ハッカー視点から始まる

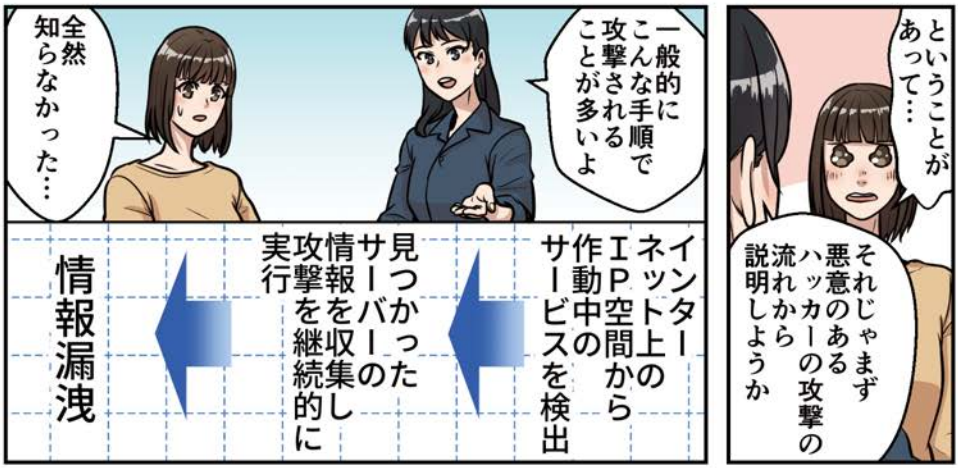
セキュリティ強化物語

ワンストップで実現する
セキュリティ対策

Securify


へへへ
ポチッとな…
…っていうことが
あってさぁ
まさか
あんなところから
攻撃を仕掛けられる
なんて思わなくて…
Cafe
へー
でもそれ
セキュリティ対策
ちゃんと
してたの〜？
まぁともかく
うちは対策したけど
つぐちゃんの
ところも
気をつけなよ？
大丈夫だって！
うちは
セキュリティ対策
万全だから！
継田（つぐた）
大手企業A社の
情報システム部
続木（つづき）
大手企業B社の
情報システム部
継田とは大学の友達


どっどうして…
こんなことに…
バタ
バタ
バタ
ガヤ
ガヤ
セキュリティ対策は
完璧だったはずじゃ
ないんですか…！
外部公開されたまま
放置されていた
開発サーバーが
狙われたんだ…
まさか
こんなものが
のこって
いたなんて…
ぷっ部長！
部長、他にも
同じような状態の
我々の知らない
サーバーが…
守谷（もりや）
大手企業A社の
情報システム部 部長
ハハハ
もう私はダメかも
知れない……
あとは任せるぞ…！
フル
部長
早まらないで
ください！
ガシッ
私、最近サイバー攻撃の
対策をした友人が
いるので聞いてみます！
本当か！
ありがとう～！


ということがあって…
それじゃまず悪意のあるハッカーの攻撃の流れから説明しようか
一般的にこんな手順で攻撃されることが多いよ
全然知らなかった…
インターネット上のIP空間から作動中のサービスを検出
見つかったサーバーの情報を収集し攻撃を継続的に実行
情報漏洩


インターネット上にIT資産を置くことは常に攻撃のリスクがあるってことだね
じゃあどうすれば…


・無駄なIT資産をインターネット上に公開しない
・脆弱性対策をし続けてハッカーよりも先に脆弱性を見つけて直す
そこで大切な考えがこの2つ！


だから今"ASM"が重要って言われているの
ASM…前に聞いた気がするけどなんだっけ？


「ASM(=Attack Surface Managementの略)
組織の外部(インターネット)からアクセス可能なIT資産を発見してそれらにある脆弱性などのリスクを継続的に検出・評価する一連のプロセス のこと」
ASMは経済産業省からこのように定義されているよ
ちなみにIT資産って具体的にはどんなもののこと？


一般的なIT資産はこんなところかな
・Webサーバー
・VPN機器
・IoT機器
・Webアプリケーション
・クラウドサービス
こんなところまで狙われていたんだ!?
でも全部を手作業で確認なんて現実的じゃないよね?
うーん
うーん
そこで活用できるのが『Securify ASM』なんだ!
Securify
セキュリファイ
教えて下さい!続木先生!
①パブリッククラウドの外部アクセスできる資産検出が可能
②高精度な脆弱性診断との組み合わせが可能
③資産検出時にテクノロジー情報を収集し最新の脆弱性を元に対策をレコメンド
①パブリッククラウドの外部アクセスできる資産検出が可能
『Securify ASM』ではパブリッククラウドとの連携で外部のIT資産を管理できるよ
うちも基本的にクラウドでの管理が多いからこれは嬉しい
・AWS
・Azure
・Google Cloud
定常的な棚卸しで外部からアクセスできるサーバーの変動性にも対応できるんだ
もし設定ミスでサーバーが公開状態になっても検知と診断が可能ってことかぁ

②パブリックアクセスが可能な外部資産検出ツールってのは検出はするけどそのあとどうすればいいかって悩むよね

確かに…

でも『Securify ASM』なら発見したIT資産に対して脆弱性診断を自動で行えるんだよ

そうか！発見されたIT資産に適合した脆弱性診断でセキュリティリスクの見える化ができるんだね

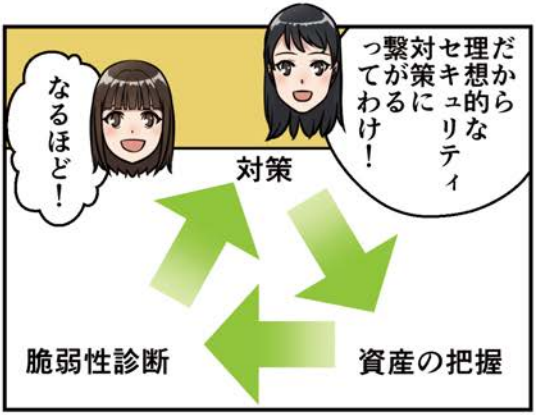
③資産検出時にテクノロジー情報を収集し最新の脆弱性を元に対策をレコメンド

それがなんなの？

資産検出時にはハッカーと同じ手順で資産に使われたテクノロジーの情報を収集しているんだ！

この情報を元に対策をレコメンドするから新しい脆弱性にもどのIT資産でどんな対応が必要かわかるの

うふん!!



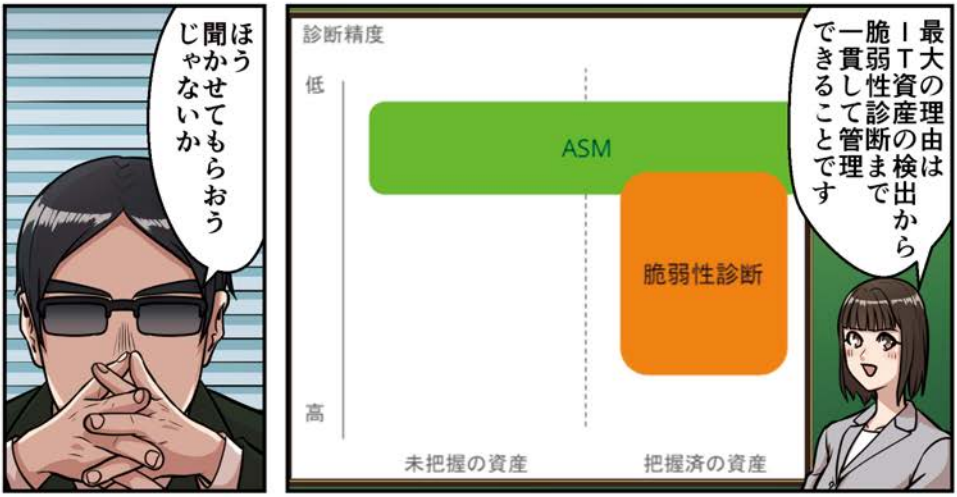

今日は急な相談だったのにありがとう！
部長にも提案してみるよ！
また何か聞きたいことがあったらなんでも聞いて！


部長！


今こそ私達も『Securify ASM』の導入をする時期ではないでしょうか？
バ
なんだって!?


今の私達は膨大なIT資産を管理どころか把握すらできていないと思うんです
確かにこの前のトラブルもあったしこの前かなり古いVPNも見つけたんだよな


まずはそこから認識するべきだと思うんです
すぃっ
ふむ
それでなぜ『Securify ASM』が良いんだ？


最大の理由はIT資産の検出から脆弱性診断まで一貫して管理できることです
診断精度
低
高
ASM
脆弱性診断
未把握の資産
把握済の資産
ほう聞かせてもらおうじゃないか


通常のASMでは検出までを対応しますが
検出後
対策・評価
Securify
こちらでは検出後に脆弱性診断ツールの『Securify』で対策・評価までを網羅的に行えるんです


なるほど同じスリーシェイクの脆弱性診断ツールが使えるのはとても安心できる
同じトラブルは必ず避けなければならないし『SecurifyASM』の導入を進めよう！
ありがとうございます！部長！


数日後
あっあぶない…
どうしてこのサーバー
公開されてたんだろ…
どうしたんだ？
はい
恐らくなにかのエラーで
長期間使用されてない
サーバーが
公開状態に
なっていたのを
『Securify
ASM』で
見つけたんです
本当に導入して
よかったな…
しかし
私は今回の件で
2つ改めて
思い知らされたよ
セキュリティ対策は
継続し続けなければ
いけないし
だからこそ完璧は
無いってことを
そうですね
私も現状に満足せず
セキュリティ対策の
プロフェッショナルを
目指します！
よろしく
頼むよ!!
はい!!

ワンストップで実現するセキュリティ対策

Securify

SecurifyではASMから高度な脆弱性診断まで
一気通貫で実現できる唯一無二のセキュリティツールです。

Securifyでできる 3つのこと

Securifyがない状態

資産棚卸し
- 資産管理台帳作成
- エンドポイント毎の技術要件まとめ

脆弱性診断
- 脆弱性診断のスコープ決め
- 業者選定
- 脆弱性診断の実施とレポート対応

運用
- 定期的な資産棚卸し
- 定期的な脆弱性診断の実施

Securify

資産棚卸し
脆弱性診断を
全て自動化！

運用
定期的な
脆弱性診断結果の確認

工数 コスト を大幅削減！

Securifyご利用までの 4ステップ

Step 1

アセットリソース登録

お客様にてご利用のPublic CloudやDNS情報/IP情報の登録をしていただきSecurifyの監視スコープを設定します

Step 2

エンドポイントの種別を棚卸し実施

Securifyにて検出されたエンドポイント一覧から資産の棚卸しを行います

Step 3

エンドポイントに併せた脆弱性診断の実施

エンドポイントの種別毎に適合する脅威件数等の実施を行い、本質的なセキュリティリスクを洗い出します

Step 4

エンドポイント増減の定常監視と脆弱性診断サイクルの実現によるIT環境の堅牢化

エンドポイントの検出・脆弱性診断の実施・0day攻撃や新規CVE検出に適合するために定常的なサイクルを作ります

経済産業省「情報セキュリティサービス基準」適合

Securify

IS 752246 / ISO27001

詳しくはこちら

3-SHAKE

各サービス導入に関する
お問い合わせはこちらから

事業者が抱える
セキュリティリスクを無くす

Securify

日本のSREを
リードする

Sreake

あらゆるサービスを
連携するハブになる

Reckoner

良いエンジニアに
いい条件を

Relance

株式会社スリーシェイク

〒160-0015
東京都新宿区大京町22-1 グランファースト新宿御苑3F・4F
https://www.3-shake.com