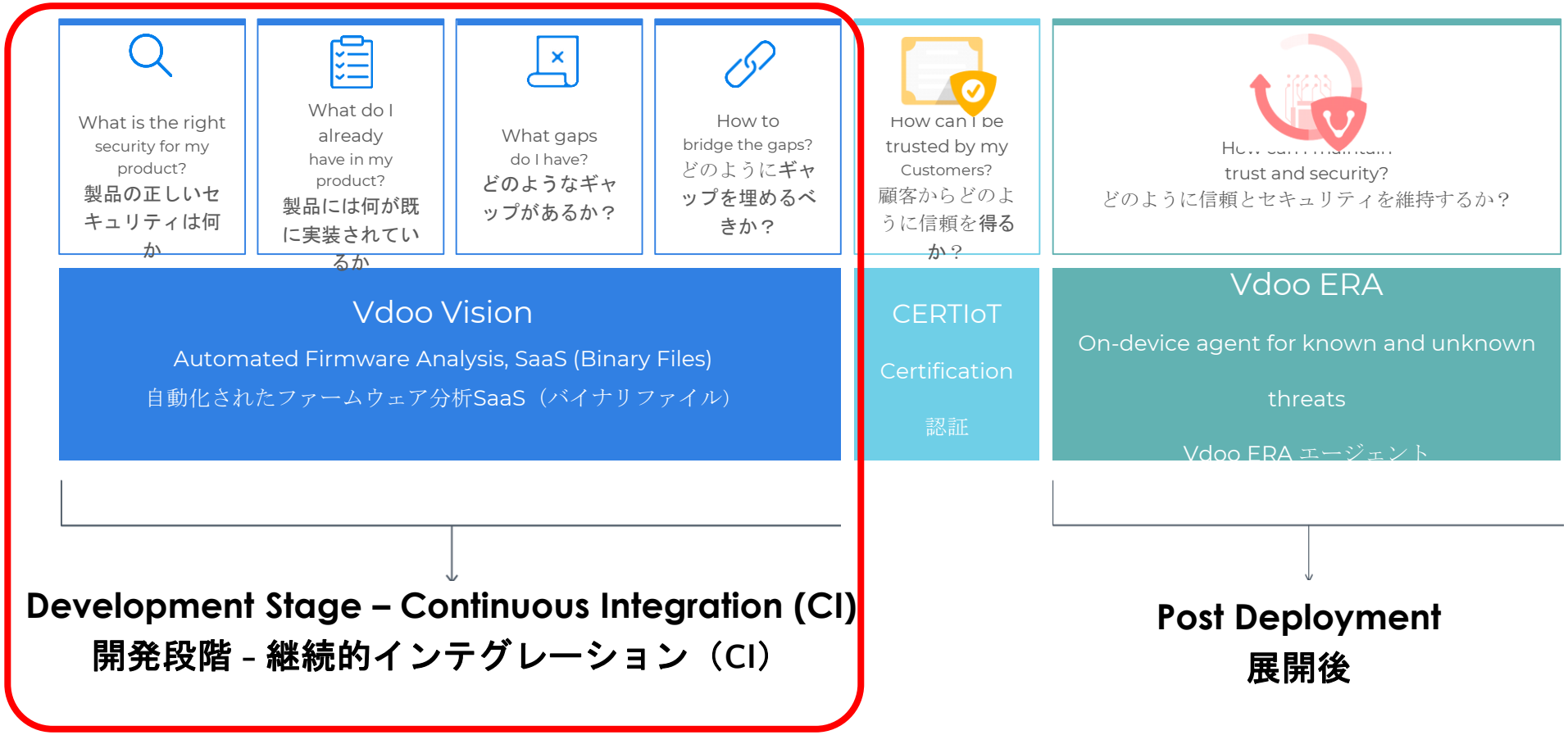
# FW脆弱性検査「Vdoo Vision」
# 「脆弱性対策クイックレポートサービス」のご紹介

# 開発段階：Vdoo Vision

## 開発段階で脆弱性を解析し、サイバー攻撃に対する セキュリティソリューションを提供します。

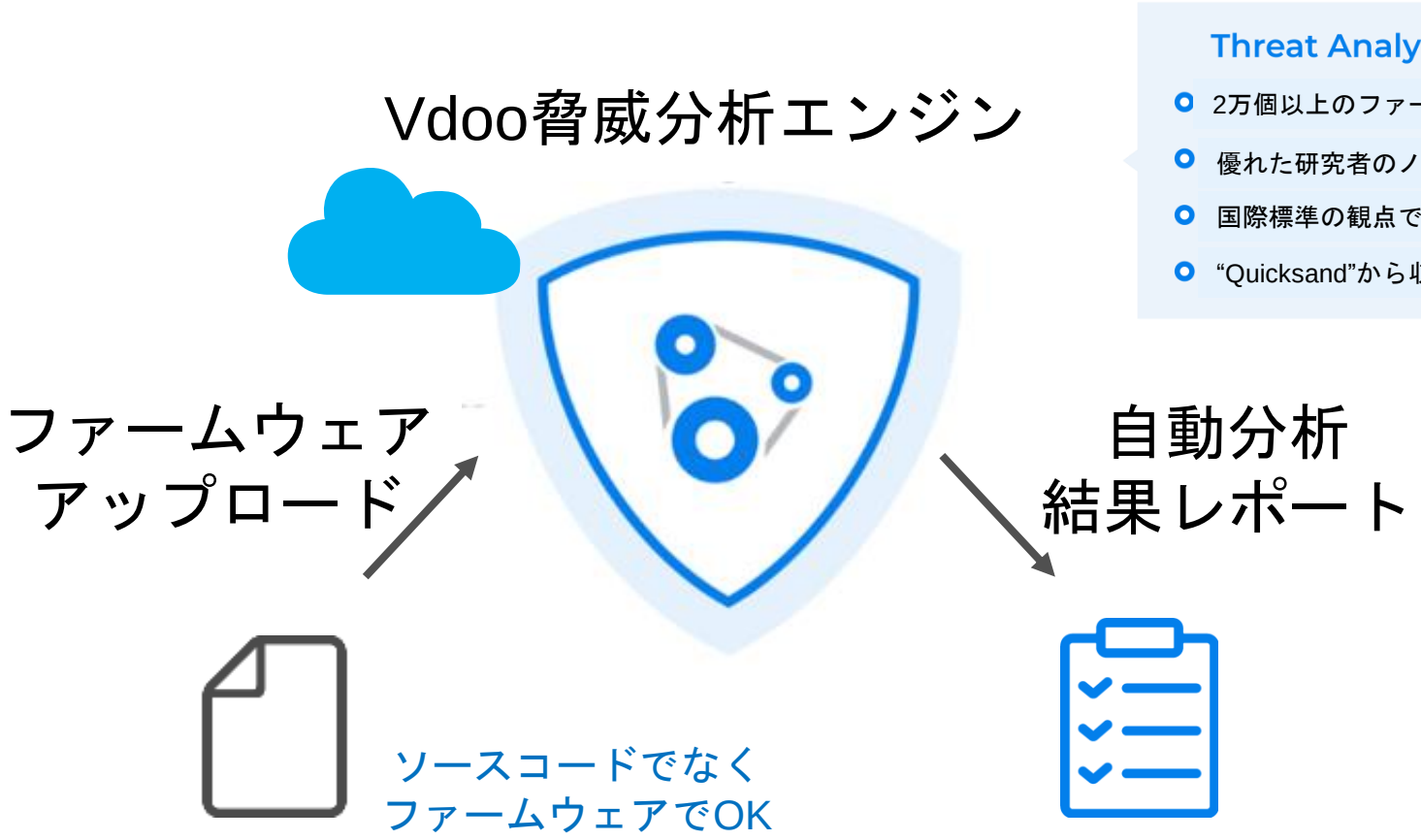





公開

# Vdoo Vision概要

IoTデバイスのファームウェアをSaaSにアップロードすると、
自動的に分析し、レポートを提出します。




**Threat Analysis Engine**

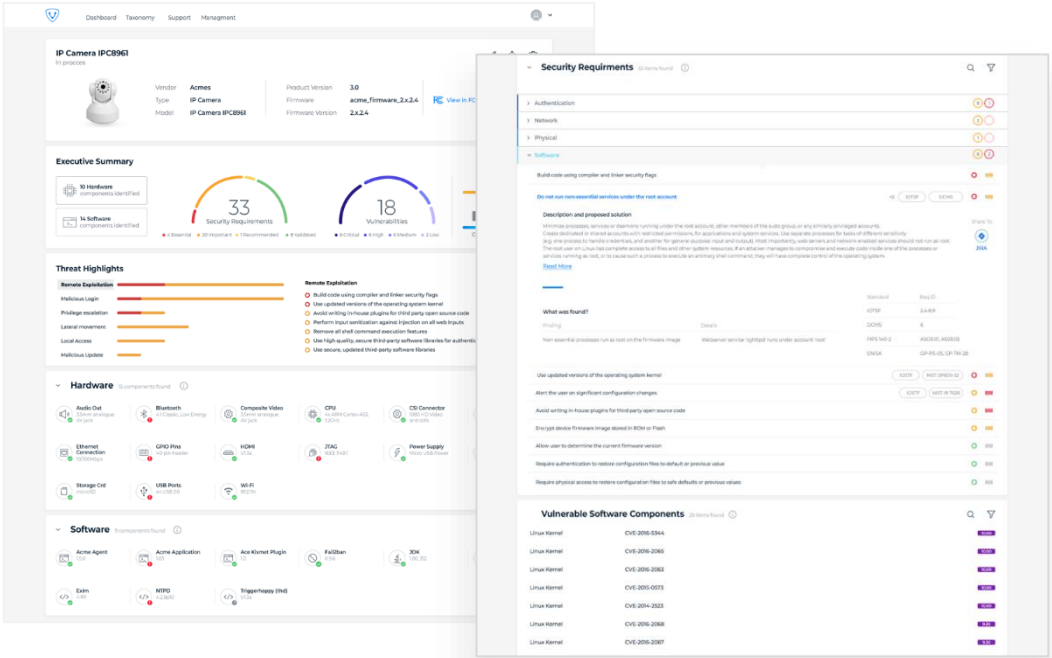
- 2万個以上のファームウェアデータの実績
- 優れた研究者のノウハウ
- 国際標準の観点で評価
- “Quicksand”から収集した情報

# Vdoo Vision 分析レポート(例)

レポートのガイダンスに提示された項目を改善していくことで、
漏れなくセキュリティ対策を実現できます。

## CCDS・NIST等の基準に準拠

- ベンダーダッシュボード
- エグゼクティブサマリ
- リスクアセスメント
- ハードウェア構成品リスト
- ソフトウェア構成品リスト
- 詳細なガイダンス
- CI/CDとの統合




- Security Essentials の欠如
- 欠陥のあるセキュリティ・アーキテクチャ
- 望ましくないプロセスとサービス
- 間違った構成
- バックドアと組み込みの認証鍵が残っている状態を指摘
- サードパーティモジュールの既知の脆弱性
- 追加の疑わしい脆弱性

ファームウェア分析結果レポートには、
- どのような攻撃要因があるのか
- 何に取り組むべきなのか
- 各国・地域の規格・基準に準拠しているか

等の改善リストに優先順位を付けて、その解決に向けたガイダンスを提示します。

# IoT脆弱性診断サービスの必要性

日々進化し複雑化していくサイバーセキュリティ対策要件
HWに対する要件も増えてきております。企画・設計する前に現状把握することが第一歩。
対象となる規格要件に対するGAP分析及び対処方法についてレポート提供します。

＜主な報告内容＞

- リスクエリアの特定と、デバイス特有の詳細ガイドラインによる修正方法を優先付け
- 詳細なデバイス バイナリ分析で既知の脆弱性やゼロデイ脆弱性の可能性を検知
- サプライヤに依存せずにサードパーティ製品やコンポーネントの脆弱性をアセスメント

# 脆弱性対策クイックレポートサービス

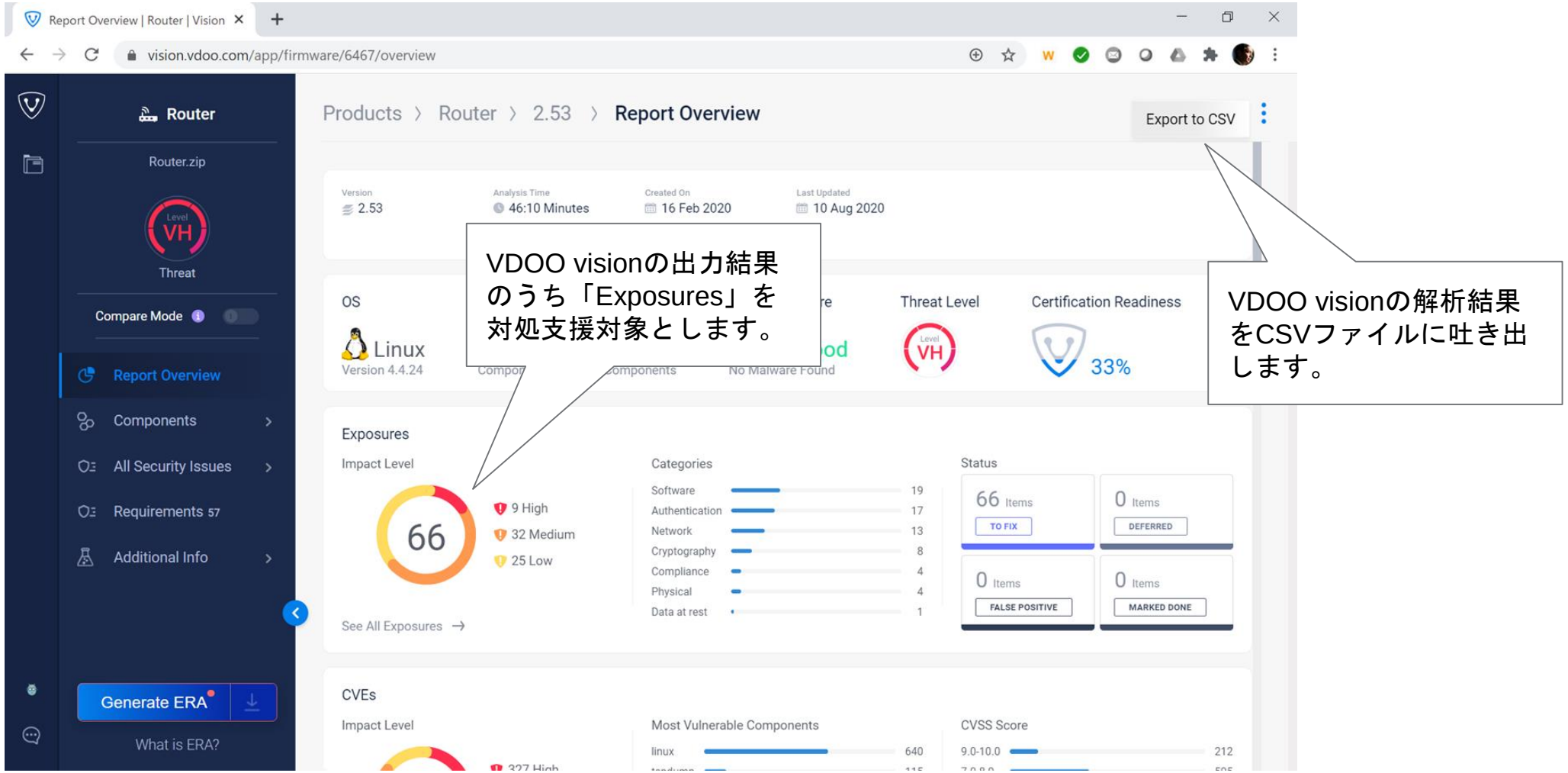
- サービス内容
  - ➢ Vdooでバイナリ診断を適用した際に出力されるリポートに対して、対処策の分類をします。
  - ➢ 対策を進めるうえで一般的な機器に求められる必要最小限な対策に絞り込んだアドバイスを診断実施から約二週間で提示します。
  - ➢ 対処策の分類のうち、Yoctoでの対応が可能と判断した場合にYoctoレシピもしくはコンフィグレーションでの対応策を提示します。

- サービスを受けるために必要な情報
  - ➢ Vdooでのバイナリ診断結果
  - ➢ Vdooが表示する「What should I do？」リポート

- 本サービスによる効果
  - ➢ Vdooの「What should I do？」リポートでは個別の対処策を提示していますが、これをYoctoレシピもしくはコンフィグレーションに適用することで、プロダクトのセキュリティ対策を継続的に適用することができ、さらに他プロジェクトへの転用も可能となります。

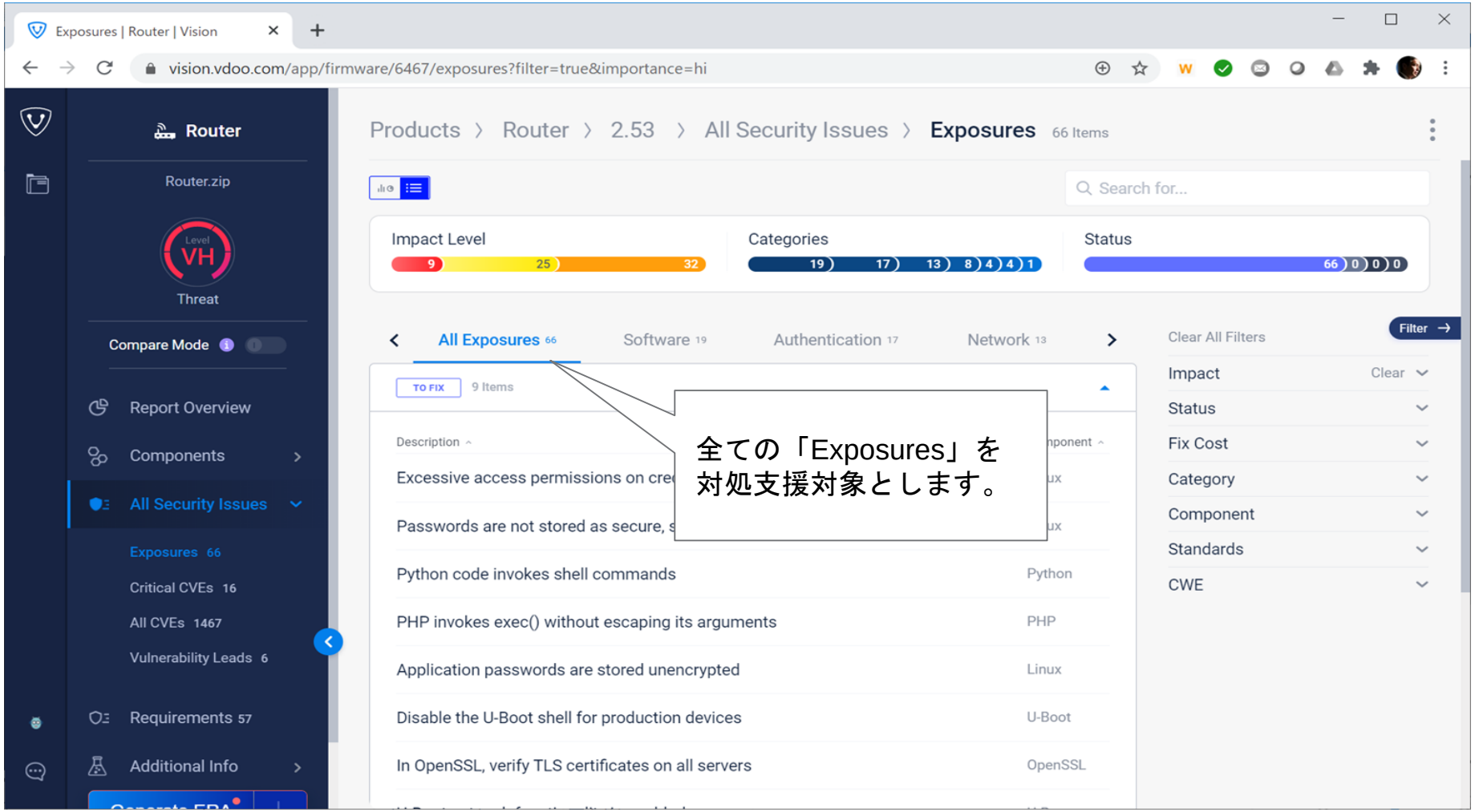
- Visionライセンス料＋時間単位でのご契約方式となります。

# 脆弱性対策クイックレポートサービスイメージ 1/4



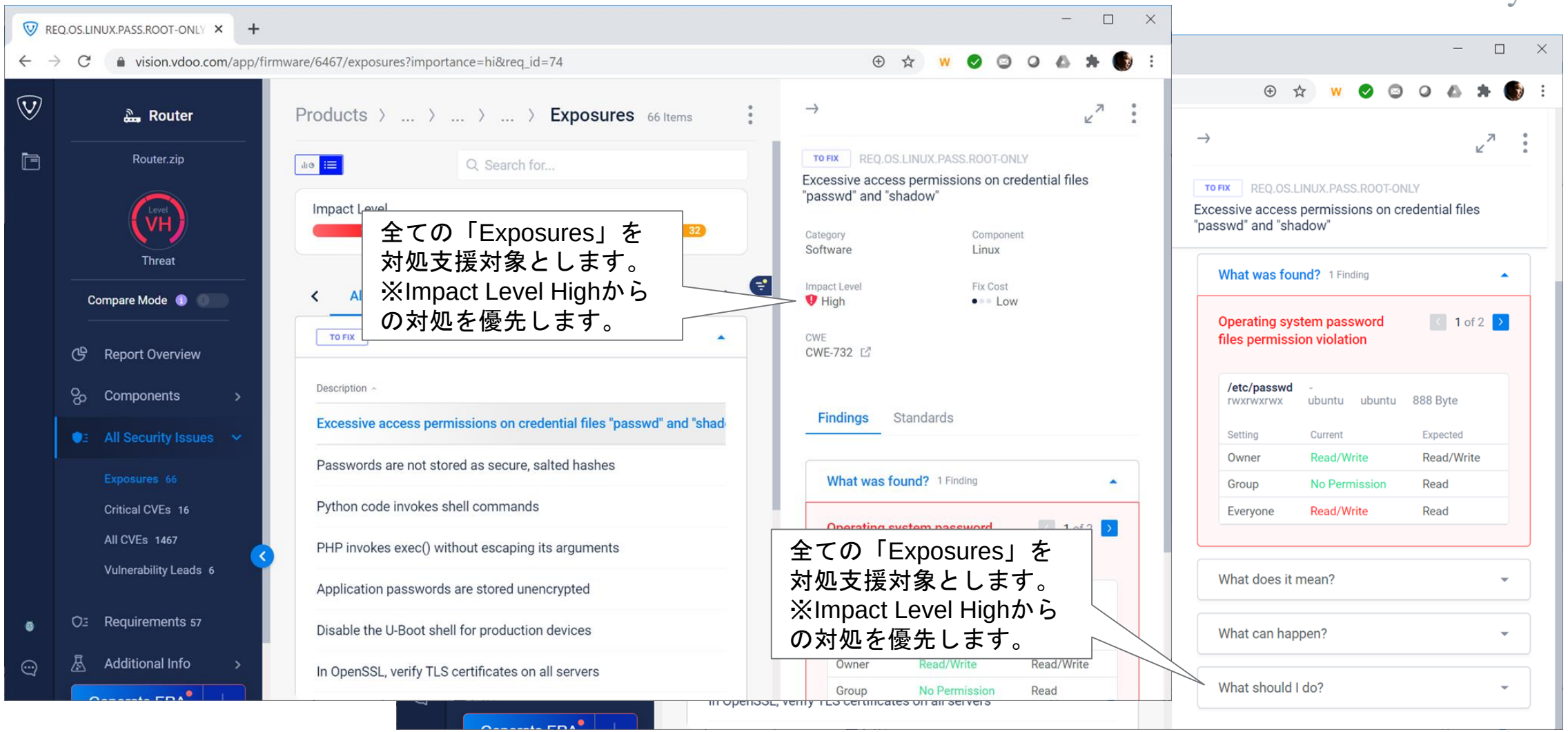

Vdoo vision のOverviewリポート

# 脆弱性対策クイックレポートサービスイメージ 2/4




Vdoo vision のExposuresリポート

# 脆弱性対策クイックレポートサービスイメージ 3/4

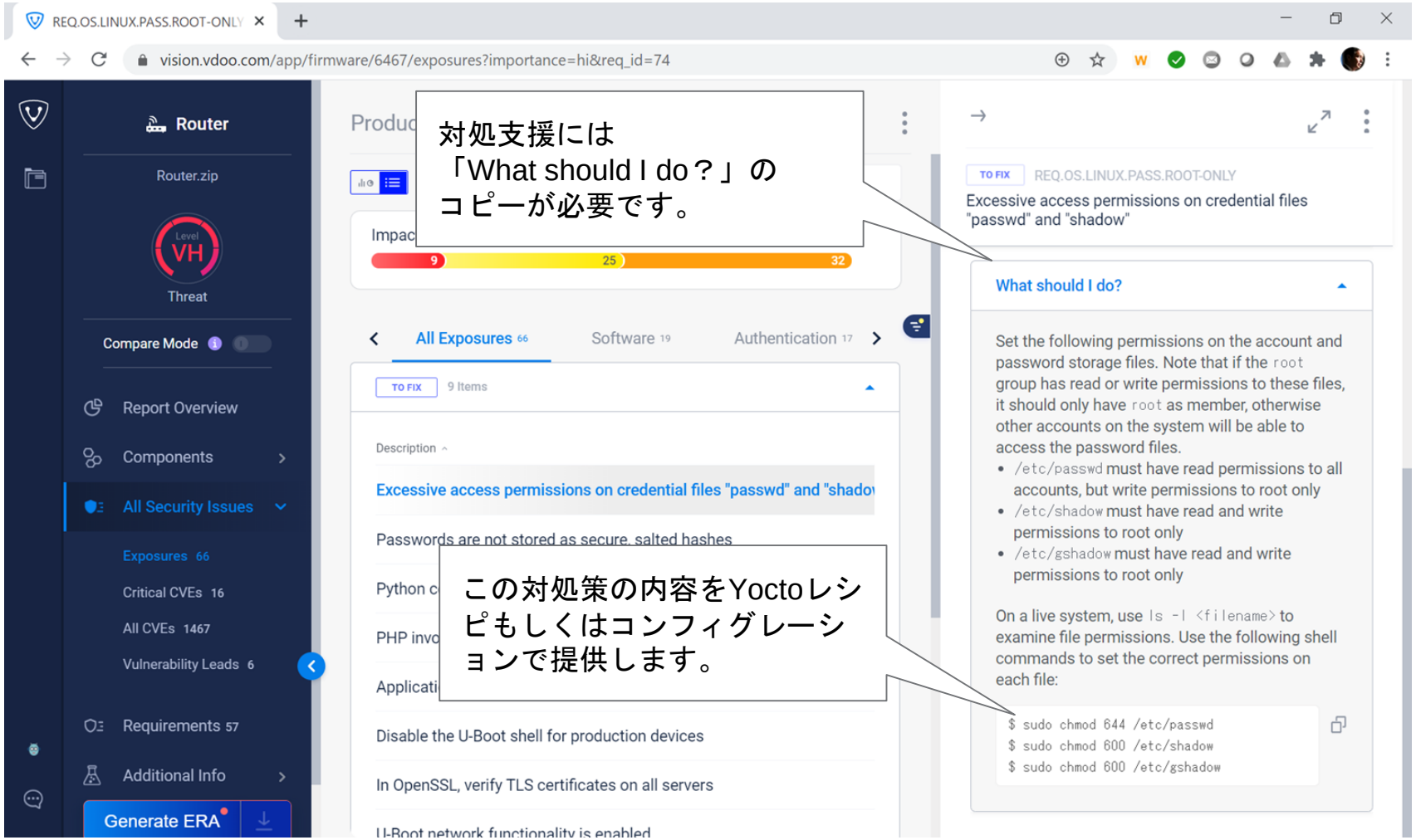



Vdoo vision のExposuresリポート



公開

# 脆弱性対策クイックレポートサービスイメージ 4/4




Vdoo vision のExposuresリポート



公開

# 対処策例

[課題]

Operating system password files permission violation

[対策]

ユーザレシピ内でイメージ作成後の処理コマンドとして、以下を設定します。

```
$ cat repos/meta-user/recipes-images/images/core-image-minimal.bbappend
ROOTFS_POSTPROCESS_COMMAND += "set_shadow_files_permission; "
set_shadow_files_permission () {
   chmod 644 ${IMAGE_ROOTFS}/etc/shadow
   chmod 600 ${IMAGE_ROOTFS}/etc/gshadow
   chmod 600 ${IMAGE_ROOTFS}/etc/passwd
}
```

[備考]

この設定により、起動イメージ作成時に適切なパーミッションが設定されます。この設定はライブラリのバージョンによる影響を受けません。ただし、OSのメジャーバージョンが変更になった場合には、ファイル構成の変更などへの対応が必要となります。

# お問い合わせはこちら

サイバートラスト株式会社
IoT 総合お問い合わせ窓口

iot-contact@cybertrust.co.jp


# 信頼とともに

## 留意事項