SIMってなぁに？

ふたぎ　まさあき

日本 Snort Users Group

Open Source Conference 2005

自己紹介

- ふたぎ　まさあき
  - 17年間のプログラマー歴 (Z80/8*86/680?0 assembler, C, C++,Java.....)
  - FreeBSDベースのファイアウォールを開発
  - いまはなき FWDの残党・・・・ (笑)
  - もともと国産 (自分で作るぞ！) 主義者だが、なぜか現在は敵情視察に入った商社系で海外製品日本進出の手引きをしている・・・
    - ミイラ取りが・・・・・かもしれない

今日のお題

- SIM (Security Information Management)
  - セキュリティについての情報を一括管理・監視しようという極めて「あたりまえ」の考え方
  - SOC (セキュリティオペレーションセンタ) での監視業務の効率化が目的
  - でも、現実には難しい問題が多い・・・・

氾濫する「セキュリティ」機器・製品

- ファイアウォール
- IDS
- IPS
- アンチ・ウイルス
- 認証、リモート接続
- 暗号化
- ログ管理
- ポリシー管理、強制

集中監視と簡単に言うが

- 管理方法、アラームやログの書式は各社各様
  - 大手メーカーによる囲い込み戦略
    - 独自仕様の押しつけ！？‥‥
  - 新興ベンチャーによる新分野の開拓
    - セキュリティイベント、アラームのカテゴリーの増加
  - ＳＯＣに、「似て非なる」監視コンソールが乱立するハメに
- 監視機構のマルチベンダ対応が望まれるのだが
  - とりあえず格納･表示するならば簡単だが‥
  - でも、それじゃ、syslogサーバのログを眺めてるのと何もかわらない
  - すべての機器を統一的な方法で監視できないものか･･･

SIMの機能と役割

- マルチベンダ機器の集中監視
  - ログやアラームの収集と書式の正規化
    - 同種の機器のログやアラームに含まれる内容はほぼ共通。最大公約数的な共通フォーマットに変換
    - アラームやログのカテゴライズ（同種のアラームやログをグループ化）
- リアルタイムな自動解析
  - 複数イベントの関連性（相関性：correlation）をチェック
  - ログやアラーム発生状況に関するアノマリー（異常）の発見
  - 監視下にあるネットワーク全体での事象の把握と本当に対応が必要なアラームの識別（全体としてのfalse positivesの軽減）
- インシデント対応の管理
  - トラブルチケットの管理、対応者による情報共有の機能
- 総合的なレポーティング
  - 傾向の掌握（多拠点観測）
  - マネジメント層や顧客に対しての総合的な報告提供

ルールによる関連づけ

- **複数のイベントから、真の原因を特定したり深刻さを判断する**

クラッカーによる攻撃手順の例と発生する可能性のあるイベント

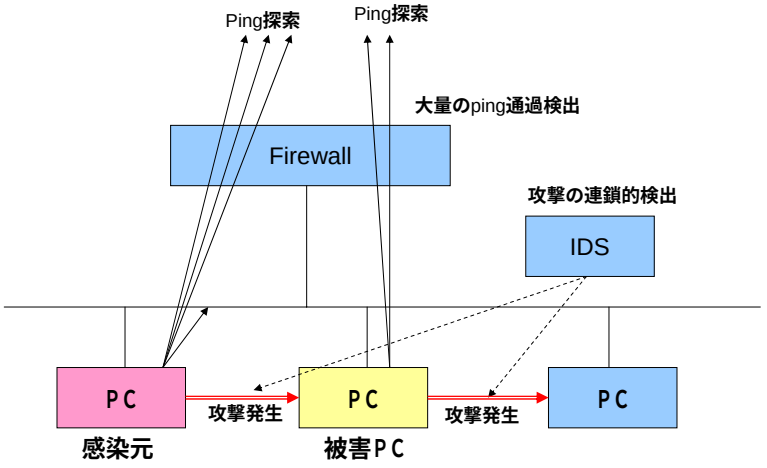
STEP1: ポートスキャン → IDS のアラーム、ファイアウォールでの連続したログの発生

STEP2: 脆弱性を攻撃 → IDSのアラーム

STEP3: 攻撃成功 → サーバからの Accept ログ発生もしくは、一定時間内にログが発生しないなどの状況

STEP4: バックドア設置など → サーバから外部に向けた不審な通信の発生

ワームの侵入検知



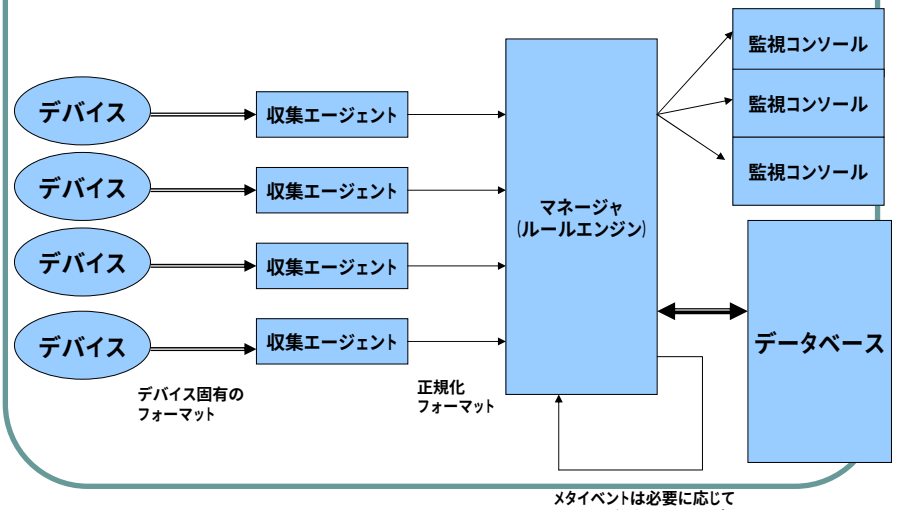
サーバ不正使用可能性の検知

- 同時ログイン（ID盗用の可能性）
  - 物理的に離れた位置にあるサーバに短時間で同じIDによるコンソールからのログインが試みられたようなケース
- 入退室管理システムとの連携
  - 入室していない人のIDを使用したログインの検知（ID盗用の可能性もしくはポリシー違反）
  - 内部にいるはずの人のIDによるリモートアクセスの利用（ID盗用の可能性もしくはポリシー違反）

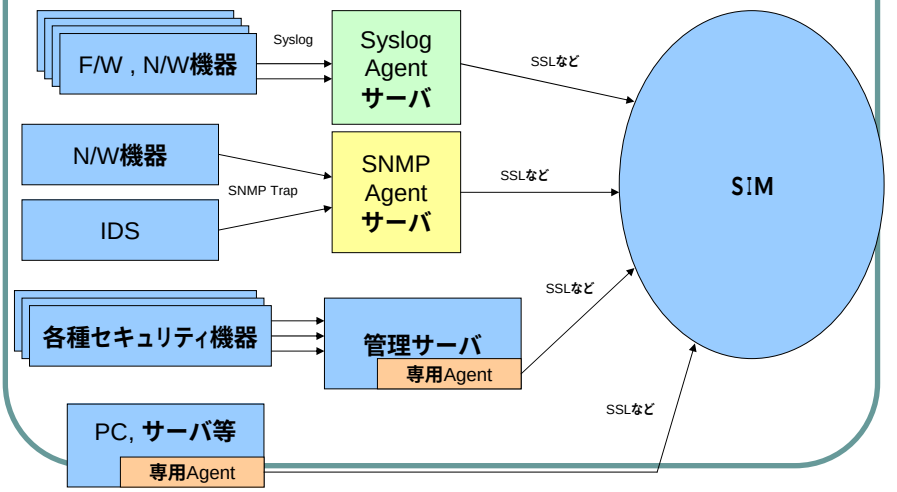
Meta IDS としての SIM

- ネットワーク全体に対する監視と不審な兆候の検出
  - 特定の部分を監視するIDS（点）に対して、ネットワーク全体（面）を時系列的に（時間軸に沿って）監視するもの。
  - 個々の事象から、その本質を見つけ出す（Intrusion Detection というよりも Incident Detectionなのかもしれない）

SIMの構成



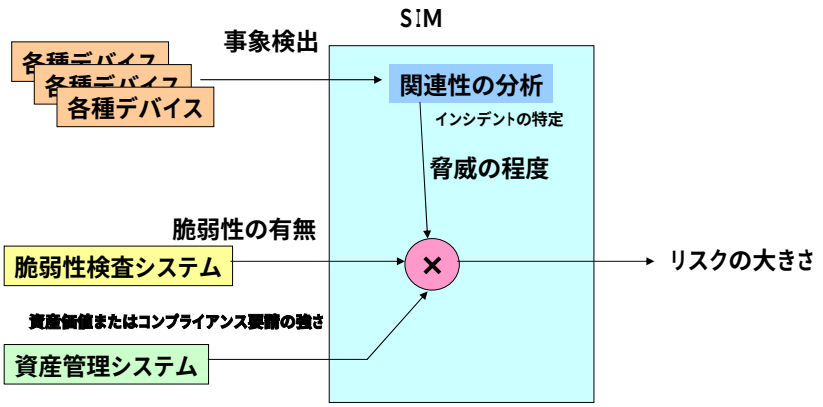
ログ、アラームの収集方法



SIMの可能性

- リアルタイムなリスク評価
  - 資産管理システムとの連携による攻撃対象の価値の認識（たとえば、個人情報を格納したサーバなどでは、コンプライアンス違反の可能性もリスク評価に加えられるべき）
  - スキャナなどとの連携による脆弱性の評価
  - 複数イベントの関連性評価を元にした脅威の度合いの評価
- リスク＝脅威×脆弱性×攻撃対象の価値

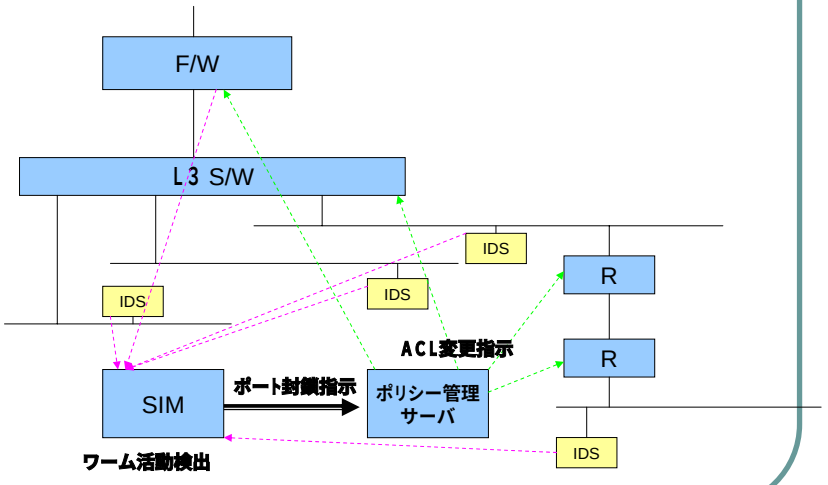
リアルタイムなリスク評価



SIMの可能性

- Meta IPS（ネットワーク防衛システム）への可能性
  - インシデントの検知→ネットワーク全体での自己防御
  - 完全阻止よりもむしろ、影響緩和または拡大防止（個々の防御はIPSなどにまかせて）
  - たとえば、ワーム侵入の検知→コアスイッチでの特定サービス通過禁止
- ネットワーク全体のポリシーを管理するようなシステムとの連携
  - サービスのフィルタリング
  - セグメントの隔離
  - 帯域の制限

ネットワーク防衛システム



SIMの使い方

- SOCオペレーションの効率化
  - マルチベンダ機器監視の統合
  - 「マニュアル」化できる作業の自動化
  - エキスパートによる解析作業の効率化
  - リスクの的確な把握によるインシデントレスポンスの迅速化
  - 緊急時の初動の自動化

完全自動化はまだ難しい点に留意：最終的な判断は人間の仕事
将来的にはA･I化できる？？？

SIMとNMS

- よく似た切り口なので統合も考えられる
  - Network の Availabilityも重要なセキュリティ要素
  - NMSにSIMをプラグイン？？？
- 統合よりも連携の方向が好ましいかもしれない
  - 「ネットワーク屋」と「セキュリティ屋」のカルチャーの違い（時として反目しがち）
    - 互いに独立させて牽制関係においたほうがいい
  - 監視･対応する視点、優先順位の違い
    - （極論だが）たとえばある機器が落ちたときに、復旧を優先するか原因究明を優先するか･･･（どちらも大事）
  - システム相互に情報を交換できるようなインターフェイスの標準化が望まれる（SNMP/MIBだけではちょっと弱い･･･）

OpenSourceなSIM (OSSIM)

- http://www.ossim.net/
- 最新版は 0.9.8rc2　Linux上で動作
- SIMとして必要な機能ほぼ網羅
  - 関連性 (相関) 分析機能
  - リスク分析機能
  - 脆弱性スキャナ連携
  - レポーティング
- 中小規模サイト向け
  - 商用SIMは高機能だが高い・・・ (大企業、大規模MSSP向け)
  - 大規模用途には現状では不向きかも (DBMSの制約)
  - 商用SIMと組み合わせた階層構成ができるかも・・・
    - 拠点はOSSIM、本社に商用SIM…

ご清聴ありがとうございました

- 参考資料
  - N+Iネットワークガイド　2005年2月号特集記事
  - 商用SIMサイト
    - http://www.arcsight.com/
    - http://www.esecurityinc.com/
    - http://www.netforensics.com/
- 資料は以下のサイトから
  - http://www.kazamidori.jp/SECURITY/osc2005.pdf

2005/3/26 ふたぎ　まさあき