실행 파일이 있는 포함된 하이퍼링크를 캡처하고 차단하려면 어떻게 해야 합니까?

목차

질문

실행 파일이 있는 포함된 하이퍼링크를 캡처하고 차단하려면 어떻게 해야 합니까?

응답

메시지 필터를 사용하여 본문 및 HTML 첨부 파일을 스캔할 수 있습니다.일반적으로 이러한 이메일은 HTML 이메일을 통해 전송됩니다. 검사 엔진이 이를 탐지하려면 body-contains 조건을 사용해야 합니다.아웃바운드 메일만 처리하는 경우 'only-body-contains' 조건을 사용할 수 있습니다.

다음 메시지 필터는 실행 파일로 끝나는 모든 길이 하이퍼링크를 찾습니다.조건이 충족되면 두 가지 작업이 활성화됩니다.첫 번째 작업은 admin@example.com으로 이메일을 보내 로컬 관리자에게 알리는 것입니다.

두 번째 작업은 이메일을 삭제하는 마지막 작업입니다.이메일을 삭제할 필요는 없지만 대신 격리할 수 있습니다. 'drop();'아래의 작업 제거하는 것은 '`quarantine('Policy');`' 바꿀 수 .

격리를 정의해야 합니다. 그렇지 않으면 필터 엔진이 필터를 허용하지 않습니다.기본 정책 격리를 사용하거나 고유한 격리를 생성할 수 있습니다(격리를 생성하거나 삭제하려면 매뉴얼의 격리를 참조하십시오).

```
Block_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
notify ("admin@example.com");
drop();
}
```

또한 본문으로부터 잘못된 URL을 제거하고 URL REMOVED로 대체한 이 버전을 사용할 수 있습니다.

```
remove_exe_urls: if body-contains("://\\S*\\.exe(\\s|\\b|$)")
{
```

```
edit-body-text("://\\S*\\.exe(\\s|\\b|$)", "URL REMOVED");
}
```

메시지 필터를 입력하는 방법에 대한 자세한 지침은 Cisco IronPort Appliance에 새 메시지 필터를 추가하려면 어떻게 합니까?를 검토하십시오.

메시지 필터를 검토하려면 Policy enforcement(정책 시행)라는 Email Security Appliances용 Cisco ESA AsyncOS ADVANCED USER GUIDE(고급 사용 설명서) 섹션을 참조하십시오.