Cisco Stealthwatch

バージョン 7.0 内部アラーム ID

Stealthwatch 内部アラーム ID

以前に使用されていたいくつかのアラームは使用されなくなり、このファイルにリストされなくなりました。

1	ホスト ロック違反
5	SYN フラッド
6	UDP フラッド
7	ICMP フラッド
8	パケット フラッド
9	大容量のメール
10	メール リレー
11	スパム送信元
12	メール拒否
13	アクティブなポートを表示
14	新規ホストがアクティブ状態
15	上位のターゲット インデックス
16	上位の合計インデックス
17	最大フローを開始
18	新規フローを開始
19	SYN 受信済み
20	上位のファイル共有インデックス
24	疑わしい UDP アクティビティ
25	MAC アドレス違反

26	ハーフオープン攻撃
28	アクセス
29	低トラフィック
30	高トラフィック
31	ホストのアクティブを確認
32	懸念事項インデックス
33	疑わしい長いフロー
34	トラップされたホスト
35	ワーム アクティビティ
36	ワーム伝播
37	最大フローの提供
38	新規フローの提供
39	ホストに対してビーコンを実行
40	データ損失
41	ボット感染ホスト：C&C 活動の試行（部分一致）
54	ボット感染ホスト：C&C 活動の成功（完全一致）
43	ボット コマンド アンド コントロール サーバ（制御される）
44	低速接続フラッド
45	データ漏洩
46	コマンド & コントロール
47	ポリシー違反
48	疑わしい静かな長いフロー

49	受信されたUDP
50	受信されたICMP
51	偵察
52	データ ホーディング
53	高 DDoS 攻撃ターゲット インデックス
54	高 DDoS ソース インデックス
55	ポート スキャン
56	エクスプロイト
57	異常
58	ブルート フォース ログイン
59	ファントムとの通信
60	過大な SMB ピア
61	SSH リバース シェル
62	疑わしいアプリケーションの検出
63	スキャナ通信
257	Ping
258	ICMP タイムアウト
259	タイムアウト UDP
260	タイムアウト TCP
261	リセット UDP
262	リセット TCP
263	不正なフラグすべて

264	不正なフラグ SYN FYN
265	不正な予約済みのフラグ(Sflow のみ)
266	不正なフラグ RST
267	不正なフラグ ACK
268	不正なフラグ URG
269	不正なフラグ フラグなし
271	ステルス スキャン UDP
272	ステルス スキャン TCP
273	SRC=DES
276	Addr スキャン TCP
277	Ping スキャン
278	特大サイズの Ping パケット
281	フラグ Pkt が短すぎる
282	フラグ Pkt が長すぎる
283	フラグのサイズが異なる
286	Addr スキャン UDP
289	ICMP ネット到達不能
290	ICMP ホスト到達不能
291	ICMP プロトコル到達不能
292	ICMP ポート到達不能
293	ICMP フラグが必要
294	ICMP SRC ルート失敗

295	ICMP 宛先ネットワーク不明
296	ICMP 宛先ホスト不明
297	ICMP 送信元ホスト孤立
298	ICMP 宛先ネット管理者
299	ICMP 宛先ホスト管理者
300	ICMP ネット到達不能 TOS
301	ICMP ホスト到達不能 TOS
302	ICMP 通信管理者
303	ICMP ホスト優先順位
304	ICMP 優先順位の遮断
310	フロー拒否
315	疑わしいデータ ホーディング
316	ターゲット データ ホーディング
317	TOR からの接続試行
318	TOR からの接続成功
319	内部 TOR 終了の検出
513	TOR への接続試行
514	TOR への接続成功
515	内部 TOR エントリの検出
516	Bogon アドレスへの接続成功
517	Bogon アドレスからの接続成功
518	Bogon アドレスへの接続試行

519	Bogon アドレスからの接続試行
4010	フローコレクタのフローデータ損失
4020	インターフェイス使用率がインバウンドを超過
4030	インターフェイス使用率がアウトバウンドを超過
5010	FlowSensor VE 設定エラー
5011	FlowSensorトラフィック損失
5012	FlowSensor RAID 障害
5013	FlowSensor RAID の再構築
5998	FlowSensor 時間のミスマッチ
5999	FlowSensor の管理チャネルダウン
6010	新規 VM
6020	V-Motion
7001	リレーションシップ高トラフィック合計
7002	リレーションシップ高トラフィック
7003	リレーションシップ低トラフィック
7004	リレーションシップ最大フロー
7005	リレーションシップ新規フロー
7006	リレーションシップ ラウンドトリップ時間
7007	リレーションシップ サーバ応答時間
7008	リレーションシップ TCP 再送率
7009	リレーションシップ SYN フラッド
7010	リレーションシップ UDP フラッド

7011	リレーションシップ ICMP フラッド
9021	フローコレクタのデータ削除
9022	フローコレクタのデータベース使用不可
9023	フローコレクタのデータベースのチャネルダウン
9040	フローコレクタログの保存期間削減
9050	フローコレクタエクスポータカウントの超過
9051	フローコレクタ FlowSensor VE カウントの超過
9052	フローコレクタフロー率の超過
9053	フローコレクタインターフェイスカウントの超過
9100	フローコレクタ RAID 障害
9102	フローコレクタ RAID の再構築
9998	フローコレクタパフォーマンスの低下
9999	フローコレクタ停止
60000	フローコレクタタイムミスマッチ
60001	Cisco ISE 管理チャンネルダウン
60002	フローコレクタ管理チャンネルダウン
60003	SMC RAID 障害
60005	SMC RAID の再構築
60007	SMC ディスク容量低下
60008	SMC プライマリの重複
60012	Stealthwatch フローライセンスの超過
60013	ライセンスの破損

60014	ライセンスされていない機能
60015	SLIC チャネル ダウン
60024	ライセンスされていない FPS(1 秒あたりのフロー) 機能 **重要:** このアラームは v6.9 でのみ機能します。v6.10 では、Stealthwatch フロー レート ライセンス利用不可アラーム(アラーム ID # 60025) に置き換えられています。
60025	Stealthwatch フロー レート ライセンス利用不可 **重要:** このアラームは v6.10 以降で機能します。これは、v6.9 のみで機能するライセンスされていない FPS 機能アラーム(アラーム ID # 60024) と置き換えられます。
600016	ID チャネル ダウン
600017	SMC フェールオーバー チャネル ダウン
600018	ライセンス期間 90 日未満
600019	ライセンス期間 60 日未満
600020	ライセンス期間 30 日未満
600021	ライセンス期間 14 日未満
600022	ライセンス期間 3 日未満

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、https://www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。