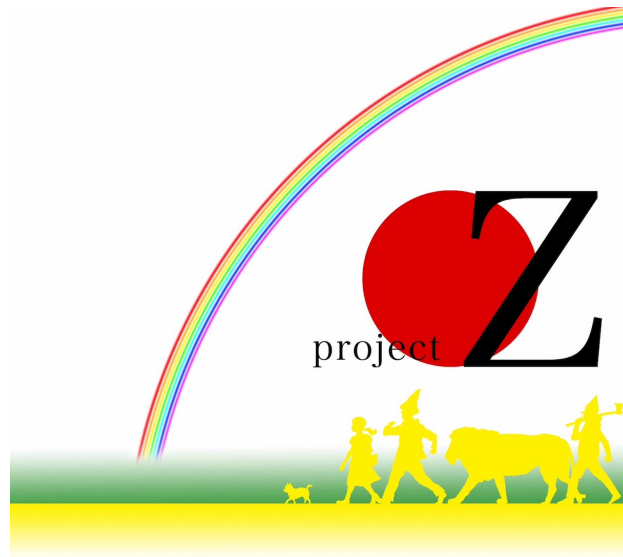
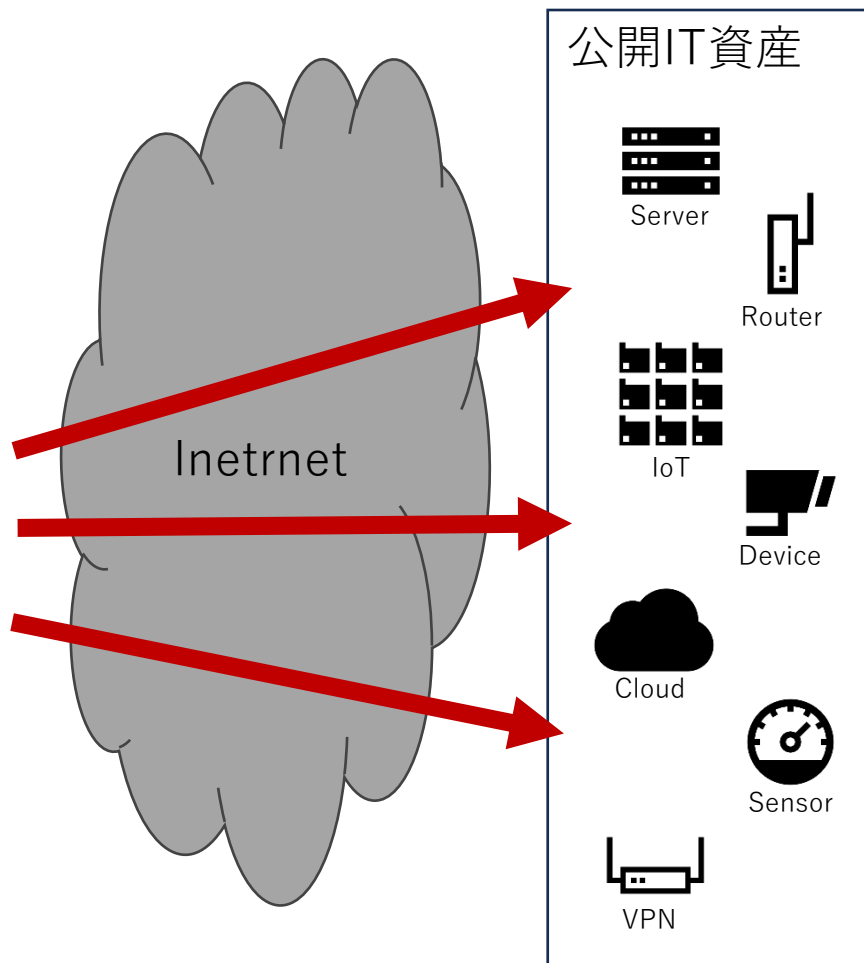
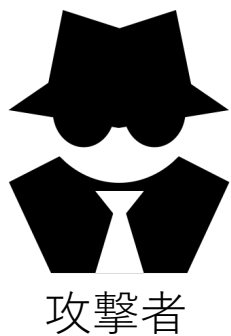


 censys & kr:ns

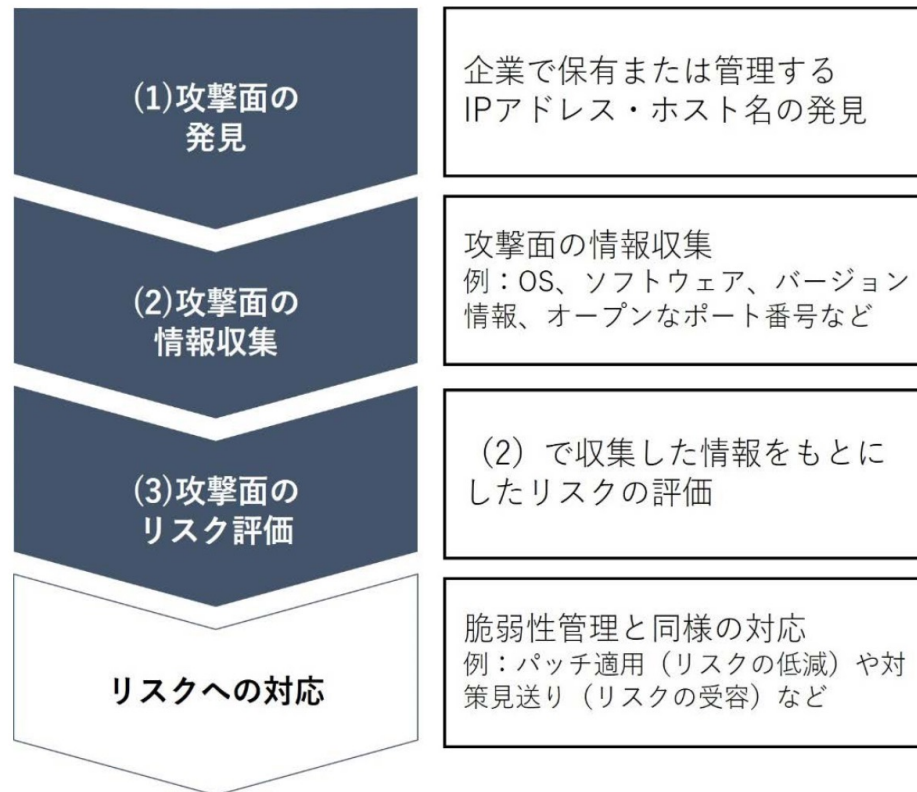
ASM (Attack Surface Management)



RainForest



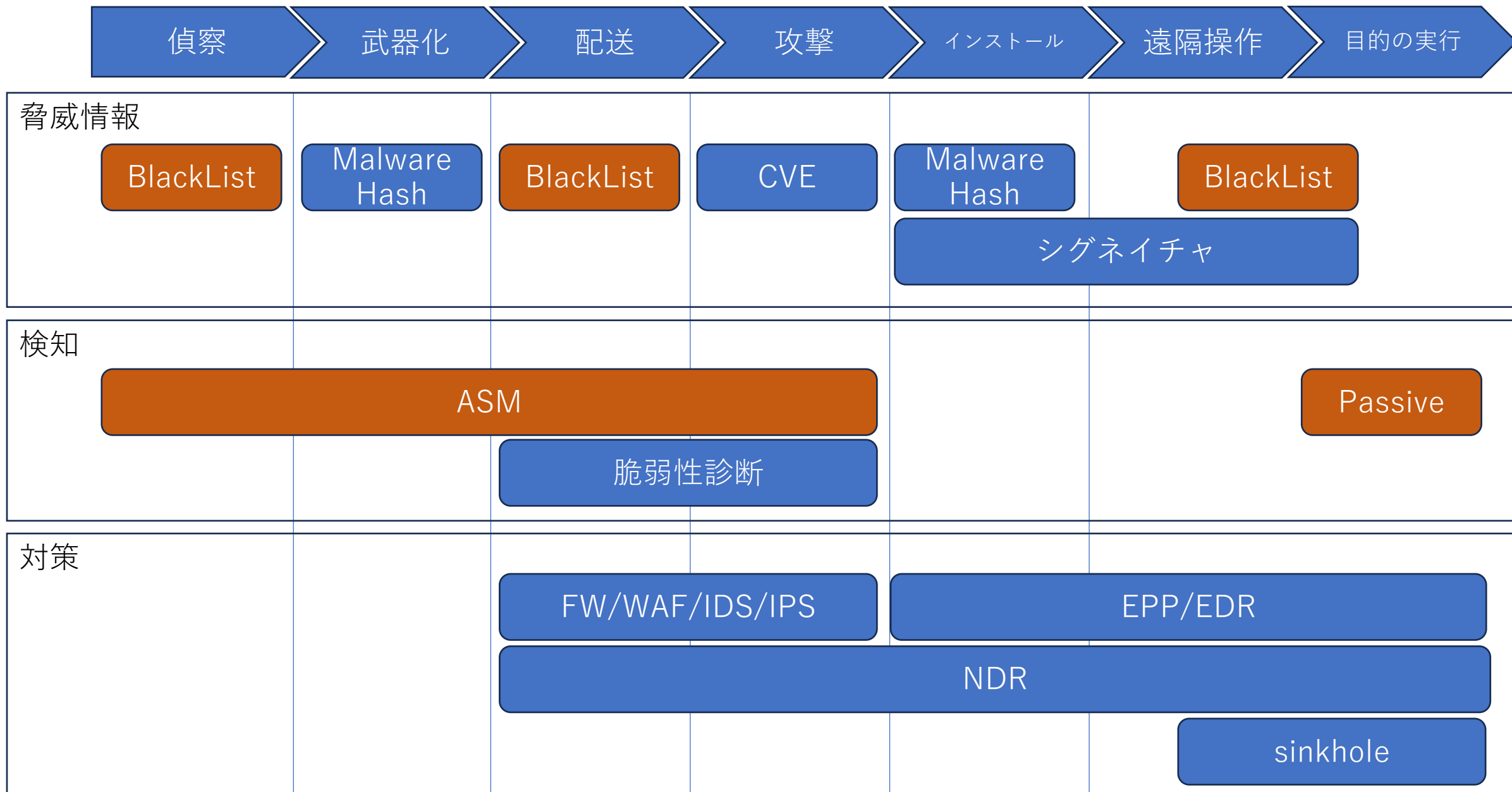
IT資産を守るためインターネットに向けて弱点をさらしているIT資産を特定・把握することが重要



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。

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>

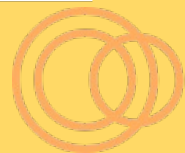
サイバーキルチェーンとのマッピング



 : 機能提供範囲



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

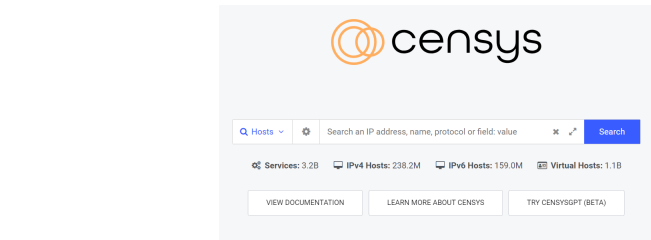
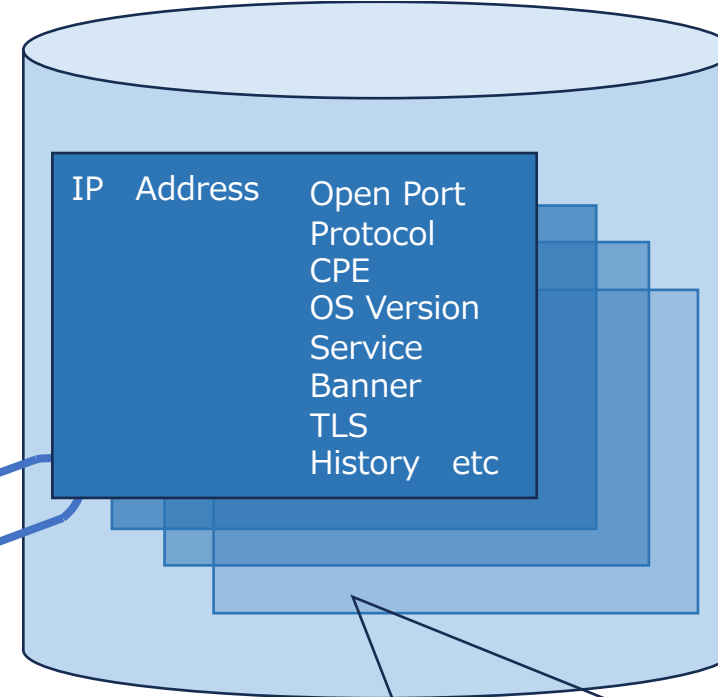
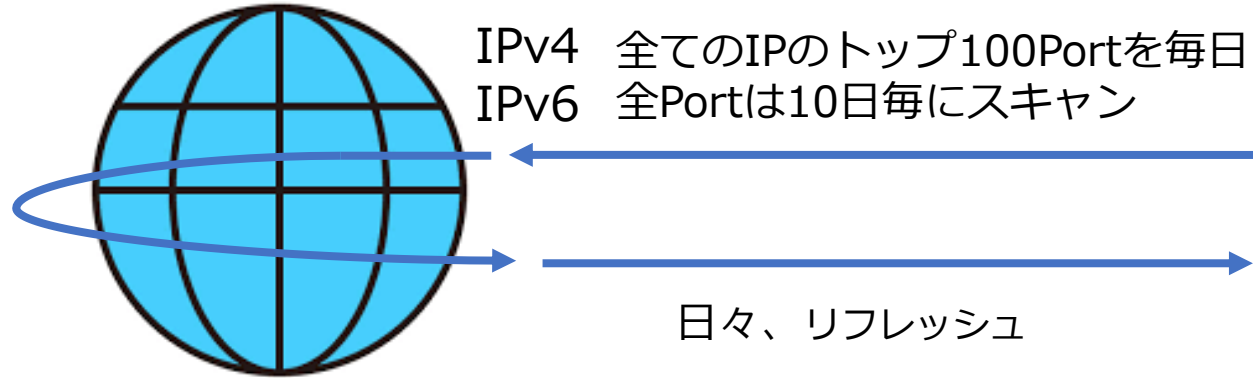


サプライチェーン全体においてのInternet Assetへの対応も可能

- ✓ 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



ユーザー



IPアドレス
IPレンジ



クエリー数/月で課金

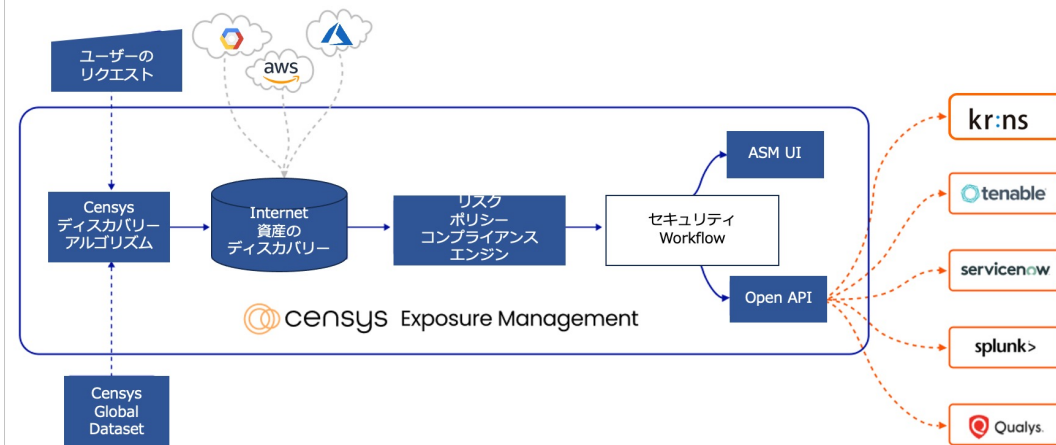


2億1100万のIPv4のホスト
6700万のIPv6のホスト
5億12000万の仮想のホスト
AWS、Azure、GCPに対応
3500以上のポート
オープンなポートとプロトコルを見える化
機器、OS、サービスの特定

ASM

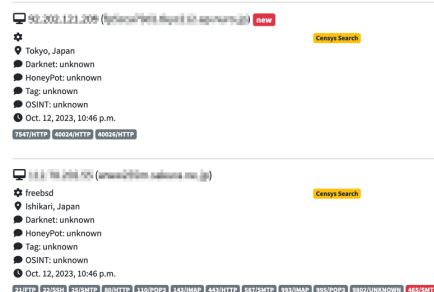
Censys Exposure Management (Scanner)

- 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

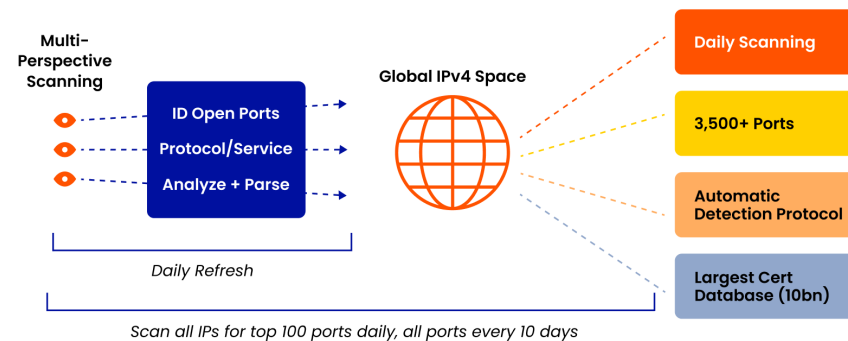


kr:ns(Passive)

- Darknet
- honeypot
- DRDoS

Censys Search(Scanner)

- IPv4,IPv6 両方に対応
- 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

Search results for IP 112.78.202.28. The interface shows various details including Basic Information, Geographic Location, and 21/FTP service details. A 'History' tab is highlighted, and an arrow points to a detailed history view on the right. The history view shows three events for 'Service Observed' with changed fields like banner, banner_hashes, smtp.ehlo, and smtp.banner.

検索結果

Attribute	Value
services.banner	220 ProFTPD Server (SAKURA Internet FTP Server) [::ffff:112.78.202.28]\v\n
services.banner_hashes	sha256:bde32db6d8f7975fa0be1cf0cd2ffb55aa1d972dbd3b27cfc9dd8e4e7475f88
services.banner_hex	3232302050726f4654504420536572766572202853414b55524120496e7465726e6574204664502053657276657229205b3a3a6666666663a3131322e37382e3230322e32385d0d0a
services.certificate	89abb2170f49afe6301e43d7f97c5e285032bb8f275828967196b738cecefc8
services.extended_service_name	FTPes
services.ftp.banner	220 ProFTPD Server (SAKURA Internet FTP Server) [::ffff:112.78.202.28]\v\n
services.ftp.auth_tls_response	234 AUTH TLS successful\v\n
services.ftp.status_code	220
services.ftp.status_meaning	Service ready for new user.
services.ftp.implicit_tls	false
services.labels	file-sharing
services.observed_at	2023-10-13T21:33:30.6083436Z
services.perspective_id	PERSPECTIVE_TATA
services.port	21
services.service_name	FTP
services.software.uniform_resource_identifier	cpe:2.3:a:proftpd:proftpd:***.***.***
services.software.part	a
services.software.vendor	ProFTPD Project
services.software.product	ProFTPD
services.software.other.family	ProFTPD
services.software.source	OSI_APPLICATION_LAYER
services.software.other.ip	::ffff:112.78.202.28

詳細データ

履歴データ

- 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](#)



111.78.228.121 (www.film-culture.eu.jp)
frebsd
Ishikari, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 12, 2023, 6:55 p.m.
21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3 143/IMAP 443/HTTP 465/SMTP 587/SMTP 993/IMAP 9800/HTTP 9802/HTTP 995/POP3

111.78.228.121 (www.film-culture.eu.jp)
frebsd
Ishikari, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 12, 2023, 6:54 p.m.
21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3 143/IMAP 443/HTTP 465/SMTP 587/SMTP 993/IMAP 995/POP3 9802/UNKNOWN

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/>



CLI Tool例

VPN Hosts

111.78.228.121 (www.film-culture.eu.jp)
microsoft
Saitama, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 10, 2023, 6:23 p.m.
443/HTTP 500/IKE 992/HTTP 1194/OPENVPN 5555/HTTP

111.78.228.121 (www.film-culture.eu.jp)
Minamirinkan, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 14, 2023, 8:14 p.m.
1194/OPENVPN 40536/HTTP 40538/HTTP 50002/HTTP 50004/HTTP

LabelでVPNサービスを検索した結果

RainForest ASM

1.1.1.1 (www.1.1.1.1.jp) Censys Search

freebsd
Ishikari, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 12, 2023, 6:55 p.m.

21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3 143/IMAP 443/HTTP 465/SMTP 587/SMTP 993/IMAP 9800/HTTP 9802/HTTP 995/POP3

1.1.1.1 (www.1.1.1.1.jp) Censys Search

freebsd
Ishikari, Japan
Darknet: unknown
HoneyPot: unknown
Tag: unknown
OSINT: unknown
Oct. 12, 2023, 6:54 p.m.

21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3 143/IMAP 443/HTTP 465/SMTP 587/SMTP 993/IMAP 995/POP3 9802/UNKNOWN

- 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

vendor	product	version	cpe
	linux		cpe:2.3:o:*:linux:*:*:*:*:*
MikroTik	RouterOS	7.9.2	cpe:2.3:o:mikrotik:routers:7.9.2:*:*:*:*
MikroTik	RouterOS		cpe:2.3:o:mikrotik:routers:*:*:*:*

▶ cpe:2.3:o:mikrotik:routers:*:*:*:*

CVE-2008-6976

CWE	CWE-20
description	
accessVector	NETWORK
accessComplexity	LOW
severity	MEDIUM
exploitabilityScore	10.0
impactScore	4.9

- 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 Instances

● New 2,082 Active 2,082 Accepted 0 Closed 0

2,082 Risks ● 2082 New

Severity	Type	Asset ID
Critical	Vulnerable Dropbear SSH [CVE-2016-7406]	110.135.56.222
High	Expired Domain	or.tl
High	Microsoft Message Queuing (MSMQ) Service Exposed	110.130.168.198
High	Unencrypted Weak Auth Page	110.130.124.36
High	Unencrypted Weak Auth Page	110.130.135.225
High	Unencrypted Login Page	110.130.128.126
High	FTP Service Exposed	110.130.116.62
High	SNMP Service Exposed	110.130.144.143
High	Unencrypted Weak Auth Page	110.130.124.36
High	Unencrypted Weak Auth Page	110.130.177.40

Risk一覧

- 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まれている

2,082 Risks ● 2082 New

Severity	Type	Asset ID	Category	First Seen	Accept Risk
Critical	Vulnerable Dropbear SSH [CVE-2016-7406]	110.135.56.222	VULNERABILITY Software	Oct 04, 2023	Accept

Risk Information

DESCRIPTION
The Dropbear SSH service before version 2016.74 allows remote attackers to execute arbitrary code via format string specifiers in the username or host argument.

REMIEDIATION RECOMMENDATIONS
Primary
Upgrade the Dropbear SSH service to the latest version.

[View Scan Data](#)

IP ADDRESS
110.135.56.222

URI
ssh://110.135.56.222:22

DISCOVERED AT
Oct 4, 2023 09:40 AM UTC

LAST SEEN
Oct 4, 2023 09:40 AM UTC, 1 hours ago

CATEGORIES
SOFTWARE VULNERABILITY

Risk詳細

Scan Data

Table JSON

Copy JSON Download Print

Attribute	Evidence
services.banner	SSH-2.0-dropbear_2012.55
services.banner_hashes[0]	sha256:92fd2876b96eea97f81a0f2a533007171af0641a047237db5018e6d416d38729
services.discovery_method	IPV4_WALK_FULL_PRIORITY_1
services.extended_service_name	SSH
services.observed_at	2023-10-02T20:10:23Z
services.perspective_id	PERSPECTIVE_TATA
services.port	22
services.service_name	SSH
services.software[0].part	o

Scan詳細

Censys Exposure Management

Risk Instances

New 2,082 Active 2,082 Accepted 0 Closed 0

2,082 Risks 2082 New

	Severity	Type	Asset ID	Category
> <input type="checkbox"/>	Critical	Vulnerable Dropbear SSH [CVE-2016-7406]	110.135.56.222	VULNERABILITY
> <input type="checkbox"/>	Critical	Expired Domain	or.tl	VULNERABILITY
> <input type="checkbox"/>	High	Microsoft Message Queuing (MSMQ) Service Exposed	110.130.168.198	EXPOSURE
> <input type="checkbox"/>	Medium	Unencrypted Weak Auth Page	110.130.124.36	MISCONFIG
> <input type="checkbox"/>	Low	Unencrypted Weak Auth Page	110.130.135.225	MISCONFIG
> <input type="checkbox"/>	High	Unencrypted Login Page	110.130.128.126	MISCONFIG
> <input type="checkbox"/>	High	FTP Service Exposed	110.130.116.62	EXPOSURE
> <input type="checkbox"/>	High	SNMP Service Exposed	110.130.144.143	EXPOSURE

Riskの設定変更

- 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

110.135.56.222 NEW 110-135-56-222.rev.f

Manage Tags Add Comment This asset was

Summary Risks **▲ 5**

5 Active Risks Sort: Newest to Oldest

▲ Vulnerable Dropbear SSH [CVE-2016-7406] on TCP port 22 **CRITICAL RISK** Accept

ssh://110.135.56.222:22 Open for: 1 day

The Dropbear SSH service before version 2016.74 allows remote attackers to execute arbitrary code via format string specifiers in the username or host argument. [View Scan Data](#) [Hide Details](#)

RISK DETAILS		REMIEDIATION RECOMMENDATIONS
CPE	cpe:2.3:a:dropbear_ssh_project:dropbear_ssh:2012.55:*:*:*:*:*	Primary Upgrade the Dropbear SSH service to the latest version.
Port	22	
Service	SSH	
Transport	TCP	
First Seen	OCT 4, 2023 12:40 AM UTC	
Last Seen	OCT 4, 2023 12:40 AM UTC	
Type	Vulnerable Dropbear SSH [CVE-2016-7406]	

CHANGE HISTORY

- 2023年10月04日 午前0:40 UTC by Censys
Risk Status: **First seen**

IPアドレスに対するリスク詳細

Censys Exposure Management

Configure Risk Types

< Back to Risk Instances

RISKS BY SEVERITY 65 194 133 56

New since last: MONTH | Severity: 🟢🟡🔴 | State: Enabled | Risk Categories: ... | Asset Types: ALL | Q Search

426 Risk Types | 1 New | View only Edited Risk Types | Download CSV

Risk Type	Risk Instances	Asset Type	Category	Edited	State	Severity	
Vulnerable Dropbear SSH [CVE-2016-7406]	2	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Pulse Connect Secure Application [CVE-2021-22893, CVE-2021-22894, CVE-2021-22899, CVE-2021-22900]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Pulse Connect Secure [CVE-2019-11507, CVE-2019-11509, CVE-2019-11541, CVE-2019-11543, CVE-2018-18284, CVE-2019-11508, CVE-2018-15909, CVE-2019-11510, CVE-2019-11538, CVE-2019-11540, CVE-2019-11542, CVE-2019-11539]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Pulse Connect Secure [CVE-2018-20810, CVE-2018-20813, CVE-2018-0486, CVE-2018-14366, CVE-2018-6320]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Exchange Server [CVE-2021-34523, CVE-2021-26858, CVE-2021-31207, CVE-2021-34473]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Bitbucket Server [CVE-2022-43781]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Fortinet FortiOS [CVE-2022-40684]	0	Host	VULNERABILITY Software		Enabled	Critical	→
Vulnerable Cisco Router [CVE-2023-20025]	0	Host	VULNERABILITY Software		Enabled	Critical	→

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

Vulnerable Fortinet FortiOS [CVE-2022-40684]

This service runs a version of Fortinet FortiOS that is vulnerable to CVE-2022-40684 (CVSSv3 9.8 out of 10). Exploitation of this vulnerability involves authentication bypass and a subsequent ability to issue commands as an administrative user.

ASSET TYPE	VULNERABILITY	ADDED ON
Host	Software Vulnerability	JAN 5, 2023 12:27 AM UTC 9 months ago

RISK STATE: Enabled Disabled

CENSYS RECOMMENDED SEVERITY: Critical

(Optional note) Add a comments or provide a reason for change.

ⓘ Historical Data will reflect the severity of the risk type at the time.

Cancel Save

Risk Type(アラート対象)詳細



RISK STATE: Enabled Disabled

CENSYS RECOMMENDED SEVERITY: Critical

(Optional note) Add a comments or provide a reason for change.

ⓘ This risk will still be present in historical data.

Save your new severity configuration × Cancel Save

有効・無効を定義



RISK STATE: Enabled Disabled

CENSYS RECOMMENDED SEVERITY: Medium

(Optional note) Add a comments or provide a reason for change.

ⓘ This risk will still be present in historical data.

Save your new severity configuration × Cancel Save

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



手法	データ	ユーザーへの意義	結果
Data Oriented	Global Internet Scanning	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 高い運用コスト● 低い信頼性● 盲点



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ことで、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。



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



SwissLife



NATO



Swiss Armed Forces
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']}
```

- マルウェ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:マルウェアの特徴の packets 送信
- Malware Download : マルウェ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
- マルウェアの特徴の packets 送信
- マルウェ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

```
{
  "file_info": {
    "timestamp": "2023-10-01 09:23:51",
    "file_format": "ELF 32-bit LSB executable, ARM, EABI5
eader",
    "md5": "9b6c3518a91d23ed77504b5416bfb5b3",
    "sha1": "0a2d170abbf5031566377b01431e3b82d342630a",
    "file_hash": "a04ac6d98ad989312783d4fe3456c53730b212c7
  },
  "domain": [
    "pool.ntp.org",
    "router.utorrent.com",
    "router.bittorrent.com"
  ],
  "download": [
    {
      "url": "http://*.*.224.19:57262/.i",
      "host": "*.*.224.19",
      "port": 57262,
      "hostname": "*.*.*.net",
      "timestamp": "2023-10-01 09:10:42",
```

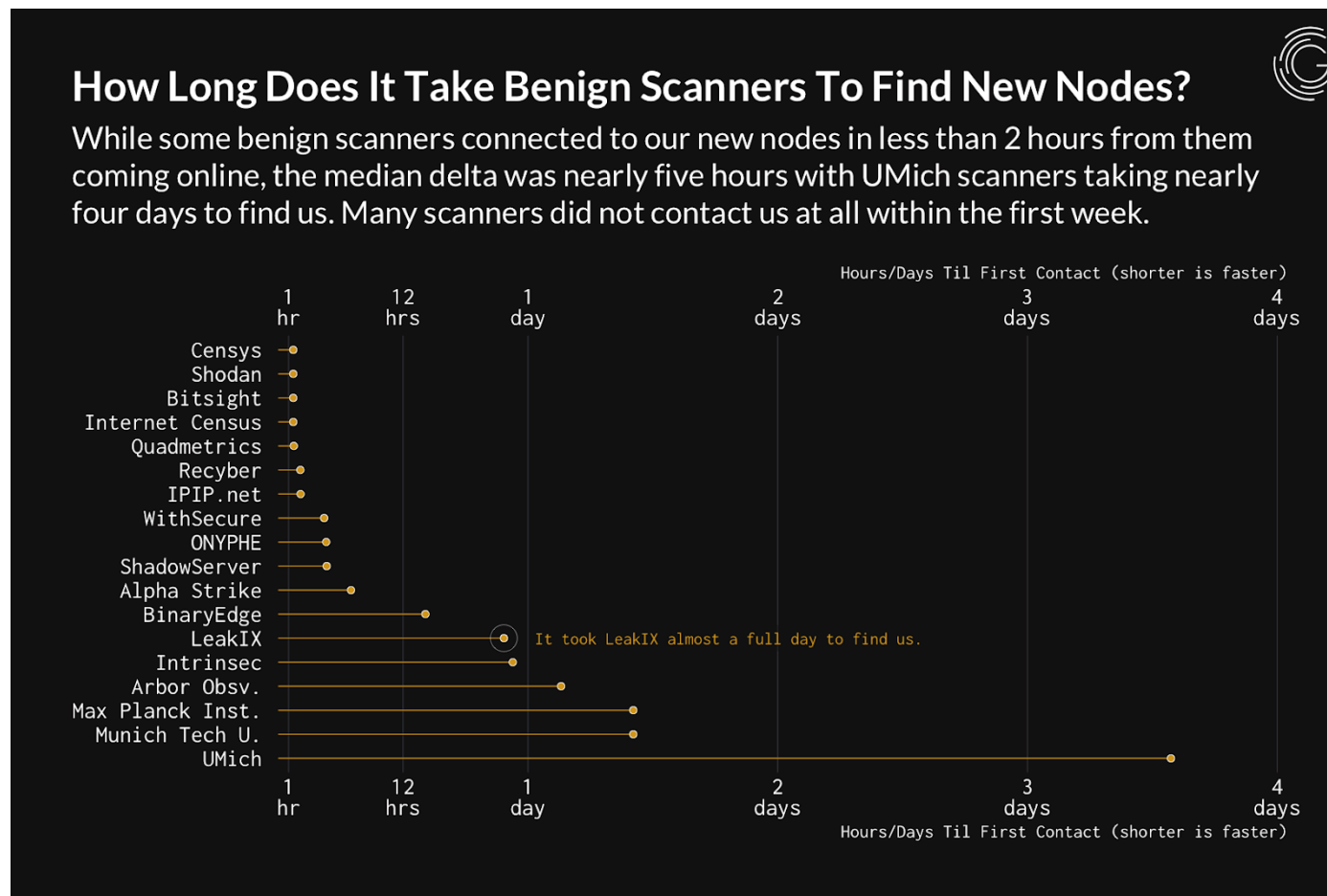
```

    },
    "scan": [
      23
    ],
    "listen": [
      {
        "ip": "0.0.0.0",
        "port": 24529
      }
    ],
    "connect": [
      {
        "ip": "*.*.92.20",
        "port": 59666,
        "hostname": "",
        "darknet": null,
        "black": [
          {
            "timestamp": "2023-09-26T00:00:00"
          }
        ]
      }
    ],
```

- 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
 - マルウェアdownload site
 - scan対象port
 - 待ち受けport
 - 通信先情報

Censysの特徴

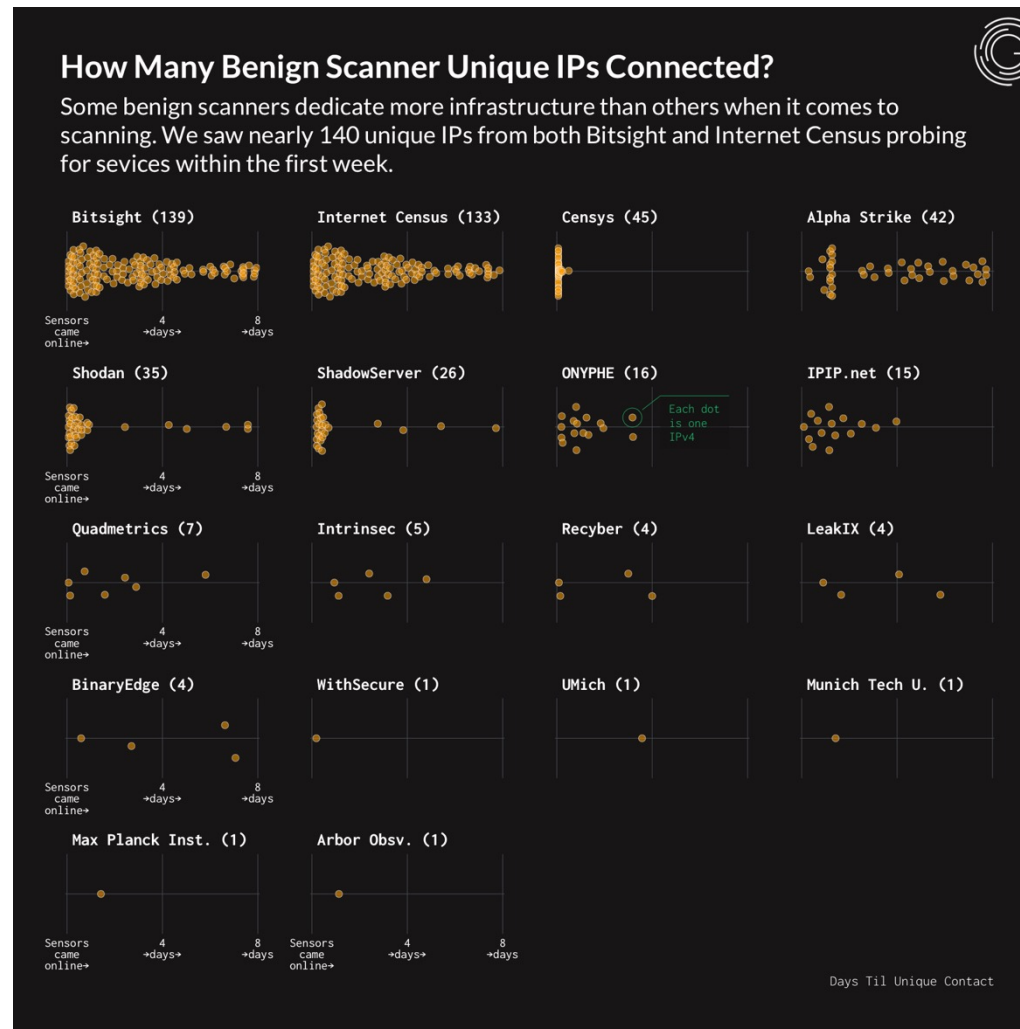
Censysの特徴－ 1



- **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。

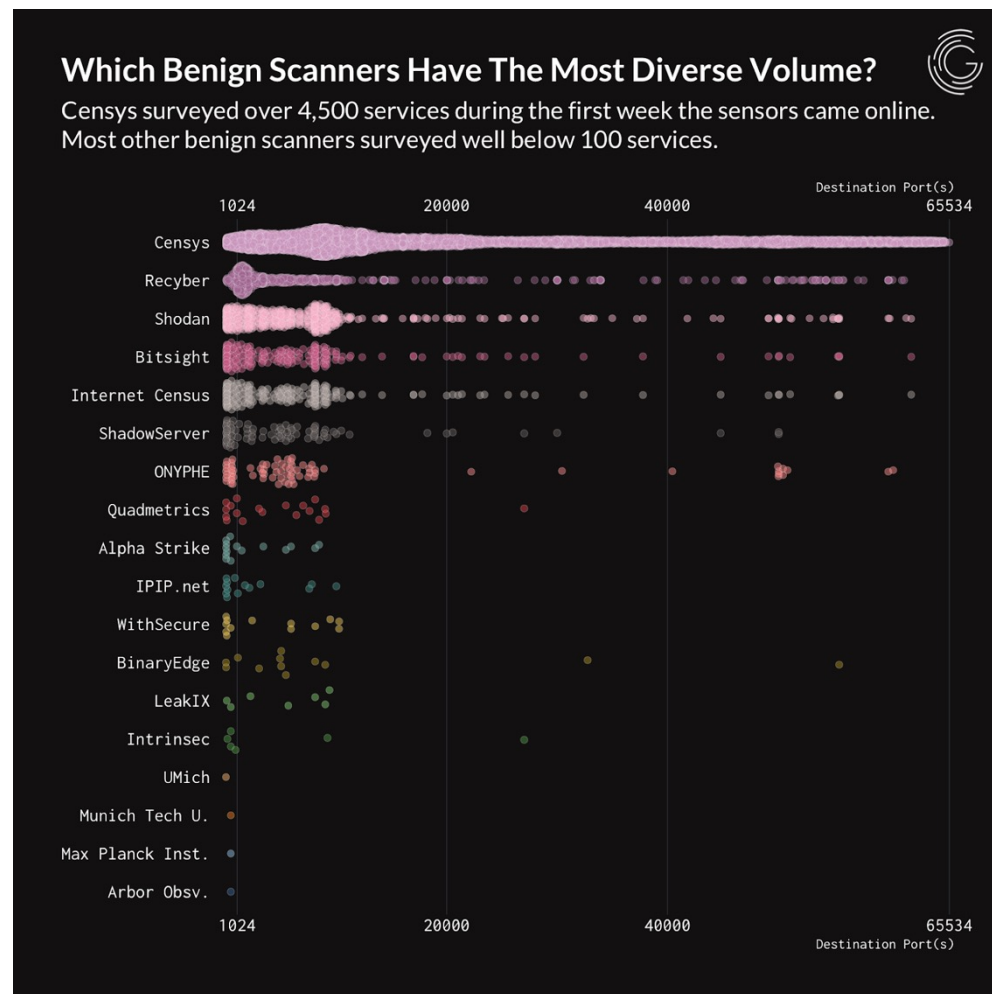
<https://www.greynoise.io/blog/new-sensor-benign-activity>

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事がわかります。

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事がわかります。

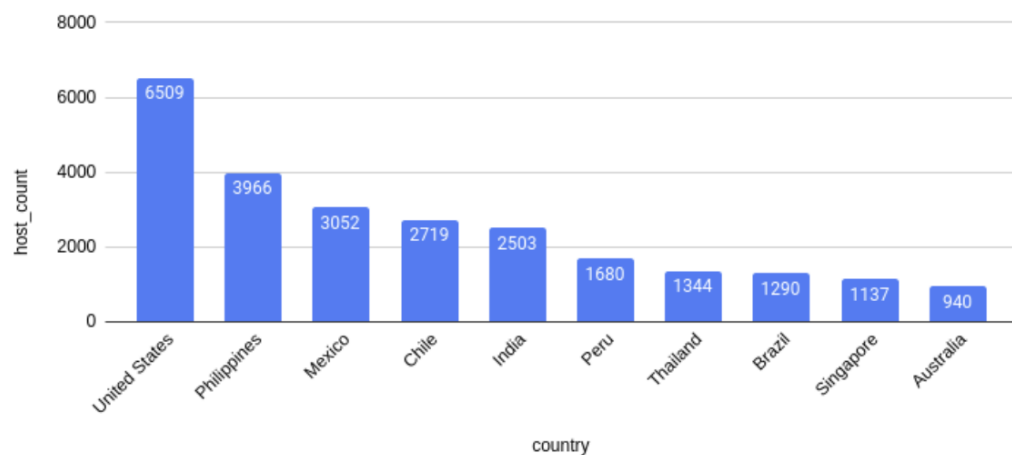
Censysの特徴-4

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.

Compromised Cisco / Country



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.

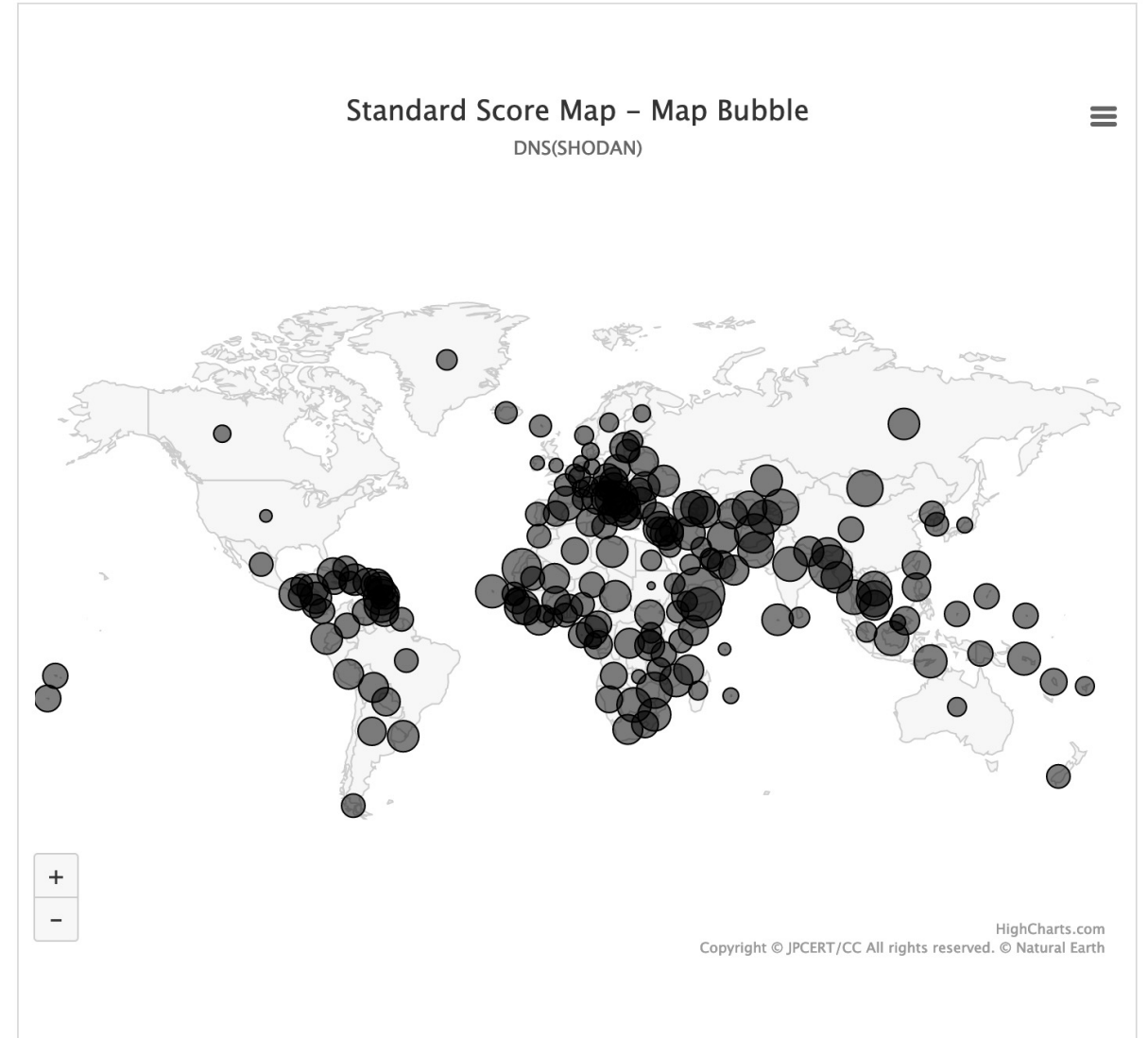
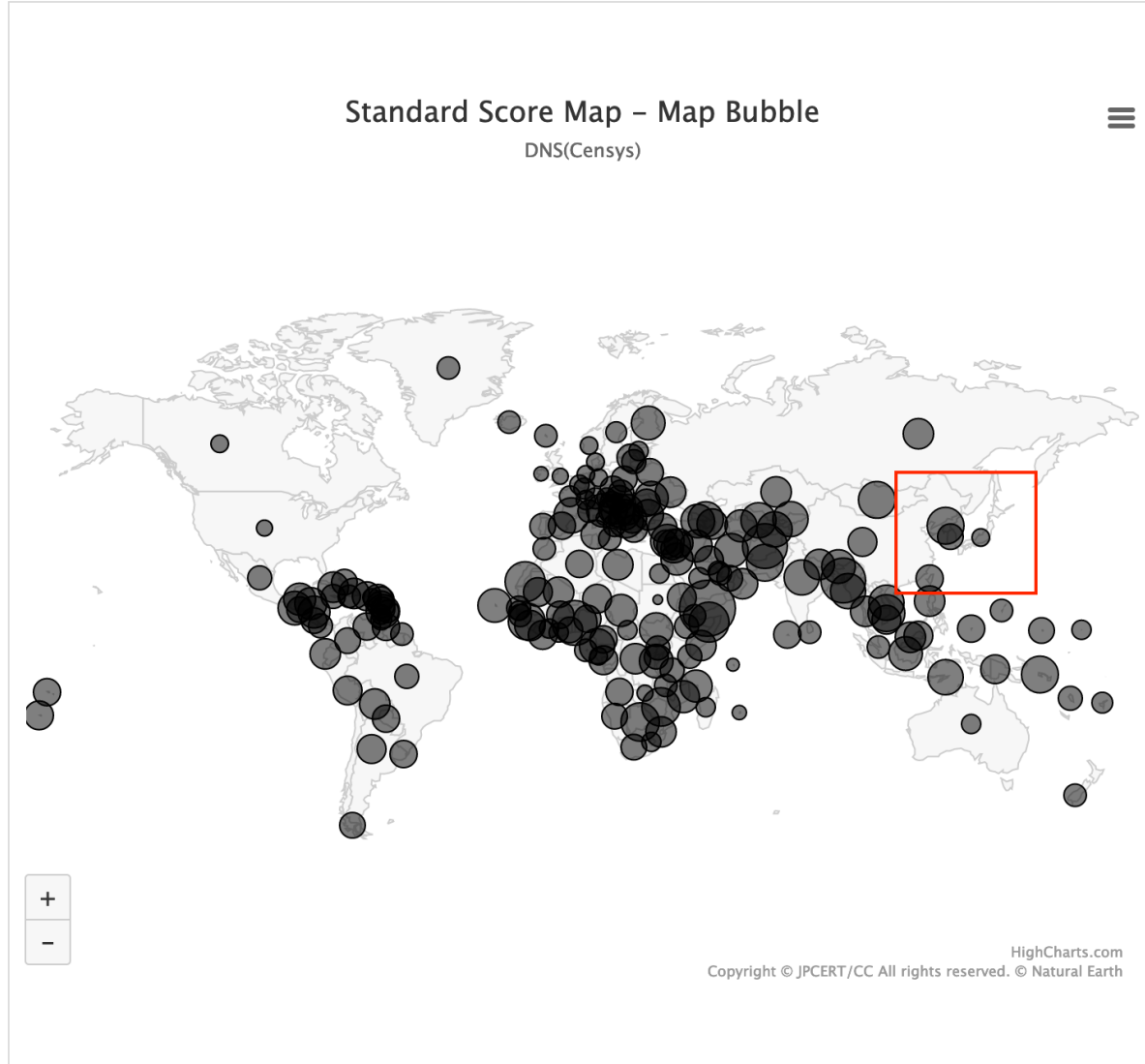
```
$ censys search 'services.labels=cisco-xe-webui' \  
| jq -cr '[] | .ip as $ip \  
| .matched_services[] \  
| { ip: $ip, sn: .extended_service_name | ascii_lowercase, port: .port } \  
| "\""(.sn):/^(.ip):(.port)"" | \  
httpx -bp -title -sc -x POST \  
-path /webui/logoutconfirm.html?logon_hash=1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

<https://censys.com/cve-2023-20198-cisco-ios-xe-zero-day/>

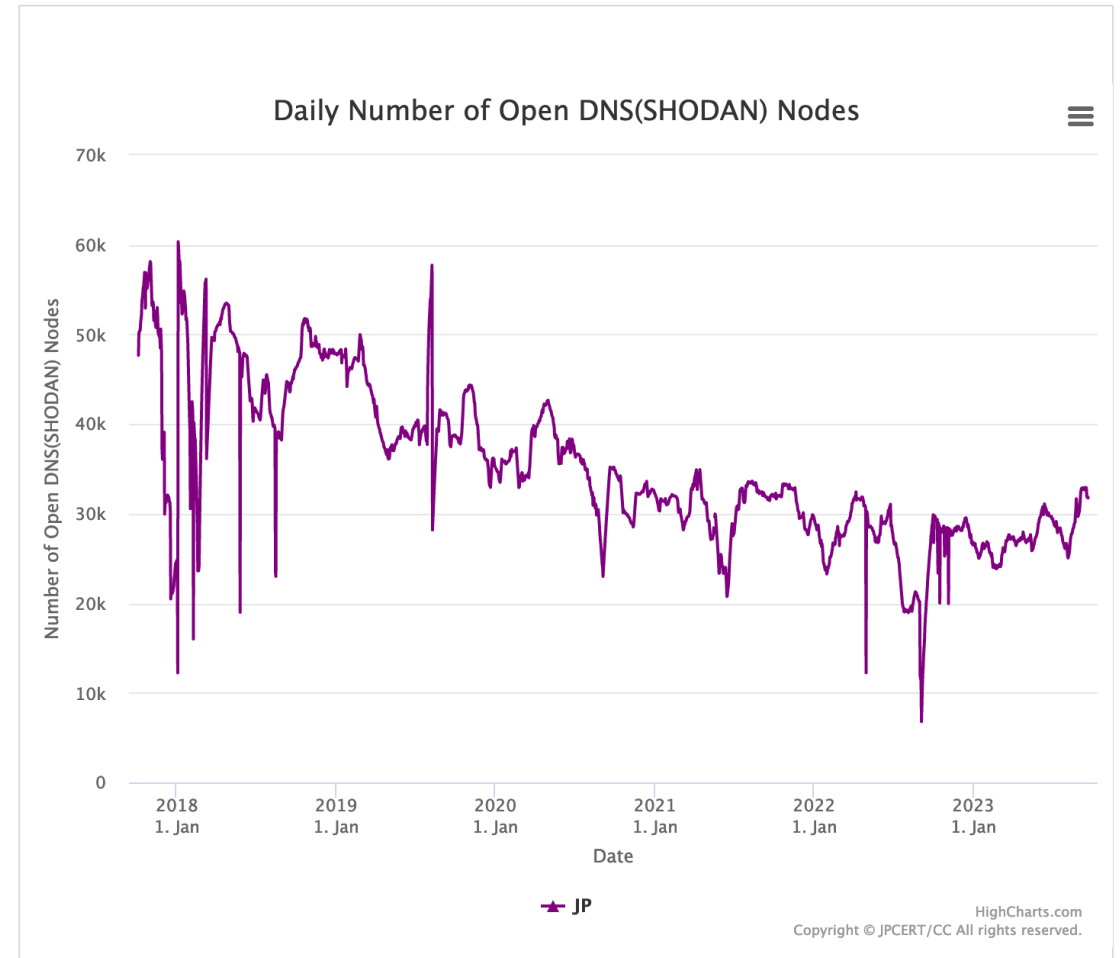
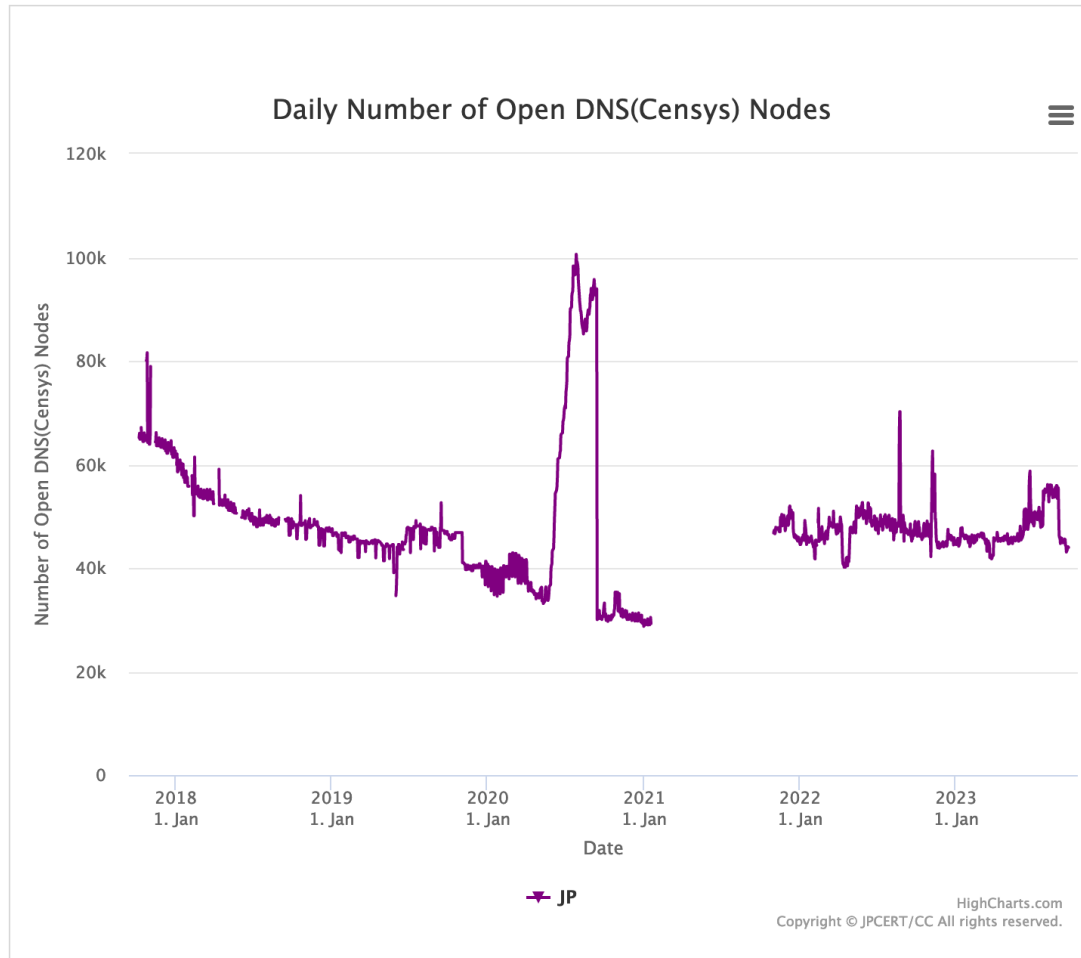
世界におけるDNSのNode数
一部の地域のバブル(円)の大きさをCensys Search が大きいことがわかる。



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。



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

22 / SSH TCP Observed Sep 22, 2023 at 12:30am UTC

Labels

Remote Access

Software

linux

Details

Host Key

Algorithm Unknown

Negotiated

Key Exchange Unknown

Symmetric Cipher Unknown [📄] Unknown [📄]

MAC Unknown [📄] Unknown [📄]

23 / TELNET TCP Observed Sep 22, 2023 at 12:46pm UTC

Labels

Network Administration

Remote Access

Software

linux

Censys

```
// 25 / TCP 615825674 2023-09-20T04:26:50.796832
\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03\r\r\nDebian GNU/Linux 10\r\n\r\nrd31851e40fd9 login:

// 26 / TCP 363851947 2023-08-26T18:32:27.255703
HTTP/1.0 401 Unauthorized
Server: Server: uhttpd/2.4.1
Date: Sat, 26 Aug 2023 18:32:22 GMT
WWW-Authenticate: Basic realm="First Gate VPN Realm"
Content-type: application/json

// 37 / TCP 509546351 2023-09-06T14:55:39.740309
HTTP/1.0 401 Unauthorized
Server: Server: uhttpd/2.4.1
Date: Wed, 06 Sep 2023 14:55:30 GMT
WWW-Authenticate: Basic realm="First Gate VPN Realm"
Content-type: application/json

// 43 / TCP 21125599 2023-09-15T20:44:43.182884
\xff\xfd\x01\xff\xfd\x1f\xff\xfb\x01\xff\xfb\x03\r\r\nDebian GNU/Linux 10\r\n\r\nraa8629794678 login:
```

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-4 GRV2 BS-GS2008P DBA-1510P DGS-1100-08P DS-2CD2143G0-I DS-7604NI-E1 DS218j DV R_1080P_AHD_4 ER-X FON2601E FortiWiFi-40C GS108E HDL-TA2_E HS3LC2 NPort5110 R T-AC68U RT2600ac SRX300 SWX3100-10G TL-WR902AC TS-231P VR-S1000 Vigor_2860a c WATCHBOOT_nino_RPC-M2C WF1200CR WG1200HS2 WG1900HP2 WG2600HS WSR-1 166DHPL2_N WSR-2533DHP3 WSR-3200AX4S_DWH WXR-2533DHP2 WXR-5700AX7S Zy WALL_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>\r\n<head>\r\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">\r\n<meta	🔍

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

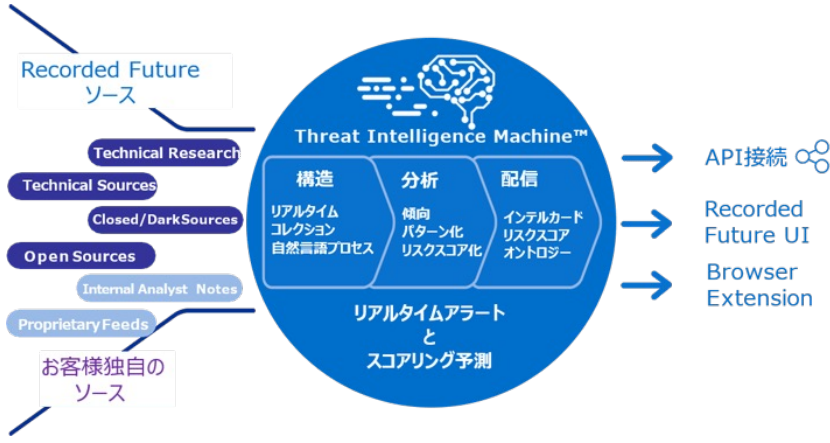
<html>
<head>
  <meta http-equiv="X-DEVICE" content="AE1021PE Archer_A10 BBR-4HG BBR-4MG BHR-4GRV2 BS-GS2008P DBA-1510P DGS-1100-08P DS-2CD2143G0-I DS-7604NI-E1 DS218j DVR_1080P_AHD_4 ER-X FON2601E FortiWiFi-40C GS108E HDL-TA2_E HS3LC2 NPort5110 RT-AC68U RT2600ac SRX300 SWX3100-10G TL-WR902AC TS-231P 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">
  <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"/>
</head>
</html>
```

Shodan

Shodanはport毎に表示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



CONTEXT

Company 6 of 98	Risk	Hash 6 of 100+	Risk	Email Address 6 of 100+	Risk
2,618	87	27b064969...	22	@gmail.com 745	78
3	99	0362331c8...	21	@yahoo.com 653	82
5	91	bbe08d5066...	19	@microsoft.com 645	76
4,157	24	d6866016e...	19	@hotmail.com 586	76
354	99	380f56470c...	18	@it@gmail.com 491	71
	57	33a0d5a2f9...	16	@gmail.com 491	71

Technology 6 of 100+	Risk	IP Address 6 of 100+	Risk	Domain 6 of 100+	Risk
Cryptocurrency 9,599	3,252	16	24	.com 926	0
Bitcoin 4,854	135	6	34	.se.com 40	0
Computer Networking 2,271	3,222	6	24	.com 37	24
Cyber Security 2,141	7.52	6	24	.in.ae 32	5
Monero 724	9.22	6	24	.net 32	24
Computer Software 524	3.11	6	5	.com 27	24

Organization 6 of 100+	Risk	Country 6 of 100+	Risk	Malware 6 of 100+	Risk
North Korean hackers 5,603	25,780	North Korea	15,542	Wcry Ransomware	15,542
Bluenoroff 4,398	7,050	United States	DarkSeoul Wiper Malware, B...	DarkSeoul Wiper Malware, B...	1,248
U.S. Government 3,807	4,047	South Korea	DTrack Spyware, Remote Ac...	DTrack Spyware, Remote Ac...	1,135
Andarief 3,555	1,795	Bangladesh	Ryuk Ransomware Ransomware 581	Ryuk Ransomware Ransomware 581	581
Guardians of Peace 2,842	1,307	United Kingdom	Delta Charlie DDOS Toolkit 555	Delta Charlie DDOS Toolkit 555	555
North Korean government 2,027	1,126	India	FASTCash 526	FASTCash 526	526

Malware Category 6 of 32	Risk	Vulnerability 6 of 39	Risk	Threat Actor 6 of 100+	Risk
Ransomware 17,992	MS17-010 51	89	99	North Korean hackers 5,603	89
Trojan 4,317	MS17-017 48	89	89	Bluenoroff 4,398	89
Backdoor 2,057	ETERNALBLUE 38	99	99	Andarief 3,555	99
Banking Trojan 2,051	CWE-119 28	99	99	Guardians of Peace 2,842	99
Wiper Malware 1,683	CVE-2014-0160 20	99	99	Stardust Chollima 1,653	99
Spyware 1,182	CWE-704 18	99	99	APT38 1,286	99

脅威に関連する情報

7547/HTTP TCP Observed Oct 15, 2023 at 3:15pm UTC

Labels

- Network.Device

Software

- Huawei Home Gateway

Details

http://[redacted] 7547

Request GET /

Protocol HTTP/1.1

Status Code 401

Status Reason Unauthorized

40024/HTTP TCP Observed Oct 13, 2023 at 11:06pm UTC

Software

- Apache HTTPD



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
 - honeypotへのアクセス
 - Honeypotへの侵入
- 脅威情報の根拠を提示