Cisco Secure Network Analytics

v7.4.2 内部アラーム ID

Cisco Secure Network Analytics 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（v7.2.0 の時点で廃止）
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 サーバー（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
4040	フローコレクタ最長期間エクスポートの超過

5010	FlowSensor Virtual Edition 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
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 サーバー応答時間
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
9050	フローコレクタエクスポータ数の超過
9051	フローコレクタ FlowSensor Virtual Edition の数の超過
9052	フローコレクタフロー率の超過

9053	フローコレクタ インターフェイス数の超過
9054	フローコレクタデータベースの更新廃止
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	フローコレクタ時間不一致
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（v7.2.0 より廃止）
60013	ライセンス破損（v7.2.0 より廃止）
60014	ライセンスのない機能（v7.2.0 より廃止）
60015	SLIC チャネル ダウン
60016	UDPD 通信がダウンしている
60023	UDPD HA がダウンしている
60024	ライセンスされていない FPS（1 秒あたりのフロー）機能（v7.2.0 より廃止） **重要：**このアラームは v6.9 でのみ機能します。v6.10 では、Secure Network Analytics 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（v7.2.0 より廃止） **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。
60030	データストアとの SMC クエリ接続が失われました
60040	データストアと SMC データベースとの間の取り込みおよびメンテナンス接続が失われました
60041	データノードがダウンしています
60042	データノードが回復しています
60043	データストアのタイムスタンプが過度にずれています
60044	データノードのダウンが多すぎるためにデータストアがシャットダウンしました
60045	データストアの回復に失敗しました
60046	データノードの回復がエラーになりました
60047	データノードの回復のロックエラーになりました
60048	データストアの更新が失敗しました
60049	データノードがダウンしました。残りのデータノード数もクリティカルです
60050	ROS コンテナの運用ファイルがデータストアの上限に到達しました
60051	アプライアンス証明書の有効期限が 90 日未満
60052	アプライアンス証明書の有効期限が 60 日未満
60053	アプライアンス証明書の有効期限が 30 日未満
60054	アプライアンス証明書の有効期限が 14 日未満
60055	アプライアンス証明書の有効期限が 3 日未満
60056	アプライアンス証明書の有効期限切れ
60080	分析結果が不完全
60081	Analytics のパフォーマンス低下

60082	Analytics でサポートされていないドメイン
70026	UDPD RAID 障害
70027	UDPD RAID の再構築
70028	UDPD の停止
70029	UDPD の低下
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	ライセンス期間が 90 日未満（v7.2.0 より廃止）
600019	ライセンス期間が 60 日未満（v7.2.0 より廃止）
600020	ライセンス期間が 30 日未満（v7.2.0 より廃止）
600021	ライセンス期間が 14 日未満（v7.2.0 より廃止）
600022	ライセンス期間が 3 日未満（v7.2.0 より廃止）

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 2 月	最初のバージョン

著作権情報