MWS Cup 2022 x DFIR ポストミーティング

MWS Cup 2022
DFIR作問チーム
株式会社エヌ・エフ・ラボラトリーズ　保要　隆明

本日の内容

- 今年のDFIR課題 振り返り
- 競技結果
- アンケート結果の共有と考察

DFIR課題メンバー

- 全体取りまとめ
  - 保要 隆明（株式会社エヌ・エフ・ラボラトリーズ）

- 攻撃シナリオ検討・ログ取得環境構築
  - 荒木 粧子（株式会社ソリトンシステムズ）
  - 後藤 公太（株式会社ソリトンシステムズ）
  - 尾曲 晃忠（株式会社ソリトンシステムズ）
  - 木野田 渉（株式会社ソリトンシステムズ）
  - 伊神 和馬（株式会社ソリトンシステムズ）
  - 白鳥 隆史（株式会社ソリトンシステムズ）
  - 竹澤 一輝（株式会社ソリトンシステムズ）

- 攻撃シナリオ検討・検証・実施・問題作成（Red Team）
  - 久保 佑介（NTTコミュニケーションズ株式会社）
  - 田口 裕介（NTTコミュニケーションズ株式会社）
  - 戸祭 隆行（NTTセキュリティ・ジャパン株式会社）
  - 阿部 航太（株式会社エヌ・エフ・ラボラトリーズ）
  - 飯田 良（株式会社エヌ・エフ・ラボラトリーズ）
  - 市岡 秀一（株式会社エヌ・エフ・ラボラトリーズ）
- 攻撃シナリオ検討・問題作成（Blue Team）
  - 大倉 有喜（NTTセキュリティ・ジャパン株式会社）
  - 小林靖幸
    （GMOサイバーセキュリティ byイエラエ株式会社）

今年の方針

- 2021
  - 人の手による攻撃
  - 複数端末
  - EDRログ（InfoTrace Mark II）＋プロキシログから侵害状況を明らかにする
  - 環境情報やフォーマットの事前アナウンス
  - 現実の攻撃を再現した擬似攻撃
- 2022
  - 人の手による攻撃
  - 複数端末
  - EDRログ（InfoTrace Mark II）＋プロキシログから侵害状況を明らかにする
  - 環境情報やフォーマットの事前アナウンス
  - 現実の攻撃を再現した擬似攻撃
  - 昨年よりも攻撃を少なめにする
  - 昨年の課題1をカバーする問題作成
  - 知識問題を追加

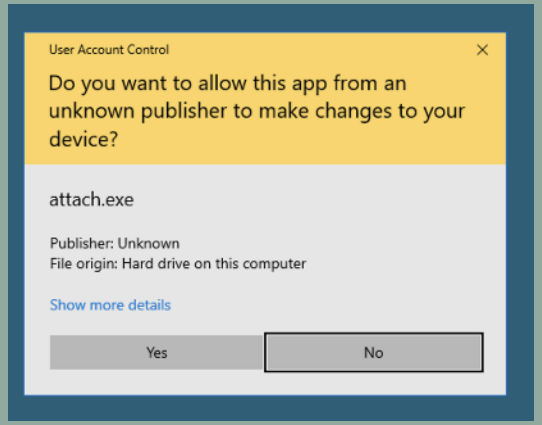
今年のあらすじ

イーデン・カレッジは、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。

そんなイーデン・カレッジは、これまで日々の作業を紙で行っていたが、世の中のIT化の流れに伴い、業務をデジタル化することにした。

ある日、IT管理者に一つの相談が…

SwanからIT管理者に対して、「普段見ない画面が表示されて、Yesを押してしまったけど大丈夫か？」との相談があった。



IT管理者はこの画面に心当たりがなかったため、ヒアリングを実施。
ヒアリングを行ったところ、「画面が表示される少し前にExcelファイルが送られてきたので、開いたような…」と話している。

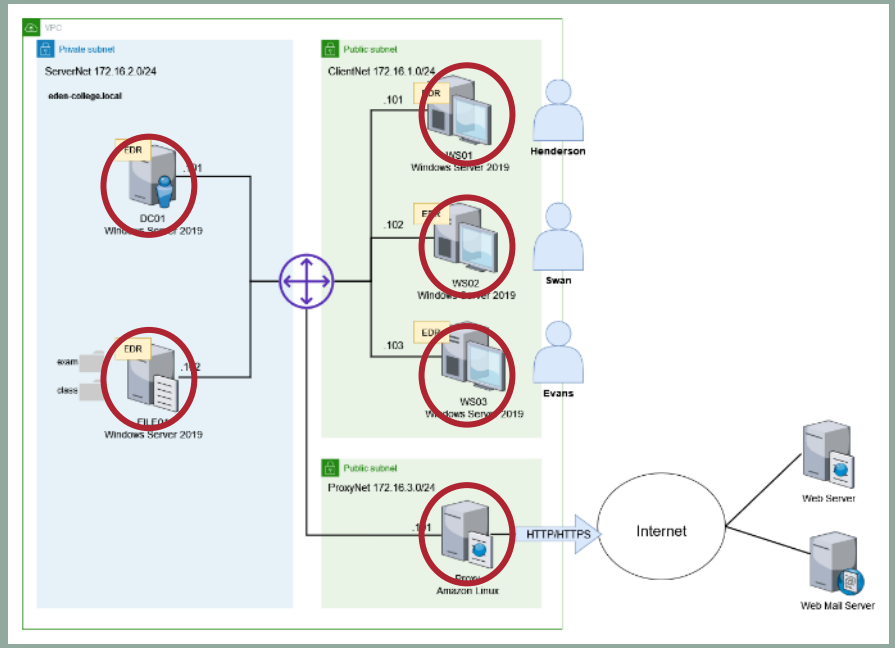
事件を解決せよ！

最近、敵国の諜報活動が活発化しているとの情報がある。
もしかしたら、敵国スパイの諜報活動かもしれない。。

EDRログ、プロキシログを解析し、イーデン・カレッジで
どのような出来事が起きたか明らかにして欲しい。

競技で解析するログ

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



課題概要

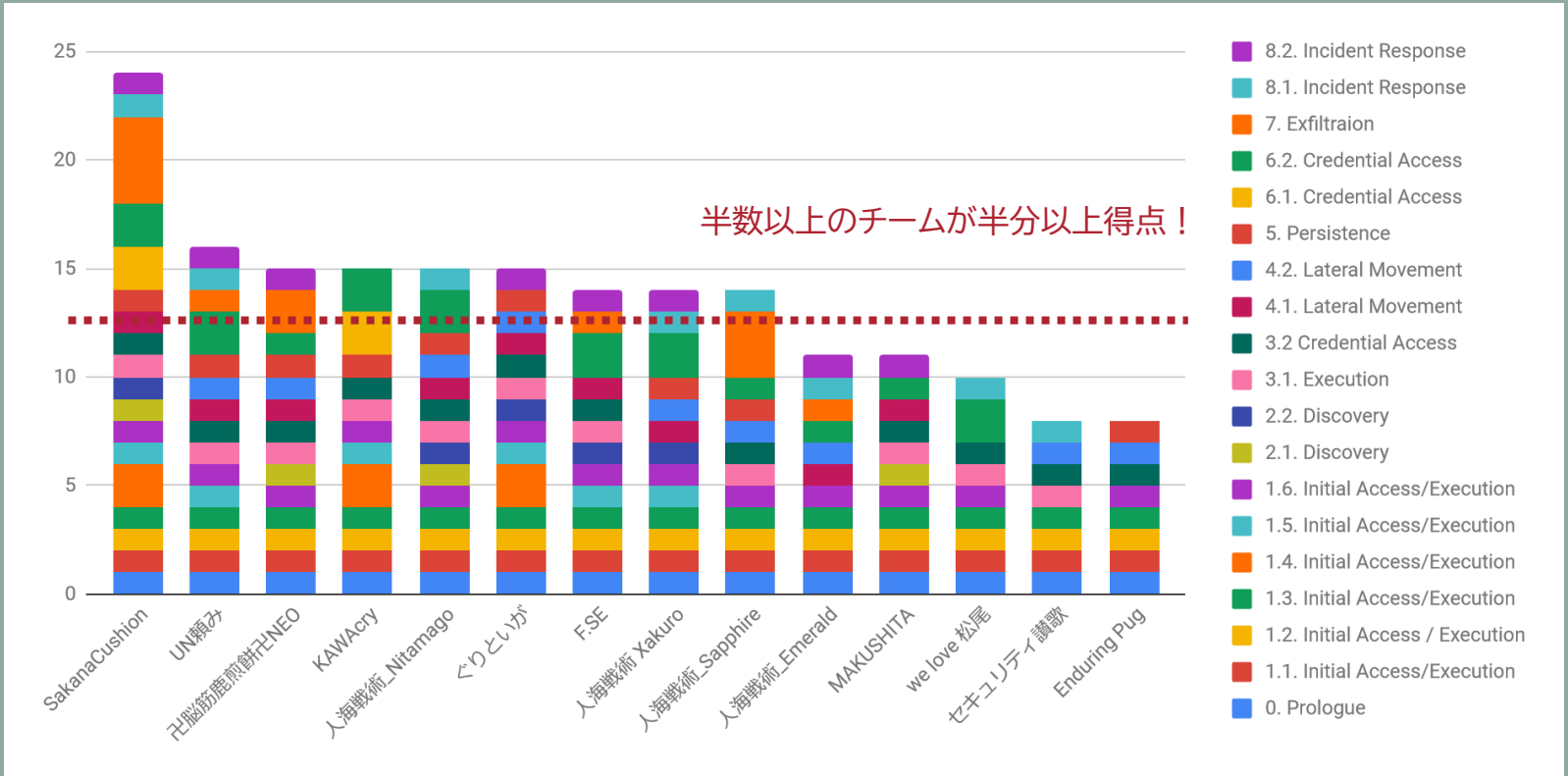
0. Prologue 1			
1-1. Initial Access/Execution 1	1-2. Initial Access/Execution 1	1-3. Initial Access/Execution 1	
1-4. Initial Access/Execution 2	1-5. Initial Access/Execution 1	1-6. Initial Access/Execution 1	
2-1. Discovery 1	2-2. Discovery 1	3-1. Execution 1	3-2. Credential Access 1
4-1. Lateral Movement 1	4-2. Lateral Movement 1	5. Persistence 1	6-1. Credential Access 2
6-2. Credential Access 2	7. Exfiltration 4	8-1. Incident Response 1	8-2. Incident Response 1

FLAG/選択形式：17pts

記述形式: 8pts

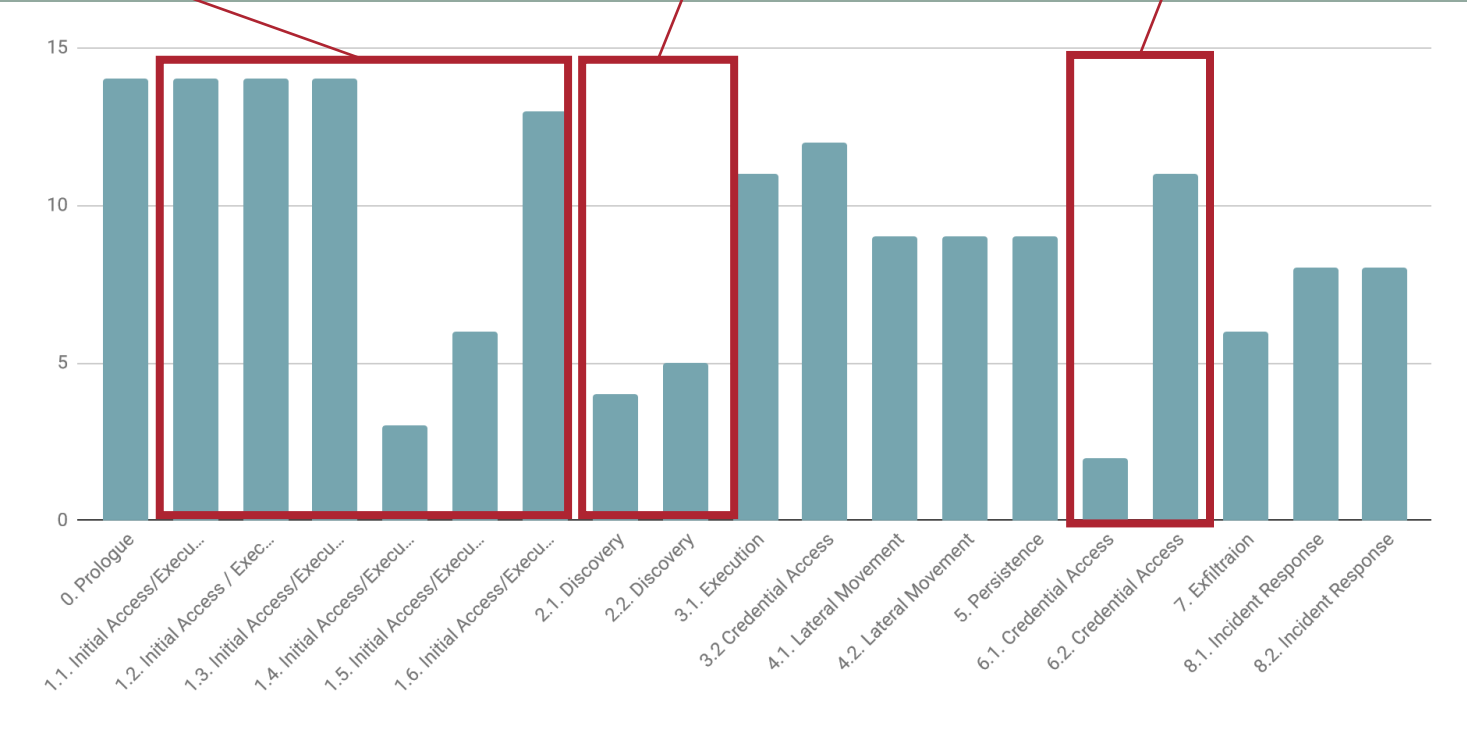
競技結果

チーム別


25
20
15
10
5
0
半数以上のチームが半分以上得点！
SakanaCushion
UN頼み
卍脳筋鹿煎餅卍NEO
KAWAcry
人海戦術_Nitamago
ぐりとりが
F.SE
人海戦術 Xakuro
人海戦術_Sapphire
人海戦術_Emerald
MAKUSHITA
we love 松尾
セキュリティ講歌
Enduring Pug
8.2. Incident Response
8.1. Incident Response
7. Exfiltraion
6.2. Credential Access
6.1. Credential Access
5. Persistence
4.2. Lateral Movement
4.1. Lateral Movement
3.2 Credential Access
3.1. Execution
2.2. Discovery
2.1. Discovery
1.6. Initial Access/Execution
1.5. Initial Access/Execution
1.4. Initial Access/Execution
1.3. Initial Access/Execution
1.2. Initial Access / Execution
1.1. Initial Access/Execution
0. Prologue

問題別

初期アクセスのマルウェアの問題　“情報収集(AD含む)”の問題　Golden Ticketの問題

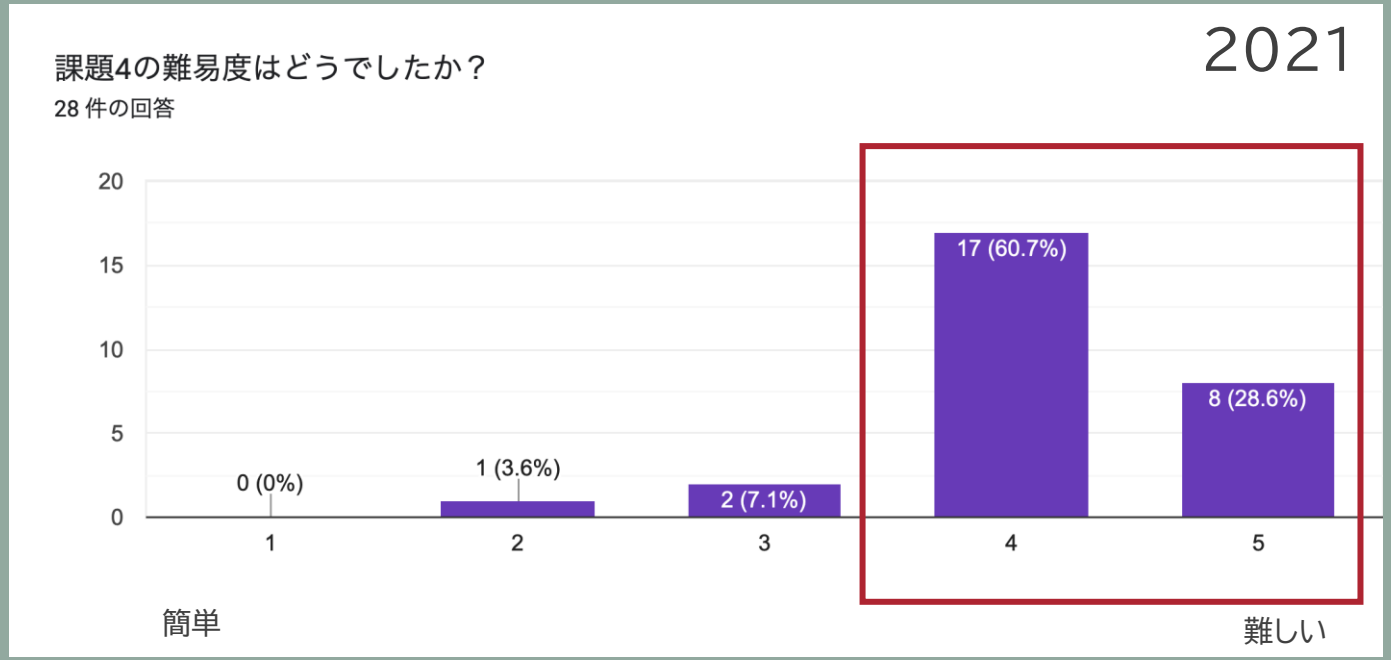


※ 記述問題は得点したチーム数

アンケート結果

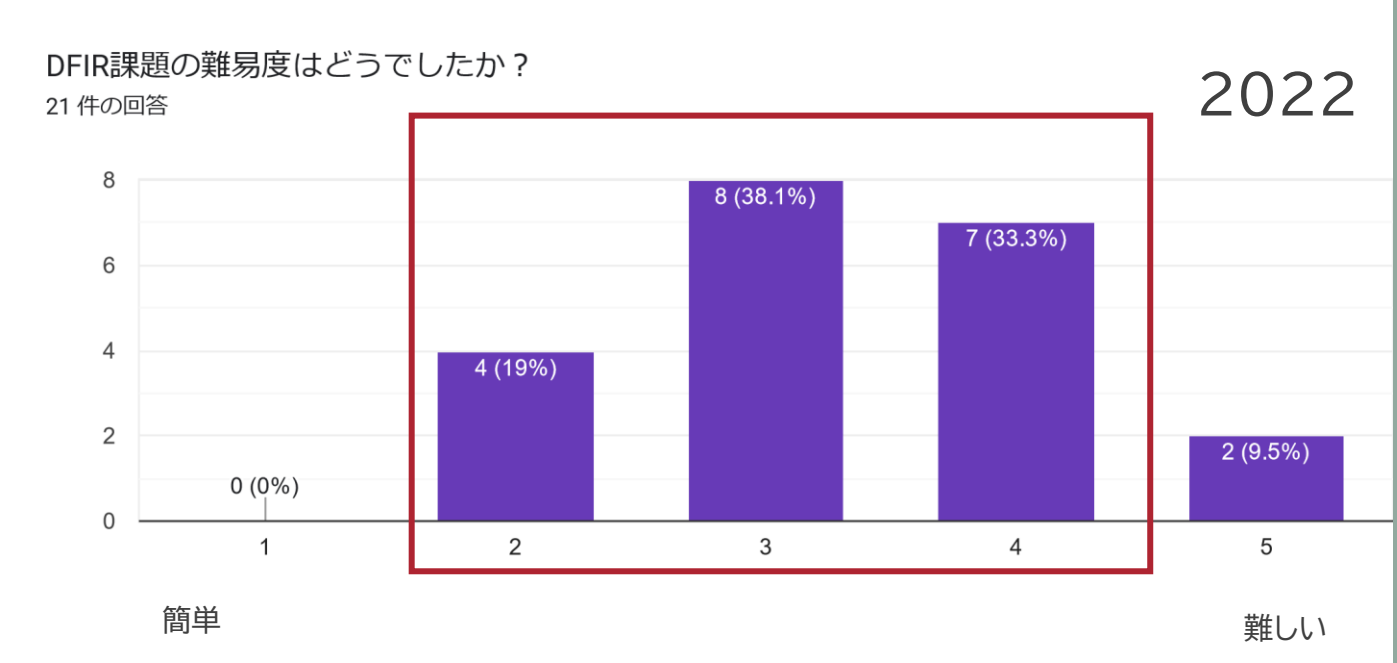
問題の難易度(昨年)

- 約90%の参加者が「難しい」(4以上)と回答



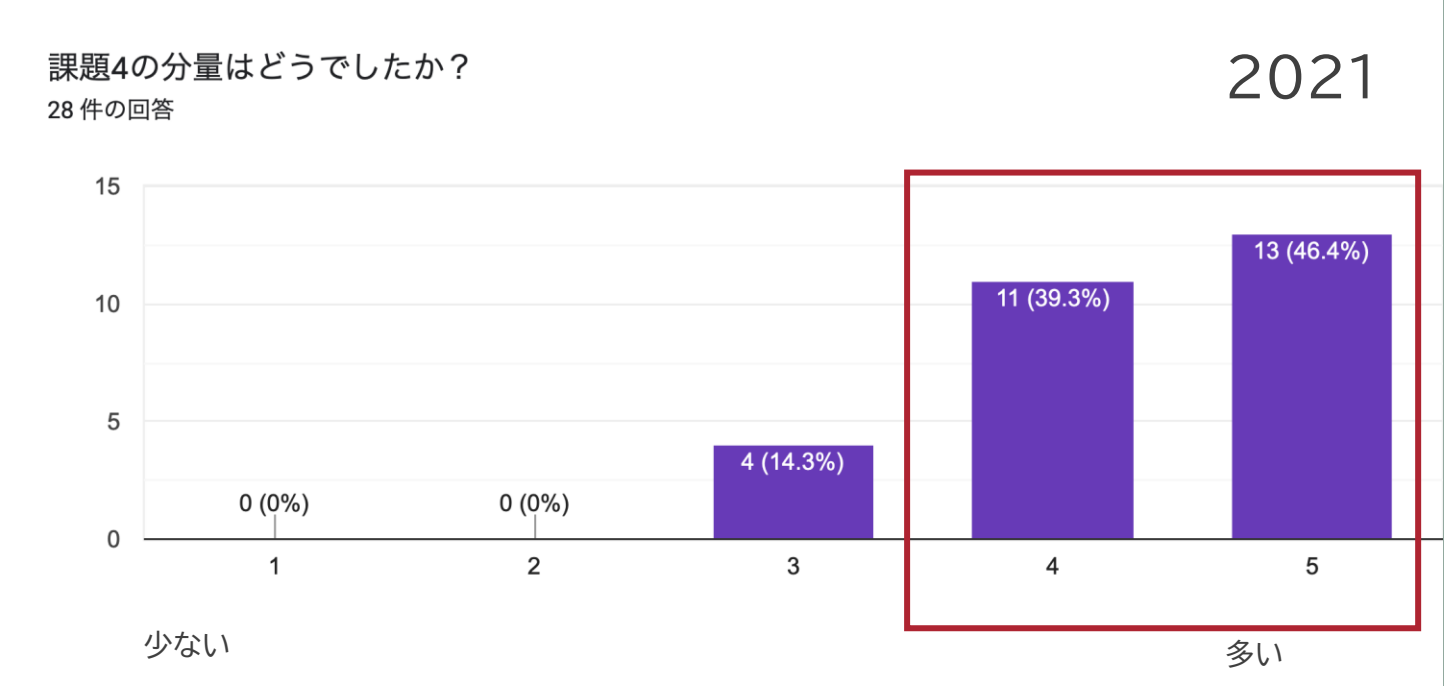
問題の難易度

- 「難しい」と答える人の割合が減った



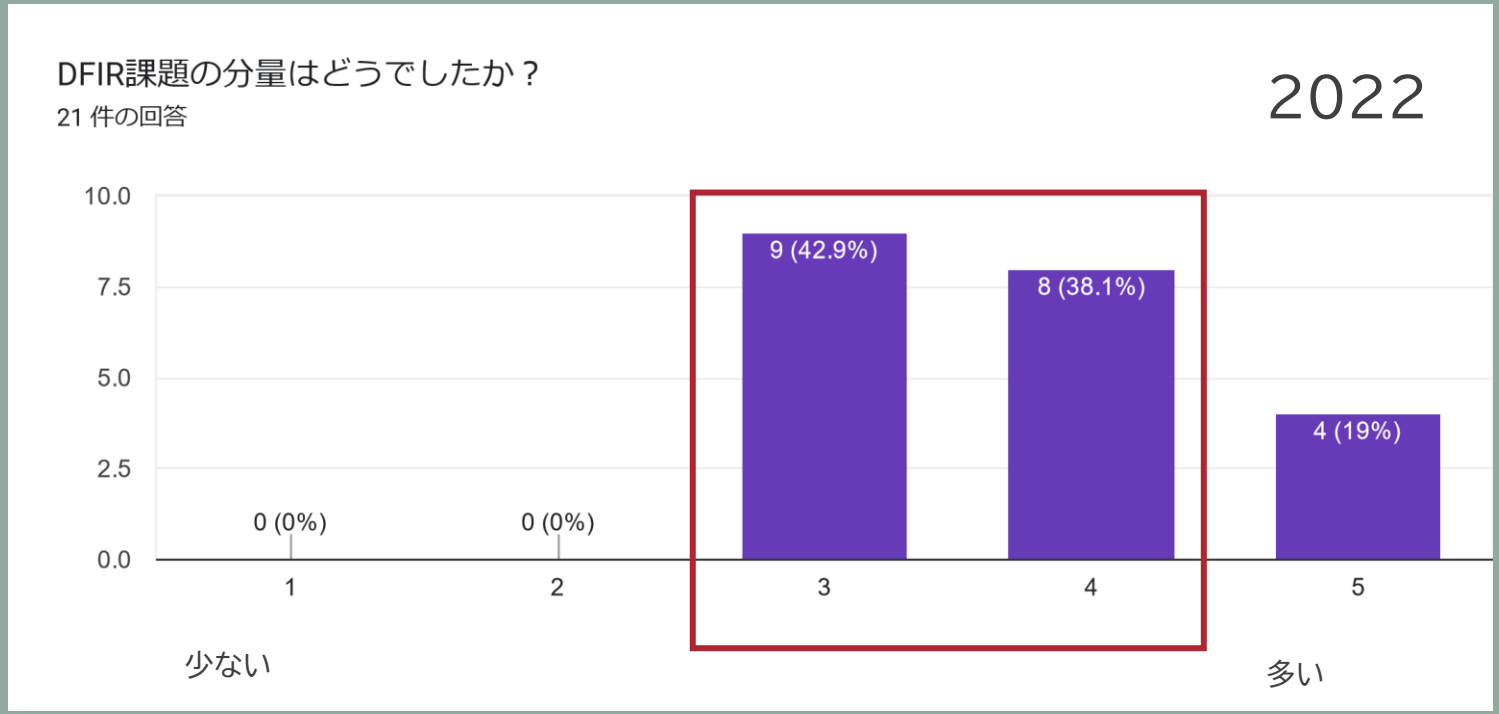
課題分量(昨年)

- 約85%の参加者が「多い」(4以上)と回答



課題分量

- 「多い」と答える人の割合が減った



解くために使ったツール

- Visual Studio Code
- メモ帳
- grep
- findstr
- Splunk
- Excel
- CyberChef
- …

記述回答(抜粋)

MWS Cup の取り組み全体に関して、意見や感想、提言等をお願いします。

(DFIRに関連するものを抜粋)

- DFIRのような問題はCTFでもなかなか触れることができないので非常に貴重な経験になった。来年リベンジしたい。
- 初めての参加, DFIRのみへの取り組みでしたが, 問題の解説などとてもわかりやすく, 勉強になりました.
- DFIR課題は難易度がちょうどよく、非常に解いていて面白かったです。
- DFIRを体験できるような、サービスやツール、サイトがあれば知りたいなと思いました。

記述回答（抜粋）

DFIR課題を解く上で、行き詰まった箇所があれば教えて下さい

- 1-3のLog分析の際Base64のデコードに手を付けてしまい、関係のないところで詰まってしまった。
- powershellのコマンドが途中でbase64エンコードされていたが、復号することができずかなりの時間を要してしまった。
- 1-3 .pngという拡張子に惑わされ、BASE64の解析を試みた結果大幅な時間ロスとなってしまった。

Base64のデコード

- Active Directoryの部分。
- Kerberos認証。今回の問題で初めて知った。
- アクティブディレクトリの調査に関する問題でツール名がわからなかった

Active Directory

記述回答（抜粋）

今回のDFIR課題に関して良かった点

- 全体的に流れで追うことができたので、どのフェーズかかみ砕きながら解くことができてよかった。
- 解説でレッドチームの観点からの話がたくさん聞けたのがよかった。
- 実際のインシデント対応を想定した作問で、非常に参考になった。
- スパイなアニメ大好きなので面白かったです。知識問の量も適切でよかったです。
- 課題の題材やシナリオ部分など最近の話題やトレンドなどを取り入れられていた部分がよかった。楽しむことができた。解説にて、どのようにログを作る際に攻撃を行ったかについての解説があった部分がとても興味深かった。

記述回答（抜粋）

今回のDFIR課題に関して悪かった点

- 数珠つなぎのように解く形式の問題では点数に格差が開きやすいと感じた。また、全体のタイムラインを整理しないと解けないような、本来のDFIRの趣旨に沿った問題があると良いと思った。

- 過去問でしか対策ができないため、初学者には少し対策しづらい状況にあるのかもしれない。前年の傾向に沿った問題は解けたがADやパスワードクラックなど少し新しい要素が加わると途端に手が止まるので、事前学習にいい教材があれば、参加者のレベルもあがり、問題の質と量もあげることが出来ると思う。
- どのように事前学習を進めればよいかが少し分かりにくかったです。

競技、アンケート結果に対する考察・反省

競技、アンケート結果に対する考察

- 誘導がわかりやすい問題、調べればわかる知識問題が今年は多かったので、全体的に簡単だった
- 攻撃シナリオを控えめにしたため、昨年より分量が控えめという意見が多かった
  - 設問自体は昨年より増やしている

- 出題の仕方が悪く、答えにブレが出やすい問題は正答率が低かった
- Active Directoryに関する問題は、あまり身近ではないためか正答率が低かった

競技、アンケート結果に対する反省

- リアリティと攻撃者視点は意識していたので、その点伝わって良かった
- 楽しんで参加してもらえた人が多くて良かった
- 事前学習についてもう少し伝えるべきだった？

事前学習としてやっておくと良いこと

- ログのフォーマットを理解しておく
  - フォーマットは大きく変わらない
- ログを解析するツールに慣れておく
  - 解説ではVSCodeを使ってますが、他にも解析ツールはある
- 世の中の最新のセキュリティ動向を追っておく
- Windows OSやActive Directoryの仕組みを理解しておく
  - 手を動かして実際に構築してみるのがベスト
- Windowsに対する攻撃手法を学習しておく
  - セキュリティ教育プラットフォーム（TryHackMe, HackTheBox など）に取り組む
  - 構築した環境に対して攻撃をしてみる、どのようなログが出るかわかるとベスト
- DFIRの手法を学習しておく
  - セキュリティ教育プラットフォーム（CyberDefenders, Blue Team Labs Online など）に取り組む

さいごに

- 今日話したこと
  - 今年のDFIR課題 振り返り
  - 競技結果
  - アンケート結果の共有

- 作問にご協力いただける方がいれば、ご連絡お待ちしております
  - 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