ランサムウェア・標的型攻撃を中心とした サイバーセキュリティ最新動向と対策

F-Secure

Shinichiro Kawano
Corporate Sales
F-Secure K.K.
Shinichiro.Kawano@f-secure.com

F-SECURE IN SHORT

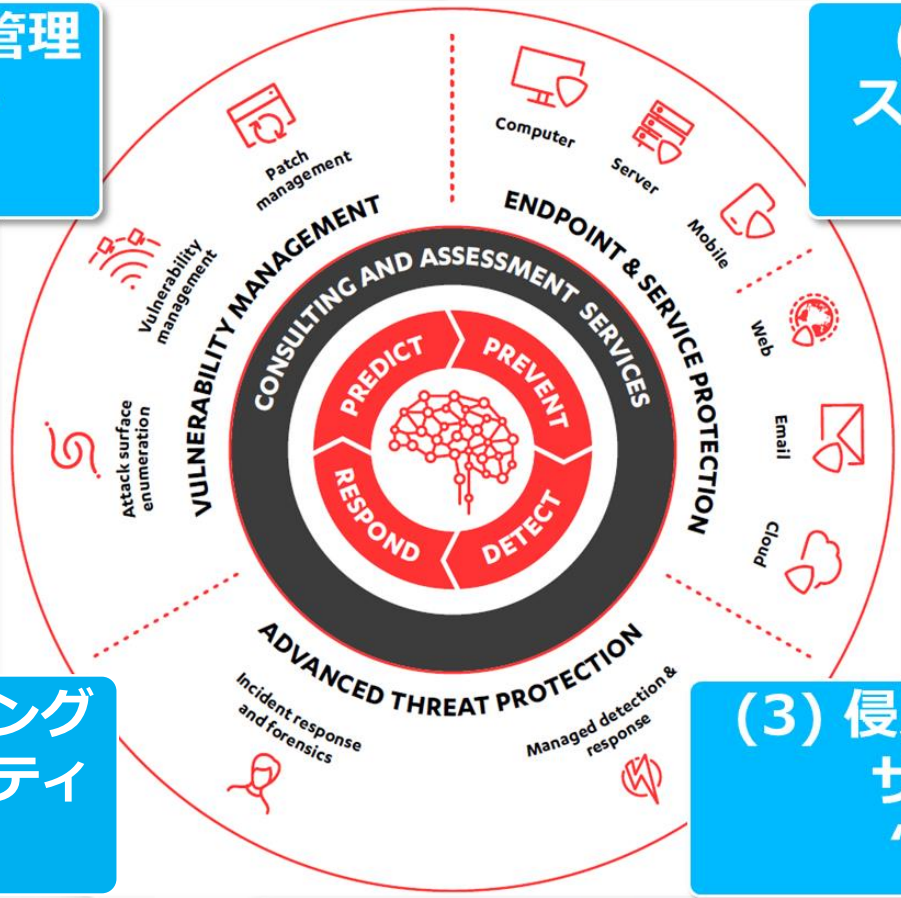
F-Secure

- 1988年に設立
- 世界25か国、社員数　約1100人
- 2016年収益$170million
- ヘルシンキのNASDAQ　OMXに上場
- 100ヵ国でビジネスを展開し、オペレーター数200以上、リセラー数1000以上
- 世界中でコーポレートカスタマー数100,000以上
- ヨーロッパでサイバークライムインシデントが起こった際の調査機関として史上最多の依頼数
- 過去6年間で5回のAVテスト最優秀保護賞を受賞した唯一の企業

F-Secure.

(2) 脆弱性診断・管理
ソリューション
“Radar”

(1) PC, Server
スマートフォン向け
アンチウイルス



(4) レッドチーミング
サイバーセキュリティ
コンサルティング

(3) 侵入対応・検出
サービス
“RDS”

F-Secureは
サイバーセキュリティ コンサルを含む
トータルサービスをご提供可能

F-Secure

本日ご説明のアジェンダ

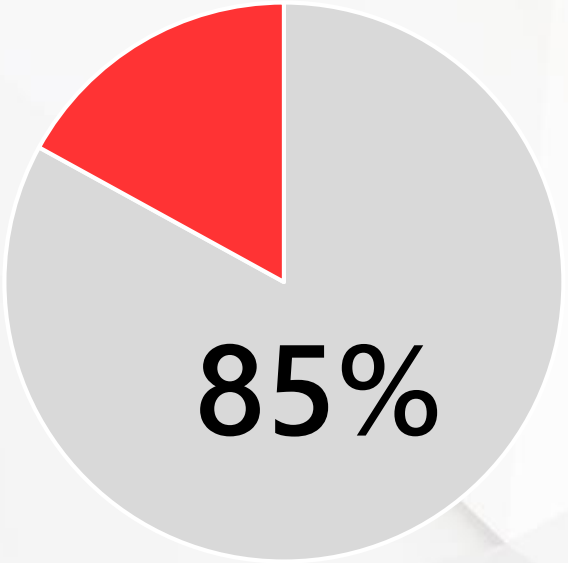
1. F-Secure セキュリティレポート 最新情報アップデート (配布資料)
2. ランサムウェア・標的型攻撃と セキュリティアップデートの重要性 (デモ)
3. 更に強化したセキュリティ対策 侵入検出

1. F-Secure セキュリティレポート 最新情報アップデート

2. ランサムウェア・標的型攻撃と セキュリティアップデートの重要性、対策

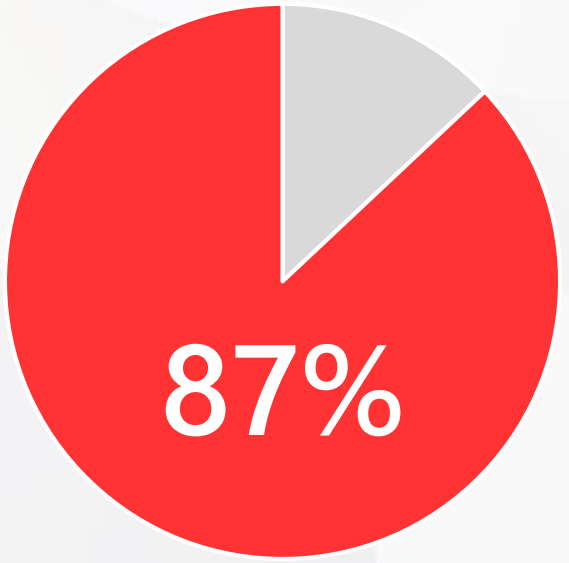
F-Secure.

脆弱性管理をしていない ソフトウエアがセキュリティリスク



TOP10攻撃の85%は
ソフトウェアアップデートで
防止可能

ところが



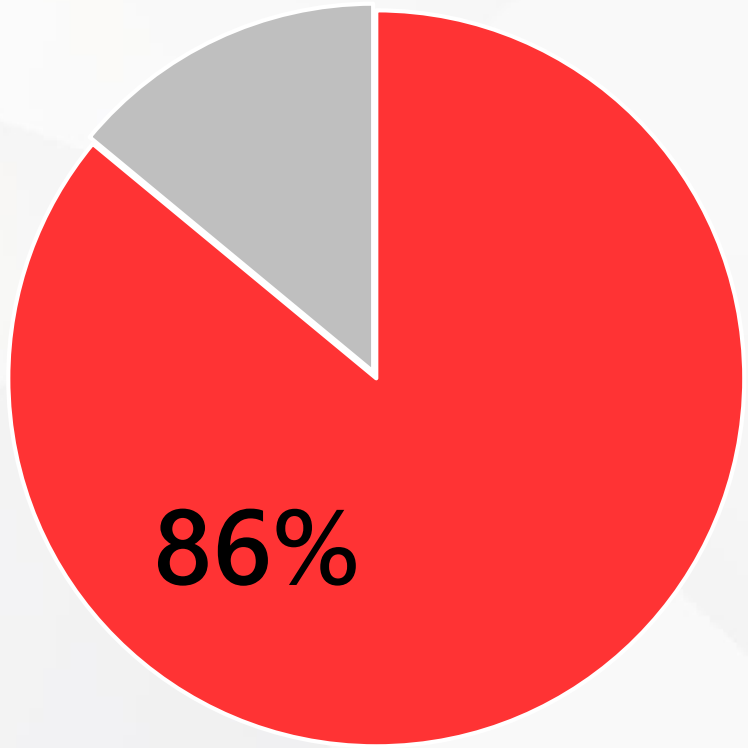
87%の企業が重要な
アップデートを未実施

Source: HP2016 Cyber Risk Report

F-Secure.

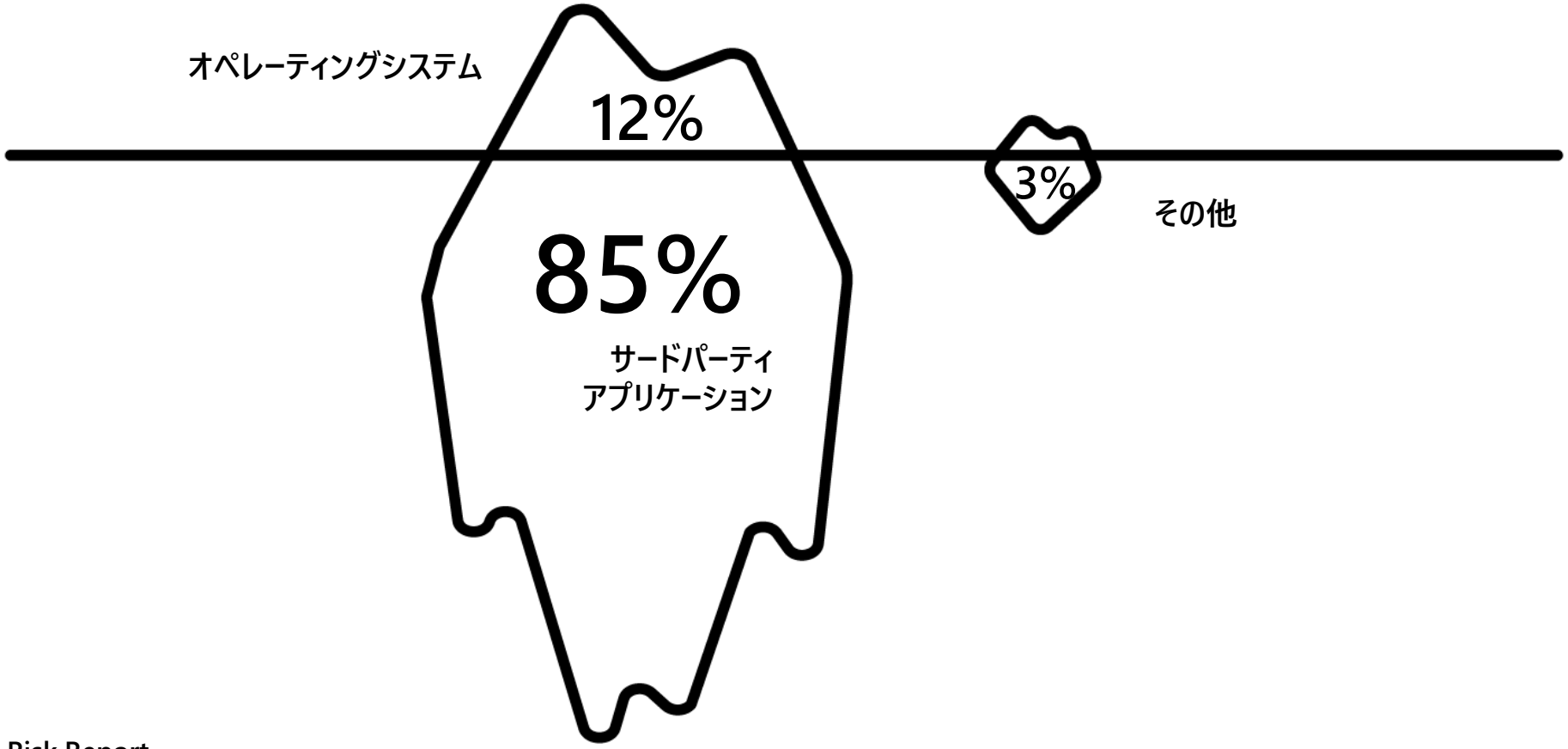
86%

重大なセキュリティの問題を抱えているWEBアプリケーション



Source: HP2016 Cyber Risk Report

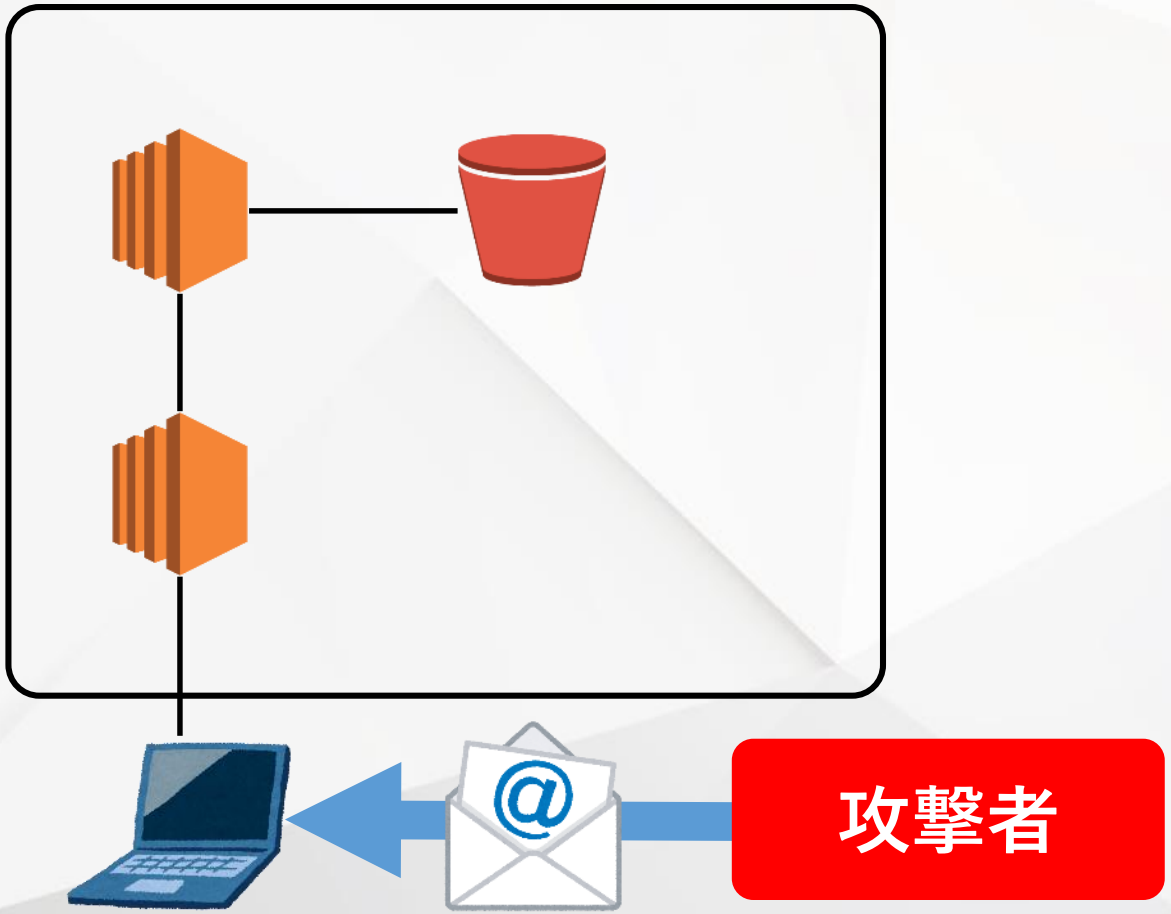
OSのパッチ管理だけでは
不十分



Source: HP2016 Cyber Risk Report

F-Secure.

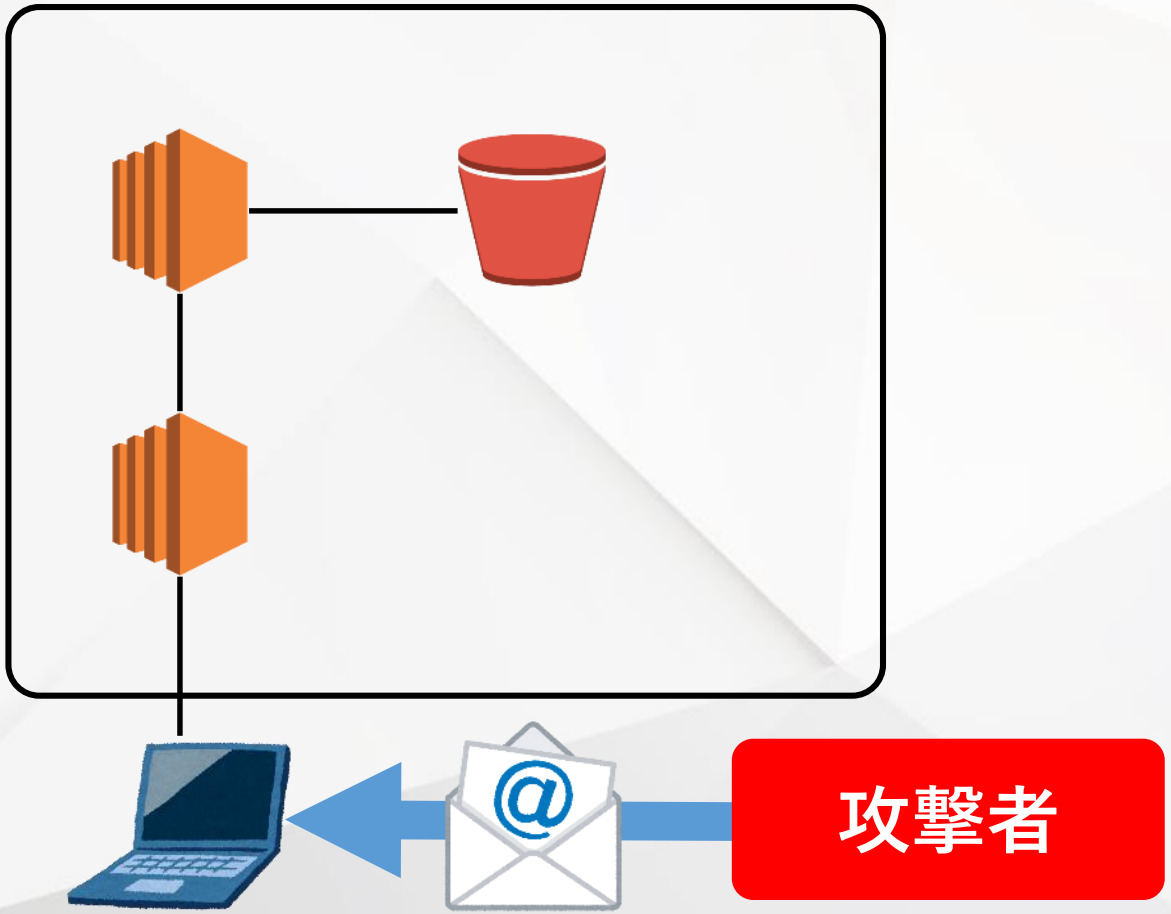
脆弱性を突いた攻撃、所要時間は？



1. 1時間半
2. 15分30秒
3. 5分30秒

F-Secure

脆弱性を突いた攻撃、所要時間は？



1. 1時間半
2. 15分30秒
3. 5分30秒

※ F-Secure エンジニアによる 検証環境デモ実施時参考値

F-Secure

デモンストレーション

F-Secure.

ランサムウェア・標的型攻撃のまとめ

1. 2016年以降、ランサムウェアの被害は急増
   →攻撃者側

2. 万が一に備えた対策

   - バックアップ（自社内、サーバ、クラウド、）
   - ランサムウェア対策ソフトウェアおよび設定
   - OSおよびアプリケーションのアップデート
   - 24時間365日 の監視サービス

F-Secure.

F-SECURE のご提供サービス

1. OS, アプリケーション, ネットワークの脆弱性診断 “F-Secure Radar”

2. サンドボックス機能を含むアンチウイルス

3. 高度な標的型攻撃 (ATP) 対策およびセキュリティコンサルティング

F-SECURE RADARとは

■企業ネットワーク内の脆弱性管理ソリューション
3種類のスキャン技術でネットワーク内の脆弱性を検査

- Discovery Scan：
  ネットワーク全体のマッピング
- System Scan：
  システム構成不備、OS及びアプリケーションの脆弱性
- Web Scan：
  Webアプリケーションの脆弱性

1.3. Current system health

1.3.1. Top 10 most vulnerable targets

Target	Platform Scan Findings		
	High	Medium	Low
Lee Cisco 1721	56	18	1
Vita Ubuntu Linux	30	63	18
McCarthur Cisco 1242	29	11	0
Barney Windows 2003	26	61	3
Fred Fedora Linux	10	23	5
Diaz Windows 2008	10	23	
Pebbles Ubuntu Linux	6	11	
Betty Windows 2003	2	16	
Hoppy CentOS Linux	2	13	
Patton Windows 2008	2	10	

1.3.2. Top 3 most frequent high/medium risk vulnerabilities

Platform Scan	
Vulnerability instance	
HTTP Response Date is not Synchronised	
Cisco IOS Software Crafted TCP Packet Denial of Service Vulnerability	
Guessable SSH User Login and Password	
Management protocol detected	
Database service exposed	
SSL certificate is not valid	

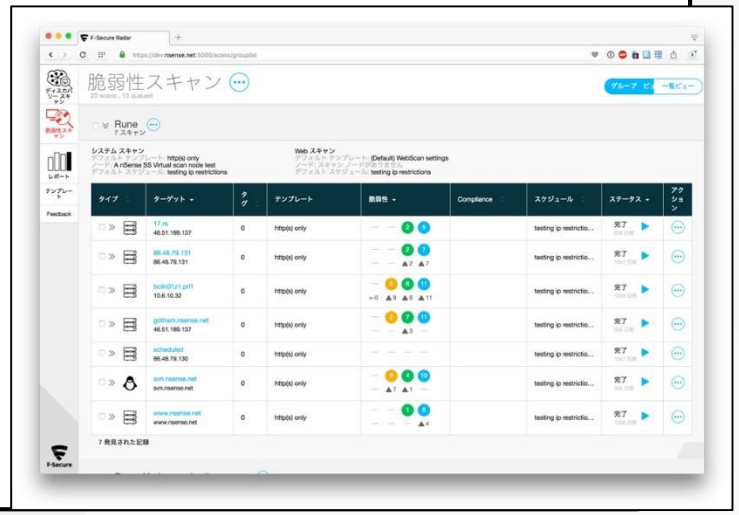
F-Secure

F-Secure Radar で診断できる脆弱性

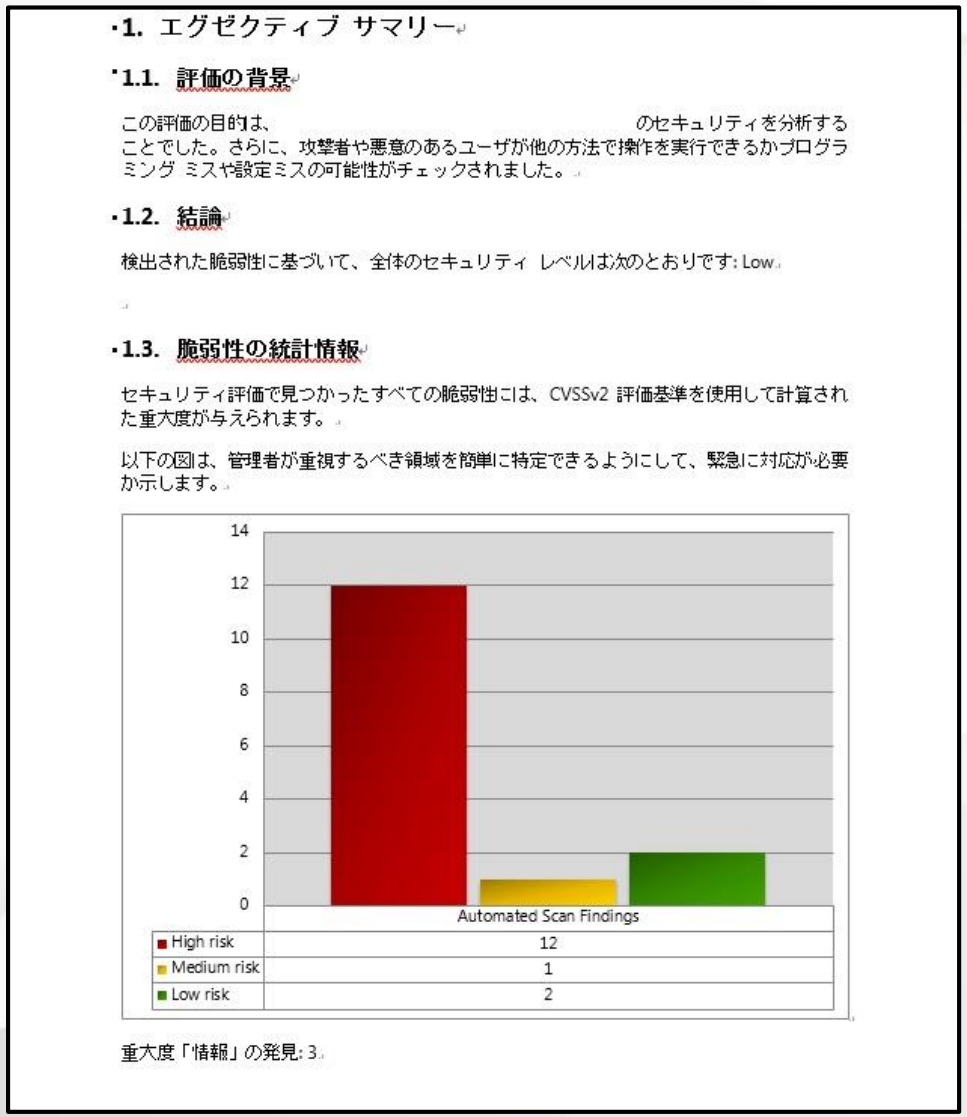
1. ディスカバリースキャン
   -> ネットワーク全体をポートスキャン

2. システムスキャン
   -> OS, Appli セキュリティパッチ, 構成情報

3. Web スキャン
   -> クロスサイト
   スクリプティング
   SQLインジェクションetc..



脆弱性診断レポート例



1. エグゼクティブ サマリー

1.1. 評価の背景

この評価の目的は、　　のセキュリティを分析することでした。さらに、攻撃者や悪意のあるユーザが他の方法で操作を実行できるかプログラミング ミスや設定ミスの可能性がチェックされました。

1.2. 結論

検出された脆弱性に基づいて、全体のセキュリティ レベルは次のとおりです: Low

1.3. 脆弱性の統計情報

セキュリティ評価で見つかったすべての脆弱性には、CVSSv2 評価基準を使用して計算された重大度が与えられます。

以下の図は、管理者が重視するべき領域を簡単に特定できるようにして、緊急に対応が必要か示します。

重大度「情報」の発見: 3

特長

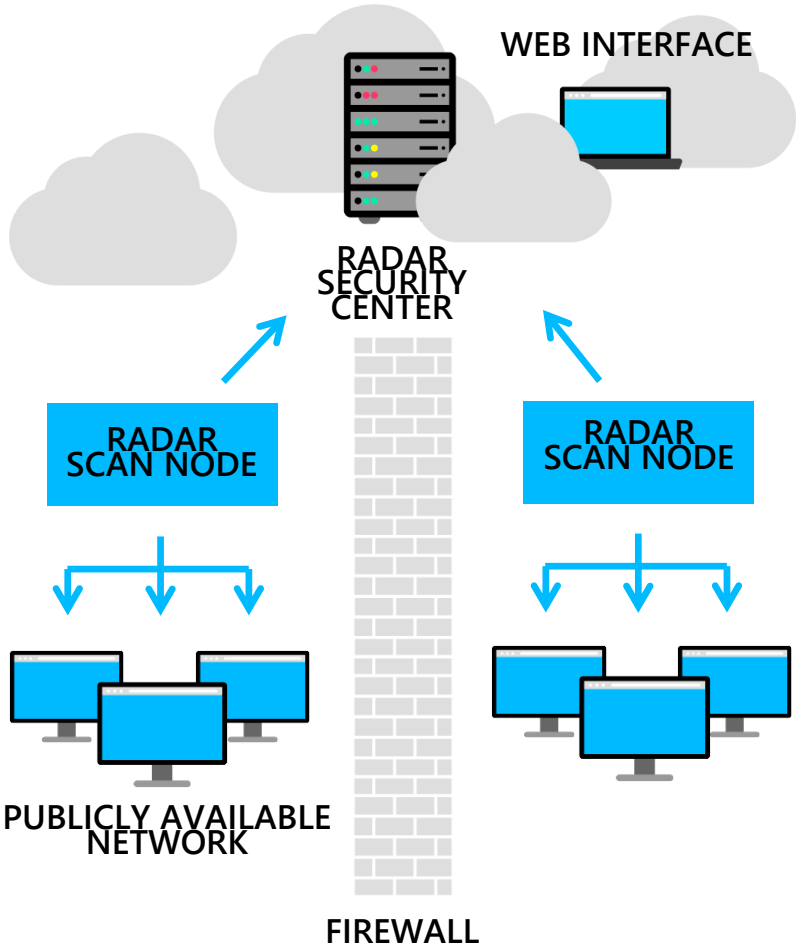
1.スキャン対象一括レポート

(2) ネットワーク, OS/アプリ, Web 脆弱性を網羅

→必要な脆弱性を可視化

脆弱性診断 (1) クラウド型スキャン

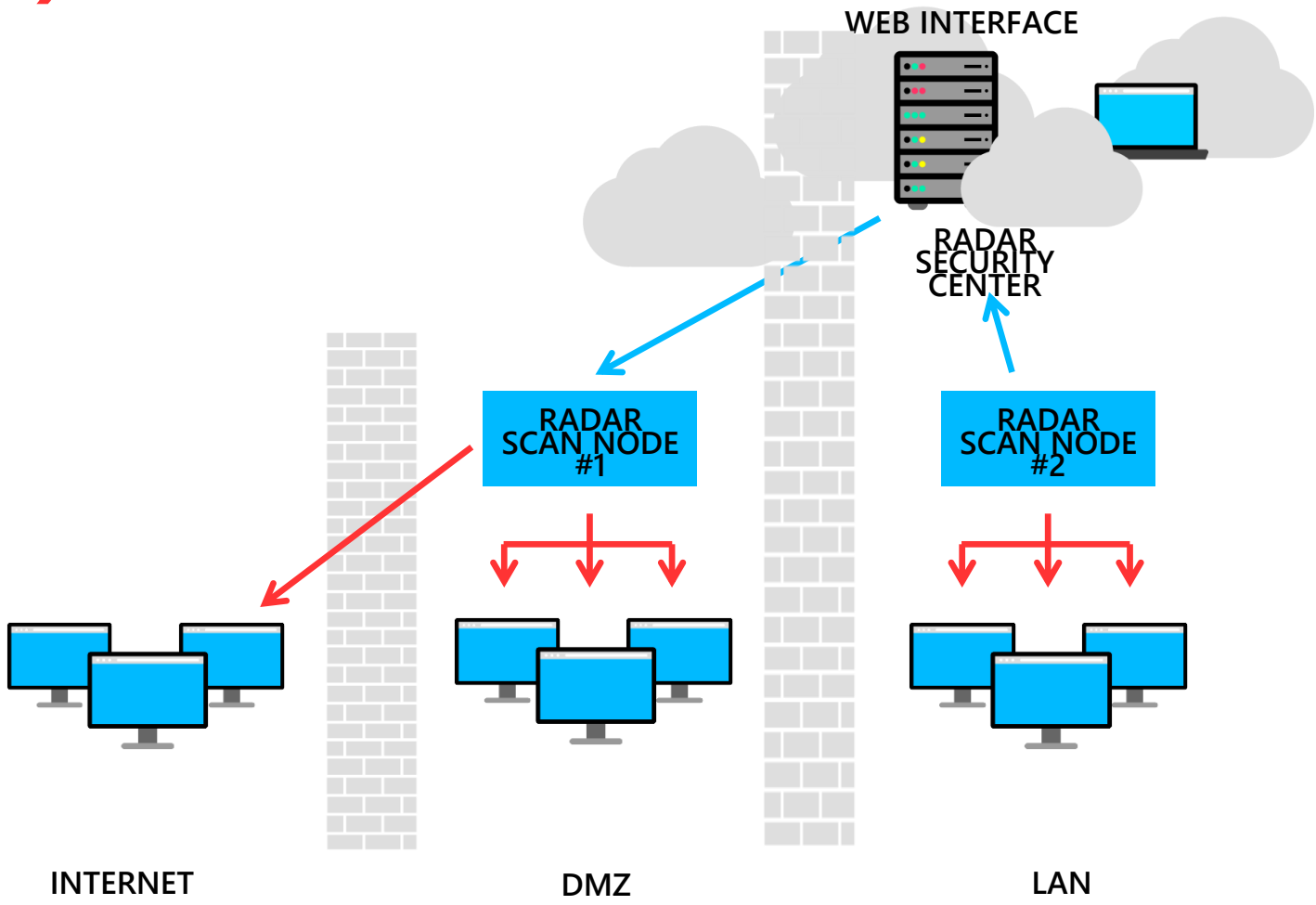
- クラウドホスト型のセキュリティセンター＆スキャンノード
- オンプレミス型スキャンノード
- 特長：
  - 容易なインストール
  - メンテナンス不要
  - より低価格
  - クラウドパワー



F-Secure.

脆弱性診断 (2) スキャンノード 使用

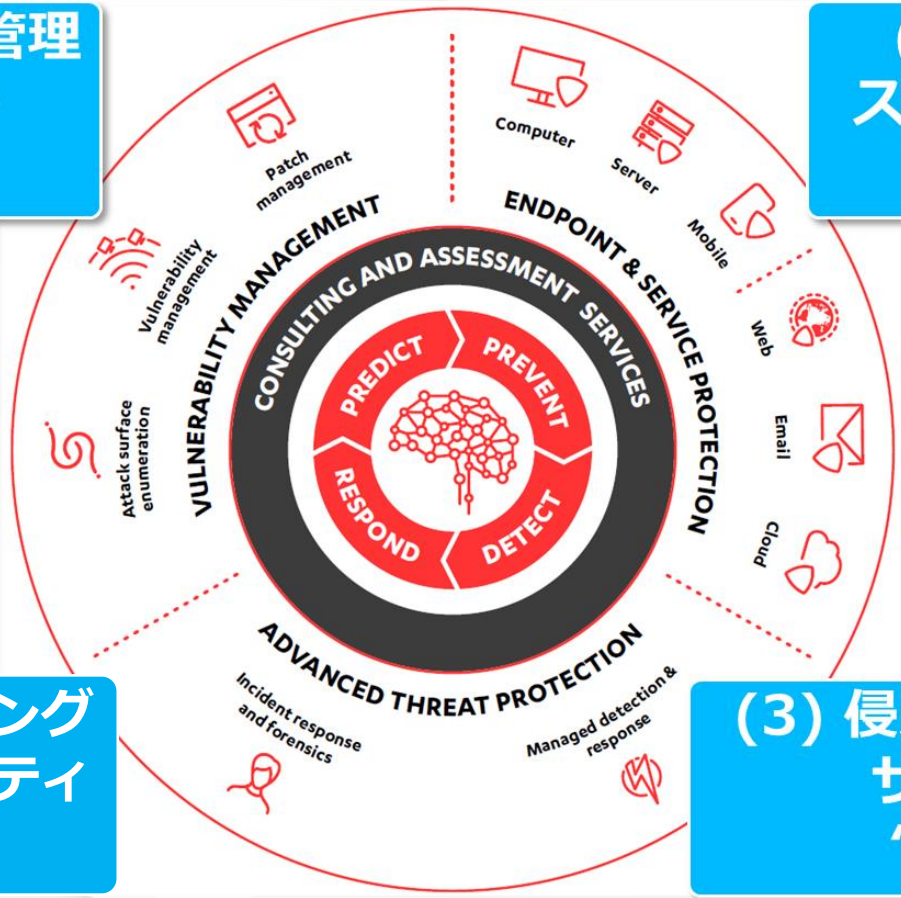
- セキュリティセンターは
  オンプレミス型
- セキュリティーセンターと
  スキャンノードは双方向で
  通信可能



F-Secure.

(2) 脆弱性診断・管理
ソリューション
“Radar”

(1) PC, Server
スマートフォン向け
アンチウイルス



(4) レッドチーミング
サイバーセキュリティ
コンサルティング

(3) 侵入対応・検出
サービス
“RDS”

脆弱性診断の先の、F-Secureサービス

F-Secure.

アンチウイルス～F-Secure Business Suite

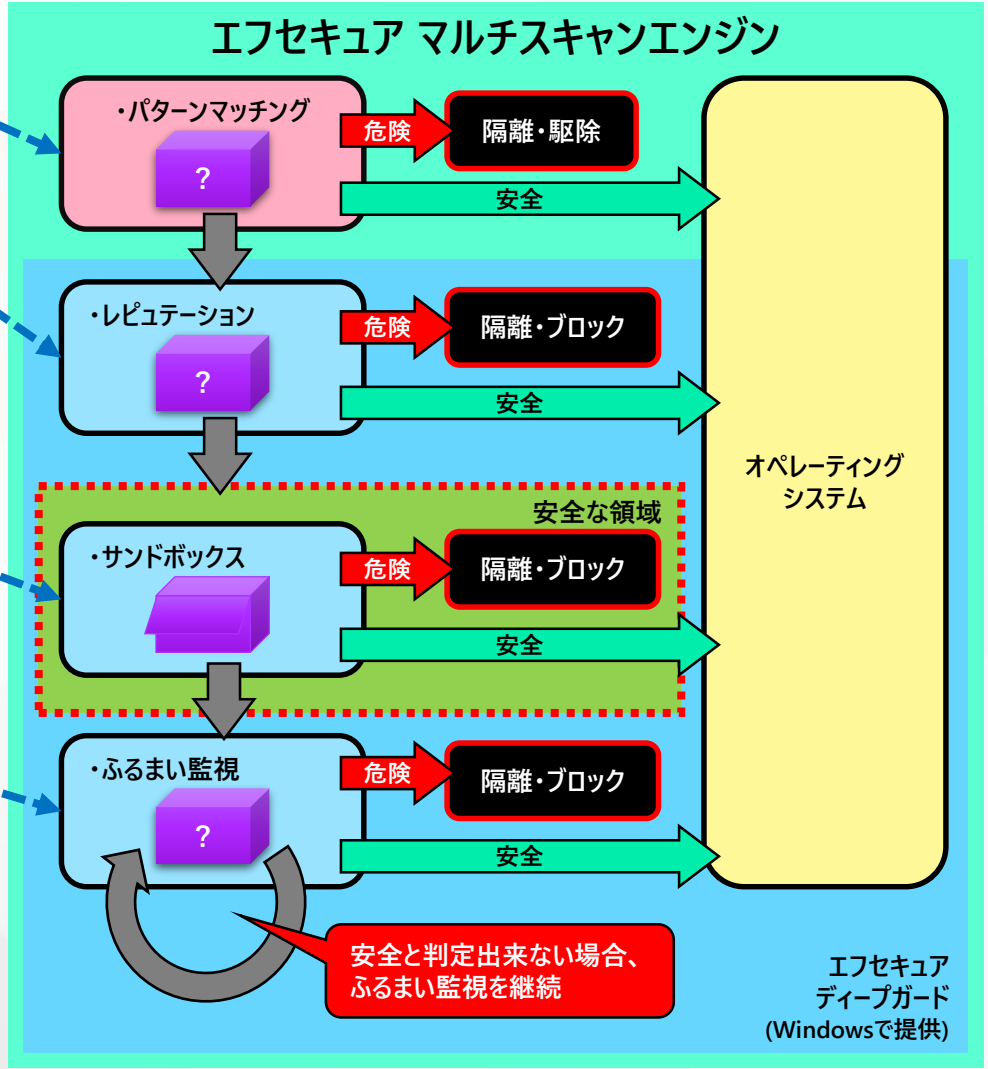
ウイルス発生の都度パターンファイルを生成し、配信します(1日あたり5～6回)。
AT TESTの評価による検知率100%

エフセキュアのレピュテーション(クラウドサービス)は発見された未知のウイルスの情報を60秒で全世界に展開します。

PC、サーバー内のサンドボックス(隔離空間での動作検証)が不明なファイルを危険と判定した場合、即座に隔離、ブロックします。ネットワーク型サンドボックスでは実現不可能な機能です。

最も対策が難しいサンドボックスをすりぬける未知のウイルスが侵入しても、ふるまいを常時監視し、危険と判定した場合、即座に隔離、ブロックします。

**既知、未知のウイルスに対して、最も確実な対策が行える仕組み、仕様です。
加えて、動作の軽さはトップクラス！**

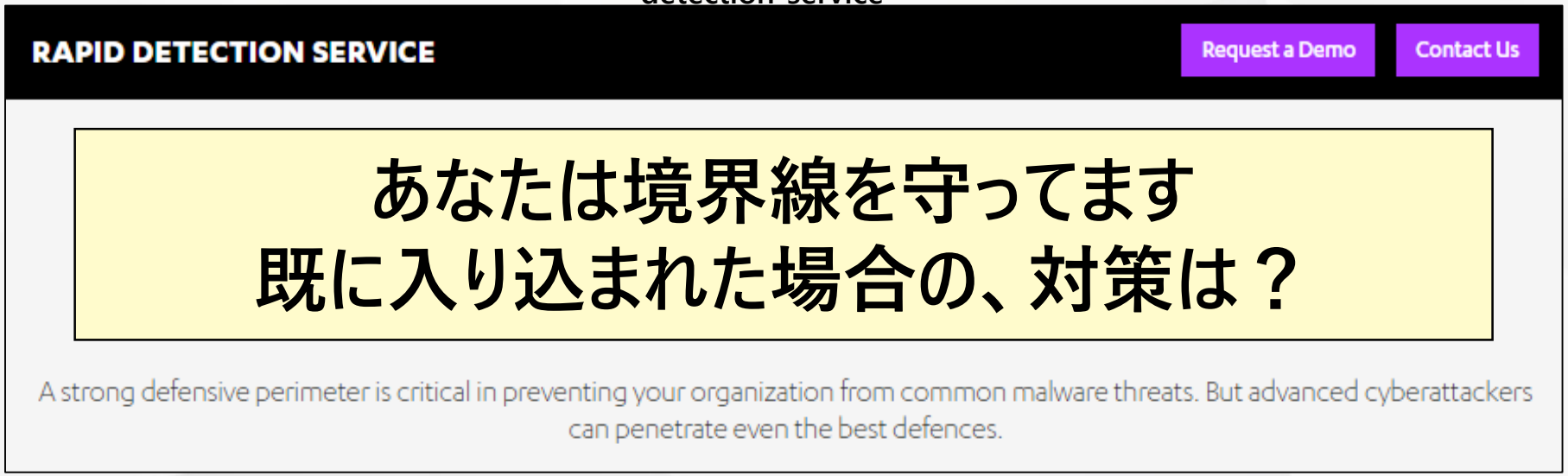


F-Secure

F-SECURE RDS

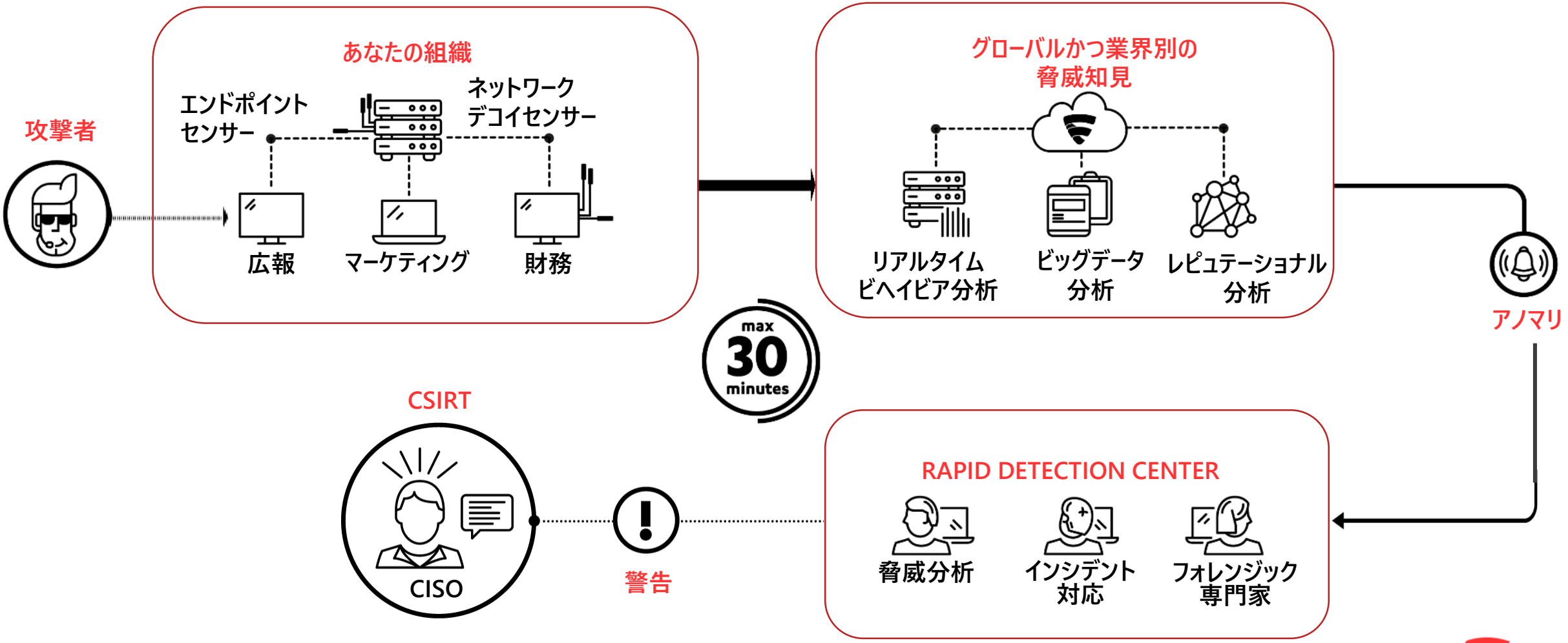
“RAPID DETECTION SERVICE”

https://www.f-secure.com/en/web/business_global/rapid-detection-service



F-Secure.

F-Secure RDS による
侵入検出サービス (30分以内に侵入検出)



F-Secure

F-Secure RDS 実際の中規模企業（社員1000人以上）での稼働・検知例

20億件
データイベント/月
組織全体に導入された約1300のエンドポイントセンサーで収集

90万件
不審なイベント
RDCの検出エンジンが生データイベントを分析した結果

25件
検出
RDCの脅威アナリストが異常を確認し、顧客に連絡

15件
真の脅威
顧客が脅威が事実であることを確認

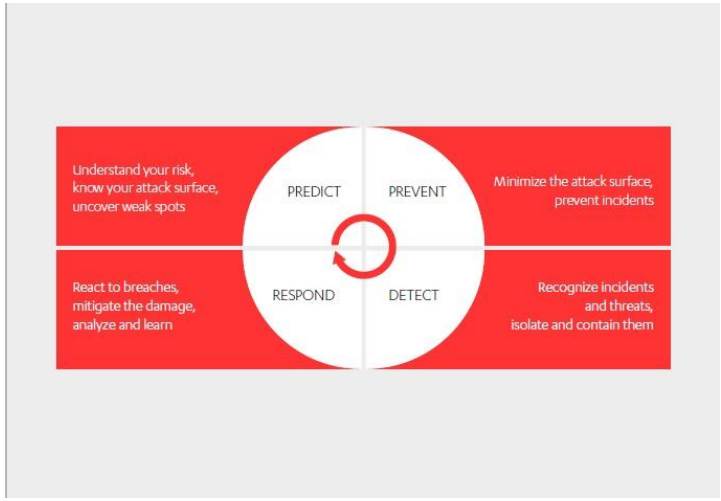
F-Secure

F-Secure の提供するセキュリティコンサル

レッドチーム演習

- 標的型攻撃テスト　　フィッシング攻撃演習
- ネットワーク攻撃テスト　Wifi, LAN攻撃演習
- Firewall, IDS/IPS　　ネットワーク攻撃・侵入演習
- 物理的セキュリティ　　ソーシャルエンジニアリング, 侵入演習

https://jp.business.f-secure.com/f-secure-does-red-teaming



F-Secure®