MWS Cup 2025
DFIR+OFFENSIVE

CODE：PostMeeting

MWS Cup 2025
DFIR+Offensive作問チーム
遠藤 行人

目次

- 今年の出題について
- 競技結果
- アンケート結果と分析
- 振り返りと来年度に向けて
- まとめ

作問メンバー

- ソリトンシステムズ
  - 荒木 粧子
  - 尾曲 晃忠
  - 後藤 公太
  - 西井 雅人
  - 近藤 龍一
  - 伊神 和馬
  - 白鳥 隆史
- ラック
  - 天笠 智哉
- 日立製作所
  - 鬼頭 哲郎
- 日立システムズ
  - 関谷 信吾
- エヌ・エフ・ラボラトリーズ
  - 保要 隆明
  - 市岡 秀一
- NTT西日本
  - 前 竜郎
  - 高田 知弥
- NTTセキュリティ・ジャパン
  - 大倉 有喜
  - 戸祭 隆行
- NTTドコモビジネス
  - 遠藤 行人
  - 阿部 航太
  - 大森 敬仁
  - 高木 泉希
  - 密 行成

今年の出題について

あらすじ

- Eden・Collegeは、学問、スポーツ、芸術など様々な分野において優れた学生が集まる小中高一貫の国を代表する学校である。そのため、国を代表する著名人の子息も多く在学している。

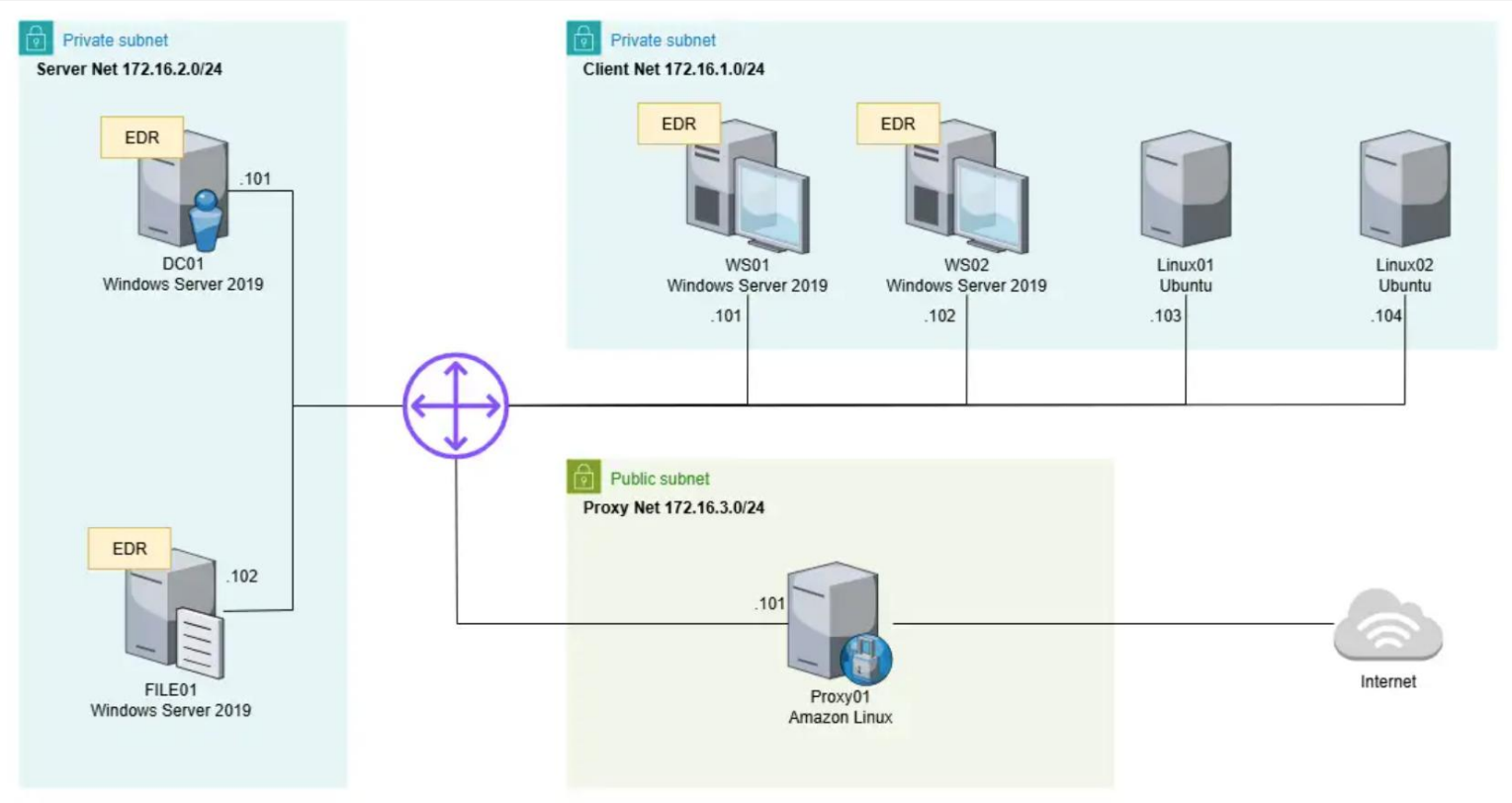
- AI教育の成果が実り、生徒たちは自作のアプリケーションやAIモデルを校内ネットワークで実行するようになっていた。特に、機械学習モデルの学習用データを自動取集するための、独自のWebクローラは生徒の評判もよいものだった。

- 一方で、昨年度に導入されたゼロトラストセキュリティの運用が軌道に乗りつつあり、校内では「セキュリティはもう大丈夫」という空気が流れ始めていた。

Mission：Damianとともに謎を解明せよ！

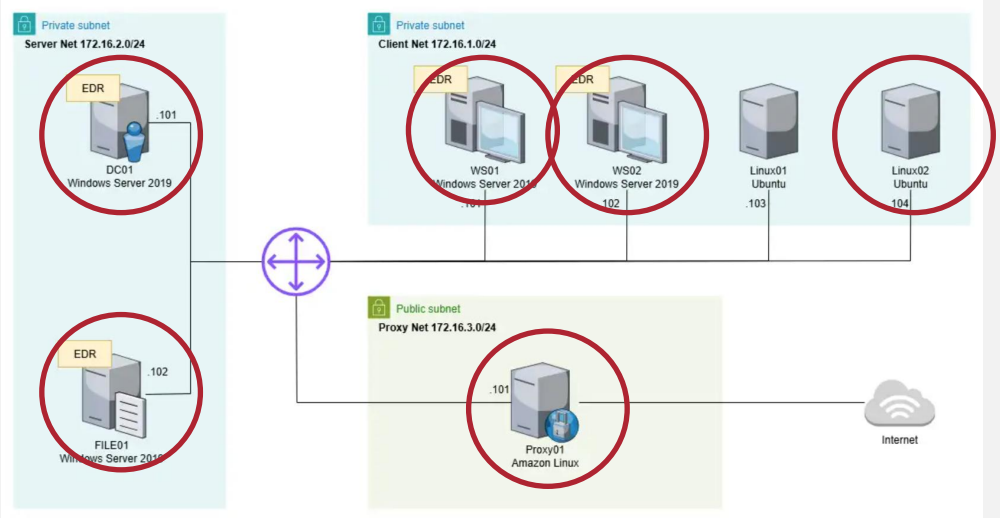
- そんなある日のこと、新学期科目別クラス替えテストでAnyaのテスト結果を覗き見たDamianは衝撃を受けた
- 100点だったからだ！！
- AnyaはDamian同様、国語力に難がありクラスもFクラスと最下位のクラスに所属している
- テスト結果に疑念を抱いたDamianは、IT環境の調査に名乗りを上げることにした
- EDRログ、プロキシログ、Auditログを解析し、Eden・Collegeでどのような出来事が起きたか明らかにして欲しい

イーデンカレッジのIT環境構成図



競技で解析するログ

- 各エンドポイントのEDRログ
- LinuxマシンのAuditログ
- インターネットの接続点に設置したProxyのログ



競技で解析するログ：EDRログ

- Soliton InfoTrace Mark II のログ
  - Soliton Dataset で提供されているデータと同様のフォーマット
- 記録されている情報
  - プロセスの起動・終了
  - ファイルの作成・削除
  - レジストリ操作
  - ネットワーク接続・切断
  - Windowsイベントログ情報
  - など

競技で解析するログ：Proxyログ

- OSSのプロキシソフトウェア Squid のアクセスログ
- 記録されている情報
  - クライアントIPアドレス
  - HTTP リクエストメソッド
  - HTTP アクセス先URL
  - HTTP レスポンスステータスコード
  - クライアントから送信（アップロード）されたデータ量の合計
  - クライアントへ送信（ダウンロード）したデータ量の合計
  - リファラ
  - User-Agent
  - など

競技で解析するログ：Auditログ

- Linuxの監査デーモン (auditd) によって生成されるシステム監査ログ
  - システムコールやファイルアクセスなど、システム上の重要な操作を詳細に記録する。
- 記録されている情報
  - プロセス名
  - 実行ファイルパス
  - 実行ユーザー
  - UID
  - システムコール番号
  - 対象ファイルパス（open、writeなど）
  - 成否（success/failure）
  - 時刻
  - PID
  - など

課題概要：25pts満点

0. Prologue 1				
1.1. Impact 1	1.2. Impact 1	1.3. Impact 1		
2.1. Initial Access/ Execution？ 1	2.2. Initial Access/ Execution？ 1	3.1. Credential Access/ Lateral Movement 2	3.2. Privilege Escalation 3	3.3. Credential Access 1
4.1. Initial Access/ Execution 1	4.2. Initial Access/ Execution 1	5.1. Lateral Movement 2	5.2. Command and Control 2	
6.1. Impact/Privilege Escalation 2	6.2. Lateral Movement 2	7.1. Incident Response 2	7.2. Incident Response 1	

Offensive問題：5pts

今年のテーマ その1

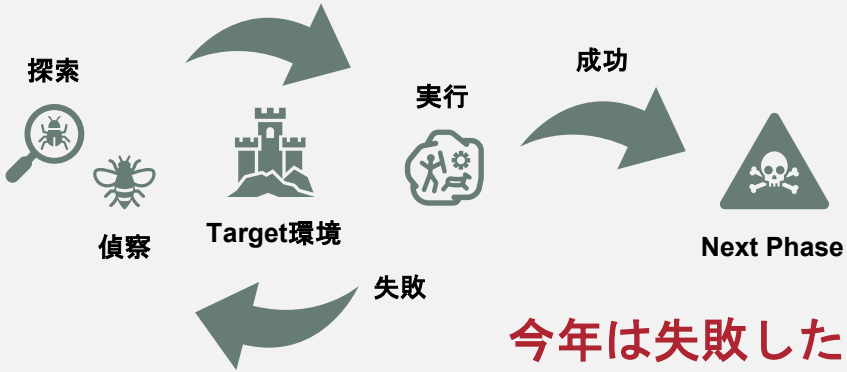
「May the Offensive Security be with DFIR」

オフェンシブセキュリティが共にあらんことを

今年のテーマ その1(裏)

すべての攻撃が成功するわけじゃない

攻撃者も最初からターゲット環境のすべてを把握して行動しているわけではない
探索->実行->失敗->探索->実行->失敗->…->実行->成功
こういった試行錯誤をしてターゲット環境を侵害し、目標達成を目指している



今年は失敗したコマンドも多いです

今年のテーマ その2

ClickFix/FileFix

ClickFix（クリックフィックス）とは？

ClickFixは、**ソーシャルエンジニアリング**のひとつの手口です。
攻撃者がブラウザ上などで偽のエラー画面や偽CAPTCHA認証画面を表示し、「解決するには（ボットではないことを証明するには）このステップを実行してください」というようにユーザの操作を促す、というものです。ユーザが疑問を持たずにそのとおりに操作すると、パソコンがマルウェアに感染してしまいます。**次の画面に進むための正当な操作に見せかけ、ユーザ自身に不正なコードを実行させる**のです。

https://www.trendmicro.com/ja_jp/jp-security/25/i/securitytrend-20250905-01.html

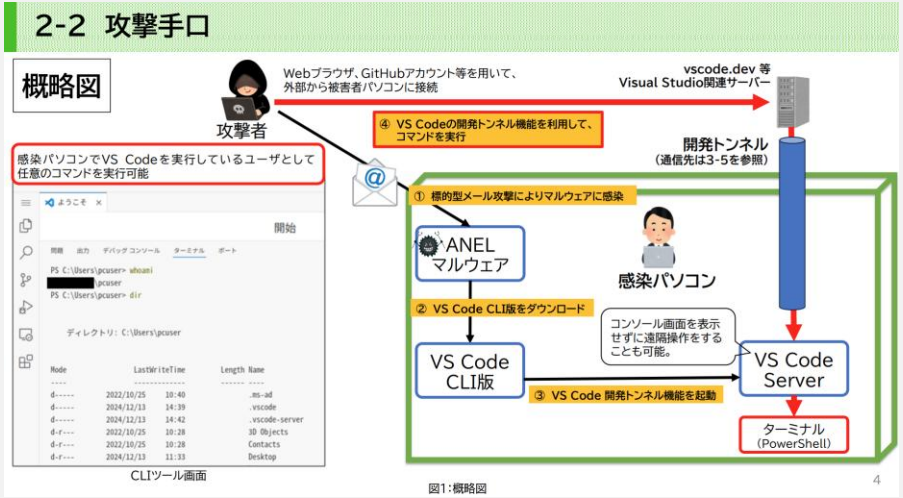
今年のテーマ その3

VSCodeによるC2チャネル

別添資料

VS Codeを悪用した手口及び痕跡・検知策

2025年1月8日
警察庁



https://www.npa.go.jp/bureau/cyber/pdf/20250108_vscode.pdf

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
16:23:28	Initial Access	FileFixによりSliverチャネル確立	WS01	Damian
16:25:19	Discovery	防御機構確認 (Defender未インストールにつきいくつか失敗)		
16:26:50		ネットワーク探索		
16:29:46		ホスト探索		
16:30:59		AD探索(LDAP)		
16:31:36		Linux01へのHTTPリクエスト		
16:33:02		FILE01の共有フォルダアクセス (失敗)		
16:33:43		DC01にDCOMで横展開 (失敗)		

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
16:35:45	Privilege Escalation	Sharpupで権限昇格探索	WS01	Damian
16:40:29		Game.exe配送し、Unquoted Service Pathの脆弱性により権限昇格		
16:40:29	Command and Control	linkファイルを配送し、VSCodeの開発トンネルを確立(失敗)		
16:52:05	Lateral Movement	WS01からWS02へDCOMを利用した横展開		
16:56:07	Command and Control	linkファイルを配送し、VSCodeの開発トンネルを確立		
16:59:36	Discovery	SSHの秘密鍵を探索・窃取	WS02	
17:05:13	Credential Access	WS01にSSHの秘密鍵を配送	WS01	

攻撃シナリオまとめ

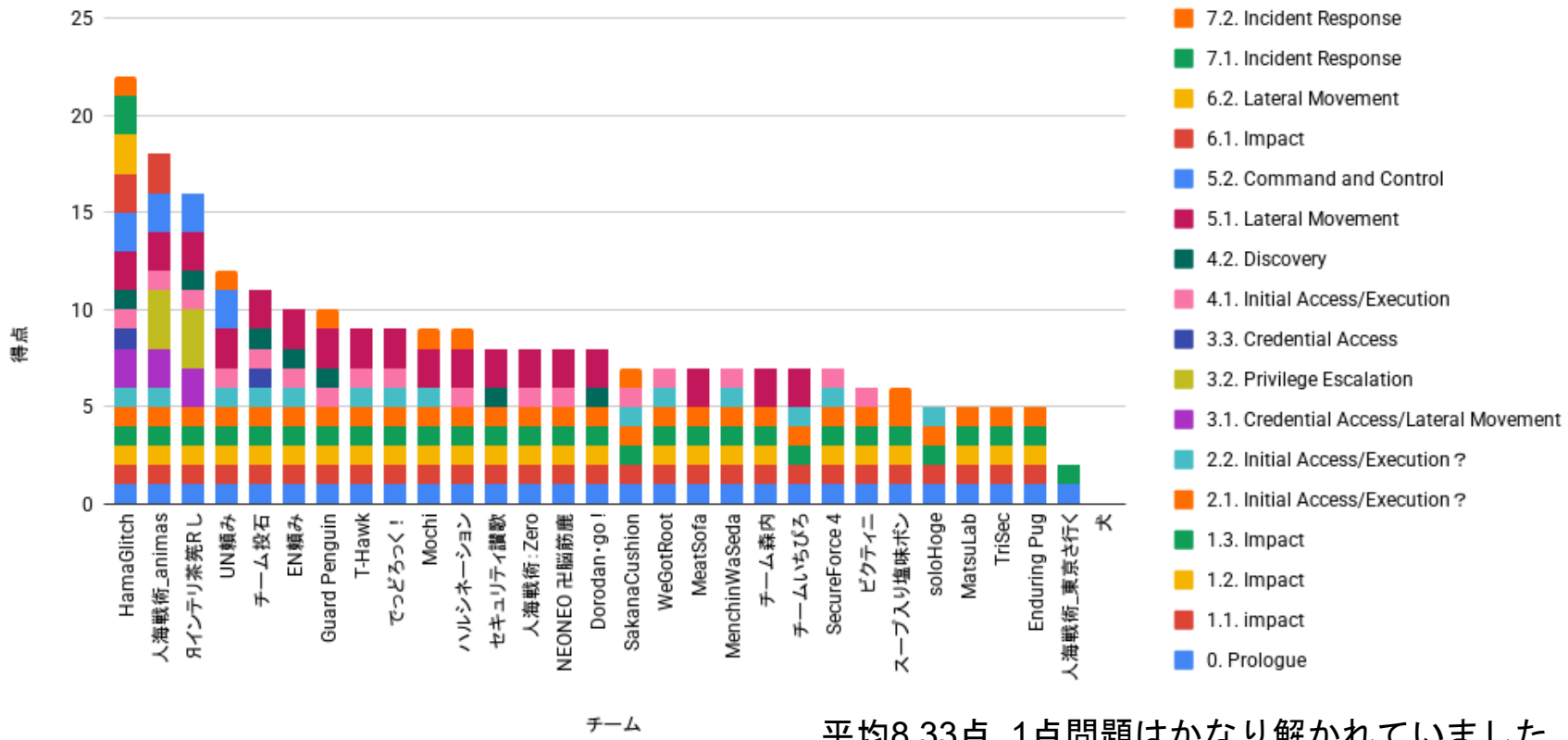
Timestamp	Tactics	Event	Host	User
17:07:24	Lateral Movement	WS01からLinux02にBeckyの秘密鍵を使用してSSHで侵入	WS01	Damian
17:08:51	Privilege Escalation	権限昇格に使える脆弱性な設定やファイルを探索	Linux02	Becky
17:12:50		sudoの脆弱性(CVE-2025-32463)を使用してrootに権限昇格		
17:13:31	Credential Access	/tmp配下にあるswanのKerberosチケットを窃取		root
17:19:34	Lateral Movement	窃取したKerberosチケットを換装	WS01	Damian
17:20:10		FILE01にSwanのチケットを使用しPsExecで横展開		

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
17:21:11	Impact	Anyaのテスト結果をダウンロード	FILE01	Swan
17:22:27		既存のAnyaのテスト結果を削除		
17:22:36		Anyaのテスト結果を再配置		
17:23:25		イベントログの削除	WS01	System
17:30:00		EDRのプロセスを停止 (実際には停止させていない)		

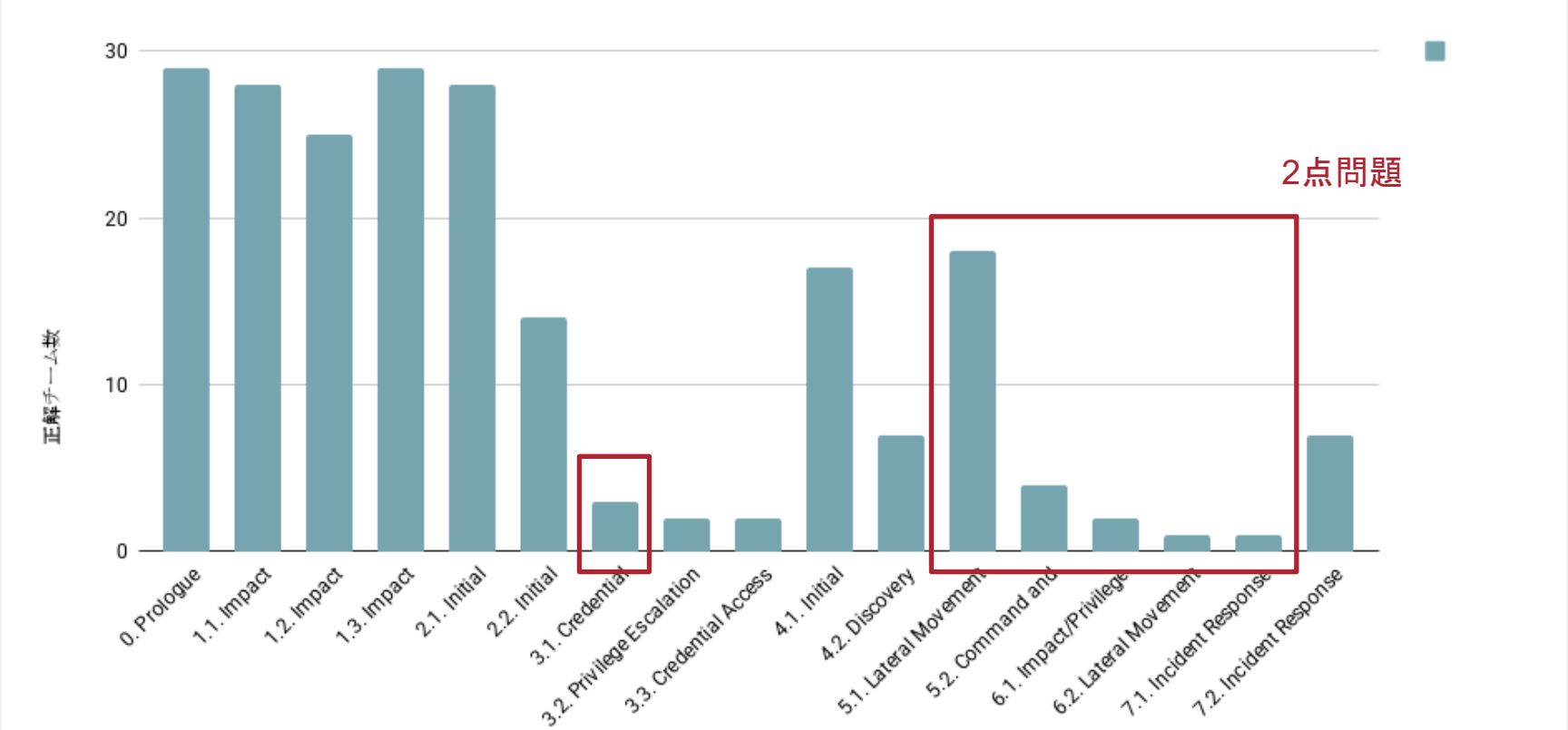
競技結果

チーム別得点グラフ



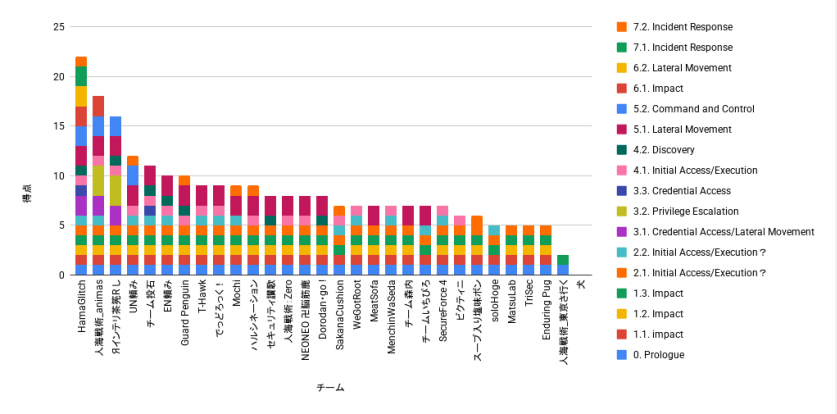
平均8.33点. 1点問題はかなり解かれていました.

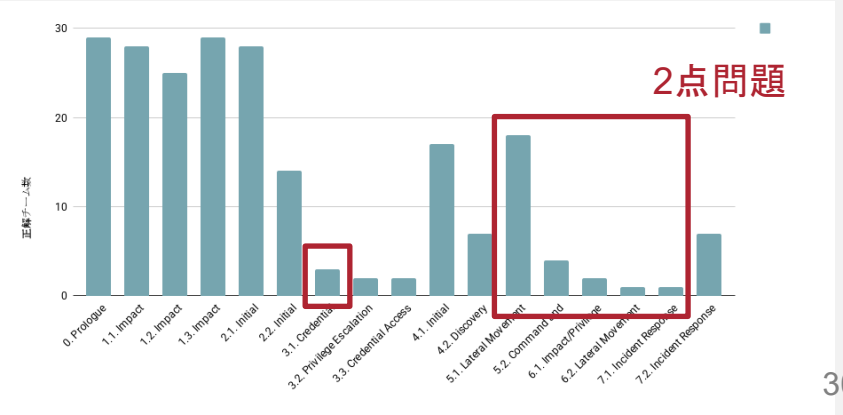
課題別正解チーム数グラフ



得点グラフの傾向

- 勝敗を分けたポイント
  - 1点問題は多くのチームが正答
  - 上位4チームは2点問題を2問以上正答
- Offensive問題の関与
  - 優勝チームはOffensive問題0点(if)でも優勝
  - Offensive問題を解けなくても
    全体のインシデントを把握できれば
    高得点の可能性はあった
- 平均点推移（25点満点）
  - 2023: 17.2点
  - 2024: 12.7点
  - 2025: 8.3点

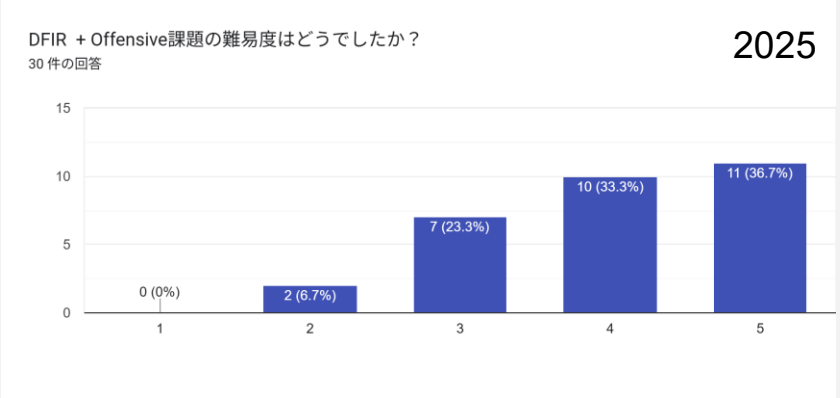


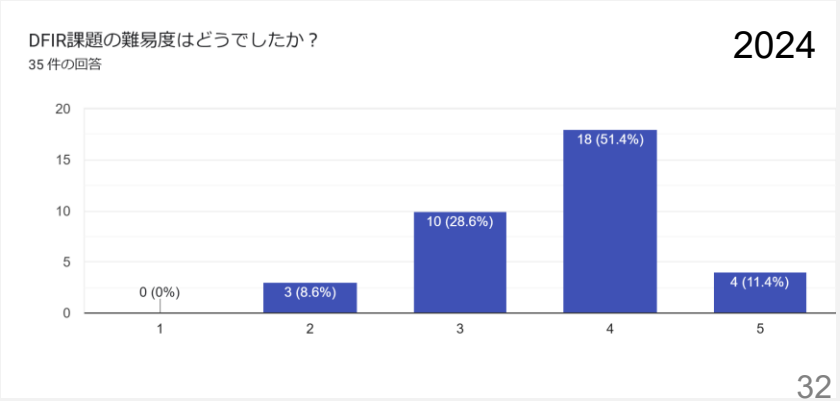


アンケート結果と分析

難易度の考察

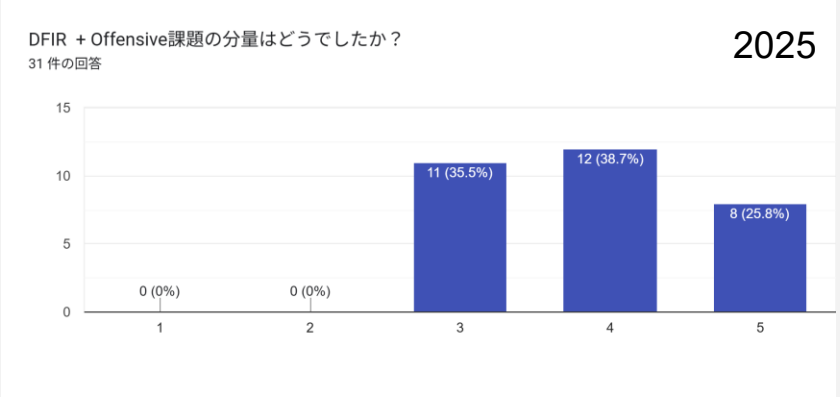
- 難しい(大)と答える割合が多かった
  - 難しいと答えた割合
    - 2024：62.8%
    - 2025：70%
  - 難しいと答える割合はそこまで増加していないが、2024より5の回答が増えた
- 事由考察
  - 単純にログを生成AIに投げるだけでは解けないような問題を増やしたため

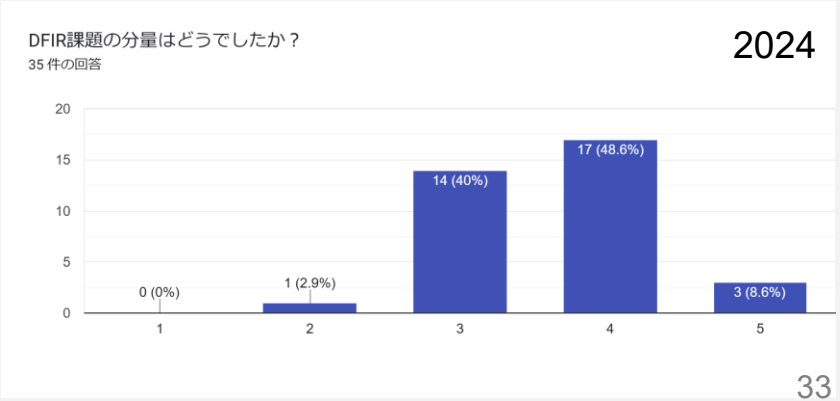




問題量の考察

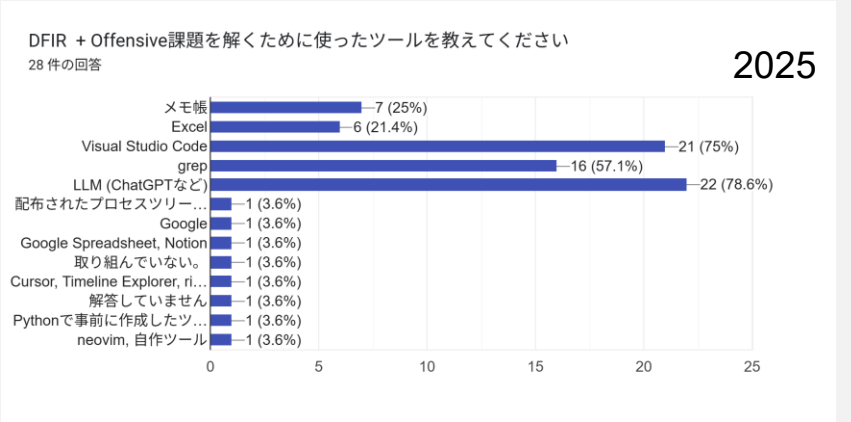
- 多い(大)と答える割合が多かった
  - 多いと答えた割合
    - 2024：57.2%
    - 2025：64.5%
  - 多いと答える割合はそこまで増加していないが、2024より5の回答が増えた
- 事由考察
  - 生成AIとの対話によってログの根拠を明確にできることを受けて、TTPを少し増やした
  - Offensive問題は問題内容やログから分析できるとはいえ、慣れていなければ時間がかかる問題だった

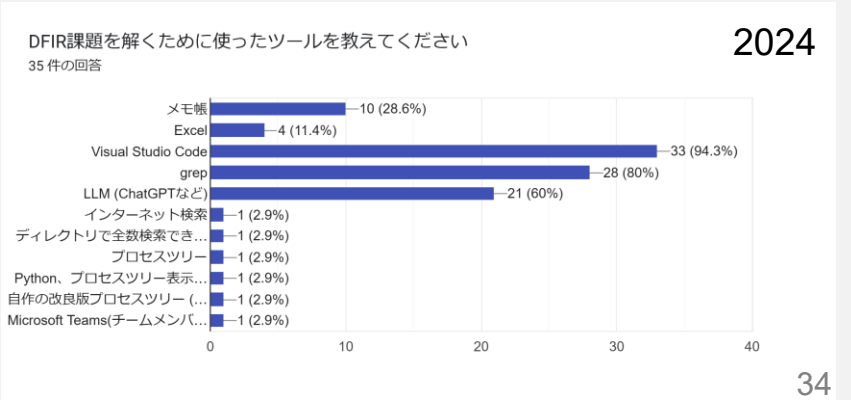




ツールの考察

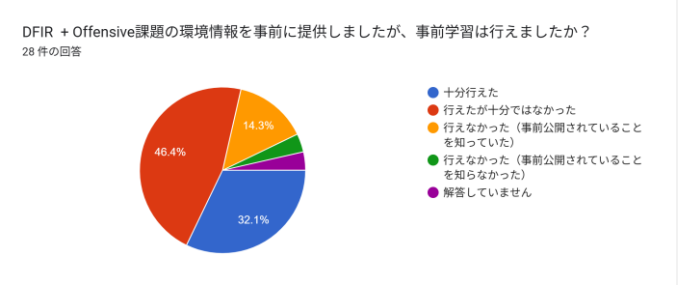
- LLM8割
  - 問題を解く上でも作問する上でも差異が大きい
    - 2024と比較して性能が桁違いすぎて作問でも簡単に解かれてしまうのではないかという懸念との闘い
    - 正直来年が怖い
- Grep減少
  - 今年はプロセスを追跡する問題が多かった

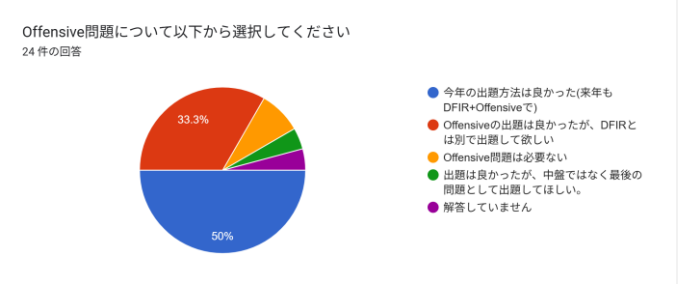




事前学習(Purple Flair)およびOffensive問題の考察

- 事前学習(Purple Flair)
  - 8割の参加者は事前にPurple Flairそのもの(操作)について学習できた
    - 十分行えた：32.1%
    - 行えたが、十分ではない：46.4%
  - Offensiveのテクニックは網羅的に学習しようとすると500時間は必要(個人的な経験に基づく)
    - MWSの課題の範疇を超えてしまう
    - "十分"な事前学習など不可能に近い => **学生活動・研究への影響大**
- Offensive問題について
  - そもそも膨大な学習をしないと解けないような問題は
    MWSでは出題意図にそぐわない
    - **今回は、昨年度も出題したパスワードクラック+ログから分析できるsudoの脆弱性を用いた権限昇格**
  - 4hという制限の中では何らかの手がかりに基づく必要がある
  - **攻撃者のテクニックを問うような問題をMWSで出題するのであれば、+DFIRが妥当**
  - **一方で、DFIR単体としては、"Offensive Security"の思考を十分に出題可能ではある**
    - **アンケート結果も割れた**
- 環境
  - 複数VMを参加者のPCで構築するのは厳しい=>Purple Flairは濃厚
    - **現地参加者とNetwork強度のトレードオフ**





振り返りと来年度に向けて

振り返りと来年度に向けて

- 生成AIとのかかわり
  - 試み：ログを分析した上でないと、尋ねにくい問題を選択した
    - 逆に、ログを追跡できれば、ほとんど利用なしで回答可能
  - 予想：来年度も生成AIは進化
  - Try：Offensive問題だけではなく、従来のDFIR課題もログやartifactの探索を含めてPurple Flairを活用した実際に手を動かす問題を試行したい。
    - 手を動かすためにPupleFlairを使いたいが、今回のようなOffensive問題をDFIRとして継続するかは要検討
      - Offensive問題がなくても十分DFIRとしてはOffensive Securityの要素があるため
      - 一方で攻撃者のテクニックを問うような問題は、+DFIRにするのが現実妥当
  - Try：難易度、分量については0知識の作問メンバーに引き続き解いてもらいたい。
- 出題テーマ
  - 試み：ClickFixやVSCode開発トンネルなど最新の攻撃をシナリオに採択
  - 結果：参加者/作問チームそれぞれもナレッジができてハッピー
  - Try：来年も取り入れたい。逆に言えば流行している攻撃はWatchしていてほしい

振り返りと来年度に向けて

- 問題形式
  - 昨年のアンケート：日本語をフラグで投入するのはやめてほしい
  - 試み：
    - 回答数に制限のある問題は英数字記号のみ
    - 日本語が入る問題、1回しか回答させたくないような問題は、記述式を採用
  - 結果：誤回答減少
  - Try：来年も続ける。フォーマット形式やフラグ例も問題提示は続ける。
- 回答数/配点
  - アンケート：回答数が少ない
  - 振り返り：ログに答えがあるDFIRの課題の性質上、対象となる選択肢が少ない場合はどうしても回答数を絞らざるを得ない
  - アンケート+α：FirstBloodポイント
    - ボーナスポイントがあっても面白いかも？(25点にどう傾斜をつけるかは要検討)

振り返りと来年度に向けて

- 問題提供方法
  - 結果：競技開始時にダウンロードでトラブル
  - Try：ログを固めたファイルについては事前に配布し、当日はパスワードを提供する
- 問題提供方法
  - 試み：IPを含めて、参加者に誤解を当てるプロセスの削除やIPのかいざんを行った
  - アンケート；よくわからないプロセスが判断に迷った
  - Try：ログの改ざんを含めて、出題に耐えるログにしたい。AWS固有のものは参加者に判断をしてもらいたいログではないため削除する

振り返りと来年度に向けて

- 問題提供方法
  - 試み：DFIRの性質上、問題が繋がりをもってしまうのは避けられないが、今年は問題内容から特定のログを発見できれば解けるものをなるべく配置した
  - Try：Offensive問題にしてもDFIR問題にしても1つできなかったら後ろ問題が解けなくなってしまうような出題形式は避けていきたい

まとめ

まとめ

- PostMeeting内容
  - 今年の出題について
  - 競技結果
  - アンケート結果と分析
  - 振り返りと来年度に向けて
- 作問チームへの参加協力
  - 自分の経験を下の世代に還元したい方
  - リアルなフォレンジック業務や攻撃手法に精通している方
  - 様々な攻撃ツールを検証してみたい方
- ご意見・ご質問は Slack-MWSの #mwscup までお気軽にどうぞ！

Thank you for trying harder!!