典型的な詐欺行為の検出

Secure Bankと一緒に

どうしてGroup-IB

Group-IB — ハイテク技術を使用したサイバー犯罪および詐欺の予防および調査のための有力な国際企業の1つである。

EUROPOL INTERPOL

EUROPOL とINTERPOL
の正式なパートナー

OSCE

欧州安全保障協力機構（OSCE）
が弊社を推薦する

WORLD ECONOMIC FORUM

世界経済フォーラム常任委員

1000+

全世界で成功的な調査、その中で150特に困難な刑事事件がある。

$3億

弊社の仕事により、IBグループの顧客に返還された

Forrester Gartner

Group-IBの Threat Intelligence – Forrester とGartnerの評価によりますと世界一番良いシステムの1つである。

BUSINESS INSIDER

Business Insiderによると7つの最も影響力のあるサイバーセキュリティ会社の1つ

IDC

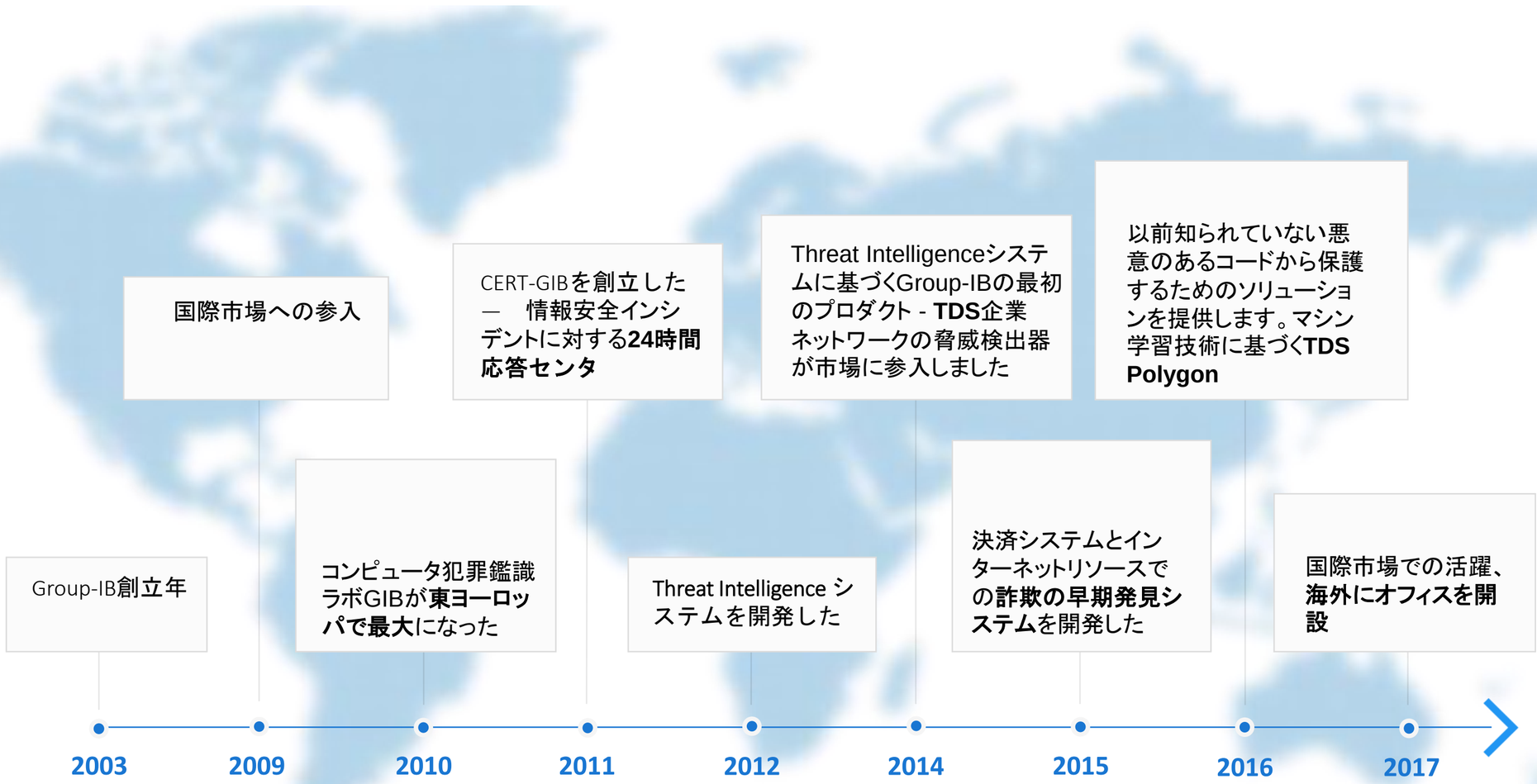
ロシアのサイバー脅威研究市場のリーダー

弊社に関して色んなマスコミは情報を伝えています:

theguardian Bloomberg Forbes REUTERS Esquire

ПЕРВЫЙ КАНАЛ РОССИЙСКАЯ ГАЗЕТА ИЗВЕСТИЯ ВЕДОМОСТИ РОССИЯ 1 Коммерсантъ

会社の歴史



GROUP-IB

グループIBの長年の経験は、サイバー脅威の早期検出システム、最新のデータに基づくハイテクプロダクトのライン、および実際のハッカー攻撃の詳細な分析に組み込まれています。

260+
職員

40%
解発者

27
平均年齢

45 000
反応時間

ユニークな資源基盤

15年間の仕事によって納めたユニークな資源基盤

ハッカーの活動を監視し、ボットネットワークを追跡し、インシデントを防ぐために必要なデータを抽出するためのハイテクインフラストラクチャを作成しました。**データの90%が密封されたソースからシステムに入り**、そのほとんどはユニークです。閉式のサイトを観測し、ボットネットの変更を監視し、マルウェア設定ファイルを抽出し、盗まれた識別子に関する情報を収集します。

1 ネットワクインフラストラクチャ

- 分散された監視とHoneyNetトラップのネットワーク
- ボットネットの分析
- ネットワーク攻撃トラッカー
- ハッカーフォーラムと閉式のネットワークコミュニティの監視
- TDSセンサーデータ

2 HUMAN INTELLIGENCE

- グループIBラボの犯罪鑑識的検証の結果
- 調査資料
- マルウェアの監視と分析
- 問い合わせデータベースとCERT-GIBインシデント対応プラクティス
- 監査結果
- グループ-IBターゲット分析

3 データー交換

- CERT応答チーム
- レジストラとホスティングプロバイダ
- セキュリティ手段メーカー
- サイバー脅威に対抗する組織と団体
- Europol、Interpolと法執行当局

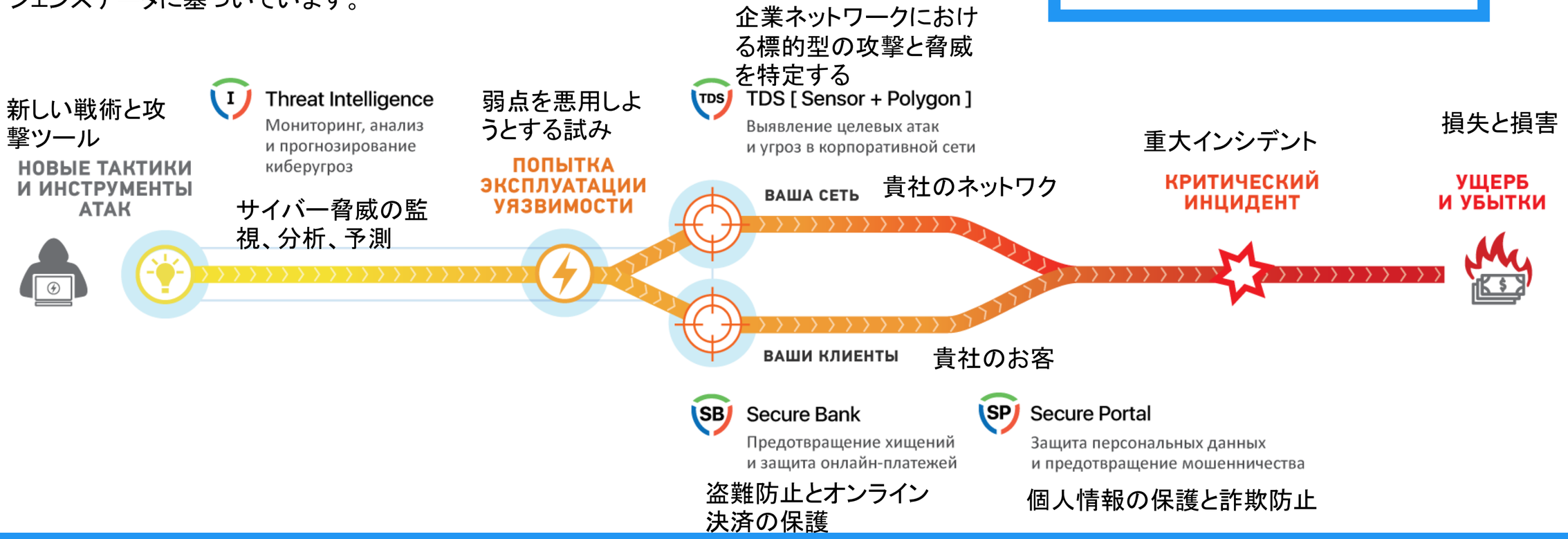
サイバー脅威に関する早期警告システム

あなたに最も重要なことを提供します：時間、インシデントに準備しかかる時間。

グループ - IBのサイバー脅威早期警戒システムにより、新たな脅威について迅速に把握し、防御ライン上の出現を阻止することができます。私たちのチームの15年の経験、ハッカーキャンペーンの詳細な分析とサイバー犯罪世界からの実際のインテリジェンスデータに基づいています。

15 年

コンピュータ犯罪鑑識、コンサルティング、情報セキュリティ監査の専門経験



会社構成

GROUP IB

早期警戒システム

- Threat Intelligence
- TDS
- Secure Bank
- Secure Portal

脅威の予防

- セキュリティ監査
- Compromise Assessment
- Red Teaming
- Brand Protection
- Anti-Piracy

反応 24/7/365

- 情報セキュリティインシデント対応センター CERT-GIB

インシデントの調査

- コンピュータ犯罪鑑識と悪意のあるコードの研究
- 情報安全インシデントの調査
- 独立した財務的および企業的調査

GROUP IB

グループIBのプロダクトとサービスの方向は互いに補完しあうため、さまざまな種類の脅威に対処する上で相乗効果が得られます。

Group-IB & AIG CyberEdge

サイバー犯罪から守り、保険するロシア初の統合的プロダクト

サイバー犯罪者は、マルウェアだけでなく、社会工学、欺瞞を使用し、従業員に賄賂をを使う場合もあります。AIGとの協力のおかげで、グループIBの顧客はそのような複雑な攻撃からも保護されます。

保険証書

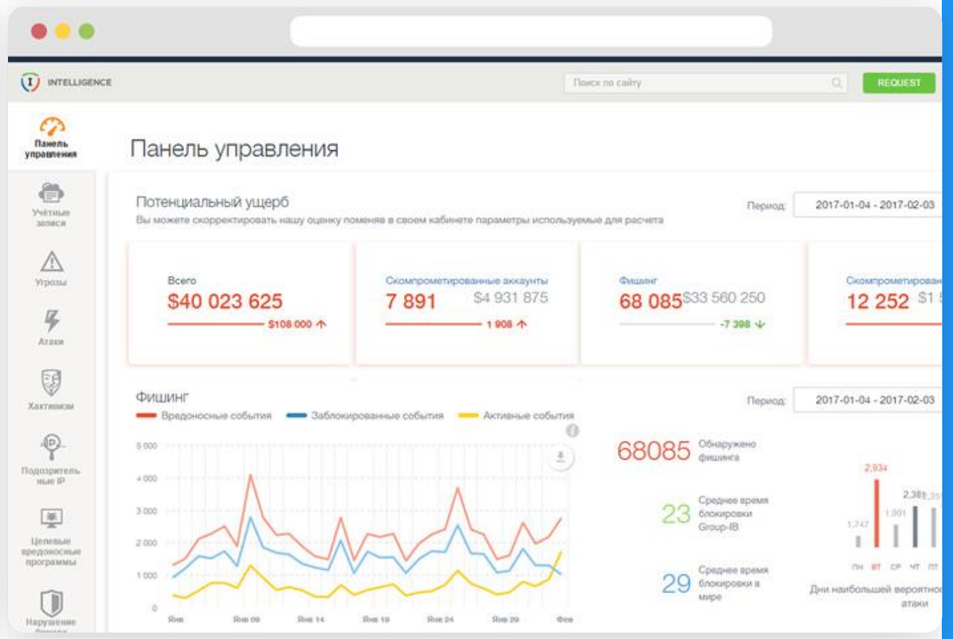
保険は何をカーバーしているか

- データ侵害による損失
- データに関連した管理的調査
- データ侵害対応のコスト

Threat Intelligence

企業、顧客、パートナーに対する脅威の監視、分析、予測

- 慎重なリスクアセスメントと脅威の優先順位付け用の戦略的情報
- 攻撃に準備するための作戦データと防御システムの調整
- インシデントレスポンスタイムを縮小する戦術的インジケータ



国産のソフトウェアの目録に入っている

Forrester Gartner IDC

Group-IBは、Gartner（2015年）とForrester（2017年）の分析機関によれば、世界で最も優れたThreat Intelligence提供企業の1つです。2017年、IDCエジェンシーはGroup-IBをサイバー脅威研究の市場リーダーとして認識しました。

早期警戒システム：

Threat Intelligence　TDS　Secure Bank　Secure Portal

GROUP-IB

- 攻撃と脅威についての迅速な通知
- あきらかなWebインターフェイス
- 関心のある分野でのハッカー活動の追跡、分析、予測
- 脅威レポート提供際、STIX / TAXIIのサポート
- 漏洩されたデータや識別子への直接アクセス
- 24時間サポート

Threat Intelligence利用結果

アナリストとインシデント対応チーム

Threat Intelligenceデータに基づく質的なインシデント優先順位付け
Incident Responseプロセスの迅速化
脅威の詳細なコンテキストに陥れること、潜在的に会社に関心のある犯罪グループの戦略やツールの理解

CEOとトップマネジメント

セキュリティシステム、インシデント対応チーム、アナリストへの投資のROIの最大化
経営上の決議に影響を与える脅威に関する情報の入手
企業のブランドを犯罪目的で使用するのを防ぎ、評判のリスクを減らす

CISO

サイバー脅威の進化の深い理解と貴社のセクターにおける事実上の攻撃の分析に基づいて情報セキュリティ戦略を構築する
当面の脅威から守るために技術的解決の慎重した選択
アナリストとインシデント対応チームの効率と能力を高める

MSSP

- 脅威のコンテキストを深く理解した上でクライアントにサービスを提供する
- クライアントに当面のある脅威に関するデータに基づいて、クライアントに対するオファーのより良いターゲティング
- グロバルThreat intelligenceデータに基づいて脅威の発展予測と対抗手段

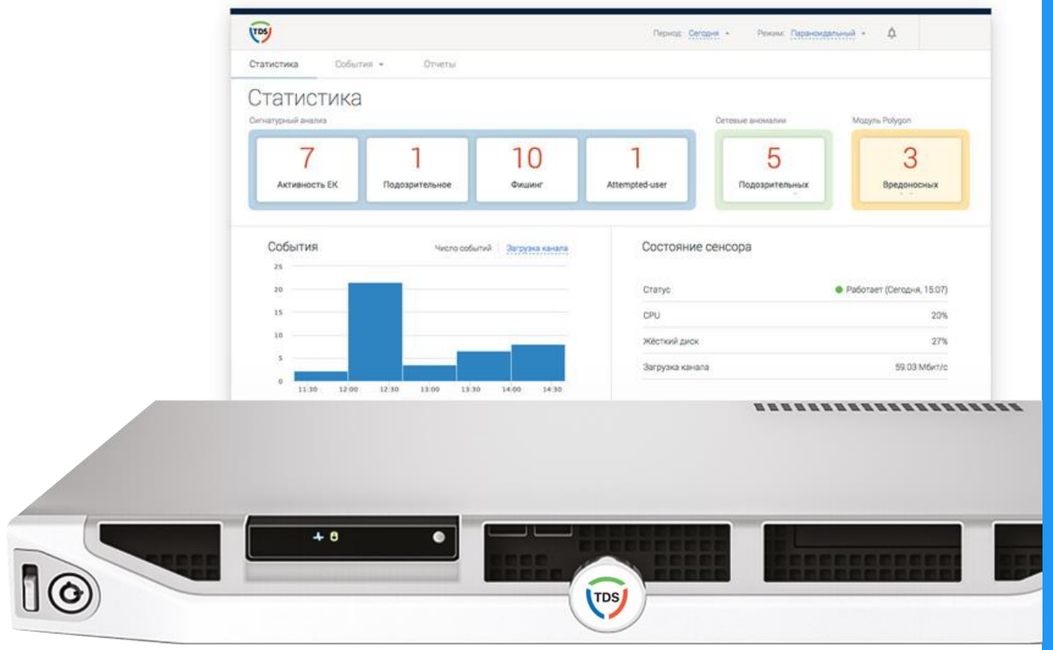
Group-IBのThreat Intelligence 貴社に以下の可能性を与える:

- ✓ インシデントへの応答時間を最小限まで短縮
- ✓ 新しいツールと攻撃方法の登場を追跡する
- ✓ 閉式のハッカーサイトからパーソナライズされたデータを受信する
- ✓ 会社の情報セキュリティに冠する選択された投資戦略の有効性の評価

TDS Sensor

TDS - ターゲットされた攻撃の検出

感染されたサイトを検出し、侵入、漏出、標的攻撃および産業スパイ行為を防止する



ターゲットとなる攻撃の詳細と世界中のさまざまな地域の犯罪グループの活動を深く理解することにより、以下のような、見えない脅威を発揮する:

- 望ましくないと危険なネットワークとの相互作用
- 危険な伝達渡されるオブジェクト
- スパイウェア
- リモート管理ツール
- 弱点を悪用しようとする試み

高精密の脅威検出用の独自のソースと作者のノウハウ:

1. 行動分析のアルゴリズム＋機械的学習
2. コンピュータ犯罪鑑識ラボからの攻撃に関する情報
3. グループIBのThreat Intelligenceシステムのデーター

GROUP-IB

すべての当面のおよび未知のマルウェアファミリーに対する即時通知

Wi-Fiネットワークで感染されたモバイルデバイスの特定

24時間サポートとアドバイス

使いやすいWebインターフェイスと明らかなルレポート。

グループIBの専門家によるログの手動分析と重大インシデントの選び出し

オブジェクトの危険度を識別するための定期的に更新された分類器

Polygon ー企業ネットワークにおける脅威検出器

Polygonは、TDSから受信したファイルをセキュリティループ内の安全な隔離環境で起動し、その動作を分析し、オブジェクトのハザードレベルについて客観的な結論を出します。

TDS Sensor + TDS Polygon

仮想マシンのファーム

疑わしいファイルは、お客様のビジネスと地域の特性に基づいてカスタマイズされたテスト環境で起動されます。

低レベルシステムモニタ

その存在を開示せずに、最低レベルでポリゴンは、安全な環境で起動されたときのオブジェクトの動作を監視します

定期的に更新される分類器

オブジェクトの危険性は、Machine Mindを使用して特定の規則性分類器で新しい情報を受信することによって決定されます。

電子メールの添付
ソーシャルエンジニアリングの使用に起因する悪意のあるファイル

ダウンロードされるファイル
バックグラウンドでユーザーおよび/またはそのコンピュータによってダウンロードされたオブジェクト

ターゲットとする攻撃
貴社のインフラストラクチャだけを対象とした悪意のあるソフトウェア

およびその他の
以前には知られていない- アンチウイルスおよびシグネチャベースのアプローチでは検出されない悪意のあるオブジェクト

TDSのしくみ

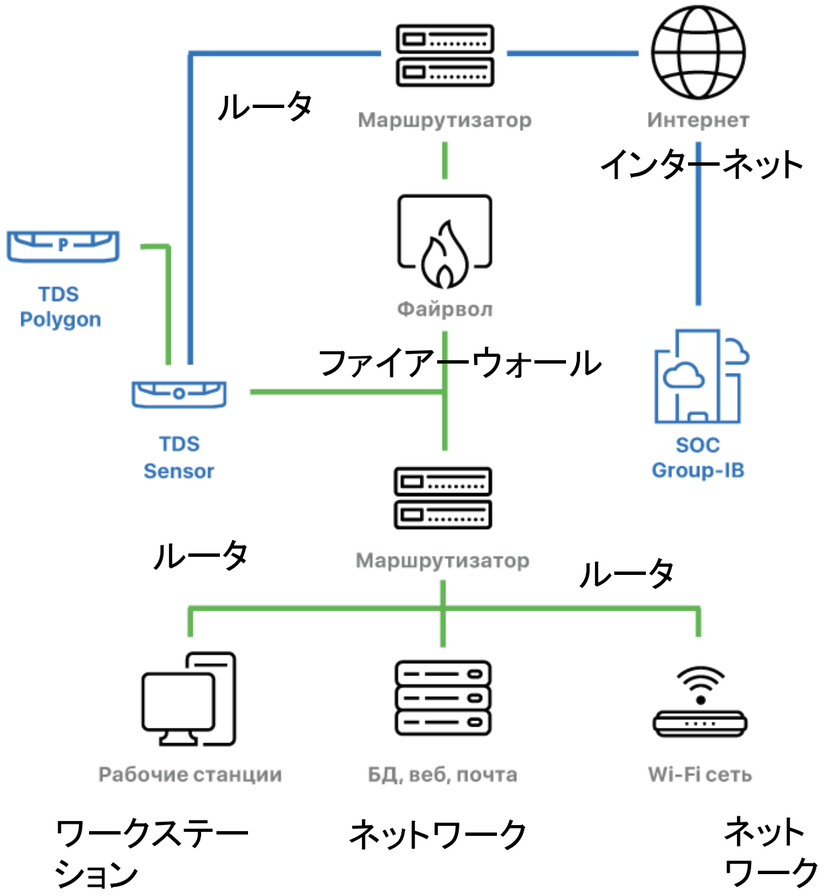
トラフィック分析センサー

独自の情報源からのデータに基づいて開発された悪意のある活動の兆候について、コマンドセンターとの相互作用を確立することによって、感染したサイトを検出します。

マシン学習アルゴリズムを使用してマルウェアによって生成されたネットワーク異常を検出します。

以前に未知の悪意のあるコードを検出するためのTDS Polygon行動分析システムト統合する。

検出されたインシデントに関する情報を、セキュリティ保護されたチャネルを通じてSOC Group-IBに、または情報セキュリティイベントを記録するための社内システムに送信します。



SOC GROUP-IB

- センサーから受け取ったインシデントに関する情報は、データ処理センタで分類され相関されます。
- ベントは、認定されたGroup-IBスペシャリストによって手動で分析されます。
- SOCの専門家は電話や電子メールで重要な脅威について貴社の専門家に通知し、すべての分析結果は便利なWebインターフェイスで利用できるようになります。

経験豊富なGroup-IBスペシャリストは重要なインシデントを発揮し、貴社のISサービスがレスポンスに集中できるようにします。

Secure Bank

支払いシステム用の詐欺の早期発見システム

リアルタイムですべてのデバイスおよびクライアントプラットフォームで銀行詐欺を積極的に検出

弊社のソリュション:

- ✔ 詐欺の早期発見による盗難を防止します。
- ✔ 偽陽性の反応処理と顧客の呼び出しのコストを削減します。
- ✔ オンラインおよびモバイルバンキングシステムのセキュリティと魅力を向上させます。
- ✔ 銀行の信頼性を強化し、顧客に感染や攻撃について警告する機会を与えます。

Secure Bank は国内ソフトウェアの登録簿に含まれています

Secure Bankは
“Sberbank Online”
を保護する

GROUP-IB

- 詐欺的な支払いとその準備を特定する
- 新しい攻撃と詐欺行為を検出する
- 規則とチェックサムの毎日の更新
- 分析サポートとアドバイス
- オンラインバンキングを保護するためのJavaScriptモジュール
- AndroidおよびiOS向けモバイルSDK
- クライアントデバイスにインストールは不要です

早期警戒システム: : Threat Intelligence TDS Secure Bank Secure Portal

Secure Bankの仕組み

Secure Bankは、銀行やモバイルバンキングアプリケーションのWebページと共にロードされ、クライアントにそのデバイスの感染または傷つけの可能性がある

か速やかに通知することができます。

システムは、悪意のあるWebインジェクション、ソーシャルエンジニアリング、フィッシング、ボットネットワーク、アカウント奪取、不正な現金引き出しネットワーク、および他の種類の銀行詐欺を検出します。

Secure Bankの反詐欺防止技術

- バイスのデジタルプリント
- ユーザーのグローバルプロファイル
- 先進的なルールビルダー
- 行動分析
- エージェントレスマルウェア検出
- クロスチャネル分析
- Group-IB Threat Intelligenceのデーター

Secure Bank использует расширенные средства обнаружения вредоносных программ и поведенческого анализа для выявления мошенничества до его возникновения

Secure Bankはマルウェア検出と行動分析のために、詐欺が発生する前に拡大された検出手段をりようする。

AF

Классические системы по противодействию мошенничеству анализируют транзакции, они не обнаруживают, заражено ли клиентское устройство вредоносным ПО, происходит ли что-то подозрительное на нём до совершения транзакции

クラシックの不正防止スキームはトランザクションを分析し、クライアントデバイスがマルウェアに感染しているかどうか、トランザクションが完了する前に疑わしいことが起こっているかどうかを検出しません。

1. Попытка совершения мошеннических действий
(запуск вредоносных программ, социальная инженерия, удалённый доступ)
不正行為を試みる（悪質なプログラムの起動、社会工学、リモートアクセス）

2. Совершение мошеннического платежа
詐欺支払を行う

3. Вывод денег
お金の引き出し

詐欺には数秒から数か月かかる場合があります

Мошенничество может занять от нескольких секунд до нескольких месяцев

早期警戒システム： Threat Intelligence TDS Secure Bank Secure Portal

すぐに使える銀行と統合されたインフラ

反詐欺伝統的システムが見えない脅威の発揮

支払い詐欺

- クレジットの詐欺
- CNP操作との詐欺
- 3悪意のあるWebインジェクション

Secure Bank は、電子決済と顧客のクレジットカード情報を保護するのに役立ちます。

個人データーの盗難

- アカウントキャプチャ
- アカウントを開くとの詐欺
- ボットのアクション

行動分析システムとデバイスのデジタル “フィンガープリント”テクノロジを使用すると、盗まれた登録報の使用状況を追跡できます。

社会工学

- 詐欺的な郵送
- 標的型攻撃
- フィッシング

単一のクライアントプロファイルを作成し、Group-IB Threat Intelligence（脅威インテリジェンス）データを使用すると、データ漏洩やネットワーク詐欺を防ぐことができます。

マネーロンダリング

- 違法な現金引き出しネットワーク
- 脱税スキーム

アカウントと他の銀行組織との間のやりとりを分析することで、不審な取引を特定することができます。

悪意のあるプログラム

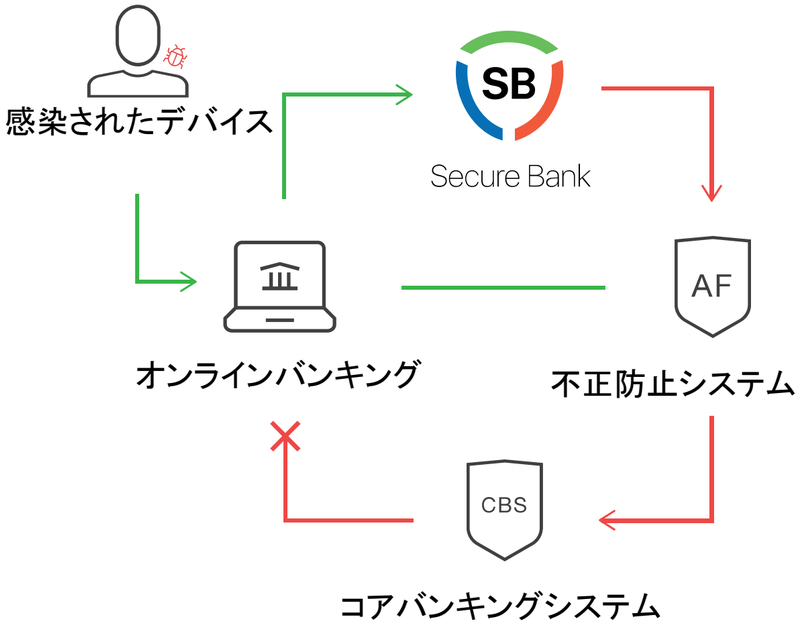
- ロイの木馬
- ファーミング
- ボットネット

特許を取得したSecure Bankのアルゴリズムは、クライアント側に追加のプログラムをインストールすることなく、銀行のトロイの木馬を明らかにします。

クロスチャネル攻撃クロスクライアント攻撃

- 電子商取引
- モバイルデバイス
- ウェブインターフェース

Secure Bankは、オンライン小売店や企業ポータルを含むすべてのモバイルおよびWebプラットフォーム上の顧客を保護します。

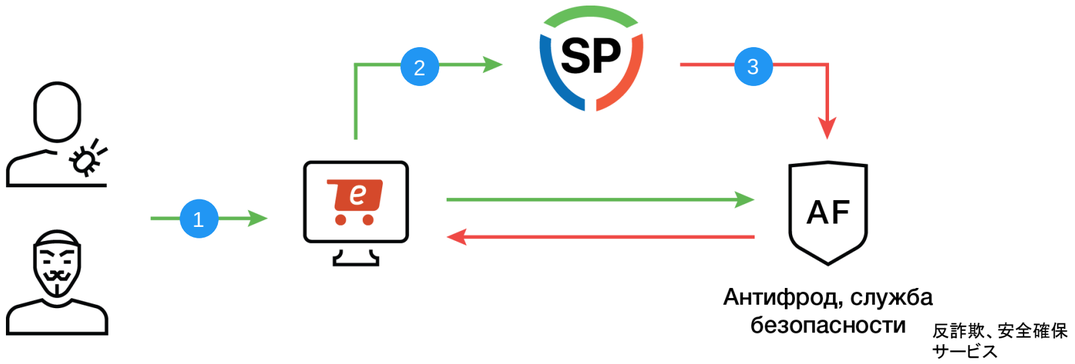


早期警戒システム： Threat Intelligence TDS Secure Bank Secure Portal

Secure Portal

詐欺の早期発見システムはユーザの側（最も弱点）で
インターネットポータルのセキュリティを確保する

国内ソフトウェアの登録に含まれる



1. ポータルページのJavaScriptモジュールは、クライアントデバイスの“プリント”を定義し、不正行為のインジケータを収集します。
2. 個性を欠いたデータは、セキュアなチャネルを介してSPに送信され、そこではThreat　Intelligenceシステムのデータを使用して処理されます。
3. 顧客はリアルタイムで詐欺について通知され、APIを使用してインシデントへの対応を自動化することができます

このソリューションにより、以下防止：

- 企業ポータルへのボーナスポイントへの第三者の不正なアクセス
- パスワードの選択、不正な投票増加、偽のレビューの配置
- 有で有料の定期購入の使用
- ポータルページに競合他社の広告を表示してバイヤーを傍受する
-

GROUP-IB

- 個人情報や銀行カード情報の盗難防止
- 盗まれたカードでの購入を識別します
- ボットの使用を防ぎます
- ポータルのITインフラストラクチャに投資する必要はありません
- 不正防止システム、SIEM、ファイアウォール、EPSと統合用のAPI
- 分析サポートとアドバイス

情報セキュリティ監査

私たちは、最大規模の銀行や有望な新興企業、エネルギー大手、小規模法律事務所と協力して、規模と目的のITインフラストラクチャの弱点を理解しています。

- 追加のバンキングシサービスステムとモバイルバンキングアプリケーション
- DoS / DDoS攻撃の防止、負担テストの実施
- 切り替えの正しさ
  電気通信オペレーターの信号ネットワークの切り替えの正しさ
- 企業/国家のポータル、eコマースサイトなどのWebリソース
- 社会技術試験（ソーシャルエンジニアリング）
- ネットワークインフラストラクチャの弱点スキャン
- iOS、Android、Windows Phoneなどのソフトウェア
- POS、mPOSターミナルのセキュリティ研究
- 商業秘密および個人データ保護システム
- 自動プロセス制御システムおよびSCADAシステム用ソフトウェア

グループIBによる情報セキュリティ監査：

- 々は10年以上にわたって弱点を分析している
- 貴社システムの操作内部ロジックに深く陥れる
- 他の方が見えないリスクを発揮する
- 各レポートには、決議を取る方向けの簡単な要約とならんで専門家用の詳細な説明と具体的な助言が含まれています

Compromise Assessment

侵害の跡形とハッカーの攻撃の準備の兆候の発揮。

Compromise Assessment ハッカーの攻撃の準備の跡形、データの侵害の兆候、破損の程度の評価の助けとなり、どのシステムが攻撃されたのか、そしてどのように起こったのかを確認します。

グループIBの専門家は実際の被害を受ける前に潜在的な脅威を明らかにする

Compromise Assessment 枠内でGroup-IBの専門家はTDSソフトウェアとハードウェアをインストールし、何百もの調査をしている専門家がインフラストラクチャと検出された侵害の兆候を分析します。

Compromise Assessmentの結果:

1. **侵害の報告**
   侵害の報告
   インフラストラクチャの侵害の時系列の記述、侵入者の行動の詳細な分析
2. **実行された作業についての報告**
   Compromise Assessment の各段階での作業範囲と結果の詳細な説明
3. **勧告**
   将来の攻撃を防ぐためにインフラストラクチャをアップグレードするための勧告
4. **経営者への報告**
   インフラストラクチャチェックの主な結果を説明する簡単なレポート

コンピュータフォレンジックの専門家が主要インフラストラクチャの要素を侵害がないかチェックする

- 独自のフォレンジックな自己開発ツールと独自のThreat Intelligenceデータを使用する
- .主要インフラストラクチャ・ノードの検査:ドメイン・コントローラ、処理、支払いゲートウェイなど
- 定期的なインシデントを防ぐためにインフラストラクチャの侵害の年表を復元する

TDSコンプレックスは、未知の「ターゲットサイバー攻撃の以前の兆候」を発揮するのに役立ちます。

- TDS Sensor がネットワークの異常や感染、異常なデバイスの動作ををを検出する
- TDS Polygonは、潜在的に危険なオブジェクトを独立した環境で起動し、オブジェクトの動作を分析し、その危険度を判断します。
- 識別されたすべてのイベントは、専門家によって24時間体制で分析されます。

あなたは何ヶ月も隠された脅威を見えないことは可能である。

ターゲット攻撃の準備

ハッカーは数ヶ月間攻撃するためにインフラストラクチャを展開して- あなたが気付かない

合併および買収

別のビジネスとの統合により、ブックマーク、バックドア、CVEなどのリスクがある

不道徳な競合企業

営業秘密へのアクセスを得ることで、競合他社は市場での優位性を確保する

内部者または解雇された従業員

同社のインフラストラクチャーがどのように機能しているかを知ると、彼らは静かにデータを「マージ」し、長い間気づかれないままです。

Red Teaming

ターゲットとする攻撃を定期的に模倣してセキュリティサービスを強化する。
貴社のセキュリティチームを含む本格的な訓練は、以下の質問に答えます：

- ✔ 貴社のシステムはインシデントを効果的に防止、検出、対応する準備ができていますか？
- ✔ ターゲットとする攻撃中にセキュリティ担当者はどのように行動しますか？
- ✔ 攻撃に耐える企業の能力を高めるためにセキュリティアプローチで正確に何を変更する必要がありますか？

Red Teamingは、攻撃の定期的な模倣の結果として、目的型攻撃の準備をし、新しい弱点を特定して排除し、チームを鍛え、実際の脅威に対抗プロセスを改善しています。

Red Teamingの結果:

•経営者向けの簡単なレポート

• セキュリティシステムを改善するための詳細な結果レポートと専門家への勧告重

•大な弱点を検出した場合の緊急警報

Red Teaming Methodology:

目的の合意、ツールの選択 → 数ヶ月間に渡って：セキュリティ部門の責任者のみが警告された目的型攻撃の定期的なイミテション → 新たな攻撃の対象となるインフラストラクチャの変化を常時監視します。

Red Teamingは時間に制限はありません。この無制限のアプローチにより、Red Teamingは、さまざまなツールや攻撃方法を試すことによって何ヵ月も攻撃を準備できる実際の攻撃者の行動モデルに近づくことは可能になる。

Red Teamingという用語は軍事から来たもので、運動中は赤チームが攻撃している、青は自らを守る。

Brand Protection

インターネット上のブランドに対する脅威を特定し、除去するための技術サービス。
当面のオンライン脅威による企業の損失や評判の損失を防止します：

- ブランドとオンライン詐欺の不正使用
- 偽造品の拡散とアフィリエイトポリシーへの違反
- 情報攻撃と否定的なレビュー

違反を発見するための先進的な技術：

Machine learning
システムは以前の経験に基づいて違反格付けを独自に認定します。

Big data
ビッグデータ分析技術は、ソーシャルネットワーク内のサイト間やグループ間のリンクを自動的に検出します。

Intelligence driven
サイバー犯罪調査で使用されているグループIBの技術による、違反者との直接なコンタクトが結ばれる

3 百万のリソースは
自動的に24時間追跡される

1万の
違反が、毎日解消される

85%の違反は
プレ審判で廃止される

危険なサイトのクイックロック

ルネット外での対応能力

24時間監視

デジタル証拠収集

詐欺サイト間のリンクを特定する

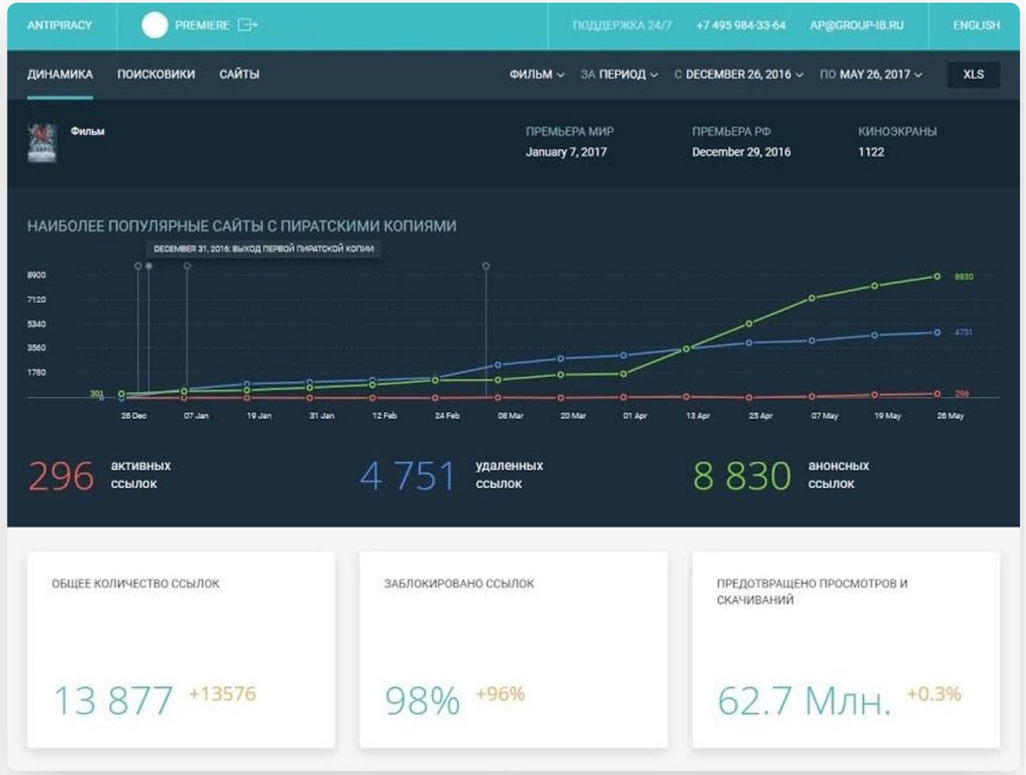
再発防止

防止:
安全監査 Compromise Assessment | Red Teaming | Brand Protection | Anti-Piracy

Anti-Piracy

デジタルコンテンツスマート保護市場のリーダー

- vk.ru、veterok.tv、kinostock.tvを含む120,000以上のリソースを監視する
- 海賊サイトの司法遮断の成功例
- 大規模な海賊サイトでのオンラインコンテンツのブロック
- ユーザーを貴社の公式リソースにリダイレクトする



30 分で

大幅な変更があっても、弊社は海賊のコンテンツを見つける、

24 時間で

最大のルネット海賊サイトでコンテンツの配信を停止する

7 日で

貴社のコンテンツへのリンクを99%までブロックし、ネゴし難いサイトとの解決策を提供します

- ブロッキングの正確的取りまとめ
- 通知による高い結果
- 直感的に理解できるインターフェイス
- 24時間監視
- 広範囲の裁判前の措置
- 「ワンボタン」で 海賊コンテンツの削除

CERT-GIBの反応センター

CERT-GIB (Computer Emergency Response Team) —
24時間の情報セキュリティインシデント対応センター

- 我々は、フィッシングリソースの出現、マルウェアの拡散、侵害製品の売買を監視する
- ドメイン.RU、.PФ、および1000を超えるドメインゾーンで危険なサイトをすばやくブロックする
- 私たちは、すべての対応と調査の段階で完全な法的サポートを提供しています。
- パートナーネットワーク、ホスティングプロバイダ、ドメイン名レジストラとの接触を通じて弊社は世界中で仕事をしている。

Ростех

ロシア最大のロシア企業の1つであるロステックは、独自のCERT RT-Informを作成するためにグループIBをパートナーとして選択した

インターネットの全国的領域のコーディネーションセンターとインターネット開発基金の権力組織である

FIRSTとTrusted Introducerの国際社会の認定メンバー

IMPACTのパートナー - サイバー脅威に対抗する国際的なパートナーシップ

カーネギー大学の認可を受け、正式にCERTの商標を使用します。

コンピュータフォレンジックの研究室と調査局

コンピュータフォレンジックと悪意のあるコード分析用の東ヨーロッパで最大の研究所。

最先端の装置と高度なウイルス解析
トレースを隠す技術を迂回できる世界最高の開発

法執行機関との相互作用
実施検索活動の公式参加を含む

あらゆる情報メディア上のデータを検索する
データが削除、非表示、または暗号化されていても、そのデータが検索されます

モバイル対応チーム
現場でのデジタル証拠の収集と調査、その結果を排除する勧告

80% ロシアの反響のあるハイテク犯罪は、当社の専門家の参加により調査されます

それぞれに個別のアプローチを見つける
専門家チーム:「 E-Discovery とフォレンジック」から法人法律
まで

撤回された資産が返還される経験があります。
ある捜査の結果、被害会社に33億ルーブルを返還された

サイバー犯罪の経済を理解する
Threat Intelligence
専有情報を使って資金フローチェーンを復元

弁護士、捜査官、検察官にアドバイスする
調査のすべての段階で相談が可能です。

GROUP IB

- コンピュータと技術の鑑識
- デジタル証拠を裁判所で発表する豊富な経験
- デジタル証拠の収集
- マルウェア調査
- アウトソーシングと独立した鑑識
- 犯罪鑑識研究

PRE-IR ASSESSMENT

情報セキュリティインシデントへの効果的な対応を準備する。

Pre-IR Assessment（事前IRアセスメント）は、システム、チーム、プロセスが対応に、事件が発生した場合に明確な計画を立てる準備ができているかどうかを確認するのに役立ちます。

典型的な問題

- 大量のデータが失われたり、ログに誤りがあります。
- インシデントはパニックとコントロールされない行動を引き起こす
- 応答プロセスはデバッグされず、役割は分散されません

Pre-IR Assessmentの結果

- インシデントに効果的に対応するためのシステムのセットアップに関する勧告
- 自信と確立された行動計画
- 局間のコミュニケーションの確立

主要コンポーネントの包括的な評価

1 技術

ネットワークとシステムインフラストラクチャの**検証** - デジタル証拠を完全かつ正確に収集する能力、侵害の兆候を検出する能力、迅速にインシデントを停止し、応答中にネットワークを管理する準備ができている。

その**結果**、スクリプトの実行、さまざまな種類のインシデントに必要なデータの検索と収集といった、実際のシステム上でのプロセスの開発が行われます。

2 人物

ITサービスの従業員の能力と情報セキュリティの検証 その**結果**、グループIBの専門家が2日間のインシデント対応トレーニングを行い、訓練されたチームが自信を持つようになる。

3 規制

規制と文書の完全性、関連性、実用性の**検証**。

その**結果**、実際にインシデントが発生した場合に役立つ規則と文書が作成されます。

4 構成

チームの責任と組織構造の分配を**調査**する。
その**結果**は、インシデントへの対応中に様々な部署の調整とチームワークが行われます。

Pre-IR Assessmentはどう行っているか

準備

- 情報の収集
- 特定のクライアントおよび業界向けのプログラムの適応
- 検証規則の承認
- 期間の合意

プロセス

- グループIBの専門家が顧客の会社へ出張する
- 異なるインシデントの典型的なデータの問い合わせ
- 完全性、可用性、データ取得率と速度の分析
- インシデント対応のトレーニングの実施

結論

- 果的な対応のためのシステムの設定に関する勧告
- 構造とプロセスの最適化
- 対応計画
- 出来た規制
- 訓練されたチーム

弊社は2003年からサイバー犯罪の防止と調査を行っています。

www.group-ib.ru
info@group-ib.ru
twitter.com/groupib
t.me/group_ib
group-ib.ru/blog
+7 495 984 33 64
facebook.com/group-ib
instagram.com/group_ib