SecHack365

Cloud Incidentalis

クラウドセキュリティを自主学習するためのプラットフォーム

学習駆動コース　社会実装ゼミ　森　悠仁

Cloud Incidentalisとは

●**クラウドセキュリティ**を学ぶときの
●**自主学習**の障壁を和らげながら
●**攻撃**と**防御**をどっちもやるプラットフォーム

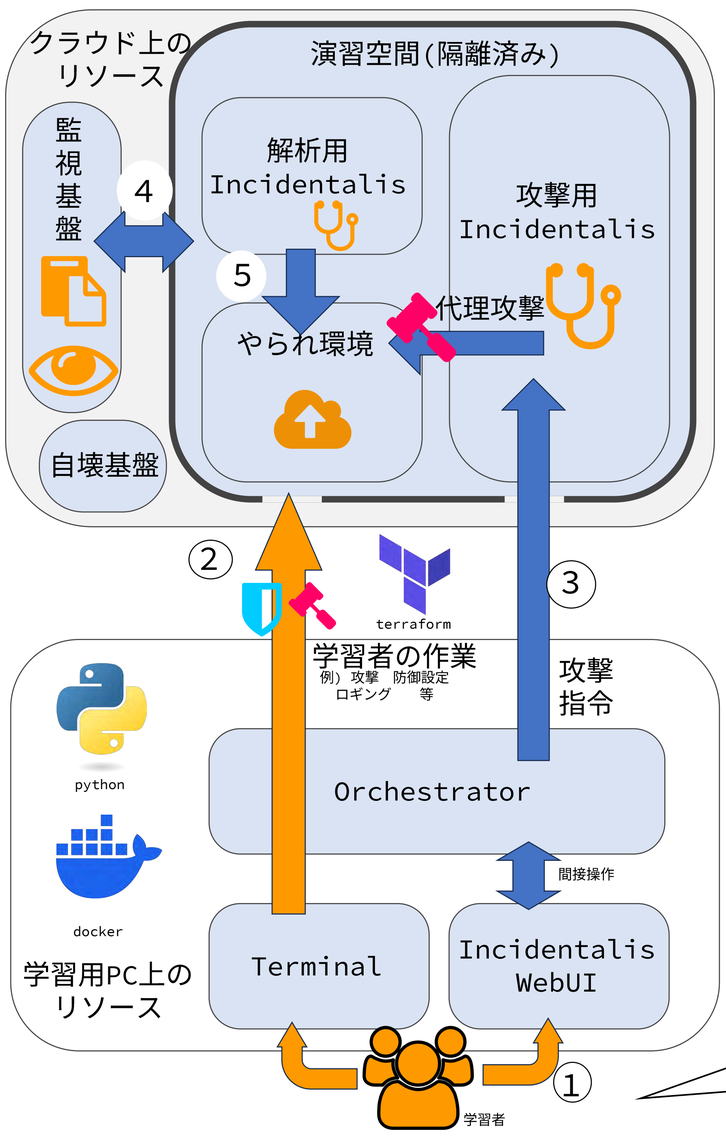
→**地に足ついたセキュリティ力**を身に着ける

既存のクラウドセキュリティの学習
- 攻撃して攻撃手法を学んだ。
- ログ見てインシデント対応を行った。

「で、私のサービスをどう守るの?」

- ベストプラクティスやログ設定の構成例は転がっているが、実際には「やってみないと分からない部分」がある。
- ただ手を動かすだけでなく、試行錯誤できるようにした。

Cloud Incidentalisの構成



Plan
やられ環境を分析して
攻撃と**防御**の両視点で
何が良いか**考える**

Do
やられ環境に対して
防御・**ロギング**を
設定・強化する

Check
Incidentalisが攻撃し
分析者の視点から
侵害後分析を行う

Action
防御者の視点に戻り
ロギング・検知強化
脆弱性の**修正**・**改善**

**反復演習による
実験・定着で
包括的に技術を獲得する**

環境構築時
ユーザーは
クラウドを
触らない

ベンチマーク
学習目的であり
**攻撃ツール
ではない**

学習開始の促進

● 環境構築の軽減
ユーザ環境の差異やクラウドベンダーの仕様変更に伴うドキュメントの老朽化等が影響し、自主学習用の**環境構築**には随分手間がかかるため、少なくない**初学者が挫折**してしまう。
Cloud Incidentalisを用いた環境構築が要求するのは**DockerとPythonだけ**。スムーズに学習に取り組める。

● 学習費用の軽減
クラウドセキュリティの学習を始めたい初学者が、高価な研修サービスや月額会員制ハンズオンプラットフォームにお金を払うのには障壁が大きい。下記の学習補助機能の一部を除き、**お小遣いレベルのコスト感**で学習を開始できる。

学習補助機能の3つの柱

● self exploit機能
自主学習の最大の障壁は自己評価の難しさ。
学習者は目標の達成度を自分で測ることができない。
self exploit機能により、現状のセキュリティ上の課題を確認できるため、学習上の**到達度**を確認できる。

● インシデント解析機能
自主学習の障壁の二つ目は有用情報の識別。
学習者はどんな情報を収集すればいいかを判断できない。
self exploit結果をLLMにより分析することで、
未知のセキュリティホールの**見落としを防止**できる。
何を守ればよいかが明確になれば、学習者は**自走**できる。

● ロールバック
演習中に演習環境がめちゃくちゃになってしまうことがあるが、学習者は演習環境を自分では戻せない。
演習環境の操作はシステムによって**全て記録**されているので、学習者は自由なタイミングで**巻き戻し**ができる。

自身のセキュリティ対策

● 通信の遮断
学習環境は脆弱なので外部から攻撃を受けることがあるため、**学習環境自体を防御**する機能がある。
また、内部の攻撃が漏れないように**フィルター**する機能がある。

● 自壊システム
学習環境は様々な要因で放置されがちであり、セキュリティホールになる。
学悪用され攻撃の踏み台にされ**過剰な課金が起こらない**ように、システムは一定時間で**自滅する**ようになっている

SecHack365での一年

6月： AIによるインシデントハンドリング自動化
Active Incidentalis

8月： セキュリティ・キャンプ全国大会(開発Zチュータ)
プログラム難読化/解析,OffSecツール/AI agent開発
- AI駆動ツールではこれが重要
  - 手足となるMCPの性能があること
  - 無意味なMCPが取り除かれていること

9月： AIを鍛えるにはサンドボックス環境が必須
ActiveLearn Incidentalis

やられ環境は
模擬オンプレ

勉強会で使用
↓
反響が良かったのでk
教育に方向転換

11月： サンドボックス環境をCloudに特化
Cloud Incidentalis
クラウドにシフトし、学習環境に舵を完全に切った

1月:学習機能の強化
初期のActive Incidentalisを学習補助として搭載
学習教材としてのセキュリティを確保するよう動いた

検証：ケーススタディ

● 方法
AWSの機能を用いた研究を行うが、本格的なサービスの開発経験はない、**情報工学を専攻する大学生**3人を対象にに5段階評価と自由筆記のアンケート調査を行った。
初めに、被験者のAWS知識の均一化のため、AWSの概要に関する基本説明を30分程度行った。
続けて被験者には以下の三通り体験してもらった。

1. Cloud Incidentalisを用いてシナリオを遂行した。
2. AWS CIRTのSecurity Workshop[1]を遂行した。
3. 1,2の**両方**を遂行した。

● ユーザ評価
インタフェースに関する満足度は**やや高**。
内容の理解しやすさは、AWS Workshopと同じ程度。
AWS Workshopより**取るべき情報が理解しやすい**と思った。
初回アクセスまでの方法がイメージしづらいと思った。

まとめ・今後

● システム
クラウドセキュリティを丸ごと自主学習するためのツールを作成した。学習対象は、クラウド上の攻撃、ログ収集、防御。
学習を効率的に継続するために、self exploit機能とユーザーのexploit行動を解析する機能を作成した。

● 分析
本システムにより、学習者は自主学習を加速させられるようになった。既存の学習システムと同程度の理解感に加え、学習目標の達成に関する困難を軽減した。
初回アクセス時のユーザ体験と難易度の高さと、自主学習の継続についてはまだ課題がある。

● 残課題
Incidentalisの攻撃システムは大きく制限して公開している。悪用可能性を減らして公開しより良い自主学習を提供したい。
具体的な脅威シナリオを用意し、より現実的なセキュリティ学習を提供することを目指す。

クラウドベンダによる
ワークショップ

攻撃シミュレート用
攻撃ツール

Related Works
[1]AWS Workshop – Security (https://workshops.aws/categories/Security)
[2]Sadcloud (https://github.com/nccgroup/sadcloud)
[3]Stratus Red Team (https://github.com/DataDog/stratus-red-team)
[4]Atomic Red Team (https://github.com/redcanaryco/atomic-red-team)

謝辞・引用
ケーススタディはJAWS-UG (AWS User Group – Japan) の桑原 大輔 さんの支援のもと
ご協力いただいた被験者の皆さんに実施しました。
様々な助言をくださった各社のエンジニアの皆さんやSecHack365のトレーナー、アシスタントの方々に多大なる感謝を申し上げます。

[1] https://catalog.workshops.aws/aws-cirt-ransomware-simulation-and-detection/en-US

NICT National Institute of Information and Communications Technology