network system
Vulnerability Diagnosis Probe

KATABAMI VDP

～ しくみ編 ～

2022年8月（初版）

2023年1月（社外向け 1.0版）

株式会社SYNCHRO 中村 健

SYNCHRO

CSCC

Cyber Security
Countermeasures
Center

期待されること

簡単、安全、有効 な 脆弱性診断

- 簡単
  - 対象となるネットワークに設置するだけ
  - 対象となるネットワークの設定変更は不要
  - 脆弱性診断用デバイスを送付し、対象ネットワークに接続するだけ
    - 作業員が訪問しての設置・設定作業は不要
- 安全
  - 脆弱性診断用デバイスが収集した情報は安全にセンタに伝送
  - 脆弱性診断用デバイスの通信経路が抜け道にならない
  - 脆弱性診断用デバイスが対象ネットワークの通信に影響しない
- 有効
  - 脆弱性診断用デバイスを投入することで対象ネットワークの内部からのチェックも可能
    - セキュリティ対策は、入口対策、出口対策、内部対策 の３つが必要
  - 外側と内側から挟撃
    - 外側からの検証：センタからインターネット経由でのチェック
    - 内側からの検証：脆弱性検証用デバイスからのチェック

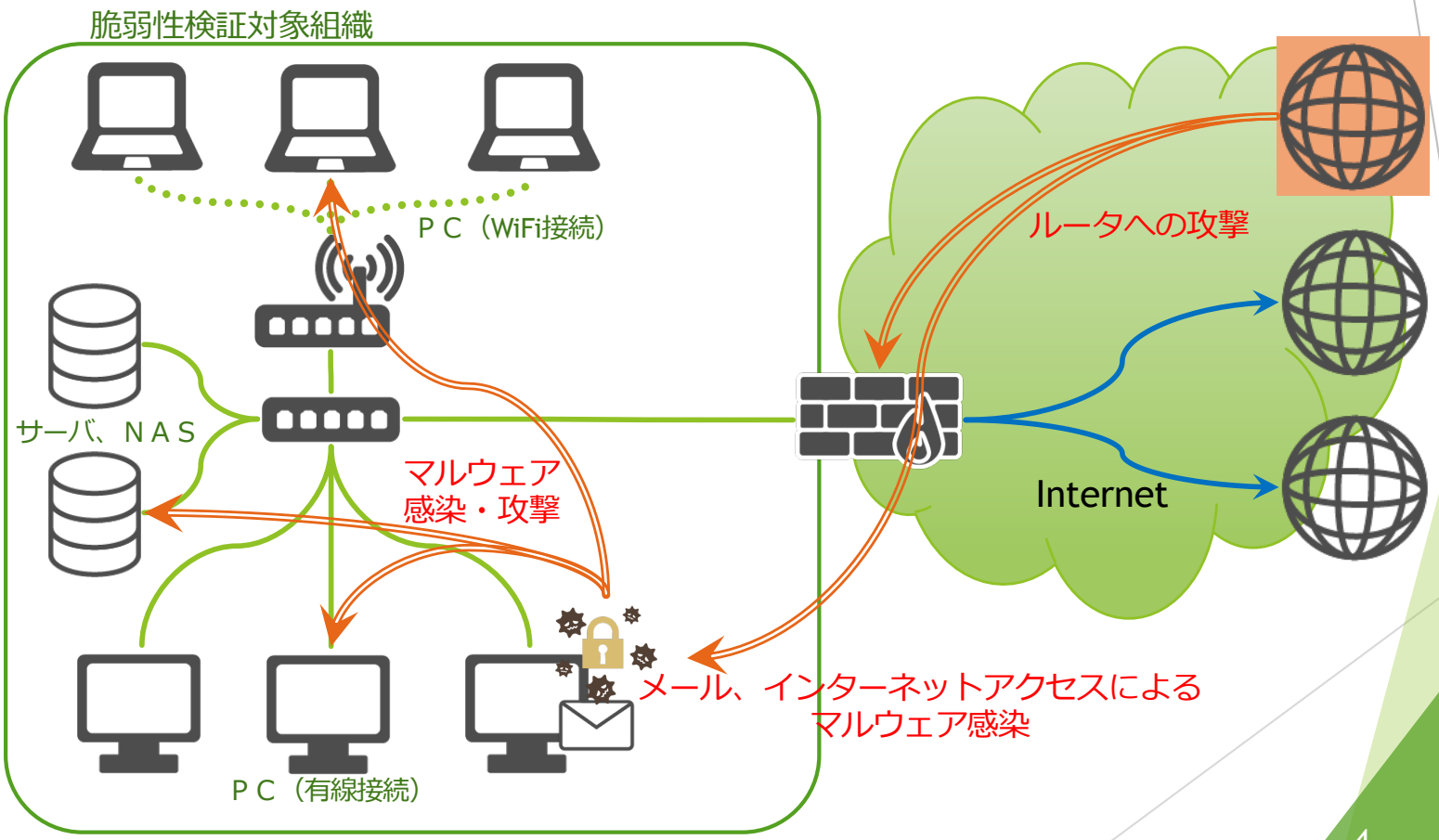
SYNCHRO®
CSCC
Cyber Security Countermeasures Center

実現方法
手順 と 技術的概要

- 手順
  - 事業者さまから「ネットワーク脆弱性診断」のご依頼を頂く
  - SYNCHROから脆弱性診断用デバイスを送付
    - KATABAMI VDP（以下、K.VDP） と managed L2SW
  - 事業者さまが受け取った脆弱性診断用デバイスをネットワークに接続
    - K.VDPはDHCP参照でローカルアドレスを取得
    - 対象ネットワークのインターネット接続を利用しセンタに自動接続
    - 作業員が訪問しての設置・設定作業は不要
- 技術的概要
  - K.VDP = Kali Linux + KATABAMI
    - Kali Linux は診断用のツールを満載した専用OS
    - KATABAMI は SYNCHRO のゼロトラストネットワークアクセス用ツール
  - Kali Linux 上のツールが内側からネットワークを診断
  - Managed L2SW がネットワークを流れるパケットをモニタしK.VDPが収集
  - 診断結果、パケットキャプチャデータはK.VDPが安全にセンタに伝送

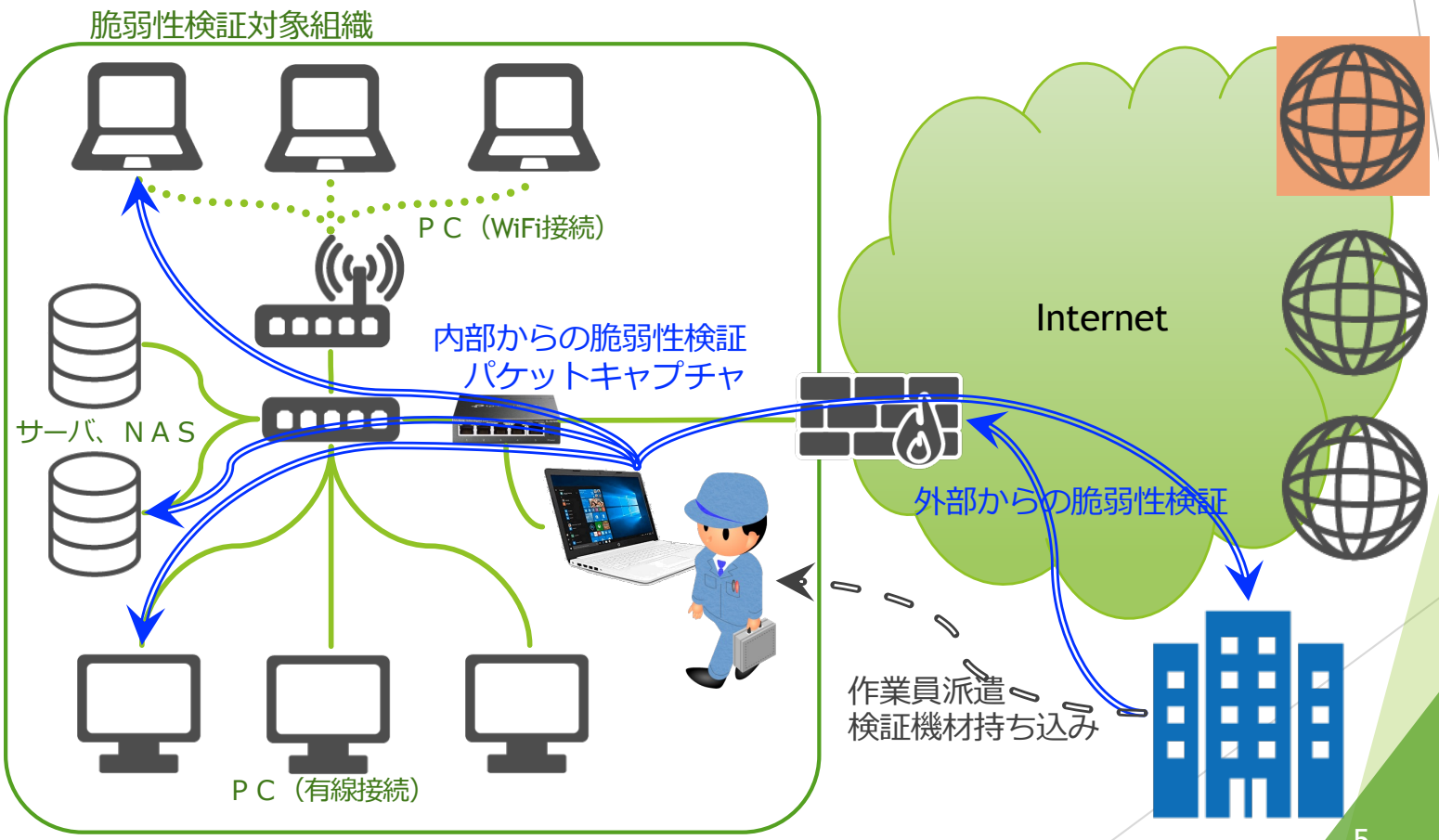
SYNCHRO®
CSCC
Cyber Security Countermeasures Center

組織へのサイバー攻撃



SYNCHRO
CSCC
Cyber Security
Countermeasures
Center

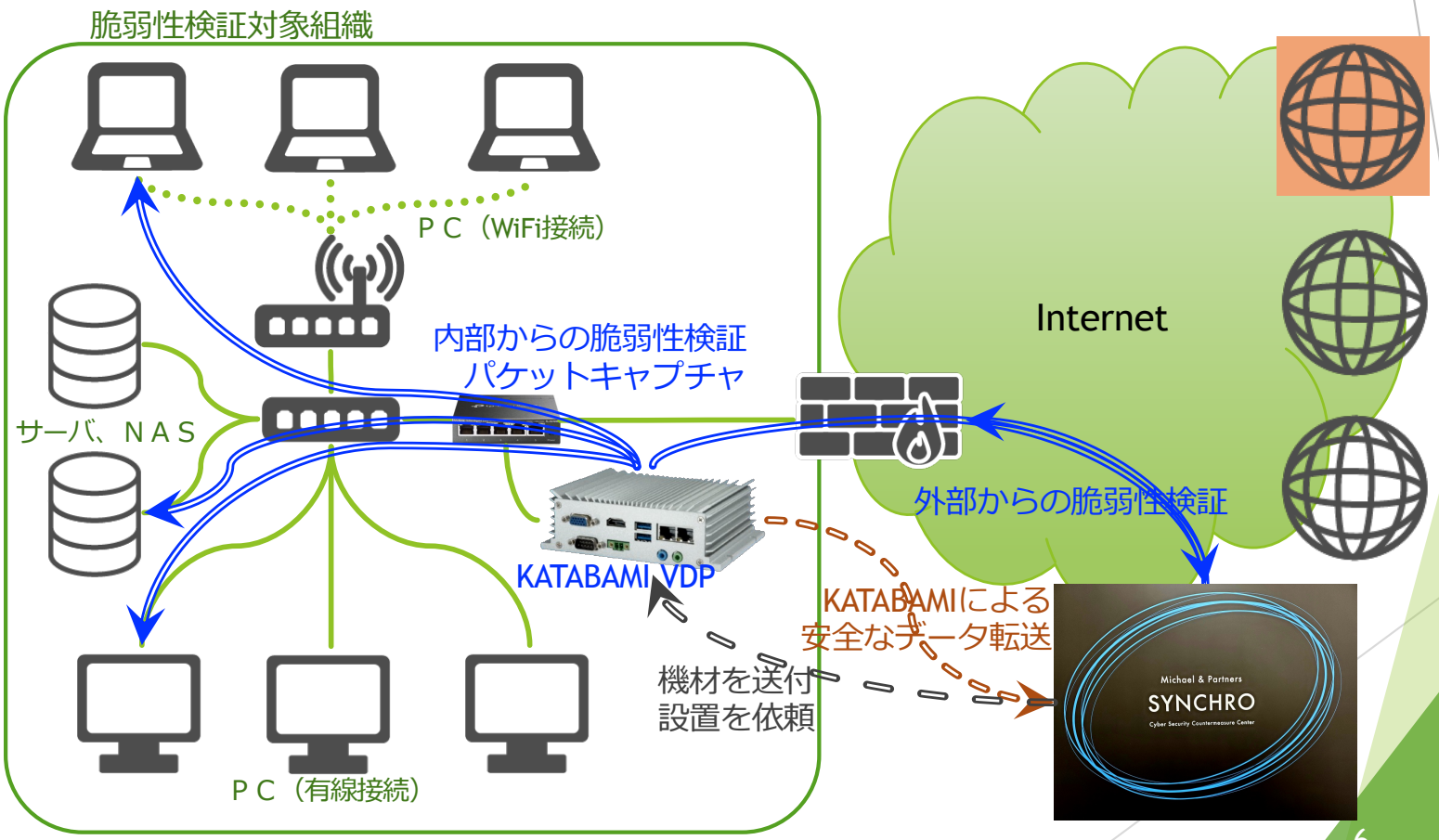
一般的な組織対象の脆弱性診断



SYNCHRO
CSCC
Cyber Security Countermeasures Center

SYNCHROの組織対象の脆弱性診断

機器設置→人員派遣ナシ、持続的検証可能



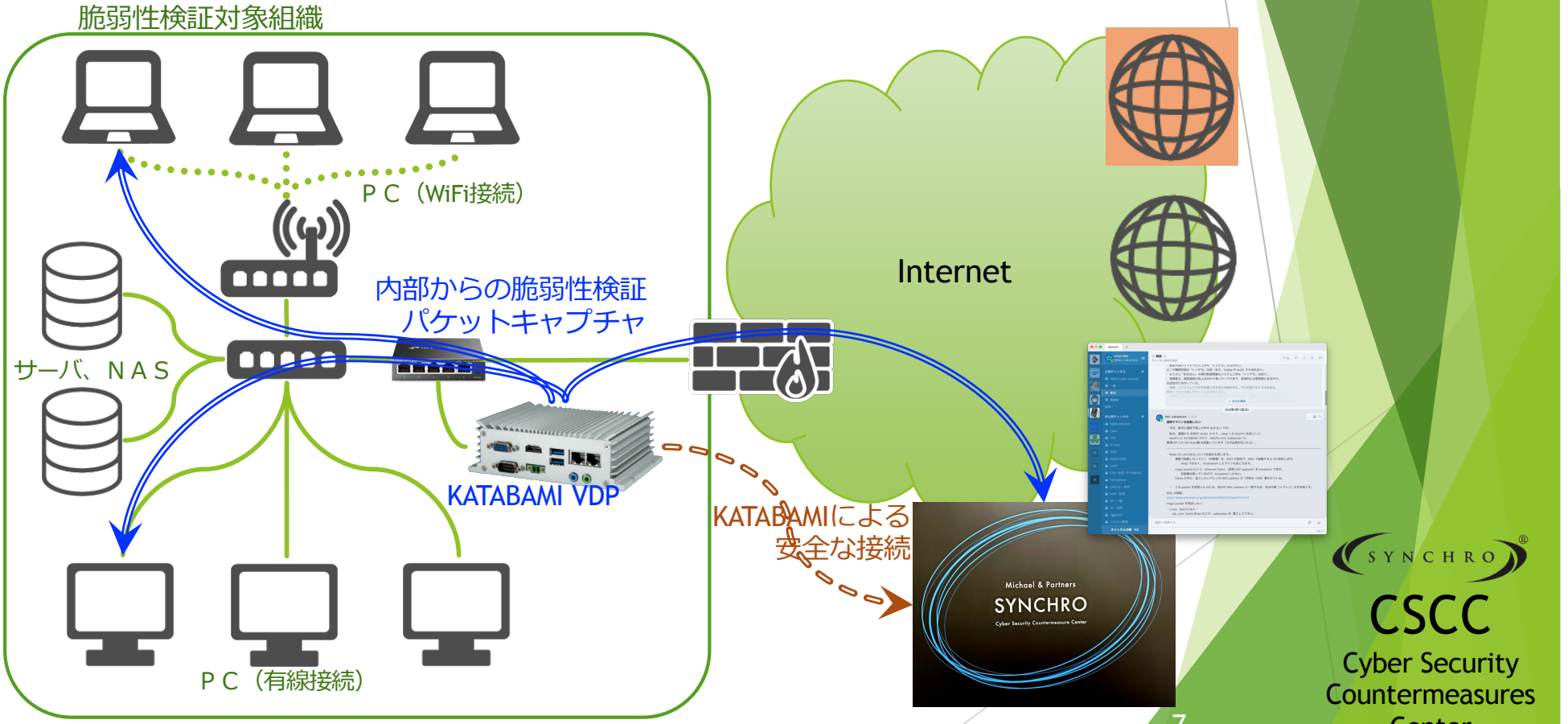
SYNCHRO®

CSCC

Cyber Security Countermeasures Center

SYNCHROの組織対象の脆弱性診断

情報連携は KATABAMI Chat で
暗号化は不要、インターネット経由でも安全



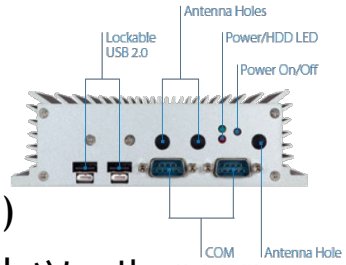
SYNCHRO
CSCC
Cyber Security
Countermeasures
Center

KATABAMI VDP

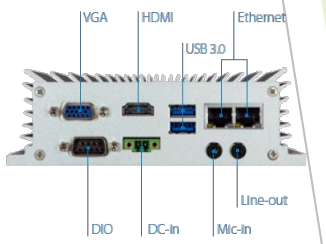
KATABAMI Vulnerability Diagnosis Probe

- KATABAMI VDP の 特徴
  - 充実した脆弱性診断ツール
    - Kali Linux (Every Thing Version)
    - 約600のペネトレーションテストツール
  - 高いセキュリティ性能
    - センタとの通信はKATABAMI
    - ゼロトラストネットワークアクセス
    - 既存のネットワークへの影響ナシ
  - 安定稼働
    - ファンレスで長期運用も可能。静音
  - 小型で設置が容易
    - 約150 x 110 x 50

Front Panel External I/O



Back Panel External I/O



基本仕様

動作環境条件	温度条件: -20~+60°C 湿度条件: 0~95%RH(結露なきこと)
保存環境条件	温度条件: -20~+70°C 湿度条件: 0~95%RH(結露なきこと)
電源	AC100Vアダプタ (DC-IN 9~36V, typ.19W)
外形寸法	150.5 x 109.8 x 48.1mm
重量	1.4kg(本体のみ)
同梱物	本体、ACアダプタ
各種取得規格	VCCI Class-?、FCC Class B、CCC、CE、 RoHS指令(EU)2015/863

インターフェース仕様

有線LANインタフェース	RJ-45:×2 10Base-T / 100Base-TX / 1000Base-T(自動認識)
ディスプレイ	HDMI x 1, VGA x 1
オーディオ	Mic-In x 1, Line-Out x 1
デバイスインタフェース	USB:×4(USB3.0 x 2, USB2.0 x 2 Type-A) シリアル:×2(DSub9, RS-232/422/485)
DIO	8 bits GPIO
スイッチ	プッシュスイッチ:×1
LED	POWER x 1, HDD/SSD x 1

SYNCHRO®

CSCC

Cyber Security Countermeasures Center

KATABAMI Chat
Slack clone を使って 協働の効率向上 を図る

- KATABAMI Chat の 特徴
  - 高いセキュリティ
    - 自社サーバ で 運用可能
      - 機密情報を社外に出さない
    - サーバと通信は KATABAMI で 完全防御
  - 使い易さ
    - 機能、操作性は Slack と同様
      - ∵ Slack clone (OSS) が base
    - 社外（パートナ）との連携も可能
  - クライアント動作環境 (Chrome base)
    - Windows10, MacOS
    - Android, iOS, Debian, Raspberry Pi OS
    - Ubuntu, RHEL/CentOS

Countermeasures
Center