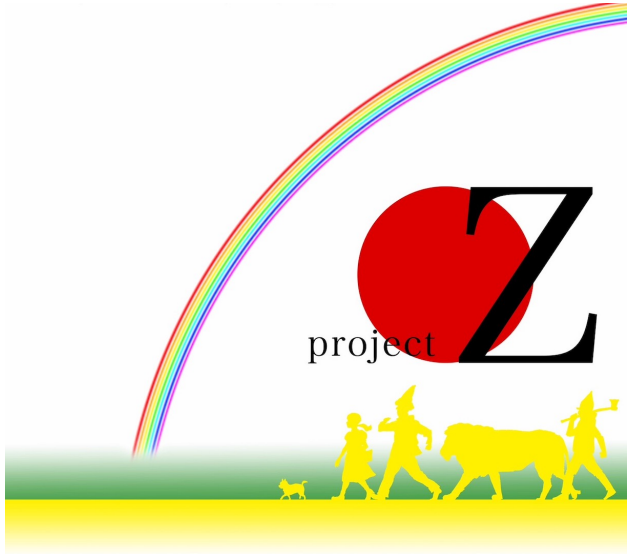
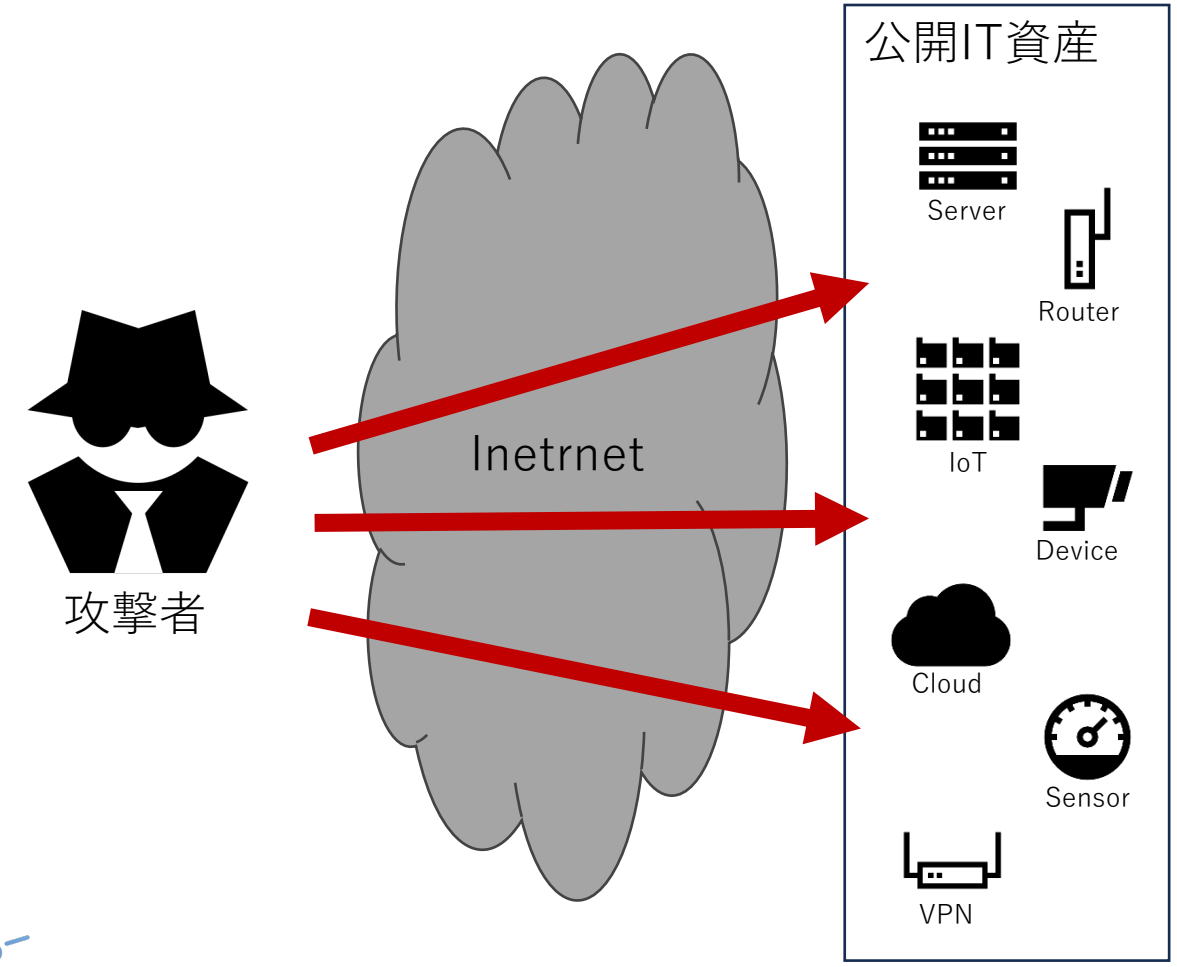
censys & kr:ns

ASM (Attack Surface Management)



RainForest



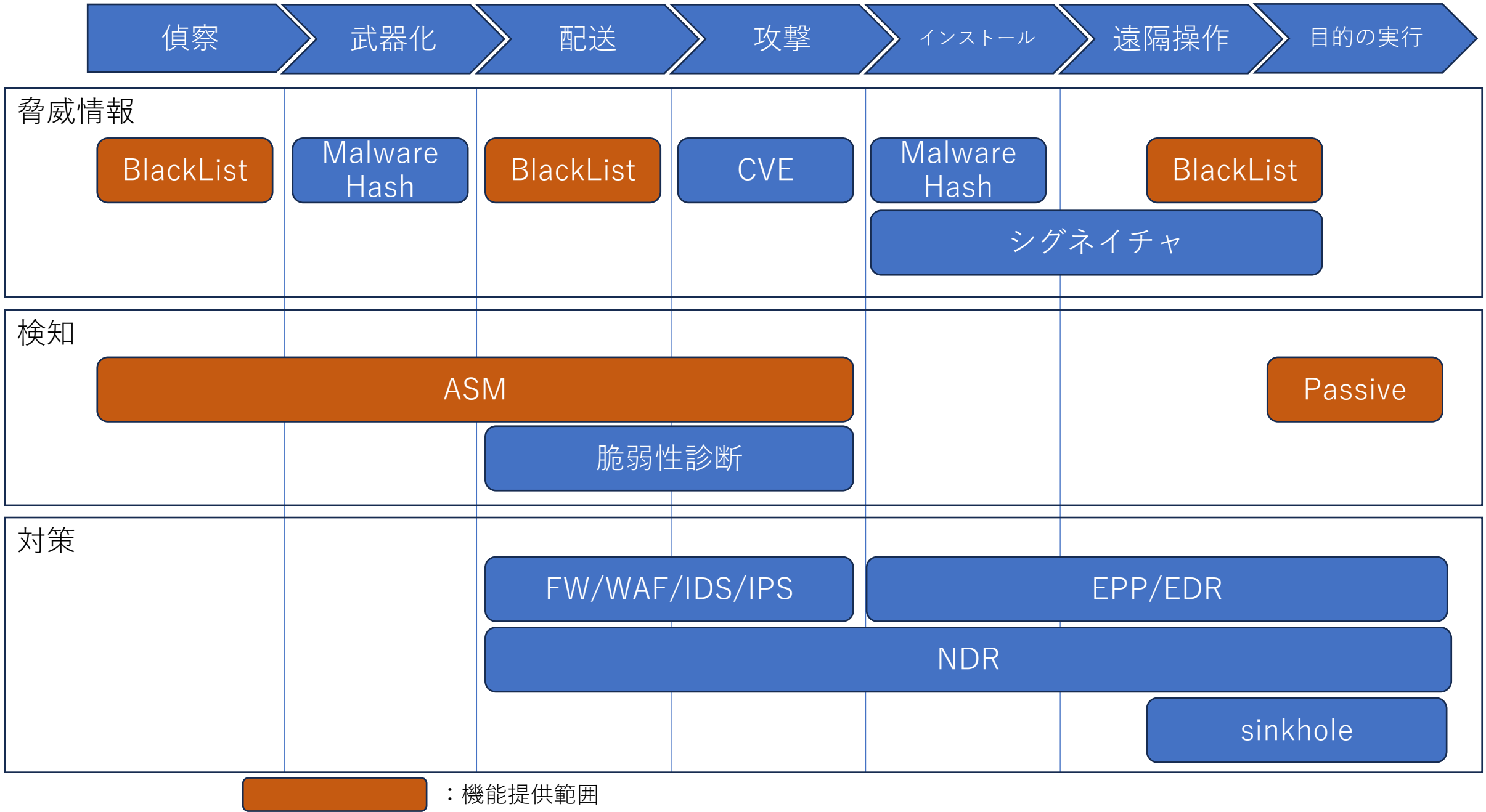
IT 資産を守るためインターネットに向けて弱点をさらしているIT資産を特定・把握することが重要

(1)攻撃面の発見	企業で保有または管理するIPアドレス・ホスト名の発見
(2)攻撃面の情報収集	攻撃面の情報収集 例：OS、ソフトウェア、バージョン情報、オープンなポート番号など
(3)攻撃面のリスク評価	（2）で収集した情報をもとにしたリスクの評価
リスクへの対応	脆弱性管理と同様の対応 例：パッチ適用（リスクの低減）や対策見送り（リスクの受容）など

参照:経済産業省 商務情報政策局 サイバーセキュリティ課
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

サイバー攻撃の初期段階では、公開されている情報やインターネットからアクセス可能な IT 資産から得られる情報を用いて攻撃対象を選定したり、攻撃手法を確立したりする「偵察」が行われるとされています。

サイバーキルチェーンとのマッピング



Internet Assetにおけるセキュリティリスク

censys のベネフィット

✓ 即時性の向上

- **デイリーによる全てのInternet Assetに対するスキャン**
  - ✓ シャドーITの即時検査
  - ✓ インシデントの可能性の即時検査

✓ より深くより詳細に

- **3,500以上のPortを対象に、オープンなポート等を明示**
  - ✓ IoT機器の管理画面などの公開の即時検査

✓ 履歴の管理

- **全ポートの過去の履歴も全て記録**

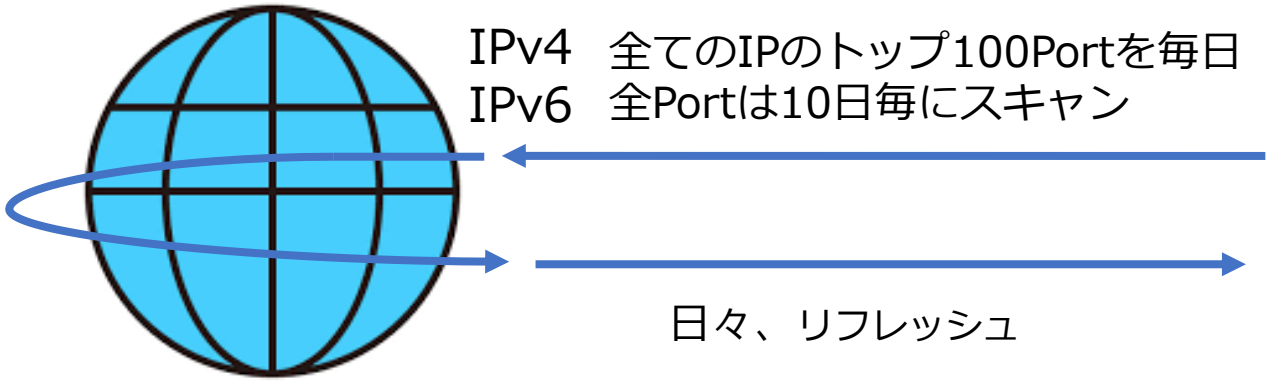
サプライチェーン全体においてのInternet Assetへの対応も可能

✓ 即時検査を行うことで現在の状態を把握し問題の認識ができ、より安全な運用を行うこと可能となります。

censys Search 概要

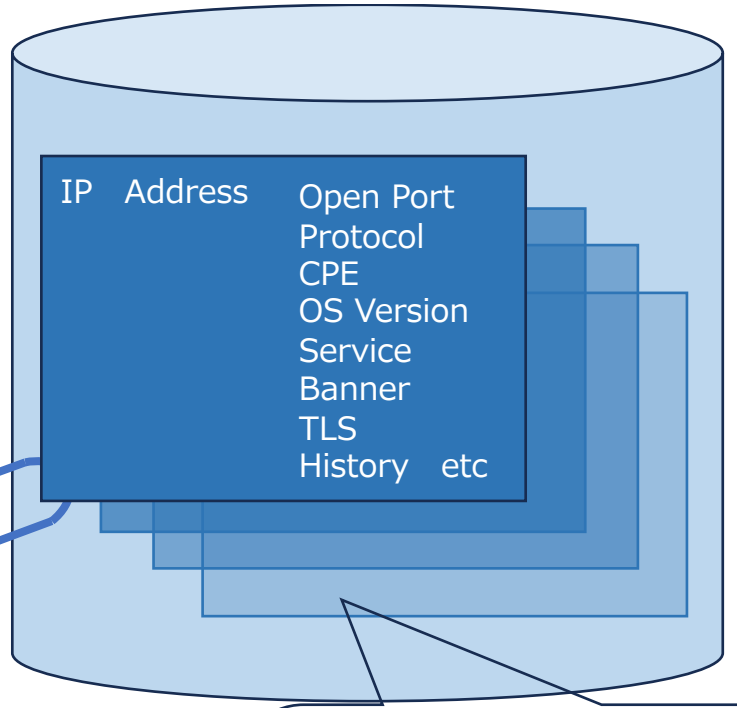
censys

スキャン結果のBig Data



IPv4 全てのIPのトップ100Portを毎日
IPv6 全Portは10日毎にスキャン

日々、リフレッシュ



ユーザー

IPアドレス
IPレンジ

クエリー

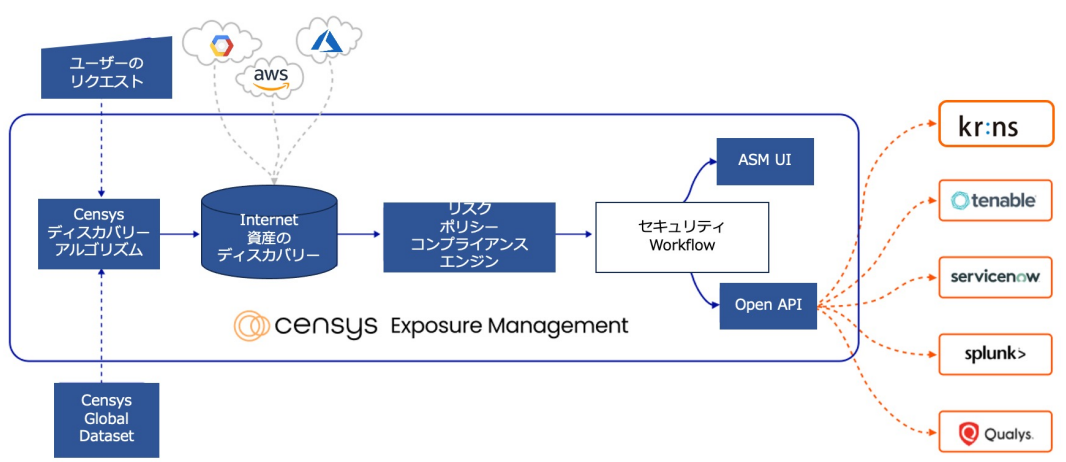
クエリー数/月で課金

2億1100万のIPv４のホスト
6700万のIPv6のホスト
5億12000万の仮想のホスト
AWS、Azure、GCPに対応
3500以上のポート
オープンなポートとプロトコルを見える化
機器、OS、サービスの特定

ASM

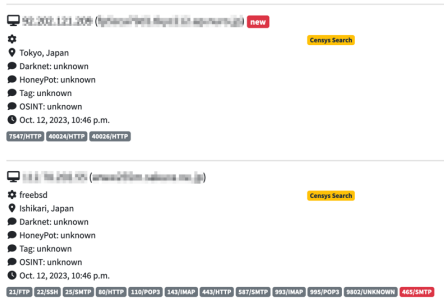
Censys Exposure Management (Scanner)

- インターネットに公開された資産の管理＝Exposure Management
- Censys Attack Surface Managementは、高度な脅威とそれにさらされている資産を特定し、修復するための必要な重要な情報を提供します。



RainForest ASM (OSS)

- Censysの検索方法の提供
- 日々の差分
- サービスの検索
- CPEから取得したCVE情報

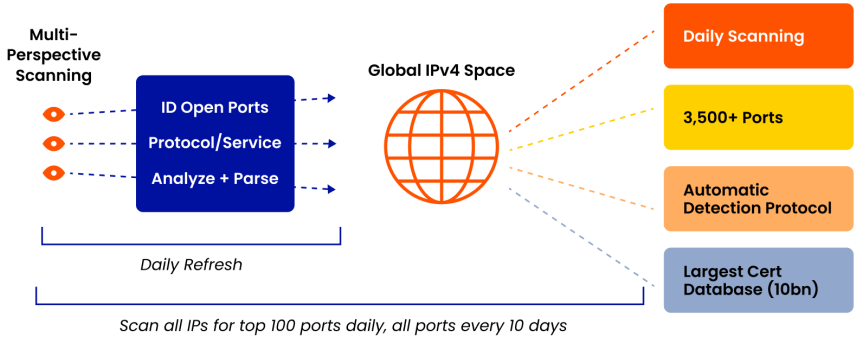


kr:ns(Passsive)

- Darknet
- honeypot
- DRDoS

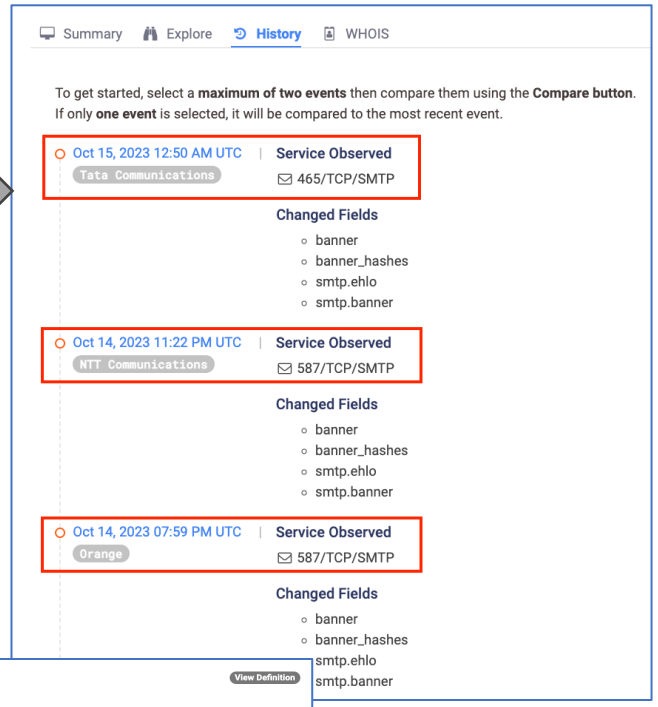
Censys Search(Scanner)

- IPv4,IPv6　両方を対応
- 約3,500のPortをActiveScan
- クラウドリソースへの対応
- Open Portの見える化
- 機器、OS、サービスの特定

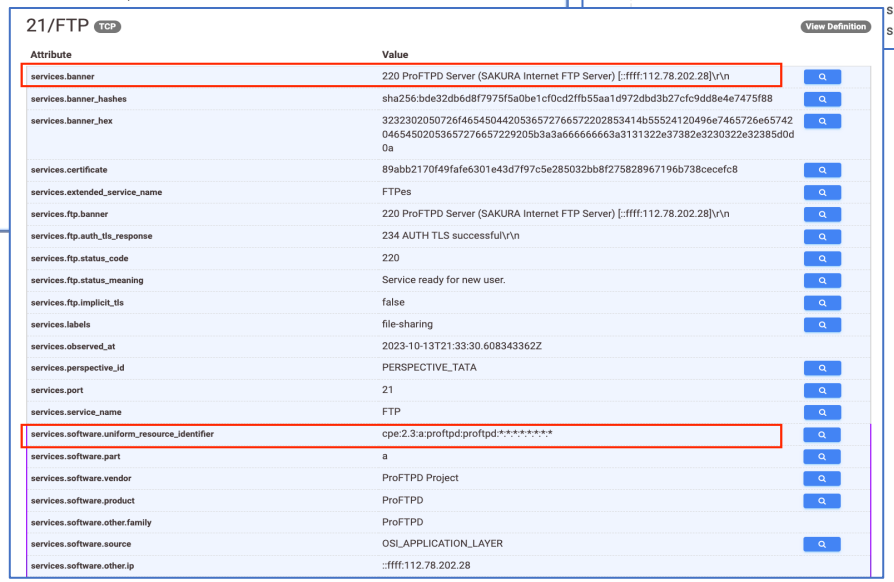


Censys Search

検索結果



履歴データ



詳細データ

- Censys search APIを利用することでこのようなデータをJSON形式で取得が可能
- 取得されるデータはプログラムやSIEMなどへの取り込みが可能

https://search.censys.io/api

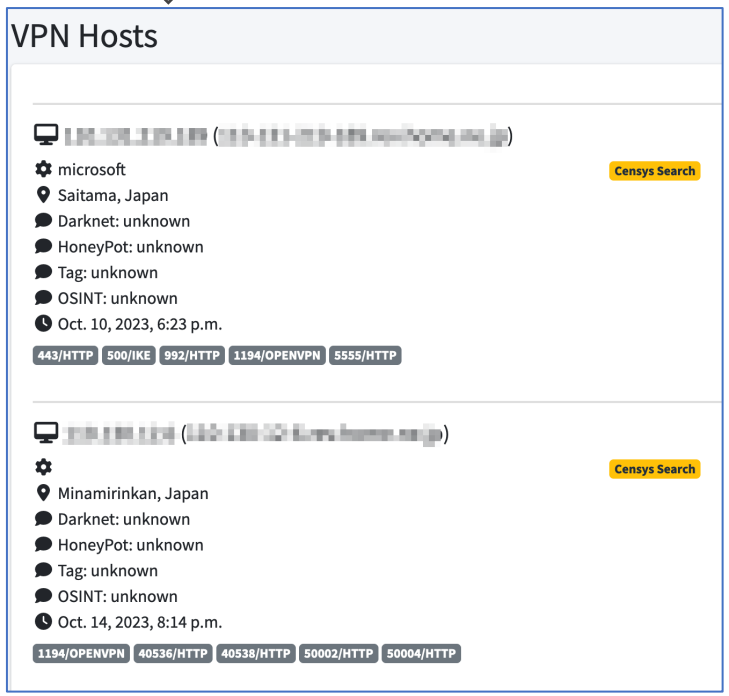
RainForest ASM

Censys Tools

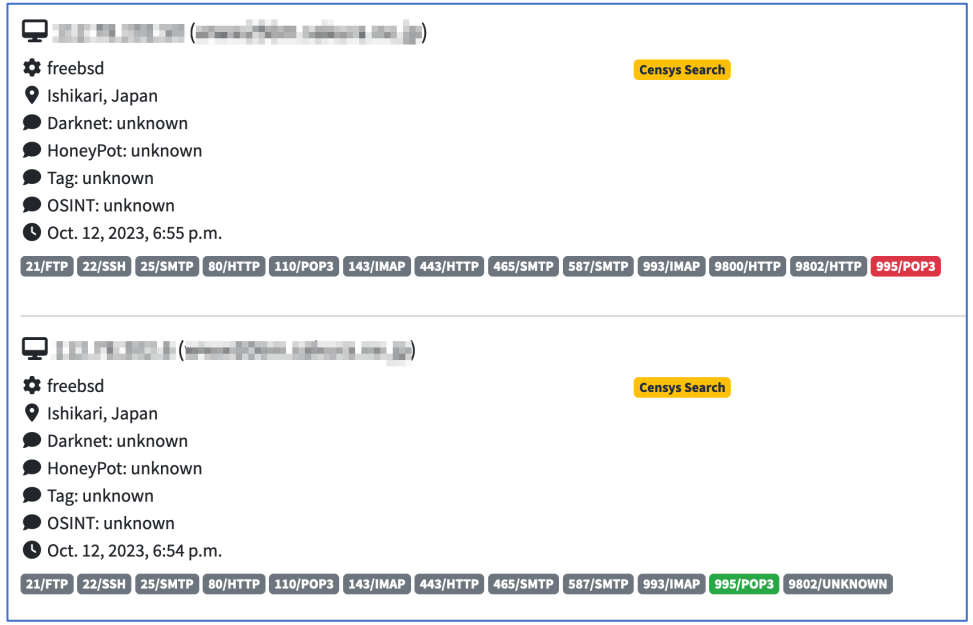
issue_idが各データに付与される。このissue_idを確認することでいつクエリーが実行されたかがわかる

- Search APIを利用して対象のIPアドレス情報の収集 link
- Search APIをの差分を取得 link
- Search APIを利用してLabel検索 link
- View APIを利用して対象のIPアドレス情報の収集 link
- Censys GPT(β)を利用した検索 link

CLI Tool例



LabelでVPNサービスを検索した結果

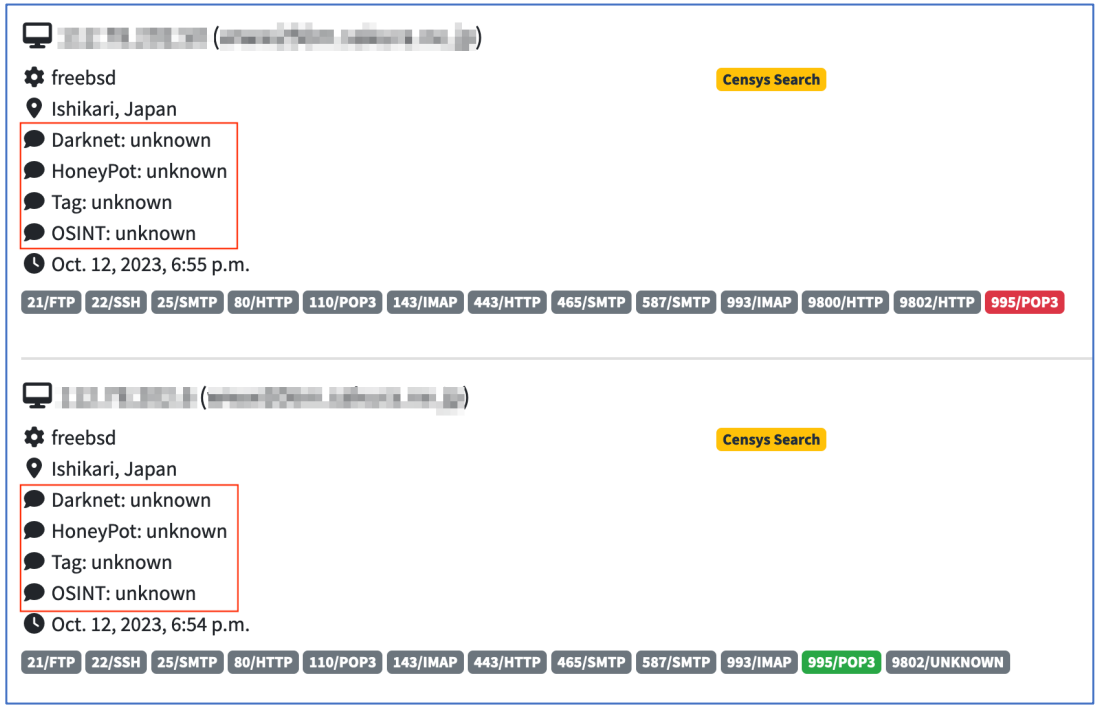


日毎の差分結果

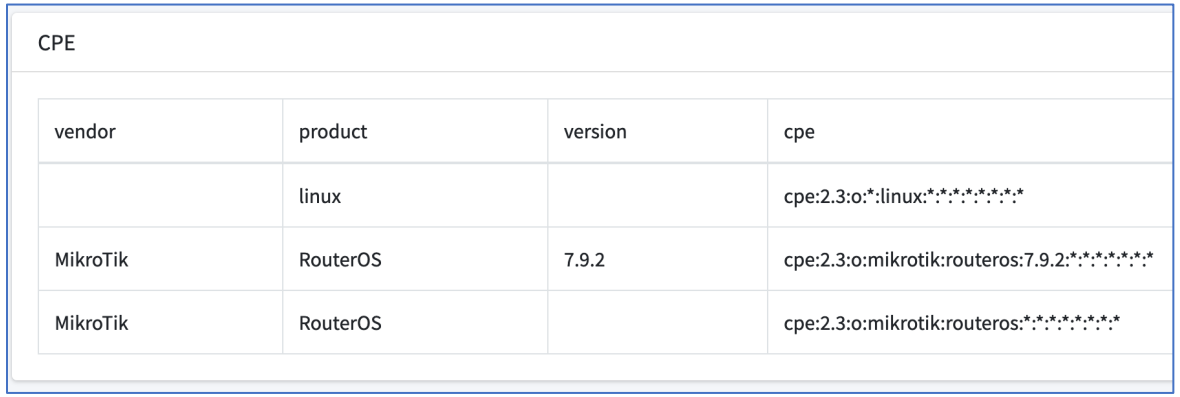
- censys APIを利用するpythonスクリプトをOSSで提供します
- スクリプトでの検索結果はMongoDBに蓄積され、蓄積されたデータから下記のデータを閲覧するweb UIも提供します
  - 日々の差分
    - ✓ 赤：openになったサービス
    - ✓ 緑：closeになったサービス
  - Censysが付与するラベルで検索した結果一覧

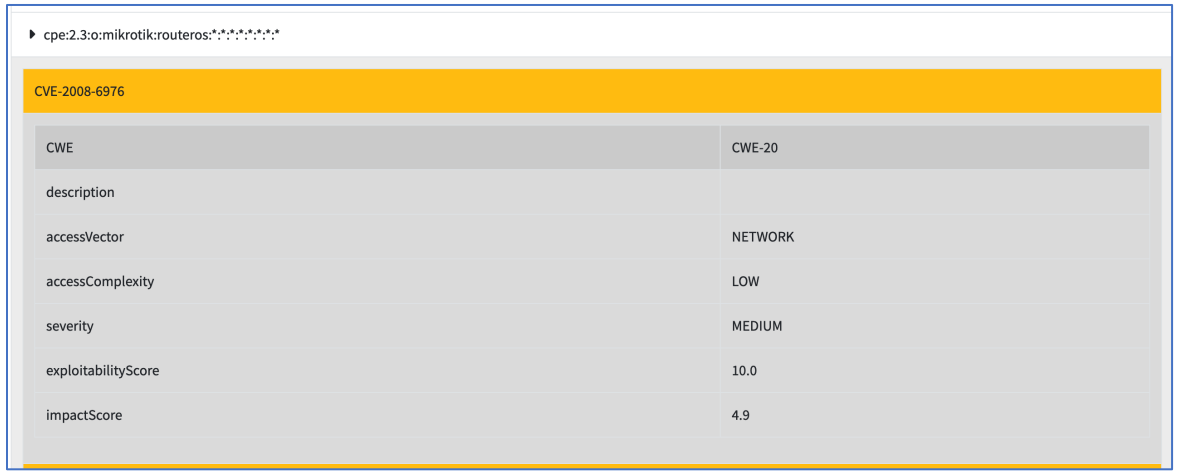
https://bitbucket.org/rainforest-tokyo/censys/src/master/

RainForest ASM



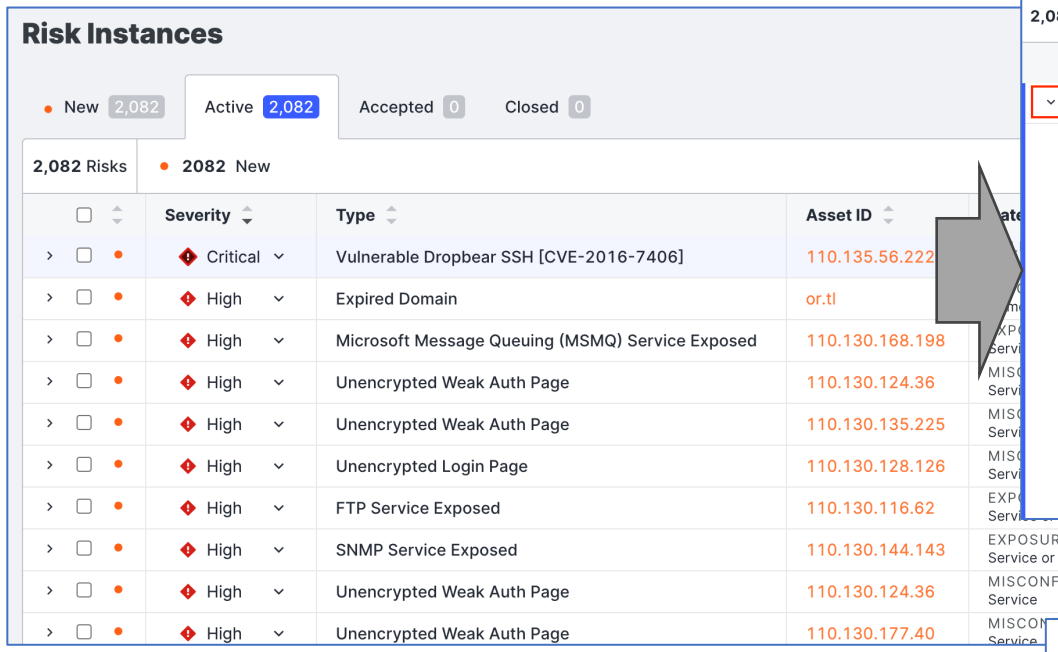
- kr:nsのライセンス購入時には赤枠の部分に下記の情報が付与されます
  - Darknet
  - honeypot
  - DRDoS
  - OSINT



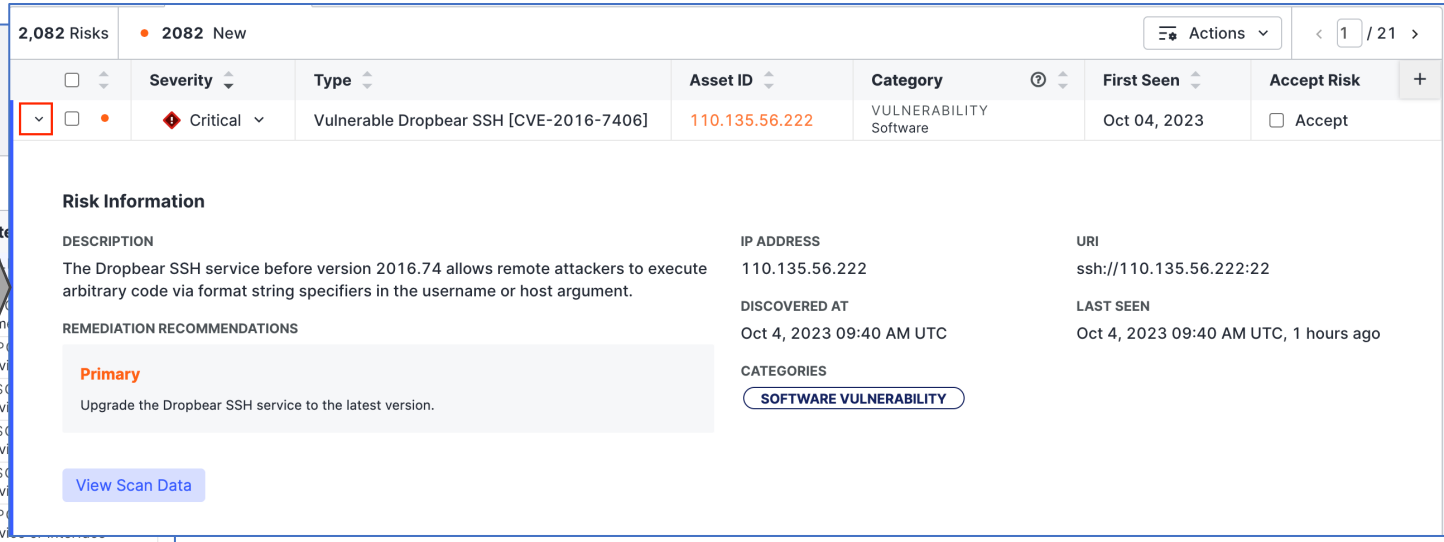


- 詳細情報収集機能を有効時にはCPE情報やそのCPEに関連するCVE情報などが表示されます。

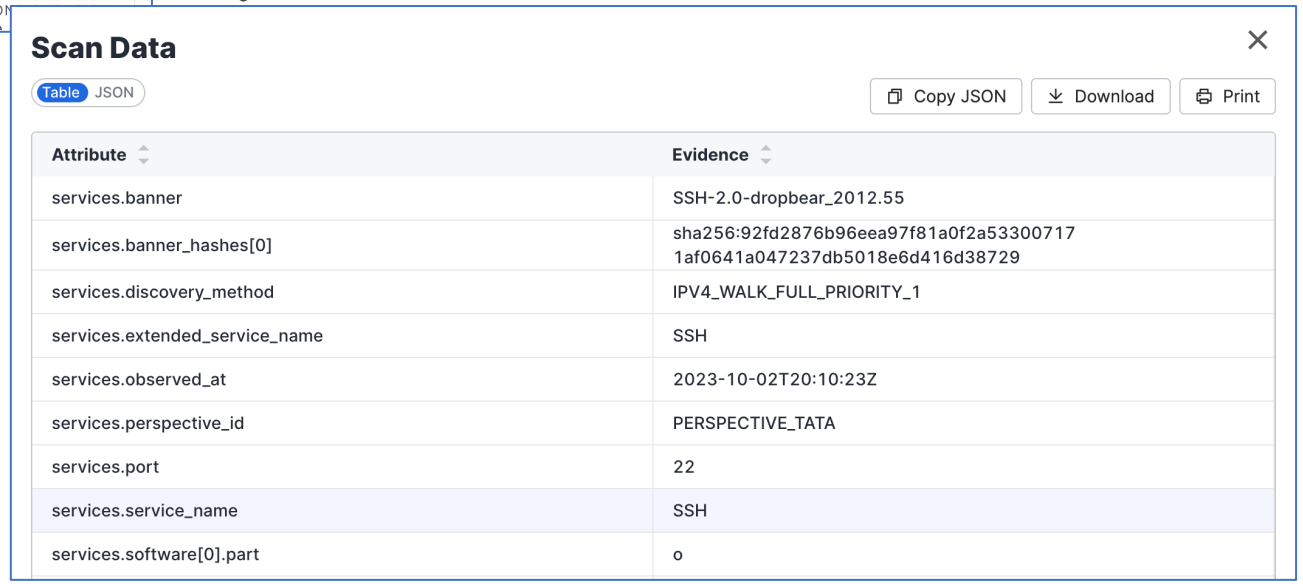
Censys Exposure Management



Risk一覧



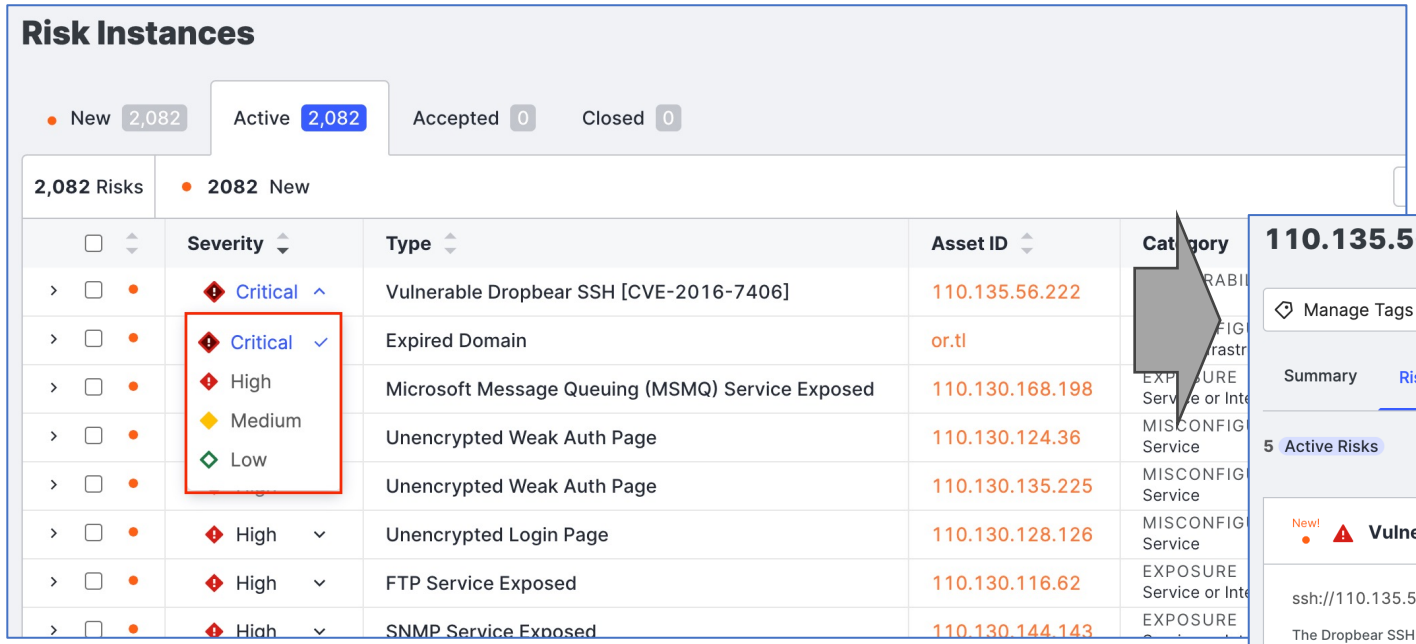
Risk詳細



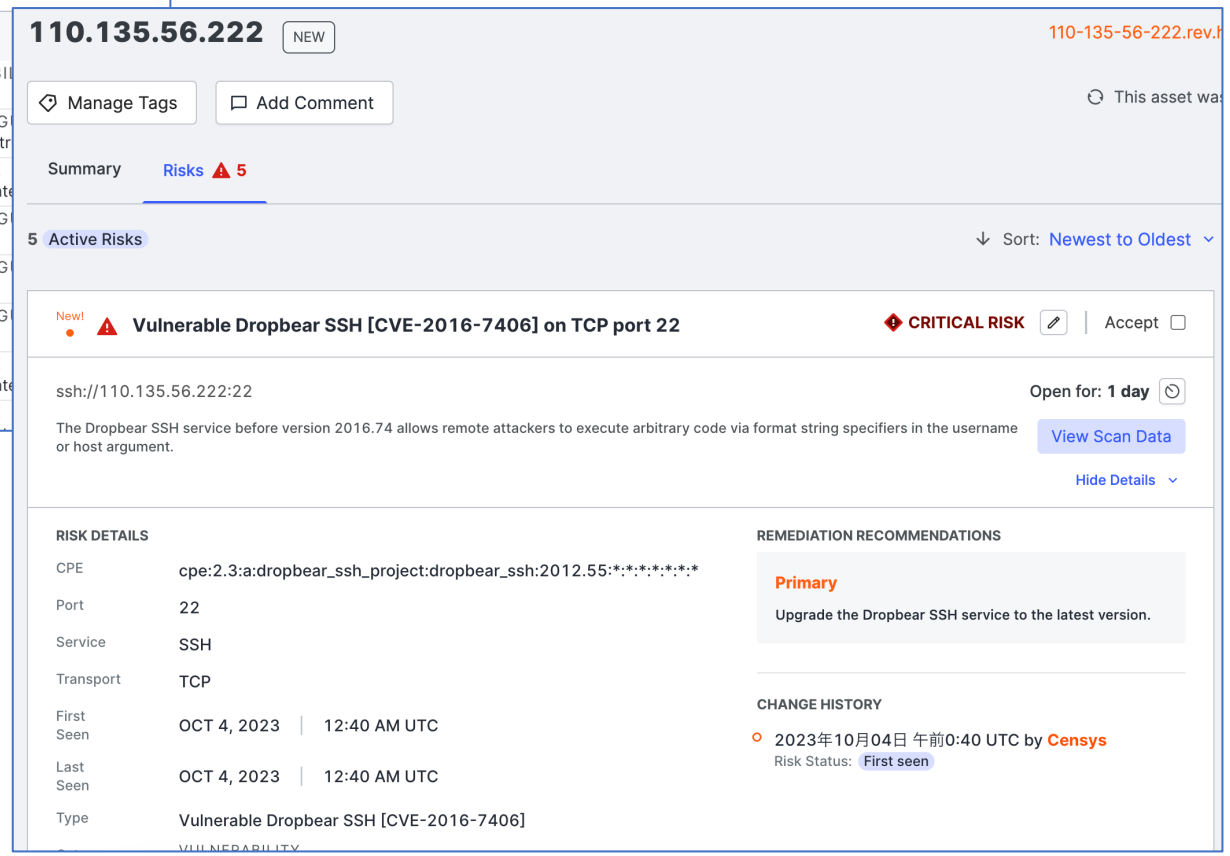
Scan詳細

- 検知されたRisk一覧からリスクの詳細情報とscan詳細を参照することができる
- Scan詳細データにはバナー情報などが含めれている

Censys Exposure Management



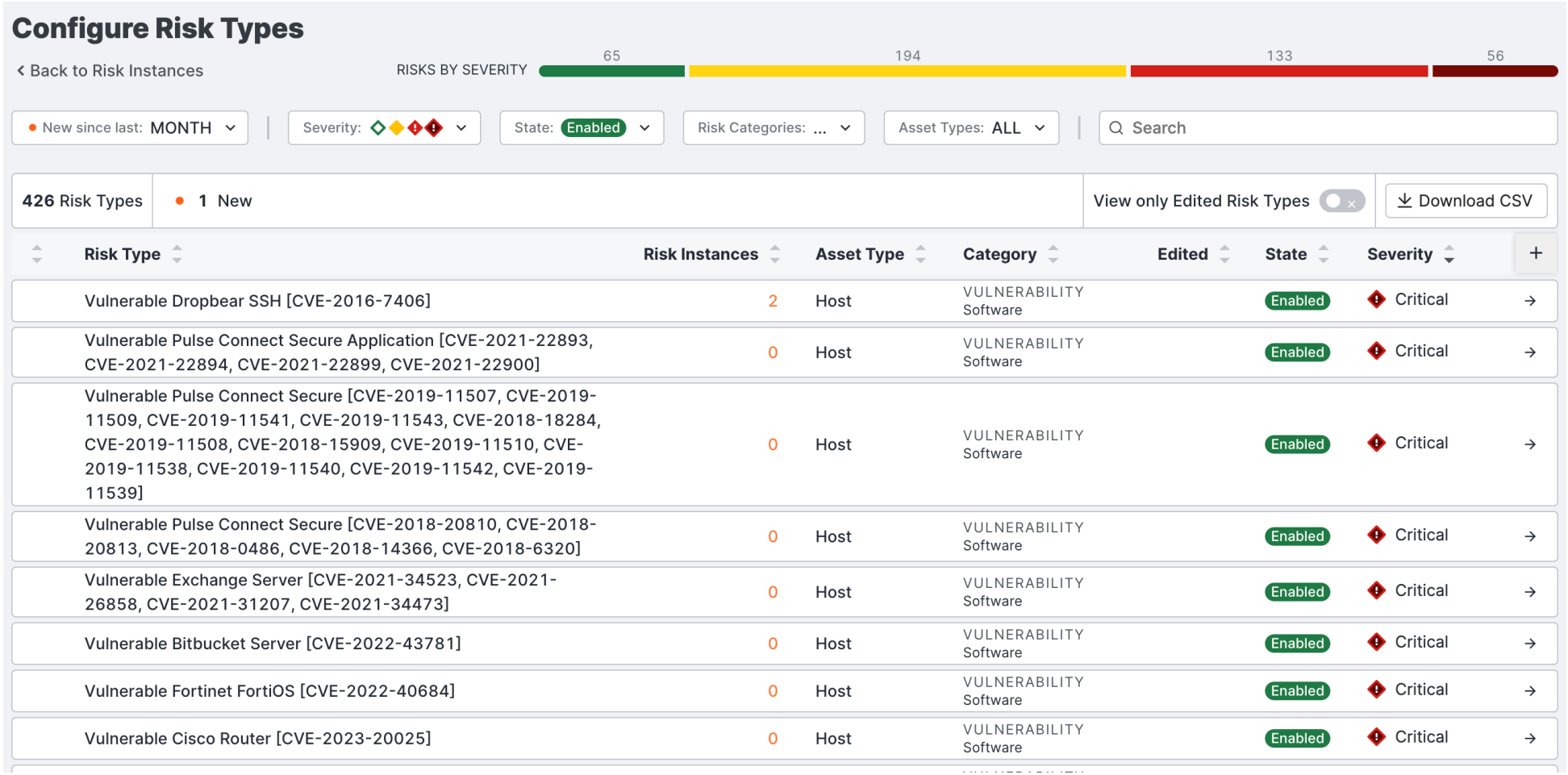
Riskの設定変更



IPアドレスに対するリスク詳細

- リスクに対するSeverity(リスクレベル)を利用者側で設定が可能
- リスクが見つかったIPアドレスの詳細を閲覧することができる

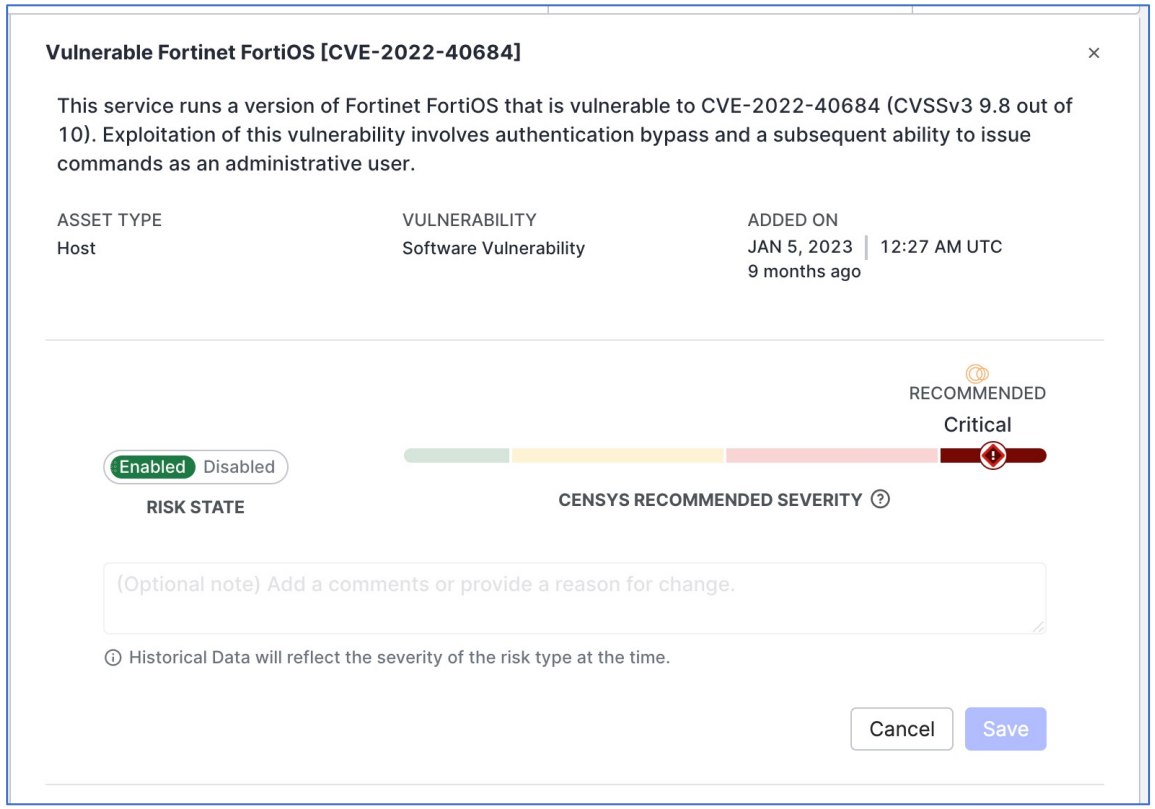
Censys Exposure Management



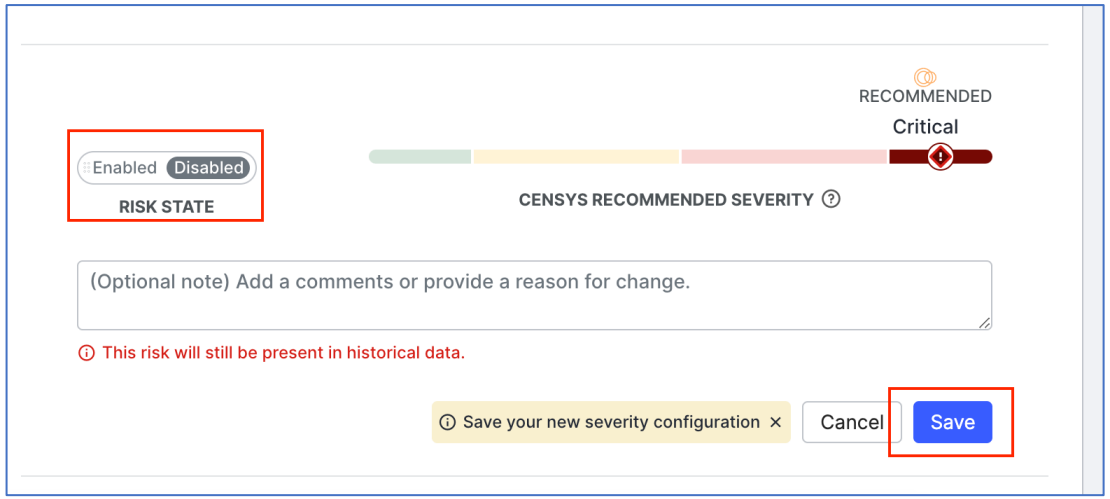
Risk Type(アラート対象)一覧

- リスクタイプ(アラート対象)の一覧が表示される
- 各アラートの有効無効/リスクレベルを利用者側で設定が可能

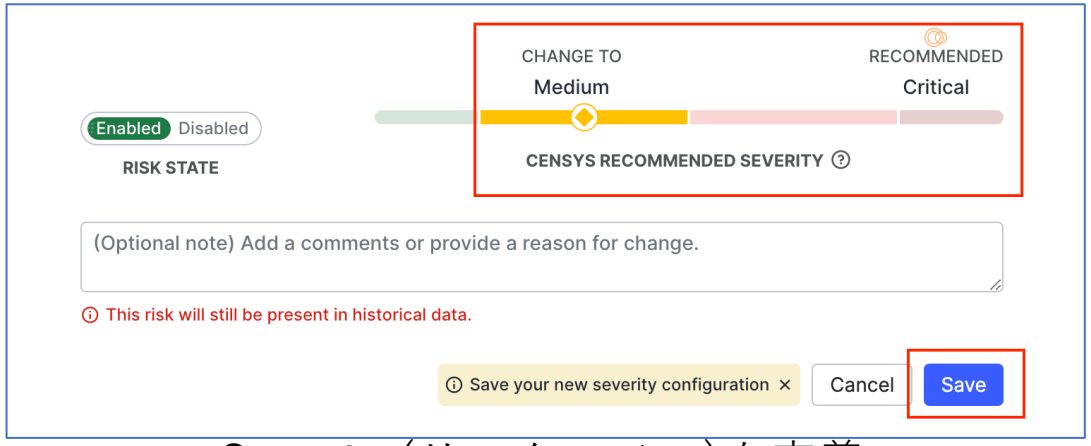
Censys Exposure Management



Risk Type(アラート対象)詳細



有効・無効を定義



Severity(リスクレベル)を定義

- 対象のリスクタイプの有効・無効を定義することができる
- 対象のリスクタイプのSeverity(リスクレベル)を定義することができる

他社との違い

censys

手　法	データ	ユーザーへの意義	結果
Data Oriented	Global Internet Scanning	● 精度（少ない誤検知） ● 鮮度（日々のアップデート） ● 情報（オーナー、属性） ● 攻撃対象のコントロール ● 登録なしに、攻撃対象領域のあらゆるデータポイント閲覧	● 運用効率化 ● TCO削減 ● リスク低減

他のASM

手　法	データ	ユーザーへの意義	結果
Vulnerability Oriented	脆弱性診断 Pen Test	● 低い精度（無駄な検知） ● 古くて不完全なデータ（週次、月次のアップデート） ● 情報不足（オーナー、属性） ● ベンダーに依存	● 高い運用コスト ● 低い信頼性 ● 盲点

censys KEY USE CASES

継続的な攻撃対象のディスカバリー

外部の攻撃対象が常に最新であることを確認します。すべてがどこにあり、攻撃者の視点からどのように見えるかを把握します。外部攻撃サーフェスの発見とインベントリは、あらゆるセキュリティ・プログラムの基礎となる要素です。

クラウド上に公開されたリソースの管理

３大クラウドプロバイダーにネイティブに統合された唯一のASMプラットフォームにより、攻撃対象から　シャドウクラウドを排除します。すべてのプロバイダーにわたるクラウドインベントリを毎時更新で簡単に管理し、許可されたクラウドアカウント以外に何が存在するかを把握できます。

公開されたリソースのリスクを管理

深いコンテキストと、影響度、悪用可能性、可能性に基づく重大度評価を提供する設定可能なリスクエンジンを使用して、すべての公開されたリソースの優先順位を決定します。攻撃者の視点から組織の公開されたリソースを把握するとで、セキュリティ・プログラムが最も緊急なニーズに最初に対処できるようになります。

小会社化や買収、合併

最近になって継承されたものであれ、事業部門やチームが独立して機能するようになったものであれ、バラバラの環境は、それらを保護するセキュリティチームに負担をかけます。ビジネスのあらゆる部分の外部アタックサーフェスを一元管理したり、ワークスペースを個別に作成して個別に処理したりできます。当社の自動オンボーディング機能は、20分以内に新しいアタックサーフェスを構築し、新しい企業を買収する際にチームが優位に立てるよう支援します。

Users

Cybersecurity and Infrastructure Security Agency
セキュリティ・インフラストラクチャセキュリティ庁(CISA)

Department of Homeland Security
国土安全保障省

Defense Intelligence Agency
国防情報局

Department of Defense
米国国防総省

NATO

スイス軍

Kr:ns BlackList Malware IP

```
{'ip': '*.*.186.222', 'osint': ['cinsscore']}
{'ip': '*.*.98.103', 'osint': []}
{'ip': '*.*.7.125', 'osint': ['cinsscore']}
{'ip': '*.*.103.93', 'osint': []}
{'ip': '*.*.193.156', 'osint': ['cinsscore']}
{'ip': '*.*.11.5', 'osint': ['cinsscore']}
{'ip': '*.*.56.138', 'osint': []}
{'ip': '*.*.49.22', 'osint': []}
{'ip': '*.*.74.73', 'osint': ['cinsscore']}
{'ip': '*.*.249.67', 'osint': []}
{'ip': '*.*.74.173', 'osint': ['cinsscore']}
{'ip': '*.*.145.158', 'osint': ['blocklist', 'cinsscore']}
```

- マルウエアの特徴を持ったパケットを送信してきたIP情報にOSINTでの有無を付与し配信されます

参照しているOSINT

- abuse.feodotracker
- abuse.sslbl
- abuse.urlhouse
- alienvault
- blocklist
- cinsscore
- cleantalk
- emergingthreats
- greensnow
- multiproxy
- talosintel

Kr:ns BlackList Black IP


```
{'ip': '*.*.94.122', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.110.77', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.47.133', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
{'ip': '*.*.27.68', 'behavior': ['Exec Command'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.208.251', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.107.214', 'behavior': ['Exec Command'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.222.209', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.107.240', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.59.157', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.186.222', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
{'ip': '*.*.7.125', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
{'ip': '*.*.49.22', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.254.73', 'behavior': ['Exec Command'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.74.173', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
{'ip': '*.*.213.100', 'behavior': ['Exec Command'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.91.249', 'behavior': ['Exec Command'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.163.25', 'behavior': ['Malware Download'], 'dl_ip': {}, 'osint': ['urlhouse', 'cinsscore']}
{'ip': '*.*.73.92', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.218.140', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['blocklist']}
{'ip': '*.*.133.202', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.50.123', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.57.42', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': []}
{'ip': '*.*.48.130', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
{'ip': '*.*.54.198', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore', 'blocklist', 'greensnow']}
{'ip': '*.*.15.87', 'behavior': ['Malware'], 'dl_ip': {}, 'osint': ['cinsscore']}
```


- Black IPとして認識された情報にOSINTでの有無を付与し配信されます
- 1日約2000 IP

Black判定の根拠はbehaviorを確認することで把握可能

- Malware:マルウエアの特徴のパケット送信
- Malware Download：マルウエアダウンロードサイト
- Exec Command：ハニーポットに侵入

Kr:ns BlackList Risk

```
{'ip': '*.*.18.59', 'level': 6}
{'ip': '*.*.245.87', 'level': 1}
{'ip': '*.*.190.133', 'level': 2}
{'ip': '*.*.238.113', 'level': 1}
{'ip': '*.*.245.177', 'level': 2}
{'ip': '*.*.251.159', 'level': 2}
{'ip': '*.*.238.213', 'level': 2}
{'ip': '*.*.18.106', 'level': 5}
{'ip': '*.*.81.12', 'level': 1}
{'ip': '*.*.207.251', 'level': 1}
```

- 観測網で通信があったIPアドレスにリスクレベルを付与し配信されます
- 1日40000 IP程度

リスクレベルは下記を考慮して決定しています

- Darknetへの通信
- マルウエアの特徴のパケット送信
- マルウエアダウンロードサイト
- Exec Command：ハニーポットに侵入
- OSINTに登録されている

Kr:ns BlackList Malware Access Port

port	name	malware	darknet	mirai	exploit	total
23	"telnet"	true	true	true	true	100
2323	""	true	true	true	true	98.935
37215	""	true	true	true	true	98.566
52869	""	true	true	true	true	97.338
8080	"http-alt"	true	true	true	true	97.013
80	"http"	true	true	true	true	96.436
5555	""	true	true	true	true	95.297
443	"https"	true	true	true	true	95.061
8081	"tproxy"	true	true	true	true	93.478
81	""	true	true	true	true	92.473
8443	""	true	true	true	true	91.127
22	"ssh"	true	true	true	false	89.825
7547	""	true	true	true	true	89.515
55555	""	true	true	true	true	89.352

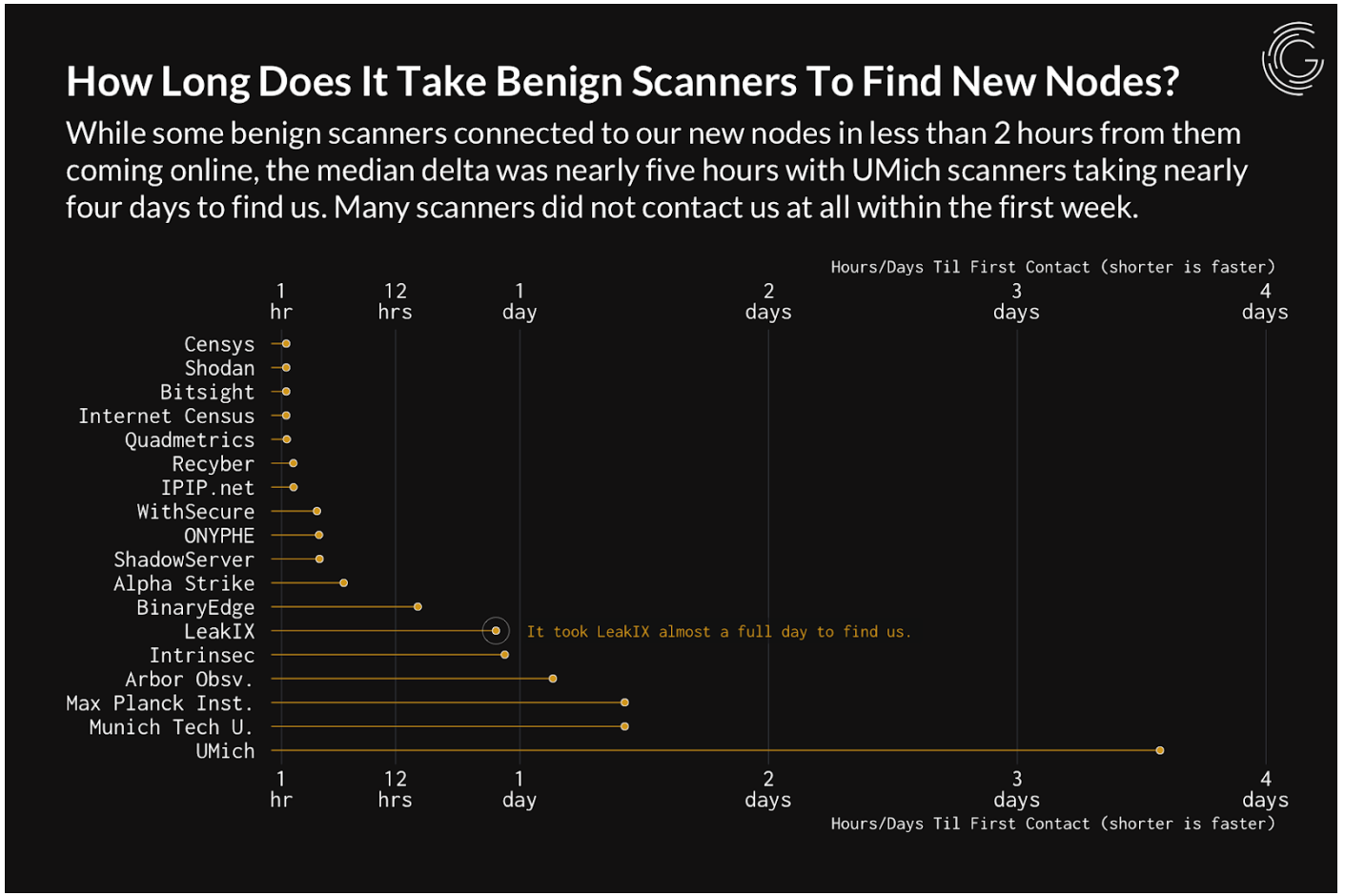
- 動的解析の結果と観測環境のLive情報からPortのリスクを評価し配信されます

Kr:ns BlackList Malware info

- 日々収集されるMalwareに関連する下記の情報が配信されます
  - Malware ファイル情報
  - DNS解決
  - マルウエアdownload site
  - scan対象port
  - 待ち受けport
  - 通信先情報

Censysの特徴

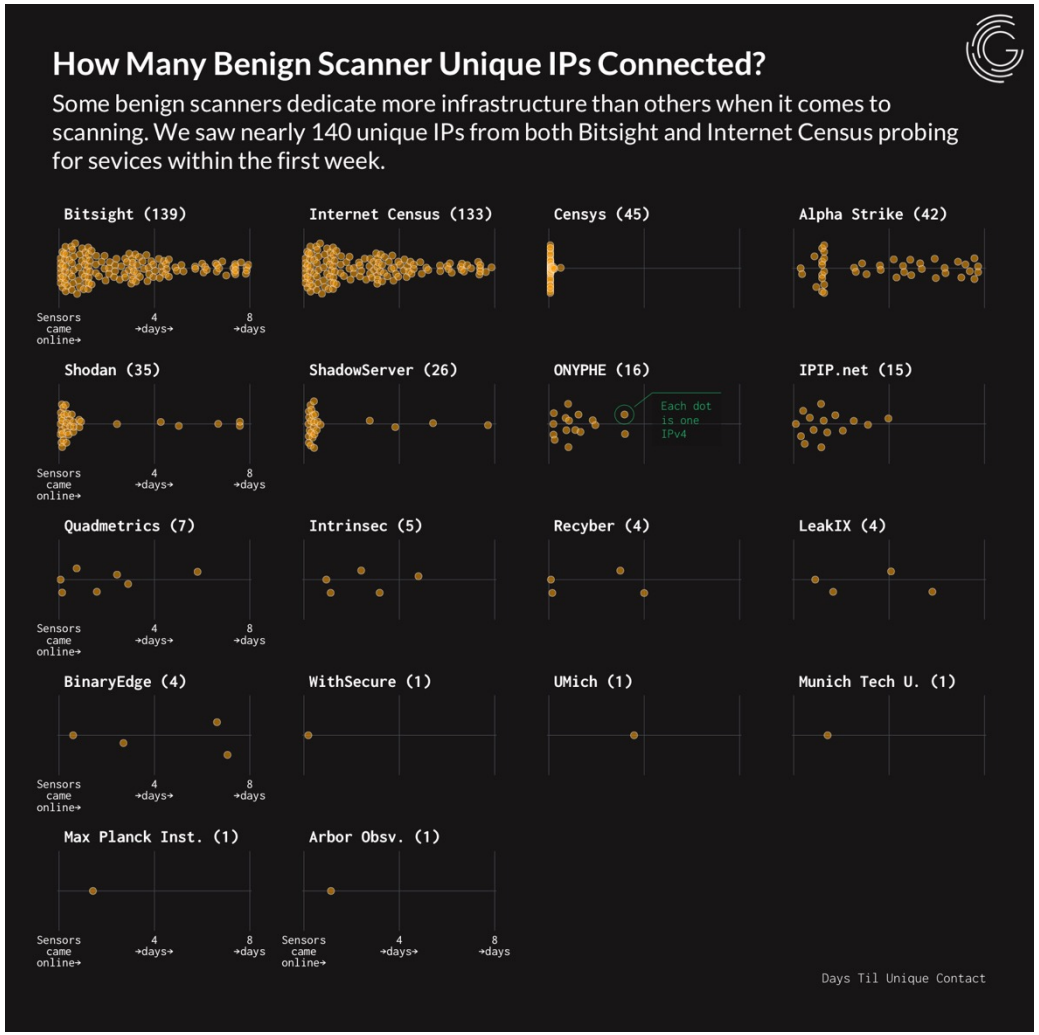
Censysの特徴– 1



- **GreyNoise社**での観測データから新しく立ち上げたサーバに最も短い時間で調査が行われる事がわかります。
  - IPの登録を行わずにcensys searchにクエリーを投げることでシャドーITなどをいち早く見つけ出すことができることがわかります。

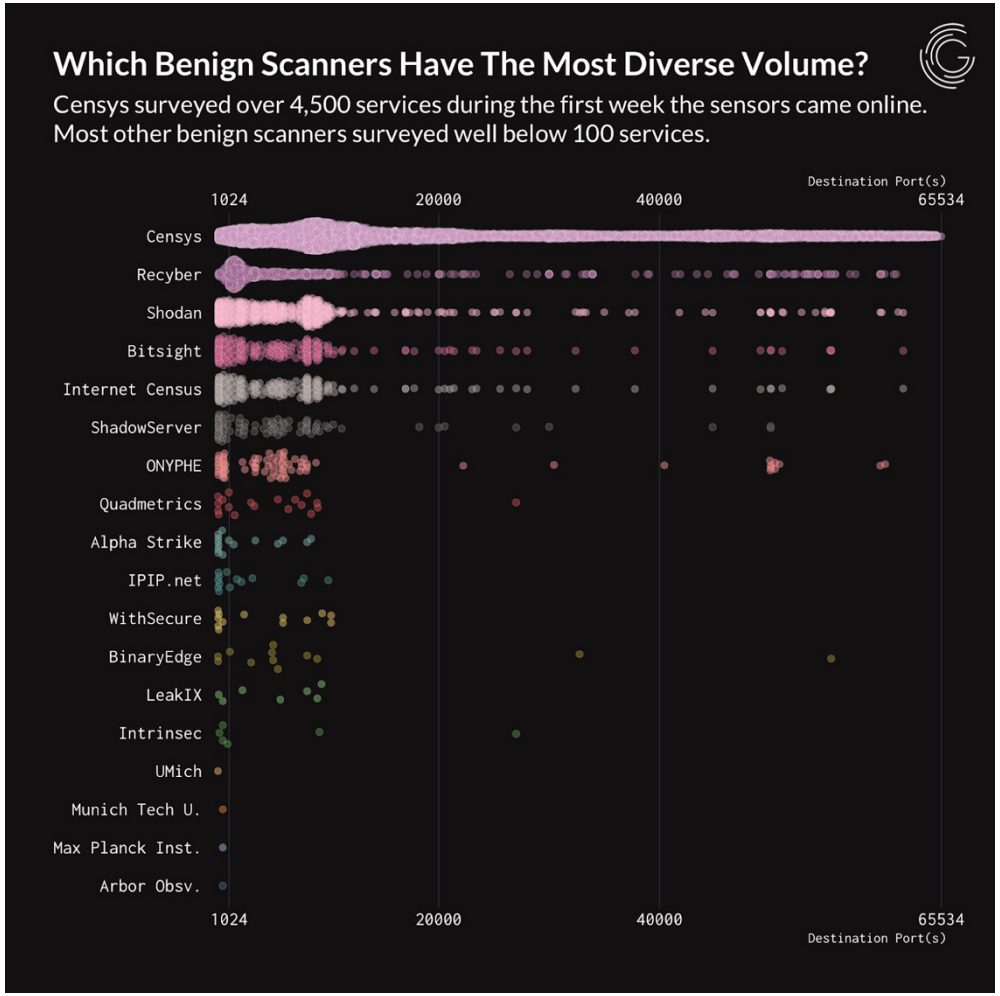
https://www.greynoise.io/blog/new-sensor-benign-activity

Censysの特徴– 2



- **GreyNoise社**での観測データから多くのサーバ対しても最も短い時間で調査が行われる事がわかります。
  - IPの登録を行わずにcensys searchにクエリーを投げることで対象のIPの最新の情報をいち早く取得できることができることがわかります。

Censysの特徴－３



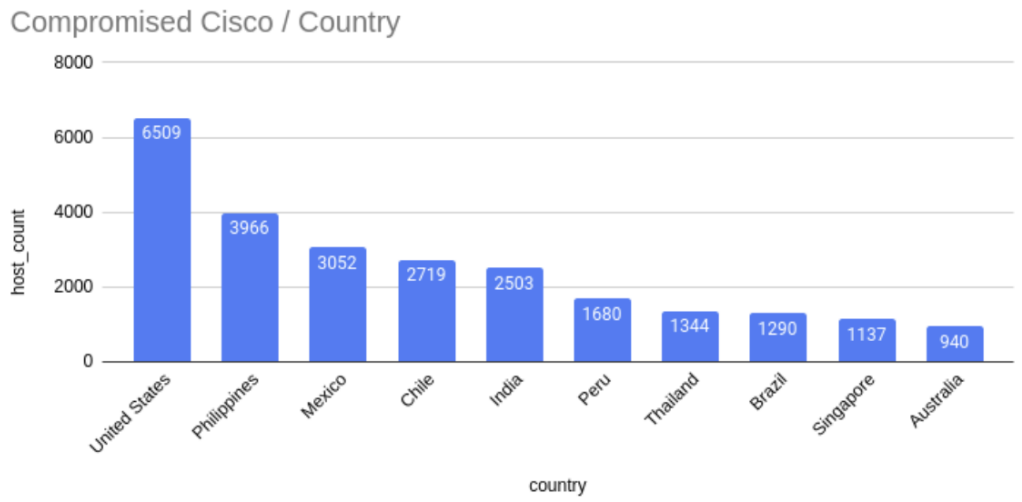
- **GreyNoise社**での観測データから多くのport対しても調査が行われる事がわかります。
  - IPの登録を行わずにcensys searchにクエリーを投げることで対象のIPの多くのportの状態を取得することができることがわかります。

Censysの特徴−4

CVE-2023-20198 – Cisco IOS-XE ZeroDay

October 18th, 2023

We reran the scan overnight and found a sharp increase in infections. Iterating on our current query to find potential targets, we updated it with some more generic conditionals, hoping to find even more potentially vulnerable hosts. Unfortunately, the updates were successful, and we found even more compromised hosts this morning. Here is an updated set of statistics.



We have also conducted a secondary scan to analyze just how widespread this vulnerability is by using Censys data as a baseline and utilizing the open-source utilities censys-cli, httpx, and jq to conduct our analysis.

```
$ censys search 'services.labels=cisco-xe-webui' \
| jq -cr '.[] | . | .ip as $ip \
| .matched_services[] \
| { ip: $ip, sn: .extended_service_name | ascii_downcase,   port: .port } \
| "\(.sn)://\(.ip):\(.port)"' | \
httpx   -bp -title -sc -x POST \
-path /webui/logoutconfirm.html?logon_hash=1 -mr '([a-f0-9]{18})'
```

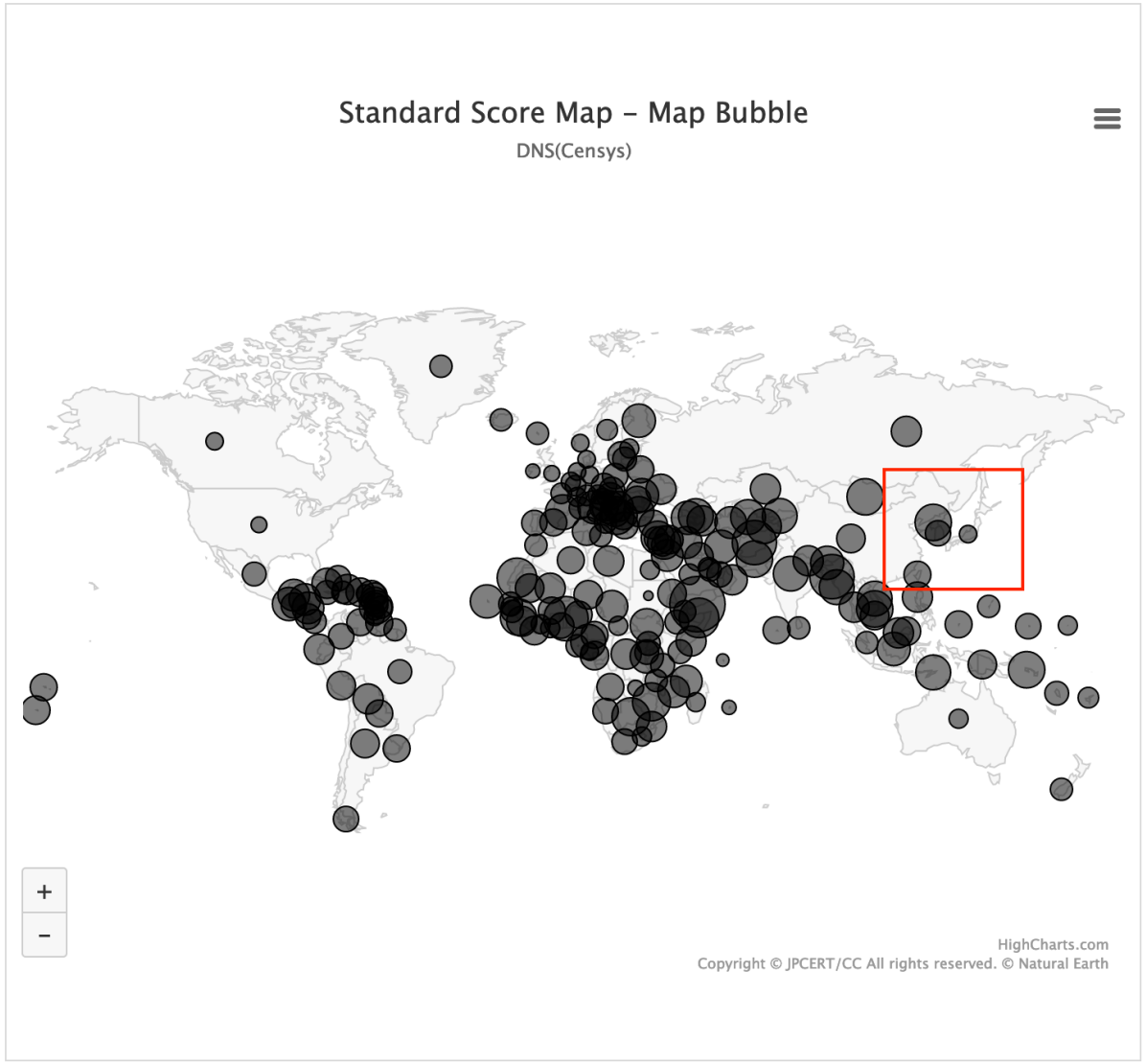
CVE-2023-20198の可能性のあるIPの検索方法

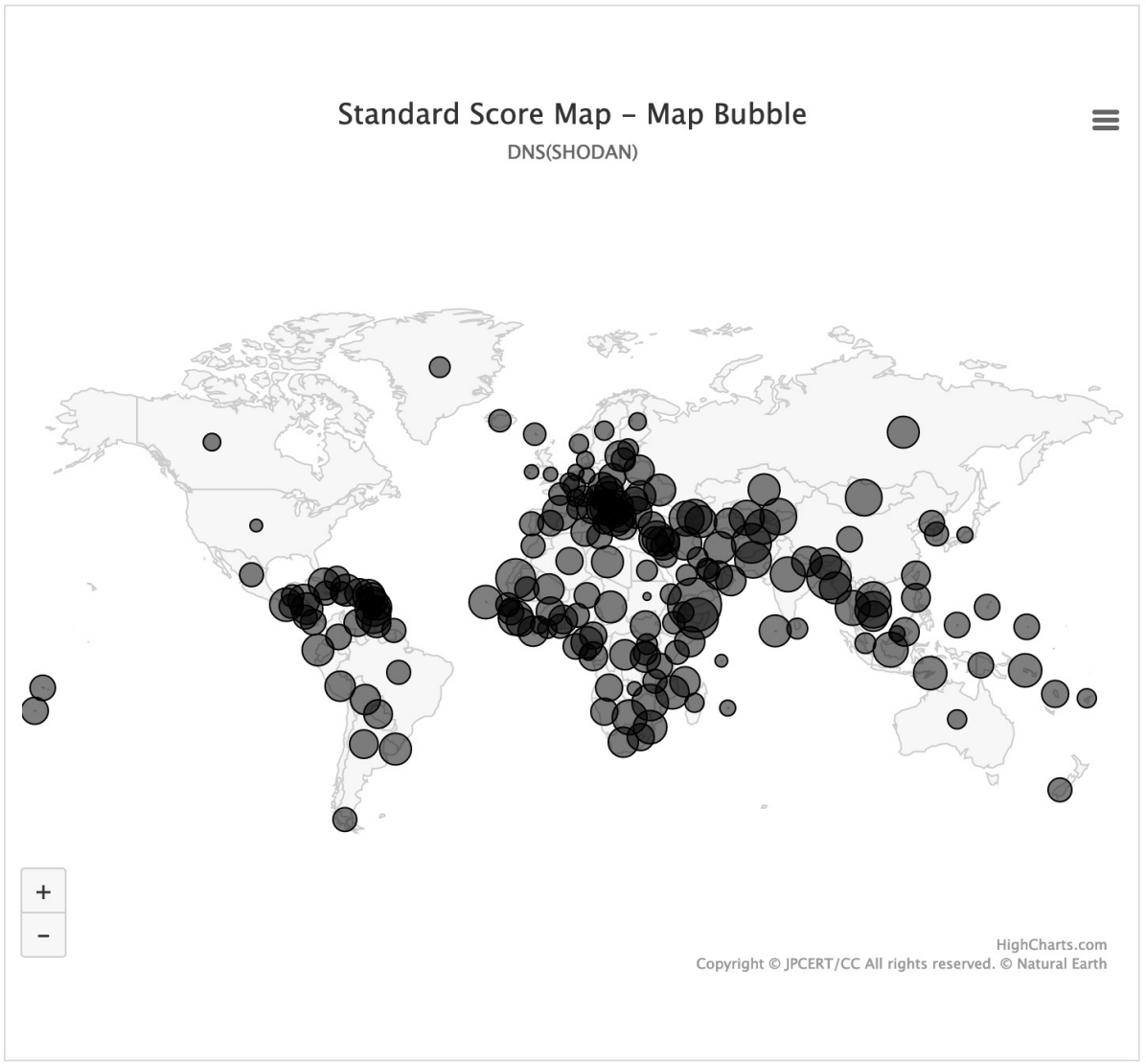
- 上記のようなZeroDayが発生した場合もIPの登録を行わずにcensys searchにクエリーを投げることで対象のIP抽出できる場合があます。

https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday/

実証実験:インターネットリスク可視化サービス―Mejiro―

世界におけるDNSのNode数
　　一部の地域のバブル(円)の大きさでCensys Search が大きいことがわかる。





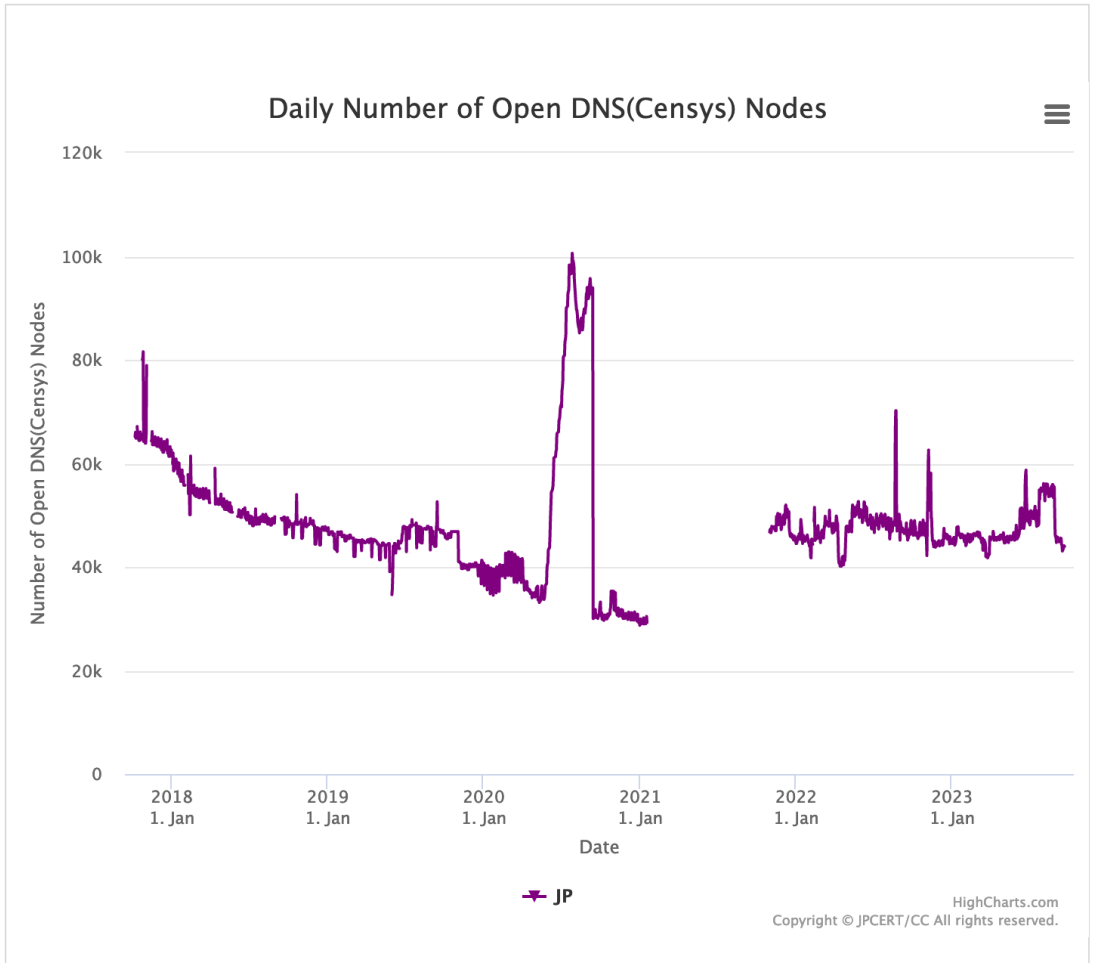
https://www.jpcert.or.jp/mejiro/

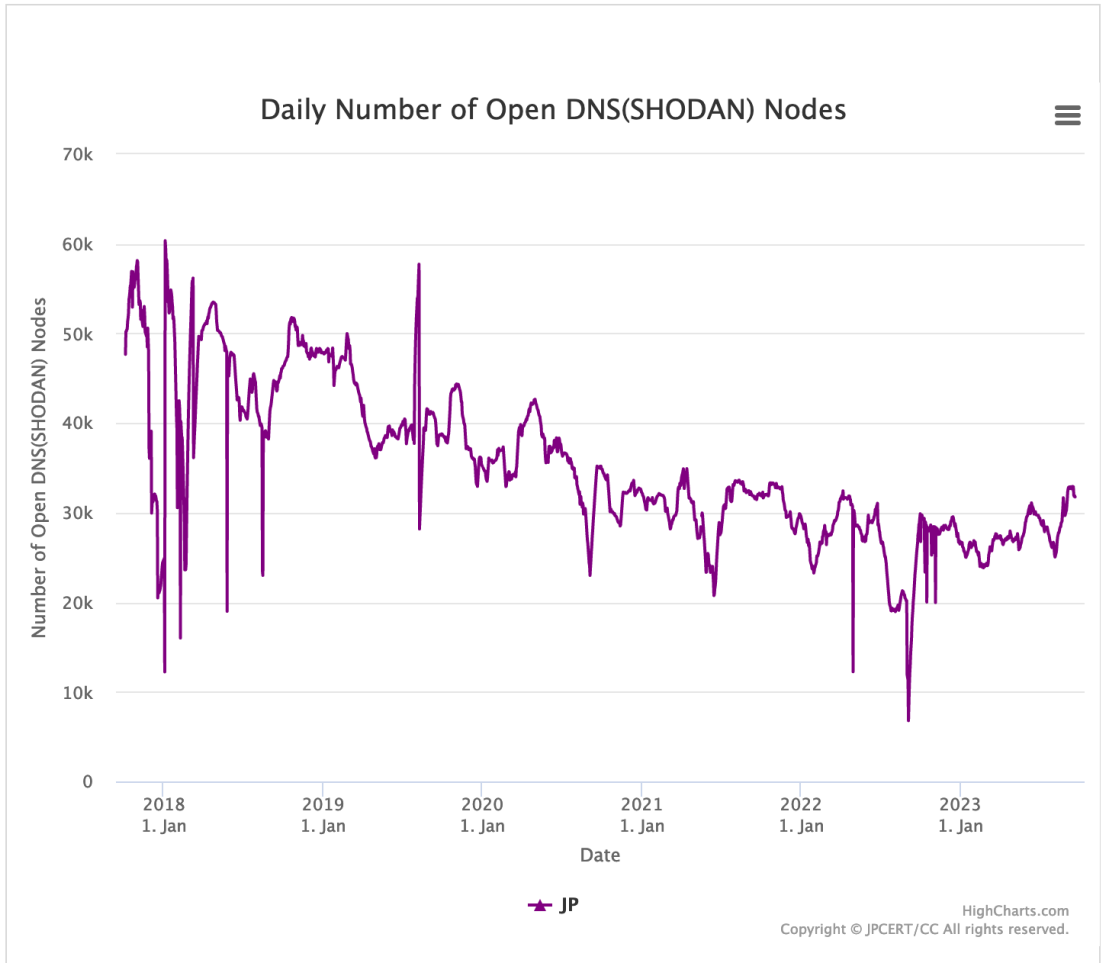
実証実験:インターネットリスク可視化サービス―Mejiro―

日本国内におけるDNSのNode数

Y軸のNode数を見るとCensys Searchの方がデータ数が多いということがわかる。

このことからcensysの方がより多くのIPアドレスと定期的に探索していることが分かる。

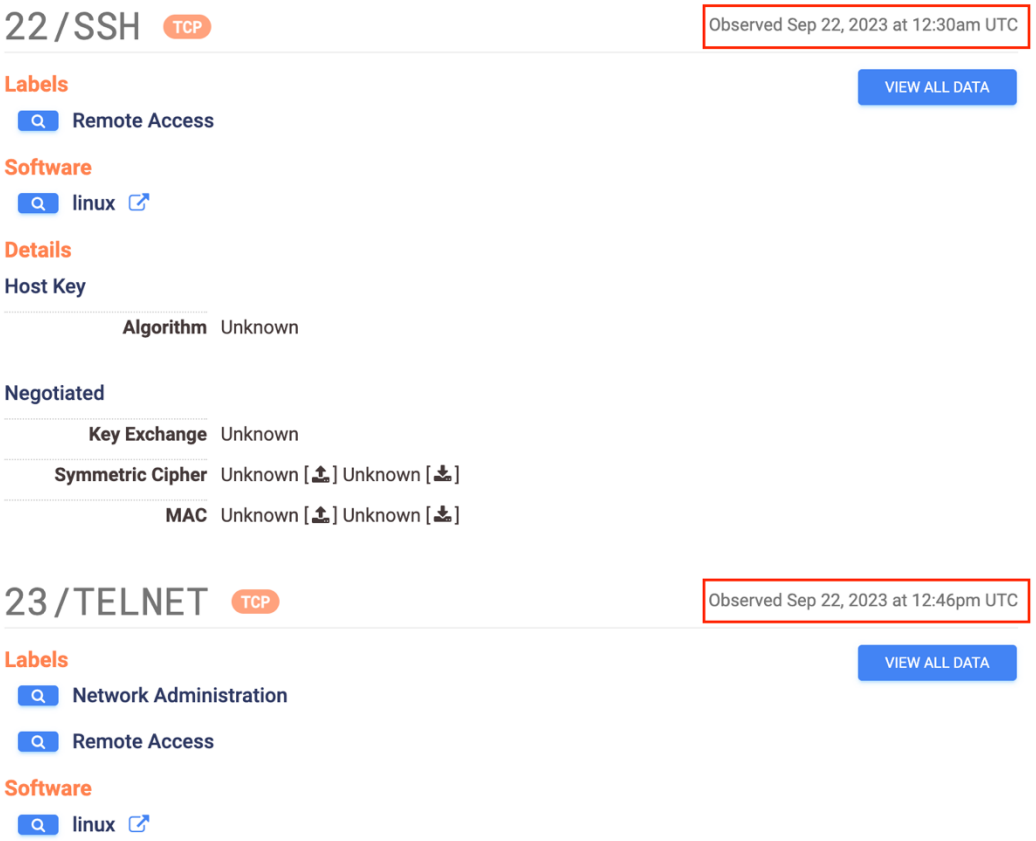




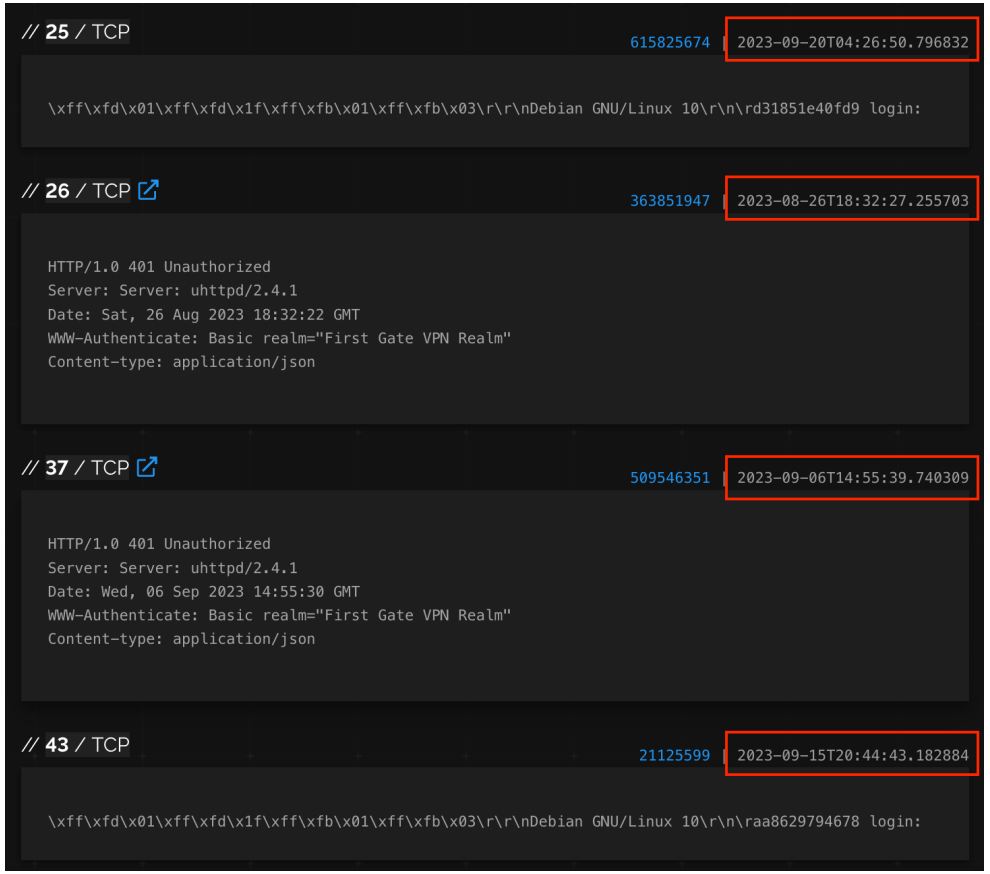
https://www.jpcert.or.jp/mejiro/

データの新鮮さについて

RainForestで運用しているハニーポットの検査情報で比較してみた。
実施日：2023/09/23 AM 8:00



Censys



Shodan

赤枠の部分が検査日だと思われます。Shodanは日付がバラバラなのに対してcensysは前日のタイムスタンプとなっています。このことからcensysのデータがより新鮮だとわかります。

情報の精度について

RainForestで運用しているハニーポットの検査情報で比較してみた。
実施日：2023/09/23 AM 8:00

services.http.response.headers.WWW_Authenticate	Basic realm="First Gate VPN Realm"
services.http.response.headers.Server	Server: uhttpd/2.4.1
services.http.response.html_tags	<title></title>
services.http.response.html_tags	<meta http-equiv="X-DEVICE" content="AE1021PE Archer_A10 BBR-4HG BBR-4MG BHR-4GRV2 BS-GS2008P DBA-1510P DGS-1100-08P DS-2CD2143G0-I DS-7604NI-E1 DS218j DVR_1080P_AHD_4 ER-X FON2601E FortiWiFi-40C GS108E HDL-TA2_E HS3LC2 NPort5110 RT-AC68U RT2600ac SRX300 SWX3100-10G TL-WR902AC TS-231P VR-S1000 Vigor_2860ac WATCHBOOT_nino_RPC-M2C WF1200CR WG1200HS2 WG1900HP2 WG2600HS WSR-1166DHPL2_N WSR-2533DHP3 WSR-3200AX4S_DWH WXR-2533DHP2 WXR-5700AX7S ZyWALL_USG_50 uM310RC">
services.http.response.html_tags	<meta property="product:retailer_title" content="EC-CUBE SHOP">
services.http.response.html_tags	<meta property="product:retailer_title" content="EC-CUBE SHOP">
services.http.response.html_tags	<meta name="description" content="VyOS Forinet FortiOS CISCO VPN OpenWRT"/>
services.http.response.html_tags	<meta name="description" content="IoT Router buffalo Netcomm"/>
services.http.response.html_tags	<meta name="description" content="NAS Camera"/>
services.http.response.body_size	1739
services.http.response.body	HTTP/1.0 200 OK\r\nServer: Server: uhttpd/2.4.1 \r\nDate: Thu, 21 Sep 2023 21:17:45 GMT\r\nContent-Type: text/html\r\n\r\n<html>\n<head>\n <meta http-equiv="X-DEVICE" content="AE1021PE Archer_A10 BBR-4HG BBR-4MG BHR-4GRV2 BS-GS2008P DBA-1510P DGS-1100-08P DS-2CD2143G0-I DS-7604NI-E1 DS218j DVR_1080P_AHD_4 ER-X FON2601E FortiWiFi-40C GS108E HDL-TA2_E HS3LC2 NPort5110 RT-AC68U RT2600ac SRX300 SWX3100-10G TL-WR902AC TS-231P VR-S1000 Vigor_2860ac WATCHBOOT_nino_RPC-M2C WF1200CR WG1200HS2 WG1900HP2 WG2600HS WSR-1166DHPL2_N WSR-2533DHP3 WSR-3200AX4S_DWH WXR-2533DHP2 WXR-5700AX7S ZyWALL_USG_50 uM310RC">\n <met

Censys

// 1024 / TCP 1631899301 | 2023-09-15T16:51:45.336972

```
HTTP/1.0 401 Unauthorized
Server: Server: uhttpd/2.4.1
Date: Fri, 15 Sep 2023 16:51:39 GMT
WWW-Authenticate: Basic realm="First Gate VPN Realm"
Content-type: application/json
```

// 1337 / TCP -542592120 | 2023-08-26T10:14:29.898304

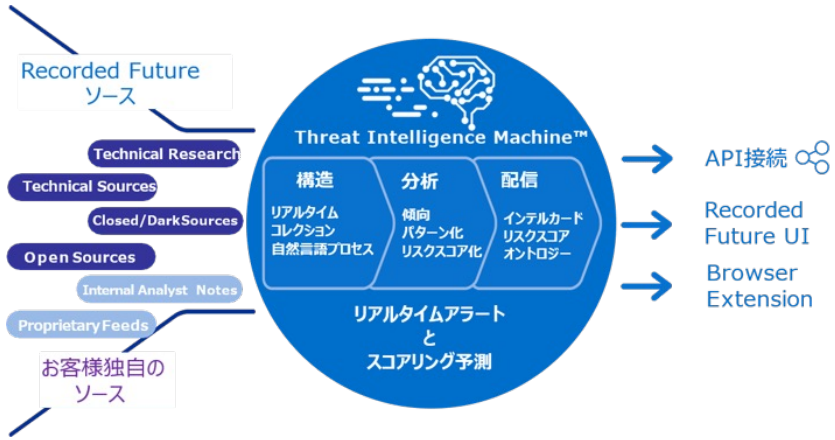
```
HTTP/1.0 401 Unauthorized
Server: Server: uhttpd/2.4.1
Date: Sat, 26 Aug 2023 10:14:24 GMT
WWW-Authenticate: Basic realm="First Gate VPN Realm"
Content-type: application/json

HTTP/1.0 200 OK
Server: Server: uhttpd/2.4.1
Date: Sat, 26 Aug 2023 10:14:24 GMT
Content-Type: text/html

<html>
<head>
  <meta http-equiv="X-DEVICE" content="AE1021PE Archer_A10 BBR-4HG BBR-4MG BHR-4GRV2 BS-GS2008P DBA-
1510P DGS-1100-08P DS-2CD2143G0-I DS-7604NI-E1 DS218j DVR_1080P_AHD_4 ER-X FON2601E FortiWiFi-40C GS
108E HDL-TA2_E HS3LC2 NPort5110 RT-AC68U RT2600ac SRX300 SWX3100-10G TL-WR902AC TS-231P VR-S1000 Vig
or_2860ac WATCHBOOT_nino_RPC-M2C WF1200CR WG1200HS2 WG1900HP2 WG2600HS WSR-1166DHPL2_N WSR-2533DHP3
WSR-3200AX4S_DWH WXR-2533DHP2 WXR-5700AX7S ZyWALL_USG_50 uM310RC">
  <meta property="product:retailer_title" content="EC-CUBE SHOP">
  <meta property="product:retailer_title" content="EC-CUBE SHOP">
  <meta name="description" content="VyOS Forinet FortiOS CISCO VPN OpenWRT"/>
  <meta name="description" content="IoT Router buffalo Netcomm"/>
  <meta name="description" content="NAS Camera"/>
  <title></title>
</head>
```

Shodan

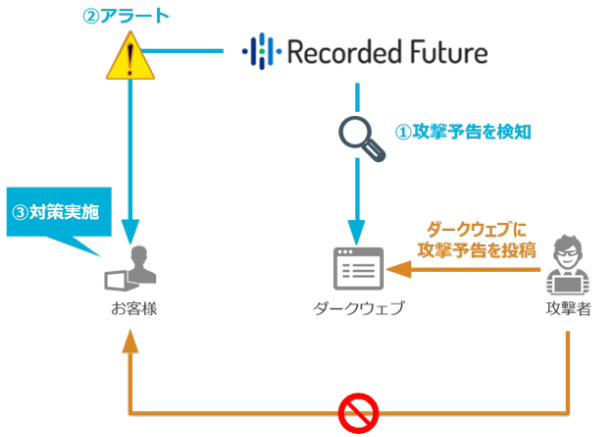
Shodanはport毎に表されるデータが異なる場合がある、この場合はHTTPのHeaderのみのportとHTTPのBodyも表示されるportがある、一方censysはどのportに対してもHTTP HeaderとBodyが正確に収集されている

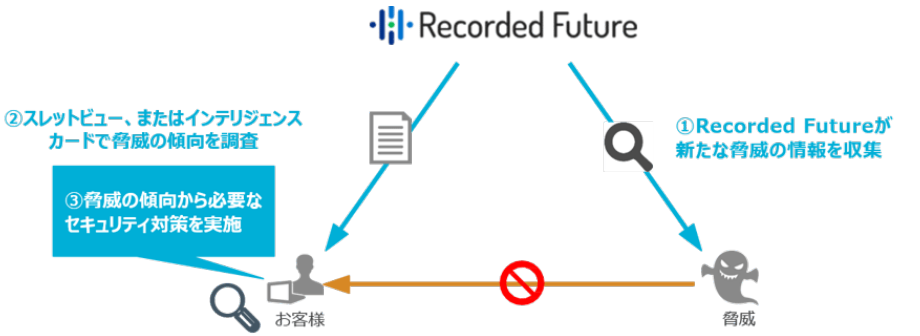
ユースケース案

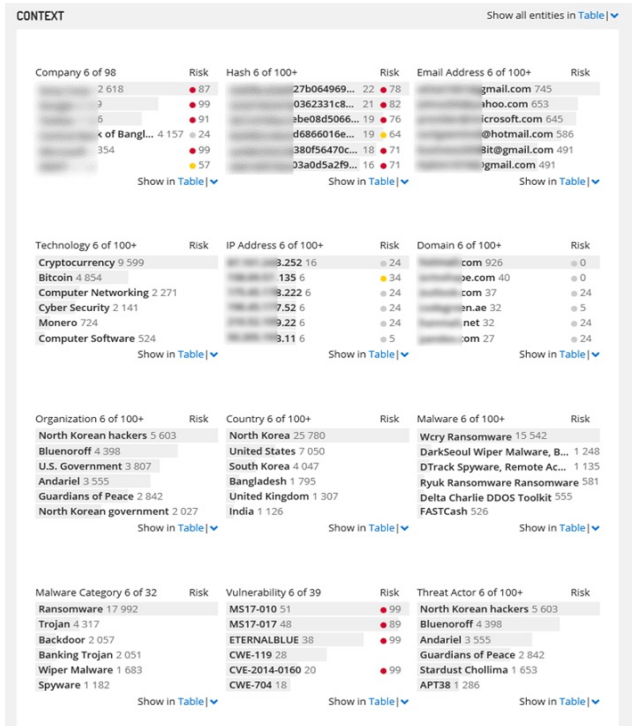
Recorded Futureの特長



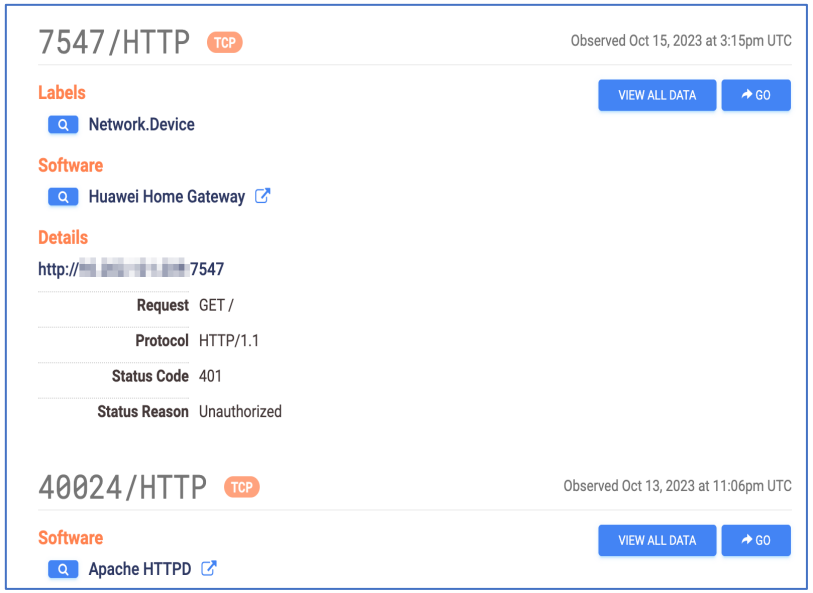
Recorded Futureの活用例







脅威に関連する情報



censys & kr:ns

インターネット上の現在の状態

- 対象の現在の状態を把握
  - IPアドレスの存在
  - Domainの存在
- 対象の情報を収集
  - OS情報
  - 動作しているサービス
- Passiveセンサに対する対象のBehavior
  - Darknetへのアクセス
  - honypotへのアクセス
  - Honypotへの侵入

- 脅威情報の根拠を提示