SecureBrain®

EDR導入における課題を解決する SOCサービスの事例

株式会社セキュアブレイン
プロフェッショナルサービス本部

セキュアブレイン会社概要

SecureBrain

会社概要

商号	株式会社セキュアブレイン
設立	2004年10月5日
所在地	〒102-0094 東京都千代田区紀尾井町3－12 紀尾井町ビル7F
資本金	2億5,180万円
代表	青山　健一 （代表取締役社長 兼 CEO）
株主	株式会社日立システムズ

主要製品 ・ サービス

不正送金・フィッシング対策

PhishWall®

Web改ざん対策

gred Web 改ざんチェック

セキュリティアプリ用SDK

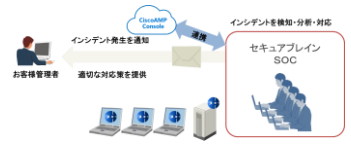
・Android用マルウェア検知
・アンチランサムウェア

サイバースパイ対策情報

・月次の脅威情報提供
・攻撃者グループの調査報告

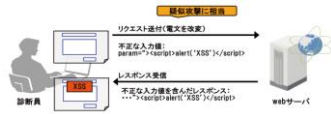
SOCサービス

・エンドポイント監視サービス
　イベント分析サービス
　インシデント対応サービス



脆弱性診断サービス

・ITインフラ診断
・Webアプリ診断
・ソースコード診断



セキュアブレインは国内で最も古くから CiscoAMPをサポートしています

CiscoAMPの沿革

	2009年11月	2012年9月	2014年3月	2017年9月
SecureBrain	Immunet ProtectのOEM gred AVXを提供	FireAMP 国内総代理店	Ciscoによる買収後は CiscoAMP代理店	CiscoAMPの SOCサービス開始

セキュアブレインの実績

ライセンス販売実績	30社以上
導入支援実績	10社以上
テクニカルサポート実績	10社以上
SOCサービス実績	6社

＜導入企業業種＞
大手製薬企業、大手流通企業、大手新聞社、
大手法律事務所、官公庁、独立行政法人 等

CiscoAMP稼動実績（グローバル）

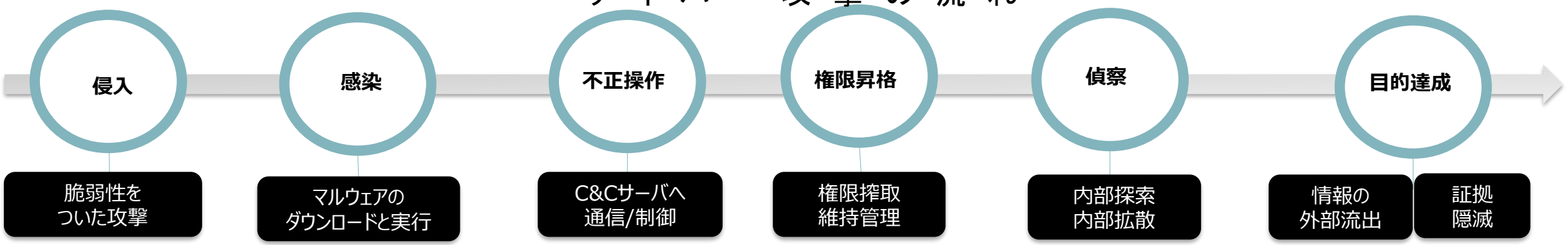
海外600万台以上
100,000台：10社超（最大規模は200,000台規模）
20,000～100,000台：50社超

国内
10,000台以上：複数社
（メディア、流通、金融、大学等）
5,000台以上：10社超
（流通、金融、製造業、製薬会社、IT企業、大学等）

サイバー攻撃対策にはEDRが不可欠

SecureBrain

サイバー攻撃の流れ



従来型アンチウィルスがカバーする範囲

- パターンマッチング
- 侵入の防御と隔離が目的
- 既知の脅威に有効
- 未知の脅威には無力

次世代アンチウイルスがカバーする範囲

- 不審な動作を検知するふるまい検知機能
- 脅威の検知・封じ込め
- 未知の攻撃にも対応

EDR（Endpoint detection and response）がカバーする範囲

- 侵入されることを前提に、いち早くその脅威を検出して対応することが主目的
- 不審な動作を検知するふるまい検知機能、詳細な履歴を記録する機能
- 脅威の検知・封じ込め・侵入後の挙動を可視化
- 影響範囲の特定・原因調査が可能、再発防止のための対策に役立つ

脅威を侵入させない対策 → **侵入を前提とした対策**

Cisco AMP がカバーする領域

EDRを導入検討されているお客様の3大課題（お客様の声）

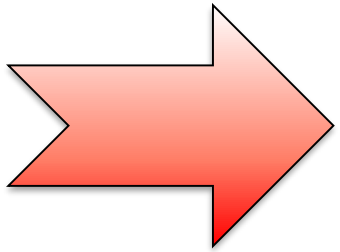
SecureBrain

- リソース問題
  - セキュリティの重要性は理解しているが、セキュリティの専任担当者がいない（決まっていない）
  - 新規のプロジェクトのテストに手いっぱいで、セキュリティ要員に投資する余裕がない
- スキル問題
  - EDRには様々な機能が備わっているが、機能が多すぎて使いこなせない
  - アラートが出た端末をドリルダウンして調べるには、マルウェアの知識と経験が必要
  - そもそもEDRは詳細な調査ができる専門家向けに設計されている
- 脅威への対応問題
  - EDRは検知がメインなので、脅威の判断や特定、駆除などはユーザがやる必要があり運用の負荷が増大してしまう
  - EDRからたくさんのアラートが飛んでくるが、対応が必要な検知かどうかの判断ができない
  - 脅威を特定できても、それが悪性なのか非悪性なのか判断できない

EDR導入における課題の解決策

課題

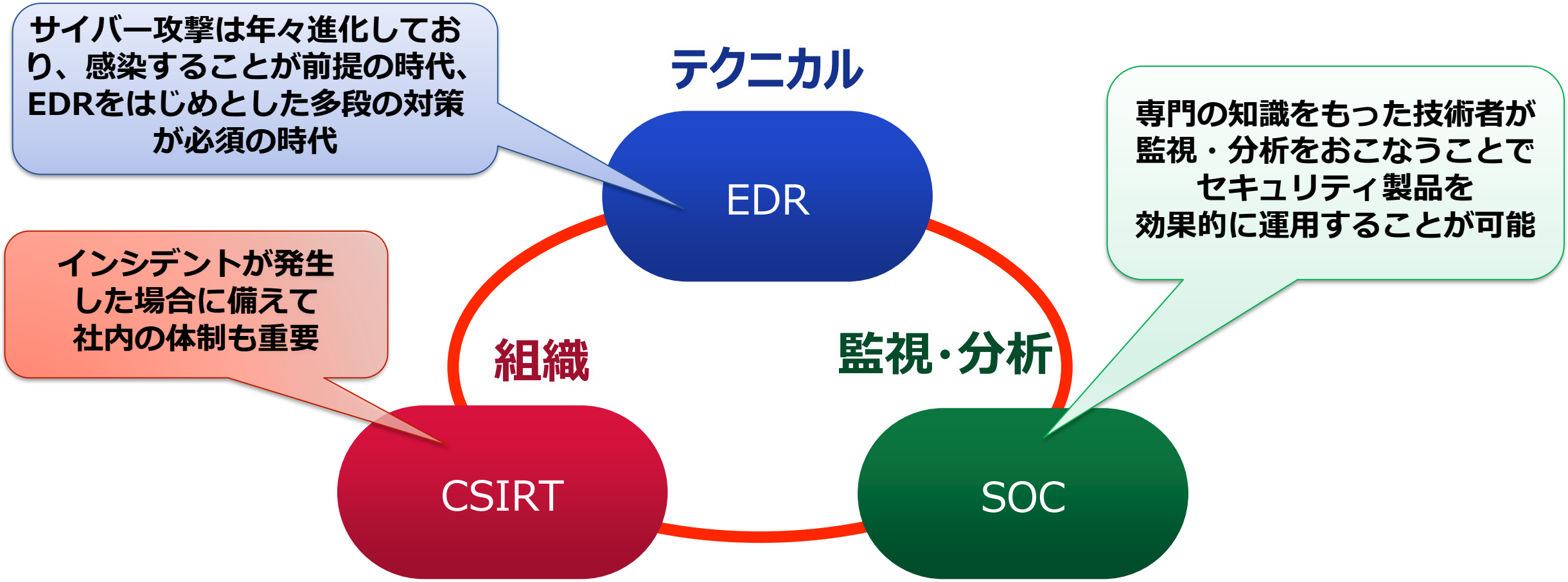
- リソース問題
- スキル問題
- 脅威への対応問題



SOCサービスが提供する解決策

- EDR製品とマルウェアに精通した弊社アナリストがお客様に代わり、EDRを監視・分析します
- お客様にとって重要な検知イベントを抽出し、詳しい分析結果をご報告します
- 悪性／非悪性の判断について弊社の見解と、根拠となる情報をご提供します
- 分析の結果、お客様で行うべき対応についてご報告します

組織のセキュリティを高める3つの要素



それぞれの要素が相乗効果となる
EDRの導入効果を高めるにはSOCの活用が効果的！

7

SecureBrain®

お客様導入事例

１．『EDR＋SOC』をセットで検討した理由

EDR＋SOC導入決意までのプロセス

01
AVだけでは守れないご時世

今この瞬間、インシデントが起きているかもしれない。
でも、検知・対処する術がない。

AVだけで事足りる時代でないことは確実。

02
NGAV？EDR？Isolation？

エンドポイント製品の情報収集開始

カテゴリ分けをして、理解を深める

→新しいコンセプトの製品、どれも良さそうに見える。。。

03
真面目に選定開始

自社に必要な製品ってどんな？
→チーム内の意見とりまとめ、調整

導入までのハードル、運用のハードルなどもヒアリング

04
AV＋EDR＋SOC

EDR必要だよね。

でも、AV・NGAVで絶対数減らすのが大前提だよね。

EDRからのアラート判断できなければ意味ないよね
→SOCもいるよね。

EDR＋SOCで実現したいこと

課題１	PCのインシデントをリアルタイムで検知・感染経路の可視化をしたい
課題２	どんなに優秀なEDRを導入しても、検知情報を確認する人的リソースもなければ、インシデントを切り分けるスキルもない
施策	EDRを導入するが、社内の人的リソースは使わない(使えない) →EDR＋SOCサービス
ゴール	本当に対応が必要なインシデントのみ対応する仕組みを構築する

→SOCも一緒に導入必須！

２．『CiscoAMP＋セキュアブレインSOC』に決めた理由

選定のプロセス

候補の絞り込みを行い、実際に試用(PoC)して評価・選定を実施

01
主要製品の絞込

要件定義から、
カタログスペック比較を経て
９製品→3製品

02
製品試用(PoC)

3製品の試用を実施

申し込みから実現までのベンダー側の対応も重要視

03
比較･検討

Must要件クリアか確認

04
採用製品決定

自社要件に対して、機能面で決定的な差はなかった

選定結果

総合的な評価から、CiscoAMPを採用した。

※2018年12月時点

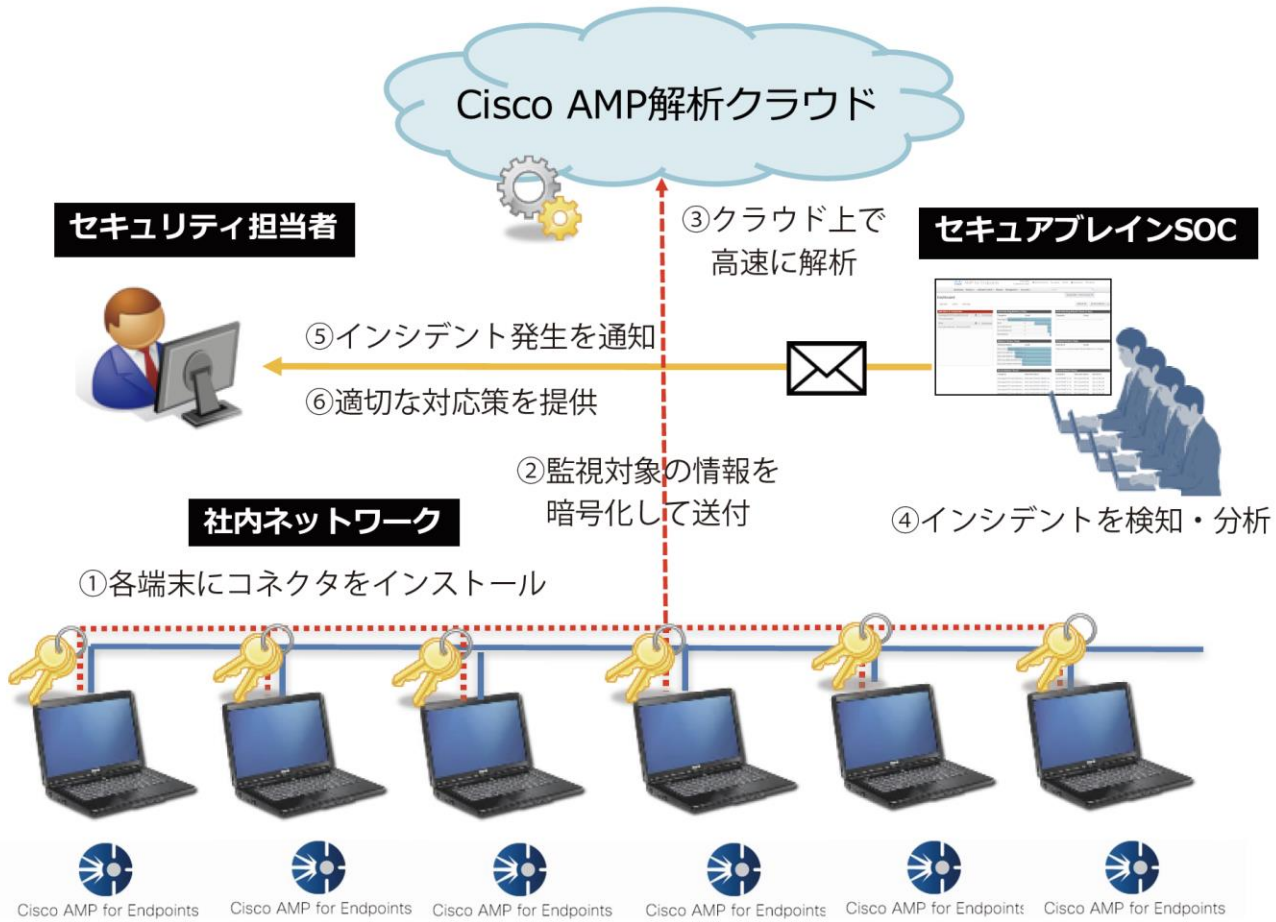
製品	CiscoAMP	A社EDR	C社EDR
SOC	セキュアブレイン	B社SOC	D社SOC
安定性・PC負荷	○	○	○
機能	△ → ○ (2019年上期実装予定)	○	○
SOCの実績	○	△	×
コスト	◎	×	△

→他の2製品に価格差を埋めるだけの優位性を見いだせなかった。
SOCに実績がある点で、セキュアブレインSOCは評価できた。

SecureBrain®

セキュアブレインSOCサービスのご紹介

セキュアブレイン　SOCサービス概要



- 国内トップレベルのマルウェア解析技術で培った知見でお客様で発生する検知イベントを分析します
- Cisco AMP for Endpointsについての豊富な経験により、検知イベントを詳細に分析します
- 導入の初期段階にチューニングを行うことにより、お客様での無駄な検知を削減し、重要な検知イベントにフォーカスして対応します
- 導入が簡単：EDRに弊社のアカウント作成していただくだけで導入可能です。
- EDRな豊富な機能を活用することによりサイバー攻撃の状況把握と迅速な対策が可能になります
- 検知イベントの監視は24x365で監視します

SOCサービスメニュー

初期チューニングサービス
EDRを初めて導入されるお客様向けの過検知対策サービスです。
EDR導入当初は大量の過検知が発生する場合があります。初期チューニングサービスを利用して
導入初期の大量の過検知を短期間に除去することにより、早期に通常運用が可能となります。

スタンダードサービス（アラート監視・検知イベント分析サービス）
1次対応
EDRから送信される検知アラートについてセキュアブレインの技術者が検知内容を確認し、
検知内容の解説とお客様での対応の必要性などをメールでご連絡いたします。
2次対応
EDRの脅威検知イベントについてセキュアブレインの技術者が
検知状況を分析し、感染端末の感染経路や、被害状況を確認し、対応方法について
適切なアドバイスをご提供いたします。

アドバンスドサービス（インシデント対応サービス）
Standardサービスに加えて、検知した脅威に対する対応を弊社が実施いたします。
カスタムブラックリストの登録や除外設定、攻撃者サーバへの通信遮断などの対応を行います。
通常のアラート監視・検知イベント分析に加えて、お客様からのご依頼ベースでの分析にも対応します。
お客様で重要なインシデント（大規模感染など）が発生した場合の対応方法について支援します。

オプションサービス
EDR製品導入支援サービス 、 マルウェアの詳細解析サービス 、 半期・年次レポートサービス

17

SOCサービス項目一覧

番号	サービス項目	契約区分	サービス提供時間
(1)	初期チューニングサービス	必須	弊社営業時間
	① 過検知の確認		
	② 過検知のホワイトリスト登録		
(2)	スタンダードサービス	必須	–
	① SOC監視設定サービス		弊社営業時間
	② 検知イベントの受信		24時間365日
	③ 検知イベントの内容確認		24時間365日
	④ お客様への一次報告（検知イベントの解説）		24時間365日
	⑤ 検知範囲・規模の確認		弊社営業時間
	⑥ 被害状況確認		
	⑦ 検知経緯・経路の確認		
	⑧ 未検知検体の有無の確認		
	⑨ 過検知の確認・悪性判断		
	⑩ お客様側で必要な対応の確認		
	⑪ お客様への二次報告（上記⑤－⑩）		
(3)	アドバンスドサービス	任意	弊社営業時間
	① 外部通信先のブラックリスト登録		
	② 過検知の場合ホワイトリスト登録		
	③ 除外設定		
	④ 未検知の検体のブラックリスト登録		
	⑤ お客様への対応報告（上記①－④）		
	⑥ お客様からのご依頼ベースでの分析対応		
	⑦ 重大インシデント発生時の対応支援		
(4)	半期・年次レポートサービス	任意	–
(5)	マルウェア解析サービス（簡易解析）	任意	–
(6)	マルウェア解析サービス（詳細解析）	任意	–

2019年8月現在のサービス項目です

18

SOCサービス　インシデント対応の流れ

SecureBrain

お客様へのご報告例	弊社のインシデント対応の流れ	
	アラート受信	スタンダード
	アラートの内容確認	
一次報告のご連絡 ←	マルウェアのナレッジの提供	
	感染イベントの詳細確認	
	感染被害内容確認（攻撃内容確認）	
	悪性／非悪性の判断	
	未検知の検体がある場合のご連絡	
	情報流出の可能性がある場合のご連絡	
二次報告のご連絡 ←	拡散状況の確認	
感染経路・拡大防止策	感染拡大防止策のご連絡	
（切り離し・駆除手順など）	マルウェアの外部への通信の確認	
	犯人サーバへの通信の遮断対応	アドバンスド
	未検知の場合のブラックリスト対応	
	過検知の場合のホワイトリスト対応	
対応報告の送付 ←	除外設定などの事後対応	
	お客様のご依頼による個別分析対応	
	重大インシデントの発生時のご支援	

19

SOCサービス　一次対応 対応事例

〇〇〇〇株式会社　御中

平素はセキュアブレインの監視サービスをご利用いただきありがとうございます。
脅威の検知イベントを受信いたしましたので下記にご報告させていただきます。

検知日時（JST）: 2019-MM-DD HH:MM:SS
検知したイベントタイプ：Executed malware
検知したPCのコンピュータ名：pc-XXXXXXX.abc..local
PCのIPアドレス：192.168.0.XXX
ユーザ名：hogehogeXXXX
検出名：W32.Application.22ik.1201　W32.DFC.MalParent
ファイル名：Adobe Reader(Acrobat Reader)_XXXX.exe
ファイルパス
c[:]¥users¥hogehogeXXXX¥appdata¥local¥packages¥XXXXXX¥temp¥
ハッシュ値(SHA256)：XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
関連したファイル名：記載なし
関連したファイルのハッシュ値（SHA-256）：XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

弊社からの報告事項:
本検知イベントは、マルウェアと疑われるアプリケーションの実行を検知しました。
実行されたアプリケーションが問題のないアプリケーションかどうか確認を行って下さい。

本検知につきましては引き続き弊社のほうで分析し、ご報告させていただきます。
もし、お客様がこの検知イベントを誤検知とご認識されている場合には、ご一報いただけますようお願いいたします。

株式会社セキュアブレイン
SOCチーム
xxxxxxx@securebrain.co.jp

20

SOCサービス　二次対応　分析報告例（1）

SecureBrain

1. 検知PC情報:
PC名:pc-XXXXXXX.abc..local
検知時内部IPアドレス:192.168.0.XXX
ユーザ名: hogehogeXXXX
検出名:W32.Application.22ik.1201　W32.DFC.MalParent
重要度:High

2. 検知時間:
2019年XX月XX日 XX時XX

3. 検体情報:
ファイル名:Adobe Reader(
Adobe_Reader_
フォルダパス:c[:]¥users¥h(
C[:]¥temp¥ot
ハッシュ値(SHA256):XXX

外部への通信先等の情報:
1.193.XXX.XXX Port 80
122.112.XXX.XXX Port 80
47.94.XXX.XXX Port 80
hxxp[:]//[:]//api11.xxxxxxxx
hxxp[:]//[:]//api22.xxxxxxxx
hxxp[:]//[:]//d.onlinexxxxxx
hxxp[:]//[:]//source.xxxxxxx
hxxp[:]//[:]//static.xxxxxxxx

4. 判定: 悪性(中)

5. 状態: 未検疫

6. 検知理由:
「ファイルのレピュテーション機能によるMalware検知」と AMPに認識されております。

7. 検体概要:
本検体はVirusTotalのアンチウイルスベンダーの検出名より、アドウェア関連を取得するダウンローダーの実行ファイルであると推測されますが、アドウェア以外も取得される可能性がございます。

認することは出来ませんでした。

加でアプリケーションを取得する

ら、Microsoft Edgeによるブラウザ

奨いたします。

スのブラックリスト登録

ファイル削除
確認

※上記のファイル削除によりマルウェアの駆除は可能ですが、完全な復旧をご希望の場合は当該PCでクリーンインストールを実施なさることを推奨いたします。
―以上―

本対応事例におけるSOCの効果

1．SOCの分析で未検疫のファイルが存在することがわかった
2．ユーザがAcrobatReaderだと思い込んでマルウェア付きのファイルのダウンロードを発見（ポリシー違反）
3．お客様で行うべき駆除作業のご報告により元を断つことができた

再発防止策
ダウンロードしたユーザへの注意
当該ファイルのダウンロードURL、IPアドレスのブラックリスト登録
未検疫ファイルの駆除の実施

本報告例は実際の報告を基にしたサンプル版になります。実際の報告書とは異なる場合があります。

SOCサービス　二次対応　分析報告例(2)

SecureBrain

1. 検知PC情報
PC名:XXXXXXXXXX.local
検知時内部IPアドレス:10.XXX.XXX.XXX
検知名:Html.Downloader.Forbix::in01
Cloud IOCでの検出名:W32.VBScriptEncodedEngineExecution.ioc
Vbs.Worm.SysinfY2X_46894.ioc
重要度:Medium　※Cloud IOCの検

2. 検知時間
2019年XX月XX日 XX時XX分4

3. 検体情報
ファイル名:SysXXXXXX.db
フォルダパス:C:¥Users¥xxxxx
ハッシュ値(SHA256):XXXXXX
ファイルトラジェクトリ:
https://console.amp.cisco.com/

外部への通信:上記検体は、生
行っておりません。ただし、後述
発生させております。
通信内容:hxxp[:]//xxxxxx.xxxx
IPアドレス:146.XXX.XXX.XXX
※Cisco Umbrellaのブロックペ

4. 判定
悪性(中)　※接続先は無害化され

5. 状態
一部検疫済み
(※実行のきっかけとなった「Manuel.doc」は検疫されていない可能性がございます。)

6. 検知理由
「Tetra(Offline Engine)によるパターン検知」と AMPに認識されております。

7. 検体概要
Cisco AMPの検知名やファイルのハッシュ値から取得可能な情報により、本検体はC&Cサーバーと通信し
攻撃者からの指令により他の悪意のあるプログラムをダウンロードするものとなります。
バブルドライブに自身をコピーする
で追うことは出来ませんが、
自動実行されるようにレジス

%temp%¥SysinfY2X.db

xxxxx xxxxx ?? & xxxxx
レを(中身は検体と同じものと
)実行したことで本検体が
保存されたかはCisco AMPでは

せんでした。

します。

・ネットワーク内の共有フォルダやUSBメモリなどリムーバブルディスクへの感染の確認
・「Manuel.doc」が存在する場合は削除

PCの復旧について
※上記のファイル削除によりマルウェアの駆除は可能ですが、完全な復旧をご希望の場合は
当該PCでクリーンインストールを実施なさることを推奨いたします。　―以上―

本対応事例におけるSOCの効果

１．Cloud　IOCのよる警告の意味の解説
２．Cisco Umbllera を併用していることにより、外部と不審な通信をしているPCがあることがSOCの分析により判明
３．不審な通信を送信している未検疫のマルウェア（ドロッパーまたはダウンローダー）が存在することが可視化された
４．お客様で行うべき駆除作業のご報告により被害拡大を防止

再発防止策
当該ファイルのダウンロードURL、IPアドレスのブラックリスト登録

本報告例は実際の報告を基にしたサンプル版になります。実際の報告書とは異なる場合があります。

SOCサービス　二次対応　分析報告例（3）

SecureBrain

1. 検知PC情報:
PC名 XXXXXXX.local
内部IPアドレス 10.XXX.XXX.XXX

2. 検知時間:
2019年XX月XX日 XX時XX分XX秒(JST)から

3. 検体情報:
ファイル名:mond_xxxxxxxxxx
検出名:Win.Trojan.Generic::9
ハッシュ値(SHA256):XXXXX
検体のファイルトラジェクトリ:
htt[p]s://console.amp.cisco.co

4. 検体概要:
検知しているファイルはRainme
（スキン:　自分好みのデスクト
Rainmeter自体に悪性評価はこ
そのため、スキンファイルにはマ

また、今回ご報告させていただ
そのため、アンインストール後の

5. お客様へのお願い事項:
以下の内容を実施していただくこ
・フルスキャンの実施
・コネクタのアンインストールが意図して行われたものかどうかヒアリング
・コネクタの再インストール
・業務に不要なアプリケーションであった場合、アンインストールの実施。

―以上―

本対応事例におけるSOCの効果

1．SOCの分析によりマルウェア感染の温床になる可能性のあるソフトウェアがインストールされていることが判明（検知したのはアドウェアのスキン）

2．マルウェアを検知したPCでのEDRエージェントのアンインストール（重大なポリシー違反）の発見

再発防止策
当該PCユーザ様への事情ヒアリング、注意等

本報告例は実際の報告を基にしたサンプル版になります。実際の報告書とは異なる場合があります。

SOCサービス　目標対応時間

サービス項目	目標対応時間
お客様への一次報告 検知イベントの概要報告	弊社が登録したメールアドレスにアラートメールが到着後、またはAPIコールにより検知イベントを取得後1時間以内
お客様への二次報告 詳細な分析結果 お客様行うべき対応 再発防止策	弊社が登録したメールアドレスにアラートメールが到着後、またはAPIコールにより検知イベントを取得後翌営業日以内

本サービスでは、各評価項目ついて目標値を設定いたします。
サービス品質がこれを著しく下回る場合は当該インシデントについてはサービスチケットを消費しないものとします。

24

まとめ　お客様がSOCサービスを導入する理由とお客様のメリット

SecureBrain

- サイバー攻撃が高度化、複雑化している昨今、自社の環境を常に監視し、攻撃を検出・分析する必要がある！
- 社内にSOCを構築するのは困難、無理！　外部にアウトソースするのが現実解
- アウトソースのメリット
  - 自社では構築が困難な24時間365日の体制で監視可能
  - セキュリティ対策コストの削減
  - 専門家による分析により、本当に対応が必要なイベントを早期に検出
  - 自分たちだけでは判断の難しい検知イベントも専門家がサポート
  - セキュリティ侵害だけでなく、ポリシー違反やリテラシー問題のあぶり出しにもなる
  - 万が一セキュリティが侵害されても、早期発見と専門家の支援により被害を最小限に

重要なのはEDRとSOCの導入がお客様のセキュリティを高めること！

SecureBrain®

Our Knowledge, Your Security.

ネット犯罪からすべての人を守る

Our Knowledge, Your Security.