인시던트

다음 주제에서는 인시던트 처리를 설정하는 방법을 설명합니다.

- 인시던트 처리 정보, 1 페이지
- 인시던트 라이선스 요구 사항, 5 페이지
- 인시더트 요구 사항 및 사전 요건, 5 페이지
- 맞춤형 인시던트 유형 생성, 5 페이지
- 인시던트 생성, 6 페이지
- 인시던트 편집, 6 페이지
- 인시던트 보고서 생성, 7 페이지

인시던트 처리 정보

인시던트 처리란 보안 정책 위반이 의심될 때 조직에서 취하는 대응을 가리킵니다. Firepower System에는 인시던트의 조사와 관련된 정보의 수집 및 처리를 지원하는 기능이 포함되어 있습니다. 이러한 기능을 통해 인시던트와 관련이 있을 수 있는 침입 이벤트와 패킷을 수집할 수 있습니다. 공격의 효과를 완화하기 위해 Firepower System의 외부에서 수행하는 활동에 대한 메모의 저장소로 인시던트를 사용할 수도 있습니다. 예를 들어 감염된 호스트를 네트워크에서 격리하도록 보안 정책에서 요구하는 경우 인시던트에 그 내용을 메모할 수 있습니다.

또한 Firepower System은 인시던트 라이프사이클을 지원하며, 따라서 공격에 대한 대응을 진행할 때 인시던트의 상태를 변경할 수 있습니다. 인시던트를 종료할 때 학습 내용의 결과로서 보안 정책에 대해 변경한 내용을 메모할 수 있습니다.

인시던트의 정의

일반적으로 인시던트는 보안 정책 위반과 관련이 있을 것으로 의심되는 하나 이상의 침입 이벤트로 정의됩니다. 또한 Firepower System에서 이 단어는 인시던트에 대한 응답을 추적하는 데 사용할 수 있는 기능을 말합니다.

일부 침입 이벤트는 네트워크 자산의 가용성, 기밀성 및 무결성에서 다른 이벤트보다 더 중요합니다. 예를 들어 포트 스캔 탐지 기능은 네트워크에서의 포트 스캐닝 활동을 지속적으로 알려줄 수 있습니다. 그러나 보안 정책에서는 포트 스캐닝을 명시적으로 금지하지 않거나 우선순위가 높은 위협으로

간주하지 않을 수 있으며, 따라서 직접적인 조치를 취하기보다는 향후 포렌식 연구를 위해 포트 스캐닝의 로그를 보존하고자 할 수 있습니다.

반면 네트워크 내 호스트가 감염되었으며 DDoS(Distributed Denial-of-Service)에 참여하고 있음을 나타내는 이벤트가 생성되면, 이 활동은 명백한 보안 정책 위반이 될 수 있으므로 해당 이벤트의 조사를 추적하는 데 도움이 되도록 Firepower System에서 인시던트를 생성해야 합니다.

일반 인시던트 처리 프로세스

준비

두 가지 방법으로 인시던트를 준비할 수 있습니다.

- 분명하고 포괄적인 보안 정책과 더불어 이를 적용할 하드웨어 및 소프트웨어 리소스를 지정합니다.
- 확실하게 정의된 인시던트 대응 계획을 세우고, 계획을 구현할 수 있도록 적절하게 팀을 훈련합니다.

인시던트 처리의 중요한 부분은 네트워크의 어떤 부분이 가장 위험한가를 파악하는 것입니다. 그러한 네트워크 세그먼트에 Firepower System 구성 요소를 구축하면 인시던트가 언제 어떻게 발생하는지를 더 잘 인지할 수 있습니다. 또한 각각의 매니지드 디바이스에 대해 침입 정책을 세부적으로 조정하면, 최고의 품질로 이벤트가 생성되도록 보장할 수 있습니다.

탐지 및 알림

인시던트를 탐지하지 못하면 인시던트에 대응할 수 없습니다. 인시던트 처리 프로세스에는 탐지할 수 있는 보안 관련 이벤트의 종류와 탐지에 사용되는 메커니즘(소프트웨어와 하드웨어 모두)을 명시해야 합니다. 또한 보안 정책의 위반을 어디서 탐지할 수 있는지도 명시해야 합니다. 네트워크에 능동적으로 또는 수동적으로 모니터링되지 않는 세그먼트가 포함되어 있으면 그러한 내용도 명시해야 합니다.

네트워크에 구축한 매니지드 디바이스는 각각 설치된 세그먼트에서 트래픽을 분석하여 침입을 탐지하고 이를 설명하는 이벤트를 생성해야 합니다. 매니지드 디바이스 각각에 구축하는 액세스 컨트롤 정책은 탐지할 활동의 종류 및 우선순위 지정 방법을 결정합니다. 인시던트 팀이 수백 개의 인시던트를 엄밀히 조사하지 않아도 되도록 특정 침입 이벤트 유형에 대한 알림 옵션을 설정할 수 있습니다. 특정 레벨의 우선순위, 특정 레벨의 심각도 이벤트가 탐지될 때 자동으로 알림을 전송하도록 지정할 수 있습니다.

조사 및 자격

인시던트 처리 프로세스에는 보안 인시던트가 탐지된 이후 조사를 수행하는 방법을 지정해야 합니다. 일부 조직에서는 팀의 신입이 모든 인시던트를 분류하고 심각도나 우선순위가 낮은 사건을 처리하며, 선임자는 심각도나 우선순위가 높은 인시던트를 처리합니다. 각 팀 멤버가 인시던트의 중요도를 결정하는 기준을 이해할 수 있도록 에스컬레이션 프로세스를 신중하게 정리해두어야 합니다.

에스컬레이션 프로세스의 일부는 탐지된 이벤트가 네트워크 자산의 보안에 어떤 영향을 미칠 수 있는지를 파악하는 것과 연결됩니다. 예를 들어 Microsoft SQL 서버를 실행하는 호스트에 대한 공격은

다른 데이터베이스 서버를 사용하는 조직에서는 우선순위가 높지 않습니다. 마찬가지로 이 공격은 네트워크에서 SQL Server를 사용하는 경우에도 덜 중요하지만, 모든 서버가 패치되었고 공격에 취약하지 않은지를 확인해야 합니다. 그러나 누군가가 최근에 (아마도 테스트 목적으로) 취약한 소프트웨어 버전을 설치했다면, 피상적인 조사에서 제시하는 것보다 문제가 더 클 수 있습니다.

Firepower System은 조사 및 자격 프로세스의 지원에서 특별히 뛰어납니다. 사용자는 고유한 이벤트 분류를 생성한 다음 네트워크 취약성에 가장 적합하게 적용할 수 있습니다. 네트워크의 트래픽이 이벤트를 트리거하면 특수 지표를 통해 해당 이벤트에 대한 우선순위와 자격이 자동으로 지정되어, 어떤 공격이 취약한 것으로 알려진 호스트로 향하는지를 알 수 있습니다.

또한 Firepower System의 인시던트 추적 기능에는 어떤 인시던트가 에스컬레이션되었는지를 표시하기 위해 변경할 수 있는 상태 지표도 포함됩니다.

의사소통

모든 인시던트 처리 프로세스에는 인시던트 처리 팀과 내부 및 외부 담당자 간 인시던트의 커뮤니케이션 방법을 지정해야 합니다. 예를 들면, 관리 개입이 필요한 인시던트 종류 및 해당 레벨을 고려해야 합니다. 외부 조직과의 커뮤니케이션 방법 및 시기에 대해서도 프로세스에 명시해야 합니다. 다음과 같은 변화에 주목하십시오.

- 일부 인시던트의 경우 법 집행 기관에 알려야 합니까?
- 호스트가 원격 사이트에 대한 DDoS(distributed denial of service)에 참여하고 있는 경우 해당 사이트에 알려야 합니까?
- CERT/CC(CERT Coordination Center) 또는 FIRST 등의 조직과 정보를 공유하고자 합니까?

Firepower System에는 타인과 손쉽게 공유할 수 있도록 침입 데이터를 HTML, PDF, CSV(comma-separated values) 등의 표준 형식으로 수집할 수 있는 기능이 있습니다.

예를 들어 CERT/CC는 웹사이트의 보안 인시던트에 대한 표준 정보를 수집합니다. CERT/CC는 Firepower System에서 손쉽게 추출할 수 있는 다음과 같은 유형의 정보를 찾습니다.

- 영향을 받는 시스템에 대한 다음과 같은 정보:
  - 호스트 이름 및 IP
  - 표준 시간대
  - 호스트의 목적 또는 기능
- 공격 소스에 대한 다음과 같은 정보:
  - 호스트 이름 및 IP
  - 표준 시간대
  - 공격자와 접촉이 있었는지 여부
  - 인시던트 처리 예상 비용
- 인시던트에 대한 다음과 같은 설명:

- 날짜
- 침입 방법
- 관련 된 침입자 도구
- 소프트웨어 버전 및 패치 레벨
- 침입자 툴 출력
- 악용된 취약성 상세정보
- 공격의 소스
- 기타 관련 정보

인시던트의 코멘트 섹션을 사용하여 문제에 대해 누구와 언제 커뮤니케이션했는지를 기록할 수 있습니다.

봉쇄 및 복구

인시던트 처리 프로세스에는 호스트 또는 다른 네트워크 구성 요소가 손상될 때 어떤 단계를 따라야 하는지를 분명히 명시해야 합니다. 봉쇄 및 복구 옵션의 범위는 취약한 호스트에 패치를 적용하는 것부터 대상을 종료하고 네트워크에서 제거하는 것까지 다양합니다. 또한 공격의 본질과 심각도에 따라, 형사 고발로 이어질 경우에 대비하여 증거 보존의 중요도를 고려해야 합니다.

인시던트의 봉쇄 및 복구 단계 중에 취한 작업의 레코드를 유지 관리하려면 Firepower System의 인시던트 기능을 사용할 수 있습니다.

습득한 교훈

성공적인 공격이든 아니든, 각 보안 인시던트는 보안 정책을 검토할 수 있는 기회입니다. 방화벽 규칙을 업데이트해야 합니까? 패치 관리에 대해 좀 더 구조적인 접근 방식이 필요합니까? 무단 무선 액세스 포인트가 새로운 보안 문제입니까? 각각의 습득한 교훈을 보안 정책에 반영하여 다음 인시던트에 더 잘 대비해야 합니다.

Firepower System의 인시던트 유형

생성하는 각 인시던트에 인시던트 유형을 할당할 수 있습니다. Firepower System에서는 기본적으로 다음 유형을 지원합니다.

- 침입
- Denial of Service(서비스 거부)
- 무단 관리자 액세스
- 웹사이트 파손
- 시스템 무결성 손상
- 사기

- 도난
- 손상
- 알 수 없음

자체 인시던트 유형을 생성할 수도 있습니다.

인시던트 라이선스 요구 사항

FTD 라이센스

위협

기본 라이선스

보호

인시더트 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 침입 관리자

맞춤형 인시던트 유형 생성

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** **Create Incident(**인시던트 생성**)**를 클릭합니다.

단계 **3** **Type(**유형**)** 영역에서 **Types(**유형**)**를 클릭합니다.

기본 인시던트 유형이 페이지 하단에 나열됩니다.

단계 **4** **Incident Type Name(**인시던트 유형 이름**)** 필드에 새 인시던트 유형의 이름을 입력합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

다음에 인시던트를 생성하거나 수정할 때 새 인시던트 유형을 사용할 수 있습니다.

인시던트 생성

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 인시던트만 보고 수정할 수 있습니다. 상위 도메인의 경우에는 모든 하위 도메인의 인시던트에 이벤트를 추가할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** **Create Incident(**인시던트 생성**)**를 클릭합니다.

단계 **3** **Type(**유형**)** 드롭다운 메뉴에서 인시던트를 가장 잘 설명하는 옵션을 선택합니다.

단계 **4** 인시던트에 사용한 시간을 #d #h #m #s 형식으로 **Time Spent(**사용한 시간**)** 필드에 입력합니다. #은 일수, 시간, 분 또는 초를 나타냅니다.

단계 **5** 인시던트에 대한 짧은 설명을 **Summary(**요약**)** 텍스트 상자에 입력합니다(최대 255자의 영숫자 문자, 공백 및 기호).

단계 **6** 인시던트에 대한 좀 더 완전한 설명을 **Add Comment(**코멘트 추가**)** 텍스트 상자에 입력합니다(최대 8,191자의 영숫자 문자, 공백 및 기호).

단계 **7** 인시턴트에 이벤트 추가:

- 선택한 이벤트를 추가하려면 클립보디에서 이벤트를 선택하고 **Add to Incident(**인시던트에 추가**)**를 클릭합니다.
- 클립보드의 이벤트를 모두 추가하려면 **Add All to Incident(**모두 인시던트에 추가**)**를 클릭합니다.

참고 둘 이상의 클립보드 페이지에서 개별 이벤트를 추가하려는 경우, 먼저 한 페이지의 이벤트를 추가한 후 다른 페이지의 이벤트를 별도로 추가해야 합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

인시던트 편집

다중 도메인 구축의 경우에는 현재 도메인에서 생성된 인시던트만 보고 수정할 수 있습니다. 상위 도메인의 경우에는 모든 하위 도메인의 인시던트에 이벤트를 추가할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** 편집할 인시던트 옆에 있는 수정( )을 클릭합니다.

단계 **3** 인시던트의 다음과 같은 부분을 수정할 수 있습니다.

- 상태 변경
- 유형 변경
- 클립보드에서 이벤트 추가
- 이벤트 삭제

단계 **4** 인시던트에 사용한 추가 시간을 **Time Spent(**사용한 시간**)** 필드에 입력합니다.

단계 **5** 인시던트에 대한 변경 사항의 설명을 **Add Comment(**코멘트 추가**)** 텍스트 상자에 입력합니다(최대 8,191자의 영숫자 문자, 공백 및 기호).

단계 **6** 선택적으로, 인시던트에서 이벤트를 추가 또는 삭제할 수 있습니다.

- 클립보드의 이벤트를 추가하려면 클립보드에서 원하는 이벤트를 선택하고 **Add to Incident(**인시던트에 추가**)**를 클릭합니다.
- 클립보드의 이벤트를 모두 추가하려면 **Add All to Incident(**모두 인시던트에 추가**)**를 클릭합니다.
- 인시던트에서 특정 이벤트를 삭제하려면 이벤트를 선택하고 **Delete(**삭제**)**를 클릭합니다.
- 인시던트에서 모든 이벤트를 삭제하려면 **Delete All(**모두 삭제**)**을 클릭합니다.
- 이벤트를 추가 또는 삭제하지 않고 인시던트를 업데이트하려면 **Save(**저장**)**를 클릭합니다.

인시던트 보고서 생성

Firepower System을 사용하여 인시던트 보고서를 생성할 수 있습니다. 이러한 보고서는 인시던트에 추가한 이벤트의 정보와 함께 인시던트 요약, 인시던트 상태 및 코멘트를 포함할 수 있습니다. 또한 보고서에 이벤트 요약 정보를 포함할지 여부를 지정할 수 있습니다.

프로시저

단계 **1** **Analysis(**분석**)** > **Intrusions(**침입**)** > **Incidents(**사고**)**을(를) 선택합니다.

단계 **2** 보고서에 포함할 인시던트 옆에 있는 수정( )을 클릭합니다.

단계 **3** 다음 2가지 옵션을 사용할 수 있습니다.

- 인시던트의 모든 이벤트를 보고서에 포함하려면 **Generate Report All(**모든 보고서 생성**)**을 클릭합니다.

- 인시던트의 특정 이벤트를 보고서에 포함하려면 원하는 이벤트 옆의 확인란을 선택하고 **Generate Report(**보고서 생성**)**를 클릭합니다.

단계 **4** 보고서의 이름을 입력합니다.

단계 **5** **Incident Report Sections(**인시던드 보고서 섹션**)**에서, 보고서에 포함할 인시던트의 부분에 대한 확인란(**status**, **summary**, 및 **comments**)을 선택합니다.

단계 **6** 보고서에 이벤트 정보를 포함하려면 사용하려는 워크플로를 선택하고, **Report Sections(**보고서 섹션**)**에서 이벤트 요약 정보의 포함 여부를 지정합니다.

단계 **7** 보고서에 포함할 워크플로 페이지 옆에 있는 확인란을 선택합니다.

단계 **8** 보고서에 대해 사용할 출력 형식(**PDF**, **HTML** 및 **CSV**) 옆에 있는 확인란을 선택합니다.

참고 CSV 기반 인시던트 보고서에는 이벤트 정보만 포함됩니다. 인시던트의 상태, 요약 또는 코멘트는 포함되지 않습니다.

단계 **9** **Generate Report(**보고서 생성**)**를 클릭하고 보고서 프로파일 업데이트를 확인합니다.