GREYNOISE

Anchor Technologies

モジュール間のデータ差分（Triage / Investigate / Hunt）

No.	フィールド名	Triage	Investigate	Hunt	例	説明
1	actor	YES	YES	YES	unknown	IPアドレスの確認済みの所有者または運用者。
2	bot	YES	YES	YES	false	IPが既知のボット活動に関連しているかどうか。
3	classification	YES	YES	YES	unknown	IPアドレスの分類。分類の値: benign, unknown, malicious, suspicious
4	cve		YES	YES	CVE-2025-12345	IPがスキャンまたは悪用していることが確認されたCVEのリスト。
5	first_seen		YES	YES	2021-11-23	IPがGreyNoiseセンサーネットワークで最初に観測された日付 (YYYY-MM-DD 形式)。
6	ip	YES	YES	YES	1.2.3.4	GreyNoiseセンサーネットワークで観測されたIPアドレス。
7	last_seen	YES	YES	YES	2021-12-31	IPがGreyNoiseセンサーネットワークで最後に観測された日付 (YYYY-MM-DD 形式)。
8	metadata.asn	YES	YES	YES	AS37963	IPアドレスに関連付けられたASN。
9	metadata.category	YES	YES	YES	hosting	IPアドレスのカテゴリ。例: hosting, ISP
10	metadata.city	YES	YES	YES	Miami	IPアドレスが登録されている、または運用されている都市。
11	metadata.destination_countries		YES	YES	Belarus	IPのスキャントラフィックを観測したセンサーが存在する国のリスト。
12	metadata.destination_country_codes		YES	YES	BY	IPのスキャントラフィックを観測したセンサーが存在する国のコードリスト。
13	metadata.mobile	YES	YES	YES	true	IP アドレスが既知のセルラーネットワークに属しているかどうか。
14	metadata.organization	YES	YES	YES	FranTech Solutions	IPアドレスに関連付けられた組織。
15	metadata.os			YES	Windows XP	IPアドレスに関連付けられたオペレーティングシステム。
16	metadata.rdns	YES	YES	YES	miamitor4.us	IPアドレスのrDNS (逆引きDNS) の値。
17	metadata.region	YES	YES	YES	Florida	IPアドレスが登録または運用されている地域。
18	metadata.sensor_count		YES	YES	20	イベントが観測されたセンサーの数。
19	metadata.sensor_hits		YES	YES	210	観測されたスキャンイベントの数。
20	metadata.source_country	YES	YES	YES	United States	IPアドレスが登録または運用されている国。
21	metadata.source_country_code	YES	YES	YES	US	IPアドレスのISO 3166-1 alpha-2形式の国コード。
22	metadata.tor	YES	YES	YES	true	IPが既知のTor出口ノードであるかどうか。
23	raw_data.hassh.fingerprint			YES	a7a87fbe86774c2e40cc4a7ea2ab1b3c	観測されたSSHアクティビティのフィンガープリント値。
24	raw_data.hassh.port			YES	22	観測されたSSHアクティビティに関連するポート。
25	raw_data.ja3.fingerprint			YES	19e29534fd49dd27d09234e639c4057e	観測されたJA3アクティビティのフィンガープリント値。
26	raw_data.ja3.port			YES	8443	観測されたTLSアクティビティに関連するポート。
27	raw_data.scan.port		YES	YES	22	観測されたスキャン活動のポートを記録。
28	raw_data.scan.protocol		YES	YES	TCP	観測されたスキャン活動のプロトコルを記録。
29	raw_data.web.paths			YES	/favicon.ico	観測されたスキャン活動がアクセスしたウェブパス。
30	raw_data.web.useragents			YES	Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)	観測されたスキャン活動が使用したユーザーエージェント。
31	seen（またはnoise）	YES	YES	YES	true	IPがGreyNoiseセンサーネットワークをスキャンしていたかどうか。
32	spoofable	YES	YES	YES	false	IPがGreyNoiseセンサーネットワークと3ウェイハンドシェイクを完了したかどうか。Falseの場合、偽装されたトラフィック（スプーフィング）の可能性が高い。
33	tags	YES	YES	YES	"Carries HTTP Referer", "Cobalt Strike SSH Client", "Follows HTTP Redirects"	IPアドレスの観測されたスキャン動作を説明するタグ。
34	vpn	YES	YES	YES	false	IPが既知のVPNサービスに関連付けられているかどうか。
35	vpn_service	YES	YES	YES	PIA_VPN	IPに関連付けられたVPNサービスの名前 (該当する場合)。