보안 이벤트 및 알람 카테고리

(Stealthwatch System v6.9.0용)

저작권 및 상표

NOTICE

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이센스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이센스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 공개 도메인 버전의 일부로서 UCB(University of Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 보증을 포함하여(단, 이에 제한되지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화번호는 실제 주소와 전화번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

모든 인쇄 사본 및 소프트 카피 복제본은 비통제 사본으로 간주되며 원본 온라인 버전을 최신 버전으로 참조해야 합니다.

Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다. 각 지사의 주소, 전화번호 및 팩스 번호는 Cisco 웹 사이트 www.cisco.com/go/offices에서 확인하십시오.

목차

1

소개

개요

이 문서에서는 SMC(Stealthwatch Management Console)를 사용하여 확인할 수 있는 보안 이벤트 및 알람 카테고리에 대한 설명 목록을 제공합니다.

대상

이 문서는 네트워크를 관리 및 보호하기 위해 SMC를 사용하는 네트워크 관리자와 보안 담당자용 참조 문서로 활용하기 위해 작성되었습니다.

관련 정보

이 정보는 *SMC 클라이언트 온라인 도움말*의 다음 항목에서도 확인할 수 있습니다.

- 보안 이벤트 목록
- 알람 카테고리 정보

약어

이 문서에서는 다음 용어 및 약어를 사용합니다.

약어	용어
ASA	Adaptive Security Appliance
CI	Concern Index(관심 지표)
DNS	Domain Name System(서비스 또는 서버)
DoS	Denial of Service(서비스 거부)

약어	용어
dvPort	Distributed Virtual Port(분산된 가상 포트)
ESX	Enterprise Server X(엔터프라이즈 서버 X)
FSI	File Sharing Index(파일 공유 지수)
FTP	File Transfer Protocol(파일 전송 프로토콜)
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System(침입 탐지 시스템)
IP	Internet Protocol(인터넷 프로토콜)
IRC	Internet Relay Chat
ISE	Identity Services Engine
MAC	Media Access Control(미디어 액세스 제어)
NAT	Network Address Translation(네트워크 주소 변환)
NTP	Network Time Protocol
OS	Operating System(운영 체제)
OVF	Open Virtualization Format
RAID	Redundant Array of Independent Discs
SMC	Stealthwatch Management Console
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol(전송 제어 프로토콜)
TI	Target Index(대상 지표)
UDP	User Datagram Protocol(사용자 데이터그램 프로토콜)
VDS	Virtual Network Distributed Switch(가상 네트워크 분산형 스위치)
VE	Virtual Edition(가상 버전)
VLAN	Virtual Local Area Network(가상 LAN)
VM	Virtual Machine(가상 머신)
VPN	Virtual Private Network(가상 프라이빗 네트워크)

2

보안 이벤트 목록

보안 이벤트는 지표 포인트를 알람에 할당하는 메커니즘입니다. 보안 이벤트를 비활성화하면 지표 포인트가 연결된 알람을 대상으로 누적되지 않습니다.

보안 이벤트는 특정 알람 카테고리의 지표 포인트에 영향을 줍니다. 알람 카테고리 및 보안 이벤트는 정책에 적용된 설정에 따라 알람을 트리거할 수 있습니다. 자세한 내용은 SMC 클라이언트 인터페이스 온라인 도움말 항목인 *Add/Edit Role Policy(역할 정책 추가/편집)*를 참조하십시오.

보안 이벤트는 특정 서비스를 대상으로 비활성화될 수 있으며 호스트 그룹 수준에서도 비활성화될 수 있습니다. 자세한 내용은 SMC 클라이언트 인터페이스에 있는 호스트 그룹 속성 및 온라인 도움말을 참조하십시오.

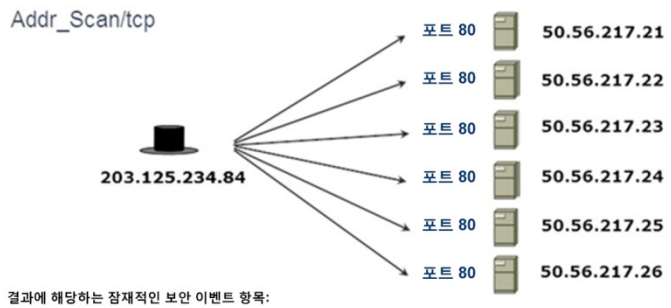
> **참고:** 현재 보안 이벤트 정보를 업데이트 및 확장하는 중입니다. 새로운 형식은 이벤트 설명, 이벤트 트리거 시 새로운 형식의 의미, 추가로 훨씬 더 조사하기 위해 취해야 할 조치와 같은 정보(여러 테이블에 표시됨) 등을 포함합니다. 이 전환이 이루어지는 동안 이 항목의 일부 보안 이벤트는 추가 정보로 보완되고 새로운 형식으로 변환될 때까지 원래 형식으로 유지됩니다.

보안 이벤트에 대한 내용은 다음을 참조하십시오.

** Stealthwatch Flow Collector for NetFlow는 Stealthwatch FlowSensor와 결합하여 사용되는 경우에만 이러한 보안 이벤트를 지원합니다.

Addr_Scan/tcp

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Addr_Scan/tcp-80(6)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	Stealthwatch System은 누군가가 TCP를 사용해 네트워크 스캔을 수행 중임을 나타낼 수 있는 활동을 탐지하면 해당 활동을 스캔 이벤트로 기록합니다. 스캔 이벤트가 많이 발생하여 많은 수의 호스트에 영향을 주는 경우 SMC에서 보안 이벤트를 발생시킵니다. '스캔 이벤트'의 예로는 잘못된 TCP 플래그의 다양한 조합, SYN을 전송해도 다음 SYN-ACK에 응답하지 않는 현상, 그리고 기타 지표가 포함됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	호스트가 이용 가능성이 있는 특정 서비스를 실행 중인 호스트 검색을 시도하고 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	호스트가 스캔 중이었던 항목을 확인하십시오. 처음에는 네트워크를 광범위하게 조사하고 그 후에 범위를 좁히십시오. 먼저 Top Ports(상위 포트)(아웃바운드) 보고서를 실행합니다. 이벤트 날짜까지의 기간과 이벤트의 소스 IP로 사용할 클라이언트 호스트를 설정합니다. 나열되는 대상 IP 범위와 관계없이 모든 유형의 호스트를 스캔할 수 있으므로 내부 호스트나 외부 호스트 중 하나를 검색할지 아니면 둘 다 검색할지를 결정합니다. 그런 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Server(서버) 필터를 적절하게 설정하고 Advanced(고급) 탭에서 'Order the records returned by'(반환되는 기록 순서 지정 기준)를 *Flows(플로우)*로 설정합니다. 결과가 반환된 후에는 Peers(피어)를 기준으로 정렬하면 도움이 될 수 있습니다. Flows(플로우) 또는 Peers(피어)를 기준으로 정렬한 목록 맨 위에서부터 시작하여 해당 범위에 속하지 않거나 숫자가 비정상적으로 높은 포트를 찾습니다. 원하는 IP 주소를 마우스 오른쪽 버튼으로 클릭하면 플로우로 피벗해 다양한 IP 주소를 확인하고 특정 호스트 그룹이 기본 대상으로 지정된 그룹인지를 확인할 수 있습니다. 또한, 마우스 오른쪽 버튼을 클릭하여 Top Peers(상위 피어) 보고서로 피벗한 다음 대상 전체에 걸쳐 트래픽이 전반적으로 동일하게 분산되는지를 확인할 수도 있습니다. 스캔에 응답한 호스트의 백분율을 확인하는 것도 도움이 됩니다. 이 시점이 되면 호스트가 스캔 중이었던 대상과 스캔 대상이었던 포트를 확인할 수 있습니다.

이 이벤트에 대한 질문	응답
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	FlowSensor가 전송한 플래그 또는 방화벽에서 전송한 플래그에 따라서만 기록되는 스캔도 있습니다. (이러한 스캔의 경우 이벤트 세부사항에 참고 사항이 표시됩니다.) 이러한 참고 사항이 없는 스캔 이벤트의 경우 특정 데이터가 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	소스 호스트에서 이벤트를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음

이벤트에 대한 질문	응답
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	disable_stealth_probe lc_threshold.txt 값을 사용하여 특정 은폐형 스캔 탐지 사례를 비활성화할 수 있습니다.
이벤트에 기본 완화 기능이 있습니까?	아니요
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	스캔일 수 있는 활동을 수행하는 호스트
대상은 무엇입니까?	소스 호스트가 스캔 중인 호스트.
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

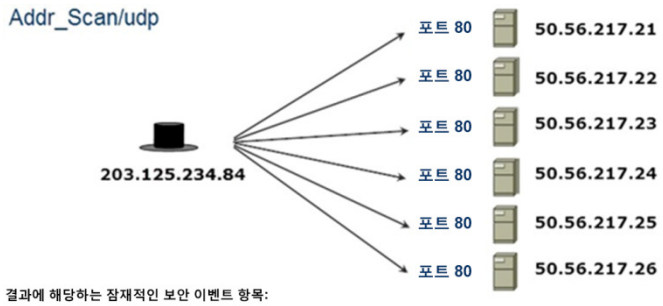
이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	웹 애플리케이션 인터페이스: View details(세부사항 보기) SMC 클라이언트 인터페이스: 해당 없음
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	웹 애플리케이션 인터페이스: addr_scan_tcp를 보여주는 보안 이벤트 세부사항 페이지가 표시됩니다. SMC 클라이언트 인터페이스: 해당 없음
연결된 플로우에 어떤 정보가 표시됩니까?	웹 애플리케이션 인터페이스: 해당 없음 연결된 플로우에 다음을 기준으로 필터링된 플로우 테이블이 표시됨: 마지막 5분

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TCP_ADDR_SCAN (276)
이벤트의 syslog 유형은 무엇입니까?	HostAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Addr_Scan/udp

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Addr_Scan/udp-80(6)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	Stealthwatch System은 누군가가 UDP를 사용해 네트워크 스캔을 수행 중임을 나타낼 수 있는 활동을 탐지하면 해당 활동을 스캔 이벤트로 기록합니다. 스캔 이벤트가 많이 발생하여 많은 수의 호스트에 영향을 주는 경우 SMC에서 보안 이벤트를 발생시킵니다. '스캔 이벤트'의 예로는 UDP 패킷 전송 시 여러 유형의 ICMP 거부 응답이 수신되거나 방화벽 플로우 거부 메시지가 수신되는 등의 여러 지표가 있습니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	호스트가 이용 가능성이 있는 특정 서비스를 실행 중인 호스트 검색을 시도하고 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	호스트가 스캔 중이었던 항목을 확인하십시오. 처음에는 네트워크를 광범위하게 조사하고 그 후에 범위를 좁히십시오. 먼저 Top Ports(상위 포트)(아웃바운드) 보고서를 실행합니다. 이벤트 날짜까지의 기간과 이벤트의 소스 IP로 사용할 클라이언트 호스트를 설정합니다. 나열되는 대상 IP 범위와 관계없이 모든 유형의 호스트를 스캔할 수 있으므로 내부 호스트나 외부 호스트 중 하나를 검색할지 아니면 둘 다 검색할지를 결정합니다. 그런 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Server(서버) 필터를 적절하게 설정하고 Advanced(고급) 탭에서 'Order the records returned by'(반환되는 기록 순서 지정 기준)를 *Flows(플로우)*로 설정합니다. 결과가 반환된 후에는 Peers(피어)를 기준으로 정렬하면 도움이 될 수 있습니다. Flows(플로우) 또는 Peers(피어)를 기준으로 정렬한 목록 맨 위에서부터 시작하여 해당 범위에 속하지 않거나 숫자가 비정상적으로 높은 포트를 찾습니다. 원하는 IP 주소를 마우스 오른쪽 버튼으로 클릭하면 플로우로 피벗해 다양한 IP 주소를 확인하고 특정 호스트 그룹이 기본 대상으로 지정된 그룹인지를 확인할 수 있습니다. 또한, 마우스 오른쪽 버튼을 클릭하여 Top Peers(상위 피어) 보고서로 피벗한 다음 대상 전체에 걸쳐 트래픽이 전반적으로 동일하게 분산되는지를 확인할 수도 있습니다. 스캔에 응답한 호스트의 백분율을 확인하는 것도 도움이 됩니다. 이 시점이 되면 호스트가 스캔 중이었던 대상과 스캔 대상이었던 포트를 확인할 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	FlowSensor가 전송한 플래그 또는 방화벽에서 전송한 플래그에 따라서만 기록되는 스캔도 있습니다. (이러한 스캔의 경우 이벤트 세부사항에 참고 사항이 표시됩니다.) 이러한 참고 사항이 없는 스캔 이벤트의 경우 특정 데이터가 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	소스 호스트에서 이벤트를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, DHCP 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, DHCP 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	해당 없음
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	disable_stealth_probe lc_ threshold.txt 값을 사용하여 특정 은폐형 스캔 탐지 사례를 비활성화할 수 있습니다.

이벤트에 대한 질문	응답
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	스캔일 수 있는 활동을 수행하는 호스트
대상은 무엇입니까?	소스 호스트가 스캔 중인 호스트.
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	웹 애플리케이션 인터페이스: View details(세부사항 보기) SMC 클라이언트 인터페이스: 해당 없음
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	웹 애플리케이션 인터페이스: addr_scan_udp를 보여주는 보안 이벤트 세부사항 페이지가 표시됩니다. SMC 클라이언트 인터페이스: 해당 없음

이벤트에 대한 질문	응답
연결된 플로우에 어떤 정보가 표시됩니까?	웹 애플리케이션 인터페이스: 해당 없음 연결된 플로우에 다음을 기준으로 필터링된 플로우 테이블이 표시됨: 마지막 5분

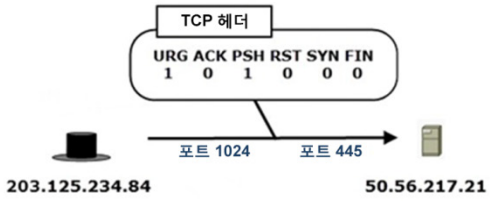
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_ADDR_SCAN (286)
이벤트의 syslog 유형은 무엇입니까?	HostAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_ACK**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_ACK



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_ACK-445(1)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	TCP 승인 플래그를 포함하지 않으며 재설정 또는 동기화 이외의 플래그만 포함하는 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_ACK를 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

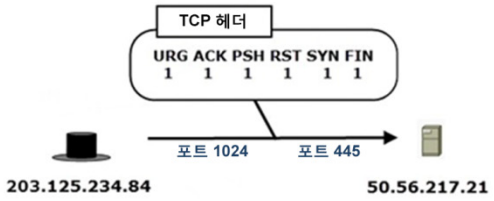
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_NO_ACK (267)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_All**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_All



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_All-445(1)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	모든 TCP 플래그(동기화, 승인, 재설정, 푸시, 긴급, 마침)가 포함된 패킷이 관찰되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 모든 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_All을 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	해당 없음
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	내부 호스트, 외부 호스트

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	해당 없음
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

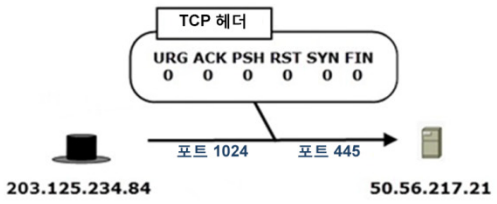
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_XMAS (263)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_NoFlg**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_NoFlg



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_NoFlg-445(1)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	TCP 플래그가 포함되지 않은 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_NoFlg를 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

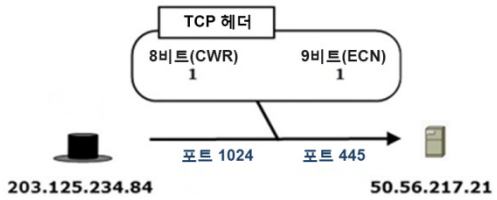
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_NOFLAG (269)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_Rsrvd

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_Rsrvd



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_Rsrvd-445(1)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	초기 TCP 표준에서 예약된 TCP 플래그를 포함하는 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전에서는 이 이벤트가 트리거되지 않습니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_Rsrvd를 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

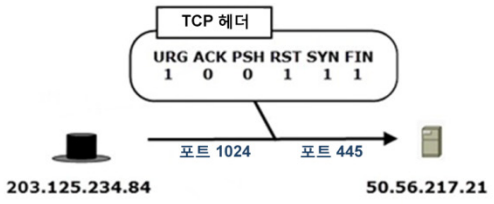
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_RESERVED (265)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_RST**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_RST



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_RST-445(1)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	푸시 또는 승인 이외의 다른 플래그와 TCP 재설정 플래그가 포함된 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_RST를 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

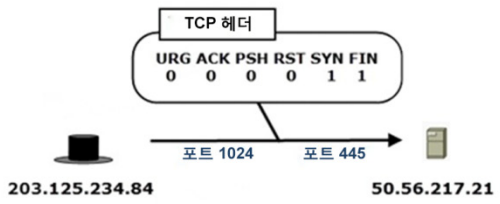
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_BAD_RST (266)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_SYN_FIN**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_SYN_FIN



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_SYN_FIN-445(1)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	TCP 동기화 및 마침 플래그가 포함된 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_SYN_FIN을 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

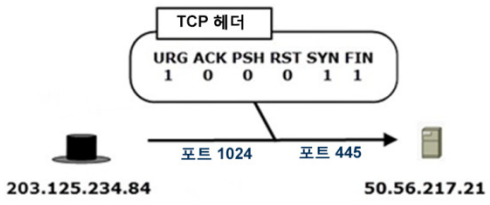
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_SYN_FIN (264)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bad_Flag_URG**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Bad_Flag_URG



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Bad_Flag_URG-445(1)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	승인 이외의 다른 플래그와 TCP 긴급 플래그가 포함된 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 잘못된 플래그가 설정된 TCP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 시스템 컨피그레이션마다 여러 비정상적 플래그 조합에 대해 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 플래그 조합을 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Bad_Flag_URG를 활성화합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스의 호스트 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BAD_FLAG_URG (268)

이벤트에 대한 질문	응답
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

비콘 호스트

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	비콘 호스트는 다른 호스트에서 명령이나 업데이트를 찾습니다. 이 트래픽은 Keepalive(하트비트), C&C(command and control) 서버에서 새 명령 받기, 업데이트 다운로드 등의 여러 가지 이유로 사용될 수 있습니다. 참고로, 악성코드도 이러한 행동을 유발할 수 있습니다.
다음 단계는 무엇입니까?	목표는 외부 호스트가 실제로 C&C 서버인지 확인하는 것입니다. 이 호스트를 Stealthwatch System 내부 및 외부 모두에서 조사하는 것이 유용할 수 있습니다. 올바른 첫 번째 단계는 Stealthwatch System 내의 대상 호스트에서 Top Peers(상위 피어)(아웃바운드) 보고서를 여는 것입니다. 이 보고서는 외부 호스트와 통신한 내부 피어의 목록을 데이터의 양을 기준으로 정렬하여 제공합니다. 이 목록을 활용하여 호스트가 사용자 환경 내에서 일반적인 피어인지 확인할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BEACONING_HOST (39)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

봇 C&C(Command & Control) 서버

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	사용자 환경 내 호스트가 C&C(Command & Control) 서버 역할을 함으로써 환경 외부에 있는 다른 호스트의 보안 침해를 지원하는 데 사용되고 있음을 의미합니다. 이 호스트 자체도 보안이 침해되었을 가능성이 높습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command & Control) 지표, 상위 관심 지표
값은 무엇입니까?	• 상위 C&C(Command & Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_COMMAND_AND_CONTROL_HOST (43)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

봇에 감염된 호스트 - C&C 활동 시도됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	네트워크의 호스트가 알려진 C&C(command and control) 서버와 통신하려고 시도했습니다. 호스트가 통신에 성공하지 못했지만 호스트가 시도하도록 유발하는 원인이 있기 때문에 여전히 걱정스러운 상황입니다. 참고로, 악성코드 또는 악의적인 리디렉션도 이러한 행동을 유발할 수 있습니다.
다음 단계는 무엇입니까?	이 보안 이벤트는 일반적으로 제품 내에서 지나치게 많은 검증을 필요로 하지 않습니다. 단, 기타 호스트가 의심스러운 C&C 서버와 상호 작용하는지 확인하기 위해 이벤트의 대상과 다른 모든 호스트 간의 플로우에 대해 플로우 쿼리를 수행해야 합니다. 쿼리 기간은 이벤트 날짜로 설정하거나 더 길게 설정합니다. 통신 기간에 따라서는 이 쿼리를 사용하여 소스 호스트가 의심스러운 C&C 서버에 대한 연결을 시작한 시기도 확인할 수 있습니다. 대상 호스트와 통신하는 많은 수의 호스트를 보유한 경우 또는 통신 내역을 확인하는 경우, C&C 서버가 잘못 식별되었을 가능성이 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	'전체' 정책: 상위 C&C(command and control) 지표, 상위 관심 지표(CI) *'부분' 정책: 상위 C&C(command and control) 지표, 상위 관심 지표(CI)*
값은 무엇입니까?	'전체' 정책: • 상위 C&C(command and control) 지표: 참 • CI: 참 '부분' 정책: • 상위 C&C(command and control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	'전체' 정책: 상위 대상 지표(TI) *'부분' 정책: 상위 대상 지표(TI)*
값은 무엇입니까?	'전체' 정책: • TI: 참 '부분' 정책: • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BOT_INFECTED_HOST (41)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

봇에 감염된 호스트 - C&C 활동 성공

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	네트워크의 호스트가 알려진 C&C(command and control) 서버와 통신했습니다. 이 행동은 악성코드 또는 악의적인 리디렉션으로 인해 발생했을 수 있습니다. 또는 이러한 통신은 익스플로잇 킷과 같은 공격으로 감염되었을 때 시도된 것입니다. 이러한 현상은 호스트의 보안이 침해되었다는 거의 확실한 징후입니다.
다음 단계는 무엇입니까?	이 보안 이벤트는 일반적으로 제품 내에서 지나치게 많은 검증을 필요로 하지 않습니다. 단, 기타 호스트가 의심스러운 C&C 서버와 상호 작용하는지 확인하기 위해 이벤트의 대상과 다른 모든 호스트 간의 플로우에 대해 플로우 쿼리를 수행해야 합니다. 쿼리 기간은 이벤트 날짜로 설정하거나 더 길게 설정합니다. 통신 기간에 따라서는 이 쿼리를 사용하여 소스 호스트가 의심스러운 C&C 서버에 대한 연결을 시작한 시기도 확인할 수 있습니다. 대상 호스트와 통신하는 많은 수의 호스트를 보유한 경우 또는 통신 내역을 확인하는 경우, C&C 서버가 잘못 식별되었을 가능성이 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	'전체' 정책: 상위 C&C(Command And Control) 지표, 상위 관심 지표(CI) *'부분' 정책: 상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)*
값은 무엇입니까?	'전체' 정책: • 상위 C&C(Command And Control) 지표: 참 • CI: 참 '부분' 정책: • 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	'전체' 정책: 상위 대상 지표(TI) *'부분' 정책: 상위 대상 지표(TI)*
값은 무엇입니까?	'전체' 정책: • TI: 참 '부분' 정책: • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BOT_INFECTED_HOST_CONTROLLED (42)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

무차별 대입 로그인

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이러한 현상은 호스트가 시스템 액세스 권한을 획득하기 위해 다른 호스트의 로그인 크리덴셜을 추측하려는 시도를 나타내는 것일 수 있습니다. 또한, 서버 연결을 여러 번 반복 시도하는데 인증이 실패하는 클라이언트의 잘못 구성된 애플리케이션을 나타내는 것일 수도 있습니다.
다음 단계는 무엇입니까?	목표는 서버에 대한 연결 시도가 정상적인지 확인하는 것입니다. 클라이언트가 외부 호스트인 경우 클라이언트 주소가 이러한 연결을 시작하는 데 사용될 수 있는, 알려지고 신뢰할 수 있는 비즈니스 파트너 네트워크의 일부분인지를 확인합니다. 이에 해당하는 경우, 애플리케이션이 잘못 구성되었을 수 있습니다. 또한, 대상 호스트의 DShield에 대해 외부 조회를 실행하여 보안 이벤트 알람의 대상 IP 소유자를 확인해야 합니다. 클라이언트가 내부 호스트인 경우에는 해당 호스트가 연결 대상 서버에 대해 이러한 유형의 연결을 시도하는 것이 정상적인 행동인지를 확인합니다. 소스 호스트에 대해 Top Peers(상위 피어) 보고서를 실행하면 해당 호스트가 유사한 바이트 수 또는 많은 양의 플로우를 사용하여 네트워크의 다른 호스트에 연결하는지를 확인할 수 있습니다. 또한, Top Ports(상위 포트) 보고서를 실행하여 소스 IP가 트리거된 보안 이벤트 알람(SSH일 수 있음)에 대해 동일한 포트를 통해 연결하고 있는 기타 호스트를 찾을 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BRUTE_FORCE_LOGIN (58)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bogon 주소에서 연결 시도됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Bogon 주소는 할당되지 않은 IP 주소로, 사용해서는 안 됩니다. Bogon 주소에서 시작되는 단방향 통신은 대개 큰 문제가 되지는 않지만, 정상적인 사용 중에는 수행되지 않아야 합니다. 실제로 이러한 종류의 트래픽은 네트워크 경계에서 차단되는 경우가 많습니다. 이러한 트래픽이 대량으로 나타날 때 찾아보아야 하는 구체적인 행동 유형은 공격자가 소스 IP 주소를 스푸핑하는 DoS(denial-of-service) 공격입니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	Bogon 주소로부터의 단방향 트래픽을 조사할 때 먼저 두 가지 사항, 즉 1) 해당 Bogon 주소나 다른 Bogon 주소가 네트워크의 다른 호스트와 통신을 시도하는지, 2) Bogon 주소에서 전송 중인 트래픽의 대상 호스트가 비정상적으로 많은 양의 트래픽을 수신하고 있는지 살펴봐야 합니다. 첫 번째 사항을 확인하려는 경우 Bogon 호스트 그룹에 대해 Top Hosts(상위 호스트) 쿼리나 플로우 쿼리를 실행하면 됩니다. 보안 이벤트에서 Bogon IP만을 대상으로 하여 해당 쿼리를 실행할 수도 있지만, 스푸핑된 트래픽의 경우에는 공격자가 각기 다른 여러 Bogon IP를 사용하는 경우가 많습니다. 이것이 DoS 공격의 일부인지 또는 네트워크에서 잠재적으로 잘못된 컨피그레이션/분류되지 않은 호스트인지 확인하려면 쿼리에서 반환된 결과를 평가합니다. 일반적으로, 많은 양의 데이터 또는 패킷은 DoS 공격의 표시입니다. 두 번째 사항을 확인하려는 경우에는 보안 이벤트의 대상 호스트에 대한 쿼리를 중점적으로 확인해야 합니다. 트래픽을 전송하는 Bogon 주소와 관계없이 트래픽의 양이 비정상적으로 많은지만 확인하면 되기 때문입니다. 유용한 정보를 얻기 위한 빠른 방법은 대상 호스트의 다른 보안 이벤트를 확인하고 SYNs Received(SYN 수신됨) 또는 New Flows Served(새 플로우 제공됨)와 같은 DoS 이벤트를 찾거나 Bogon과의 통신이 많이 수행되었는지 살펴봅니다. 더욱 철저하게 조사하려면 Flow Traffic(플로우 트래픽) 보고서를 실행합니다. Bogon 통신 시간과 이 시간보다 2시간 전의 시간을 포함하도록 Date/Time(날짜/시간) 필터를 설정합니다. 기간을 길게 설정할수록 쿼리는 길어지지만 더욱 자세한 상황 정보가 제공됩니다. 내부에서 시작된 DoS 공격은 확인하지 않아도 되는 경우 여기서 Hosts(호스트)를 필터링하여 외부 호스트의 트래픽만 포함할 수도 있습니다. 트래픽이 급격하게 증가하거나, 서서히 증가하더라도 전체 트래픽 양이 많은 것은 DoS 공격을 나타내는 현상일 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 관심 지표(CI)
값은 무엇입니까?	• CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 이상 징후 지표: 참 • 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_CONN_FROM_BOGON_ATTEMPTED (519)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bogon 주소에서 연결 성공

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Bogon 주소는 할당되지 않은 IP 주소로, 사용해서는 안 됩니다. Bogon 주소와의 양방향 통신은 발생하지 않아야 합니다. 이러한 행동은 사용자의 네트워크 또는 Stealthwatch 구축 내의 컨피그레이션이 잘못되었다는 징후일 가능성이 높습니다.
다음 단계는 무엇입니까?	사용자 환경에서 실제로 특정 Bogon IP 주소 범위를 내부적으로 사용하는지 또는 캐리어급 NAT를 사용하는지 확인합니다. 사용자 환경에서 Bogon 범위를 내부적으로 사용하며 이러한 사용 방식이 정상적인 상태라면 내부 호스트 그룹에 해당 범위만 추가하면 됩니다. Stealtwatch System 내에서 이를 확인하는 방법은 Bogon의 /24에서 활성화된 플로우를 찾아보는 것입니다. 해당 범위의 대부분이 활성화된 상태이면 사용자 환경 내에서 해당 범위가 특정 목적을 위해 사용되고 있을 가능성이 높습니다. Bogon IP 범위가 100.64.0.0/10 내에 포함되는 경우에는 캐리어급 NAT용으로 예약된 IP 공간을 사용 중인 것이므로 환경에서 NAT를 사용한다면 문제가 되지 않습니다. 두 가지 경우에 모두 해당하지 않는 경우, 호스트 스냅샷(SMC 클라이언트 인터페이스 내부에서 액세스됨)에 호스트를 식별하는 데 유용한 정보가 포함됩니다. 예를 들어 Exporter Interface(엑스포터 인터페이스) 탭에는 호스트 플로우가 나타나는 엑스포터와 인터페이스가 표시되므로 디바이스가 호스팅되는 위치를 확인하는 데 도움이 됩니다. 또한, Security Events(보안 이벤트) 탭, Alarms(알람) 탭 및 Identification(ID) 탭도 확인하십시오. 이러한 탭에는 Bogon 호스트가 관련되어 있는 다른 모든 행동이 표시됩니다. 마지막으로, 상호 작용하고 있는 다른 호스트가 있는지 확인하려면 Bogon 호스트의 보안 이벤트를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 관심 지표(CI)
값은 무엇입니까?	• CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 이상 징후 지표: 참 • 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_CONN_FROM_BOGON_SUCCEEDED (517)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Tor에서 연결 시도됨

Tor 종료 노드에서 네트워크 내부 호스트로의 연결 시도가 탐지됩니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_EXIT_ATTEMPTED (317)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Tor에서 연결 성공

Tor 종료 노드에서 네트워크 내부 호스트로의 연결 성공이 탐지됩니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_EXIT_SUCCEEDED (318)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bogon 주소로 연결 시도됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Bogon 주소는 할당되지 않은 IP 주소로, 사용해서는 안 됩니다. 이러한 주소에 대한 단방향 통신이 설정되어 있는 것은 특정 요소가 네트워크의 호스트에 해당 통신을 설정하라고 지시한 것이므로 비정상적인 현상입니다. 이는 DoS(denial-of-service) 공격의 백스캐터일 가능성이 있습니다. 공격자가 DDoS(distributed denial-of- service)의 일부분으로 임의 지정된 소스 주소를 포함하는 패킷을 전송하여 임의 지정된 해당 주소에 응답하는 경우 이러한 현상이 발생합니다. 공격자가 전체 IP 공간을 임의 지정하는 경우 해당 공간의 주소 중 일부는 Bogon 주소가 됩니다. Bogon IP에 대한 단방향 통신은 정찰 또는 잘못 구성된 호스트의 징후일 수도 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	사용자 환경에서 실제로 특정 Bogon IP 주소 범위를 내부적으로 사용하는지 또는 캐리어급 NAT를 사용하는지 확인합니다. 사용자 환경에서 Bogon 범위를 내부적으로 사용하며 이러한 사용 방식이 정상적인 상태라면 내부 호스트 그룹에 해당 범위만 추가하면 됩니다. Stealtwatch System 내에서 이를 확인하는 방법은 Bogon의 /24에서 활성화된 플로우를 찾아보는 것입니다. 해당 범위의 대부분이 활성화된 상태이면 사용자 환경 내에서 해당 범위가 특정 목적을 위해 사용되고 있을 가능성이 높습니다. Bogon IP 범위가 100.64.0.0/10 내에 포함되는 경우에는 캐리어급 NAT용으로 예약된 IP 공간을 사용 중인 것이므로 환경에서 NAT를 사용한다면 문제가 되지 않습니다. 이 두 가지 경우에 모두 해당하지 않는 경우 이벤트 소스에서 다른 보안 이벤트를 검토합니다. Bogon과의 통신이 많이 수행되었는지 살펴보거나 SYNs Received(SYN 수신됨) 또는 New Flows Served(새 플로우 제공됨)와 같은 DoS(denial-of-service) 이벤트를 찾아봅니다. Ping Scan(Ping 스캔) 또는 Addr_Scan과 같은 정찰 관련 이벤트도 찾아봅니다. 잠재적 DDoS 비트를 더욱 철저하게 조사하려면 Flow Traffic(플로우 트래픽) 보고서를 실행합니다. Bogon 통신 시간과 이 시간보다 2시간 전의 시간을 포함하도록 Date/Time(날짜/시간) 필터를 설정합니다. 기간을 길게 설정할수록 쿼리는 길어지지만 더욱 자세한 상황 정보가 제공됩니다. 내부에서 시작된 DoS 공격은 확인하지 않아도 되는 경우 여기서 Hosts(호스트)를 필터링하여 외부 호스트의 트래픽만 포함할 수도 있습니다. 트래픽이 급격하게 증가하거나, 서서히 증가하더라도 전체 트래픽 양이 많은 것은 DoS 공격을 나타내는 현상일 수 있습니다. DDoS 또는 많은 양의 정찰 활동 가능성이 없는 경우, Bogon 호스트와 상호작용을 시도했던 기타 호스트가 있는지 확인하기 위해 Bogon IP의 보안 이벤트를 확인합니다. 특정 Bogon과 상호작용을 시도 중인 호스트가 많은 경우 애플리케이션에서 잘못된 컨피그레이션이 외부로 푸시되었거나 Bogon 범위에서 호스팅되는 애플리케이션이 사라진 것일 수 있습니다. Bogon의 트래픽 기록을 확인하면 이러한 현상을 더욱 자세히 조사할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_CONN_TO_BOGON_ATTEMPTED (518)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Bogon 주소로 연결 성공

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Bogon 주소는 할당되지 않은 IP 주소로, 사용해서는 안 됩니다. Bogon 주소와의 양방향 통신은 발생하지 않아야 합니다. 이러한 행동은 사용자의 네트워크 또는 Stealthwatch 구축 내의 컨피그레이션이 잘못되었다는 징후일 가능성이 높습니다.
다음 단계는 무엇입니까?	사용자 환경에서 실제로 특정 Bogon IP 주소 범위를 내부적으로 사용하는지 또는 캐리어급 NAT를 사용하는지 확인합니다. 사용자 환경에서 Bogon 범위를 내부적으로 사용하며 이러한 사용 방식이 정상적인 상태라면 내부 호스트 그룹에 해당 범위만 추가하면 됩니다. Stealtwatch System 내에서 이를 확인하는 방법은 Bogon의 /24에서 활성화된 플로우를 찾아보는 것입니다. 해당 범위의 대부분이 활성화된 상태이면 사용자 환경 내에서 해당 범위가 특정 목적을 위해 사용되고 있을 가능성이 높습니다. Bogon IP 범위가 100.64.0.0/10 내에 포함되는 경우에는 캐리어급 NAT용으로 예약된 IP 공간을 사용 중인 것이므로 환경에서 NAT를 사용한다면 문제가 되지 않습니다. 두 가지 경우에 모두 해당하지 않는 경우, 호스트 스냅샷(SMC 클라이언트 인터페이스 내부에서 액세스됨)에 호스트를 식별하는 데 유용한 정보가 포함됩니다. 예를 들어 Exporter Interface(엑스포터 인터페이스) 탭에는 호스트 플로우가 나타나는 엑스포터와 인터페이스가 표시되므로 디바이스가 호스팅되는 위치를 확인하는 데 도움이 됩니다. 또한, Security Events(보안 이벤트) 탭, Alarms(알람) 탭 및 Identification(ID) 탭도 확인하십시오. 이러한 탭에는 Bogon 호스트가 관련되어 있는 다른 모든 행동이 표시됩니다. 마지막으로, 상호 작용하고 있는 다른 호스트가 있는지 확인하려면 Bogon 호스트의 보안 이벤트를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_CONN_TO_BOGON_SUCCEEDED (516)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Tor로 연결 시도됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Tor(구 The Onion Router)는 인터넷 연결을 익명화하는 데 사용되는 네트워크로, 여러 릴레이를 통해 연결을 전송한 후 Tor 네트워크를 종료하는 방식으로 동작합니다. Tor 엔트리 노드는 Tor 네트워크를 탐색하여 종료하기 전에 Tor 연결이 통과하는 첫 번째 서버입니다. 이 보안 이벤트는 Tor 엔트리 노드와 통신을 시도 중인 Stealthwatch System에 의해 모니터링되고 있지만 성공적인 연결 설정이 관찰되지 않은 호스트와 관련이 있습니다. 이는 C&C(command and control) 트래픽을 찾으려고 시도 중인 사용자 구현 또는 악성코드 중 하나일 수 있습니다. 사용자가 구현한 경우, 이는 사용자 트래픽의 대상을 난독 처리하거나 사용자가 검색 중인 위치를 난독 처리하려는 시도일 가능성이 있습니다. 일부 Tor 엔트리 노드는 다른 서비스도 실행하는 서버에서 실행됩니다. 예를 들어 DuckDuc kGo는 검색을 수행하기 위해 액세스된 동일한 서버에서 Tor 엔트리 노드를 실행합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)

이벤트에 대한 질문	응답
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_ENTRY_ATTEMPTED (513)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Tor로 연결 성공

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Tor(구 The Onion Router)는 인터넷 연결을 익명화하는 데 사용되는 네트워크로, 여러 릴레이를 통해 연결을 전송한 후 Tor 네트워크를 종료하는 방식으로 동작합니다. Tor 엔트리 노드는 Tor 네트워크를 탐색하여 종료하기 전에 Tor 연결이 통과하는 첫 번째 서버입니다. 이 보안 이벤트는 Tor 엔트리 노드와 통신 중인 Stealthwatch System에 의해 모니터링되고 있는 호스트와 관련이 있습니다. 이는 C&C(command and control) 트래픽을 찾으려고 시도 중인 사용자 구현 또는 악성코드 중 하나일 수 있습니다. 사용자가 구현한 경우, 이는 사용자 트래픽의 대상을 난독 처리하거나 사용자가 검색 중인 위치를 난독 처리하려는 시도일 가능성이 있습니다. 일부 Tor 엔트리 노드는 다른 서비스도 실행하는 서버에서 실행됩니다. 예를 들어 DuckDuc kGo는 검색을 수행하기 위해 액세스된 동일한 서버에서 Tor 엔트리 노드를 실행합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_ENTRY_SUCCEEDED (514)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

위조 애플리케이션 탐지됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 행동은 특정 사용자나 애플리케이션이 의도했던 것과는 다른 서비스를 사용하여 일반적으로 허용되는 포트에서 트래픽을 전송해 이그레스 필터링 우회를 시도하는 징후인 경우가 많습니다. 또한, 이 이벤트는 표준 포트가 아닌 포트를 사용하는 표준 애플리케이션도 조회하므로 TCP 8022의 SSH와 같이 보조 포트를 사용하는 애플리케이션에 대해서도 발생할 수 있습니다.
다음 단계는 무엇입니까?	조사 시에는 관련 플로우를 찾은 다음 해당 플로우가 데이터 유출 또는 C&C(command and control)의 징후로 보이는지 확인해야 합니다. 이 이벤트를 조사하는 첫 번째 단계는 이벤트에 연결된 포트와 관련 호스트를 고려하는 것입니다. 예를 들어 대상 호스트가 오프사이트 백업 서버이고 이벤트가 포트 8022에서 트리거되었다면 문제가 아닐 수도 있습니다. 반면에 대상 호스트가 알 수 없는 호스트이고 DNS가 아닌 플로우가 53 UDP 포트를 통해 전송된다면 더욱 상세하게 조사해야 할 가능성이 높습니다. 이 이벤트는 몇 가지 방법으로 조사할 수 있습니다. 보안 이벤트는 연결된 포트를 나열하고 이 포트를 매우 구체적인 필터를 생성하는 데 사용할 수 있습니다. 예를 들어 이벤트에 관련된 포트를 사용하는 관련 호스트 2개 간의 플로우를 필터링하면서 '적절한' 애플리케이션을 사용하는 플로우는 제외(예: 포트 53 UDP를 통해 전송되는 DNS가 아닌 플로우 검색)하면 이벤트 발생의 원인이 된 플로우를 찾을 수 있습니다. 더욱 일반적인 쿼리를 대신 실행하여 이벤트 날짜의 이벤트 소스 및 대상 호스트만 필터링하는 방식도 유용할 수 있습니다. 이렇게 하면 포트와 애플리케이션이 일치하지 않는 플로우가 탐지될 뿐만 아니라 조사에서 유용한 상황 정보를 제공하는 플로우의 유무도 확인할 수 있습니다. 사용할 플로우를 선택한 후 대상 호스트, 기록 및 데이터 볼륨에서 오용 징후를 검사하십시오.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FAKE_APP (62)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Flow_Denied

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 상황에 주로 의존한다는 것입니다. 예를 들어 인터넷의 호스트에서 발생하는 플로우 거부는 특히 단일 이벤트로서는 그다지 중요하지 않습니다. 내부 호스트에서 내부 호스트로의 플로우 거부됨 이벤트와 내부 호스트에서 외부 호스트로의 플로우 거부됨 이벤트는 서로 다릅니다. 그리고 같은 호스트/포트 페어링을 계속 시도하는 것은 여러 대상에서 플로우가 거부되는 것과 크게 다릅니다. 단일 포트를 통해 다른 내부 호스트와 통신하는 내부 호스트의 플로우가 여러 번 거부되는 경우 컨피그레이션이 잘못되었을 가능성이 높습니다. 다양한 포트나 내부 호스트로 전송하는 플로우가 여러 번 거부되는 경우에는 정찰이 수행되고 있을 가능성이 높습니다. 그 외의 현상은 호스트가 수행하지 않아야 하는 작업을 수행 중이라는 징후이므로 기본적으로 확인이 필요합니다. 내부 호스트에서 인터넷으로 전송되는 중에 플로우가 차단된 경우 위반을 시도한 규칙의 상황을 파악해야 합니다. 하지만 해당 상황과 관계없이 호스트는 보안 정책에 따라 수행하면 안 되는 작업을 수행 중인 것입니다.
다음 단계는 무엇입니까?	플로우 거부를 조사하기에 좋은 방법은 이벤트의 소스 호스트에 대해 보안 이벤트 쿼리를 수행하는 것입니다. 이벤트 날짜에 대해 쿼리를 실행하고, 소스 호스트를 초기 플로우 거부됨 이벤트의 소스로 설정한 후, 기타 플로우 거부됨 이벤트만 포함하도록 유형을 설정합니다. 그러면 호스트에 대해 발생한 모든 플로우 거부됨 이벤트가 표시됩니다. 반환되는 결과에서 한 번 거부된 플로우인지, 동일한 호스트에 대해 동일한 포트를 통해 여러 번 거부된 플로우인지, 여러 호스트에 대해 동일한 포트를 통해 여러 번 거부된 플로우인지를 확인할 수 있습니다. 그러면 호스트가 실제로 관여하고 있는 행동을 파악할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

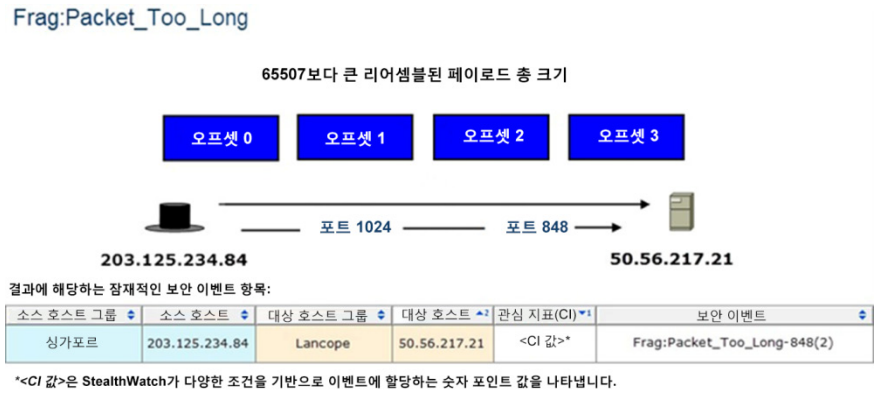
이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FLOW_DENIED (310)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Frag: Packet_Too_Long**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	프래그멘테이션 값으로 인해 최대 패킷 길이를 초과하는 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 프래그멘테이션 값이 잘못된 IP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 운영 체제와 버전마다 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 프래그먼트를 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.

이 이벤트에 대한 질문	응답
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Frag:Packet_Too_Long을 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음

이벤트에 대한 질문	응답
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트 정책
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

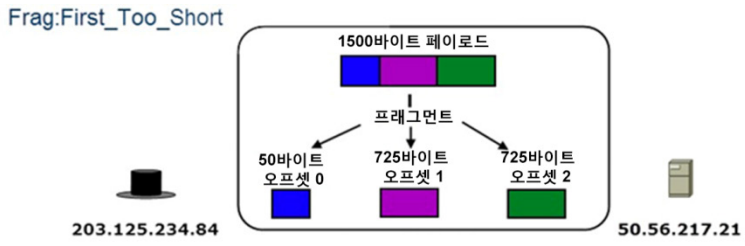
이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FRAG_PKT_TOO_LONG (282)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Frag: Packet_Too_Short**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Frag:First_Too_Short-445(1)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	프래그멘테이션 길이가 너무 짧아 프로토콜 헤더가 잘린 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 프래그멘테이션 값이 잘못된 IP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우 패킷이 전송된 시스템에 대한 정보를 수집하기 위해 의도적으로 전송된 것일 수 있습니다. 운영 체제와 버전마다 서로 다른 방식으로 응답할 수 있기 때문입니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 프래그먼트를 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.

이 이벤트에 대한 질문	응답
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Frag:First_Too_Short를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음

이벤트에 대한 질문	응답
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트 정책
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

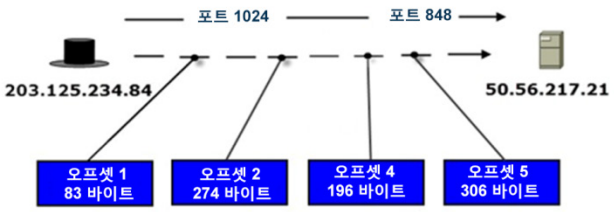
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FRAG_PKT_TOO_SHORT (281)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Frag: Sizes_Differ**

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Frag:Sizes_Differ



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Frag:Sizes_Differ-848(2)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	프래그멘테이션 크기가 세그먼트 간에 서로 다른 패킷이 확인되는 경우 해당 패킷이 생성된 호스트에서 보안 이벤트가 트리거됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	일반적으로는 각 세그먼트의 프래그멘테이션 크기가 다른 IP 패킷이 전송되어서는 안 됩니다. 이러한 패킷이 전송되는 경우, 경로를 따라 패킷 검사 툴 우회를 시도하기 위해 의도적으로 전송된 것일 가능성이 높습니다.
다음 단계는 무엇입니까?	이 이벤트의 소스가 내부 호스트인 경우 정찰 활동의 다른 징후를 파악하는 것이 좋습니다. 예를 들어 호스트가 잘못된 프래그먼트를 여러 호스트로 전송하는지, 동일한 포트에서 여러 호스트를 스캔하는지, 하나의 호스트에서 여러 포트를 스캔하는지 등을 확인해 볼 수 있습니다. 내부 호스트가 정찰을 수행하는 현상은 원치 않는 활동이 수행되고 있거나 보안이 침해되었다는 대표적인 징후일 수 있습니다.

이 이벤트에 대한 질문	응답
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	Flow Collector NetFlow 버전의 경우 FlowSensor가 필요합니다. Flow Collector sFlow의 경우에는 특별히 추가 기능이 필요하지 않습니다.
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	생성된 호스트에서 보안 이벤트인 Frag:Sizes_Differ를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책, 안티바이러스 및 SMS 서버, 방화벽, 프록시 및 NAT 디바이스, 네트워크 관리 및 스캐너
이 이벤트를 조정할 수 있습니까?	아니요
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	해당 없음
기본값과 단위는 무엇입니까?	
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음

이벤트에 대한 질문	응답
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	해당 없음
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	잘못된 패킷을 전송한 호스트
대상은 무엇입니까?	잘못된 패킷의 대상으로 나열된 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트 정책
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

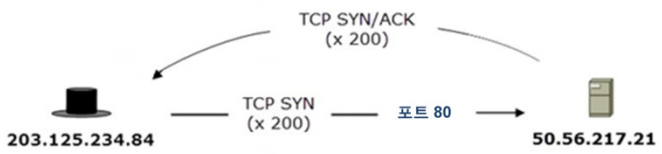
이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FRAG_DIFFERENT_SIZES (283)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

절반 열림 공격

Half_Open_Attack



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Half_Open_Attack

***<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.**

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 DoS(denial-of-service) 공격입니다. 절반 열림 공격은 대역폭 또는 연결 처리기를 소진시키기 위한 시도일 수 있습니다. 이 공격은 연결을 열기만 하고 실제로 설정하지는 않음으로써 피해 대상 호스트가 악의적인 연결이 시간 초과될 때까지 오랫동안 기다리도록 강제로 설정하기 때문입니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	목표는 대상에 대한 연결이 정상적인지 그리고 대상이 성능 저하를 경험하는지 확인하는 것입니다. 이러한 연결은 두 개의 내부 호스트 간의 악의적인 행동일 수도 있지만, 이 이벤트는 내부 호스트와 외부 호스트 사이에서 더 확인이 필요할 수 있습니다. 먼저 이벤트 날짜의 이벤트 소스와 대상 간에 플로우 쿼리를 실행합니다. 플로우 지속 여부를 기록합니다. 플로우가 지속되지 않으면 서비스 장애가 없으며 문제가 아닐 가능성이 있습니다. 소스 호스트와 대상 호스트 둘 다의 보안 이벤트 기록을 확인할 수도 있습니다. 소스 호스트에서 여러 대상에 대해 또는 이전에도 이 이벤트가 발생한 적이 있었다면 이는 추가 조사가 필요한 상황입니다. 대상 호스트에서 이전에는 이 이벤트가 발생하지 않았는데 현재는 여러 호스트가 동시에 이 이벤트를 트리거하는 경우 이는 DDoS(distributed denial-of-servce) 공격의 징후일 수 있습니다. 이전에도 이벤트가 발생했다면 서비스가 호스팅하는 애플리케이션의 정상 행동일 수도 있습니다. 이 경우 해당 특정 호스트에 대해 이벤트를 해제할 수 있습니다. Flow Sensor에서 관련 트래픽이 관찰된 경우에는 성능 보고서를 실행하여 트래픽의 특성으로 인해 SRT(Server Response Time, 서버 응답 시간)가 영향을 받았는지를 확인합니다. 이는 트래픽이 정상적인지를 나타낼 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	'A' 정책: 상위 Ddos 소스 지표, 상위 관심 지표(CI) *'B' 정책: 상위 Ddos 소스 지표, 상위 관심 지표(CI)*
값은 무엇입니까?	'A' 정책: • 상위 Ddos 소스 지표: 참 • CI: 참 'B' 정책: • 상위 Ddos 소스 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	'A' 정책: 상위 Ddos 대상 지표, 상위 대상 지표(TI) *'B' 정책: 상위 Ddos 대상 지표, 상위 대상 지표(TI)*
값은 무엇입니까?	'A' 정책: • 상위 Ddos 대상 지표: 참 • TI: 참 'B' 정책: • 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HALF_OPEN (26)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

높은 파일 공유 지수

파일 공유 활동에서 FSI(File Sharing Index) 임계값이 초과되었습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FILE_SHARING (20)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

높은 SMB 피어

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이벤트가 특정 시나리오에서 발생해야 한다는 점을 알지 못하는 경우 또는 임계값을 매우 낮게 설정한 경우, 이 이벤트는 거의 확실하게 손상된 호스트의 징후입니다. 이는 SMB를 통해 자동으로 확산하는 방법을 찾고 있는 악성코드의 징후인 경우가 많습니다.
다음 단계는 무엇입니까?	이 보안 이벤트는 손상 가능성을 나타내는 징후이지만, 외부 호스트가 특정 범위에 속하는지 확인하거나 얼마나 많은 수의 외부 호스트에 접속되었는지 확인하기 위해 조사를 수행할 수 있습니다. 이렇게 하려면 플로우 쿼리를 시작합니다. 쿼리의 시작 시간을 이벤트 날짜로 설정합니다. Filter(필터) 대화 상자에 있는 Hosts(호스트) 탭에서 *Client(클라이언트)* 또는 *Server Host(서버 호스트)*를 이벤트의 소스로 설정하고 *Other Host(기타 호스트)*를 Inside Hosts(내부 호스트) 호스트 그룹으로 설정합니다. Services & Applications(서비스 및 애플리케이션) 탭에서 *Services(서비스)* 기준으로 필터링하고 *SMB*를 포함합니다. 쿼리는 관련된 모든 플로우를 반환합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HIGH_SMB_PEERS (60)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

높은 총 트래픽

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	인바운드 트래픽과 아웃바운드 트래픽이 모두 계산에 포함되므로 높은 총 트래픽은 보통 비정상적인 행동의 징후입니다. 인바운드 트래픽이나 아웃바운드 트래픽 중 하나가 특히 많을 수도 있고 두 트래픽이 모두 많을 수도 있습니다. IP가 비정상적으로 많은 양의 트래픽에 사용되는 것입니다.
다음 단계는 무엇입니까?	이동 중인 데이터의 양과 해당 데이터가 수신되는 위치 및 생성되는 위치를 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 소스 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 기간은 관련 보안 이벤트 날짜로 설정하고 소스 호스트는 클라이언트 호스트 또는 서버 호스트로 설정합니다. 결과가 반환되면 가장 많은 양의 데이터가 발신되거나 수신되는 위치를 찾습니다. 이렇게 하려면 Total Bytes(총 바이트 수)를 기준으로 플로우를 정렬합니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOTAL_TRAFFIC (16)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

높은 트래픽

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	인바운드 트래픽과 아웃바운드 트래픽이 모두 계산에 포함되므로 높은 총 트래픽은 보통 비정상적인 행동의 징후입니다. 인바운드 트래픽이나 아웃바운드 트래픽 중 하나가 특히 많을 수도 있고 두 트래픽이 모두 많을 수도 있습니다. IP가 비정상적으로 많은 양의 트래픽에 사용되는 것입니다. 이 이벤트는 수신 또는 발신 DoS를 나타낼 수 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	이동 중인 데이터의 양과 해당 데이터가 수신되는 위치 및 생성되는 위치를 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 소스 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 소스 호스트는 클라이언트 호스트 또는 서버 호스트로 설정합니다. 결과가 반환되면 가장 많은 양의 데이터가 발신되거나 수신되는 위치를 찾습니다. 이렇게 하려면 Total Bytes(총 바이트 수)를 기준으로 플로우를 정렬합니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HI_TRAFFIC (30)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

대량의 이메일

호스트가 이메일 웜에 감염되었을 수 있으며, 해당 호스트에서 5분 동안 허용되는 횟수보다 많은 경고가 발생했습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HIGH_VOLUME_EMAIL (9)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

호스트 잠금 위반

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 사실상 라우터 ACL에 해당하는 사용자가 구성한 모니터링입니다. 이벤트의 의미는 사용자가 특정 호스트 잠금을 구현하기로 결정한 이유에 따라 달라질 수 있지만, 대개 사용자가 소스, 대상 및 잠재적인 애플리케이션을 기준으로 하여 부적절한 것으로 간주한 연결입니다.
다음 단계는 무엇입니까?	호스트 잠금 위반의 조사 단계는 전적으로 호스트 잠금이 설정된 상황에 따라 달라집니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HOST_LOCK_VIOLATION (1)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP 플러드

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 소스 호스트가 DoS 공격에 사용되고 있거나(호스트 보안이 침해되었거나 사용자가 공격을 진행했을 수 있음), 네트워크 애플리케이션이 잘못 구성되었거나, 정찰이 수행되고 있음을 나타냅니다(해당 정찰 중에 소규모 그룹이 아니라 매우 광범위한 IP로 패킷이 전송됨).

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	전송되는 ICMP 패킷의 양과 전송 속도, 전송된 시간, 전송 대상을 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 소스 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 프로토콜 필터를 *ICMP only(ICMP 전용)*로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 ICMP 패킷이 전송된 위치를 찾습니다. 이벤트의 주체가 ICMP가 많이 전송되는 플로우의 클라이언트 호스트인 경우 Client Packets(클라이언트 패킷) 또는 Client Packet Rate(pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 소스 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 Ddos 소스 지표: 참 • CI: 참

이벤트에 대한 질문	응답
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_ICMP_FLOOD (7)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP 수신됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 대상 호스트가 DoS 공격의 대상이 되었거나 네트워크 애플리케이션이 잘못 구성되었음을 나타냅니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	수신되는 ICMP 패킷의 양과 수신 속도, 수신된 시간, 수신 출처를 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 대상 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 프로토콜 필터를 *ICMP only(ICMP 전용)*로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 ICMP 패킷 전송이 시작된 위치를 찾습니다. 이벤트의 주체가 ICMP가 많이 전송되는 플로우의 클라이언트 호스트인 경우 Client Packets(클라이언트 패킷) 또는 Client Packet Rate (pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표

이벤트에 대한 질문	응답
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_ICMP_RECEIVED (50)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Comm_Admin*

소스 호스트가 "관리자가 통신을 금지했습니다."라는 ICMP 메시지를 받았습니다. 라우터가 관리 필터링으로 인해 패킷을 전달할 수 없는 경우 이 메시지가 생성됩니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)

이벤트에 대한 질문	응답
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_COMM_ADMIN_PROHIBITED (302)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Dest_Host_Admin*

소스 호스트가 "관리자가 대상 호스트를 금지했습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_DEST_HOST_ADMIN_PROHIBITED (299)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Dest_Host_Unk*

소스 호스트가 "대상 호스트를 알 수 없음" 오류가 발생했다는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_DEST_HOST_UNKNOWN (296)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Dest_Net_Admin*

소스 호스트가 "관리자가 대상 네트워크를 금지했습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_DEST_NETWK_ADMIN_PROHIBITED (298)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Dest_Net_Unk*

소스 호스트가 "대상 네트워크를 알 수 없음" 오류가 발생했다는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_DEST_NETWORK_UNKNOWN (295)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Frag_Needed*

소스 호스트가 "IP 데이터그램이 너무 큽니다."라는 ICMP 메시지를 받았습니다. 패킷 프래그멘테이션이가 필요한데 IP 헤더에 DF 비트가 설정되어 있습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_FRAG_NEEDED_DF_SET (293)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Host_Precedence*

소스 호스트가 "호스트 우선순위 위반"이 발생했다는 ICMP 메시지를 받았습니다. 이 이벤트는 요청한 우선순위가 소스/대상 호스트 또는 네트워크, 상위 레이어 프로토콜, 소스/대상 포트의 특정 조합에 허용되지 않음을 나타내기 위해 첫 번째 홉 라우터가 호스트로 전송하는 이벤트입니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HOST_PRECEDENCE_VIOLATION (303)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Host_Unreach*

소스 호스트가 "대상 호스트에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HOST_UNREACHABLE (290)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Host_Unreach_TOS*

소스 호스트가 "지정된 서비스 유형으로 인해 대상 호스트에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_HOST_UNREACHABLE_FOR_SVC (301)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Net_Unreach*

소스 호스트가 "대상 네트워크에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_NETWORK_UNREACHABLE (289)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Net_Unreach_TOS*

소스 호스트가 "지정된 서비스 유형을 사용하기 위해 네트워크에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_NETWK_UNREACHABLE_FOR_SVC (300)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Port_Unreach*

소스 호스트가 "대상 포트에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다. 지정된 전송 프로토콜(예: UDP)이 데이터그램 다중화를 취소할 수 없으나, 발신인에게 알릴 수 있는 프로토콜 메커니즘이 없습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PORT_UNREACHABLE (292)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Precedence_Cutoff*

소스 호스트가 "우선순위 컷오프"가 적용되었다는 ICMP 메시지를 받았습니다. 네트워크 운영자가 작업에 필요한 최소 우선순위 레벨을 적용했는데 이 레벨보다 우선순위가 낮은 데이터그램이 전송되었습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PRECEDENCE_CUTOFF (304)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Proto_Unreach*

소스 호스트가 "대상 프로토콜에 연결할 수 없습니다."라는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PROTOCOL_UNREACHABLE (291)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Src_Host_Isolated*

소스 호스트가 "소스 호스트 격리 오류"가 발생했다는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SOURCE_HOST_ISOLATED (297)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Src_Route_Failed*

소스 호스트가 "소스 경로 실패" 오류가 발생했다는 ICMP 메시지를 받았습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

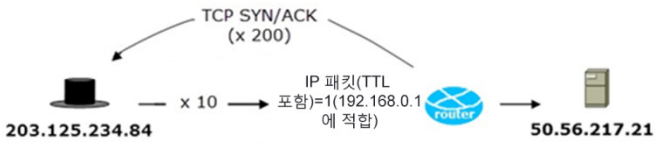
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SOURCE_ROUTE_FAIL (294)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

ICMP_Timeout

호스트가 전송한 메시지로 인해 "전송 중에 연결 유지 시간이 초과됨" ICMP 메시지가 생성되었습니다. 이러한 메시지는 트레이스라우트(traceoute), 네트워크 오작동(라우팅 루프) 및 파이어워킹(firewalking) 기술로 인해 생성되는 경우가 많습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

ICMP_Timeout



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	ICMP_Timeout(10)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_ICMP_TO (258)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

내부 Tor 엔트리 탐지됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Tor(구 The Onion Router)는 인터넷 연결을 익명화하는 데 사용되는 네트워크로, 여러 릴레이를 통해 연결을 전송한 후 Tor 네트워크를 종료하는 방식으로 동작합니다. Tor 엔트리 노드는 Tor 네트워크를 탐색하여 종료하기 전에 Tor 연결이 통과하는 첫 번째 서버입니다. 이 보안 이벤트는 Stealthwatch System에 의해 모니터링되는 중이며 Tor 엔트리 노드라는 알림을 제공받는 중인 호스트와 관련이 있습니다. Tor 종료 노드를 호스팅하는 것이 반드시 문제가 되는 것은 아니지만, 네트워크 관리자가 모르는 상태로 수행해서는 안 되는 작업이라는 점은 거의 확실합니다. Tor 종료 노드와는 달리 Tor 엔트리 노드는 Tor 네트워크 내에서만 트래픽을 전달하므로 주된 문제는 대개 대역폭입니다.
다음 단계는 무엇입니까?	이 이벤트를 조사하는 것은 주로 기술 외적인 목적입니다. 누군가가 Tor 엔트리 노드를 알고 있는지 그리고 이 노드가 허용되는지 확인합니다. 허용되는 경우에는 허용되는 특정 호스트에 대해 이벤트를 비활성화합니다. 호스트의 보안 이벤트 기록을 확인하여 해당 호스트가 Tor 엔트리 노드라는 알림을 제공받는 중에 통신을 시작한 시간을 파악할 수도 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_ENTRY_INSIDE_HOST (515)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

내부 Tor 종료 탐지됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	Tor(구 The Onion Router)는 인터넷 연결을 익명화하는 데 사용되는 네트워크로, 여러 릴레이를 통해 연결을 전송한 후 Tor 네트워크를 종료하는 방식으로 동작합니다. Tor 종료 노드는 Tor 네트워크를 탐색 및 종료하기 전에 Tor 연결이 통과하는 첫 번째 서버이자, 네트워크 연결 대상에 연결 소스로 마지막에 표시되는 서버입니다. 이 보안 이벤트는 Stealthwatch System에 의해 모니터링되는 중이며 Tor 종료 노드라는 알림을 제공받는 중인 호스트와 관련이 있습니다. Tor 종료 노드를 호스팅하는 것이 반드시 문제가 되는 것은 아니지만, 네트워크 관리자가 모르는 상태로 수행해서는 안 되는 작업이라는 점은 거의 확실합니다. Tor 종료 노드 호스팅에 대한 문제에는 대역폭 사용량, 그리고 노드를 통해 프록시되는 활동과 관련한 법적 문제 가능성이 포함되는 경우가 많습니다.
다음 단계는 무엇입니까?	이 이벤트를 조사하는 것은 주로 기술 외적인 목적입니다. 누군가가 Tor 종료 노드를 알고 있는지 그리고 이 노드가 허용되는지 확인합니다. 허용되는 경우에는 허용되는 특정 호스트에 대해 이벤트를 비활성화합니다. 호스트의 보안 이벤트 기록을 확인하여 해당 호스트가 Tor 종료 노드라는 알림을 제공받는 중에 통신을 시작한 시간을 파악할 수도 있습니다. 또한, Top Peers(상위 피어) 보고서를 실행하여 서버가 사용하는 대역폭 양과 대역폭이 이동하는 위치를 확인할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOR_EXIT_INSIDE_HOST (319)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

낮은 트래픽

마지막 5분 동안 호스트의 평균 트래픽이 허용되는 최소값 미만으로 감소했습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_LOW_TRAFFIC (29)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

MAC 주소 위반

호스트가 MAC 주소를 마지막 아카이브 시간 이후 허용되는 횟수보다 많이 변경했습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_MAC_ADDRESS (25)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

메일 거부

대상 호스트가 거부된 이메일 시도를 허용되는 횟수보다 많이 수신했으며, 이로 인해 5분 동안 허용되는 수보다 많은 관련 알림이 생성되었습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_MAIL_REJECTS (12)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

메일 릴레이

대상 호스트에서 5분 동안 허용되는 횟수보다 많은 경고가 발생했습니다. 해당 호스트가 이메일 릴레이로 작동하고 있을 가능성이 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_MAIL_RELAY (10)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

최대 플로우 시작됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 여러 가지 문제를 나타낼 수 있지만, 먼저 해당 이벤트가 정찰을 나타내는 징후인지 아니면 호스트가 DoS 공격을 수행 중임을 나타내는 징후인지를 확인해야 합니다.
다음 단계는 무엇입니까?	이러한 유형의 플로우 간 공통 링크를 찾아 해당 플로우를 생성하는 원인을 확인하십시오. 예를 들어 해당 플로우 중 대부분이 동일한 호스트로 이동하는지 아니면 같은 포트를 사용하는 다른 호스트로 이동하는지를 확인할 수 있습니다. 이러한 정보를 확인하는 가장 좋은 방법은 상위 보고서 중 하나를 실행하는 것입니다. 먼저 Top Peers(상위 피어) 보고서 또는 Top Ports(상위 포트) 보고서부터 실행할 수 있습니다. 보고서에 액세스한 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Direction(방향) 필드를 *Total(전체)*로 설정합니다. 이때 *Client(클라이언트)*가 이벤트의 소스이고, *Server Host(서버 호스트)*에서 제외 항목은 없습니다. Date/Time(날짜/시간) 탭에서 기간을 이벤트의 시작 활성 시간 5분 전부터 이벤트의 시작 활성 시간까지로 설정합니다. Advanced(고급) 탭에서 *Flows(플로우)*를 기준으로 정렬합니다. 대부분의 플로우가 특정 행 집합에 적용되는지를 확인합니다. 그렇지 않은 경우에는 제안된 두 가지 상위 보고서 중에서 다른 보고서를 실행합니다 주요 포트나 피어를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_MAX_FLOWS_INIT (17)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

최대 플로우 제공됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 여러 가지 문제를 나타낼 수 있지만, 먼저 해당 이벤트가 정찰을 나타내는 징후인지 아니면 호스트가 DoS 공격의 대상임을 나타내는 징후인지를 확인해야 합니다. 일반적으로 많은 양의 트래픽을 제공하는 호스트의 경우에는 임계값 및 허용치 설정에 따라 정상적인 사용 중에 플로우 수가 많아지는 것뿐일 수 있습니다.
다음 단계는 무엇입니까?	이러한 유형의 플로우 간 공통 링크를 찾아 해당 플로우를 생성하는 원인을 확인하십시오. 예를 들어 해당 플로우 중 대부분이 동일한 호스트에서 오는지 아니면 같은 포트를 대상으로 하는 다른 호스트에서 오는지 확인합니다. 이러한 정보를 확인하는 가장 좋은 방법은 상위 보고서 중 하나를 실행하는 것입니다. 먼저 Top Peers(상위 피어) 보고서 또는 Top Ports(상위 포트) 보고서부터 실행할 수 있습니다. 보고서에 액세스한 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Direction(방향) 필드를 *Total(전체)*로 설정합니다. 이때 *Server Host(서버 호스트)*가 이벤트의 소스이고, *Client(클라이언트)*에서 제외 항목은 없습니다. Date/Time(날짜/시간) 탭에서 기간을 이벤트의 시작 활성 시간 5분 전부터 이벤트의 시작 활성 시간까지로 설정합니다. Advanced(고급) 탭에서 *Flows(플로우)*를 기준으로 정렬합니다. 대부분의 플로우가 특정 행 집합에 적용되는지를 확인합니다. 그렇지 않은 경우에는 제안된 두 가지 상위 보고서 중에서 다른 보고서를 실행합니다 주요 포트나 피어를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 대상 지표
값은 무엇입니까?	• 이상 징후 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_MAX_FLOWS_SERVED (37)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

새 플로우 시작됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 여러 가지 문제를 나타낼 수 있지만, 먼저 해당 이벤트가 정찰을 나타내는 징후인지 아니면 호스트가 DoS 공격을 수행 중임을 나타내는 징후인지를 확인해야 합니다.
다음 단계는 무엇입니까?	이러한 유형의 플로우 간 공통 링크를 찾아 해당 플로우를 생성하는 원인을 확인하십시오. 예를 들어 해당 플로우 중 대부분이 동일한 호스트로 이동하는지 아니면 같은 포트를 사용하는 다른 호스트로 이동하는지를 확인할 수 있습니다. 이러한 정보를 확인하는 가장 좋은 방법은 상위 보고서 중 하나를 실행하는 것입니다. 먼저 Top Peers(상위 피어) 보고서 또는 Top Ports(상위 포트) 보고서부터 실행할 수 있습니다. 보고서에 액세스한 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Direction(방향) 필드를 *Total(전체)*로 설정합니다. 이때 *Client(클라이언트)*가 이벤트의 소스이고, *Server Host(서버 호스트)*에서 제외 항목은 없습니다. Date/Time(날짜/시간) 탭에서 기간을 이벤트의 시작 활성 시간 5분 전부터 이벤트의 시작 활성 시간까지로 설정합니다. Advanced(고급) 탭에서 *Flows(플로우)*를 기준으로 정렬합니다. 대부분의 플로우가 특정 행 집합에 적용되는지를 확인합니다. 그렇지 않은 경우에는 제안된 두 가지 상위 보고서 중에서 다른 보고서를 실행합니다 주요 포트나 피어를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 이상 징후 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_NEW_FLOWS_INIT (18)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

새 플로우 제공됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 여러 가지 문제를 나타낼 수 있지만, 먼저 해당 이벤트가 정찰을 나타내는 징후인지 아니면 호스트가 DoS 공격의 대상임을 나타내는 징후인지를 확인해야 합니다. 일반적으로 많은 양의 트래픽을 제공하는 호스트의 경우에는 임계값 및 허용치 설정에 따라 정상적인 사용 중에 플로우 수가 많아지는 것뿐일 수 있습니다.
다음 단계는 무엇입니까?	이러한 유형의 플로우 간 공통 링크를 찾아 해당 플로우를 생성하는 원인을 확인하십시오. 예를 들어 해당 플로우 중 대부분이 동일한 호스트로 이동하는지 아니면 같은 포트를 사용하는 다른 호스트로 이동하는지를 확인할 수 있습니다. 이러한 정보를 확인하는 가장 좋은 방법은 상위 보고서 중 하나를 실행하는 것입니다. 먼저 Top Peers(상위 피어) 보고서 또는 Top Ports(상위 포트) 보고서부터 실행할 수 있습니다. 보고서에 액세스한 다음 Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Direction(방향) 필드를 *Total(전체)*로 설정합니다. 이때 *Server Host(서버 호스트)*가 이벤트의 소스이고, *Client(클라이언트)*에서 제외 항목은 없습니다. Date/Time(날짜/시간) 탭에서 기간을 이벤트의 시작 활성 시간 5분 전부터 이벤트의 시작 활성 시간까지로 설정합니다. Advanced(고급) 탭에서 *Flows(플로우)*를 기준으로 정렬합니다. 대부분의 플로우가 특정 행 집합에 적용되는지를 확인합니다. 그렇지 않은 경우에는 제안된 두 가지 상위 보고서 중에서 다른 보고서를 실행합니다 주요 포트나 피어를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_NEW_FLOWS_SERVED (38)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

새 호스트 활성화

새 호스트가 탐지되었습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

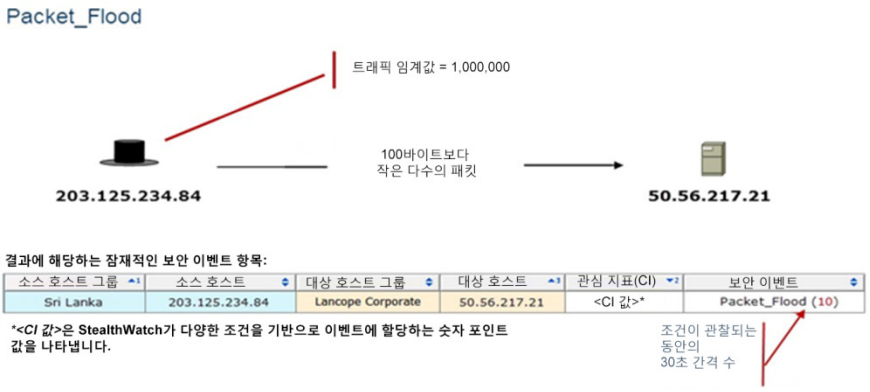
이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_NEW_HOST (14)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

패킷 플러드

소스 호스트가 대상 호스트에 지나치게 많은 수의 짧은 패킷을 전송했습니다. 이 보안 이벤트는 무차별 대입 공격, DoS 공격 및 네트워크 애플리케이션 오작동의 결과로 나타납니다.



어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 소스 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 Ddos 소스 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

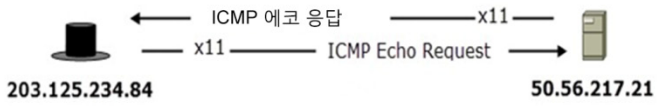
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PACKET_FLOOD (8)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Ping

소스 호스트가 ICMP 에코 응답을 전송하여 대상으로부터 ICMP 에코 응답을 수신했습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Ping



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Ping(11)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

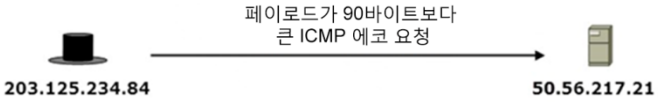
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PING_PROBE (257)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Ping_Oversized_Packet

소스 호스트가 데이터를 90바이트 이상 포함하는 ICMP 에코 요청이나 응답을 전송했습니다. 이러한 이벤트는 무해한 네트워크 상태 확인용일 수도 있고 은폐 데이터 채널을 포함할 수도 있습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

Ping_Oversized_Packet



Ping_Oversized_Packet 이벤트는
ICMP 에코 응답에도 적용됨

결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Ping_Oversized_Packet(58)

***<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.**

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

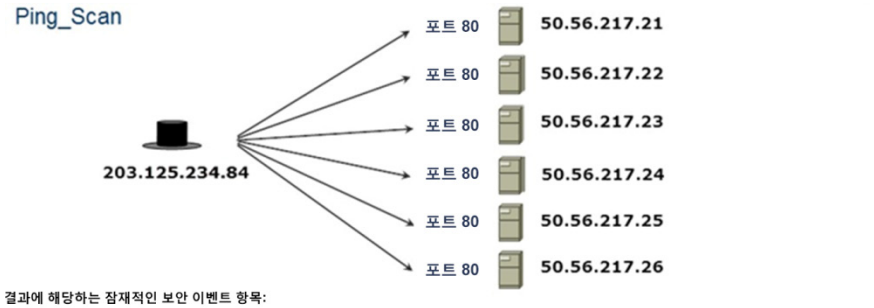
이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_LONG_PING (278)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Ping_Scan

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	Ping_Scan(72)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	ICMP 스캔은 대개 초기 유형의 정찰이라 할 수 있습니다. 호스트 전체의 특정 포트나 단일 호스트의 여러 포트 스캔과는 달리 ICMP 스캔에서는 특정 서비스가 아닌 응답하는 호스트만 검색하기 때문입니다. 호스트 ping 스캔에서는 일반적으로 추가 조사에 사용하기 위해 네트워크에서 활성화된 다른 호스트 찾기만 시도합니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	호스트가 스캔 중이었던 항목을 확인하십시오. 이 스캔은 ICMP 기반 스캔이므로 기본적으로는 UDP 또는 TCP 스캔에서와같이 스캔의 대상인 특정 서비스가 아니라 스캔되고 있었던 호스트만 확인하면 됩니다. 이벤트의 소스는 클라이언트 호스트 또는 서버 호스트이고, 기간은 이벤트 날짜이며, 프로토콜은 ICMP인 플로우 쿼리를 수행하면 이러한 호스트를 조사할 수 있습니다. 피어의 IP 또는 호스트 그룹을 기준으로 결과를 정렬하여 호스트에 스캔되는 중인 패턴이 있는지 확인해 봅니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PING_ADDR_SCAN (277)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

포트 스캔

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	포트 스캔에서는 단일 호스트가 다른 호스트에 연결할 때 사용하는 1024 포트의 수를 계산합니다. 구성 가능한 임계값을 초과하면 이벤트가 트리거됩니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 호스트가 다른 호스트의 '포트 스캔'을 수행 중인 것으로 관찰되었다는 의미입니다. 즉, 스캔 중인 호스트가 스캔 대상인 호스트에서 제공할 수 있는 서비스를 식별하려고 시도하고 있습니다. 외부 호스트에서 이러한 시도를 하는 경우 이는 익스플로잇 시도의 전조 현상일 수 있습니다. 하지만 인터넷의 스캔은 정상적인 행동입니다. 스캔 중인 호스트가 내부 호스트인 경우 이러한 현상은 공격자나 보안이 침해된 호스트가 조직 네트워크 내부에서 이동을 시도하는 징후일 수 있습니다.
다음 단계는 무엇입니까?	이 보안 이벤트의 소스 호스트가 외부 호스트인 경우에는 스캔했던 호스트와 통신을 계속 진행했는지를 확인합니다. 이렇게 하려면 소스 및 대상 호스트 간의 플로우 쿼리를 엽니다. 소스 호스트와 네트워크 간의 모든 트래픽만 확인하는 방식도 유용할 수 있습니다. 이 호스트의 소스가 내부 호스트인 경우에는 플로우 쿼리를 사용하여 소스와 대상 간의 플로우를 보고 이러한 현상이 정상적인 행동인지를 확인합니다.

이 이벤트에 대한 질문	응답
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	없음
참고	없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	스캔을 수행 중인 호스트에서 포트 스캔을 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트
이 이벤트를 조정할 수 있습니까?	예
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	임계값 기반
기본값과 단위는 무엇입니까?	해당 없음
허용치	해당 없음
최소 임계값	해당 없음
최대 임계값	해당 없음

이벤트에 대한 질문	응답
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	조정 가능한 파라미터는 이벤트 발생에 필요한, 스캔되는 포트의 수이며 기본값은 10입니다.
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	해당 없음
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	스캔을 수행하는 호스트
대상은 무엇입니까?	스캔되는 호스트
어떤 정책에서 이벤트를 트리거합니까?	소스 호스트
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 웹 애플리케이션 UI에서는 세부사항 열에 'View details'(세부사항 보기)가 표시됩니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• 웹 애플리케이션 UI에서는 소스 호스트에 대한 보안 이벤트를 표시합니다. • SMC 클라이언트 인터페이스에는 아무 내용도 표시되지 않습니다.
연결된 플로우에 어떤 정보가 표시됩니까?	• 웹 애플리케이션 UI에서는 인터페이스에 아무 내용도 표시되지 않습니다. • SMC 클라이언트 인터페이스에서는 마지막 5분 동안 해당 플로우가 표시된 Flow Collector의 플로우가 표시됩니다.

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

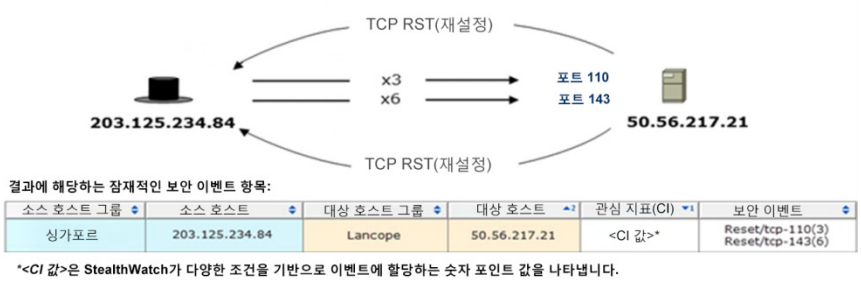
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_PORT_SCAN (55)
이벤트의 syslog 유형은 무엇입니까?	HostFlowAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostFlowAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

재설정/TCP

소스 호스트가 전송한 TCP 패킷이 대상 호스트에서 거부되었습니다. 이 보안 이벤트는 보통 애플리케이션 오작동 및 TCP 포트 스캔의 결과로 표시됩니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

재설정/TCP



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Reset/tcp-110(3) Reset/tcp-143(6)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

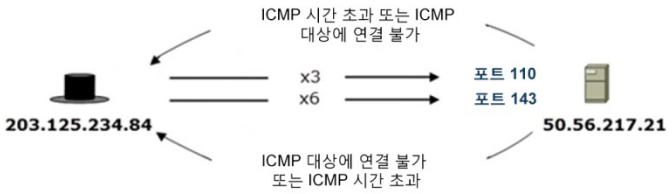
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TCP_PROBE (262)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

재설정/UDP

소스 호스트가 전송한 UDP 패킷이 대상 호스트에서 거부되었습니다. 이 보안 이벤트는 대개 ICMP 포트 연결 불가 보안 이벤트와 함께 발생합니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

재설정/UDP



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Reset/udp-110(3) Reset/udp-143(6)

***<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.**

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_PROBE (261)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

스캐너 통신

이 보안 이벤트는 네트워크를 스캔 중이었던 호스트가 이제는 스캔했던 대상 호스트 중 하나와 양방향 통신을 설정했음을 나타냅니다. 이 이벤트는 내부 호스트 정책 및 외부 호스트 정책에서 기본적으로 활성화됩니다. 그러나 네트워크 관리 및 스캐너 역할 정책에서는 기본적으로 비활성화됩니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_ADDR_SCAN_TALKING (63)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

느린 연결 플러드

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	호스트가 매우 낮은 패킷 속도의 대상에 다중 연결을 시작하는 중임을 나타냅니다. 이러한 연결은 많은 대역폭을 사용하지 않고도 열린 연결을 유지하기 위한 것입니다. 이러한 방식의 연결은 많은 양의 대역폭 없이도 서비스를 사용 불가 상태로 만들 수 있는 일종의 애플리케이션 DoS(denial-of-service) 공격 유형입니다. 이러한 방식을 사용하는 경우 취약한 호스트에 대해 공격을 더욱 쉽게 수행할 수 있으며, 해당 공격을 탐지하기도 더 어려운 경우가 많습니다.
다음 단계는 무엇입니까?	목표는 대상에 대한 연결이 정상적인지 그리고 대상이 성능 저하를 경험하는지 확인하는 것입니다. 이러한 연결은 두 개의 내부 호스트 간의 악의적인 행동일 수도 있지만, 내부 호스트와 외부 호스트 간의 연결을 나타내는 이벤트인 경우에는 처리하기 더 까다로울 가능성이 높습니다. 먼저 이벤트 날짜의 이벤트 소스와 대상 간에 플로우 쿼리를 실행합니다. 플로우 지속 여부를 기록합니다. 플로우가 지속되지 않으면 서비스 장애가 없으며 문제가 아닐 가능성이 있습니다. 소스 호스트와 대상 호스트 둘 다의 보안 이벤트 기록을 확인할 수도 있습니다. 소스 호스트에서 여러 대상에 대해 또는 이전에도 이 이벤트가 발생한 적이 있었다면 이는 추가 조사가 필요한 상황입니다. 대상 호스트에서 이전에는 이 이벤트가 발생하지 않았는데 현재는 여러 호스트가 동시에 이 이벤트를 트리거하는 경우 이는 DDoS(distributed denial-of-servce) 공격의 징후일 수 있습니다. 이전에도 이벤트가 발생했다면 서비스가 호스팅하는 애플리케이션의 정상 행동일 수도 있습니다. 이 경우 해당 특정 호스트에 대해 이벤트를 해제할 수 있습니다. Flow Sensor에서 관련 트래픽이 관찰된 경우에는 성능 보고서를 실행하여 트래픽의 특성으로 인해 SRT(Server Response Time, 서버 응답 시간)가 영향을 받았는지를 확인합니다. 이는 트래픽이 정상적인지를 나타낼 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 소스 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 Ddos 소스 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SLOW_CONNECTION_FLOOD (44)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

스팸 소스

소스 호스트가 이메일 스팸의 소스일 수 있습니다. 이메일당 허용되는 주소 수가 초과되었거나, 5분 동안 허용되는 수보다 많은 관련 알림이 생성되었기 때문입니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

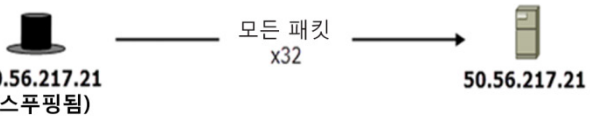
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SPAM_SOURCE (11)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

소스=대상

IP 데이터그램의 소스 호스트와 대상 호스트가 같습니다. 이 보안 이벤트는 대개 라우팅을 중단시키기 위해 작성된 패킷으로 인해 발생합니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

소스=대상



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	50.56.217.21	Lancope Corporate	50.56.217.21	<CI 값>*	소스=대상(32)

***<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.**

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	이상 징후 지표
값은 무엇입니까?	• 이상 징후 지표: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_BOOMERANG (273)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

SSH 역방향 셸

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 보안 이벤트 알람은 역방향 SSH 셸을 찾기 위한 것입니다. 공격자는 아웃바운드 SSH 연결처럼 보이는 연결을 통해 보안이 침해된 네트워크에 대한 온디맨드 액세스를 설정하는 방법으로 SSH 역방향 셸을 사용할 수 있습니다. 이 연결을 설정한 공격자는 수신 연결이 방화벽 등으로 차단되더라도 시스템에 계속 액세스할 수 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	이 보안 이벤트를 조사할 때는 대개 내부 네트워크에서 전체적으로 소스 호스트의 역할을 유지해야 합니다. 해당 호스트의 공식적인 용량을 제공하는 디바이스가 SSH 또는 SFTP 서버인 경우에는 알람이 잘못된 것일 수 있으며, 해당 디바이스에서 이러한 알람을 제한하기 위해 추가로 호스트 정책을 조정해야 할 수 있습니다. 그러나 내부 호스트에 디바이스 등의 명확한 용량을 제공하는 항목이 없다면 해당 외부 호스트의 ID를 설정해야 합니다. 디바이스가 알려진 엔티티의 소유인지를 확인하십시오. 알려진 엔티티가이 디바이스를 소유한 경우에는 알람이 잘못 생성되었을 수 있습니다. 엔티티가 알려져 있지 않은 경우, 대상 호스트에서 Top Peers(상위 피어)(아웃바운드) 보고서를 실행합니다. 이 보고서는 외부 호스트와 통신한 내부 피어의 목록을 데이터의 양을 기준으로 정렬하여 제공합니다. 이 목록은 사용자 환경 내에서 매우 일반적인 피어인지를 표시하며 이 행동이 예상되는지 확인하는 데 잠재적으로 도움을 줄 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

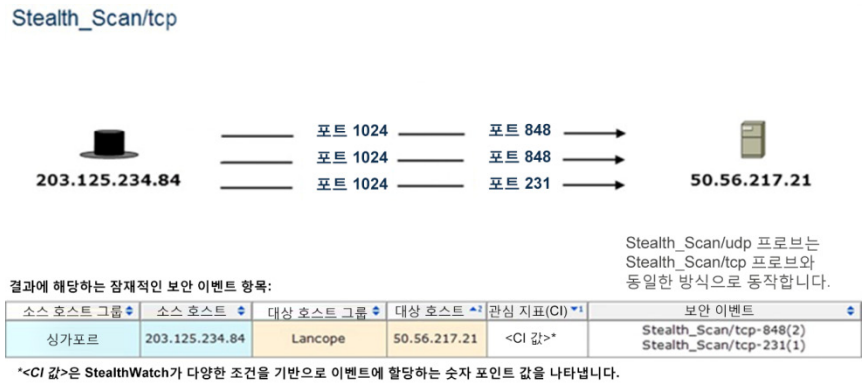
이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SSH_REV_SHELL (61)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Stealth_Scan/tcp

소스 호스트가 동일한 소스 포트를 사용하여 대상 호스트의 서로 다른 여러 포트에 동시에 연결했습니다. 이 행동은 애플리케이션이 원시 소켓을 사용하여 TCP 또는 UDP 연결을 생성했음을 나타냅니다. 이 보안 이벤트에는 해당 이벤트를 확인하기 전에 마지막으로 액세스한 대상 포트가 표시됩니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.



어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	'1' 정책: 상위 관심 지표(CI) *'8000' 정책: 상위 정찰 지표, 상위 관심 지표(CI)*
값은 무엇입니까?	'1' 정책: • CI: 참 '8000' 정책: • 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	'1' 정책: 상위 대상 지표 *'8000' 정책: 상위 대상 지표*
값은 무엇입니까?	'1' 정책: • TI: 참 '8000' 정책: • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TCP_STEALTH (272)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

Stealth_Scan/udp

소스 호스트가 포트 번호를 재사용한, 조작된 UDP 스캔이 탐지되었습니다. 이 이벤트는 공격할 호스트를 찾고 있을 수 있는 스캔 호스트가 '패킷 조작'을 수행 중임을 나타내는 경우가 많습니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)*	보안 이벤트
싱가포르	203.125.234.84	Lancope	50.56.217.21	<CI 값>*	Stealth_Scan/udp-5000(2) Stealth_Scan/udp-5001(2)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	'1' 정책: 상위 관심 지표(CI) *'8000' 정책: 상위 정찰 지표, 상위 관심 지표(CI)*
값은 무엇입니까?	'1' 정책: • CI: 참 '8000' 정책: • 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	'1' 정책: 상위 대상 지표 *'8000' 정책: 상위 대상 지표*
값은 무엇입니까?	'1' 정책: • TI: 참 '8000' 정책: • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_STEALTH (271)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

의심스러운 데이터 호딩

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	의심스러운 데이터 호딩은 내부 호스트가 클라이언트 역할을 하는 동안 재설정 기간에 다른 내부 호스트에서 다운로드하는 TCP/UDP 데이터의 양을 모니터링합니다. 이 데이터의 양이 지정된 호스트의 임계값을 초과하면 이벤트가 발생합니다. 이 임계값은 기준을 적용하여 자동으로 작성할 수도 있고 수동으로 설정할 수도 있습니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 특정 호스트가 데이터 유출을 준비하기 위해 데이터를 수집하고 있음을 나타낼 수도 있고, 기타 비정상적으로 많은 양의 내부 데이터 다운로드를 나타낼 수도 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	다운로드된 데이터의 양과 해당 데이터가 다운로드된 소스 위치를 확인하십시오. 이러한 정보를 조사하는 가장 좋은 방법은 Top Peers(상위 피어)(인바운드) 보고서를 실행하는 것입니다. 쿼리의 기간을 이벤트 날짜로 설정합니다. *Client(클라이언트)* 또는 *Server Host(서버 호스트)*를 보안 이벤트의 소스 IP로 지정하고 *Other Host(기타 호스트)*를 Inside Hosts(내부 호스트) 호스트 그룹으로 지정하도록 보고서를 필터링합니다. 이렇게 하면 대부분의 데이터를 전송한 주요 피어를 찾을 수 있습니다. 주요 피어를 찾은 후에는 해당 피어에서 관찰된 양의 데이터를 전송하는 현상이 정상적인 행동인지를 확인합니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	해당 없음
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	Inside Host(내부 호스트) 호스트 그룹에서 이벤트를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	방화벽, 프록시 및 NAT 디바이스
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음

이벤트에 대한 질문	응답
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 방화벽, 프록시 및 NAT 디바이스
이 이벤트를 조정할 수 있습니까?	예
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	차이 또는 임계값 기반.
기본값과 단위는 무엇입니까?	
허용치	92
최소 임계값	24시간 내 클라이언트 페이로드 바이트 500M.
최대 임계값	24시간 내 다운로드한 페이로드 바이트 1T.
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	이벤트는 기준이나 허용치를 고려하지 않은 특정 바이트 수에서 트리거되도록 설정할 수 있습니다.
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	아니요
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	아니요
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	페이로드 데이터를 수신 중인 내부 호스트.
대상은 무엇입니까?	페이로드 데이터를 전송 중인 하나 이상의 내부 호스트.
어떤 정책에서 이벤트를 트리거합니까?	소스의 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 데이터 호딩 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 데이터 호딩 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	웹 애플리케이션 인터페이스: 4.02G 포인트가 관찰되었습니다. 정책 최대값은 최대 30만 개의 포인트를 허용합니다. SMC 클라이언트 인터페이스: 4.02G 포인트가 관찰되었습니다. 정책 최대값은 최대 30만 개의 포인트를 허용합니다. 더블 클릭하여 자세한 내용을 확인할 수 있습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	웹 애플리케이션 인터페이스: 소스 호스트 IP에 대한 Security Events Details(보안 이벤트 세부사항)로 이동하여 발견된 이벤트가 있으면 나열합니다. SMC 클라이언트 인터페이스: 소스 호스트 IP에서 필터링된 Security Events(보안 이벤트) 탭을 열고 발견된 이벤트가 있으면 나열합니다.
연결된 플로우에 어떤 정보가 표시됩니까?	웹 애플리케이션 인터페이스: Dragon squad의 텍스트로 대체합니다. SMC 클라이언트 인터페이스: Dragon squad의 텍스트로 대체합니다.

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SUSPECT_DATA_HOARD (315)
이벤트의 syslog 유형은 무엇입니까?	HostVarianceAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostVarianceAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

의심스러운 데이터 손실

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	클라이언트 역할을 하는 내부 호스트가 외부 호스트에 일정량 누적된 TCP 또는 UDP 페이로드 데이터를 업로드했는데 누적된 데이터의 양이 내부 호스트에 적용된 정책에 설정되어 있는 임계값을 초과하는 경우 이 이벤트가 트리거됩니다. 이 이벤트를 차이 기반 알람으로 사용할 수 있습니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	호스트가 허용되는 것보다 많은 정보를 인터넷에 업로드하는 데 사용되고 있습니다. 누군가가 외부 백업 서비스를 사용 중인 것일 수도 있고, 기업 데이터를 악의적으로 유출하고 있는 것일 수도 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	업로드된 데이터의 양과 해당 데이터 중 대부분이 전송된 위치를 확인하십시오. 이러한 정보를 확인하는 가장 좋은 방법은 보안 이벤트의 소스였던 호스트에서 Top Peers(상위 피어)(아웃바운드) 보고서를 실행하는 것입니다. 클라이언트를 이벤트의 소스로 지정하고 서버 호스트 그룹을 *Outside Hosts(외부 호스트)*로 지정하도록 보고서를 필터링합니다. 이렇게 하면 대부분의 데이터를 수신한 주요 피어를 찾을 수 있습니다. 주요 피어를 찾은 후에는 해당 피어에서 관찰된 양의 데이터를 수신하는 현상이 정상적인 행동인지를 확인합니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	아니요
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	소스와 대상 호스트 둘 다에 적용된 정책에서 이 이벤트를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	방화벽, 프록시 및 NAT 디바이스, 게스트 무선, 메일 서버 정책, 신뢰할 수 있는 인터넷 호스트
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	내부 호스트, 외부 호스트, 클라이언트 IP 정책
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	방화벽, 프록시 및 NAT 디바이스, 게스트 무선, 메일 서버 정책, 신뢰할 수 있는 인터넷 호스트

이벤트에 대한 질문	응답
이 이벤트를 조정할 수 있습니까?	예
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	차이 또는 임계값 기반
기본값과 단위는 무엇입니까?	
허용치	50
최소 임계값	24시간 내 클라이언트 페이로드 바이트 1G
최대 임계값	24시간 내 클라이언트 페이로드 바이트 100G
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	이벤트는 기준이나 허용치를 고려하지 않은 특정 바이트 수에서 트리거되도록 설정할 수 있습니다.
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	해당 없음
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음
이벤트에 기본 완화 기능이 있습니까?	아니요
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	페이로드 데이터를 전송 중인 클라이언트 역할을 하는 내부 호스트.
대상은 무엇입니까?	내부 호스트에서 페이로드 데이터를 수신 중인 하나 이상의 외부 호스트.
어떤 정책에서 이벤트를 트리거합니까?	소스의 정책

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 유출 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 유출 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	• 3.54G의 포인트가 관찰되었습니다. • 정책 최대값은 최대 3만 개의 포인트를 허용합니다. 더블 클릭하여 자세한 내용을 확인할 수 있습니다.
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	• SMC 웹 애플리케이션 UI에서 Security Events Details(보안 이벤트 세부사항) 페이지가 소스 호스트 IP에 대해 표시됩니다. 이 페이지는 발견된 이벤트가 있으면 나열합니다. • SMC 클라이언트 인터페이스에서 Security Events(보안 이벤트) 테이블을 엽니다. 이 테이블은 소스 호스트 IP에서 필터링되어 있으며 발견된 이벤트가 있으면 나열합니다.

이벤트에 대한 질문	응답
연결된 플로우에 어떤 정보가 표시됩니까?	SMC 클라이언트 인터페이스에서 연결된 플로우에는 다음 기준을 충족하는 모든 플로우가 표시됩니다. • 자정부터 현재까지의 시간 • 클라이언트 호스트의 IP가 이벤트 소스 IP와 같음 • 서버 호스트가 외부 호스트 그룹을 포함함 • 프로토콜이 TCP 또는 UDP임 • 총 바이트 수가 1000 이상임 • 클라이언트 바이트 수가 1 이상임

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_DATA_LOSS (40)
이벤트의 syslog 유형은 무엇입니까?	HostVarianceAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	HostVarianceAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

의심스러운 긴 플로우

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 보안 이벤트는 원격 데스크톱 기술과 VPN에서 사용하는 것과 같은, 오랫동안 설정되어 있는 연결을 탐지할 뿐만 아니라 스파이웨어, IRC 봇넷 및 기타 은폐 통신 수단 등의 통신 채널도 탐지합니다. 이 이벤트 자체가 반드시 악의적인 행동이나 보안 침해를 나타내는 것은 아니지만, 확인이 필요한 호스트를 식별하는 데는 도움이 됩니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	목표는 이 트래픽이 정상적인 활동을 나타내는지 확인하는 것입니다. 트래픽 대상을 식별함으로써 이 작업을 자주 수행할 수 있습니다. 먼저 보안 이벤트의 연결된 플로우 테이블로 피벗하여 소스 및 대상 IP 주소, 포트, 서비스, 플로우 시작 시간, 지리 위치 정보, 사용자 이름(제공되는 경우) 등의 자세한 플로우 세부사항을 확인하는 것이 좋습니다. 대상이 외부 호스트인 경우에는 외부 조회를 실행하여 IP 소유자를 확인합니다. 대상이 알려진 비즈니스 파트너 또는 신뢰할 수 있는 네트워크인 경우에는 해당 그룹으로 대상을 분류해야 합니다. 호스트에 대한 외부 조회만으로는 호스트를 식별할 수 없는 경우, Top Peers(상위 피어) 보고서를 실행하여 대상과 통신하는 기타 호스트를 식별해 유사한 행동을 파악합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SUSPECT_LONG_FLOW (33)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

의심스러운 조용한 긴 플로우

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 보안 이벤트는 특정 유형의 C&C(command and control) 활동에서 사용되는 하트비트 연결뿐만 아니라 스파이웨어, IRC 봇넷 및 기타 은폐 통신 수단 등의 다른 의심스러운 통신 채널도 식별합니다. 이 이벤트는 적은 용량의 데이터가 전송되는 경우 양방향 통신이 포함된다는 점을 제외하고는 비콘 호스트와 유사합니다. 이 이벤트는 배경 웹사이트 하트비트도 확인할 수 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	목표는 이 트래픽이 정상적인 활동을 나타내는지 확인하는 것입니다. 트래픽 대상을 식별함으로써 이 작업을 자주 수행할 수 있습니다. 먼저 보안 이벤트의 연결된 플로우 테이블로 피벗하여 소스 및 대상 IP 주소, 포트, 서비스, 플로우 시작 시간, 지리 위치 정보, 사용자 이름(제공되는 경우) 등의 자세한 플로우 세부사항을 확인하는 것이 좋습니다. 대상이 외부 호스트인 경우에는 외부 조회를 실행하여 IP 소유자를 확인합니다. 대상이 알려진 비즈니스 파트너 또는 신뢰할 수 있는 네트워크인 경우에는 해당 그룹으로 대상을 분류해야 합니다. 호스트에 대한 외부 조회만으로는 호스트를 식별할 수 없는 경우, Top Peers(상위 피어) 보고서를 실행하여 대상과 통신하는 기타 호스트를 식별해 유사한 행동을 파악합니다. 또한, Flow Traffic(플로우 트래픽) 보고서를 실행하여 의심스러운 트래픽 패턴을 시각화할 수도 있습니다. C&C 서버로의 하트비트에서는 바이트 전송량이 낮은 주기적 패턴이 나타납니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 C&C(Command And Control) 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 C&C(Command And Control) 지표: 참 • CI: 참

이벤트에 대한 질문	응답
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_QUIET_LONG_DURATION_FLOW (48)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

의심스러운 UDP 활동

소스 호스트가 UDP 포트에서 여러 호스트를 스캔했으며 이전에 스캔했던 다른 호스트로 대형 UDP 패킷을 전송했음이 확인되었습니다. 이러한 유형의 행동은 'SQL Slammer' 및 'Witty'와 같은 대다수 단일 패킷 UDP 기반 웜에서 일관되게 나타납니다. 이 보안 이벤트는 즉시 조사해야 합니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SUSPECT_UDP_ACTIVITY (24)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

SYN 플러드

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	즉, 소스 호스트가 DoS 공격에 사용되고 있거나(호스트 보안이 침해되었거나 사용자가 공격을 진행했을 수 있음), 네트워크 애플리케이션이 잘못 구성되었음을 나타냅니다. 대부분의 SYN 패킷은 더욱 규모가 큰 DDoS(distributed denial-of-service) 공격의 일부분으로 대상의 대역폭을 소비하기 위해 전송되는 경우가 많습니다. 그러나 애플리케이션이 TCP 연결을 설정하지 못하여 매우 빠른 속도로 연결을 다시 설정하려는 경우일 수도 있습니다. IP 수는 많은 데 비해 패킷 수는 적은 것도 정찰의 징후일 가능성이 높습니다.
다음 단계는 무엇입니까?	전송되는 SYN의 양과 전송 속도, 전송된 시간, 전송 대상을 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 소스 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 SYN 패킷이 전송된 위치를 찾습니다. 이벤트의 주체가 SYN이 많이 전송되는 플로우의 클라이언트 호스트인 경우 Client SYN Packets(클라이언트 SYN 패킷), Client Packets(클라이언트 패킷) 또는 Client Packet Rate (pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 잘못된 컨피그레이션으로 인한 것인지를 확인합니다. 내부에서 내부로의 SYN 플러드는 잘못된 컨피그레이션으로 인한 경우가 많으며, 내부에서 외부로의 SYN 플러드도 경우에 따라 잘못된 컨피그레이션으로 인해 발생할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 소스 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 Ddos 소스 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SYN_FLOOD (5)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

SYN 수신됨

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 대상 호스트가 DoS 공격의 대상이 되었거나 네트워크 애플리케이션이 잘못 구성되었음을 나타냅니다. 대부분의 SYN 패킷은 더욱 규모가 큰 DDoS 또는 DoS 공격의 일부분으로 대상의 대역폭을 사용하기 위해 전송되는 경우가 많습니다. 그러나 애플리케이션이 TCP 연결을 설정하지 못하여 매우 빠른 속도로 연결 재설정을 시도하는 것일 수도 있습니다.
다음 단계는 무엇입니까?	전송되는 SYN의 양과 전송 속도, 전송된 시간, 전송 출처를 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 대상 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 SYN 패킷 전송이 시작된 위치를 찾습니다. 이벤트의 대상이 SYN이 많이 전송되는 플로우의 서버 호스트인 경우 Client SYN Packets(클라이언트 SYN 패킷), Client Packets(클라이언트 패킷) 또는 Client Packet Rate (pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 컨피그레이션이 잘못되었는지를 확인합니다. 내부에서 내부로의 SYN 플러드는 잘못된 컨피그레이션으로 인한 경우가 많습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_SYNS_RECEIVED (19)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

가상 호스트와의 통신

이 호스트는 이전에 확인된 적이 없으며 응답하지 않는 다른 호스트와 통신하고 있습니다.

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	컴퓨터가 존재하지 않는 호스트에 원치 않는 트래픽 전송을 시도하는 경우는 거의 없으므로 이러한 활동에 사용되는 호스트는 확인해 보아야 합니다. 해당 활동은 누군가 정찰 수행을 시도하고 있다는 징후일 수도 있지만, 존재하지 않는 호스트와 통신하도록 호스트가 잘못 구성된 것일 수도 있습니다.
다음 단계는 무엇입니까?	이 보안 이벤트는 조사하기가 다소 까다로울 수 있습니다. 현재는 '가상' 호스트를 플로우 쿼리의 일부분으로 지정할 수 없기 때문입니다. 하지만 그와 유사한 조사를 수행할 수는 있습니다. 이 조사에서는 응답하지 않는 호스트로 전송된 플로우를 찾은 다음 플로우 간의 공통 스레드에서 의미를 도출합니다. 단방향 플로우를 찾습니다. 시간 범위가 보안 이벤트 날짜인 플로우 쿼리를 작성합니다. 클라이언트 호스트를 보안 이벤트의 소스 IP로 지정하고, 서버 호스트는 임의의 IP로 설정합니다. Traffic(트래픽) 탭에서 서버 패킷 수가 0개 이하가 되도록 필터링합니다.* 이러한 플로우 간의 공통 스레드를 찾습니다. 예를 들어 플로우가 모두 동일한 서버 포트로 이동했는지, 모든 플로우가 대략 비슷한 시간에 발생했는지, 이전에 있었던 호스트로 전송되었는지, 호스트의 수는 몇 개였는지 등을 확인해 볼 수 있습니다. * 모든 정보를 캡처하려면 이벤트 소스를 플로우 쿼리의 서버로 설정하고 클라이언트 패킷 수를 0개 이하로 설정하여 이 쿼리를 반복해야 합니다. 이렇게 해도 추가적인 결과가 매우 빈번하게 생성될 가능성은 거의 없습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TALKS_TO_PHANTOMS (59)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

표적 데이터 호딩

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 찾고 있는 행동의 유형은 무엇입니까?	표적 데이터 호딩은 내부 호스트가 서버 역할을 하는 동안 재설정 기간에 다른 내부 호스트에 제공하는 TCP/UDP 데이터의 양을 모니터링합니다. 이 데이터의 양이 지정된 호스트의 임계값을 초과하면 이벤트가 발생합니다. 이 임계값은 기준을 적용하여 자동으로 작성할 수도 있고 수동으로 설정할 수도 있습니다.
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 하나 이상의 내부 호스트가 데이터 유출이나 오용을 준비하기 위해 특정 내부 호스트에서 비정상적으로 많은 데이터를 수집 중임을 나타낼 수 있습니다.
다음 단계는 무엇입니까?	전송된 데이터의 양과 해당 데이터 중 대부분이 전송된 위치를 확인하십시오. 이러한 정보를 확인하는 가장 좋은 방법은 보안 이벤트의 소스였던 호스트에서 Top Peers(상위 피어)(아웃바운드) 보고서를 실행하는 것입니다. *Client(클라이언트)* 또는 *Server Host(서버 호스트)*를 보안 이벤트의 대상 IP로 지정하고 *Other Host(기타 호스트)*를 Inside Hosts(내부 호스트) 호스트 그룹으로 지정하도록 보고서를 필터링합니다. 이렇게 하면 업로드된 데이터 중 대부분을 수신한 주요 피어를 찾을 수 있습니다. 주요 피어를 찾은 후에는 해당 피어에서 관찰된 양의 데이터를 수신하는 현상이 정상적인 행동인지를 확인합니다.
비표준 플로우 데이터가 필요합니까? (FlowSensor, 프록시, 방화벽 등)	해당 없음
참고	해당 없음

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정책 설정이 이 보안 이벤트를 트리거하는 데 필요합니까?	Inside Host(내부 호스트) 호스트 그룹에서 이벤트를 활성화해야 합니다.
어떤 정책에서 기본적으로 이 이벤트가 켜져 있습니까?	내부 호스트, 외부 호스트
어떤 정책에서 기본적으로 이 이벤트가 꺼져 있습니까?	방화벽, 프록시 및 NAT 디바이스
어떤 정책에서 기본적으로 이 알람이 켜져 있습니까?	없음
어떤 정책에서 기본적으로 이 알람이 꺼져 있습니까?	내부 호스트, 외부 호스트, 방화벽, 프록시 및 NAT 디바이스
이 이벤트를 조정할 수 있습니까?	예
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	차이 또는 임계값 기반.
기본값과 단위는 무엇입니까?	
허용치	92
최소 임계값	24시간 내 클라이언트 페이로드 바이트 500M.
최대 임계값	24시간 내 다운로드한 페이로드 바이트 1T.
차이 기반이 아닌 파라미터를 사용하여 이벤트를 조정할 수 있습니까?	예
가능한 경우, 조정 가능한 특성 및 단위는 무엇입니까?	이벤트는 기준이나 허용치를 고려하지 않은 특정 바이트 수에서 트리거되도록 설정할 수 있습니다.
일반 정책 편집기 외부에서 이벤트를 조정할 수 있습니까?	아니요
가능한 경우, 조정 가능한 값의 대체 위치는 어디입니까?	해당 없음

이벤트에 대한 질문	응답
이벤트에 기본 완화 기능이 있습니까?	아니요
있는 경우, 어떤 기능입니까?	해당 없음

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이벤트의 소스는 무엇입니까?	페이로드 데이터를 전송 중인 내부 호스트.
대상은 무엇입니까?	페이로드 데이터를 수신 중인 하나 이상의 내부 호스트.
어떤 정책에서 이벤트를 트리거합니까?	소스의 정책
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 데이터 호딩 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 데이터 호딩 지표: 참 • TI: 참

어떤 정보를 이 이벤트에 대한 Stealthwatch System 사용자 인터페이스에서 사용할 수 있습니까?

이벤트에 대한 질문	응답
어떤 정보가 알람 세부사항에 표시됩니까?	웹 애플리케이션 인터페이스: 4.02G 포인트가 관찰되었습니다. 정책 최대값은 최대 30만 개의 포인트를 허용합니다. SMC 클라이언트 인터페이스: 4.02G 포인트가 관찰되었습니다. 정책 최대값은 최대 30만 개의 포인트를 허용합니다. 더블 클릭하여 자세한 내용을 확인할 수 있습니다.

이벤트에 대한 질문	응답
알람 세부사항을 클릭하면 무슨 일이 발생합니까?	웹 애플리케이션 인터페이스: 소스 호스트 IP에 대한 Security Events Details(보안 이벤트 세부사항)로 이동하여 발견된 이벤트가 있으면 나열합니다. SMC 클라이언트 인터페이스: 소스 호스트 IP에서 필터링된 Security Events(보안 이벤트) 탭을 열고 발견된 이벤트가 있으면 나열합니다.
연결된 플로우에 어떤 정보가 표시됩니까?	SMC 클라이언트 인터페이스에서 연결된 플로우에는 다음 기준을 충족하는 모든 플로우가 표시됩니다. • Time Period(기간): Today(오늘) • Server Host(서버 호스트): Event Source IP(이벤트 소스 IP) • Other Host(기타 호스트): Inside Hosts(내부 호스트) • Protocol(프로토콜): TCP 또는 UDP • Total Bytes(총 바이트 수): >=1000 • Server Bytes(서버 바이트 수): >=1

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

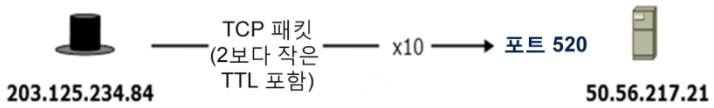
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TARGET_DATA_HOARD (316)
이벤트의 syslog 유형은 무엇입니까?	HostVarianceAlarm입니다. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	hostVarianceAlarmCondition입니다. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

시간 초과/TCP

소스 호스트가 TTL이 2 미만인 TCP 패킷을 전송했습니다. 트레이스라우트(traceroute)는 UDP를 통해 수행되므로 TTL이 짧은 TCP 패킷은 대개 악의적인 활동(예: 파이어워킹(firewalking))이나 네트워크 손상(예: 라우팅 루프)을 나타냅니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

시간 초과/TCP



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	시간 초과/tcp-520(10)

**<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.*

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

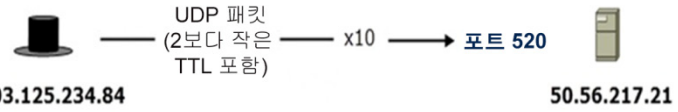
이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TCP_TO (260)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

시간 초과/UDP

소스 호스트가 TTL이 2 미만인 UDP 패킷을 전송했습니다. 트레이스라우트(traceroute)는 UDP를 통해 수행되므로 이 보안 이벤트는 매우 흔히 발생할 수 있습니다. 그러나 이 이벤트가 많이 발생하는 현상은 네트워크 손상(예: 라우팅 루프)을 나타내는 것일 수 있습니다. Norton Antivirus 서버를 허용하기 위해 포트 38293은 UDP 시간 초과에서 제외됩니다.

참고: 완화 기능은 이 보안 이벤트와 연결된 알람에 사용할 수 없습니다.

시간 초과/UDP



결과에 해당하는 잠재적인 보안 이벤트 항목:

소스 호스트 그룹	소스 호스트	대상 호스트 그룹	대상 호스트	관심 지표(CI)	보안 이벤트
싱가포르	203.125.234.84	Lancope Corporate	50.56.217.21	<CI 값>*	시간 초과/udp-520(10)

*<CI 값>은 StealthWatch가 다양한 조건을 기반으로 이벤트에 할당하는 숫자 포인트 값을 나타냅니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_TO (259)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

연결됨

알람이 발생한 호스트(상위 관심 지표(CI) 알람 또는 트랩된 호스트 보안 이벤트가 발생한 호스트)에서 대상 호스트와의 연결을 시작했으며 데이터를 교환했습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 대상 지표
값은 무엇입니까?	• 공격 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TOUCHED (28)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

트랩된 호스트

호스트가 한 달에 트랩된 호스트 알림을 수신할 수 있는 일수가 초과되었습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정찰 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정찰 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_TRAPPED_HOST (34)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

UDP 플러드

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	즉, 소스 호스트가 DoS 공격에 사용되고 있거나(호스트 보안이 침해되었거나 사용자가 공격을 진행했을 수 있음), 네트워크 애플리케이션이 잘못 구성되었거나, 소스에서 전송되는 초당 UDP 패킷의 수가 비정상적으로 많은 연결을 사용 중임을 나타냅니다. 대부분의 패킷은 더욱 규모가 큰 DDoS 공격의 일부분으로 대상의 대역폭을 사용하기 위해 전송되는 경우가 많습니다. 하지만 높은 UDP 패킷 속도는 높은 SYN 패킷 속도보다 일반적으로 나타나는 현상이므로 임계값 또는 허용치 설정이 낮으면 오탐 항목이 대량으로 발생할 수 있습니다. IP는 많은 데 비해 패킷 수는 적은 것도 정찰의 징후일 가능성이 높습니다.
다음 단계는 무엇입니까?	전송되는 UDP 패킷의 양과 전송 속도, 전송된 시간, 전송 대상을 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 소스 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 프로토콜 필터를 *UDP only(UDP 전용)*로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 UDP 패킷이 전송된 위치를 찾습니다. 이벤트의 주체가 UDP가 많이 전송되는 플로우의 클라이언트 호스트인 경우 Client Packets(클라이언트 패킷) 또는 Client Packet Rate (pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다. 정상적인 행동의 예로는 UDP를 사용한 웹 서버로의 업로드(Google에서 흔히 사용하는 방식) 또는 UDP 기반 VPN 연결 등이 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 소스 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 Ddos 소스 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_FLOOD (6)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

수신된 UDP

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 이벤트는 대상 호스트가 DoS 공격의 대상이 되었거나, 네트워크 애플리케이션이 잘못 구성되었거나, 연결에 소스로부터 전송되는 초당 UDP 패킷 수가 비정상적으로 많음을 나타냅니다. 대부분의 패킷은 더욱 규모가 큰 DDoS 공격의 일부분으로 대상의 대역폭을 사용하기 위해 전송되는 경우가 많습니다. 하지만 높은 UDP 패킷 속도는 높은 SYN 패킷 속도보다 일반적으로 나타나는 현상이므로 임계값 또는 허용치 설정이 낮으면 오탐 항목이 대량으로 발생할 수 있습니다.
다음 단계는 무엇입니까?	수신되는 UDP 패킷의 양과 수신 속도, 수신된 시간, 전송 출처를 확인하십시오. 이 정보를 조사하는 가장 좋은 방법은 대상 호스트에 대해 플로우 쿼리를 수행하는 것입니다. 쿼리 시작 시간은 관련 보안 이벤트 시작 시간 5분 전으로 설정하고 종료 시간은 알람(있는 경우)의 종료 시간으로 설정합니다. 프로토콜 필터를 *UDP only(UDP 전용)*로 설정합니다. 결과가 반환되면 검색한 기간 중 대부분의 UDP 패킷 전송이 시작된 위치를 찾습니다. 이벤트의 대상이 UDP가 많이 전송되는 플로우의 서버 호스트인 경우 Client Packets(클라이언트 패킷) 또는 Client Packet Rate (pps)(클라이언트 패킷 속도(pps))를 기준으로 이벤트를 정렬할 수 있습니다. 이렇게 하면 주요 플로우를 찾을 수 있습니다. 주요 플로우를 찾은 후 해당 현상이 정상적인 행동인지를 확인합니다. 정상적인 행동의 예로는 UDP 기반 VPN 연결 등이 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 Ddos 대상 지표, 상위 대상 지표
값은 무엇입니까?	• 상위 Ddos 대상 지표: 참 • TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_UDP_RECEIVED (49)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

호스트 감시 활성화

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 특정 호스트가 통신 중임이 관찰되면 알림을 제공하는 사용자 구성 이벤트입니다. 이벤트의 의미는 사용자가 감시 목록에 특정 호스트를 포함하기로 결정한 이유에 따라 달라질 수 있지만, 대개 모니터링하는 호스트와의 통신이 부적절하다는 징후입니다.
다음 단계는 무엇입니까?	이 보안 이벤트의 조사 단계는 전적으로 호스트가 감시 목록에 추가된 상황에 따라 달라집니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_WATCH_LIST (31)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

포트 감시 활성화

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 특정 호스트가 특정 포트를 통해 통신 중임이 관찰되면 알림을 제공하는 사용자 구성 이벤트입니다. 이벤트의 의미는 사용자가 감시 목록에 특정 호스트를 포함하기로 결정한 이유에 따라 달라질 수 있지만, 대개 모니터링하는 호스트와의 통신이 부적절하다는 징후입니다.
다음 단계는 무엇입니까?	이 보안 이벤트의 조사 단계는 전적으로 포트가 감시 목록에 추가된 상황에 따라 달라집니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	상위 정책 위반 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 상위 정책 위반 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_WATCH_PORT (13)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

웜 활동

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이 보안 이벤트는 호스트가 여러 내부 네트워크에서 과도한 정찰을 수행 중인 것으로 보임을 나타냅니다. 이러한 현상은 보안이 침해된 호스트가 네트워크 전체에 걸쳐 감염 항목 전파를 시도하고 있음을 나타낼 수 있습니다.

이 이벤트에 대한 질문	응답
다음 단계는 무엇입니까?	이 이벤트는 빈번하게 발생할 수 있으며, 이벤트가 실제 문제를 나타내는지는 대개 네트워크 스캐너가 식별되어 네트워크 스캐너 호스트 그룹에 얼마나 잘 배치되었는지에 따라 달라집니다. 네트워크 스캐너가 적절하게 식별 및 배치되면 이러한 디바이스는 웜 활동을 비활성화하는 정책을 상속합니다. 웜 활동의 비활성화 여부는 대개 서로 다른 논리적 /24 범위에서 수행되는 유사 포트에 대한 호스트 스캔에 따라 결정됩니다. 먼저 Top Ports(상위 포트)(아웃바운드) 보고서를 실행합니다. 이벤트 날짜까지의 기간과 이벤트의 소스 IP로 사용할 클라이언트 호스트를 설정합니다. 나열되는 대상 IP 범위와 관계없이 모든 유형의 호스트를 스캔할 수 있으므로 내부 호스트나 외부 호스트 중 하나를 검색할지 아니면 둘 다 검색할지를 결정합니다. Filter(필터) 대화 상자의 Hosts(호스트) 탭에서 Server(서버) 필터를 적절하게 설정하고 Advanced(고급) 탭에서 'Order the records returned by'(반환되는 기록 순서 지정 기준)를 Flows(플로우)로 설정합니다. 피어별로 결과를 정렬합니다. 플로우 또는 피어를 기준으로 정렬한 목록 맨 위에서부터 시작하여 해당 범위에 속하지 않거나 숫자가 비정상적으로 높은 포트를 찾습니다. 원하는 IP 주소를 마우스 오른쪽 버튼으로 클릭하면 플로우로 피벗해 다양한 IP 주소를 확인하고 특정 호스트 그룹이 기본 대상으로 지정된 그룹인지를 확인할 수 있습니다. 또한, 마우스 오른쪽 버튼을 클릭하여 Top Peers(상위 피어) 보고서로 피벗한 다음 대상 전체에 걸쳐 트래픽이 전반적으로 동일하게 분산되는지를 확인할 수도 있습니다. 스캔에 응답한 호스트의 백분율을 확인하는 것도 도움이 됩니다. 이 시점이 되면 호스트가 스캔 중이었던 대상과 스캔 대상이었던 포트를 확인할 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	
값은 무엇입니까?	

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_WORM_ACTIVITY (35)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

웜 전파

보안 이벤트는 무엇입니까?

이 이벤트에 대한 질문	응답
이 이벤트가 트리거될 때 의미하는 바는 무엇입니까?	이는 다음과 같은 일련의 이벤트와 관련이 있습니다. 1) 호스트가 여러 호스트를 스캔하는 과정 중인 다른 호스트에 의해 스캔됩니다. 2) 방금 스캔된 호스트가 이제 다른 호스트 스캔을 시작합니다. 이 첫 번째 호스트에서는 보안이 침해된 다른 호스트에 의해 보안이 침해되었으며 이제는 다른 호스트의 보안 침해를 시도하고 있는 호스트를 찾습니다.
다음 단계는 무엇입니까?	Top Peers(상위 피어) 보고서를 실행하여 다른 호스트가 지정된 포트에서 접속한 항목을 확인하기 위해 해당 포트별로 보고서를 필터링하여 해당 호스트를 검사합니다. 이러한 호스트가 알 수 없는 스캐너이며, 관찰된 스캔 활동에 참여하지 말았어야 함을 확인합니다. 알려진 스캐너인 경우에는 위험성이 줄어들 수 있습니다. 알려진 스캐너가 아닌 경우에는 정상적이거나 제어되는 스캔이 아니었던 것이므로 위험성이 커질 수 있습니다. 이 경우 이벤트는 호스트의 보안이 침해되었음을 나타낼 수 있습니다.

어떤 정책 설정을 이 보안 이벤트에 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트가 차이 기반, 임계값 기반이거나 다른 유형입니까?	

이 보안 이벤트는 카테고리에 어떻게 영향을 줍니까?

이벤트에 대한 질문	응답
이 보안 이벤트가 소스에 영향을 주는 알람 카테고리는 무엇입니까?	공격 지표, 상위 관심 지표(CI)

이벤트에 대한 질문	응답
값은 무엇입니까?	• 공격 지표: 참 • CI: 참
이 보안 이벤트가 대상에 영향을 주는 알람 카테고리는 무엇입니까?	상위 대상 지표(TI)
값은 무엇입니까?	• TI: 참

이 보안 이벤트에 대한 응답에 어떤 정보를 사용할 수 있습니까?

이벤트에 대한 질문	응답
이벤트 ID는 무엇입니까?	SEC_ID_WORM_PROPAGATION (36)
이벤트의 syslog 유형은 무엇입니까?	. 자세한 내용은 Alarm(알람) 필드 및 Rule Types(규칙 유형)의 Host Alarm(호스트 알람) 열을 참조하십시오.
이벤트의 SNMP 유형은 무엇입니까?	. 자세한 내용은 SNMP Alarm(SNMP 알람) 필드의 Host Alarm(호스트 알람) 열을 참조하십시오.

3

알람 카테고리

특정 유형의 보안 이벤트는 특정 알람 유형의 지표 포인트에 영향을 줍니다. 일부 보안 이벤트는 둘 이상의 알람 카테고리 유형에 영향을 줍니다. 알람은 발생하는 보안 이벤트의 유형을 기반으로 생성됩니다. 알람 유형에 따라 하나 이상의 알람 카테고리로 그룹화되며 이 내용은 아래 테이블에 나와 있습니다. 알람 카테고리는 호스트 알람만 포함합니다.

참고:

- 시스템 알람은 알람 카테고리에 영향을 주지 않습니다. 알람 카테고리는 위협을 나타내는 것으로 간주되는 이벤트만 포함합니다. SMC(Stealthwatch Management Console) 클라이언트에 표시되는 시스템 알람은 어플라이언스에 문제가 있음을 나타냅니다. 자세한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.
- 호스트 그룹 관계 알람도 알람 카테고리에 포함되지 않습니다. 대신, 이 알람은 호스트 그룹 관계에 연결되어 맵에 표시되며 SMC(Stealthwatch Management Console) 클라이언트에 표시됩니다. 이러한 알람은 정책 설정을 위반하여 알람을 유발하는 특정 호스트 그룹 간의 상호작용을 나타냅니다. 자세한 내용은 *SMC 클라이언트 온라인 도움말*을 참조하십시오.
- 보안 이벤트에 할당된 포인트는 원래 관심 지표(CI)에 영향을 주었습니다. 알람 카테고리가 추가되었으므로 각각에는 연결된 지표가 있으며 포인트는 알람 카테고리에 할당된 보안 이벤트에 따라 해당 지표에 영향을 줍니다. 아래 테이블은 알람 카테고리와 연결된 지표, 알람 카테고리에 할당된 보안 이벤트와 각 보안 이벤트의 기본 포인트 숫자를 나타냅니다.

알람 설정을 구성하려면 SMC 클라이언트 인터페이스에서 호스트 정책 관리자를 사용하십시오.

중요: 알람을 비활성화하면 SMC 웹 애플리케이션 인터페이스에 표시되지 않습니다.

다음과 같은 알람 카테고리가 사용됩니다. 알람 카테고리에서 보안 이벤트 목록은 마지막 릴리스 날짜에 완료됩니다.

이상 징후

알람 카테고리 지표: AN

호스트가 비정상 행동을 하고 있거나 비정상적인 트래픽을 생성하고 있음을 나타내지만 다른 활동 카테고리와 일치하지 않는 이벤트를 추적합니다.

다음 보안 이벤트는 이상 징후 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 카테고리에 할당된 포인트 수
Bogon 주소에서 연결 시도됨	900
Bogon 주소에서 연결 성공	14,400
Bogon 주소로 연결 시도됨	8,100
Bogon 주소로 연결 성공	14,400
높은 총 트래픽	관찰된 플로우 기반
높은 트래픽	관찰된 플로우 기반
ICMP 프래그먼트 필요	700
ICMP 호스트 우선순위	700
ICMP 호스트 연결 불가 TOS	2,800
ICMP 네트워크 연결 불가 TOS	2,800
ICMP 우선순위 컷오프	700
ICMP 프로토 연결 불가	700
ICMP 소스 경로 실패	700
낮은 트래픽	3,000
최대 플로우 시작됨	관찰된 플로우 기반
최대 플로우 제공됨	관찰된 플로우 기반
새 플로우 시작됨	관찰된 플로우 기반
소스=대상	4,000

C&C(Command & Control)

알람 카테고리 지표: C&C 또는 CC

네트워크 내에서 C&C 서버와의 접속을 시도하는 봇에 감염된 서버 또는 호스트의 유무를 나타냅니다.

다음 보안 이벤트는 C&C 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
비콘 호스트	9,000
봇 C&C(Command And Control) 서버	32,000
봇에 감염된 호스트 - C&C 활동 시도됨	32,000
봇에 감염된 호스트 - C&C 활동 성공	22,400
위조 애플리케이션 탐지됨	4,000
Ping_Oversized_Packet	2,400
SSH 역방향 셸	11,700
의심스러운 긴 플로우	4,000
의심스러운 조용한 긴 플로우	4,000

유출

알람 카테고리 지표: EX

참고: 데이터 유출 알람에 영향을 주도록 다음 보안 이벤트를 활성화하고 발생한 데이터 유출 알람에 대한 자세한 정보를 확인할 수 있도록 설정하려면 Stealthwatch 기능 라이선스를 구입해야 합니다.

비정상적인 양의 데이터가 전송되는 내부 및 외부 호스트를 추적합니다. 호스트가 구성된 임계값을 초과하는 이러한 이벤트를 다수 트리거할 경우 데이터 유출 알람이 발효됩니다.

다음 보안 이벤트는 데이터 유출 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
의심스러운 데이터 손실	관찰된 플로우 기반

데이터 호딩

알람 카테고리 지표: DH

네트워크의 소스나 대상이 하나 이상의 호스트에서 비정상적인 양의 데이터를 다운로드했음을 나타냅니다.

다음 보안 이벤트는 데이터 호딩 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
의심스러운 데이터 호딩	관찰된 플로우 기반
표적 데이터 호딩	관찰된 플로우 기반

공격

알람 카테고리 지표: EP

웜 전파, 무차별 대입 비밀번호 크래킹 등 호스트 간의 직접적인 보안 침해 시도를 추적합니다.

다음 보안 이벤트는 익스플로잇 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
무차별 대입 로그인	10,800
Frag:First_Too_Short	6,000
Frag:Sizes_Differ	6,000
Frag:Packet_Too_Long	6,000
높은 SMB 피어	32,000
스캐너 통신	180
의심스러운 UDP 활동	9,000
연결됨	8,000
웜 활동	400
웜 전파	19,200

관심 지표(CI)

알람 카테고리 지표: CI

관심 지표(CI) 임계값을 초과하거나 급속하게 증가한 관심 지표(CI)의 호스트를 추적합니다.

관심 지표(CI) 및 대상 지표(TI) 카테고리는 동일한 이벤트를 사용합니다. 이벤트가 소스 호스트에 의해 트리거되는 경우 관심 지표(CI) 알람이 발생합니다. 이벤트가 대상 호스트에 의해 트리거되는 경우 대상 지표(TI) 알람이 발생합니다.

다음 보안 이벤트는 관심 지표(CI) 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
Addr_Scan/TCP	4,000
Addr_Scan/UDP	4,800
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800

보안 이벤트 이름	기본적으로 할당된 포인트 수
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	0
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
비콘 호스트	9,000
봇 C&C(Command and Control) 서버	32,000
봇에 감염된 호스트 - C&C 활동 시도됨	22,400
봇에 감염된 호스트 - C&C 활동 성공	32,000
무차별 대입 로그인	10,800
Bogon 주소에서 연결 시도됨	900
Bogon 주소에서 연결 성공	14,400
Tor에서 연결 시도됨	1,000
Tor에서 연결 성공	4,000
Bogon 주소로 연결 시도됨	8,100
Bogon 주소로 연결 성공	14,400
Tor로 연결 시도됨	5,400
Tor로 연결 성공	5,400
위조 애플리케이션 탐지됨	4,000
플로우 거부됨	162
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
절반 열림 공격	12,600
높은 파일 공유 지수	관찰된 플로우 기반
높은 SMB 피어	32,000

보안 이벤트 이름	기본적으로 할당된 포인트 수
높은 총 트래픽	관찰된 플로우 기반
높은 트래픽	관찰된 플로우 기반
대량의 이메일	3,200
호스트 잠금 위반	32,000
ICMP 플러드	관찰된 플로우 기반
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Frag_Needed	700
ICMP_Host_Precedence	700
ICMP_Host_Unreach	7
ICMP_Host_Unreach_TOS	2,800
ICMP_Net_Unreach	7
ICMP_Net_Unreach_TOS	2,800
ICMP_Port_Unreach	7
ICMP_Precedence_Cutoff	700
ICMP_Proto_Unreach	700
ICMP_Src_Host_Isolated	7
ICMP_Src_Route_Failed	700
ICMP_Timeout	1
내부 Tor 엔트리 탐지됨	32,000
내부 Tor 종료 탐지됨	32,000
낮은 트래픽	3,000
MAC 주소 위반	6,300

보안 이벤트 이름	기본적으로 할당된 포인트 수
메일 거부	2,400
메일 릴레이	2,400
최대 플로우 시작됨	관찰된 플로우 기반
새 플로우 시작됨	관찰된 플로우 기반
새 호스트 활성화	2,800
패킷 플러드	5,600
Ping	7
Ping_Oversized_Packet	2,400
Ping 스캔	14,400
포트 스캔	10,800
재설정/TCP	3
재설정/UDP	2
스캐너 통신	180
느린 연결 플러드	10,800
스팸 소스	9,000
SSH 역방향 셸	11,700
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
의심스러운 데이터 호딩	관찰된 플로우 기반
의심스러운 데이터 손실	관찰된 플로우 기반
의심스러운 긴 플로우	4,000
의심스러운 조용한 긴 플로우	4,000
의심스러운 UDP 활동	9,000
SYN 플러드	관찰된 플로우 기반
가상 호스트와의 통신	1,440
시간 초과/TCP	4

보안 이벤트 이름	기본적으로 할당된 포인트 수
시간 초과/UDP	3
트랩된 호스트	11,700
UDP 플러드	관찰된 플로우 기반
호스트 감시 활성화	32,000
포트 감시 활성화	32,000
웜 활동	400
웜 전파	19,200

DDoS 소스

알람 카테고리 지표: DS

호스트가 DDoS 공격의 소스로 식별되었음을 나타냅니다.

다음 보안 이벤트는 DDoS 소스 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
절반 열림 공격	12,600
ICMP 플러드	관찰된 플로우 기반
패킷 플러드	5,600
느린 연결 플러드	10,800
SYN 플러드	관찰된 플로우 기반
UDP 플러드	관찰된 플로우 기반

DDoS 대상

알람 카테고리 지표: DT

호스트가 DDoS 공격의 대상으로 식별되었음을 나타냅니다.

다음 보안 이벤트는 DDoS 대상 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
Bogon 주소에서 연결 시도됨	900
Bogon 주소에서 연결 성공	14,400
절반 열림 공격	12,600
ICMP 수신됨	관찰된 플로우 기반
새 플로우 제공됨	관찰된 플로우 기반
패킷 플러드	5,600
느린 연결 플러드	10,800
SYN 수신됨	관찰된 플로우 기반
수신된 UDP	관찰된 플로우 기반

대상 지표(TI)

알람 카테고리 지표: TI

허용 가능한 수보다 많은 스캔 또는 기타 악의적인 공격을 받은 내부 호스트를 추적합니다.

관심 지표(CI) 및 대상 지표(TI) 카테고리는 동일한 이벤트를 사용합니다. 이벤트가 소스 호스트에 의해 트리거되는 경우 관심 지표(CI) 알람이 발생합니다. 이벤트가 대상 호스트에 의해 트리거되는 경우 대상 지표(TI) 알람이 발생합니다.

다음 보안 이벤트는 대상 지표(TI) 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	0
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
비콘 호스트	9,000
봇에 감염된 호스트 - C&C 활동 시도됨	22,400
봇에 감염된 호스트 - C&C 활동 성공	32,000
무차별 대입 로그인	10,800
Bogon 주소에서 연결 시도됨	900
Bogon 주소에서 연결 성공	14,400
Tor에서 연결 시도됨	1,000
Tor에서 연결 성공	4,000
Bogon 주소로 연결 시도됨	8,100
Bogon 주소로 연결 성공	14,400
위조 애플리케이션 탐지됨	4,000
플로우 거부됨	162
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
절반 열림 공격	12,600

보안 이벤트 이름	기본적으로 할당된 포인트 수
높은 SMB 피어	32,000
ICMP 수신됨	관찰된 플로우 기반
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Frag_Needed	700
ICMP_Host_Precedence	700
ICMP_Host_Unreach	7
ICMP_Host_Unreach_TOS	2,800
ICMP_Net_Unreach	7
ICMP_Net_Unreach_TOS	2,800
ICMP_Port_Unreach	7
ICMP_Precedence_Cutoff	700
ICMP_Proto_Unreach	700
ICMP_Src_Host_Isolated	7
ICMP_Src_Route_Failed	700
ICMP_Timeout	1
내부 Tor 엔트리 탐지됨	32,000
내부 Tor 종료 탐지됨	32,000
Ping_Oversized_Packet	2,400
MAC 주소 위반	6,300
최대 플로우 제공됨	관찰된 플로우 기반
새 플로우 제공됨	관찰된 플로우 기반
패킷 플러드	5,600

보안 이벤트 이름	기본적으로 할당된 포인트 수
Ping	7
Ping_Oversized_Packet	2,400
포트 스캔	10,800
재설정/TCP	3
재설정/UDP	2
스캐너 통신	180
느린 연결 플러드	10,800
소스=대상	4,000
SSH 역방향 셸	11,700
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
의심스러운 긴 플로우	4,000
의심스러운 조용한 긴 플로우	4,000
의심스러운 UDP 활동	9,000
SYN 수신됨	관찰된 플로우 기반
가상 호스트와의 통신	1,440
시간 초과/TCP	4
시간 초과/UDP	3
연결됨	8,000
트랩된 호스트	11,700
수신된 UDP	관찰된 플로우 기반
웜 전파	19,200

정책 위반

알람 카테고리 지표: PV

정상적인 네트워크 정책을 위반하는 동작이 주체에 표시됩니다.

다음 보안 이벤트는 정책 위반 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
Tor에서 연결 시도됨	1,000
Tor에서 연결 성공	4,000
Tor로 연결 시도됨	5,400
Tor로 연결 성공	5,400
높은 파일 공유 지수	관찰된 플로우 기반
대량의 이메일	3,200
호스트 잠금 위반	32,000
내부 Tor 엔트리 탐지됨	32,000
내부 Tor 종료 탐지됨	32,000
MAC 주소 위반	6,300
메일 거부	2,400
메일 릴레이	2,400
새 호스트 활성화	2,800
스팸 소스	9,000
호스트 감시 활성화	32,000
포트 감시 활성화	32,000

정찰

알람 카테고리 지표: RC

TCP 또는 UDP를 사용 중이며 조직의 호스트에 대해 실행 중인 악성일 수 있는 무단 스캔 상태를 나타냅니다. '정찰'이라고 부르는 이러한 스캔은 네트워크에 대한 공격을 예고하는 초기 지표이며, 스캔의 출처가 조직의 내부 또는 외부일 수 있습니다.

다음 보안 이벤트는 정찰 알람과 연결되어 있습니다. 두 번째 열은 보안 이벤트가 발생할 때 알람 카테고리에 할당된 기본 포인트의 수를 표시합니다. 일부 보안 이벤트에는 포인트가 없지만 변수는 있습니다.

보안 이벤트 이름	기본적으로 할당된 포인트 수
Addr_Scan/TCP	4,000
Addr_Scan/UDP	4,800
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	0
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
플로우 거부됨	162
높은 SMB 피어	32,000
ICMP_Comm_Admin	7
ICMP_Dest_Host_Admin	7
ICMP_Dest_Host_Unk	7
ICMP_Dest_Net_Admin	7
ICMP_Dest_Net_Unk	7
ICMP_Host_Unreach	7

보안 이벤트 이름	기본적으로 할당된 포인트 수
ICMP_Net_Unreach	7
ICMP_Port_Unreach	7
ICMP_Src_Host_Isolated	7
ICMP_Timeout	1
Ping	7
Ping_Scan	14,400
포트 스캔	10,800
재설정/TCP	3
재설정/UDP	2
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
가상 호스트와의 통신	1,440
시간 초과/TCP	4
시간 초과/UDP	3
트랩된 호스트	11,700