Cisco Secure Network Analytics

セキュリティイベントおよびアラームカテゴリ 7.5.0

目次

はじめに

概要

このドキュメントには、Manager（旧 StealthWatch Management Console）に表示されることがあるセキュリティイベントとアラームカテゴリを説明する一覧が示されています。

対象読者

このドキュメントは、Manager を使用してネットワークを管理および保護するネットワーク管理者およびセキュリティ担当者が参考資料として使用することを目的としています。

関連情報

この情報は、次のトピックの Web アプリケーションヘルプにも記載されています。

- セキュリティ イベント リスト
- アラーム カテゴリについて

略語

この項では、次の用語と略語が使用されます。

略語	用語
ASA	Adaptive Security Appliance
CI	リスクインデックス
DNS	ドメイン ネーム システム（サービスまたはサーバー）
DoS	Denial of Service; サービス妨害
dvPort	分散仮想ポート
ESX	Enterprise Server X
FSI	ファイル共有インデックス
FTP	ファイル転送プロトコル
ICMP	インターネット制御メッセージ プロトコル
IDS	侵入検知システム
IP	インターネット プロトコル
IRC	インターネット リレー チャット

略語	用語
ISE	Identity Services Engine
MAC	Media Access Control; メディア アクセス コントロール
NAT	ネットワーク アドレス変換
NTP	ネットワーク タイム プロトコル
OS	オペレーティング システム
OVF	オープン仮想化フォーマット
RAID	Redundant Array of Independent Discs
SNMP	Simple Network Management Protocol（簡易ネットワーク管理プロトコル）
TCP	伝送制御プロトコル
TI	ターゲット インデックス
UDP	ユーザー データグラム プロトコル
VDS	仮想ネットワーク分散スイッチ
VE	バーチャル エディション
VLAN	仮想ローカル エリア ネットワーク
VM	仮想マシン
VPN	バーチャル プライベート ネットワーク

セキュリティ イベント一覧

セキュリティイベントは、特定の動作の発生を監視し、ポリシーに適用されている設定に応じて、ネットワーク上の該当動作に対してアラートを出すことができるアルゴリズムです。これは、ホストアラームを直接生成する（そのように設定されている場合）か、アラームカテゴリにインデックスポイントを割り当てて、ホストアラームをトリガー可能にすることで実行されます（ホストアラームは、アラームをトリガーしたセキュリティイベントです）。

セキュリティ イベントは、特定のアラーム カテゴリにインデックス ポイントを加算します。セキュリティイベントを無効にすると、そのセキュリティイベントに関連付けられているアラームカテゴリに対するインデックスポイントは累積されなくなります。アラームカテゴリとセキュリティイベントはどちらも、ポリシーに適用されている設定に応じて、ホストアラームをトリガーできます。

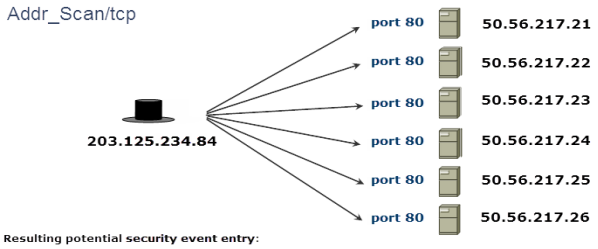
セキュリティイベントは、特定のサービスおよびホストグループレベルで無効にできます。

- 現在、セキュリティ イベント情報を更新および拡張中です。新しいフォーマットには、イベントの説明、イベントがトリガーされる場合の状況、詳しい調査のために実行する必要がある手順などの情報が（複数の表に）含まれています。この移行中に、このトピックの一部のセキュリティイベントには、他のカテゴリよりも多くの完了したカテゴリまたはテーブルが含まれます。
- Flow Collector（NetFlow） を Flow Sensor とともに使用している場合は、二重アスタリスク（**）のマークが付いているセキュリティイベントのみをサポートします。

Cisco Secure Network Analytics（旧 Stealthwatch）には、次のデフォルトのセキュリティイベントが含まれています。

Addr（アドレス）スキャン/TCP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Addr_Scan/tcp-80(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	Secure Network Analytics が TCP を使用してネットワークをスキャンしている可能性を示すアクティビティを検出すると、そのアクティビティはスキャンイベントとして記録されます。多くのスキャンイベントによって多数のホストに影響が及んでいる場合、Manager（旧 Stealthwatch Management Console）はセキュリティイベントを起動します。 「スキャン イベント」の例としては、不正な TCP フラグのさまざまな組み合わせ、SYN を送信しながら後続の SYN– ACK に応答しないなど、さまざまな兆候が挙げられます。
このイベントがトリガーされる場合、何を意味していますか。	ホストが、特定のサービスを実行して利用する可能性のあるホストの検出を試みています。
次に実行すべきステップは何ですか。	ホストがスキャンしていた内容を判断します。この調査は幅広い範囲で開始してから絞り込みます。 [最上位ポート（Top Ports）]（発信）レポートを実行して開始します。イベントの期間と、送信元 IP となるクライアント ホストを設定します。リストされている送信先 IP 範囲に関係なく任意の種類のホストをスキャンできるため、内部ホスト、外部ホスト、またはその両方で検索が必要かどうかを判断できます。次に、[フィルタ（Filter）] ダイアログの [ホスト（Host）] タブで、適切なサーバー フィルタを設定し、[詳細（Advanced）] タブで [返されるレコードの順序（Order the records returned by）] に [フロー（Flows）] を設定します。 結果が返されたら、ピア別に並べ替えると便利です。最初は

このイベントに関する質問	応答
	リストの上部をフローまたはピア別に並び替えて、所属先を持たない、あるいは異常に高い数値を示す突出したポートを検出します。IP アドレスを右クリックしてフローにピボットすることで、さまざまな IP アドレスを表示したり、特定のホストグループが主なターゲットとなっているかどうかを判断したりします。また、右クリックして [最上位ピア(Top Peers)] レポートにピボットすることで、トラフィックがターゲット全体に均等に行き渡っているかどうかを判断できます。スキャンに対応するホストの割合に着目することも可能です。この時点でホストをスキャンしたユーザーとスキャンされたポートを判断できるようにする必要があります。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	場合によっては、FlowSensor やファイアウォールから送信されたフラグによってのみ記録されるスキャンもあります(これはイベントの詳細情報に示されます)。特に注記がない限り、イベントのスキャンには特定のデータは不要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでイベントを有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]、[クライアント IP(Client IP)] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー(Antivirus & SMS Servers)]、[ファイアウォール、プロキシ、およびNATデバイス(Firewalls, Proxies, NAT Devices)]、[ネットワーク管理およびスキャナ(Network Management & Scanners)]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト(Inside Hosts)、外部ホスト(Outside Hosts)、クライアント IP(Client IP)ポリシー、ウイルス対策および SMS サーバー(Antivirus SMS Servers)、ファイアウォール、プロキシ、および NAT デバイス(Firewalls, Proxies, NAT Devices)、

イベントに関する質問	応答
	ネットワーク管理およびスキャナ（Network Management Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	はい
該当する場合、調整可能な値の代替ロケーションは何ですか。	disable_stealth_ probe lc_ threshold.txt の値を使用して、ステルススキャン検出の一定の事例を無効にできます。
イベントにデフォルトの緩和策が設定されていますか。	いいえ
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンと見なされるアクティビティを実行するホスト
ターゲットは何ですか。	送信元ホストによってスキャンされているホスト

イベントに関する質問	応答
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

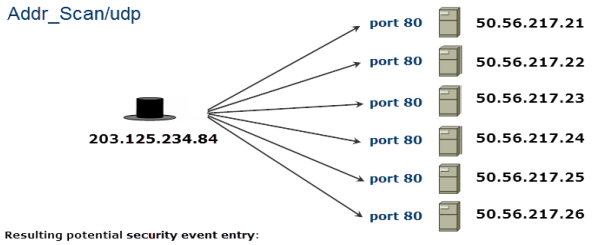
イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは、送信元 IP、ターゲットのナチュラルクラス C ネットワーク（/24）、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TCP_ADDR_SCAN（276）

Addr（アドレス）スキャン/UDP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Addr_Scan/udp-80(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	Secure Network Analytics が UDP を使用してネットワークをスキャンしている可能性を示すアクティビティを検出すると、そのアクティビティはスキャンイベントとして記録されます。スキャンイベントによって多数のホストに影響が及んでいる場合、Manager はセキュリティイベントを起動します。 「スキャン イベント」の例としては、さまざまなタイプの ICMP 拒否によって応答される UDP パケットの送信や、ファイア ウォール フロー拒否メッセージなどのさまざまな兆候が挙げられます。
このイベントがトリガーされる場合、何を意味していますか。	ホストが、特定のサービスを実行して利用する可能性のあるホストの検出を試みています。
次に実行すべきステップは何ですか。	ホストがスキャンしていた内容を判断します。この調査は幅広い範囲で開始してから絞り込みます。 [最上位ポート（Top Ports）]（発信）レポートを実行して開始します。イベントの期間と、送信元 IP となるクライアント ホストを設定します。リストされている送信先 IP 範囲に関係なく任意の種類のホストをスキャンできるため、内部ホスト、外部ホスト、またはその両方で検索が必要かどうかを判断できます。次に、[フィルタ（Filter）] ダイアログの [ホスト（Host）] タブで、適切なサーバー フィルタを設定し、[詳細（Advanced）] タブで [返されるレコードの順序（Order the records returned by）] に [フロー（Flows）] を設定します。 結果が返されたら、ピア別に並べ替えると便利です。最初は

このイベントに関する質問	応答
	リストの上部をフローまたはピア別に並び替えて、所属先を持たない、あるいは異常に高い数値を示す突出したポートを検出します。IP アドレスを右クリックしてフローにピボットすることで、さまざまな IP アドレスを表示したり、特定のホストグループが主なターゲットとなっているかどうかを判断したりします。また、右クリックして [最上位ピア(Top Peers)] レポートにピボットすることで、トラフィックがターゲット全体に均等に行き渡っているかどうかを判断できます。スキャンに対応するホストの割合に着目することも可能です。この時点でホストをスキャンしたユーザーとスキャンされたポートを判断できるようにする必要があります。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	場合によっては、FlowSensor やファイアウォールから送信されたフラグによってのみ記録されるスキャンもあります(これはイベントの詳細情報に示されます)。特に注記がない限り、イベントのスキャンには特定のデータは不要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでイベントを有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]、[クライアント IP(Client IP)] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	ウイルス対策および SMS サーバー(Antivirus SMS Servers)、DHCP サーバー(DHCP Server)、ファイアウォール、プロキシ、および NAT デバイス(Firewalls, Proxies, NAT Devices)、ネットワーク管理およびスキャナ(Network Management Scanners)
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト(Inside Hosts)、外部ホスト(Outside Hosts)、クライアント IP(Client IP)ポリシー、ウイルス対策および SMS サーバー(Antivirus & SMS Servers)、DHCP サーバー

イベントに関する質問	応答
	(DHCP Server)、ファイアウォール、プロキシ、および NAT デバイス(Firewalls, Proxies, NAT Devices)、ネットワーク管理およびスキャナ(Network Management Scanners)
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	はい
該当する場合、調整可能な値の代替ロケーションは何ですか。	disable_stealth_ probe lc_ threshold.txt の値を使用して、ステルススキャン検出の一定の事例を無効にできます。
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンと見なされるアクティビティを実行するホスト

イベントに関する質問	応答
ターゲットは何ですか。	送信元ホストによってスキャンされているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは、送信元 IP、ターゲットのナチュラルクラス C ネットワーク（/24）、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻および UDP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

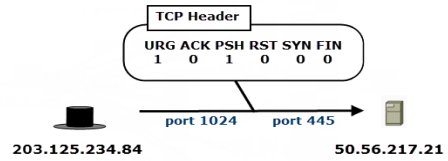
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_ADDR_SCAN (286)

不良フラグ ACK（確認）**

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_ACK



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_ACK-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	パケットに TCP 確認フラグが含まれておらず、リセットまたは同期以外のフラグが含まれている場合は、送信元ホストでセキュリティイベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_ACK を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアントIPポリシー（Client IP Policy）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

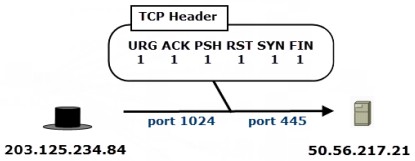
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_NO_ACK（267）

不正なフラグすべて **

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_All



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_All-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	すべての TCP フラグ（同期、確認、リセット、プッシュ、緊急、終了）が含まれているパケットが見つかった場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケットにすべてのフラグのセットが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_All を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	該当なし
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのアラームがオフであるポリシーはどれですか。	該当なし
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が	該当なし

イベントに関する質問	応答
設定されていますか。	
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし

イベントに関する質問	応答
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

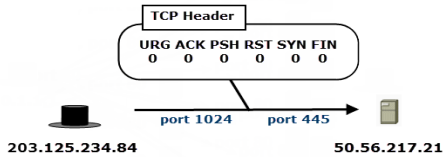
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_XMAS (263)

不良フラグ NoFlg **

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_NoFlg



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_NoFlg-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	TCP フラグが含まれていないパケットがあった場合は、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_NoFlg を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアントIPポリシー（Client IP Policy）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

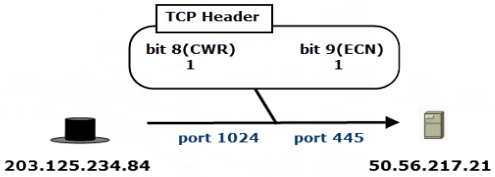
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_NOFLAG（269）

不良フラグ Rsrvd（予約済み）

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_Rsrvd



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_Rsrvd-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	パケットに最初の TCP 標準で予約された TCP フラグが含まれている場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow Edition でこのイベントがトリガーされることはありません。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_Rsrvd を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアントIPポリシー（Client IP Policy）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情	Manager：詳細が表示されます。

イベントに関する質問	応答
報が表示されますか。	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

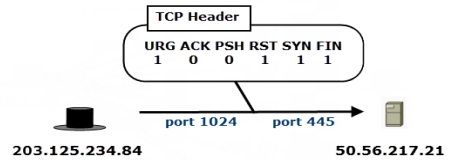
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_RESERVED（265）

不良フラグ RST（リセット）**

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_RST



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_RST-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	TCP リセットに加えてプッシュまたは確認以外のフラグが含まれているパケットが見つかった場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_RST を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアントIPポリシー（Client IP Policy）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

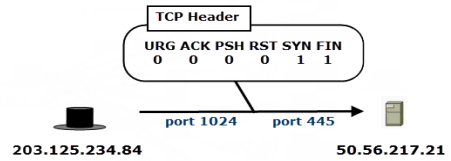
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_BAD_RST（266）

不良フラグ SYN（同期）FIN（終了）**

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_SYN_FIN



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_SYN_FIN-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	TCP 同期および終了フラグが含まれているパケットがあった場合は、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_SYN_FIN を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアントIPポリシー（Client IP Policy）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

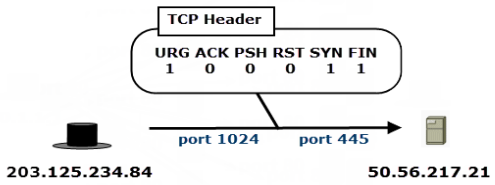
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_SYN_FIN（264）

不良フラグ URG（緊急）**

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Bad_Flag_URG



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Bad_Flag_URG-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	TCP 緊急フラグに加えて確認以外のフラグが含まれているパケットが見つかった場合は、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	TCP パケット に無効なフラグが設定されていることは、通常はあり得ません。そのような事例が見つかった場合は、パケットの送信先マシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、システム設定が異なれば、異なる組み合わせの異常フラグに対して異なる応答が行われる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは不正なフラグの組み合わせを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Bad_Flag_URG を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]、[クライアントIPポリシー(Client IP Policy)]
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー(Antivirus & SMS Servers)]、[ファイアウォール、プロキシ、およびNATデバイス(Firewalls, Proxies, NAT Devices)]、[ネットワーク管理およびスキャナ(Network Management & Scanners)]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト(Inside Hosts)、外部ホスト(Outside Hosts)、クライアント IP(Client IP)ポリシー、ウイルス対策および SMS サーバー(Antivirus SMS Servers)、ファイアウォール、プロキシ、および NAT デバイス(Firewalls, Proxies, NAT Devices)、ネットワーク管理およびスキャナ(Network Management & Scanners)
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情	Manager：詳細が表示されます。

イベントに関する質問	応答
報が表示されますか。	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BAD_FLAG_URG（268）

ホストに対してビーコンを実行

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	内部ホストと外部ホスト間の IP 通信（トラフィックは一方向のみ）が、[長いフローと見なすまでに必要な秒数（Seconds required to qualify a flow as long duration）] の設定を超えています。
このイベントがトリガーされる場合、何を意味していますか。	ビーコン発信ホストは、別のホストからの更新やコマンドを監視するホストです。このトラフィックはキープアライブ（ハートビート）などのさまざまな理由で使用でき、Command and Control（C&C）サーバーから新規オーダーを取得したり、更新をダウンロードしたりします。この動作は、マルウェアによって発生することがありますが、常にマルウェアが原因ではないことを理解することが重要です。
次に実行すべきステップは何ですか。	ビーコン発信ホスト イベントを調査する場合、その目的は外部ホストが実際に C&C サーバー であるかどうかを判断することです。多くの場合、Secure Network Analytics の内部と外部の両方でこのホストを調査すると役立ちます。 Secure Network Analytics 内で行う最初の適切な手順は、ターゲットホストで [最上位ピア（Top Peers）]（発信）レポートを開くことです。これにより、外部ホストと通信したデータ量ごとにソートされた内部ピアのリストが生成されます。その内容から、そのホストが環境内の一般的なピアであるかどうかを判断できます。 2 番目の手順は、送信元とターゲット間のトラフィックパターンを可視化するフロートラフィックレポートの実行です。C&C サーバーとの通信は、一定のアウトバウンドトラフィック量を伴う周期的なパターンを示します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	このパターンは一方向の疑わしい長いフローの場合と同じですが、疑わしい長いフローの代わりにこのイベントでトリガーされます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティイベント Beaconing Host を有効にします。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	なし
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	×
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし

イベントに関する質問	応答
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ビーコンを発信しているホスト
ターゲットは何ですか。	ビーコン発信ホストからトラフィックを受信しているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホストポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：送信元ホスト W は、ターゲット Z に対するピアとして X サービス名（Y プロトコル）を使用しています。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP およびターゲット IP、イベントのアクティブな日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、クライアントバイトおよびサーバーバイト（両方とも 0 以上）でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BEACONING_HOST（39）

Bot の Command and Control サーバー

これはどのようなセキュリティイベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	使用している環境内のホストが、指揮統制（C&C）サーバーとして動作することにより、環境を超えて他のホストの侵害を支援するために使用されていることを示します。このホスト自体も侵害されている可能性が非常に高いです。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	Command and Control 上位インデックス、高リスクインデックス
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_COMMAND_AND_CONTROL_HOST（43）

ボットに感染したホスト：試行された C&C アクティビティ

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ネットワーク上のホストが、既知のコマンドおよび指揮統制（C&C）サーバーと通信しようとしました。ホストはこの操作に失敗しましたが、何らかの原因によってホストがこのような操作を試行したことから、懸念が残ります。マルウェアまたは悪意のあるリダイレクトもこの動作を引き起こす可能性がある点に注意してください。
次に実行すべきステップは何ですか。	このセキュリティ イベントが発生した場合、一般に製品内での検証はそれほど必要とされませんが、イベントのターゲットとその他のホストの間のフローに対してフロー クエリを実行し、他のホストが疑わしい C&C サーバーと対話しているかどうかを確認してください。クエリの期間をイベント日またはそれより長く設定します。 通信の継続時間に応じて、このクエリを使用して送信元ホストが、疑わしい C&C サーバーとの通信を開始した時刻を特定できます。ターゲット ホストと通信しているホストが多数ある場合、または通信履歴を確認する場合は、C&C サーバーが誤って特定されている可能性があります。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「完全な」ポリシー：Command and Control 上位インデックス、高リスクインデックス 「部分的な」ポリシー：Command and Control 上位インデックス、高リスクインデックス

イベントに関する質問	応答
数量はどの程度ですか。	「完全な」ポリシー: • Command and Control 上位インデックス:True • CI:True 「部分的な」ポリシー: • Command and Control 上位インデックス:True • CI:True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「完全な」ポリシー:高ターゲットインデックス 「部分的な」ポリシー:高ターゲットインデックス
数量はどの程度ですか。	「完全な」ポリシー: • TI:True 「部分的な」ポリシー: • TI:True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BOT_INFECTED_HOST(41)

ボットに感染したホスト：成功した C&C アクティビティ

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ネットワーク上のホストが、既知のコマンドおよび指揮統制（C&C）サーバーと通信しました。マルウェアまたは悪意のあるリダイレクトによりこの動作が引き起こされたか、またはこの通信がエクスプロイト キットなどによる感染時の試行であった可能性があります。これはほぼ確実に侵害されたホストの兆候です。
次に実行すべきステップは何ですか。	このセキュリティ イベントが発生した場合、一般に製品内での検証はそれほど必要とされませんが、イベントのターゲットとその他のホストの間のフローに対してフロー クエリを実行し、他のホストが疑わしい C&C サーバーと対話しているかどうかを確認してください。クエリの期間をイベント日またはそれより長く設定します。 通信の継続時間に応じて、このクエリを使用して送信元ホストが、疑わしい C&C サーバーとの通信を開始した時刻を特定できます。ターゲット ホストと通信しているホストが多数ある場合、または通信履歴を確認する場合は、C&C サーバーが誤って特定されている可能性があります。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「完全な」ポリシー：Command and Control 上位インデックス、高リスクインデックス 「部分的な」ポリシー：Command and Control 上位インデックス、高リスクインデックス

イベントに関する質問	応答
数量はどの程度ですか。	「完全な」ポリシー: • Command and Control 上位インデックス:True • CI:True 「部分的な」ポリシー: • Command and Control 上位インデックス:True • CI:True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「完全な」ポリシー:高ターゲットインデックス 「部分的な」ポリシー:高ターゲットインデックス
数量はどの程度ですか。	「完全な」ポリシー: • TI:True 「部分的な」ポリシー: • TI:True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BOT_INFECTED_HOST_CONTROLLED（42）

ブルート フォース（総当たり）ログイン

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ホストがログインの繰り返しによるブルートフォース パスワード クラッキングの試行と一致する短い TCP 接続の繰り返しを検出しました。
このイベントがトリガーされる場合、何を意味していますか。	これにより、別途システムへのアクセスを試みてログイン クレデンシャルを推測しようとしているホストも検出できる可能性があります。また、何度も接続を試みながら認証に失敗しているクライアント上の誤設定されたアプリケーションを検出することも可能です。
次に実行すべきステップは何ですか。	目的は、サーバーに対する接続試行が正当であるかどうかを確認することです。クライアントが外部ホストの場合、クライアントのアドレスはこれらの接続を開始する予定の既知で信頼できるネットワークまたはビジネス パートナーのネットワークにあるでしょうか。その場合は、アプリケーションの誤設定の可能性があります。また、（ターゲット ホストの）DShield に対して外部参照を実行し、セキュリティ イベント アラームでターゲット IP の所有者を確認する必要もあります。クライアントが内部ホストの場合、このホストは問題のサーバーへの接続を試行する可能性があるでしょうか。送信元ホストの [最上位ピア（Top Peers）] レポートを実行することで、そのホストが同様のバイト数またはフローの多いネットワーク上の他のホストに接続しているかどうかがわかります。また、[最上位ポート（Top Ports）] レポートを実行して、セキュリティ イベント アラームがトリガーされた同じポート（おそらく SSH）を経由して送信元 IP が接続している他のホストを検出できます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	1(接続数)および 1(1 接続あたりの平均バイト数)
最大しきい値	3,000(接続数)および 50,000(1 接続あたりの平均バイト数)
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	接続数および 1 接続あたりの平均バイト数。
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が	

イベントに関する質問	応答
設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	攻撃ホスト
ターゲットは何ですか。	被害ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし

イベントに関する質問	応答
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントのアクティブ日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、および <port>/TCP として関連付けられたポートでフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BRUTE_FORCE_LOGIN（58）

Bogon アドレスからの接続試行

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	「Bogon」アドレスは、未割り当ての使用できない IP アドレスです。一方からの単方向通信は心配ありませんが、通常の使用ではあり得ません。実際、この種のトラフィックはネットワークの境界でブロックされる可能性が高いです。一括表示を検索する特定の種類の動作は、攻撃者が送信元 IP アドレスをスプーフィングする、サービス妨害（DoS）攻撃を示します。
次に実行すべきステップは何ですか。	Bogon アドレスからの単方向トラフィックを調査する際に最初に確認すべき 2 つの事項があります。1）その Bogon アドレス（または他の Bogon アドレス）はネットワーク内の他のホストと通信しようとしていますか。2）Bogon アドレスからのトラフィックの送信先ホストが、異常に多い量のトラフィックを受信していますか。 最初の質問に答えるには、Bogon ホストグループに対して最上位ホスト クエリまたはフロー クエリを実行できます。特にセキュリティ イベントから Bogon IP に対してクエリを実行できますが、スプーフィングされたトラフィックの場合は、攻撃者が簡単に多くの異なる Bogon IP を使用できてしまう可能性があります。クエリから返される結果を評価し、DoS 攻撃の一部であるか、またはネットワーク上の不良構成/未分類ホストによるものであるかを判断します。一般に、大量のデータまたはパケットは、DoS 攻撃の兆候です。 2 番目の質問に答えるには、セキュリティイベントの送信先ホストでのクエリに着目します。ここでの目的は、異常に大量のトラフィックがあるかどうか、それが Bogon アドレスから発生しているかどうかを判断することです。簡単に有用な情報を確認する方法として、ターゲット ホストのその他のセキュリティ イベントを表示し、SYNs Received や New Flows Served などの DoS イベントであるか、または Bogon からの大量通信であるかを確認します。 さらに詳しく調べるには、[フロートラフィック（Flow Traffic）] レポートを実行します。Bogon 通信の時刻とこの時刻から遡った 2 時間を含めるため、日付/日時フィルタを設定します。期間が長いほどクエリも長くなりますが、より適切なコンテキストを得ることができます。また、内部から開始された DoS 攻撃を懸念していない場合は、外部ホストからのトラフィックだけを含めるようにホストをフィルタ処理できます。大規模なスパイクや、徐々に増加する大量トラフィックは、DoS 攻撃を示している可能性があります。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高リスクインデックス（High Concern Index）
数量はどの程度ですか。	• CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 異常インデックス：True • 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_CONN_FROM_BOGON_ATTEMPTED（519）

Bogon アドレスからの接続成功

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	「Bogon」アドレスは、未割り当ての使用できない IP アドレスです。Bogon アドレスとの双方向通信は発生しないはずです。この動作は、ネットワーク内または Secure Network Analytics 導入環境内の不良構成を示している可能性があります。
次に実行すべきステップは何ですか。	ご使用の環境で特定の Bogon IP アドレス範囲を内部で実際に使用しているかどうか、またはキャリア グレード NAT を使用しているかどうかを確認します。Bogon 範囲を内部で使用しているか、使用する可能性がある場合は、その範囲を内部ホスト グループに追加します。Secure Network Analytics でこれを確認するには、bogon の /24 でアクティブなフローを探します。範囲の大部分がアクティブな場合、その範囲は環境内で意図的に使用されている可能性が高いです。Bogon の IP が 100.64.0.0/10 内にある場合は、キャリア グレード NAT で予約された IP 空間を使用しており、使用している環境が背後にあるかどうかは問題ではありません。 いずれも該当しない場合、ホストスナップショット（デスクトップ クライアント内でアクセスする）にはホストの識別に役立つ情報が含まれます。例えば、[エクスポータ インターフェイス（Exporter Interface）] タブに、ホストのフローを監視しているエクスポータとインターフェイスが表示されるため、デバイスがどこでホストされているかを確認できます。さらに、[セキュリティ イベント（Security Events）] タブ、[アラーム（Alarms）] タブおよび [識別（Identification）] タブを確認します。これらのタブには、Bogon ホストが関与している可能性のあるその他の動作が表示されます。最後に、Bogon ホストのセキュリティ イベントを調べ、Bogon ホストが対話した他のホストがあるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高リスクインデックス（High Concern Index）
数量はどの程度ですか。	• CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 異常インデックス：True • 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_CONN_FROM_BOGON_SUCCEEDED（517）

ToR からの接続試行

ToR 終了ノードからネットワーク内のホストへ接続しようとする試みを検出します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_EXIT_ATTEMPTED（317）

ToRからの接続成功

ToR 終了ノードからネットワーク内のホストへの接続が成功した事例を検出します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_EXIT_SUCCEEDED（318）

Bogon アドレスへの接続試行

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	「Bogon」アドレスは、未割り当ての使用できない IP アドレスです。一方からの単方向通信は希で、何者かがネットワークでホストを操作している可能性があります。これは、サービス妨害（DoS）攻撃からのバックスキャッタの可能性があります。これは、攻撃者が分散型サービス妨害（DDoS）攻撃の一環として無作為のソースアドレスにパケットを送信し、ユーザーがそれらの無作為のアドレスに応答すると発生します。攻撃者は IP 空間全体をランダム化し、これらのいくつかが Bogon アドレスになります。Bogon IP への単方向通信もまた、偵察や設定が誤っているホストの可能性があります。
次に実行すべきステップは何ですか。	ご使用の環境で特定の Bogon IP アドレス範囲を内部で実際に使用しているかどうか、またはキャリア グレード NAT を使用しているかどうかを確認します。Bogon 範囲を内部で使用しているか、使用する可能性がある場合は、その範囲を内部ホスト グループに追加します。Secure Network Analytics でこれを確認するには、bogon の /24 でアクティブなフローを探します。範囲の大部分がアクティブな場合、その範囲は環境内で意図的に使用されている可能性が高いです。Bogon の IP が 100.64.0.0/10 内にある場合は、キャリア グレード NAT で予約された IP 空間を使用しており、使用している環境が背後にあるかどうかは問題ではありません。 どちらにも当てはまらない場合は、イベントの送信元の他のセキュリティ イベントを確認します。Bogons への大量の通信か、SYNs Received または New Flows Served のようなサービス妨害（DoS）イベントかどうかを判断します。また、Ping スキャンや Addr_Scan などの偵察関連イベントも検索します。潜在的な DDoS をより徹底的に調べるには、[フロー トラフィック（Flow Traffic）] レポートを実行します。Bogon 通信の時刻とこの時刻から遡った 2 時間を含めるため、日付/日時フィルタを設定します。期間が長いほどクエリも長くなりますが、より適切なコンテキストを得ることができます。また、内部から開始された DoS 攻撃を懸念していない場合は、外部ホストからのトラフィックだけを含めるようにホストをフィルタ処理できます。大規模なスパイクや、徐々に増加する大量トラフィックは、DoS 攻撃を示している可能性があります。 DDoS または大量の偵察アクティビティのいずれの可能性もない場合は、Bogon IP のセキュリティ イベントを調べ、Bogon ホストとの対話を試行した他のホストがあるかどうかを確認します。多数のホストが特定の Bogon と対話を試行している場

このイベントに関する質問	応答
	合は、アプリケーションで不適切な構成がプッシュ アウトされたか、または Bogon 範囲でホストされているアプリケーションが消失したことを示唆しています。この点をさらに詳しく調査するには、Bogon のトラフィック履歴を調べます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_CONN_TO_BOGON_ATTEMPTED（518）

Bogon アドレスへの接続成功

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	「Bogon」アドレスは、未割り当ての使用できない IP アドレスです。Bogon アドレスとの双方向通信は発生しないはずです。この動作は、ネットワーク内または Secure Network Analytics 導入環境内の不良構成を示している可能性があります。
次に実行すべきステップは何ですか。	ご使用の環境で特定の Bogon IP アドレス範囲を内部で実際に使用しているかどうか、またはキャリア グレード NAT を使用しているかどうかを確認します。Bogon 範囲を内部で使用しているか、使用する可能性がある場合は、その範囲を内部ホスト グループに追加します。Secure Network Analytics でこれを確認するには、bogon の /24 でアクティブなフローを探します。範囲の大部分がアクティブな場合、その範囲は環境内で意図的に使用されている可能性が高いです。Bogon の IP が 100.64.0.0/10 内にある場合は、キャリア グレード NAT で予約された IP 空間を使用しており、使用している環境が背後にあるかどうかは問題ではありません。 いずれも該当しない場合、ホストスナップショット（デスクトップ クライアント内でアクセスする）にはホストの識別に役立つ情報が含まれます。例えば、[エクスポータ インターフェイス（Exporter Interface）] タブに、ホストのフローを監視しているエクスポータとインターフェイスが表示されるため、デバイスがどこでホストされているかを確認できます。さらに、[セキュリティ イベント（Security Events）] タブ、[アラーム（Alarms）] タブおよび [識別（Identification）] タブを確認します。これらのタブには、Bogon ホストが関与している可能性のあるその他の動作が表示されます。最後に、Bogon ホストのセキュリティ イベントを調べ、Bogon ホストが対話した他のホストがあるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_CONN_TO_BOGON_SUCCEEDED（516）

ToR への接続試行

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ToR（正式には Onion ルータ）は、インターネット接続の匿名化に使用するネットワークであり、ToR ネットワークを終了する前に複数のリレーを経由して接続を送信することで機能します。ToR エントリ ノードは、ToR 接続が ToR ネットワークを移動し、終了する前に通過する最初のサーバーです。このセキュリティイベントには、Secure Network Analytics によりモニターされていて、ToR エントリノードとの通信を試みたが接続の確立に成功したことが観測されていないホストが含まれています。 ユーザーまたはマルウェアが、指揮統制トラフィックを検出しようとした可能性があります。ユーザーによる操作の場合、ユーザーのトラフィックの宛先またはユーザーの閲覧元のロケーションを難読化しようとしていた可能性があります。ToR エントリノードの一部は、他のサービスも動作するサーバで動作すると認識することが重要です。たとえば、DuckDuckGo は検索を実行するためにアクセスされた同じサーバー上で ToR エントリノードを実行します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True

イベントに関する質問	応答
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_ENTRY_ATTEMPTED（513）

ToR への接続成功

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ToR（正式には Onion ルータ）は、インターネット接続の匿名化に使用するネットワークであり、ToR ネットワークを終了する前に複数のリレーを経由して接続を送信することで機能します。ToR エントリ ノードは、ToR 接続が ToR ネットワークを移動し、終了する前に通過する最初のサーバーです。このセキュリティイベントには、Secure Network Analytics によりモニターされていて、ToR エントリノードと通信しているホストが含まれています。 これは、ユーザー主導、またはマルウェアによる Command and Control トラフィックの試行の可能性があります。ユーザーによる操作の場合、ユーザーのトラフィックの宛先またはユーザーの閲覧元のロケーションを難読化しようとしていた可能性があります。ToR エントリノードの一部は、他のサービスも動作するサーバで動作すると認識することが重要です。たとえば、DuckDuckGo は検索を実行するためにアクセスされた同じサーバー上で ToR エントリノードを実行します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True

イベントに関する質問	応答
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_ENTRY_SUCCEEDED（514）

偽のアプリケーションを検出

これはどのようなセキュリティイベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ホストのアプリケーションリストを更新する場合、処理されているアプリケーションデータが偽のアプリケーションかどうかを判断するためにメソッドが呼び出されます。偽のアプリケーションロジックは、関連するホストの情報とともに、現在分析中のフローからデータを取得します。アルゴリズムではこのデータを使用して、使用されているプロトコル（TCP または UDP）とポートが、識別された想定のアプリケーションと一致するかどうかが判断されます。アプリケーションの識別は、ネットワークの構成方法に応じて、FlowSensor、Palo Alto アプライアンス、PacketShaper アプライアンス、または NBAR アプライアンスのいずれかのデバイスに基づいて行われます。現在監視されているアプリケーションは、Telnet、SSH FTP、メールサービス、NTP、および DNS などです。標準アプリケーションで非標準ポートが使用されている場合（123/UDP 経由の DNS など）や、特定のポートにそのポート経由で通信している非標準アプリケーションがある場合（80/TCP 経由の SSH など）、アラームがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	この動作は多くの場合、意図されたサービスではないサービスを使用して一般に許可されたポートからトラフィックを送信することにより、人物またはアプリケーションが出力フィルタリングを回避しようとしている兆候です。また、TCP 8022 経由の SSH のように、セカンダリ ポートを使用するアプリケーションで起動する可能性がある、標準以外のポートを使用する標準アプリケーションも見つかります。
次に実行すべきステップは何ですか。	調査の目的は、関連フローを見つけ、データ漏洩や Command and Control の兆候の有無を判断することにあります。 このイベントの調査の最初のステップは、イベントに関連付けられているポートと、関連するホストを検討することです。たとえば、ターゲットホストがオフサイト バックアップ サーバーであり、ポート 8022 でイベントがトリガーされた場合、懸念することはありません。一方、ターゲットホストが不明で、53 UDP 経由の非 DNS トラフィックが確認される場合は、詳しく調べる必要があります。 調査方法はいくつかあります。イベントで関連ポートの一覧を作成し、その一覧を使用して非常に限定的なフィルタを作成できます。たとえば、関係するポートを経由する、関係する 2 つのホスト間のフローを抽出し、「適切な」アプリケーションを

このイベントに関する質問	応答
	使用するフローを除外する場合（非 DNS のポート 53 UDP 経由のフローを検索するなど）、イベント発生の原因となったフローが見つかります。 また、代わりにより一般的なクエリを実行し、イベント日におけるイベントの送信元およびターゲット ホストだけをフィルタ処理することが役立つ場合もあります。これにより、ポート/アプリケーションの不一致があるフロー以外のフローも見つかることがあり、そのようなフローの存在は調査において貴重なコンテキストになります。 対象のフローを特定したら、誤使用の兆候がないか、宛先ホスト、履歴、およびデータ ボリュームを確認します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	FlowSensor、Palo Alto アプライアンス、Packetshaper アプライアンス、または NBAR アプライアンスの詳細情報が必要です。
注意	なし。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	×

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	該当なし
ターゲットは何ですか。	該当なし
イベントのトリガーを引き起こすポリシーはどれですか。	該当なし
送信元で、セキュリティ イベント	Command and Control 上位インデックス、高リスクインデック

イベントに関する質問	応答
が関与するアラーム カテゴリはどれですか。	ス
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：ホストはポート/プロトコル（サービス名）経由で X を使用しました。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 35 分前からイベントの最後のアクティブ時刻までの時間範囲、<port>/TCP および <port>/UDP として関連付けられたポートでフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FAKE_APP（62）

フロー拒否

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはコンテキストに大きく依存します。たとえば、インターネット上のホストからのフロー拒否は、たいてい、特に単一のイベントとして興味深いものではありません。内部ホストから内部ホストへのフロー拒否は内部から外部とは異なります。また、何度も繰り返し行われる同じホスト/ポート ペアリングの試行は、さまざまな宛先に対してブロックされることとは大きく異なります。 内部ホストで、1 つのポートを経由して別の内部ホストと対話する多数のフローが拒否されている場合は、不良構成の可能性があります。さまざまなポートまたは内部ホストへのフローが多数拒否される場合は、偵察である可能性があります。それとは別に、これは興味深いものではないと判断していることをホストが実行している兆候です。インターネット上の内部ホストからブロックされたフローでは、どの規則を違反しようとしているのかというコンテキストが必要になりますが、それとは関係なく、ホストはセキュリティ ポリシーで実行すべきではないと決定していることを実行しています。
次に実行すべきステップは何ですか。	フロー否定を調査するための適切な方法は、イベントの送信元ホストでセキュリティ イベント クエリを実行することです。イベント日に対してクエリを実行し、最初のフロー拒否イベントの送信元になる送信元ホストを設定し、その他のフロー拒否イベントのみを含めるタイプを設定します。これにより、ホストのすべてのフロー拒否イベントが表示されるようになります。返された結果から、これが 1 つの拒否フローであるのか、同一ポートを経由する同一ホストへの多数の拒否フローであるのか、同一ポートを経由する異なるホストへの多数の拒否フローであるのか、同じホスト グループへの多数の拒否フローであるのかなどを確認できます。これにより、ホストが実際に行っている動作を確認できます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

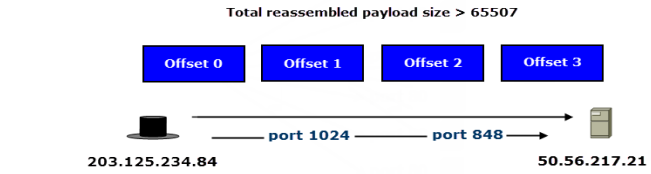
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FLOW_DENIED（310）

長すぎるフラグメンテーション パケット **

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Frag:Packet_Too_Long



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:Packet_Too_Long-848(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	最大パケット長を超えるようなフラグメント値を伴うパケットが見つかった場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	IP パケットのフラグメンテーション値が無効であることは、通常はありません。そのような事例が見つかった場合は、パケットの宛先のマシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、オペレーティング システムやバージョンが異なれば応答が異なる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは無効なフラグメントを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Frag:Packet_Too_Long を有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアント IP（Client IP）] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	攻撃インデックス、高リスクインデックス
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし

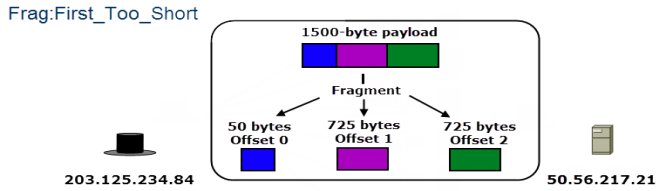
イベントに関する質問	応答
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最後のアクティブ時刻までの時間範囲、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FRAG_PKT_TOO_LONG (282)

短すぎるフラグメンテーション パケット **

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:First_Too_Short-445(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	フラグメンテーションの長さが非常に短いためプロトコル ヘッダーが切り捨てられているパケットが見つかった場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	IP パケットのフラグメンテーション値が無効であることは、通常はありません。そのような事例が見つかった場合は、パケットの宛先のマシンに関する情報収集を目的として意図的に行われている可能性があります。というのも、オペレーティング システムやバージョンが異なれば応答が異なる可能性があるからです。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは無効なフラグメントを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Frag:First_Too_Short を有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアント IP（Client IP）] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	攻撃インデックス、高リスクインデックス
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし

イベントに関する質問	応答
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最後のアクティブ時刻までの時間範囲、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

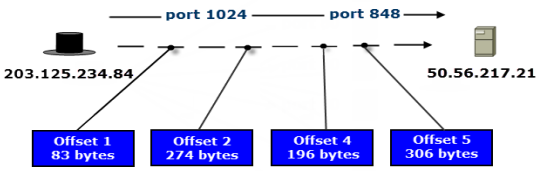
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FRAG_PKT_TOO_SHORT (281)

異なるフラグメンテーション サイズ **

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Frag:Sizes_Differ



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Frag:Sizes_Differ-848(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	パケットのフラグメンテーション サイズがセグメント間で異なる場合、送信元ホストでセキュリティ イベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	IP パケットの各セグメントのフラグメンテーション サイズが異なることは、通常はありません。そのような事例が見つかった場合は、経路上のパケット検査ツールを回避する目的で、意図的に行われている可能性があります。
次に実行すべきステップは何ですか。	このイベントのソースが内部ホストである場合、これ以外の偵察活動の兆候を探す価値があります。たとえば、ホストは無効なフラグメントを複数のホストに送信していないでしょうか。同じポートで多数のホストをスキャンしていないでしょうか。1 つのホスト上で多数のポートをスキャンしていないでしょうか。内部ホストによる偵察があれば、それは望ましくないアクティビティや侵害の兆候として捉えることができます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、FlowSensor が必要です。Flow Collector sFlow では、必要な追加コンポーネントは特にありません。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	送信元ホストでセキュリティ イベント Frag:Sizes_Differ を有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアント IP（Client IP）] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ウイルス対策およびSMSサーバー（Antivirus & SMS Servers）]、[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, NAT Devices）]、[ネットワーク管理およびスキャナ（Network Management & Scanners）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト（Inside Hosts）、外部ホスト（Outside Hosts）、クライアント IP（Client IP）ポリシー、ウイルス対策および SMS サーバー（Antivirus SMS Servers）、ファイアウォール、プロキシ、および NAT デバイス（Firewalls, Proxies, NAT Devices）、ネットワーク管理およびスキャナ（Network Management & Scanners）
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せ	該当なし

イベントに関する質問	応答
ずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	不正なパケットを送信したホスト
ターゲットは何ですか。	不正なパケットの宛先としてリストされたホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト ポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	攻撃インデックス、高リスクインデックス
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし

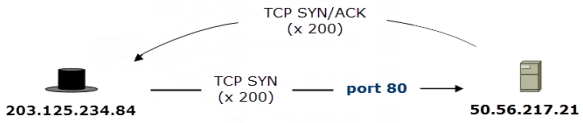
イベントに関する質問	応答
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最後のアクティブ時刻までの時間範囲、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FRAG_DIFFERENT_SIZES (283)

ハーフ オープン攻撃

Half_Open_Attack



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Half_Open_Attack

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはサービス妨害（DoS）攻撃です。ハーフ オープン攻撃は、接続を開いても伝送しないため、帯域幅または接続ハンドラを浪費させる試行となり、悪意のある接続がタイムアウトになるまで犠牲となるホストが長時間強制的に待機することになる可能性があります。
次に実行すべきステップは何ですか。	目的は、ターゲットへの接続が正当であるかどうか、およびターゲットでパフォーマンスが低下しているかどうかを判断することです。これは、2 つの内部ホスト間での悪意のある動作である可能性もありますが、内部ホストと外部ホスト間で発生した場合のほうが、一般により興味深いイベントとなります。 まず、イベント日に対して、イベントの送信元およびターゲット間でフロー クエリを実行します。フローが継続しているかどうかをメモします。継続していない場合は、サービス停止は発生しておらず、問題ではない可能性があります。また、送信元とターゲットの両方のホストのセキュリティ イベント履歴もチェックできます。送信元ホストでは、複数のターゲットに対して、または継続的にこのイベントが発生しているでしょうか。継続的に発生している場合は、詳しく調査する必要があります。 ターゲット ホストで、継続的ではなく一度に、ターゲット ホストに対して多数のホストがこのイベントをトリガーしているでしょうか。これは分散型サービス妨害（DDoS）攻撃の兆候である可能性があります。また、イベントが継続的に発生している場合は、サービスがホストしている何らかのアプリケーションの通常の動作であることがあります。この場合、特定のホストに対してイベントをオフにすることを検討してください。 関連するトラフィックがフロー センサーによって観測された場

このイベントに関する質問	応答
	合は、パフォーマンス レポートを実行し、トラフィックの特性のために SRT（サーバー応答時間）が影響を受けていないかどうかを確認します。これが正当なトラフィックであるかどうかを示している可能性があります。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「A」ポリシー：高 DDoS ソースインデックス、高リスクインデックス 「B」ポリシー：高 DDoS ソースインデックス、高リスクインデックス
数量はどの程度ですか。	「A」ポリシー： • 高 DDoS ソースインデックス：True • CI：True 「B」ポリシー： • 高 DDoS ソースインデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	「A」ポリシー：高 DDoS ターゲットインデックス、高ターゲットインデックス 「B」ポリシー：高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	「A」ポリシー： • 高 DDoS ターゲットインデックス：True • TI：True

イベントに関する質問	応答
	「B」ポリシー: • 高 DDoS ターゲットインデックス:True • TI:True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HALF_OPEN（26）

高ファイル共有インデックス

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ファイルサーバー以外からの大量のデータ転送を検索します。送信元（大量のデータをダウンロードしているホスト）は、ターゲットから大きなファイルをダウンロードするために、ピアツーピア技術または簡易ファイル共有メソッドおよびプロトコルを使用している可能性があります。
このイベントがトリガーされる場合、何を意味していますか。	送信元は、ターゲットから異常な量のデータをダウンロードしている可能性があります。これはデータ蓄積やデータ漏洩の前兆である可能性があります。
次に実行すべきステップは何ですか。	ダウンロードされたデータ量を確認します。これはデータ蓄積の疑いの前兆である可能性があります。この場合、初期ターゲットがわかっている点を除いて、手順は同じです。 これを調査する場合、送信元に対して［最上位ピア（Top Peers）］（着信）レポートを実行するのが最適な方法です。クエリ期間をイベント日に設定します。［クライアント（Client）］または［サーバー ホスト（Server Host）］がセキュリティイベントの送信元 IP で、［その他のホスト（Other Host）］が［内部ホスト（Inside Hosts）］ホスト グループであるように、レポートをフィルタ処理します。その目的は、送信元が複数のターゲット間でこれを行っているかどうかを確認することです。 ターゲットが送信元にデータを送信する唯一のホストの場合、そのターゲットに対して［最上位ピア（Top Peers）］レポートを実行して、他のホストに対して同じアクティビティが示されているかどうかを確認します。示されている場合、ターゲットをファイル共有サーバーとして調査して、アクティビティが想定されているかどうかを確認することには価値があります。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	外部ホスト
デフォルトでこのアラームがオンであるポリシーはどれですか。	デフォルトで内部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	分散
既定値と単位は何ですか。	該当なし
許容値	75
最小しきい値	24 時間で 100,000 FSI ポイント
最大しきい値	24 時間で 1,000,000,000 FSI ポイント
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が	

イベントに関する質問	応答
設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ファイルを受信しているホスト。
ターゲットは何ですか。	ファイルを送信しているホスト。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W ポイント。予想値は X ポイント、Y の許容値は最大で Z ポイント。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし

イベントに関する質問	応答
関連フローについてどのような情報が表示されますか。	Manager：フローは、送信元 IP と外部ホスト、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FILE_SHARING（20）

高 SMB ピア

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ホストで、ワームの伝播と一致する、外部へのサーバーメッセージブロック（SMB）セッションが多数発生しています。
このイベントがトリガーされる場合、何を意味していますか。	これが特定のシナリオで発生することが判明している場合、またはしきい値を非常に低く設定している場合を除き、このイベントはホストが侵害を受けている兆候をほぼ確実に示しています。これは一般に、マルウェアが SMB 経由で自動的に拡散しようとしている兆候です。
次に実行すべきステップは何ですか。	このセキュリティ イベントは、侵害の兆候である可能性がありますが、このイベントを調査して、外部ホストが特定の範囲内にあるかどうか、またはアクセスされた外部ホストの数を確認することができます。このためには、フロー クエリを実行します。クエリの開始時間をイベント日に設定します。[フィルタ（Filter）] ダイアログの [ホスト（Hosts）] タブで、[クライアント（Client）] または [サーバーホスト（Server Host）] をイベントの送信元として設定し、[その他のホスト（Other Host）] が [内部ホスト（Inside Hosts）] ホストグループであることを確認します。[サービスおよびアプリケーション（Services Applications）] タブで、[サービス（Services）] でフィルタ処理を行い、[SMB] を含めます。このクエリは、関連フローをすべて返します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	

イベントに関する質問	応答
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト、外部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト、外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[しきい値(Threshold)]
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	内部ホストから外部ホストへの 100 の SMB フロー。
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	多数の Manager ピアがある内部ホスト
ターゲットは何ですか。	SMB ピアとして動作しているホスト。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP および外部ホスト、イベントのアクティブ日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、445/TCP および 445/UDP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HIGH_SMB_PEERS（60）

高トラフィック合計

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	着信と発信の両方のトラフィックをカウントするため、過大な合計トラフィックは異常な動作の一般的な兆候です。着信が多くを占める場合、発信が多くを占める場合、またはこの 2 つの組み合わせであることがあります。IP は単に、異常に大量のトラフィックで使用されます。
次に実行すべきステップは何ですか。	どのくらいのデータが移動し、そのデータがどこからどこに向かっているのかを特定します。これを調査する理想的な方法は、送信元ホストに対してフロー クエリを実行することです。関連付けられているセキュリティ イベントの日を期間として設定し、クライアント ホストまたはサーバー ホストになる送信元ホストを設定します。 結果が返されたら、最高量のデータの宛先または発信元を調べます。これを行うには、合計バイト数で並べ替えます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True

イベントに関する質問	応答
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOTAL_TRAFFIC（16）

高トラフィック

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	着信および発信トラフィックの両方をカウントするため、過大なトラフィックは異常な動作の兆候です。着信が多くを占める場合、発信が多くを占める場合、またはこの 2 つの組み合わせであることがあります。IP は単に、異常に大量のトラフィックで使用されます。着信または発信 DoS を示している可能性があります。
次に実行すべきステップは何ですか。	どのくらいのデータが移動し、そのデータがどこからどこに向かっているのかを特定します。これを調査する理想的な方法は、送信元ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、（アラームが存在する場合）終了時刻はアラームの終了時刻に設定します。クライアント ホストまたはサーバー ホストになる送信元ホストを設定します。 結果が返されたら、最高量のデータの宛先または発信元を調べます。これを行うには、合計バイト数で並べ替えます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス

イベントに関する質問	応答
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HI_TRAFFIC（30）

大量の電子メール

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	電子メールサーバーとして指定されていないが、少量または存在しない着信メールの比率との関連で非常に大量の発信電子メールが表示されているホストを検索します。
このイベントがトリガーされる場合、何を意味していますか。	アラートが表示されているホストは、電子メールワームマルウェアに感染しているか、スパミングのために再利用されている可能性があります。
次に実行すべきステップは何ですか。	送信されているフローごとのデータ量、および送信に使用されているポートを確認します。 2 つの [最上位ピア(Top Peers)] レポート(1 つはプロトコルでフィルタ処理、もう 1 つはフローでフィルタ処理されたレポート)を実行して、ホストがネットワークにワームを伝播しているか、またはホストがスパム拡散のために SMTP リレーとして使用されているかどうかを確認します。 観測されたデータ量のうち、これらのピアから送信されているデータが想定された動作かどうかを確認します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	NetFlow を取得して連動させるには、FlowSensor が必要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのイベントがオフで	

イベントに関する質問	応答
あるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[しきい値(Threshold)]
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	アラームがトリガーされる、5 分間に大量電子メールアラートが発生した回数:デフォルトは 1。
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンされているホスト
ターゲットは何ですか。	ターゲットホストなし。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および 25/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HIGH_VOLUME_EMAIL (9)

ICMP Comm（通信）Admin **

送信元ホストが、「管理者が通信を禁止しています（communication is administratively prohibited）」というICMP メッセージを受信しました。このメッセージは、管理フィルタによってルータがパケットを転送できない場合に表示されます。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_COMM_ADMIN_PROHIBITED（302）

ICMP Dest（宛先）Host Admin **

送信元ホストが、「管理上、宛先ホストが禁止されています（destination host is administratively prohibited）」というICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_DEST_HOST_ADMIN_PROHIBITED（299）

ICMP Dest（宛先）Host Unk（不明）**

送信元ホストが、「宛先ホストが不明（destination host unknown）」エラーの発生を示す ICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_DEST_HOST_UNKNOWN（296）

ICMP Dest（宛先）Net Admin **

送信元ホストが、「管理者が宛先ネットワークを禁止しています（destination network is administratively prohibited）」というICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_DEST_NETWK_ADMIN_PROHIBITED（298）

ICMP Dest（宛先）Net Unk（不明）**

送信元ホストが、「宛先ネットワークが不明（destination network unknown）」エラーの発生を示すICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_DEST_NETWORK_UNKNOWN（295）

ICMP フラッド

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストは、5 分間に過剰な数の ICMP パケットを送信しました。
このイベントがトリガーされる場合、何を意味していますか。	これは、送信元ホストが DoS 攻撃（侵害を受けたまたはユーザーのどちらかによって発生する可能性があります）、誤設定されたネットワーク アプリケーション、または偵察（パケットが小さなグループではなく非常に広範囲の IP を使用して送信されているとき）に関係していることを示します。
次に実行すべきステップは何ですか。	送信されている ICMP パケットの数やレート、送信のタイミング、および送信先を確認します。これを調査する理想的な方法は、送信元ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、（アラームが存在する場合）終了時刻はアラームの終了時刻に設定します。プロトコル フィルタを [ICMP のみ（ICMP only）] に設定します。結果が返されたら、検索期間中に大部分の ICMP パケットがどこへ送信されたのかを確認します。このイベントの対象が、大量の ICMP パケットがあるフローのクライアントホストである場合、[クライアントパケット数（Client Packets）] または [クライアントパケットレート（pps）（Client Packet Rate（pps））] でソートできます。目的は、突出したフローを見つけることです。突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー	

イベントに関する質問	応答
設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[動作としきい値（Behavioral and Threshold）]
既定値と単位は何ですか。	
許容値	75
最小しきい値	5 分間で 1,800 ICMP パケット
最大しきい値	5 分間で 1 千万 ICMP パケット
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ICMP パケットを受信しているホスト
ターゲットは何ですか。	該当なし
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高 DDoS ソースインデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された X pp5m。予想値は Y pp5m、Z の許容値は最大で Y pp5m。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、および ICMP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_ICMP_FLOOD（7）

ICMP Frag（フラグメンテーション）が必要 **

送信元ホストが、「IP データグラムが大きすぎます（the IP datagram is too big）」という ICMP メッセージを受信しました。パケット フラグメンテーションが必要ですが、IP ヘッダーに DF ビットが設定されています。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_FRAG_NEEDED_DF_SET（293）

ICMP ホストの優先順位 **

送信元ホストが、「ホスト優先違反（host precedence violation）」の発生を示す ICMP メッセージを受信しました。これは最初のホップ ルータからホストに送信されるものです。送信元/宛先ホストまたはネットワーク、上位層プロトコル、および送信元/宛先ポートの特定の組み合わせで、要求された優先順位が許可されていないことを示します。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HOST_PRECEDENCE_VIOLATION（303）

ICMP ホスト到達不能 **

送信元ホストが、「ターゲット ホストに到達できません（target host is unreachable）」という ICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HOST_UNREACHABLE（290）

ICMP ホスト到達不能 TOS（タイプ オブ サービス）*

送信元ホストが、「指定されたサービス タイプではターゲット ホストに到達できません（target host is unreachable due to the specified Type of Service）」というICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_HOST_UNREACHABLE_FOR_SVC（301）

ICMP ネット到達不能 **

送信元ホストが、「ターゲット ネットワークに到達できません（the target network is unreachable）」というICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_NETWORK_UNREACHABLE（289）

ICMP ネット到達不能 TOS **

送信元ホストが、「指定されたサービス タイプではネットワークに到達できません（network is unreachable for the specified Type Of Service）」という ICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_NETWK_UNREACHABLE_FOR_SVC（300）

ICMP ポート到達不能 **

送信元ホストが、「宛先ポートに到達できません（the destination port is unreachable）」というICMPメッセージを受信しました。指定されたトランスポート プロトコル（UDP など）がデータグラムを逆多重化できませんが、送信者に通知するプロトコル メカニズムがありません。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PORT_UNREACHABLE（292）

ICMP 優先順位の遮断 **

送信元ホストが、「優先順位のカットオフ」が有効であるという ICMP メッセージを受信しました。ネットワーク オペレータが、操作に必要な最低の優先レベルを強制しています。データグラムが、このレベルを下回る優先順位で送信されました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PRECEDENCE_CUTOFF（304）

ICMP Proto（プロトコル）到達不能 **

送信元ホストが、「宛先プロトコルに到達できません（the destination protocol is unreachable）」というICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PROTOCOL_UNREACHABLE（291）

ICMP を受信

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これは、ターゲットホストが DoS 攻撃のターゲットにされているか、誤設定されたネットワーク アプリケーションであることを示します。
次に実行すべきステップは何ですか。	受信されている ICMP パケットの数やレート、受信のタイミング、および送信元を確認します。これを調査する理想的な方法は、ターゲット ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、(アラームが存在する場合)終了時刻はアラームの終了時刻に設定します。プロトコル フィルタを [ICMP のみ(ICMP only)] に設定します。 結果が返されたら、検索期間中に大部分の ICMP パケットがどこから送信されたのかを確認します。このイベントの対象が、大量の ICMP パケットがあるフローのクライアントホストである場合、[クライアント パケット数(Client Packets)] または [クライアント パケット レート(pps)(Client Packet Rate (pps))] で並べ替えることができます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	

イベントに関する質問	応答
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_ICMP_RECEIVED（50）

ICMP Src（送信元）ホストが隔離 **

送信元ホストが、「送信元ホストが隔離されているエラー（source host isolated error）」の発生を示す ICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SOURCE_HOST_ISOLATED（297）

ICMP Src（送信元）ルートが失敗 **

送信元ホストが、「送信元ルート失敗（source route failed）」エラーの発生を示す ICMP メッセージを受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

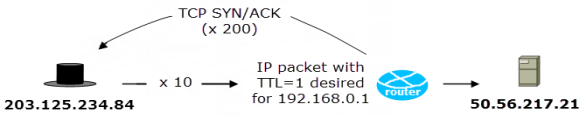
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SOURCE_ROUTE_FAIL（294）

ICMP タイムアウト

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

ICMP_Timeout



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	ICMP_Timeout(10)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	トレースルートツール、誤動作しているネットワークデバイス（ルーティングループなど）、ファイアウォーク技術（レイヤ 4 プロトコルを許可した ACL を判別するために ICMP タイムアウトを使用）の結果として生成された ICMP_TIME_EXCEEDED メッセージを検索します。
このイベントがトリガーされる場合、何を意味していますか。	ゲートウェイやファイアウォールを介して許可されているレイヤ 4 プロトコルを判断するために、ホストがネットワークをスキャンまたはマッピングしている可能性があります。
次に実行すべきステップは何ですか。	ホストが、ICMP 呼び出しとともに、ポートのスキャンを実行しているかどうかを確認します。 ICMP のパターンやさまざまなポートを識別するために、ポートおよびプロトコル別にピアを表示するレポートを実行します。通常はピア間で繰り返します。 ホストから送信されているデータパターンが想定された動作（セキュリティツール/デバイスなど）かどうかを判断します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	NetFlow を分析するには、FlowSensor が必要です。
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	×
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が	

イベントに関する質問	応答
設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットの宛先であるホスト
ターゲットは何ですか。	パケットの送信元であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし

イベントに関する質問	応答
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、および ICMP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_ICMP_TO（258）

内部 Tor エントリー検出

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ToR（正式には Onion ルータ）は、インターネット接続の匿名化に使用するネットワークであり、ToR ネットワークを終了する前に複数のリレーを経由して接続を送信することで機能します。ToR エントリ ノードは、ToR 接続が ToR ネットワークを移動し、終了する前に通過する最初のサーバーです。 このセキュリティイベントには、Secure Network Analytics によりモニターされていて、ToR エントリノードとしてアドバタイズされているホストが含まれています。ToR エントリノードをホストすることは必ずしも問題ではありませんが、ネットワークの管理者が気付かないうちに発生することがないようにするのが最善です。ToR 終了ノードとは異なり、ToR エントリ ノードは ToR ネットワーク内のトラフィックのみを転送するので、主な懸念事項は通常帯域幅です。
次に実行すべきステップは何ですか。	このイベントの調査の主な目的は技術的なものではありません。ToR エントリ ノードを認識しているユーザーがいるかどうか、および ToR エントリ ノードが許可されているかどうかを判断します。もしそうであれば、特定の許可されたホストのイベントを無効にします。ホストのセキュリティ イベント履歴を表示して、ホストが ToR エントリ ノードとしてアドバタイズされている間に通信を開始した時点を確認することもできます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス

イベントに関する質問	応答
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_ENTRY_INSIDE_HOST（515）

内部 Tor エントリー検出

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ToR（正式には Onion ルータ）は、インターネット接続の匿名化に使用するネットワークであり、ToR ネットワークを終了する前に複数のリレーを経由して接続を送信することで機能します。ToR 終了ノードは、ToR 接続が ToR ネットワークを終了する前に通過する最後のリレーであり、ネットワーク接続の接続先が最終的に接続の送信元と見なすものです。 このセキュリティイベントには、Secure Network Analytics によりモニターされていて、ToR 終了ノードとしてアドバタイズされているホストが含まれています。ToR 終了ノードをホストすることは、必ずしも問題ではありませんが、ネットワーク管理者が知らない場合は問題です。ToR 終了ノードのホスティングに関する主な懸念には、帯域幅の使用やノードを経由してアクティビティが匿名化されることの法的な懸念があります。
次に実行すべきステップは何ですか。	このイベントの調査の主な目的は技術的なものではありません。ToR 終了ノードを認識しているユーザーがいるかどうか、および ToR 終了ノードが許可されているかどうかを判断します。もしそうであれば、特定の許可されたホストのイベントを無効にします。ホストのセキュリティ イベント履歴を表示して、ToR 終了ノードとしてアドバタイズされ、通信を開始したのがいつかを確認することもできます。また、[最上位ピア（Top Peers）] レポートを実行し、サーバが消費した帯域幅の量と、帯域幅の移動先を確認できます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベント	高ポリシー違反インデックス、高リスクインデックス

イベントに関する質問	応答
が関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOR_EXIT_INSIDE_HOST（319）

低トラフィック

直近 5 分間のホストの平均トラフィックが、最小許容値を下回っています。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_LOW_TRAFFIC（29）

MAC アドレス違反

最後のアーカイブ時間以降、ホストの MAC アドレスの変更回数が、許容回数を超えました。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_MAC_ADDRESS（25）

メール拒否

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	SMTP（メール）サーバーではないホストからの過剰なメール拒否メッセージを検索します。
このイベントがトリガーされる場合、何を意味していますか。	メールサーバーではないホストがしきい値を超える数のメール拒否メッセージを受信しました。メール拒否メッセージはさまざまな理由で発生します。たとえば、送信側サーバー/IP がスパムサーバーとして登録されていて、意図したメール受信者が存在しない場合があります。
次に実行すべきステップは何ですか。	ホストがメールの送受信を目的としたホストであるかどうかを確認します。 ポート/プロトコル（25/SMTP）別の［最上位ピア（Top Peers）］レポートを実行して、サーバーの通信相手を確認します。 メールの送受信を目的としたホストの場合は、SMTP の設定をチェックして、設定が正しいことを確認します。 より広範囲のスパムやメールブラックリストをチェックして、そのホスト IP がリストされているかどうかを確認します。 サーバーが電子メールの送受信を目的としたサーバーではない場合は、ホストを調べて、サービスがインストールされたタイミング、およびホストがインストールを完了するために侵害を受けているかどうかを確認します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	フローセンサーは NetFlow を分析するために必要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	

イベントに関する質問	応答
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	外部ホスト
デフォルトでこのアラームがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	アラームがトリガーされる、5 分間にメール拒否アラートが発生した回数：デフォルトは 5。アラームがトリガーされる、5 分間に拒否メールが配信された回数：デフォルトは 5。
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	
通常のポリシー エディタを使用せずにイベントを調整できますか。	
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンされているホスト
ターゲットは何ですか。	ターゲットホストなし。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および 25/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_MAIL_REJECTS（12）

メール リレー

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	着信と発信の両方で、大量の電子メールトラフィックを累積し、受信よりも多くの電子メールを送信しているホストを検索します。
このイベントがトリガーされる場合、何を意味していますか。	ホストはメールリレーとして使用されている可能性があります。メールサーバーは、認証を使用するように設定されていない場合、SMTP ポート(25)を開いた状態、およびメールをリレーできるネットワークを制限する設定がない状態で、外部に開かれたままになっているため、スパマーに利用されている可能性があります。
次に実行すべきステップは何ですか。	通常の電子メールの量と、そのホストがメールの送受信を目的としたホストであるかどうかを確認します。サーバーが電子メールの送受信を目的としたサーバーの場合は、SMTP サーバーの設定を確認します。認証およびネットワークリレー制限を有効にします(有効になっていない場合)。 サーバーが電子メールの送受信を目的としたサーバーではない場合は、ホストを調べて、サービスがインストールされたタイミング、およびホストがインストールを実現するために侵害を受けているかどうかを確認します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	フローセンサーは NetFlow を分析するために必要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト

イベントに関する質問	応答
デフォルトでこのイベントがオフであるポリシーはどれですか。	外部ホスト
デフォルトでこのアラームがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	アラームがトリガーされる、5 分間に電子メールアラートが発生した回数：デフォルトは 5。
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンされているホスト
ターゲットは何ですか。	ターゲットホストなし。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および 25/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_MAIL_RELAY（10）

最大数のフローを開始

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはいくつかの異なる問題を示す可能性がありますが、最初に、これが偵察または DoS 攻撃に関係するホストの兆候であるかどうかを特定する必要があります。
次に実行すべきステップは何ですか。	これらの間の共通のリンクを見つけることによって、何がこれらのタイプのフローを引き起こしているのかを確認します。たとえば、これらのフローのほとんどが同じホストに向かっているのか、同じポートを使用して異なるホストに向かっているのか、などです。 これを確認する最適な方法は、いずれかの最上位レポートを実行することです。[最上位ピア(Top Peers)] レポートまたは [最上位ポート(Top Ports)] レポートのいずれかを開始できます。レポートにアクセスし、[フィルタ(Filter)] ダイアログの [ホスト(Hosts)] タブで [方向(Direction)] フィールドを [合計(Total)] に設定します。ここで、[クライアント(Client)] はイベントの送信元とし、[サーバー ホスト(Server Host)] の除外はなしにします。[日時(Date/Time)] タブで、イベントの開始アクティブ時間の 5 分前からイベントの開始アクティブ時間までを、期間として設定します。[詳細(Advanced)] タブで、[フロー(Flows)] でソートします。大半のフローが特定の行セットに適用されるかどうかを確認します(これが該当しない場合、提示された 2 つの最上位レポートのもう 1 つのレポートを実行します)。 突出したポートまたはピアを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_MAX_FLOWS_INIT（17）

最大数のフローの処理

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはいくつかの異なる問題を示す可能性がありますが、最初に、これが偵察または DoS 攻撃のターゲットになっているホストの兆候であるかどうかを特定する必要があります。通常大量のトラフィックを処理するホストの場合、しきい値と許容度の設定によっては通常の使用時の増加にすぎないことがあります。
次に実行すべきステップは何ですか。	これらの間の共通のリンクを見つけることによって、何がこれらのタイプのフローを引き起こしているのかを確認します。たとえば、これらのフローのほとんどが同じホストから発信されているのか、同じポートをターゲットにしている複数のホストから発信されているのか、などです。 これを確認する最適な方法は、いずれかの最上位レポートを実行することです。[最上位ピア(Top Peers)] レポートまたは [最上位ポート(Top Ports)] レポートのいずれかを開始できます。レポートにアクセスし、[フィルタ(Filter)] ダイアログの [ホスト(Hosts)] タブで [方向(Direction)] フィールドを [合計(Total)] に設定します。ここで、[サーバー ホスト(Server Host)] はイベントの送信元とし、[クライアント(Client)] の除外はなしにします。[日時(Date/Time)] タブで、イベントの開始アクティブ時間の 5 分前からイベントの開始アクティブ時間までを、期間として設定します。[詳細(Advanced)] タブで、[フロー(Flows)] でソートします。大半のフローが特定の行セットに適用されるかどうかを確認します(これが該当しない場合、提示された 2 つの最上位レポートのもう 1 つのレポートを実行します)。 突出したポートまたはピアを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベー	

イベントに関する質問	応答
スまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高ターゲットインデックス
数量はどの程度ですか。	• 異常インデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_MAX_FLOWS_SERVED（37）

新しいフローの開始

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはいくつかの異なる問題を示す可能性がありますが、最初に、これが偵察または DoS 攻撃に関係するホストの兆候であるかどうかを特定する必要があります。
次に実行すべきステップは何ですか。	これらの間の共通のリンクを見つけることによって、何がこれらのタイプのフローを引き起こしているのかを確認します。たとえば、これらのフローのほとんどが同じホストに向かっているのか、同じポートを使用して異なるホストに向かっているのか、などです。 これを確認する最適な方法は、いずれかの最上位レポートを実行することです。[最上位ピア(Top Peers)] レポートまたは [最上位ポート(Top Ports)] レポートのいずれかを開始できます。レポートにアクセスし、[フィルタ(Filter)] ダイアログの [ホスト(Hosts)] タブで [方向(Direction)] フィールドを [合計(Total)] に設定します。ここで、[クライアント(Client)] はイベントの送信元とし、[サーバー ホスト(Server Host)] の除外はなしにします。[日時(Date/Time)] タブで、イベントの開始アクティブ時間の 5 分前からイベントの開始アクティブ時間までを、期間として設定します。[詳細(Advanced)] タブで、[フロー(Flows)] でソートします。大半のフローが特定の行セットに適用されるかどうかを確認します(これが該当しない場合、提示された 2 つの最上位レポートのもう 1 つのレポートを実行します)。 突出したポートまたはピアを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス、高リスクインデックス
数量はどの程度ですか。	• 異常インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_NEW_FLOWS_INIT（18）

新しいフローの処理

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これはいくつかの異なる問題を示す可能性がありますが、最初に、これが偵察または DoS 攻撃のターゲットになっているホストの兆候であるかどうかを特定する必要があります。通常大量のトラフィックを処理するホストの場合、しきい値と許容度の設定によっては通常の使用時の増加にすぎないことがあります。
次に実行すべきステップは何ですか。	これらの間の共通のリンクを見つけることによって、何がこれらのタイプのフローを引き起こしているのかを確認します。たとえば、これらのフローのほとんどが同じホストに向かっているのか、同じポートを使用して異なるホストに向かっているのか、などです。 これを確認する最適な方法は、いずれかの最上位レポートを実行することです。[最上位ピア(Top Peers)] レポートまたは [最上位ポート(Top Ports)] レポートのいずれかを開始できます。レポートにアクセスし、[フィルタ(Filter)] ダイアログの [ホスト(Hosts)] タブで [方向(Direction)] フィールドを [合計(Total)] に設定します。ここで、[サーバー ホスト(Server Host)] はイベントの送信元とし、[クライアント(Client)] の除外はなしにします。[日時(Date/Time)] タブで、イベントの開始アクティブ時間の 5 分前からイベントの開始アクティブ時間までを、期間として設定します。[詳細(Advanced)] タブで、[フロー(Flows)] でソートします。大半のフローが特定の行セットに適用されるかどうかを確認します(これが該当しない場合、提示された 2 つの最上位レポートのもう 1 つのレポートを実行します)。 突出したポートまたはピアを見つけた後は、これが想定された動作であるかどうかを確認します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_NEW_FLOWS_SERVED（38）

新規ホスト アクティブ

新しいホストが検出されました。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

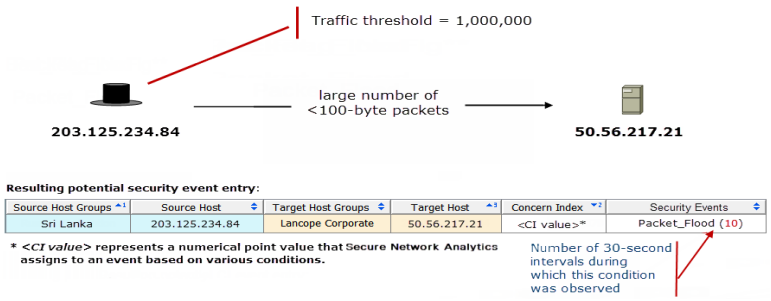
イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_NEW_HOST（14）

パケット フラッド

Packet_Flood



セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	長期間にわたって 1 つまたは複数のホストに送信されている、SYN フラッド攻撃ではない大量の小さなサイズのパケットを探します。(SYN フラッド攻撃は、3 ウェイ TCP ハンドシェイクが完了せず、TCP 接続が開いたままの場合に発生します)。
このイベントがトリガーされる場合、何を意味していますか。	送信元が、各パケットが通常の TCP パケットよりも小さいサイズのパケットを大量に送信しており、長期間送信されているため、送信元がターゲットに対してサービス妨害(DoS)攻撃やブルートフォース(総当たり)攻撃を試みていることを示しています。
次に実行すべきステップは何ですか。	送信元に対して [最上位ピア(Top Peers)] レポートを実行し、送信元が同様のフロー(長さは多少短く、サイズは他のホストに近い)を実行しているかどうかを確認します。攻撃者はさまざまなマシン上のリソースを測定し、脆弱なターゲットを特定しようとするので、これが攻撃の前兆となります。 ターゲットに対して [最上位ピア(Top Peers)] レポートを実行し、その他のマシンが侵害を受けているか、または攻撃に参加するために再利用されているが、アラームを出すタイミングしきい値にはまだ達していないのかどうかを確認します。 送信元を調べて、フローアクティビティが想定どおりに動作しているかどうかを確認します。 可能な場合は、ターゲットに DoS 緩和策を設定します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイア	フローセンサーは NetFlow を分析するために必要です。

このイベントに関する質問	応答
ウォールなど）	
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	このアラームは、内部ホストの PPS が 75,000 を超えている場合、または外部ホストの PPS が 50,000 を超えている場合にトリガーされます。
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし

イベントに関する質問	応答
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	短いパケットを送信している攻撃者。
ターゲットは何ですか。	パケットの受信者。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ソースインデックス、高リスクインデックス
数量はどの程度ですか。	• 高 DDoS ソースインデックス : True • CI : True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス : True • TI : True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：ターゲットホストは X です。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

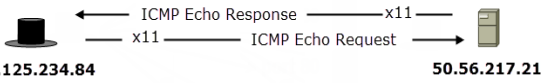
イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PACKET_FLOOD（8）

Ping

送信元ホストが ICMP エコー返信を送信し、ターゲットから ICMP エコー応答を受信しました。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Ping



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping(11)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

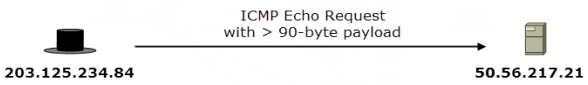
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PING_PROBE（257）

特大サイズの Ping パケット

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Ping_Oversized_Packet



Ping_Oversized_Packet events
also apply to ICMP Echo Replies

Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping_Oversized_Packet(58)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	標準サイズの 90 バイトより大きい ICMP パケットを検索します。対象パケットは、ICMP エコー要求（ホストがパケットの宛先の場合）または ICMP エコー応答（ホストがパケットの送信元の場合）です。
このイベントがトリガーされる場合、何を意味していますか。	データ漏洩または秘密通信のためのコバートチャネルが使用されていることを示している可能性があります。ICMP は、標準的な制御やエラー応答の目的で使用されますが、その他のデータを送受信するためにトンネル化できます。
次に実行すべきステップは何ですか。	[最上位サービス（Top Services）] レポートを実行して、過剰な ICMP トラフィックを、ホストで送受信されるその他すべてのトラフィックと区別します。 送信元ホストとターゲットホストを調べて、許可されていないサービスが実行されているかどうかを確認します。たとえば、プログラムまたはサービスをホスト、ターゲット、またはその両方で実行し、ICMPトラフィックをキャプチャまたは送信する必要があります。 ICMP アプリケーションでフィルタ処理された [最上位ピア（Top Peers）] レポートを実行（以下の注を参照）して、送信元またはターゲットが過剰な ICMP を介して他のピアと通信しているか、またはネットワーク外の好ましくないピアと通信（データ漏洩）しているかどうかを確認します。アプリケーションの ICMP でレポートをフィルタ処理します。 **注**：[接続（Connection）] セクションで、上位ピア レポートを設定するには、[アプリケーション（Applications）] の下の [選択（Select）] をクリックします。

このイベントに関する質問	応答
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラ	該当なし

イベントに関する質問	応答
メータを使用してイベントを調整できますか。	
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットを送信したホスト
ターゲットは何ですか。	パケットを受信したホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

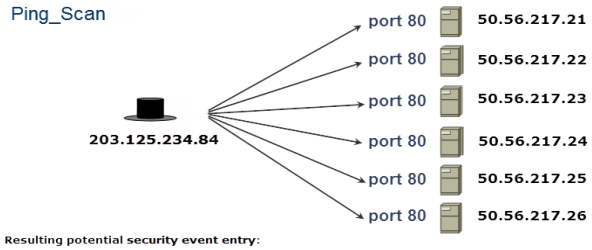
イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP とターゲット IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および ICMP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_LONG_PING（278）

Ping スキャン

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Ping_Scan(72)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	次の内容が正しい場合、スキャンイベントが記録されてアラームがトリガーされます。1) ICMP データグラムのタイムアウトを超過している。2) サービス要求ではない。3) 送信元ホストが宛先ホストではない。4) 送信元および宛先ポートが 38293（Norton AV Host Discovery に使用）ではない。
このイベントがトリガーされる場合、何を意味していますか。	ICMP スキャンは、複数のホストにわたる特定のポートまたは 1 つのホスト上の多数のポートのスキャンとは異なり、一般的に、特定のサービスではなく単に応答するホストの検索であり、偵察の早期のタイプです。ホスト ping スキャンは一般的に、さらに調査を行う可能性がある、ネットワーク上の他のアクティブ ホストを見つけようとしています。
次に実行すべきステップは何ですか。	ホストがスキャンしていた内容を判断します。これは ICMP ベースのスキャンであるため、主な目標は、UDP または TCP スキャンで行うような、どのような特定のサービスがターゲットになるのかではなく、どのようなホストがスキャンされているのかを把握することです。これは、フロー クエリを実行することで調査できます。このとき、クライアント ホストまたはサーバ ホストはイベントの送信元であり、期間はイベントの日、プロトコルは ICMP です。スキャン対象ホストにパターンがあるかどうかを確認するため、ピアの IP またはホスト グループに基づいて結果を並べ替えます。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、フローセンサーが必要です。Flow Collector sFlow エディションでは、追加コンポーネントは不要です。

このイベントに関する質問	応答
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンを実行するホスト
ターゲットは何ですか。	スキャンされているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情	Manager：詳細が表示されます。

イベントに関する質問	応答
報が表示されますか。	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは、送信元 IP、ターゲットのナチュラルクラス C ネットワーク（/24）、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および ICMP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PING_ADDR_SCAN（277）

ポート スキャン

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ポートスキャンでは、あるホストが別のホストと通信する際に使用される、ポート番号が 1024 以下の対象ポートの数がカウントされます。対象ポートの設定可能なしきい値を超えるとイベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	ホストが別のホストの「ポートスキャン」を行っていることを示します。これは、スキャン元のホストが、スキャン対象のホストによって提供可能なサービスを特定しようとしていることを意味します。これを外部ホストが実行している場合は、エクスプロイトの試みの前兆である可能性があります（ただし、インターネットからのスキャンが想定されます）。スキャン元のホストが内部ホストである場合は、攻撃者または侵害されたホストが、組織のネットワーク内で水平方向に移動しようとしていることを示す兆候である可能性があります。
次に実行すべきステップは何ですか。	このセキュリティ イベントの送信元ホストが外部ホストである場合は、スキャンされたホストと継続して通信しているかどうかを確認します。このためには、送信元ホストとターゲットホスト間でフロー クエリを開きます。送信元ホストと自社のネットワーク間のすべてのトラフィックを確認するだけでも有効な場合もあります。このホストの送信元が内部ホストである場合は、フロー クエリを使用して送信元とターゲット間のフローを確認し、それが想定された動作であるかを判定します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	送信元ポートの番号が 1024 と等しいか、それよりも大きい可能性があります。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー	スキャンを実行するホストでポート スキャンを有効にする必要があります。

イベントに関する質問	応答
設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	なし
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	しきい値ベース
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	はい
該当する場合、調整可能な属性と単位は何ですか。	調整可能なパラメータは、イベントを開始させるために必要なスキャンされたポートの数で、デフォルトでは 10 になっています。
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	該当なし

イベントに関する質問	応答
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンを実行するホスト
ターゲットは何ですか。	スキャンされているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホスト
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP とターゲット IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻でフィルタ処理されます。

イベントに関する質問	応答
	デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

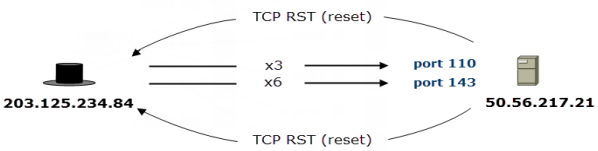
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_PORT_SCAN (55)

リセット/TCP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Reset/tcp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Reset/tcp-110(3) Reset/tcp-143(6)

*** *<CI value>* represents a numerical point value that the Secure Network Analytics engine assigns to an event based on various conditions.**

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ターゲットポートからの、次の条件を満たしている TCP リセットパケットを検索します。1) HTTP で使用されていない。2) TCP アクティビティが存在しない。3)「宛先到達不能」の ICMP タイプがある。4) SNMP ではない。5) 非特権ポート(1024 以降)を使用していない。
このイベントがトリガーされる場合、何を意味していますか。	TCP 会話が中断された場合、または会話に問題がある場合に、TCP リセットパケットが送信されます。これらのパケットは、会話の途中に誤動作しているデバイス(ロードバランサなど)によって送信されたり、ポートが開いていないか使用できない場合にターゲットによって送信されたりします。後者の場合、複数のポートがこの方法で応答していて、それらのポートがグループに含まれているか、または一致している場合、通常は、ホストで使用可能なサービス(存在する場合)を確認するためにネットワークスキャンが実行されています。
次に実行すべきステップは何ですか。	送信元に対して [最上位ピア(Top Peers)] レポートを実行して、フローで使用されているポートにパターンがあるかどうかを確認します。 送信元が、スキャンを許可されているセキュリティホスト、デバイス、またはアプライアンスであるかどうかを確認します。許可されていない場合は、ホストを調べて、スキャンしているソフトウェアやサービス、および侵害の証拠を確認します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	フローセンサーは NetFlow を分析するために必要です。

このイベントに関する質問	応答
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットの宛先であるホスト
ターゲットは何ですか。	パケットの送信元であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情	Manager：詳細が表示されます。

イベントに関する質問	応答
報が表示されますか。	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

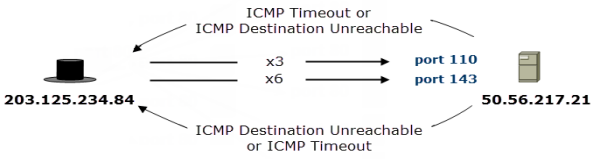
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TCP_PROBE（262）

リセット/UDP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Reset/udp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Reset/udp-110(3) Reset/udp-143(6)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ターゲットポートからの、次の条件を満たしている UDP リセットパケットを検索します。1) HTTP で使用されていない。2) UDP アクティビティが存在しない。3)「宛先到達不能」の ICMP タイプがある。4) SNMP ではない。5) 非特権ポート(1024 以降)を使用していない。
このイベントがトリガーされる場合、何を意味していますか。	閉じているか、または使用できない UDP ポートへの通信が試行された場合に、UDP リセットパケットが送信されます。これらのパケットは、会話の途中に誤動作しているデバイスによって送信されたり、ポートが開いていないか使用できない場合にターゲットによって送信されたりします。後者の場合、複数のポートがこの方法で応答していて、それらのポートがグループに含まれているか、または一致している場合、通常は、ホストで使用可能なサービス(存在する場合)を確認するためにネットワークスキャンが実行されています。
次に実行すべきステップは何ですか。	送信元に対して [最上位ピア(Top Peers)] レポートを実行して、フローで使用されているポートにパターンがあるかどうかを確認します。 送信元が、スキャンを許可されているセキュリティホスト、デバイス、またはアプライアンスであるかどうかを確認します。許可されていない場合は、ホストを調べて、スキャンしているソフトウェアやサービス、および侵害の証拠を確認します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	フローセンサーは NetFlow を分析するために必要です。

このイベントに関する質問	応答
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットの宛先であるホスト
ターゲットは何ですか。	パケットの送信元であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情	Manager：詳細が表示されます。

イベントに関する質問	応答
報が表示されますか。	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/UDP として関連付けられたポート、および UDP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_PROBE（261）

通信中のスキャナ

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ネットワークをスキャンしていたホストが、スキャン済みのいずれかのターゲットホストと双方向会話を行っています。これは、デフォルトでは、内部ホストポリシーと外部ホストポリシーの両方で有効になっています。ただし、ネットワーク管理およびスキャナ ロールのポリシーではデフォルトで無効になっています。
このイベントがトリガーされる場合、何を意味していますか。	アドレススキャナとしてフラグ付けされたマシンが、スキャン済みのいずれかのマシンと通信しています。送信元が認可されたスキャナではない場合は、スキャナがその攻撃ベクトルと一致するターゲットを発見して侵害に成功したことを示している可能性があります。
次に実行すべきステップは何ですか。	送信元が認可されたスキャナであるかどうかを確認します。 送信元が認可されたスキャナではない場合は、送信元に対してピアレポートを実行して、通信していた他のホストを確認し、フローの数やフローサイズが増大したピアを選択します。 送信元とターゲットを調べて侵害の兆候を確認します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	
注意	

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]

イベントに関する質問	応答
デフォルトでこのイベントがオフであるポリシーはどれですか。	なし
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのアラームがオフであるポリシーはどれですか。	なし
このイベントは調整可能ですか。	×
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	lc_threshold value addr_scan_talking_stale_timeout は、グローバルスキャンリストがリセットされるまでの時間を制御します。
該当する場合、調整可能な値の代替ロケーションは何ですか。	なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	通信中のスキャナ
ターゲットは何ですか。	通信中のスキャン対象ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元ホストポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、クライアントバイトおよびサーバーバイト（両方とも 1 以上）でフィルタ処理されます。 デスクトップクライアント：アラーム時刻に開始されるクライアントとサーバー間のフロー。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_ADDR_SCAN_TALKING（63）

低速接続フラッド

このセキュリティ イベントはどのようなものですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストは、過剰な数の同時接続を単一の宛先に送信しました。各接続の秒あたりのパケット レートが非常に低くなっています。
このイベントがトリガーされる場合、何を意味していますか。	ホストが非常に低いパケット レートでターゲットへの複数の接続を開始していることを示します。このような接続の目的は、多くの帯域幅を必要とせずに開いている接続を維持することです。これはアプリケーション サービス妨害（DoS）攻撃の一種です。これは、大量の帯域幅を必要とせずに使用できないサービスをレンダリングできるため、脆弱なホストに対して簡単に攻撃を実行できるようになり、多くの場合検出が困難になります。
次に実行すべきステップは何ですか。	目的は、ターゲットへの接続が正当であるかどうか、およびターゲットでパフォーマンスが低下しているかどうかを判断することです。これは、2 つの内部ホスト間で悪意のある動作である可能性がありますが、内部ホストと外部ホスト間ではより興味深いイベントである可能性があります。まず、イベント日に対して、イベントの送信元およびターゲット間でフロー クエリを実行します。フローが継続しているかどうかをメモします。継続していない場合は、サービス停止は発生しておらず、問題ではない可能性があります。また、送信元とターゲットの両方のホストのセキュリティ イベント履歴もチェックできます。送信元ホストでは、複数のターゲットに対して、または継続的にこのイベントが発生しているでしょうか。継続的に発生している場合は、詳しく調査する必要があります。ターゲット ホストで、継続的ではなく一度に、ターゲット ホストに対して多数のホストがこのイベントをトリガーしているでしょうか。これは分散型サービス妨害（DDoS）攻撃の兆候である可能性があります。また、イベントが継続的に発生している場合は、サービスがホストしている何らかのアプリケーションの通常の動作であることがあります。この場合、特定のホストに対してイベントをオフにすることを検討してください。関連するトラフィックがフロー センサーによって観測された場合は、パフォーマンス レポートを実行し、トラフィックの特性のために SRT（サーバー応答時間）が影響を受けていないかどうかを確認します。これが正当なトラフィックであるかどうかを示している可能性があります。
非標準のフロー データが必要ですか。	なし

このイベントに関する質問	応答
（FlowSensor、プロキシ、ファイアウォールなど）	
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	外部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[しきい値（Threshold）]
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	30
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	はい

イベントに関する質問	応答
該当する場合、調整可能な属性と単位は何ですか。	アラームをトリガーするのに必要な低速接続の数
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	過剰な数の低速接続を送信しているホスト
ターゲットは何ですか。	過剰な数の低速接続を受信しているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高 DDoS ソースインデックス : True • CI : True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス : True • TI : True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：ターゲットホスト X は、ポート Z を使用した Y の低 pps 接続を観測しました。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 2 分前からイベントの最後のアクティブ時刻までの時間範囲、ポート 80/TCP、443/TCP、および 8080/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SLOW_CONNECTION_FLOOD（44）

スパム送信元

このセキュリティ イベントはどのようなものですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	過剰な量の電子メールを発信している送信元、またはアドレスとメッセージの比率が過大な（つまり、1 つのメッセージに多くの受信者がいる）送信元を検索しています。
このイベントがトリガーされる場合、何を意味していますか。	サーバーは、スパム電子メールの送信に使用されている可能性があります。原因は、侵害や設定不備である可能性があります。この結果、パブリック IP がブラックリストやスパムリストによってブロックされることがあります。
次に実行すべきステップは何ですか。	送信元が電子メールの送受信を目的とした送信元であるかどうかを確認します。電子メールの送受信を目的としていない場合は、発信電子メールの量が増え始めた時期を確認します。その時期の前後で、侵害の兆候や、インストールされた悪意のあるソフトウェアを探します。 送信元が電子メールの送受信を目的としている場合は、送信元が最初にネットワークに出現した時期を確認して、侵害の兆候を探します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	フローセンサーは NetFlow を分析するために必要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	外部ホスト

イベントに関する質問	応答
デフォルトでこのアラームがオンであるポリシーはどれですか。	内部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	アラームがトリガーされる、5 分間にスパム送信元アラートが発生した回数：デフォルトは 5。スパム電子メールアラートが発生する電子メールあたりのアドレスの数：デフォルトは 10。
既定値と単位は何ですか。	
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンされているホスト
ターゲットは何ですか。	ターゲットホストなし。
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻、および 25/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

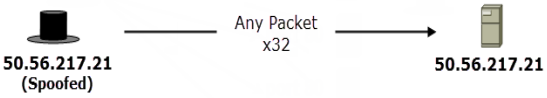
イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SPAM_SOURCE（11）

Src=Des（送信元 = 宛先）

IP データグラムの送信元ホストとターゲットホストが同じです。通常このセキュリティ イベントは、ルーティングの中断を目的として細工されたパケットが原因になっています。

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Src=Des



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	50.56.217.21	Lancope Corporate	50.56.217.21	<CI value>*	Src=Des(32)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	異常インデックス
数量はどの程度ですか。	• 異常インデックス：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_BOOMERANG（273）

SSH リバース シェル

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	リバース シェルに見える SSH セッションを検出します。外部ホストに送信されるデータが、受信するデータを上回っています。
このイベントがトリガーされる場合、何を意味していますか。	このセキュリティ イベント アラームの目的は、SSH リバース シェルを見つけることです。攻撃者は、発信 SSH 接続のように見える接続を介して、感染したネットワークへのオンデマンド アクセスを確立する方法として、SSH リバース シェルを使用することがあります。これにより攻撃者は、ファイアウォールのようなもので着信接続がブロックされる場合でもシステムへのアクセスを維持することができます。
次に実行すべきステップは何ですか。	このセキュリティ イベントを調査するときは、多くは内部ネットワーク上に置かれている、送信元ホストの役割を正しく保つことが重要です。問題になっているホストが正式な容量の SSH または SFTP サーバーである場合、これは誤ったアラームであることがあります。このようなデバイスからこれらのアラームを制限するには、ホストポリシーの調整が必要な場合があります。しかし、内部ホストにそのようなデバイスの明確な容量がない場合には、問題になっている外部ホストのアイデンティティを確立する必要があります。既知のエンティティによって所有されているかを確認し、そうである場合は誤ったアラームである可能性があります。既知のエンティティではない場合は、ターゲット ホストで [最上位ピア(Top Peers)](発信)レポートを実行します。このレポートには、外部ホストと通信されたデータ量を基準に並べ替えられた、内部ピアのリストが示されています。これは、ご使用の環境内で非常に一般的なピアであるかどうかを示し、動作が予期されているものであるかどうかを判断する上で役立つことがあります。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	なし
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[しきい値（Threshold）]
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	トラフィックが 10,000 バイトを超えると同時に、クライアント データのパーセンテージが 60 を超える。
最大しきい値	クライアントデータのパーセンテージが 80 を超える。
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし

イベントに関する質問	応答
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	外部ホストの SSH ポートへのトラフィックがある内部ホスト
ターゲットは何ですか。	SSH トラフィックを受信している外部ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• Command and Control 上位インデックス : True • CI : True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI : True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細をクリックすると何が表示されますか。	Manager : 送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント : 該当なし

イベントに関する質問	応答
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、およびポート 22/TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

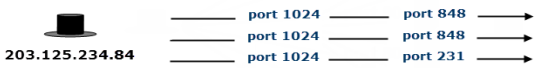
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SSH_REV_SHELL（61）

ステルス スキャン/TCP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Stealth_Scan/tcp



Stealth_Scan/udp probes operate in the same manner as Stealth_Scan/tcp probes.

Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Stealth_Scan/tcp-848(2) Stealth_Scan/tcp-231(1)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストが、同じ送信元ポートを使用して、ターゲット ホスト上の複数のポートに同時に接続していました。この動作は、raw ソケットを使用して TCP または UDP 接続を確立するアプリケーションがあることを示しています。このセキュリティ イベントでは、セキュリティ イベントが認識される前に最後にアクセスしたターゲット ポートが示されます。
このイベントがトリガーされる場合、何を意味していますか。	該当なし
次に実行すべきステップは何ですか。	該当なし
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、フローセンサーが必要です。Flow Collector sFlow エディションでは、追加コンポーネントは不要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー	

イベントに関する質問	応答
設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	×
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンを実行するホスト
ターゲットは何ですか。	スキャンされているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	「1」ポリシー: • CI:True 「8000」ポリシー: • 高偵察インデックス:True • CI:True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	「1」ポリシー: • TI:True 「8000」ポリシー: • TI:True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager:詳細が表示されます。 デスクトップクライアント:該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager:送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント:該当なし
関連フローについてどのような情報が表示されますか。	Manager:フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時

イベントに関する質問	応答
	刻までの時間範囲、<port>/TCP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TCP_STEALTH（272）

ステルス スキャン/UDP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Stealth_Scan/udp

Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope	50.56.217.21	<CI value>*	Stealth_Scan/udp-5000(2) Stealth_Scan/udp-5001(2)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	このイベントは、オペレーティングシステムによって自然に生成されたものではないトラフィックを Secure Network Analytics が検出するとトリガーされ、検出を避けるために意図的にパケットが作成されていることを示しています。
このイベントがトリガーされる場合、何を意味していますか。	該当なし
次に実行すべきステップは何ですか。	該当なし
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	Flow Collector NetFlow エディションでは、フローセンサーが必要です。Flow Collector sFlow エディションでは、追加コンポーネントは不要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	

イベントに関する質問	応答
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
このイベントは調整可能ですか。	×
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	スキャンを実行するホスト
ターゲットは何ですか。	スキャンされているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	「1」ポリシー: • CI:True 「8000」ポリシー: • 高偵察インデックス:True • CI:True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	「1」ポリシー: • TI:True 「8000」ポリシー: • TI:True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager:詳細が表示されます。 デスクトップクライアント:該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager:送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント:該当なし
関連フローについてどのような情報が表示されますか。	Manager:フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/UDP として関連付けられたポート、および UDP でフィルタ処理されます。

イベントに関する質問	応答
	デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_STEALTH（271）

データ蓄積の疑い

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	Suspect Data Hoarding では、リセット期間中に、ある内部ホストがクライアントとして他の内部ホストからダウンロードする TCP/UDP データ量がモニターされます。所定のホストでデータ量がしきい値を超えた場合にイベントが開始されます。このしきい値は、ベースライン化によって自動的に設定するか、手動で設定することができます。
このイベントがトリガーされる場合、何を意味していますか。	このイベントは、特定のホストがデータを収集して、漏洩やその他通常よりも大規模な内部データのダウンロードの準備をしていることを示している可能性があります。
次に実行すべきステップは何ですか。	ダウンロードされたデータ量と、どこからダウンロードされたかを確認します。 これを調査する場合、[最上位ピア(Top Peers)](着信)レポートを実行するのが最適な方法です。クエリ期間をイベント日に設定します。[クライアント(Client)] または [サーバー ホスト(Server Host)] がセキュリティイベントの送信元 IP で、[その他のホスト(Other Host)] が [内部ホスト(Inside Hosts)] ホスト グループであるように、レポートをフィルタ処理します。目的は、データの大部分を送信した、突出したピアを見つけることです。 突出したピアを検出したら、観測されたデータ量のうち、これらのピアから送信されているデータが想定された動作かどうかを判断します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	該当なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリ	[内部ホスト(Inside Host)] ホスト グループに対してこのイベ

イベントに関する質問	応答
ガーされるために必要なポリシー設定は何ですか。	ントを有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	ファイアウォール、プロキシ、および NAT デバイス
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト; 外部ホスト; ファイアウォール、プロキシ、NAT デバイス
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	バリアンスベースまたはしきい値ベース。
既定値と単位は何ですか。	
許容値	92
最小しきい値	24 時間のクライアント ペイロードのバイト数：500 M
最大しきい値	24 時間でダウンロードされたペイロードのバイト数：1 T
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	はい
該当する場合、調整可能な属性と単位は何ですか。	ベースラインまたは許容値を反映していない特定のバイト数をトリガー オフにするようイベントを設定することができます。
通常のポリシー エディタを使用せずにイベントを調整できますか。	いいえ
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	いいえ

イベントに関する質問	応答
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ペイロード データを受信している内部ホスト
ターゲットは何ですか。	ペイロード データを送信している 1 つまたは複数の内部ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高データ ホーディング インデックス、高リスクインデックス
数量はどの程度ですか。	• 高データ ホーディング インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W バイト。予測値は X バイト、Y の許容値は最大で Z バイト。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情	Manager：フローは、送信元対内部ホスト、イベントのアクティ

イベントに関する質問	応答
報が表示されますか。	ブ日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、53/UDP、67/UDP、68/UDP、161/TCP、161/UDP、162/TCP、162/UDP、クライアントバイトおよびサーバーバイト（両方とも 1 以上）、および 1000 バイト以上の合計バイト数でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SUSPECT_DATA_HOARD（315）

データ損失の疑い

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	このイベントがトリガーされた場合は、内部ホストがクライアントとして外部ホストにアップロードした TCP または UDP ペイロードデータの累積量が内部ホストに適用されているポリシーで設定されたしきい値を超えたことを示します。これはバリアンス ベースのアラームとして使用できます。
このイベントがトリガーされる場合、何を意味していますか。	ホストを使用して、許容できる以上の情報量がインターネットにアップロードされています。これは、何者かが外部バックアップサービスを使用し、悪意を持って企業データを漏洩している可能性があります。
次に実行すべきステップは何ですか。	アップロードされたデータの量、およびそのデータの移動先を判断します。 これを判断する最適な方法は、セキュリティ イベントの送信元であるホストで [最上位ピア（Top Peers）]（発信）レポートを実行することです。このレポートで、クライアントをイベントの送信元とし、サーバー ホスト グループを [外部ホスト（Outeside Hosts）] に設定するフィルタ処理を行います。目的は、データの大部分を受信した、突出したピアを見つけることです。 突出したピアを検出したら、観測されたデータ量のうち、これらのピアが受信しているデータが想定された動作かどうかを判断します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	×
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー	送信元ホストとターゲット ホストの両方に適用されるポリシーでこのイベントを有効にする必要があります。

イベントに関する質問	応答
設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアント IP（Client IP）] ポリシー
デフォルトでこのイベントがオフであるポリシーはどれですか。	[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, & NAT Devices）]、[ゲストワイヤレス（Guest Wireless）]、[メールサーバーポリシー（Mail Server Policy）]、[信頼できるインターネットホスト（Trusted Internet Hosts）]
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]、[クライアント IP（Client IP）] ポリシー
デフォルトでこのアラームがオフであるポリシーはどれですか。	[ファイアウォール、プロキシ、およびNATデバイス（Firewalls, Proxies, & NAT Devices）]、[ゲストワイヤレス（Guest Wireless）]、[メールサーバーポリシー（Mail Server Policy）]、[信頼できるインターネットホスト（Trusted Internet Hosts）]
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	バリアンスベースまたはしきい値ベース。
既定値と単位は何ですか。	
許容値	50
最小しきい値	24 時間のクライアント ペイロードのバイト数：1 G
最大しきい値	24 時間のクライアント ペイロードのバイト数：100 G
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	はい
該当する場合、調整可能な属性と単位は何ですか。	ベースラインまたは許容値を反映していない特定のバイト数をトリガー オフにするようイベントを設定することができます。
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし

イベントに関する質問	応答
イベントにデフォルトの緩和策が設定されていますか。	いいえ
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	クライアントとして機能し、ペイロード データを送信している内部ホスト
ターゲットは何ですか。	内部ホストからのペイロード データを受信している 1 つまたは複数の外部ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高漏洩インデックス、高リスクインデックス
数量はどの程度ですか。	• 高漏洩インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W バイト。予測値は X バイト、Y の許容値は最大で Z バイト。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると	Manager：送信元ホストのセキュリティイベントが表示されま

イベントに関する質問	応答
何が表示されますか。	す。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは、送信元 IP と外部ホスト、イベントのアクティブ日の開始時刻（リセット時間）からイベントの最後のアクティブ時刻でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_DATA_LOSS（40）

疑わしい長いフロー

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	このセキュリティ イベントは、リモート デスクトップ テクノロジーと VPN が使用する接続など、長期間確立される接続を検出しますが、スパイウェア、IRC ボットネット、およびそのほかの通信を隠れて行う方法などの通信チャネルも検出できます。このイベントは必ずしも悪意のある動作または感染を示すわけではありませんが、対象ホストの識別に役立ちます。 システムのアップグレードを実行すると、このセキュリティイベントは 6 日後に再び発生し始めます。
次に実行すべきステップは何ですか。	目的は、このトラフィックが通常のアクティビティを表しているかどうかを判断することです。多くの場合、トラフィックの宛先を特定することで判断できます。送信元と宛先の IP アドレス、ポート、サービス、フローの開始時刻、geo-location 情報、およびユーザー名（もしあれば）など、フローの詳細情報を取得するために、セキュリティ イベントの関連フロー テーブルをピボットとして調査を開始するのが適切です。 ターゲットが外部ホストの場合、外部参照を実行して IP の所有者を確認します。ターゲットが既知のビジネス パートナーまたは信頼ネットワークである場合、ターゲットを該当するグループに分類してください。ホストを外部参照しても特定が十分ではない場合は、[最上位ピア（Top Peers）] レポートを実行してターゲットと通信している他のホストを識別し、同様の動作を特定します。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	Command and Control 上位インデックス、高リスクインデックス
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SUSPECT_LONG_FLOW（33）

疑わしい非常に長いフロー

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	このセキュリティ イベントは、一部の指揮統制I（C&C）アクティビティで使用されるハートビート接続と、スパイウェア、IRC ボットネット、およびその他通信を隠れて行う方法など、他の疑わしい通信チャネルを識別します。このイベントは Beaconing Host に似ていますが、転送するデータの量が少ない場合に双方向通信が含まれることが異なります。このイベントでは、バックグラウンドの Web サイト ハートビートも特定できる点に注意してください。
次に実行すべきステップは何ですか。	目的は、このトラフィックが通常のアクティビティを表しているかどうかを判断することです。多くの場合、トラフィックの宛先を特定することで判断できます。送信元と宛先の IP アドレス、ポート、サービス、フローの開始時刻、geo-location 情報、およびユーザー名（もしあれば）など、フローの詳細情報を取得するために、セキュリティ イベントの関連フロー テーブルをピボットとして調査を開始するのが適切です。 ターゲットが外部ホストの場合、外部参照を実行して IP の所有者を確認します。ターゲットが既知のビジネス パートナーまたは信頼ネットワークである場合、ターゲットを該当するグループに分類してください。ホストを外部参照しても特定が十分ではない場合は、[最上位ピア（Top Peers）] レポートを実行してターゲットと通信している他のホストを識別し、同様の動作を特定します。また、[フロートラフィック（Flow Traffic）] レポートを実行して疑わしいトラフィック パターンを視覚化することもできます。C&C サーバーへのハートビートにより、少量のバイトが転送される周期的なパターンが示されます。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	Command and Control 上位インデックス、高リスクインデックス
数量はどの程度ですか。	• Command and Control 上位インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス（High Target Index）
数量はどの程度ですか。	• TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_QUIET_LONG_DURATION_FLOW（48）

疑わしい UDP アクティビティ

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストが、UDP ポートで複数のホストをスキャンしていることが特定され、サイズの大きい UDP パケットを以前スキャンした別のホストに送信しました。このタイプの動作は、「SQL Slammer」や「Witty」など、多くのシングル パケット UDP ベースのワームの特徴に合致しています。このセキュリティ イベントの調査をただちに行ってください。
このイベントがトリガーされる場合、何を意味していますか。	送信元ホストが、以前スキャンしたホストのいずれかに単一の大きな UDP パケットを送信しました。
次に実行すべきステップは何ですか。	このアクティビティをただちに調査してください。これは UDP ベースの多くのワームで最もよく識別されているアクティビティです。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	NetFlow を取得して連動させるには、フローセンサーが必要です。
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]

イベントに関する質問	応答
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットを送信したホスト
ターゲットは何ですか。	スキャンされていて、パ

イベントに関する質問	応答
	ケットを受信しているホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：送信元ホストは、Z に対するピアとして X サービス（Y プロトコル）を使用しています。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 35 分前からイベントの最後のアクティブ時刻までの時間範囲、<port>/UDP として関連付けられたポートでフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SUSPECT_UDP_ACTIVITY（24）

SYN フラッド

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストは過剰な数の TCP 接続要求（SYN パケット）を 5 分間送信しました。これは、サービス妨害（DoS）攻撃または非ステルス性のスキャンアクティビティの可能性を示しています。
このイベントがトリガーされる場合、何を意味していますか。	送信元ホストが DoS 攻撃（感染したホスト、またはユーザーが発生元の可能性があります）または誤設定されたネットワーク アプリケーションに関係していることを示しています。さらに大きな分散型サービス妨害（DDoS）の一環として、ターゲットの帯域幅を消費する目的で大量の SYN パケットが送信されることがよくあります。ただし、アプリケーションが TCP 接続の確立に失敗して、非常に高いレートで TCP 接続を再度確立しようとしていることも考えられます。多数の IP に対して相対的にパケット数が少ない場合も偵察行為を示している可能性があります。
次に実行すべきステップは何ですか。	送信されている SYN の数やレート、送信のタイミング、および宛先を確認します。これを調査する理想的な方法は、送信元ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、（アラームが存在する場合）終了時刻はアラームの終了時刻に設定します。結果が返されたら、検索期間中に大部分の SYN パケットがどこへ送信されたのかを確認します。このイベントの対象が、大量の SYN パケットがあるフロー内のクライアントホストの場合、[クライアント SYNパケット数（Client SYN Packets）]、[クライアントパケット数（Client Packets）]、または [クライアントパケットレート（pps）（Client Packet Rate（pps））] でソートできます。目的は、突出したフローを見つけることです。突出したフローを見つけた後は、これが設定ミスかどうかを判断します。内部から内部への SYN フラッドは多くの場合設定ミスです。内部から外部への SYN フラッドでの設定ミスはたまに発生します。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[動作としきい値（Behavioral and Threshold）]
既定値と単位は何ですか。	該当なし
許容値	75
最小しきい値	期間あたり 10 個の SYN パケット
最大しきい値	期間あたり 4 百万個の SYN パケット
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が	

イベントに関する質問	応答
設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	SYN パケットを送信しているホスト
ターゲットは何ですか。	なし
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ソースインデックス、高リスクインデックス
数量はどの程度ですか。	• 高 DDoS ソースインデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W pp5m。予想値は X pp5m、Y pp5m の許容値は最大で Z pp5m。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情	Manager：フローは送信元 IP、イベントの最初のアクティブ時

イベントに関する質問	応答
報が表示されますか。	刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SYN_FLOOD（5）

SYN を受信

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	これは、ターゲット ホストが DoS 攻撃のターゲットにされているか、誤設定されたネットワーク アプリケーションであることを示します。大きな DDoS または Dos 攻撃の一環として、ターゲットの帯域幅を消費する目的で大量の SYN パケットが送信されることがよくあります。ただし、アプリケーションが TCP 接続の確立に失敗して、非常に高いレートで TCP 接続を再度確立しようとしている場合も考えられます。
次に実行すべきステップは何ですか。	送信されている SYN パケットの数やレート、送信のタイミング、および送信元を確認します。これを調査する理想的な方法は、ターゲット ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、（アラームが存在する場合）終了時刻はアラームの終了時刻に設定します。 結果が返されたら、検索期間中に大部分の SYN パケットがどこから送信されたのかを確認します。このイベントのターゲットが、大量の SYN パケットがあるフロー内のサーバー ホストの場合、[クライアント SYN パケット数（Client SYN Packets）]、[クライアント パケット数（Client Packets）]、または [クライアント パケット レート（pps）（Client Packet Rate (pps)）] で並べ替えることができます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが設定ミスかどうかを判断します。内部から内部への SYN フラッドは多くの場合設定ミスです。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_SYNS_RECEIVED（19）

ファントムとの通信

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	あるホストが初めて通信するホストに重要なトラフィックを送信していて、フローが存在する場合は常に、通信しているホストの「ファントムリスト」にサイレントホストを追加します。ホストのファントムリストが設定されている最大許容数を超えて増加すると、通信中のホストから一番最近確認されたファントムホストにイベントがトリガーされます。
このイベントがトリガーされる場合、何を意味していますか。	コンピュータが存在しないホストに未承認トラフィックの送信を試行することはほとんどないため、このようなアクティビティに関与するホストには注意します。何者かが偵察行為をしようとしている可能性もありますが、ホストに設定ミスがあり存在しないホストと通信している可能性もあります。
次に実行すべきステップは何ですか。	現在、このセキュリティイベントはフロークエリの一部として「ファントム」を指定できないため、調査は少し難しくなりますが、理解することはできます。この調査の目的は、応答しないホストへ送信されたフローを検出し、これらのフローの共通スレッドから推測することです。 一方向のフローを検出します。時間範囲としてセキュリティ イベントの日付を設定したフロー クエリを作成します。クライアント ホストをセキュリティ イベントの送信元 IP にして、サーバ ホストを任意の IP にします。 これらのフローに共通する次のようなスレッドを検出します。宛先がすべて同じサーバ ポートになっている。すべてほぼ同時刻に発生した。かつて存在したホストが宛先になっている。フローに存在するホスト数。 **デスクトップクライアントの場合**：[トラフィック（Traffic）] タブで、サーバーパケットの数が 0 以下になるようにフィルタリングします（設定の [以上（Greater than or equal to）] の部分は空のままにします）。すべてがキャプチャされるようにするには、イベントの送信元をフロークエリのサーバーに設定し、クライアントパケット数を 0 以下に設定して、このクエリを繰り返す必要があります。これで結果が追加されることはあまりありません。 **Web アプリケーションの場合**：[フロー検索（Flow Search）] ページの [拡張サブジェクトオプション（Advanced Subject Options）] セクションで、[パケット（Packets）] フィールドを 1 未満に、[方向（Orientation）] フィールドを [サーバー（Server）] に設定します。すべてがキャプチャされるように

このイベントに関する質問	応答
	するには、イベントの送信元をフロークエリのサーバーに設定し、クライアントパケット数を 1 未満に設定して、このクエリを繰り返す必要があります。これで結果が追加されることはあまりありません。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト、外部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト、外部ホスト
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	[しきい値（Threshold）]
既定値と単位は何ですか。	該当なし
許容値	該当なし

イベントに関する質問	応答
最小しきい値	特定のホストが到達しようとしている 3 つのファントムホスト。
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ファントムホストと通信しようとしているホスト。
ターゲットは何ですか。	ファントムホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	

イベントに関する質問	応答
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントのアクティブな日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、バイトおよびパケット（両方とも 1 未満）でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TALKS_TO_PHANTOMS（59）

ターゲット データの蓄積

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	Target Data Hoarding では、リセット期間中に、ある内部ホストがサーバーとして他の内部ホストに配信する TCP/UDP データ量をモニターします。所定のホストでデータ量がしきい値を超えた場合にイベントが開始されます。このしきい値は、ベースライン化によって自動的に設定するか、手動で設定することができます。
このイベントがトリガーされる場合、何を意味していますか。	このイベントは、1 台以上の内部ホストが通常よりも多いデータを特定の内部ホストから収集している可能性と、漏洩や不正使用の準備である可能性を示しています。
次に実行すべきステップは何ですか。	転送されたデータ量とこの一括データの移動先を確認します。 これを判断する最適な方法は、セキュリティ イベントの送信元であるホストで [最上位ピア(Top Peers)](発信)レポートを実行することです。[クライアント(Client)] または [サーバー ホスト(Server Host)] がセキュリティ イベントのターゲット IP で、[その他のホスト(Other Host)] が [内部ホスト(Inside Hosts)] ホスト グループであるように、レポートをフィルタ処理します。目的は、アップロード データの大部分を受信した、突出したピアを見つけることです。 突出したピアを検出したら、観測されたデータ量のうち、これらのピアが受信しているデータが想定された動作かどうかを判断します。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	該当なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリ	[内部ホスト(Inside Host)] ホスト グループに対してこのイベ

イベントに関する質問	応答
ガーされるために必要なポリシー設定は何ですか。	ントを有効にする必要があります。
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	ファイアウォール、プロキシ、および NAT デバイス
デフォルトでこのアラームがオンであるポリシーはどれですか。	なし
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト; 外部ホスト; ファイアウォール、プロキシ、NAT デバイス
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	バリアンスベースまたはしきい値ベース。
既定値と単位は何ですか。	
許容値	92
最小しきい値	24 時間のクライアント ペイロードのバイト数：500 M
最大しきい値	24 時間でダウンロードされたペイロードのバイト数：1 T
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	はい
該当する場合、調整可能な属性と単位は何ですか。	ベースラインまたは許容値を反映していない特定のバイト数をトリガー オフにするようイベントを設定することができます。
通常のポリシー エディタを使用せずにイベントを調整できますか。	いいえ
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	いいえ

イベントに関する質問	応答
該当する場合、それは何ですか。	該当なし

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ペイロード データを送信している内部ホスト
ターゲットは何ですか。	ペイロード データを受信している 1 つまたは複数の内部ホスト
イベントのトリガーを引き起こすポリシーはどれですか。	送信元のポリシー
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高データ ホーディング インデックス、上位ターゲットインデックス
数量はどの程度ですか。	• 高データ ホーディング インデックス：True • TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W バイト。予測値は X バイト、Y の許容値は最大で Z バイト。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：ターゲットのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローはターゲット IP 対内部ホスト、イベントのアクティブな日の開始時刻（リセット時刻）からイベントの最後のア

イベントに関する質問	応答
	クティブ時刻、1 以上のサーバーバイト、および 1000 バイト以上の合計バイト数でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

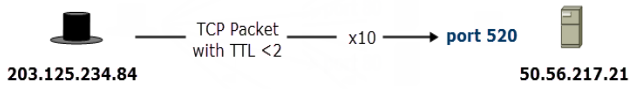
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TARGET_DATA_HOARD (316)

タイムアウト/TCP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Timeout/tcp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Timeout/tcp-520(10)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストが送信した TCP パケット内の TTL が 2 未満でした。トレースルートは UDP で発生するため、TCP パケットの TTL が短い場合は、多くの場合、悪意のあるアクティビティ（ファイアウォークなど）またはネットワークの不具合（ルーティング ループなど）を示します。
このイベントがトリガーされる場合、何を意味していますか。	該当なし
次に実行すべきステップは何ですか。	該当なし
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	NetFlow を分析するには、FlowSensor が必要です。
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	

イベントに関する質問	応答
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットの送信元であるホスト
ターゲットは何ですか。	パケットの宛先であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/TCP として関連付けられたポート、および TCP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

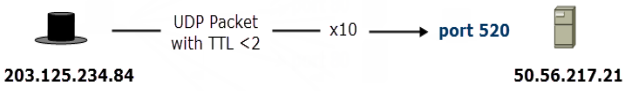
このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TCP_TO（260）

タイムアウト/UDP

このセキュリティ イベントに関連付けられているアラームに対する緩和策はありません。

Timeout/udp



Resulting potential security event entry:

Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
Singapore	203.125.234.84	Lancope Corporate	50.56.217.21	<CI value>*	Timeout/udp-520(10)

* *<CI value>* represents a numerical point value that Secure Network Analytics assigns to an event based on various conditions.

セキュリティイベントの内容

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストが送信した UDP パケット内の TTL が 2 未満でした。UDP でトレースルートが行われるため、このセキュリティ イベントはかなり頻繁に発生する可能性があります。ただし、数値が大きい場合はネットワークの不具合（ルーティング ループなど）を示している傾向があります。Norton Antivirus サーバーに対応するため、ポート 38293 が UDP タイムアウトから除外されています。
このイベントがトリガーされる場合、何を意味していますか。	該当なし
次に実行すべきステップは何ですか。	該当なし
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	NetFlow を分析するには、フローセンサーが必要です。
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリ	

イベントに関する質問	応答
ガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	内部ホスト、外部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	
デフォルトでこのアラームがオフであるポリシーはどれですか。	内部ホスト、外部ホスト
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	

イベントに関する質問	応答
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	パケットの送信元であるホスト
ターゲットは何ですか。	パケットの宛先であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高偵察インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：詳細が表示されます。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントの最初のアクティブ時刻の 1 分前からイベントの最終アクティブ時刻までの時間範囲、<port>/UDP として関連付けられたポー

イベントに関する質問	応答
	ト、および UDP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_TO（259）

接触済み

アラーム対象ホスト（高リスクインデックス アラームまたは Trapped Host セキュリティ イベントが発生しているホスト）からターゲット ホストへの接続が開始され、データ交換が行われました。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	攻撃インデックス、高ターゲットインデックス
数量はどの程度ですか。	• 攻撃インデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TOUCHED（28）

閉じ込められたホスト

設定済みのサービスに含まれていないポートで、トラップホストグループのホストとの 1 日あたりの許容通信試行数のしきい値をホストが超えました。これは「少なくて遅い」スキャンアクティビティの可能性を示しています。システムは、攻撃者、スキャンされているポート、スキャンされているホストが検出されないように、さらにはワームのリリース前に予備スキャンを実行するために、これらの種類のスキャンを実行します。

ホストグループの [ホストグループ管理(Host Group Management)] ページで [このグループの未使用アドレスをスキャンするホストをトラップする(Trap hosts that scan unused addresses in this group)] チェックボックスをオンにして、該当ホストグループに対するこの種類のアクティビティの追跡を有効にします。この拡張機能は、一定数のホストが含まれ、固定 IP アドレスを使用する十分に管理された特定の小さなホストグループ(重要な業務サーバーなど)に対してのみ有効にしてください。そうすることで、ネットワークの最も重要なエリアに侵入するホストを検出できます。

[外部ホスト(Outside Hosts)] ホストグループの未使用アドレスをスキャンするホストは、トラップされたホストの計算からは除外されるため、[外部ホスト(Outside Hosts)] ホストグループでこの設定を有効にするかどうかに関係なく、これらのホストはトラップされたホストのアラートやアラームを生成しません。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高偵察インデックス、高リスクインデックス
数量はどの程度ですか。	• 高偵察インデックス:True • CI:True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ターゲット インデックス(High Target Index)
数量はどの程度ですか。	• TI:True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_TRAPPED_HOST（34）

UDP フラッド

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	送信元ホストは、5 分間に過剰な数の UDP パケットを送信しました。これは、サービス妨害（DoS）攻撃または非ステルス性のスキャンアクティビティの可能性を示しています。
このイベントがトリガーされる場合、何を意味していますか。	送信元ホストが、DoS 攻撃（感染したホスト、またはユーザーが攻撃元である可能性があります）、誤設定されたネットワーク アプリケーション、または送信元からの秒あたりの UDP パケット数が異常に多い接続に関係していることを示しています。さらに大きな DDoS 攻撃の一環として、ターゲットの帯域幅を消費する目的で大量のパケットが送信されることがよくあります。 ただし、UDP パケット レートが高いのは、SYN パケット レートが高いことよりも一般的なため、下限しきい値や許容度設定が原因で大量の誤検知が発生する場合があります。多数の IP に対して相対的にパケット数が少ない場合も偵察行為を示している場合があります。
次に実行すべきステップは何ですか。	送信されている UDP パケットの数やレート、送信のタイミング、および送信先を確認します。これを調査する理想的な方法は、送信元ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、（アラームが存在する場合）終了時刻はアラームの終了時刻に設定します。プロトコル フィルタを [UDP のみ（UDP only）] に設定します。 結果が返されたら、検索期間中に大部分の UDP パケットがどこへ送信されたのかを確認します。このイベントの対象が、大量の UDP パケットがあるフローのクライアントホストである場合、[クライアント パケット数（Client Packets）] または [クライアント パケット レート（pps）（Client Packet Rate（pps））] で並べ替えることができます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。想定された動作の例としては、UDP ベースの VPN 接続や UDP を使用した Web サーバーへのアップロード（Google でよく見られます）などがあります。

このイベントに関する質問	応答
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	該当なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト（Inside Hosts）]、[外部ホスト（Outside Hosts）]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	はい
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	両方（Both）
既定値と単位は何ですか。	該当なし
許容値	75
最小しきい値	5 分間で 3.6k UDP パケット
最大しきい値	5 分間で 10M UDP パケット
バリアンス ベースではないパラ	該当なし

イベントに関する質問	応答
メータを使用してイベントを調整できますか。	
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	UDP パケットを送信しているホスト
ターゲットは何ですか。	なし
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 高 DDoS ソースインデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：観測された W pp5m。予測値は X pp5m、Y の許容値は最大で Z pp5m。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP、イベントの最初のアクティブ時刻の 5 分前からイベントの最後のアクティブ時刻までの時間範囲、および UDP でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_FLOOD（6）

UDP を受信

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	ホストされているターゲットが、DoS 攻撃、誤設定されたネットワーク アプリケーション、または送信元からの秒あたりの UDP パケット数が異常に多い接続のターゲットになっていることを示しています。さらに大きな DDoS 攻撃の一環として、ターゲットの帯域幅を消費する目的で大量のパケットが送信されることがよくあります。ただし、UDP パケット レートが高いのは、SYN パケット レートが高いことよりも一般的なため、下限しきい値や許容度設定が原因で大量の誤検知が発生する場合があります。
次に実行すべきステップは何ですか。	この目的は、受信されている UDP パケットの数やレート、受信のタイミング、および送信元を確認することです。 これを調査する理想的な方法は、ターゲット ホストに対してフロー クエリを実行することです。クエリの開始時刻を、関連付けられているセキュリティ イベントの開始時刻の 5 分前に設定し、(アラームが存在する場合)終了時刻はアラームの終了時刻に設定します。プロトコル フィルタを [UDP のみ(UDP only)] に設定します。 結果が返されたら、検索期間中に大部分の UDP パケットがどこから送信されたのかを確認します。このイベントのターゲットが、大量の UDP パケットがあるフローのサーバー ホストである場合、[クライアント パケット数(Client Packets)] または [クライアント パケット レート(pps)(Client Packet Rate (pps))] で並べ替えることができます。目的は、突出したフローを見つけることです。 突出したフローを見つけた後は、これが想定された動作であるかどうかを確認します。想定された動作の例は、UDP ベースの VPN 接続です。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高 DDoS ターゲットインデックス、高ターゲットインデックス
数量はどの程度ですか。	• 高 DDoS ターゲットインデックス：True • TI：True

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_UDP_RECEIVED（49）

アクティブ ホスト監視

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	特定のホストが通信していることが観測されたことを通知するユーザー設定のイベントです。このイベントの目的は、ユーザーがウォッチリストに特定のホストを追加した理由によりますが、一般的に、このイベントは監視対象ホストからの送受信が不適切であることを示します。
次に実行すべきステップは何ですか。	このセキュリティ イベントの調査手順は、ホストがウォッチ リストに追加されたコンテキストに大きく依存しています。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_WATCH_LIST（31）

アクティブ ポート監視

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントがトリガーされる場合、何を意味していますか。	特定のホストが特定のポートを経由して通信していることが観測されたことを通知するユーザー設定のイベントです。このイベントの目的は、ユーザーがウォッチリストに特定のホストを追加した理由によりますが、一般的に、このイベントは監視対象ホストからの送受信が不適切であることを示します。
次に実行すべきステップは何ですか。	このセキュリティ イベントの調査手順は、ポートがウォッチ リストに追加されたコンテキストに大きく依存しています。

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	高ポリシー違反インデックス、高リスクインデックス
数量はどの程度ですか。	• 高ポリシー違反インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_WATCH_PORT（13）

ワームの活動

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ホストが複数のサブネットにわたってスキャンを行い、特定のポートに接続しました。
このイベントがトリガーされる場合、何を意味していますか。	このセキュリティ イベントは、ホストが各種内部ネットワーク間で過度の量の偵察行為を実行している兆候を示しています。これはホストが感染しており、ネットワーク全体に感染を拡大しようとしている可能性を示します。
次に実行すべきステップは何ですか。	このイベントにはノイズが含まれている可能性があり、役に立つかどうかは、ネットワーク スキャナがどの程度特定され、ネットワーク スキャナ ホスト グループに追加されるかによります。これを行うことで、デバイスはワーム アクティビティを無効にするポリシーを継承します。ワーム アクティビティは多くの場合、異なる論理 /24 の範囲間の類似ポートに対するホスト スキャニングによって行います。[最上位ポート(Top Ports)](発信)レポートを実行して開始します。イベントの期間と、送信元 IP となるクライアント ホストを設定します。リストされている送信先 IP 範囲に関係なく任意の種類のホストをスキャンできるため、内部ホスト、外部ホスト、またはその両方で検索が必要かどうかを判断できます。[フィルタ(Filter)] ダイアログの [ホスト(Hosts)] タブで、[サーバー(Server)] フィルタを適切に設定し、[詳細(Advanced)] タブで [返されるレコードの順序(Order the records returned by)] に [フロー(Flows)] を設定します。結果をピアに基づいて並べ替えます。最初はリストの上部をフローまたはピア別に並び替えて、所属先を持たない、あるいは異常に高い数値を示す突出したポートを検出します。IP アドレスを右クリックしてフローにピボットすることで、さまざまな IP アドレスを表示したり、特定のホスト グループが主なターゲットとなっているかどうかを判断したりします。また、右クリックして [最上位ピア(Top Peers)] レポートにピボットすることで、トラフィックがターゲット全体に均等に行き渡っているかどうかを判断できます。スキャンに対応するホストの割合に着目することも可能です。この時点でホストをスキャンしたユーザーとスキャンされたポートを判断できるようにする必要があります。
非標準のフロー データが必要ですか。 (FlowSensor、プロキシ、ファイアウォールなど)	

このイベントに関する質問	応答
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	
デフォルトでこのイベントがオンであるポリシーはどれですか。	外部ホスト
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	外部ホスト
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし

イベントに関する質問	応答
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ワームであるホスト
ターゲットは何ですか。	ワームの被害者であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：ポート X サービス名（Y プロトコル）でのワームアクティビティ。

イベントに関する質問	応答
	デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元およびターゲット IP、イベントのアクティブ日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、および <port>/TCP および <port>/UDP として関連付けられたポートでフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_WORM_ACTIVITY（35）

ワーム伝播

これはどのようなセキュリティ イベントですか。

このイベントに関する質問	応答
このイベントはどのような動作によって引き起こされますか。	ホストが複数のサブネットをスキャンして、特定のポートに接続しました。このホストは以前に、ワーム アクティビティ アラームがトリガーされたホストによってスキャンおよび接続されたことがあります。
このイベントがトリガーされる場合、何を意味していますか。	このイベントは別の侵害を受けたホストによって侵害されたホストを探そうとするため、そのホストが他のホストを侵害しようとします。これは、1）ホストが、複数のホストをスキャンしている別のホストによりスキャンされ、2）スキャンされたホストが他のホストのスキャンを開始するという一連のイベントに関係しています。
次に実行すべきステップは何ですか。	問題になっているホストで［最上位ピア（Top Peers）］レポートを実行します。その他のピアホストが、指定したポートのどの情報カテゴリに接続しているのかを調べ、問題になっているポートでレポートをフィルタリングします。これらのホストが不明なスキャナであり、これまでに観測されたスキャニング アクティビティには参加していないことを確認します。既知のスキャナの場合は、リスクが軽減します。不明なスキャナの場合は、スキャンが正当ではないか、未承認であるためリスクが増加します。この場合、このイベントはホストが感染していることを示す可能性があります。
非標準のフロー データが必要ですか。 （FlowSensor、プロキシ、ファイアウォールなど）	なし
注意	なし

このセキュリティイベントに使用できるポリシー設定がありますか。

イベントに関する質問	応答
このセキュリティ イベントがトリガーされるために必要なポリシー設定は何ですか。	

イベントに関する質問	応答
デフォルトでこのイベントがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのイベントがオフであるポリシーはどれですか。	
デフォルトでこのアラームがオンであるポリシーはどれですか。	[内部ホスト(Inside Hosts)]、[外部ホスト(Outside Hosts)]
デフォルトでこのアラームがオフであるポリシーはどれですか。	
このイベントは調整可能ですか。	いいえ
このイベントは、バリアンス ベースまたはしきい値ベースのいずれですか。	該当なし
既定値と単位は何ですか。	該当なし
許容値	該当なし
最小しきい値	該当なし
最大しきい値	該当なし
バリアンス ベースではないパラメータを使用してイベントを調整できますか。	該当なし
該当する場合、調整可能な属性と単位は何ですか。	該当なし
通常のポリシー エディタを使用せずにイベントを調整できますか。	該当なし
該当する場合、調整可能な値の代替ロケーションは何ですか。	該当なし
イベントにデフォルトの緩和策が設定されていますか。	
該当する場合、それは何ですか。	

このセキュリティイベントはカテゴリにどのように関与しますか。

イベントに関する質問	応答
イベントの送信元は何ですか。	ワームであるホスト
ターゲットは何ですか。	ワームの被害者であるホスト
イベントのトリガーを引き起こすポリシーはどれですか。	
送信元で、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• 攻撃インデックス：True • CI：True
ターゲットで、セキュリティ イベントが関与するアラーム カテゴリはどれですか。	
数量はどの程度ですか。	• TI：True

Secure Network Analytics で利用可能な情報は何ですか。

イベントに関する質問	応答
アラームの詳細にはどのような情報が表示されますか。	Manager：Y サービス名（Z プロトコル）を使用して X 方向の送信元ホストにワームが伝播しました。 デスクトップクライアント：該当なし
アラームの詳細をクリックすると何が表示されますか。	Manager：送信元ホストのセキュリティイベントが表示されます。 デスクトップクライアント：該当なし
関連フローについてどのような情報が表示されますか。	Manager：フローは送信元 IP およびターゲット IP、イベントのアクティブな日の開始時刻（リセット時刻）からイベントの最後のアクティブ時刻、クライアントバイトおよびサーバーバイト（両方とも 1 以上）でフィルタ処理されます。 デスクトップクライアント：フローは直前の 5 分間でフィルタ処理されます。

このセキュリティイベントの応答についてどのような情報が利用可能ですか。

イベントに関する質問	応答
イベント ID は何ですか。	SEC_ID_WORM_PROPAGATION (36)

アラームカテゴリ

アラーム カテゴリは、セキュリティ イベントの定義済みリストがインデックス ポイント（定義された一連の基準に一致する動作の出現観測数を表す値）を提供する「バケット」です。ネットワークアクティビティが、このアラームカテゴリに指定されている定義済みの一連の基準を満たしているか、または超えている場合、アラームがトリガーされます。各アラームカテゴリには、これに対してインデックスポイントを与え、アラームを生成する原因となる、セキュリティイベントの独自のリストが含まれています。一部のセキュリティ イベントは、複数のアラーム カテゴリに関与します。セキュリティイベントは、独自のアラームも生成できます（生成するように設定されている場合）。

アラームカテゴリには、ホストアラームだけが含まれています。以下に示す Secure Network Analytics で使用される他の 4 つのアラームタイプは含まれていません。

- Manager システムアラーム
- フロー コレクタ システム アラーム
- エクスポータまたはインターフェイスアラーム
- ホストグループ関係アラーム

- これらのアラームの詳細については、デスクトップクライアントのヘルプにある「アラームリスト」トピックを参照してください。
- アラームの設定を行うには、Manager でホストポリシーマネージャを使用します。

使用されるアラーム カテゴリを次に示します。次の表は、アラームカテゴリと関連付けられたインデックス、アラームカテゴリに割り当てられたセキュリティイベント、および各セキュリティイベントのデフォルトポイントの数を示しています。

異常（Abnormaly）

ホストが異常な動作をしているか、普通ではないトラフィックを生成している活動の別のカテゴリーと一致していないことを示すイベントを追跡します。

次のセキュリティイベントは異常アラームに関連付けられます。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトでカテゴリに割り当てられるポイント数
Connection from Bogon Address Attempted	900
Connection from Bogon Address Successful	14,400
Connection to Bogon Address Attempted	8,100
Connection to Bogon Address Successful	14,400

セキュリティ イベントの名前	デフォルトでカテゴリに割り当てられるポイント数
High Total Traffic	監視対象の推定ペイロードデータに基づく。
High Traffic	監視対象の推定ペイロードデータに基づく。
ICMP Frag Needed	700
ICMP Host Precedence	700
ICMP Host Unreach TOS	2,800
ICMP Net Unreach TOS	2,800
ICMP Precedence Cutoff	700
ICMP Proto Unreach	700
ICMP Src Route Failed	700
Low Traffic	3,000
Max Flows Initiated	監視対象のフロー数に基づく。
Max Flows Served	監視対象のフロー数に基づく。
New Flows Initiated	監視対象のフロー数に基づく。
Src=Des	4,000

コマンドおよびコントロール（Command & Control）

C&C サーバーと連絡を取ろうとするネットワーク内のボットに感染したサーバーまたはホストの存在を示しています。

C&C アラームに関連付けられているセキュリティイベントを次に示します。2 番目の列は、セキュリティイベントの発生時にアラームカテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Beaconing Host	9,000
Bot Command And Control Server	32,000

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Bot Infected Host – Attempted C&C Activity	22,400
Bot Infected Host – Successful C&C Activity	32,000
Fake Application Detected	4,000
Ping_Oversized_Packet	2,400
SSH Reverse Shell	11,700
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000

リスクインデックス（Concern Index）

リスクインデックスがリスクインデックス（CI）しきい値を超えているホスト、または急速に増加しているホストを追跡します。

リスクインデックスとターゲット インデックス カテゴリは同じセキュリティイベントを使用します。イベントが送信元ホストによってトリガーされると、リスクインデックスアラームが発生します。イベントがターゲット ホストによってトリガーされると、Target Index アラームが発生します。

リスクインデックスアラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
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	4,800
Bad_Flag_RST	4,800

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Beaconing Host	9,000
Bot Command and Control Server	32,000
[ホストがボットに感染：C&C行動を試行（Bot Infected Host – Attempted C&C Activity）]	22,400
[ホストがボットに感染：C&C行動成功（Bot Infected Host – Successful C&C Activity）]	32,000
Brute Force Login	10,800
Connection from Bogon Address Attempted	900
Connection from Bogon Address Successful	14,400
Connection from Tor Attempted	1,000
Connection from Tor Successful	4,000
Connection to Bogon Address Attempted	8,100
Connection to Bogon Address Successful	14,400
Connection to Tor Attempted	5,400
Connection to Tor Successful	5,400
Fake Application Detected	4,000
Flow Denied	162
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
Half Open Attack	12,600

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
High File Sharing Index	監視対象の推定ペイロードデータに基づく。
High SMB Peers	32,000
High Total Traffic	監視対象の推定ペイロードデータに基づく。
High Traffic	監視対象の推定ペイロードデータに基づく。
High Volume Email	3,200
ICMP フラッド	監視対象の ICMP パケット数に基づく。
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

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
ICMP_Timeout	1
Inside Tor Entry Detected	32,000
Inside Tor Exit Detected	32,000
Low Traffic	3,000
MAC アドレス違反	6,300
Mail Rejects	2,400
Mail Relay	2,400
Max Flows Initiated	監視対象のフロー数に基づく。
New Flows Initiated	監視対象のフロー数に基づく。
New Host Active	2,800
Packet Flood	5,600
Ping	7
Ping_Oversized_Packet	2,400
Ping Scan	14,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2
Scanner Talking	180
Slow Connection Flood	10,800
Spam Source	9,000
SSH Rev Shell	11,700
Stealth_Scan/tcp	5,200

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Stealth_Scan/udp	4,800
Suspect Data Hoarding	監視対象の推定ペイロードデータに基づく。
Suspect Data Loss	監視対象の推定ペイロードデータに基づく。
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000
Suspect UDP Activity	9,000
[SYN フラッド（SYN Flood）]	監視対象の SYN フラグ数に基づく。
Talks to Phantoms	1,440
Timeout/tcp	4
Timeout/udp	3
Trapped Host	11,700
UDP Flood	監視対象の UDP パケット数に基づく。
Watch Host Active	32,000
Watch Port Active	32,000
Worm Activity	400
Worm Propagation	19,200

データの蓄積（Data Hoarding）

ネットワーク内のソース ホストまたはターゲットホストが 1 つ以上のホストから異常な量のデータがダウンロードしたことを示しています。

Data Hoarding アラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Suspect Data Hoarding	監視対象の推定ペイロードデータに基づく。
Target Data Hoarding	監視対象の推定ペイロードデータに基づく。

DDoS ソース（DDos Source）

ホストが DDoS 攻撃のソースであると判明したことを示しています。

DDoS ソースアラームに関連付けられているセキュリティイベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Half Open Attack	12,600
[ICMP フラッド（ICMP Flood）]	監視対象の ICMP パケット数に基づく。
Packet Flood	5,600
Slow Connection Flood	10,800
[SYN フラッド（SYN Flood）]	監視対象の SYN フラグ数に基づく。
[UDP フラッド（UDP Flood）]	監視対象の UDP パケット数に基づく。

DDoS ターゲット（DDoS Target）

ホストが DDoS 攻撃のターゲットであると判明したことを示しています。

DDoS ターゲットアラームに関連付けられているセキュリティイベントを次に示します。2 番目の列は、セキュリティイベントの発生時にアラームカテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Connection From Bogon Address Attempted	900
Connection From Bogon Address Successful	14,400

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Half Open Attack	12,600
ICMP を受信	監視対象の ICMP パケット数に基づく。
New Flows Served	監視対象のフロー数に基づく。
Packet Flood	5,600
Slow Connection Flood	10,800
SYNs Received	監視対象の SYN フラグ数に基づく。
UDP Received	監視対象の UDP パケット数に基づく。

漏洩（Data Exfiltration）

異常な量のデータが転送される内部ホストと外部ホストを追跡します。ホストでこれらのイベントが多数トリガーされ、その数が設定されているしきい値を超えると、データ漏洩アラームが発生します。

データ漏洩アラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Suspect Data Loss	監視対象の推定ペイロードデータに基づく。

エクスプロイト（Exploitation）

ワームの増殖や総当りのクラッキングなどを通じた、ホストによる相互に侵入しようとする直接の試みを追跡します。

エクスプロイト アラームに関連付けられているセキュリティイベントを次に示します。2 番目の列は、セキュリティイベントの発生時にアラームカテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Brute Force Login	10,800

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Frag:First_Too_Short	6,000
Frag:Sizes_Differ	6,000
Frag:Packet_Too_Long	6,000
High SMB Peers	32,000
Scanner Talking	180
Suspect UDP Activity	9,000
Touched	8,000
Worm Activity	400
Worm Propagation	19,200

ポリシー違反（Policy Violation）

サブジェクトは、通常のネットワーク ポリシーに違反する動作を示しています。

Policy Violation アラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Connection from Tor Attempted	1,000
Connection from Tor Successful	4,000
Connection to Tor Attempted	5,400
Connection to Tor Successful	5,400
High File Sharing Index	監視対象の推定ペイロードデータに基づく。
High Volume Email	3,200
Inside Tor Entry Detected	32,000

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Inside Tor Exit Detected	32,000
MAC Address Violation	6,300
Mail Rejects	2,400
Mail Relay	2,400
New Host Active	2,800
Spam Source	9,000
Watch Host Active	32,000
Watch Port Active	32,000

[偵察(Recon)]

TCP または UDP を使用し、組織のホストと対立している不正で、潜在的に悪意のあるスキャンの存在を示しています。これらのスキャンは、「偵察」とも呼ばれますが、ネットワークに対する攻撃の早期指標であり、このスキャンは、組織の内外からくる場合があります。

Recon アラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
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	4,800
Bad_Flag_RST	4,800

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Flow Denied	162
High SMB Peers	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
ICMP_Net_Unreach	7
ICMP_Port_Unreach	7
ICMP_Src_Host_Isolated	7
ICMP_Timeout	1
Ping	7
Ping_Scan	14,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
Talks To Phantoms	1,440

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Timeout/tcp	4
Timeout/udp	3
Trapped Host	11,700

ターゲット インデックス（Target Index）

内部ホストが複数の許容可能なスキャンまたはその他の悪意のある攻撃の受信者であったことを示しています。

リスクインデックスとターゲット インデックス カテゴリは同じセキュリティイベントを使用します。イベントが送信元ホストによってトリガーされると、リスクインデックスアラームが発生します。イベントがターゲット ホストによってトリガーされると、Target Index アラームが発生します。

Target Index アラームに関連付けられているセキュリティ イベントを次に示します。2 番目の列は、セキュリティ イベントの発生時にアラーム カテゴリに割り当てられるデフォルトのポイント数を示します。一部のセキュリティ イベントにはポイントが設定されていません。これらのイベントは可変です。

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Bad_Flag_ACK	4,800
Bad_Flag_All	4,800
Bad_Flag_NoFlg	4,800
Bad_Flag_Rsrvd	4,800
Bad_Flag_RST	4,800
Bad_Flag_SYN_FIN	4,800
Bad_Flag_URG	4,800
Beaconing Host	9,000
[ホストがボットに感染：C&C行動を試行（Bot Infected Host – Attempted C&C Activity）]	22,400
[ホストがボットに感染：C&C行動成功（Bot Infected Host – Successful C&C Activity）]	32,000

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Brute Force Login	10,800
Connection From Bogon Address Attempted	900
Connection From Bogon Address Successful	14,400
Connection From Tor Attempted	1,000
Connection From Tor Successful	4,000
Connection To Bogon Address Attempted	8,100
Connection To Bogon Address Successful	14,400
Fake Application Detected	4,000
Flow Denied	162
Frag:First_Too_Short	6,000
Frag:Packet_Too_Long	6,000
Frag:Sizes_Differ	6,000
Half Open Attack	12,600
High SMB Peers	32,000
ICMP Received	監視対象の ICMP パケット数に基づく。
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

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
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
Inside Tor Entry Detected	32,000
Inside Tor Exit Detected	32,000
MAC Address Violation	6,300
Max Flows Served	監視対象のフロー数に基づく。
New Flows Served	監視対象のフロー数に基づく。
Packet Flood	5,600
Ping	7
Ping_Oversized_Packet	2,400
Port Scan	10,800
Reset/tcp	3
Reset/udp	2
Scanner Talking	180

セキュリティ イベントの名前	デフォルトで割り当てられるポイント数
Slow Connection Flood	10,800
Src = Des	4,000
SSH Rev Shell	11,700
Stealth_Scan/tcp	5,200
Stealth_Scan/udp	4,800
Suspect Long Flow	4,000
Suspect Quiet Long Flow	4,000
Suspect UDP Activity	9,000
SYNs Received	監視対象の SYN フラグ数に基づく。
Talks to phantoms	1,440
Target Data Hoarding	監視対象の推定ペイロードデータに基づく。
Timeout/tcp	4
Timeout/udp	3
Touched	8,000
Trapped Host	11,700
UDP Received	監視対象の UDP パケット数に基づく。
Worm Propagation	19,200

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 12 月 19 日	最初のバージョン。

著作権情報