연결하여 검색 보고서 생성가 생성됩니다. 이러한 로그는 클라우드 서비스 제공업체의 VPC가 S3 버킷으로 로그를 전송하도록 구성한 경우에만 사용할 수 있습니다. 이러한 로그는 멀티 클라우드 방어 컨트롤러로 직접 전송됩니다.

보고서에는 다음이 포함됩니다.

- 검색 상위 수준 보고 - 네트워크 및 클라우드 자산 분석으로, 볼륨 및 고유한 필드 값 카운트로 표시합니다. 네트워크 행동을 수량화하여 클라우드 환경에서 진행 중인 상황에 대한 인사이트를 도출할 수 있습니다.
- 네트워크 트래픽 - 바이트 - 이 그래프는 트래픽 방향별 바이트의 볼륨을 표시합니다. 바이트 볼륨이 이동하는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 볼 수 있습니다.
- 네트워크 트래픽 - 패킷 - 이 그래프는 트래픽 방향별 패킷 볼륨을 표시합니다. 패킷 볼륨이 이동하는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 볼 수 있습니다.
- 네트워크 트래픽 - 이벤트 - 이 그래프는 트래픽 방향별 이벤트 볼륨을 표시합니다. 이벤트 볼륨이 전송되는 위치(인그레스, 이그레스 또는 이스트-웨스트)를 확인할 수 있습니다.
- 인그레스 어카운트 요약 - 이 요약에는 인그레스 네트워크 트래픽이 있는 클라우드 자산의 고유한 수가 CSP별로 표시됩니다. CSP 환경으로 통신하는 자산의 흐름을 검토할 수 있습니다.
- 이그레스 어카운트 요약 - 이 요약은 이그레스 네트워크 트래픽이 있는 클라우드 자산의 고유한 수를 CSP(Cloud Service Provider, 클라우드 서비스 제공자)별로 표시합니다. CSP 환경에서 통신하는 자산의 흐름을 검토할 수 있습니다.
- 국가별 인그레스 네트워크 이벤트 - 이 지리 히트맵은 국가별 인그레스 트래픽의 양을 보여줍니다. 클라우드 환경과 통신하는 국가를 볼 수 있습니다.
- 국가별 이그레스 네트워크 이벤트 - 이 지리 히트맵은 국가별 이그레스 트래픽의 양을 보여줍니다. 클라우드 환경과 통신하는 국가를 볼 수 있습니다.

- 상위 **10**개 소스 국가 - 이 그래프는 기타 네트워크 분석과 함께 이벤트 규모 기준 상위 10개 소스 국가를 표시합니다. 클라우드 환경과 가장 많이 통신하는 소스 국가를 요약한 것입니다.
- 상위 **10**개 대상 국가 - 이 그래프는 기타 네트워크 분석과 함께 이벤트 양 기준 상위 10개 대상 국가를 표시합니다. 클라우드 환경과 통신하는 주요 대상 국가에 대한 요약입니다.
- 상위 **10**개 인그레스 소스 **IP** 주소 - 이 그래프는 기타 네트워크 분석과 함께 볼륨 기준 상위 10개 소스 IP 주소를 표시합니다. 가장 많은 인바운드 이벤트를 생성하는 엔터티를 볼 수 있습니다.
- 상위 **10**개 이그레스 대상 **IP** 주소 - 이 그래프는 기타 네트워크 분석과 함께 볼륨별 상위 10개 대상 IP 주소를 표시합니다. 클라우드 환경이 주로 통신하는 엔터티를 볼 수 있습니다.
- 볼륨별 상위 **10**개 **FQDN** 범주 이름 - 이 그래프는 FQDN에 대한 범주 이름을 볼륨별로 표시합니다. 클라우드 환경에서 요청하는 FQDN을 기준으로 상위 범주 유형을 볼 수 있습니다.
- 볼륨별 상위 **10**개 **FQDN** - 이 그래프는 볼륨별 상위 10개 FQDN을 표시합니다. 클라우드 환경에서 요청한 상위 FQDN을 볼 수 있습니다.
- 볼륨별 상위 **10**개의 악성 **FQDN** - 이 그래프는 볼륨별 상위 10개의 악성 FQDN을 표시합니다. 악의적인 또는 의심스러운 범주 이름이 발견되면 해당 범주 이름의 상위 FQDN이 여기에 표시됩니다.
- **MITRE ATT&CK**에 매핑된 **FQDN** 범주 이름 - MITRE ATT+CK에 매핑된 상위 10개의 악성 범주 이름을 표시합니다. 이 보기에서는 엔터프라이즈 MITRE ATT+CK 프레임워크를 사용하여 FQDN 범주 이름이 공격 체인과 어떤 관련이 있는지에 대한 추가 상황을 제공합니다.

위협 지표 스냅샷

위협 및 클라우드 분석 보고서 생성 보고서는 게이트웨이 인스턴스에 대한 데이터를 편집한 것입니다. 이 보고서를 이용하여 트래픽 패턴, 임계값 충족 시기와 방법, 공격 추세 및 특정 인스턴스를 검토하여 게이트웨이의 위협 상황을 파악할 수 있습니다. 보고서에는 다음 사항이 포함되어 있습니다.

- **IDS/IPS** 탐지 - 이 데이터는 선택한 시간 범위 동안 탐지된 공격의 수, 공격 유형, 탐지된 공격 시간, 그리고 상위 10개의 IDS/IPS 서명을 보여줍니다.
- **WAF** 탐지 - 이 데이터는 WAF 규칙에 의해 탐지된 공격의 수, 탐지된 공격 시간, 선택한 시간 범위 동안의 상위 10개 WAF 서명입니다.
- 볼륨별 위협 재배치 - 이 단계 구분도는 WAF 및 IDS/IPS 이벤트 모두에 대한 공격의 볼륨을 볼륨 기준으로 국가별로 표시합니다.
- 볼륨 및 시간별 상위 **10**개 공격 국가 - 이 가로 막대 차트는 전체 기간 동안 가장 많은 이벤트를 생성한 상위 10개 국가의 볼륨을 표시한 다음, 해당 볼륨을 해당 기간 동안 이벤트가 발생한 시간 단위로 세분화하여 표시합니다.
- 정책 및 방지 - 이 데이터 차트는 게이트웨이가 구축된 CSP 환경에서 게이트웨이 보안 유형이 수행하는 작업을 보여줍니다. 여기에는 작업 유형, 작업에서 생성되는 이벤트 수, 게이트웨이 보안 유형 등이 포함됩니다.

멀티 클라우드 방어 게이트웨이에서 데이터를 수집하고 폴링하려면 정책에서 웹 애플리케이션 방화벽(WAF), 침입 탐지 및 방지(IDS/IPS) 규칙이 활성화되어 있어야 합니다.

추가 정보:

- 검색 보고서 생성, on page 3
- 위협 및 클라우드 분석 보고서 생성, 3 페이지

검색 보고서 생성

멀티 클라우드 방어 컨트롤러에서 처리하기 전에 S3 버킷으로 전송된 DNS 쿼리 및 VPC 플로우 로그를 가져와서 검색 보고서를 생성합니다.

단계 **1** 멀티 클라우드 방어 컨트롤러 페이지에서 **Report(**보고서**)**로 이동합니다.

단계 **2** **Discovery(**검색**)**를 선택합니다.

단계 **3** Threat & Cloud Analytics Report(위협 및 클라우드 분석 보고서)에서 가져오는 데이터의 드롭다운 목록에서 일별, 주별, 월별, 분기별 또는 연간 **Frequency(**빈도**)**를 선택합니다.

- **Daily(**매일**)** - 오전 12시부터 24시간 동안. 이는 UTC 시간입니다.
- **Weekly(**매주**)** - 월요일부터 일요일까지
- **Monthly(**매월**)** - 일반적으로 월의 시작부터 말일까지
- **Quarterly(**분기별**)** - 분기의 시작부터 끝까지. 일반적으로 분기는 1월 1일~3월 31일, 4월 1일~6월 30일, 7월 1일~9월 30일 및 10월 1일~12월 31일로 정의됩니다.
- **Yearly(**매년**)** - 선택한 연도의 1월 1일부터 12월 31일까지.

단계 **4** 날짜를 선택합니다. **Calendar(**달력**)** 드롭다운을 사용하여 데이터를 수집할 시간 범위 또는 특정 날짜를 선택합니다. 회색으로 표시된 날짜는 컴파일할 데이터가 없는 것입니다. 보고서를 생성하는 데 사용할 수 있는 데이터가 없는 경우 정책에 WAF 및 IDS/IP 규칙이 포함되어 있는지 확인합니다.

단계 **5** **Generate Report(**보고서 생성**)**를 클릭합니다. 검색 보고서가 새 탭에서 생성됩니다.

단계 **6** 보고서를 로컬로 저장하려면 **Print Report(**보고서 인쇄**)**를 클릭합니다. 로컬 서버의 위치로 이동하여 보고서를 저장합니다.

위협 및 클라우드 분석 보고서 생성

위협 및 클라우드 분석 보고서는 멀티 클라우드 방어 게이트웨이에서 수집하고 검사한 트래픽을 사용하여 생성되는 위협 지표 스냅샷입니다. 이 기능은 멀티 클라우드 방어이(가) 현재 데이터 경로에 있는 것처럼 더욱 포괄적인 보고서를 제공하며 검색 보고서를 보완합니다.

마감일, 월말, 분기 말 또는 연말까지는 이벤트의 질적 요약을 수행할 수 없으므로 당일의 보고서는 생성할 수 없습니다.

참고 멀티 클라우드 방어 게이트웨이에서 데이터를 수집하고 폴링하려면 정책에서 WAF(Web Application Firewall), 침입 탐지 및 보호(IDS/IPS) 규칙을 활성화해야 합니다. 자세한 내용은 각각 다음 링크를 참조하십시오.

- 웹 애플리케이션 방화벽
- 네트워크 침입(IDS/IPS) 프로파일

위협 지표 스냅샷을 포함하여 위협 및 클라우드 분석을 생성하려면 다음 절차를 사용하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 페이지에서 **Report(**보고서**)**로 이동합니다.

단계 **2** **Threat Indicators Snapshot(**위협 지표 스냅샷**)**을 선택합니다.

단계 **3** Threat & Cloud Analytics Report(위협 및 클라우드 분석 보고서)에서 가져오는 데이터의 드롭다운 목록에서 일별, 주별, 월별, 분기별 또는 연간 **Frequency(**빈도**)**를 선택합니다.

- **Daily(**매일**)** - 오전 12시부터 24시간 동안. 이는 UTC 시간입니다.
- **Weekly(**매주**)** - 월요일부터 일요일까지
- **Monthly(**매월**)** - 일반적으로 월의 시작부터 말일까지
- **Quarterly(**분기별**)** - 분기의 시작부터 끝까지. 일반적으로 분기는 1월 1일~3월 31일, 4월 1일~6월 30일, 7월 1일~9월 30일 및 10월 1일~12월 31일로 정의됩니다.
- **Yearly(**매년**)** - 선택한 연도의 1월 1일부터 12월 31일까지.

단계 **4** 날짜를 선택합니다. **Calendar(**달력**)** 드롭다운을 사용하여 데이터를 수집할 시간 범위 또는 특정 날짜를 선택합니다. 회색으로 표시된 날짜는 컴파일할 데이터가 없는 것입니다. 보고서를 생성하는 데 사용할 수 있는 데이터가 없는 경우 정책에 WAF 및 IDS/IP 규칙이 포함되어 있는지 확인합니다.

단계 **5** **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **6** 보고서가 생성됩니다. 보고서를 로컬로 저장하려면 **Print Report(**보고서 인쇄**)**를 클릭합니다. 로컬 서버의 위치로 이동하여 보고서를 저장합니다.