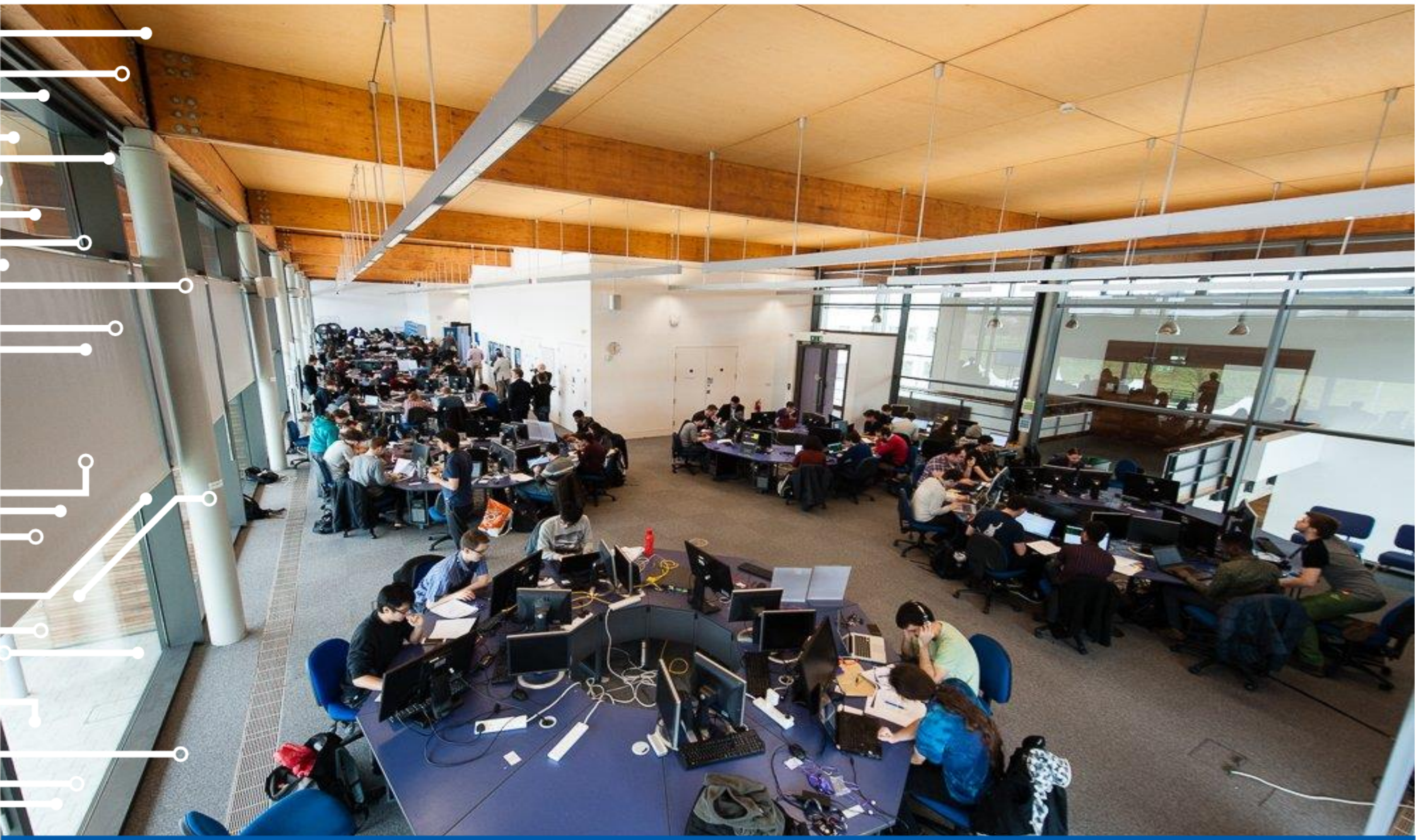
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



CTF EVENTS

Contemporary Practices and State-of-the-Art in Capture-the-Flag Competitions

MAY 2021

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe’s citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe’s critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors please use cbu@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Alastair Janse van Rensburg, University of Oxford
Richard Baker, University of Oxford

EDITORS

Ioannis Agrafiotis, Christina Skouloudi, Adrian Belmonte Martin, Filippos Papaioannou, European Union Agency for Cybersecurity (ENISA)

ACKNOWLEDGEMENTS

We would like to thank all members of the International Cyber Security Challenge Steering Committee for their valuable contributions.

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
ENISA may update this publication from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-501-2- DOI: 10.2824/313553

EXECUTIVE SUMMARY

This report addresses the contemporary use of capture-the-flag (CTF) competitions around the world. It first provides background on such competitions, their structure and variations. Analyses of recent competitions is then conducted, comprising an in-depth qualitative analysis of notable events (22 in total) and a high-level statistical analysis of a large dataset of public events of all levels (879 in total).

The results show a great deal of variation in some areas:

- team size
- challenge categories
- scoring methodology
- hosting of event online vs. in-person
- use of qualifier rounds
- inclusion of peripheral activities
- communication channels for media strategy

By contrast, little variation was seen in:

- entry restrictions (usually only upon location)
- diversity policy (mostly absent)
- format (typically a ‘Jeopardy’ format)
- prizes (usually provided)
- duration (events typically spanning a single day or a few days)

The report discusses the findings and proposes topics for consideration during event design. In particular:

Team sizes: Hard limits may not be necessary and unbounded team sizes are seen in notable events.

Formats: Recognised formats promote east of understanding among participants. Formats have commonly-associated scoring methodologies and challenge categories, which can act as a starting point for event design.

Parallel Competitions: Running parallel events with a different focus (different audience or different challenge type) can broaden appeal easily.

Range of Media: Public engagement strategies benefit from a range of media. Inclusion of CTF specific venues (such as that used in the statistical analysis) is recommended to best reach the CTF community.

Release of Data: Retrospective release of challenges, solutions, competition metrics and lessons-learned are helpful to the wider community.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 SUMMARY

This report describes capture-the-flag (CTF) competitions and their contemporary use in cyber security education and recreation worldwide. It provides background on CTFs and describes the various competition formats and practices.

It reports on an analysis of recent competitions; both an in-depth qualitative examination of a selection of major events and a quantitative analysis of a large, public dataset of events. The analysis describes a range of aspects including formats, challenge types, platforms, event structures, entry requirements and team composition. To create this report, a survey of previous significant competitions was performed and each event was tagged according to a number of research themes and questions. In addition, statistics were obtained from public datasets and used to perform a general analysis of CTF events.

Based on the results of the analysis, different events and their practices are compared and contrasted; to find commonalities and identify design decisions and their trade-offs. The report concludes by making recommendations for consideration during event design.

1.2 STRUCTURE

This report is structured into the following sections:

- **Background**: An outline of CTF competitions and formats to give background for later sections. In particular, the challenge types, scoring systems and formats of both "Jeopardy" and "Attack-Defence" events are detailed.
- **Methodology**: A full description of the methodology used in this report, including data themes, an explanation and justification of data sources, and methods used in the statistical analysis.
- **Results**: A per-theme analysis of the manually gathered data on each individual event, together with summaries of the results of the statistical data gathered.
- **Discussion**: A discussion of the results, including trends and consideration of the differences between the two datasets produced by this report.
- **Conclusions**: Conclusions drawn for running future CTF events based on the data and analysis gathered in this report.

2. BACKGROUND

A Capture-The-Flag (CTF) is a competitive computer security event where participants compete in security-themed challenges for the purpose of obtaining the highest score [1] [2]. There are a number of formats in common use. The CTF name derives from the outdoor game, in which participants seek to find and retrieve a physical "flag", and its similarity to early "wargaming" and "king-of-the-hill" cyber security competitions. Today, the CTF term encompasses a range of competition types and targets a wide audience. A renowned CTF has been run at the DEF CON security conference since 1996 and a calendar of events takes place, online and at physical sites, throughout the year.

CTFs take many forms, but the most common forms are Jeopardy and Attack-Defence [3], which are described in detail below. The information in this section is informed by the experience of the authors in participating in and organising events, by the results of the analyses of the report, and by the related work cited.

2.1 JEOPARDY

Jeopardy CTFs [2] [4] [5], the most common format for current competitions, contain a set of custom-made, artificial challenges created specifically for the event. Participants tackle each challenge as a stand-alone problem, and a solving a challenge results in a flag, which can be submitted to a scoring system for a number of points.

2.1.1 Format

Jeopardy challenges are highly variable and the only key property is that they should grant access to one (or more) flags when solved. Challenges are typically completely independent of each other (although they may have multiple parts), and participants are able to solve them, broadly, in any order. Each challenge consists of some downloadable files, a remote server, or both. When remote servers are present, participants are not able to impact the performance of the server for other teams, so that each team participants in the competition independently. Challenges that consist only of files will usually contain the flag embedded into the downloadable file and participants are expected to use any means to find the flag within the files. When a remote server is present, participants are typically expected to perform a remote exploit on the server to recover the flag, and there may be downloadable files (such as challenge source code, or compiled binaries), that aid them in the attempt.

Challenges vary across a large and diverse number of categories, and the flexible format of the contest allows for a wide degree of variation in challenges. Some common categories are expected in any CTF, while less-common categories may appear depending on the theme or format of the event. In particular, more difficult events tend to be more focused on categories that replicate real exploits (such as **pwn**, **web** and **re**), while beginner-focused events have more scope for categories that explore more gamified areas (often under the grouping of **misc** challenges). Some of the most common categories include [6]:

2.1.1.1 pwn

Deriving their name from "owning" services, these challenges replicate attacks on real vulnerable services. In some cases, these challenges may involve performing the compromise of a piece of known-vulnerable software, but more often they are custom binaries that are developed to showcase a particularly interesting exploit. These challenges are solved by participants by interacting with a remote server, usually over a command line. In easier challenges, participants may be given access to the compiled binary running on the target, or even the source code directly. In harder challenges, participants will be given no information other than access to the remote service. An example challenge might give participants access to a remote server which runs a binary vulnerable to a buffer overflow. Overflowing the buffer would cause the binary to crash and consequently output the flag.

2.1.1.2 re (or reversing)

These challenges involve reverse engineering a piece of software in order to extract the flag. They differ most clearly from **pwn** challenges in that they typically have no remote service to compromise, so participants are required to extract a flag directly from a downloaded binary. These challenges offer an opportunity for participants to practice understanding of unknown, compiled code and may involve discovering a flag hidden in the code, or may require understanding how a piece of software operates in order to cause it to act in a certain way. Solutions to these challenges may require creating patches to modify the compiled code to change the way it runs and cause it to output the flag.

2.1.1.3 web

Web challenges follow the same pattern as **pwn** challenges, but involve a target that runs a web server, usually serving over HTTP, and often backed by other common web technologies such as a database. Participants exploit the web server and cause it to provide the flag. In contrast to **pwn** challenges, these challenges rarely involve low-level exploits of the web server itself; participants will rarely gain shell access to the server. Instead, these usually involve attacks on the web pages themselves, with SQL injection and PHP vulnerabilities common themes in this category.

2.1.1.4 crypto

Cryptography challenges are similar to **re** challenges but involve reverse engineering of a particular cryptographic protocol or implementation. These challenges can take the form of encrypted messages that must be broken, or access to a flawed implementation of a cryptographic protocol on a service which can be exploited to cause it to reveal secret keys.

2.1.1.5 forensics

Forensics challenges involve participants investigating an unknown piece of data, usually determining the format of the data and then finding or building a tool capable of reading the information. In these challenges, the flag is usually contained but obfuscated inside the downloadable files and participants must understand the format in order to read the flag. There are many varieties of challenges in this category, including reverse engineering corrupted file formats, mounting obscure drive formats and finding hidden files, and investigating patterns in recorded web traffic.

2.1.1.6 misc

Miscellaneous challenges that do not fall into other categories. These challenges are popular for newer participants and beginner CTFs, where they can help participants get used to the format of CTF competitions and teach introductory skills. Miscellaneous challenges are typically more gamified than other categories and often offer a chance for organisers to include more interesting, though less realistic, challenges. Examples vary hugely but might include reading the source code for a simple maze generator and solving the maze, or interacting with a service in a highly unusual way, such as via images.

2.1.1.7 programming

Some challenges are designed particularly to test the participants ability to write code. These are less common and challenges of this nature are less favoured, in preference for challenges in other categories that may require a programmed solution. This may be a response to the popularity of programming-specific hackathon competitions, distinct from security-focused CTF events.

2.1.1.8 physical

In-person events may include physical challenges that involve the participants interacting with something in the real world. This may be security-focused, or intended to encourage participants to interact with each other or explore the area. Examples of security-focused challenges include performing wire-taps of Ethernet cables, intercepting WiFi traffic, and the perennial-favourite of picking locks. Interaction-focused challenges might include giving parts of a flag to each team so they must trade parts with each other, or hiding flags on QR codes around the event location. Interaction-focused challenges are less preferred in higher skill competitions in favour of more competitive challenges.

Flags are usually a string of text in a standardised format. This enables participants to know when the challenge is successfully solved, and means that the entire process is automated without the need for a judging process. Flag formats are standardised so that participants do not need to guess what the flag is once the challenge is solved. While some competitions may use answers to questions as flags (e.g., "which IP tried to attack the server?") this is less popular and can be a frequent source of confusion and ambiguity. Most competitions embed flags into challenges in such a way that a successful solution to the challenge results in a clear flag that can be submitted. To this end, flags often begin and end with a published string, for instance often taking the format `[CTF Name]{[Flag Text]}`. In this case, the `Flag Text` contains a challenge-specific string, typically taking one of two formats:

- **A random string of text**: This has the benefit of being un-guessable and requiring participants to solve to find the entire flag rather than a partial string. In some challenges, participants may be able to recover half the flag easily, but not the whole flag.
- **A word or phrase**: In some competitions, the flag text is a short phrase, often a joke or a play on words involving the challenge and its solution. While enjoyable for participants, these can be susceptible to guessing, particularly where participants are able to get part of the flag and infer the rest.

2.1.2 Scoring

Each successful challenge completion results in the participant gaining access to a *flag* [6]. This flag can be submitted to a scoring system which then rewards the participant with some number of points. The number of points rewarded varies according to the rules of the competition, and may be affected by:

- A base score for the challenge, which may be constant across challenges or selected by the organiser to reflect the perceived difficulty of the competition.
- The time taken to solve the challenge, with challenges decreasing in value as time goes on; in some cases, special challenges may be released that must be solved within a given period.
- The number of teams that have already solved the challenge. This is mostly commonly a reward for the first team to solve that particular challenge (sometimes referred to as a "first blood" award), but may be a decreasing amount of points awarded as more teams solve the challenge.
- The number of teams that ever solve the challenge. Many CTFs award the final points based on the number of teams that have solved the challenge by the end of the competition. This means that the value of a challenge varies over time (including for teams that have already solved it). By doing this, the number of successful solves of a challenge acts as a proxy for the difficulty of the challenge, and teams are rewarded more for solving challenges that fewer teams solve.

In addition to awarding points, some competitions award prizes to the first solutions of particular challenges; this is often done in conjunction with sponsor-provided challenges, who will provide a prize for the team that is first to solve the challenge.

Each team's score is the sum of their awarded scores for each challenge, and the winning team is decided by the highest score at the end of the competition.

2.1.3 Discussion

Jeopardy CTFs offer an excellent platform for engaging participants of all levels. Because participant teams interact with the challenges independently of each other, participants are not blocked from solving problems by the success of other teams. As a result, even the lowest-scoring teams are able to engage with, and benefit from, the experience. The wide variety of categories and difficulties makes it easy for organisers to ensure that all participants are catered to, irrespective of background or skill level. The flexible nature of challenges also make these competitions suitable for a variety of time-frames, particularly when participants are spread across time-zones. Participants can start and stop their participation during the contest as required, with no pressure to participate at te same time as other teams. Teams can distribute tasks amongst team members, either as individuals or groups, and approach multiple problems at once.

In contrast to other formats, however, Jeopardy competitions are more gamified and less representative of realistic security skillsets, although this can largely be mitigated by organisers choosing suitable challenges. When teams participate in *Jeopardy* contests it is possible (and not uncommon) for each member to tackle different categories of challenges. Consequently, the co-operation between team members may be minimal and there may be little interaction between team members during a competition.

2.1.4 Variants

There are a number of Jeopardy variants currently in use, with varying degrees of popularity

2.1.4.1 Hack Quest

Hack Quests are a Jeopardy variant where participants are guided through a series of challenges, often with a (loose) story that ties them together. In this format, participants solve each challenge in turn and are granted access to the next challenge upon completion of the previous. Hack Quests are often targeted towards beginners, and act as an introduction to the CTF format. By guiding players through challenges in order, organisers can assist new participants through easy challenges and slowly increase difficulty. Associated stories and thematic elements allow for more engaging content, particularly for players who may be slow to solve challenges. Hack Quests may be run alongside other events, enabling the involvement of teams who are not able to participate in the full event (either by not having an invitation or not being capable of solving the challenges). A notable example is the Google CTF, which has a Beginner's Quest event designed for new CTF participants.

2.1.4.2 Vulnerable VMs

While most Jeopardy competitions consist of independent challenges, a common variant is to provide contestants with one or more vulnerable Virtual Machines, which teams are then able to attack to secure flags. This is categorised here as Jeopardy because the participants are not required to defend a virtual machine, and so the existence of challenges on virtual machines acts more as a challenge distribution platform than a fundamental change in the format of the competition.

2.1.4.3 Quiz-style

Some competitions adapt the Jeopardy format slightly by asking questions about the challenges to participants which must be answered to score points. These may be objective, and judged automatically, or subjective and be given to a jury to award points.

2.2 ATTACK-DEFENCE

In an Attack-Defence CTF [2] [5], teams are given access to a set of target hosts [7]. The objective of each participant team is to take and maintain control over as many of the target hosts as possible. To enable this, challenge organisers will deploy or create a range of vulnerable services, ensuring that each target contains one or more vulnerabilities.

Teams must balance the need to attack other hosts and accrue more points, with the need to patch vulnerable services on hosts they already control -- preventing other teams from compromising those hosts instead. This was the earliest CTF format, having grown from 'wargame' activities in military and hacker communities. Because of the complexity required in setting up and running events of this format, together with the comparatively-high security risks involved, Attack-Defence CTFs are more common for invitational or private events, and infrequent in public events.

2.2.1 Format

In this format, participants are tasked with successfully compromising (and subsequently securing) target servers. Each server contains one or more vulnerable services, which may be based either on real-world vulnerabilities or novel vulnerabilities created by the organisers. Participants in an Attack-Defence CTF are tasked with performing compromises on systems designed to look and act like real servers running real services.

Attack-Defence CTFs are also unusual in that participants are expected to hold control of the target, and so to perform defensive actions such as patching or mitigating vulnerabilities. Teams may be expected to deploy specific patches to vulnerable software, which might range from updating off-the-shelf vulnerable software, through to writing and applying patches directly to custom services. They may also be expected to perform general network-hardening measures, such as updating firewall rules, resetting or strengthening passwords, and disabling unwanted or untrusted services or users.

Teams may begin the competition already in control of some or all of the target hosts. In some styles, every host is always under the control of its original owner, and teams are rewarded for repeatedly performing exploits against other hosts over time, encouraging teams to fix their vulnerabilities to prevent attacks from gaining further points from that attack.

2.2.2 Scoring

Points are typically awarded on a regular interval (for example, every minute), with each team receiving a certain number of points for each host they control at that moment. This encourages participants to compromise, and subsequently protect, the servers in the contest. Competition rules typically require services to remain active and available in order for points to be awarded, to prevent teams from simply disabling vulnerable services.

2.2.3 Discussion

Attack-Defence CTFs offer a very practical model of real security scenarios, with participants gaining experience of both red-teaming and blue-teaming. Competitions in this form are often less artificial or gamified, particularly in contrast to the more-popular Jeopardy contests. Attack-Defence competitions are more suitable for spectators and live events, as observers can witness the changing control of servers throughout the event. Participants, tasked with a more rounded set of objectives, must also manage their time, splitting their attention between seeking targets, compromising them, and defending their own servers. This makes them especially suitable to team events, particularly when building or testing team cohesion is desired.

Events in this format can be more daunting to new-comers and have a higher barrier to entry. Because of the requirement to fit challenges into the format of a practical vulnerability in a service, challenge designers have less freedom and so are less able to make challenges that cater to beginners. Compounding this, the directly-adversarial nature of Attack-Defence challenges, where participants seek to directly compromise the servers of other teams, have significant consequences when participant skill levels are imbalanced; overly-capable teams have the ability to quickly overtake servers and make them all-but-impenetrable to the other teams, resulting in contests that are decided very quickly. As participants can only make progress by capturing the servers of other teams, it is possible that some teams are then unable to perform any successful exploits during the entire contest.

Establishing and running successful Attack-Defence CTFs presents more difficulties than that of formats such as Jeopardy. Participants are granted access to the target hosts, usually via a Virtual Private Network (VPN) architecture, with the aim of isolating malicious traffic and preventing accidental attacks on non-targets. Despite these precautions, participants must still take care to target their exploits onto strictly in-scope targets.

2.2.4 Variants

2.2.4.1 Exploit Contest

Moving further than even the limited gamification of Attack-Defence CTFs, some competitions encourage participants to directly attack real software to discover unknown vulnerabilities. These contest therefore act like time-limited bug bounty programmes, with participants performing valuable security research by participating. Participants in these contests have found vulnerabilities in many well-known and widely-used pieces of software.

2.2.4.2 Wargames

Wargames are closely related to Attack-Defence CTFs, but are less gamified and have a stronger focus on capability-building, particularly in the context of training security teams with realistic experience. Wargames are frequently defender-focused, in contrast to the greater focus on attackers in Attack-Defence competitions. When red-teams are present, they are usually considered part of the organisers and not participants in their own right. While these are significant and important events, they have a different role to most CTF competitions and so are not typically categorised as CTF events.

3. REPORT METHODOLOGY

To perform the analysis presented in this report, three sources were used. Firstly, the survey of members from the International Cyber Security Challenge (ICSC)[1] provided overall guidance towards the events and methodology used throughout the rest of the data gathering. Secondly, a manual selection, analysis and coding of important events was performed. Details on the selection criteria and coding used is explained below. Thirdly, to build context into the report statistical analysis of existing events was performed on a large dataset. For this purpose, the selection criteria were broader in order to sample as many events as possible.

3.1 MANUAL ANALYSIS

The manual data-gathering and analysis component of this report follows a thematic analysis [8]. Themes were pre-determined based on the requirements of the report and the experience of the report writers in similar events. This was performed in favour of a grounded theory approach due to the specific requirements of the ICSC Steering Committee and subsequent need to gather data around specific themes. In particular, it is intended that the themes selected provide readers with sufficient detail about all aspects of the organisation of CTF events.

The core data source for this report is the manual analysis of a set of CTF events. Events were chosen via selection criteria and then researched via public information available about the event. Before events were found, a set of key themes and questions within each theme were determined based around key event information, the specified requirements of the report, the requirements of the ICSC Steering Committee, and the data likely to be accessible and practical. Data was initially stored as unstructured text per-question. Once data had been gathered for each event and question pairing, the results for each question were aggregated and grouped across events into a set of non-exclusive tags. At this point, the data was standardised into a database containing the set of appropriate tags for each question and event. This structured data formed the basis for subsequent analysis and presentation in this report.

3.1.1 Selection criteria

Events were selected according to a set of criteria to ensure a balanced selection. In particular, the following were considered for each event:

3.1.1.1 Competition Format

Events were selected only if they were Capture-the-Flag events, as defined in the Background section above. In particular, events were excluded if they were not security-themed, such as hackathons (which primarily relate to development) or programming contests (whose challenges are selected for requiring particularly challenging programming). Capture-the-Flags in all the formats described in the Background section were included, with the exception of Wargames, which were excluded because they are typically organised as training exercises for established security teams, rather than open-format contests. In particular, events with both Jeopardy and Attack-Defence formats were sought. This criterion was intended to give a broad range of Capture-the-Flag events, without including similar formats that differ in theme or content.

3.1.1.2 Online and In-Person

Preference was made for events that took place in-person, and events that took place solely online were not included unless: they were related to an in-person event (for instance, they

[1] The International Cyber Security Challenge is a CTF-type of event to be hosted by ENISA in Athens in late 2021. Several agencies, universities and governmental institutions from all regions participate in the Steering Committee which is responsible for the organisation of the event.

were used to invite participants to in-person events); they had been run in-person in previous years; or they had been intended to run in-person but had been forced to move online to due disruption from COVID-19. Because of the significant logistical differences between online and in-person events, data relating to online-only events was considered less applicable to the purposes of this report. The comparative abundance of online events, however, make them beneficial when considering challenge formats, which are typically more consistent between online and in-person events. In particular, the context-building statistical analysis considered more online events, and the statistical differences between online and in-person events are detailed later.

3.1.1.3 Significance

Events were selected only if they were significant according to one of the following tests: they had a considerable number of participants, either as part of their final event or qualifiers; they were used as a qualification event into a significant event, such as the European Cyber Security Challenge; they were run, officially or unofficially, as a national-level contest, particularly when used as a selection method for a national team.

3.1.1.4 Availability of Information

To facilitate the success of this report, events were only researched where it was apparent that sufficient information about them was available publicly online. Including events that did not meet this criterion would necessarily have lead to a decrease in the confidence in the conclusions drawn. Due to the wide sampling and significant range of events that met the criteria specified, it was deemed possible to select enough events for a significant analysis without relying on events for which insufficient or low-quality data could be gathered. In particular, when gathering potential candidates for analysis, each candidate was considered suitable if it had one or more of the following: a published and accessible document of rules; a published and accessible schedule of the event; sufficient trustworthy reporting, either by the organisers or by third parties. This enabled the analysis to avoid working with events for which little or no information could be determined, and in practice almost all candidate events passed this criterion.

3.1.1.5 Explicit Mention in Survey

Events that were explicitly mentioned in the survey were considered even if they did not meet other selection criteria. The majority of events mentioned in the survey had been included through the previous criteria.

3.1.1.6 Location

Location was not used as a selection criterion and events from anywhere in the world were included. This was a particular specification of this report, and effort was made to ensure that events represented locations across the world.

3.1.2 Data sources

Data for each event was gathered primarily from public information released by the organisers. For this purpose, two primary documents were sought for each event analysed:

- A detailed rules document. These documents typically contain, implicitly or explicitly, information about the format of the competition. This can include duration, team information, selection criteria for participants, challenge formats, competition format, and other information. Because of the formal structure of most events, almost every event surveyed had a published rules document, and working from this structured data improved the subsequent quality of our data gathering.
- Published schedules: Events often publish detailed schedules, either as information for participants or as marketing material (particularly where external sponsors are involved in aspects of the schedule). Schedules provided detailed information about the length of the competition and any organiser-planned activities during the event.

On top of these documents, information was gathered from other sources published by event organisers:

- Almost every event found contained a public webpage detailing the event, either as a post-event summary or as a record of pre-event marketing and information. These websites were a source for general information about events but often lacked specific details, except when contained within the documents listed above.
- In some cases, particularly open-format events, access into the platforms used during the event was still available. This enabled direct data gathering, particularly when concerned with challenge formats and information. Where platforms contained a record of organiser communication during the events, a considerable about of information across data themes could be gathered directly or by inference from records of public communications.

In some events, little event information was published by the organisers. This was more common for events that were not open to participation applications, such as in directly invitational events. While the majority of these events would fail to pass the stated availability of information selection criteria, some events had sufficient data published about them from third-party sources. In particular, news articles reporting the outcome of the event frequently contain some information about the structure and format of the event.

In some cases, direct experience with the events being researched was available and in these cases this was used to inform the data gathering.

3.1.3 Themes

Once events had been selected and filtered according to the selection criteria, they were researched individually through the sources described above. During the research of each event, data in a specific set of themes was gathered. Furthermore, each theme consisted of a set of questions. Each question was answered in free-text by researchers during the compilation process, before any coding was performed. Each theme was established in order to address the general concerns of this report. Questions were determined by considering the information that would be most beneficial towards the aim of the analysis and report, with concern for the practicality of gathering the data via the identified sources.

Questions were gathered into themes in order to aggregate limited information into workable collections, and to provide structure to the data gathering and analysis process. Consequently, this report is laid out with these themes in mind, and analysis is broken down by theme to aid comprehensibility and make clear the connection between gathered data and conclusions drawn.

3.1.3.1 Theme 1 – Entry Requirements

Participants for all events studied were required to meet some set of entry requirements in order to participate. In particular, events frequently had age requirements or the requirement to be at a particular school level. Data was gathered on the following questions:

Age: Did the event have specific age requirements for participants, either as an upper- or lower- bound on the ages of participants? Were teams all required to be the same age? Were teams of different ages put into different competition categories?

Status: Did the event require participants to be a member of a particular organisation, such as a school or university? Were teams of different status put into different competition categories? Did participants have to have demonstrated previous success at other events? This does not include succeeding at an event-specific qualifier.

Qualifications: Did the event require participants to hold any particular qualifications? Were they required to pass any tests, either formal or informal, in order to attend? This does not include successfully competing at other events.

Location: Did the event require participants to be of a particular nationality, or reside in a particular country? Did the event have different prizes or categories for participants from different locations?

3.1.3.2 Theme 2 - Diversity and Inclusion

To address diversity requirements, and improve inclusion across a variety of measures, events sometimes published information about efforts made to encourage, or improve access for, under-represented groups. In particular, many events have had a significant gender imbalance and had considerably more male participants. Data was gathered on the following questions:

Gender: Did the event have competition rules designed to encourage female participation? Did the event have competition structure designed to encourage female participation, such as grouping participants by gender?

Socio-economic: Did the event have competition rules designed to equalise socio-economic disadvantages? Did the event make considerations for participants with socio-economic disadvantages?

Ethnicity: Did the event have competition rules designed to encourage underrepresented ethnicities?

3.1.3.3 Theme 3 - Challenge Format

Data was gathered regarding the format of challenges; that is, specifically relating to the competition itself and how participants competed, including how they were scored and whether or not they were competing for prizes. Theme 3 is distinguished from Theme 4 by considering the specific competition process rather than the more general format of the competition.

Format: Which CTF formats did the challenges come from? Did the event contain only one format, or contain components of multiple formats?

Challenge Categories: Which categories were challenges drawn from? In the case of Jeopardy-style events, which categories were challenges from? In the case of Attack Defence-style events, which aspects of Attack-Defence competitions were part of the competition?

Scoring: What scoring methods were used for scoring participants? Were there multiple ways to score points through challenges? Were there any non-challenge ways to earn points towards winning the competition?

Platform: What platform was used by the event? Was the platform custom-made? Was the platform an existing off-the-shelf solution?

Prizes: Was there a prize for the winning team or teams? Were there prizes for particular challenges? Were there prizes for other parts of the competition, such as providing challenges or writing write-ups?

Length: How long was the competition period? Was it broken up into multiple period, or continuous? If the event was online, were participants able to begin their competition period on-demand?

3.1.3.4 Theme 4 - Competition Format

The competition format concerned more general parts of the competition that were less related to the challenges and more to how the competition took place. In particular, whether there were multiple parts to the competition, such as qualifiers or parallel events, and whether teams were allowed mentors or coaches.

Team Size: Was there a maximum team size? Was there a minimum team size? Were teams formed by participants in advance of the competition or formed by the organisers after selection of participants?

Mentors and Coaches: Were teams allowed a mentor or coach? Were teams required to have a mentor or coach? Were teams assigned a mentor or coach by the organisers?

Qualifiers: Did the event have a separate qualifier round? Did participants have to achieve the top scores in the qualifiers to compete, or was the qualifier only part of the selection process? Was the qualifier a specific event run by the same organisers or was it based on other events run by different organisers?

Parallel Contests: Were there other competitions, other than the primary competition, running at the event? Were they targeted at a different audience? Did they have a different theme or challenge categories? Were they an extension of the main competition with further challenges of the same type?

Online or In-Person: Was the event run entirely online? Was the event entirely in-person? Was the event a mixture of both, such as having an online portion leading into an in-person event? Was the event simultaneously in-person and online, for instance to cater to different groups or to host different formats? Did this differ from previous events, in particular because of COVID-19 restrictions or concerns?

Organiser Communication: Did the organisers communicate with participants during the event? Did the organisers provide help using the platform during the event? Did the organisers give hints during the competition? Did the organisers help participants with challenges when requested?

Challenge Providers: Did the organisation create all challenges? Did the event use existing challenges, such as from a platform or challenge provider? Were participants expected to provide challenges?

3.1.3.5 Theme 5 - Event Organisation

Beyond the format of the event, this report also seeks to gather data on non-competition activities run alongside competition events. For instance, whether social events were put on as part of the competition, and whether participants were expected to find their own funding for travel and accommodation expenses.

Other Activities: What other activities were organised by the event, in addition to the competition? Were there any social activities? Were there sponsor-led activities? Were there activities designed to benefit participants, such as career events?

Catering: Was the event catered by the organisers? Was catering only during the competition period or during the entire event period, such as dinners after competition days?

Transport and Accommodation: Did the organisers provide funding for transport to the event? Did the organisers provide funding for accommodation expenses for participants?

3.1.3.6 Theme 6 - Post-event

Once CTF events are completed, participants often request, or provide, solutions to the challenges. In particular, the creation and sharing of solution write-ups for challenges is a significant and important part of the community. Data was sought to discover if this was supported or resisted by organisers.

Challenge Distribution: Did organisers release the challenges publicly once the competition was over? Did the organisers explicitly prevent participants from sharing challenges themselves?

Solution Distribution: Did organisers release solutions publicly once the competition was over? Did the organisers explicitly prevent participants from sharing challenge solutions themselves? Did the organisers actively promote participants who created write-ups, for instance by having prizes or featuring solutions?

Data Release: Did organisers release data gathered during the competition? Did organisers publish participant statistics, such as participant numbers or breakdowns?

Subsequent Publications: Did the organisers make formal publications as a result of the competition and data gathered?

3.1.4 Coding and aggregation

Once data was gathered in free-text format for each theme and sub-theme, data for each question was viewed laterally across the whole set events. This was used to study the spectrum of results for each question and provide justification for a coding system. For this, a non-exclusive tagging system was used, where the free-text answers for each question were tagged with zero or more tags that categorised their answer. Tags were selected to appropriately cover and aggregate the data seen in the free-text answers. Every question could also be tagged as *Unknown*, where data found was insufficient to properly classify which tags were appropriate. In some cases, additional primary research was performed to determine which tags should be applied, and in this way research on each event was driven as a comparison to other events in the dataset.

As part of the tag creation process, data for each question underwent aggregation into suitable, granular categories. This was performed to facilitate later analysis and to avoid over-specificity in cases where considerable amounts of data were present. This was particularly important where events had very little available data.

In some cases, multiple question groups were aggregated together to provide more content across all events. The rest of this report is structured around discussion of each theme, and data is presented in these aggregated groupings so that each grouping provides sufficient detail for meaningful analysis and discussion.

3.2 STATISTICAL ANALYSIS

To augment later discussion and provide context to the events studied in detail, a statistical analysis was conducted over a large, public dataset.

The dataset consists of events tracked by the CTFTime website (https://ctftime.org); populated voluntarily by the CTF community, with records submitted either by organisers or participants. CTFTime is a notable community website that lists events and tracks team performance across multiple competitions. It is also public and free-to-access, both for readers and CTF organisers, such that announcing a CTF event is accessible even with minimal financial resources. As such it is a de facto publication platform for CTF events and therefore a data source that is likely to be accurate and complete. The website also offers an open API to allow analysis of the data.

The dataset was compiled from data retrieved via the open API and cover the period 01/01/2015 -- 06/12/2020; including data on events and contained challenges.

From manual inspection, event records were overwhelmingly complete and consistent, with only a small number of empty or invalid entries. Challenge records were less complete, with only approximately 73% of events having challenge records associated to them. Challenge records would only be expected for events in a Jeopardy format, but records were incomplete for even this subset. Nevertheless, the data were considered to be easily sufficient.

3.2.1 Dataset structure

The records contained in the dataset incorporate the following information:

Event

- **Title** : The name of the CTF event
- **URL** : Website for event
- **Format** : Event type; with values within [Jeopardy, Attack-Defence, Hack Quest]
- **Restrictions** : Entry restrictions; with values within [Open, High-School, Academic, Prequalified, Invited]
- **Start** : Event start time (to minute accuracy)
- **Finish** : Event finish time (to minute accuracy)
- **On-site?** : Flag indicating in-person events, instead of online
- **Location** : Physical location (applicable only for on-site events)
- **Weight** : A metric intended to track CTF event difficulty, for the purposes of ranking teams. The weight is determined either by voting among competing teams or by decision of CTFTime administrators. Weight values run from 0 (easiest) to 100 (most difficult).
- ***Challenge*** : Subsidiary records describing challenges within a CTF competition
    - **Name** : The name of the challenge
    - **Points** : Points awarded on completion of challenge
    - **Write-up count** : Number of published write-ups associated with the challenge
    - **Tags** : A list of attributes for the challenge, typically used to encode the challenge category at minimum, with greater specificity provided in some cases

4. ANALYSIS RESULTS

4.1 MANUAL ANALYSIS

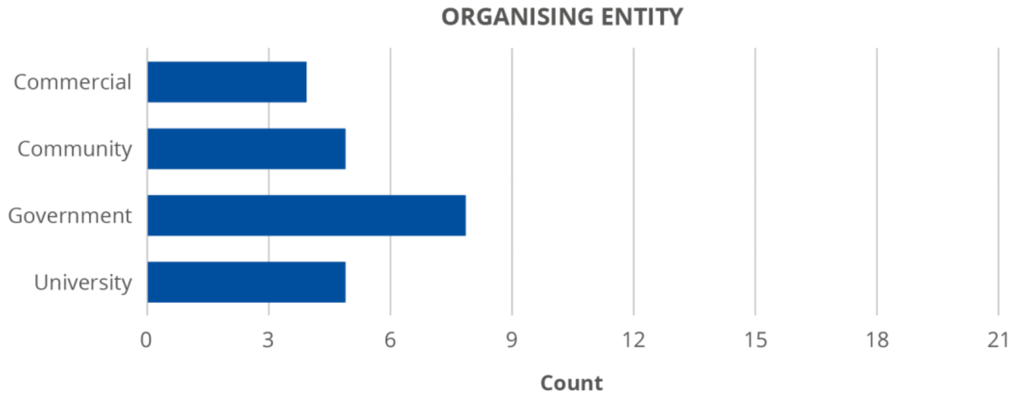
Following the selection process, a total of 22 CTF competitions were included in the manual analysis. The competitions are listed below, with a longer profile for each given in Annex A.

- European Cyber Security Challenge
- Cyber Centurion - CSC UK
- ACSC-ASEAN
- Cambridge 2 Cambridge Cyber Competition
- Country 2 Country
- Cyber Challenge Italia
- Cyber Security Challenge Canada
- Cyber Security Challenge Germany
- Cyber Security Challenge SA
- DEF CON CTF
- Midnight Sun Capture the Flag (AFCEA Sweden)
- PicoCTF
- Pwn2Own
- US Cyber Challenge
- WCTF (Qihoo 360)
- CyberTalents Arab and Africa Regional CTF
- National Collegiate Cyber Defense Competition
- International Collegiate Cyber Defense Competition
- Global Cyberlympics
- PlaidCTF
- HITCON
- Google CTF

The analysed CTF competitions were variously organised by governments, universities, for-profit companies and community groups (see **Figure 1**). Government events were organised either by national-level governments or supra-national bodies (such as the EU bloc), with no local-government events in the analysis. University-run CTFs often had government support, either through partnerships or via research-body funding.

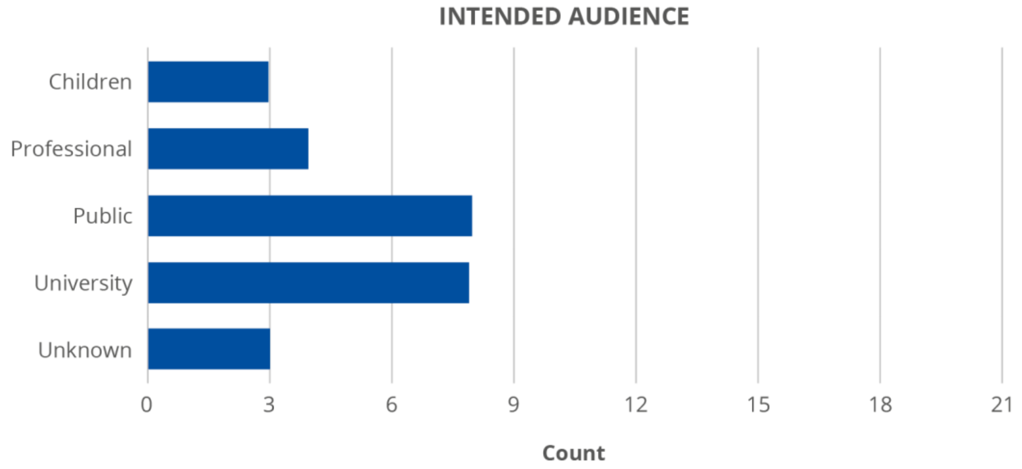
Some university events sought to perform research in cybersecurity education, using the event as a study, and publish findings as research papers. In other cases, the delivery of that education and the promotion of cybersecurity careers was the main goal. Of the four commercial events, three were operated by large, well-known technology companies, while one was run by a cybersecurity recruitment agency. Community events were often, but not always, attached to security conferences.

Figure 1: Breakdown of Events by Organising Entity



The majority of the analysed events were intended either for the general public or for students in tertiary education (see **Figure 2**). However, a small number specifically targeted school-aged children to promote early cybersecurity education. The structure of these varied; with one restricting entry solely to children, while others were open to wider age groups in another stream of the competition. Most public CTFs were open to wide participation among hobbyists and professionals. Four competitions were noted to target only skilled professionals in the area, either with specific entry restrictions or de facto due to low entrant limits and high challenge difficulties.

Figure 2: Breakdown of Events by Intended Audience



4.2 PER-THEME ANALYSIS

This section describes the results of manual analysis. Results are presented on a per-theme basis.

4.2.1 Entry requirements

Age is the most common entry restriction, with competitions open to 'children only', 'university students only' or 'adults only' (see **Figure 3**). This restriction is alternatively captured with no age specification, but a requirement that entrants be of a given type, or possess specific skills (**Figure 4, Figure 5**). Events targeted at a general audience generally make no restrictions however (excepting that minors be accompanied). While globally-available, online competitions were typical in community-organised and commercial events, location restrictions were common for publicly-funded events (operated either directly by governments or through universities). These required entrants to be from a particular nation, or group of nations, with the restrictions complemented by further regional subdivisions in two cases (**Figure 6**).

Figure 3: Breakdown of Events by Age

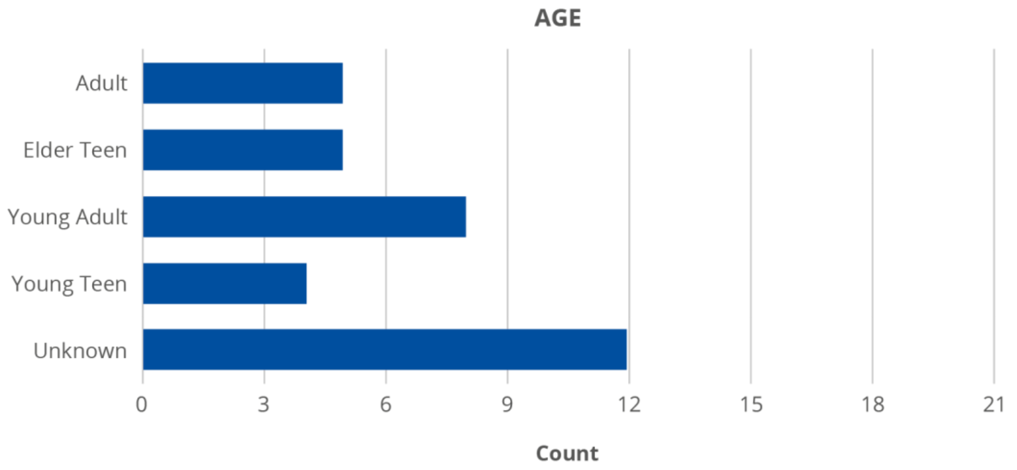


Figure 4: Breakdown of Events by Participant Type

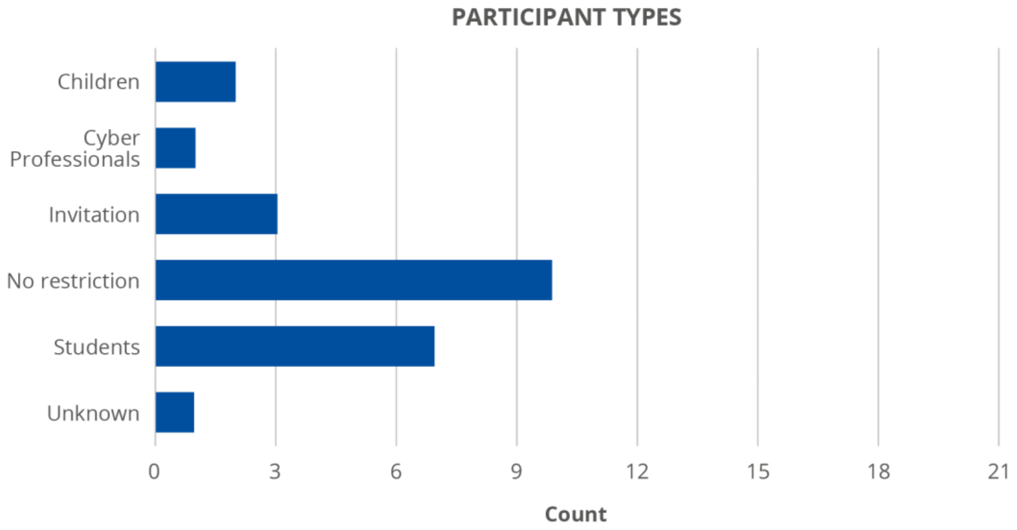


Figure 5: Breakdown of Events by Qualifications Required

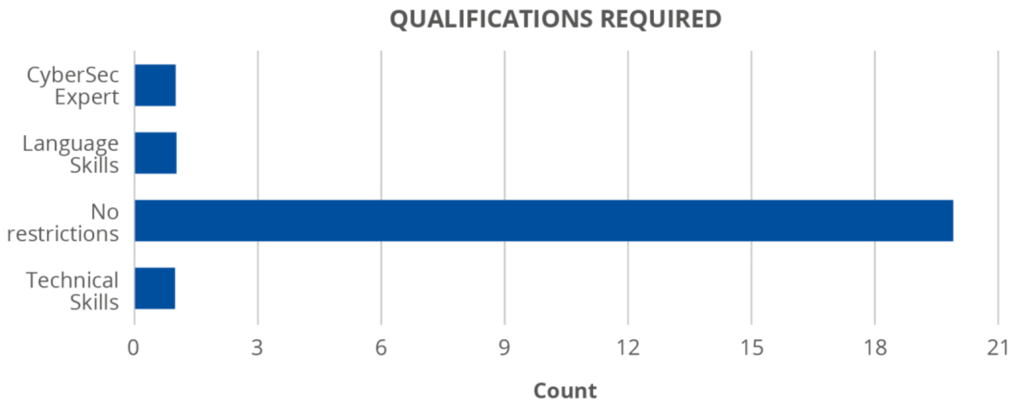
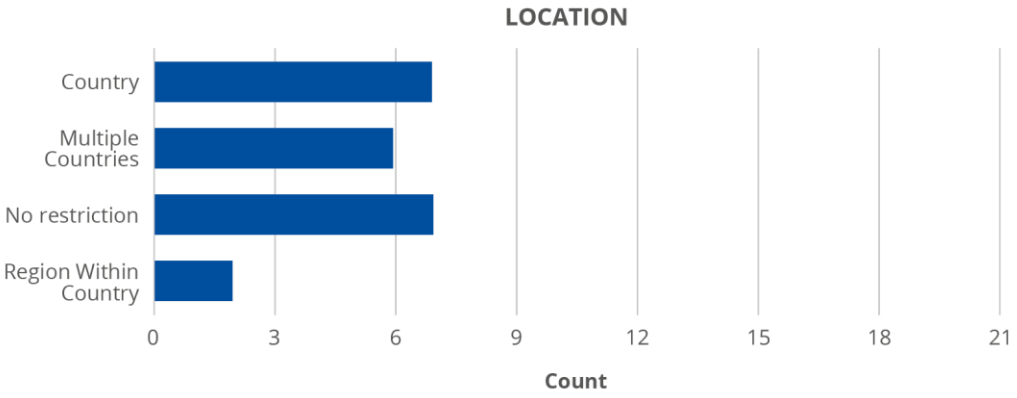


Figure 6: Breakdown of Events by Location



4.2.2 Diversity and inclusion

Of those examined, no event restricted entrance by gender (see **Figure 7**). In the case of the UK's Cyber Centurion competition (an event aimed at children), teams were categorised by gender. In two other events teams with female members received a bonus in competition. No restrictions were made by socio-economic background either (**Figure 8**). Only the large, public PicoCTF made any direct reference to economic accessibility, with the organisers specifically stating that the competition platform had been designed to be easily accessible to those with low-cost hardware. In some events, equipment was provided by the organisers, although this was typically to avoid competitive advantages, rather than to promote access. No event was found to indicate any policy for diversity by ethnicity (**Figure 9**).

Figure 7: Breakdown of Events by Gender Restrictions

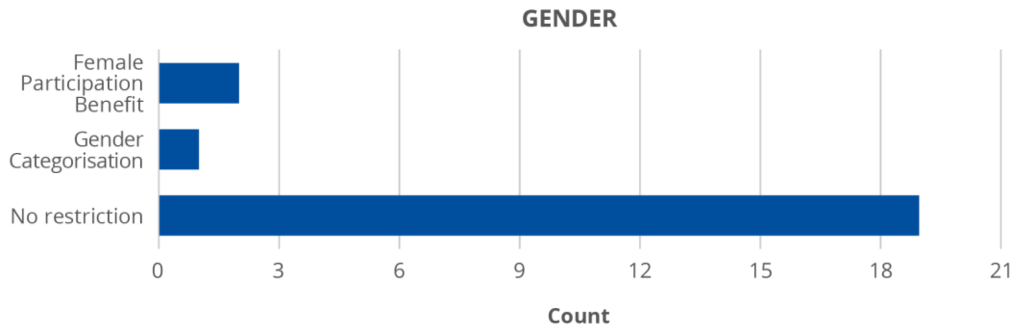


Figure 8: Breakdown of Events by Socio-Economic Restrictions

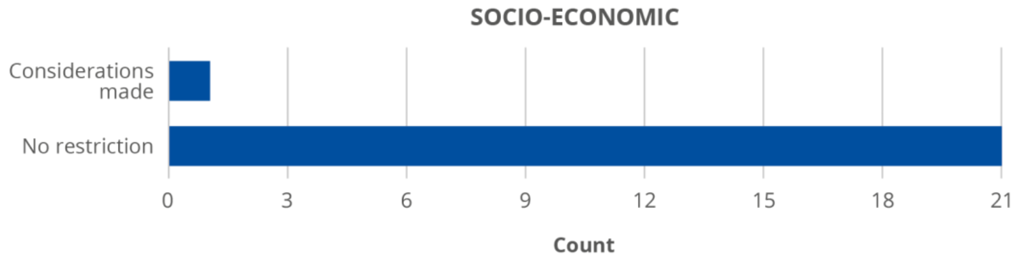
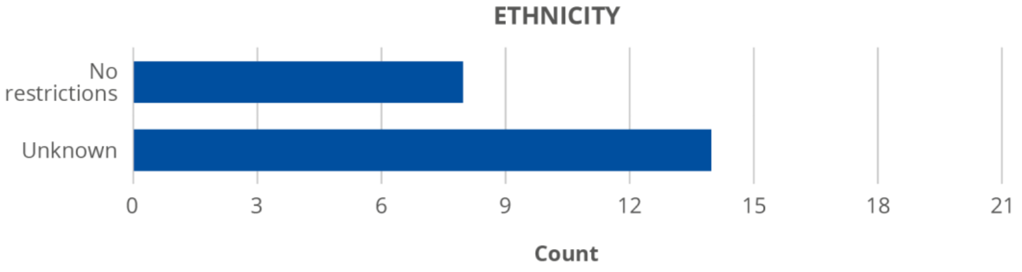


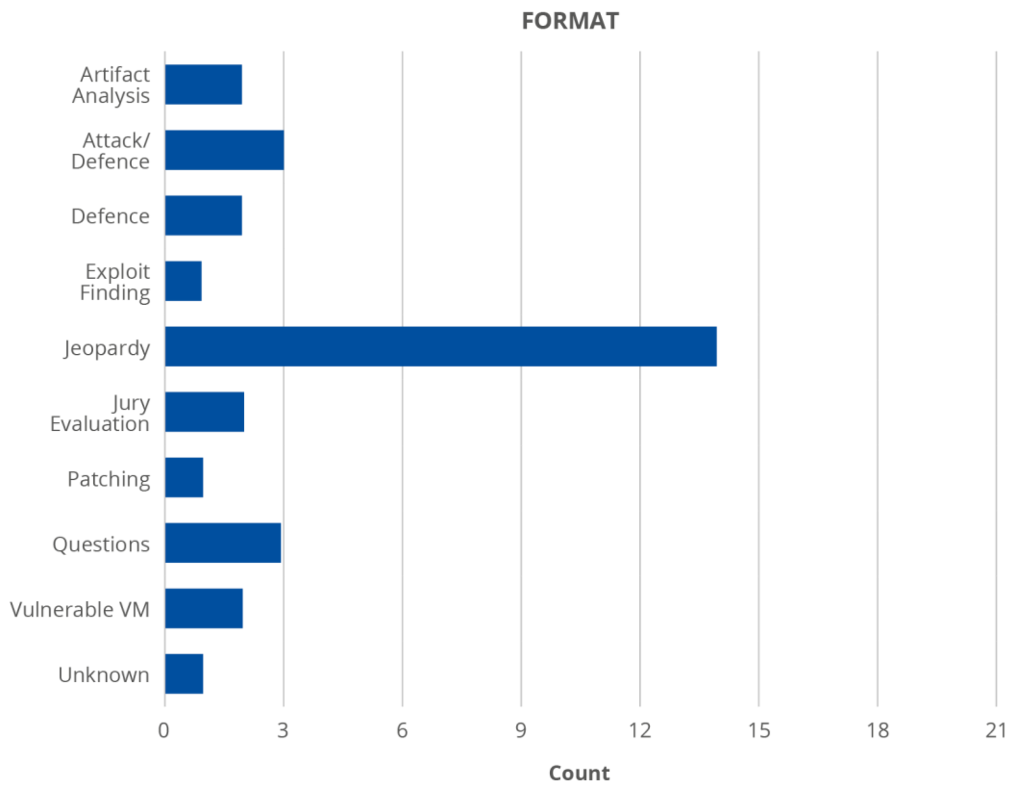
Figure 9: Breakdown of Events by Ethnicity Restrictions



4.2.3 Challenge format

The analysed CTF events displayed a wide variety of configurations. The majority of competitions were in the Jeopardy format, by a substantial margin, with Attack-Defence and question-based competitions the most popular of the other categories (see **Figure 10**). The popularity of head-to-head Attack-Defence was higher for in-person competitions, although Jeopardy competitions were also common here. Yet, a range of unusual derivatives were also noted, including questionnaires, individual attack campaigns against vulnerable virtual machines and patching exercises. The US-based National Collegiate Cyber Defense Competition and International Collegiate Cyber Defense Competition both followed an unusual defence-only format in which entrants acted as a 'Blue Team' pitted against an attacking 'Red Team' formed of volunteers who were cybersecurity professionals.

Figure 10: Breakdown of Events by Format



Popular challenge categories were represented across the examined events, with Crypto, Exploitation, Forensics, Web and Reverse Engineering commonly appearing (see **Figure 11**). As noted above, defensive categories were also well-represented, both as defence against targeted attacks and defence against malware. Where reported, major CTFs typically operated custom platforms (**Figure 12**), although external hosted services were occasionally seen (indeed, the same HackingLab hosted platform was used in two cases).

It is suspected that popular open-source platforms were utilised for these custom arrangements, rather than software developed from scratch, although hard data was not available to support that. Scoring was primarily seen to be fixed, with specific point values given for Jeopardy challenges or successful Attack-Defence captures and holds (**Figure 13**). Most variants upon scoring included either modified point values, an element of manual grading or additional points for special cases (such as 'King-of-the-Hill' in Attack-Defence). In one notable case, Qihoo 360 WCTF operated primarily on a Jeopardy model, but supplemented the main solution points with an additional round in which solutions were evaluated by a technical jury and awarded bonus points.

Figure 11: Breakdown of Events by Challenge Category

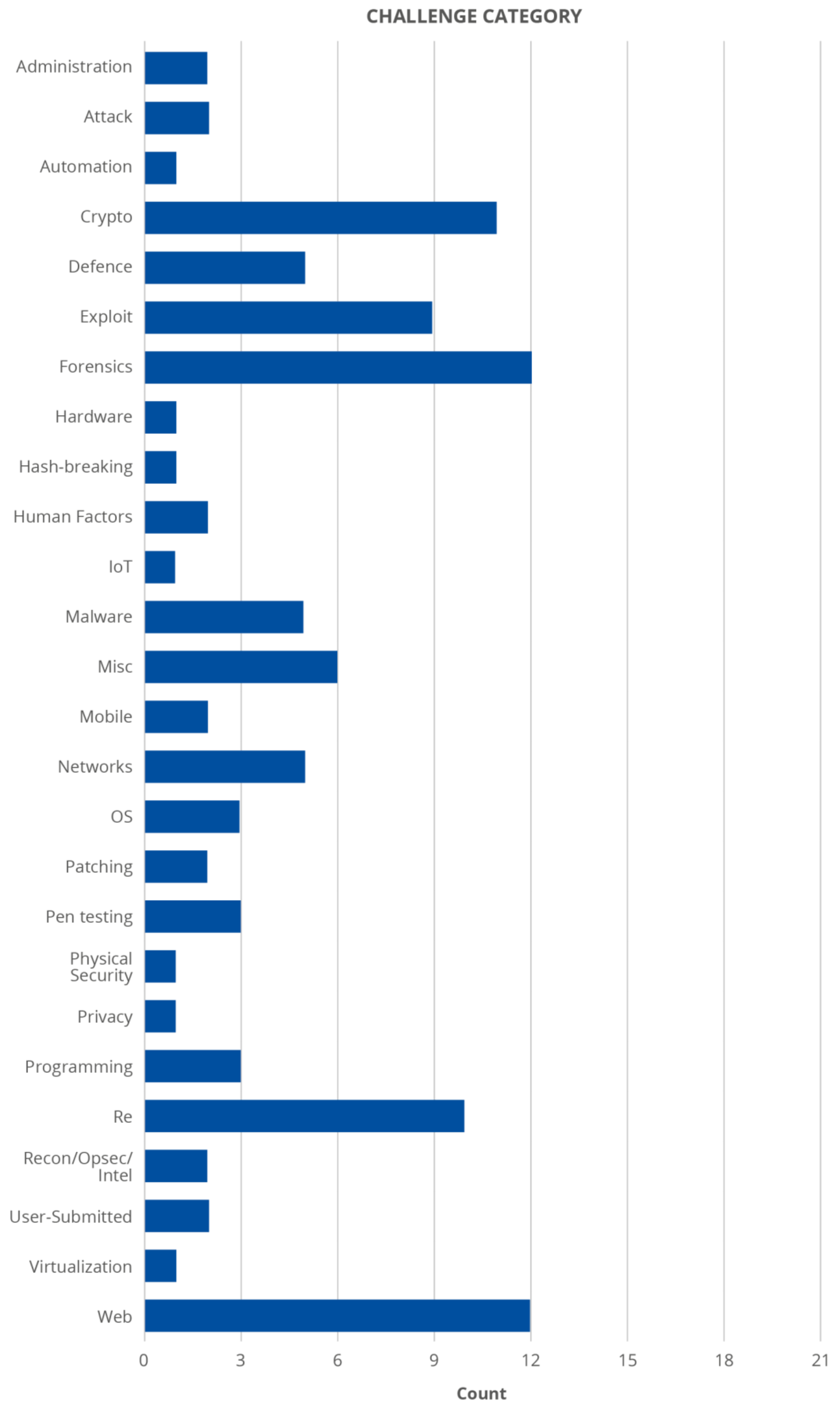


Figure 12: Breakdown of Events by Platform

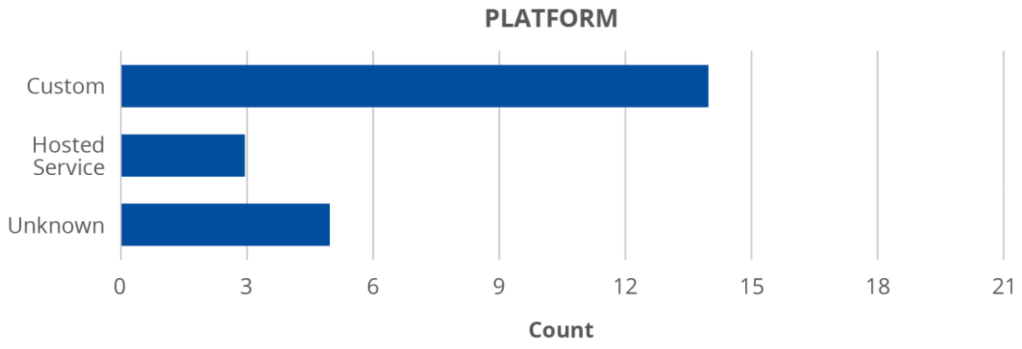
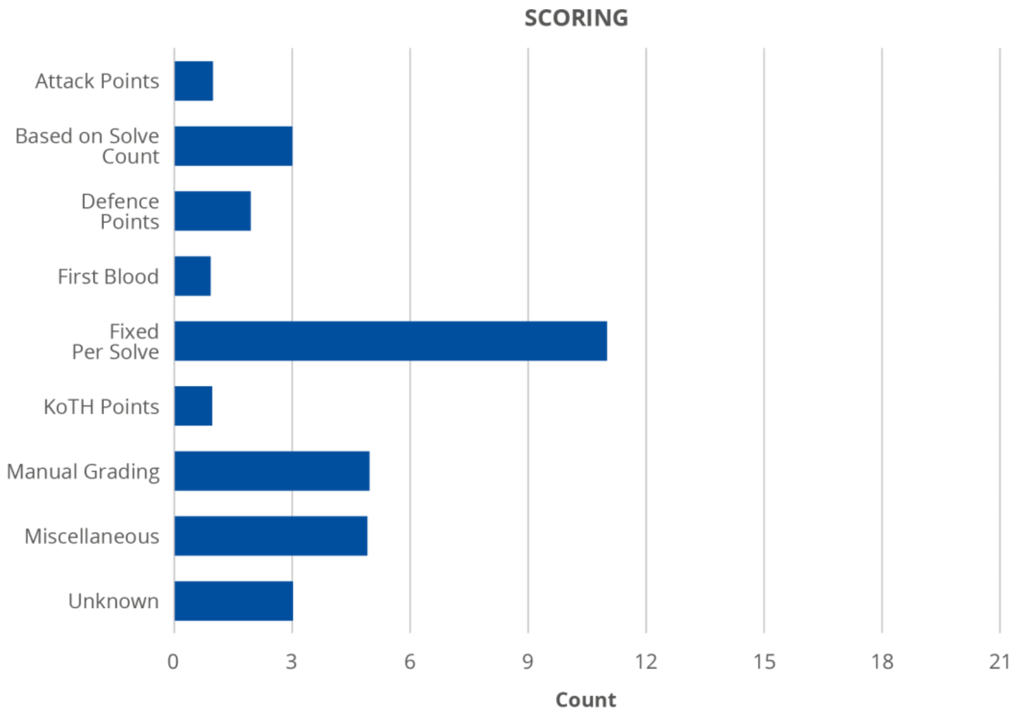


Figure 13: Breakdown of Events by Scoring



It was found that winners' prizes were commonly awarded (see **Figure 14**). These were either items of consumer technology, cash prizes, or invitations to other prestigious events. There was wide variation in this rule, however. The Pwn2Own competition operates as a live bug bounty event, in which successful attacks have direct commercial applications, and as such carries cash prizes up to $80,000 (USD).

By contrast, the very well-respected, DEF CON CTF offers prizes with low monetary value -- but enormous prestige in the community. Ancillary prizes were occasionally awarded for contributed challenges and stand-out actions ("the je ne sais quoi award" in Cambridge2Cambridge), but these were not common (**Figure 15**).

Figure 14: Breakdown of Events by Winner Prize Inclusion

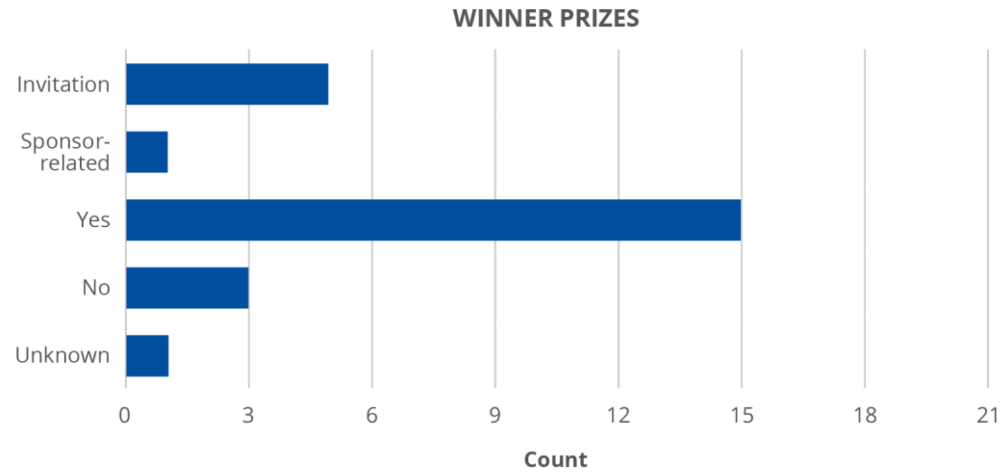
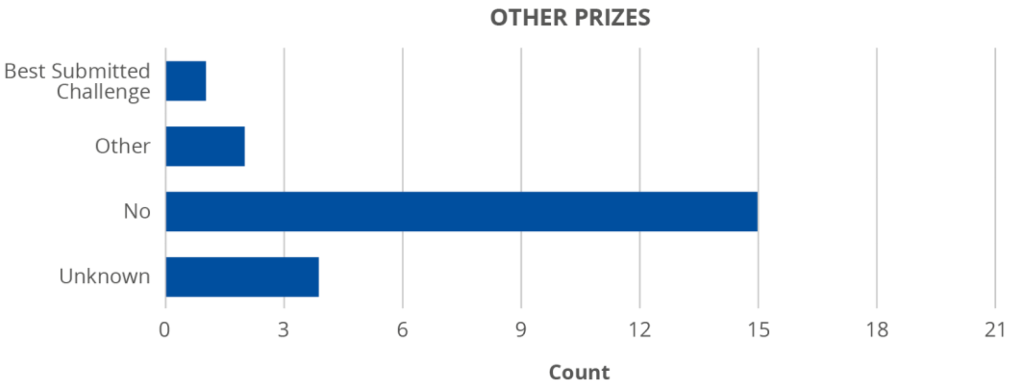
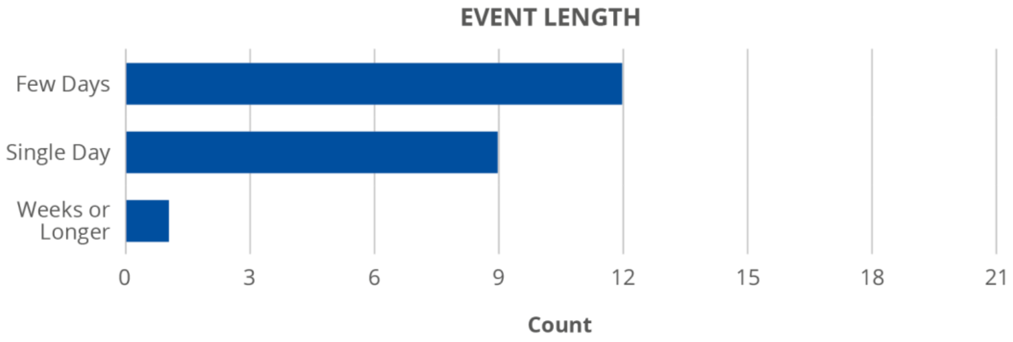


Figure 15: Breakdown of Events by Other Prize Inclusion



Most events were short, with 2--3 day CTFs marginally more popular than single-day CTFs events (see **Figure 16**Figure 16). As many of the analysed events were large, in-person competitions; operating short, focused events is understandable -- both in terms of cost and available participant time. Online competitions typically ran for longer periods; consistent with being background or hobby activities rather than full-time pursuits.

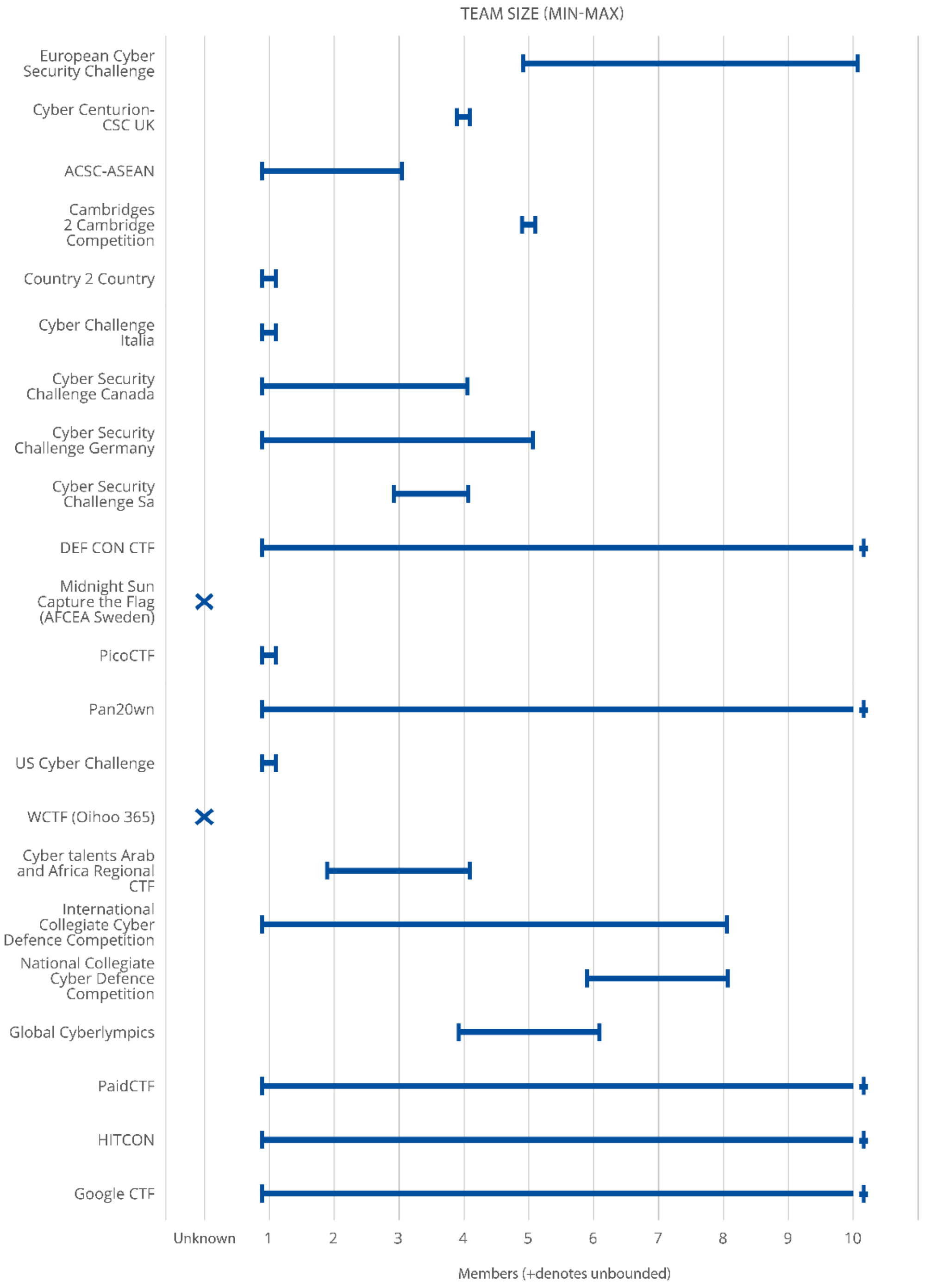
Figure 16: Breakdown of Events by Length



4.2.4 Competition format

Team size requirements in the analysed competitions varied widely, as **Figure 17** shows. More competitions permit a team-size range, than prescribe an exact team size. Where a bounded range was permitted, the largest size was never higher than 10 and usually less than 5. However, in a set of major community-run events (and one commercial event) team size is unbounded. Of these, three events were online, where team sizes cannot easily be enforced, while one was in-person (providing up to 8 team seats, but no limit on external access). The other event was Pwn2Own, an exploit finding competition, in which team size is not so strongly connected to performance as in other formats.

Figure 17: Breakdown of Events by Team Size Restrictions



From those analysed, more events incorporated qualifying rounds than did not, although this is skewed by the selection of renowned competitions and 'finals' events with limited memberships -- open competitions typically have far more entrants (see **Figure 18**). Competitions operating in-person or online were equally matched (**Figure 19**). However, in 2020, a handful of events were moved online due to COVID-19, despite otherwise being held in-person. Events were split between allowing a mentor with a team and prohibiting this (**Figure 20**). Where allowed, mentors were variously an accompanying adult (for children), an employer or a prior competitor at the event.

CTF organisers typically provide at least technical support for entrants, with hints being provided in some cases. Few CTFs made a concrete statement of the communication policy and the availability of hints was very rare (**Figure 22**). A handful of events operated parallel competitive contests alongside the main challenges (**Figure 21**) and these were either targeting another audience (i.e., a student tier of a professional competition) or adding additional challenges of a different type (e.g., hardware attacks, physical security challenges or a social engineering exercise during social events).

Figure 18: Breakdown of Events by Qualifier Round Inclusion

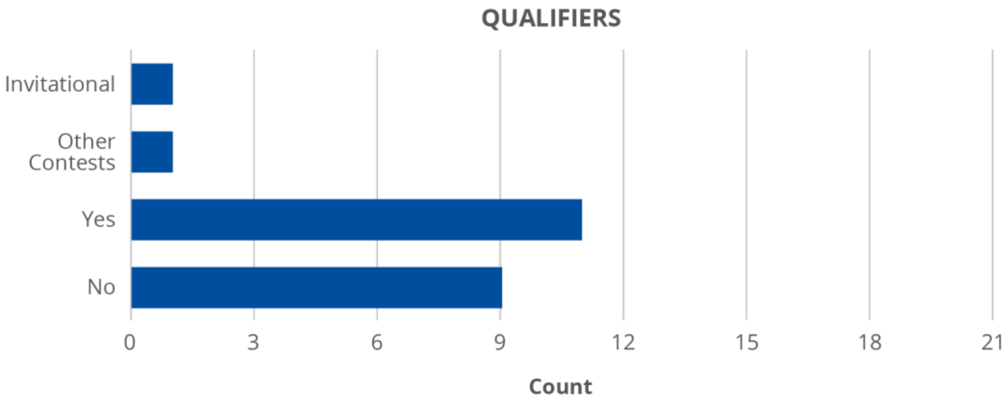


Figure 19: Breakdown of Events by Physicality

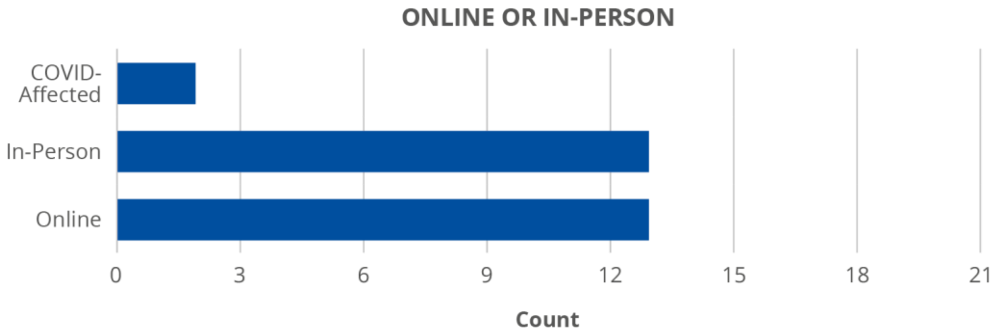


Figure 20: Breakdown of Events by Mentor/Coach Allowance

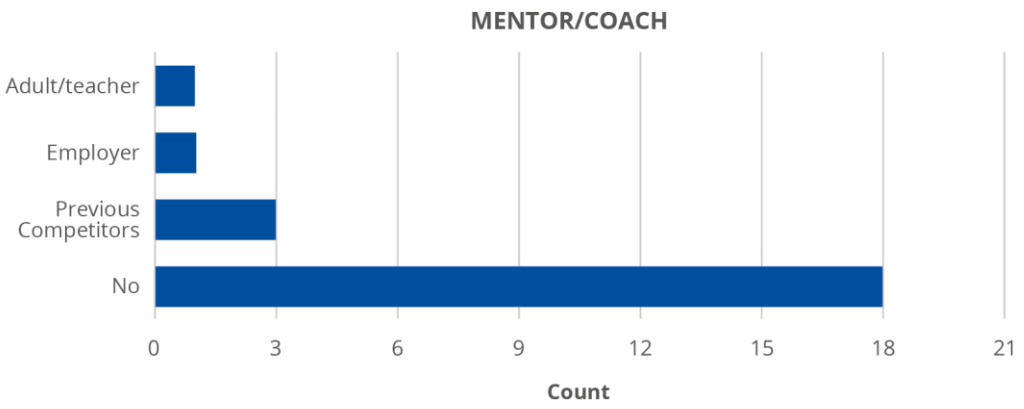


Figure 21: Breakdown of Events by Inclusion of Parallel Contests

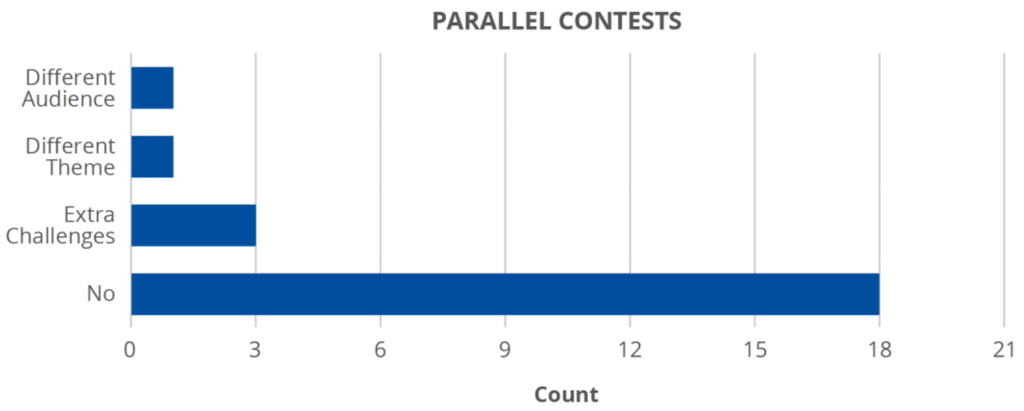
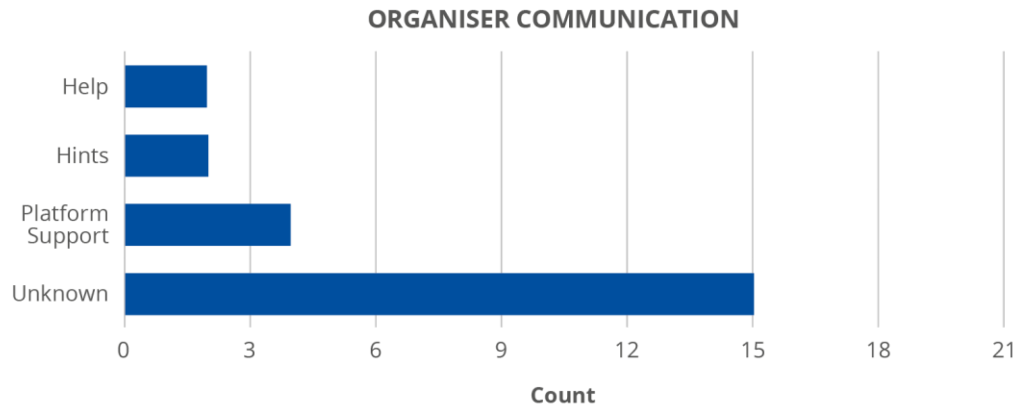


Figure 22: Breakdown of Events by Organiser Communication Policy



4.2.5 Event organisation

Peripheral activities were incorporated in just under half of the examined CTFs, principally social and careers activities (see **Figure 23**. Catering was often provided for in-person events, with transportation provided occasionally (**Figure 24, Figure 25**). In one interesting case (Cyber Security Challenge Canada), catering was provided for a nationwide, online event with participants distributed across the country. In no other cases was catering or transportation made available for an online event.

Figure 23: Breakdown of Events by Other Activity Inclusion

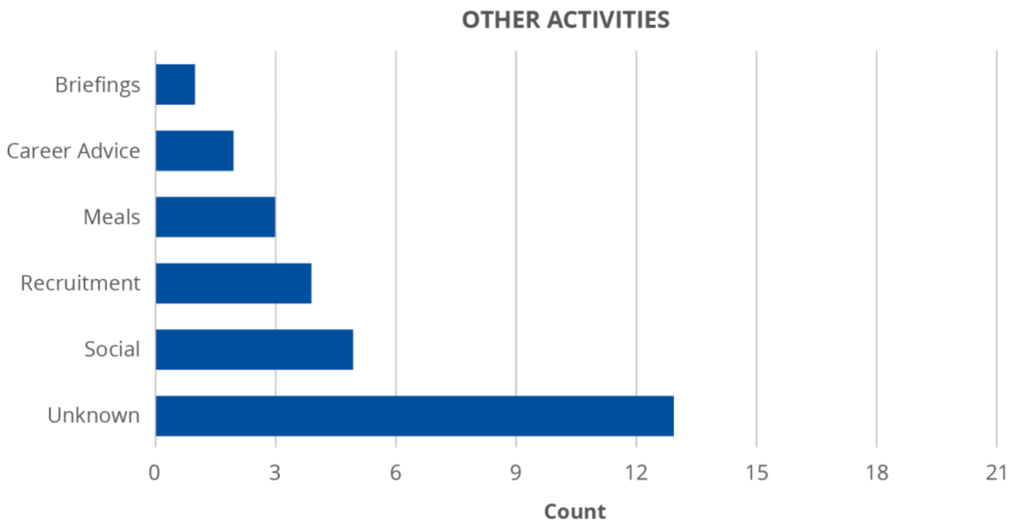


Figure 24: Breakdown of Events by Catering Provision

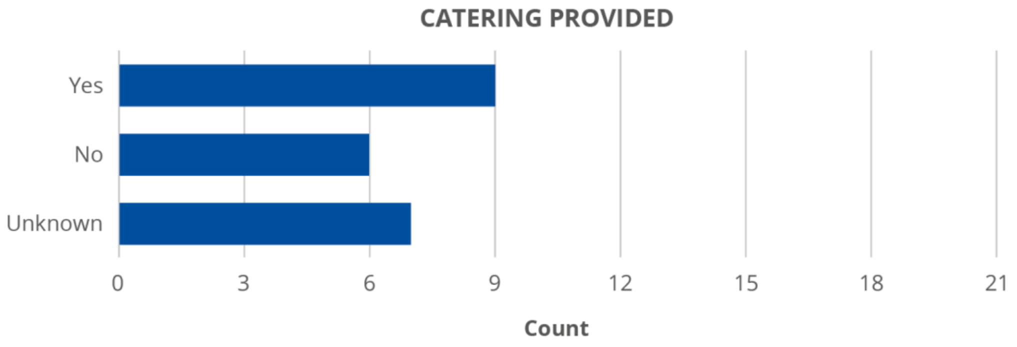
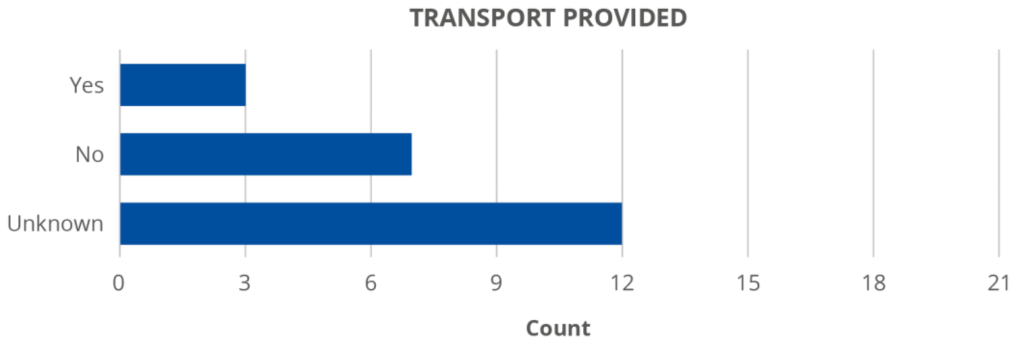
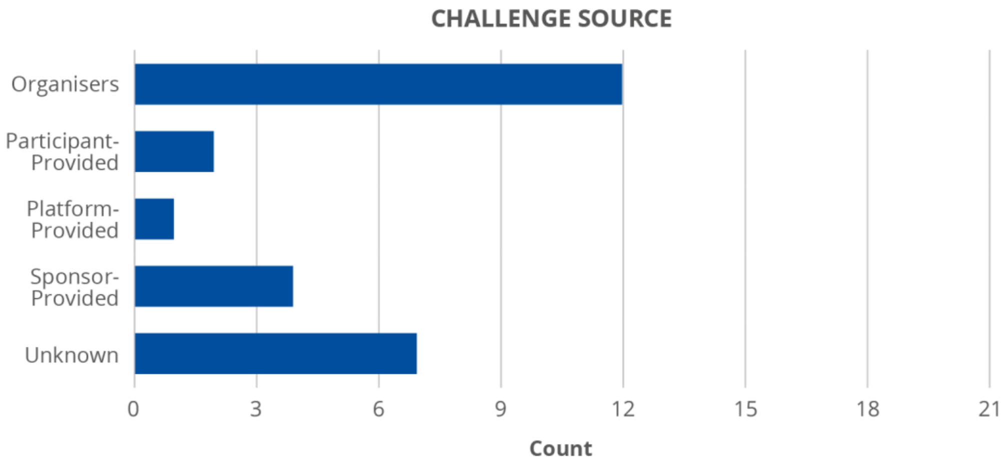


Figure 25: Breakdown of Events by Transport Provision



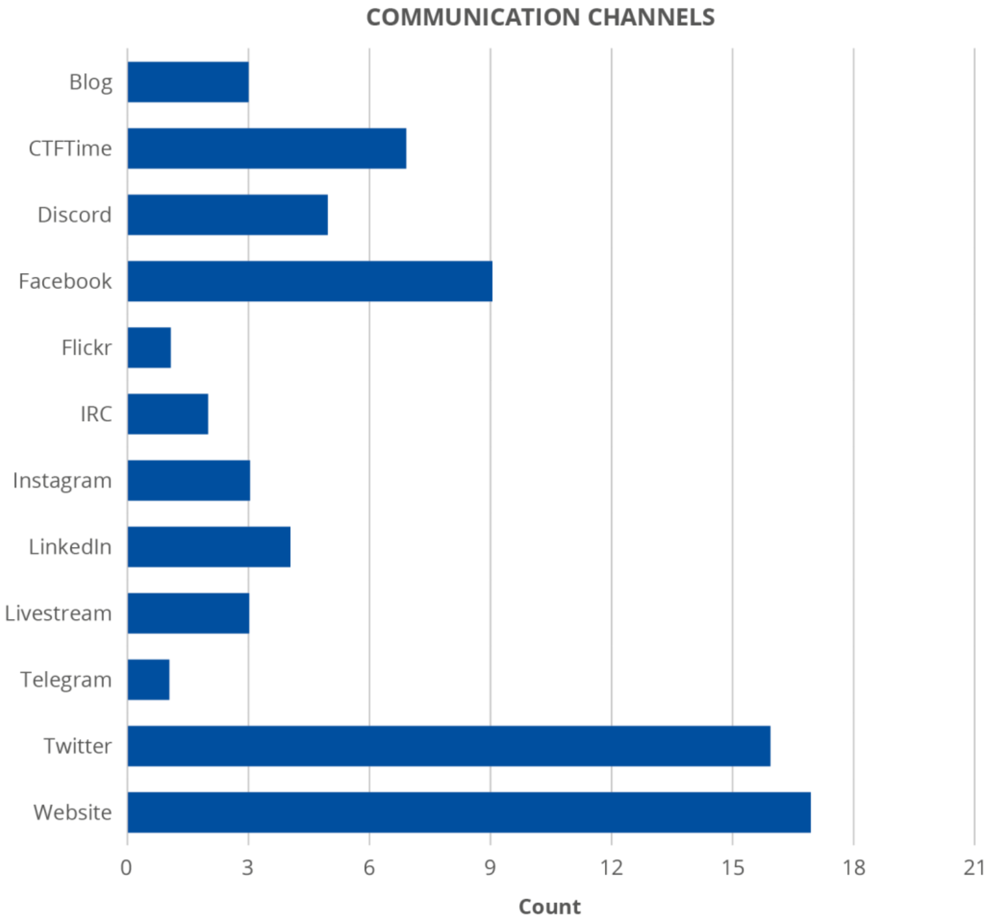
Where information was available, CTF challenges were mostly provided by event organisers, with a small number incorporating challenges from sponsors (see **Figure 26**). A handful of events asked participating teams to produce challenges, or used those provided by a hosted platform.

Figure 26: Breakdown of Events by Challenge Source



Events were advertised over a range of media (see **Figure 27**). Events usually (although not universally) hosted a public website. Twitter was used nearly as frequently to disseminate information. Live updates, via Twitter, blogs, Discord channels or a video feed were a common feature. Live streaming of competitions is rare, but seen both for in-person events (National Collegiate Cyber Defense Competition, Qihoo 360 WCTF) and one online event (GoogleCTF). In the latter case, it was a competition requirement for finalist teams to stream their work from a designated computer and these streams are available on YouTube.

Figure 27: Breakdown of Events by Communication Channel



4.2.6 Post-event

In the examined events, the amount and type of information released by CTF organisers was varied. Challenges and solutions were officially released for 28% and 23% of events, respectively (see **Figure 28, Figure 29**). However, these numbers should be considered with some context. Challenges accessed after a competition were sometimes broken (e.g., where a webservice must be attacked, this was often found to be unavailable), while unofficial solutions (in the form of participant write-ups) were often plentiful even if no official solutions were released.

Figure 28: Breakdown of Events by Challenge Release Policy

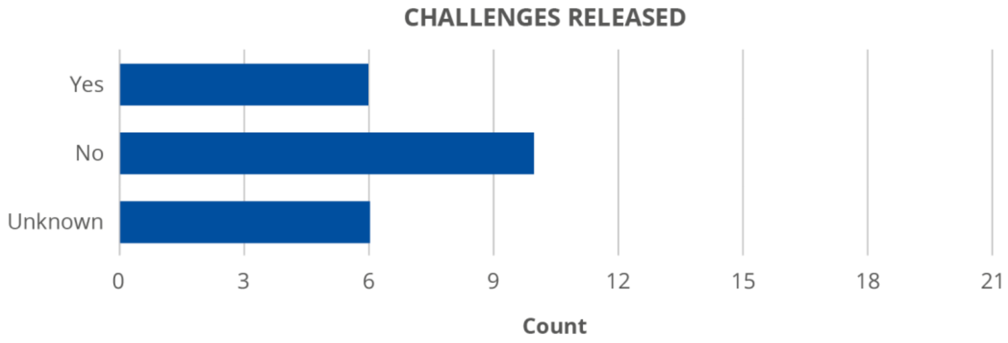
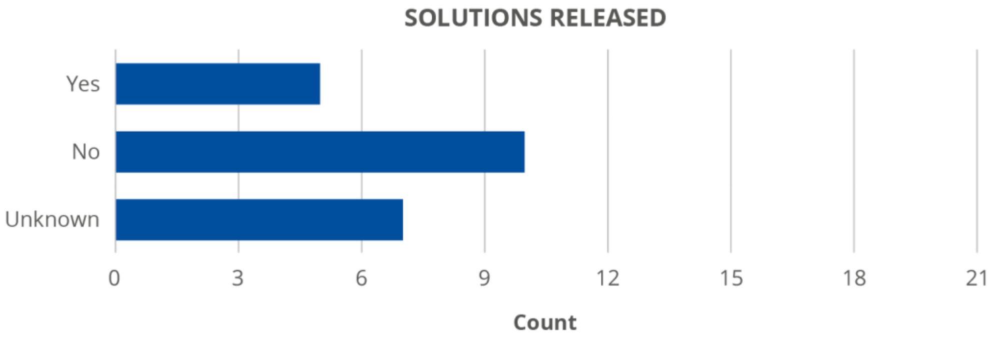


Figure 29: Breakdown of Events by Solution Release Policy



Events with an education focus, rather than an entertainment focus, sometimes released more detailed data (see **Figure 30**), or even published academic papers about the design and operation of the event (see **Figure 31**). Both were rare overall, however.

Figure 30: Breakdown of Events by Data Publication

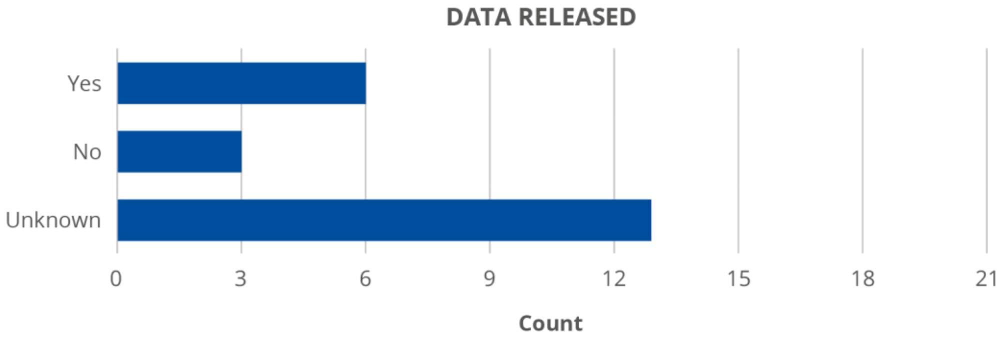
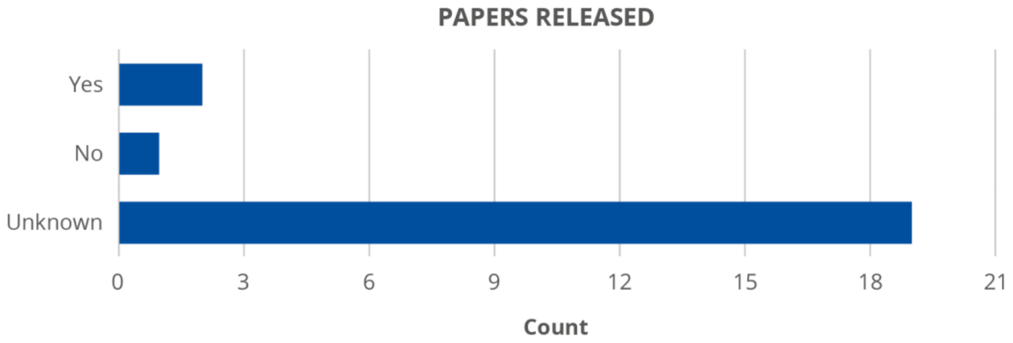


Figure 31: Breakdown of Events by Research Paper Publication



4.3 STATISTICAL ANALYSIS

In total, 879 events were recorded in the CTFTime community dataset.

The number of CTF competitions has grown every year, even reporting the highest numbers in 2020, despite the COVID-19 pandemic (see **Figure 32**). Competitions are primarily conducted online (>73%), but in-person events take place all over the world (**Figure 33**). **Figure 34** shows the locations of in-person events**.**

Figure 32: Competitions by Year

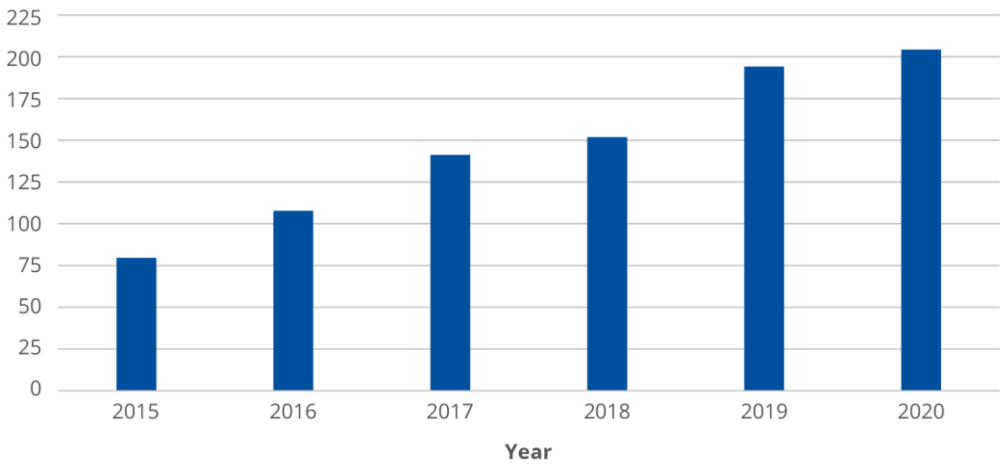


Figure 33: Competitions by Location

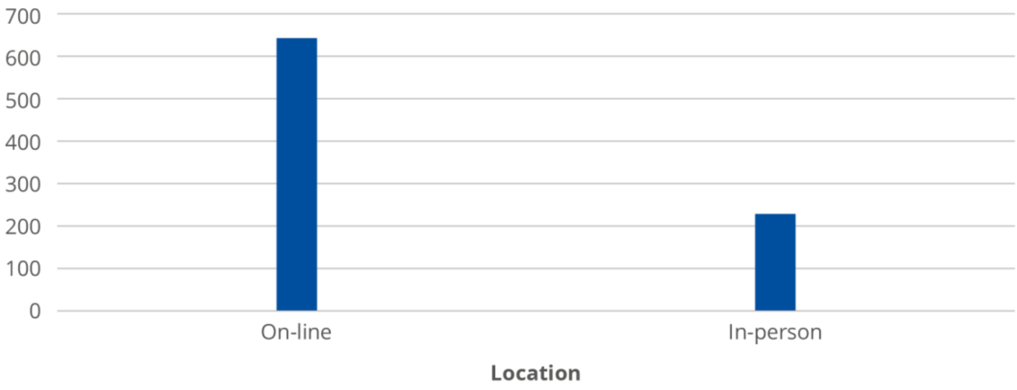
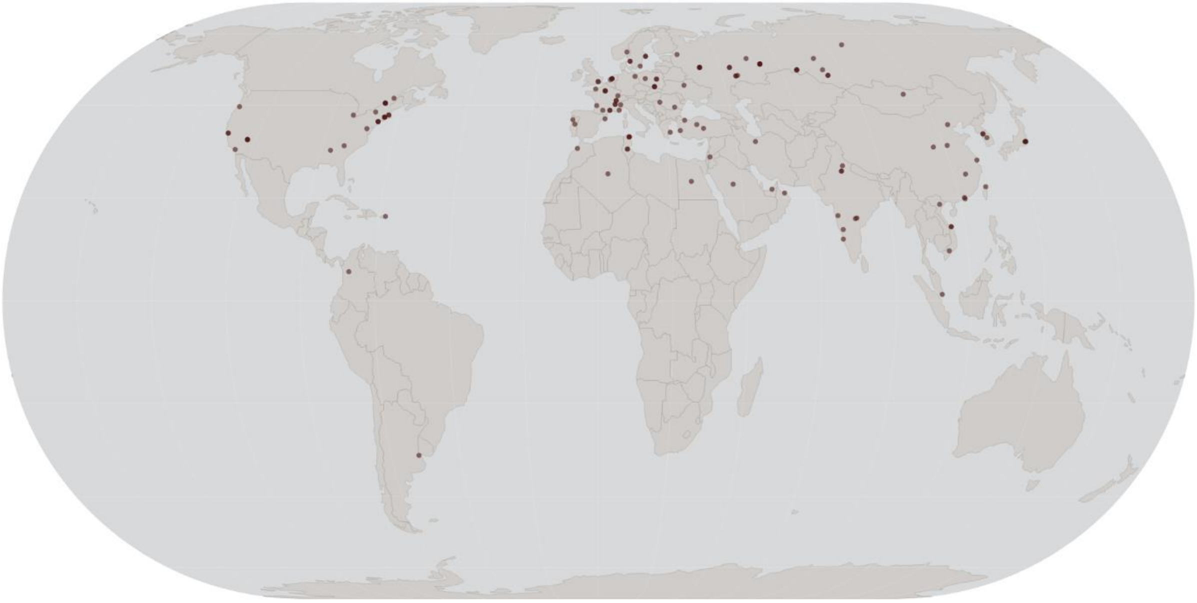
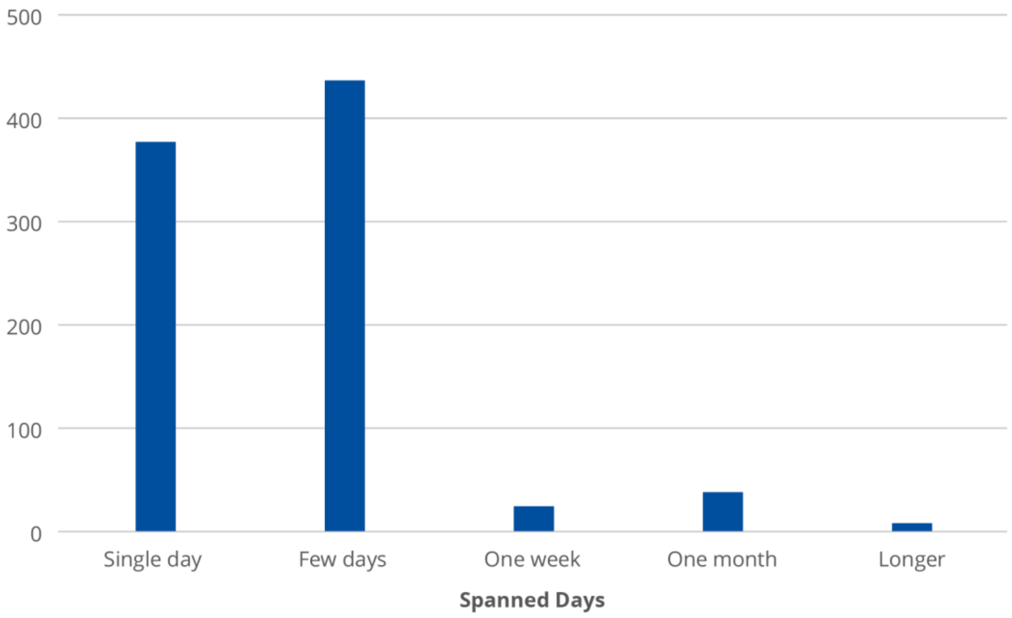


Figure 34: Map of In-person Competition Locations



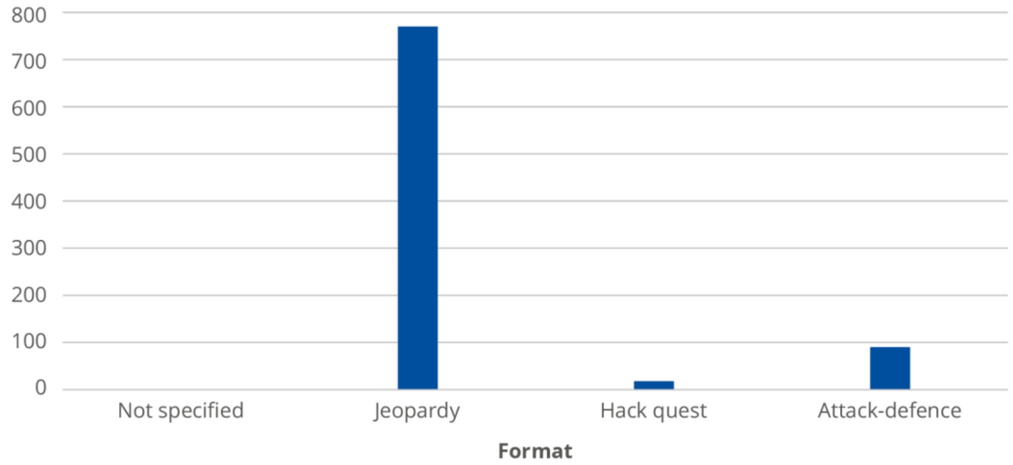
The majority of events took place over either a single day, or a few days (see **Figure 35**). A notable benefit of short multi-day events is to minimise the effect of time-zones to promote worldwide participation. Nevertheless, even the predominantly-online CTF Time events were still mostly bounded to only a small multi-day duration.

Figure 35: Competitions by Duration



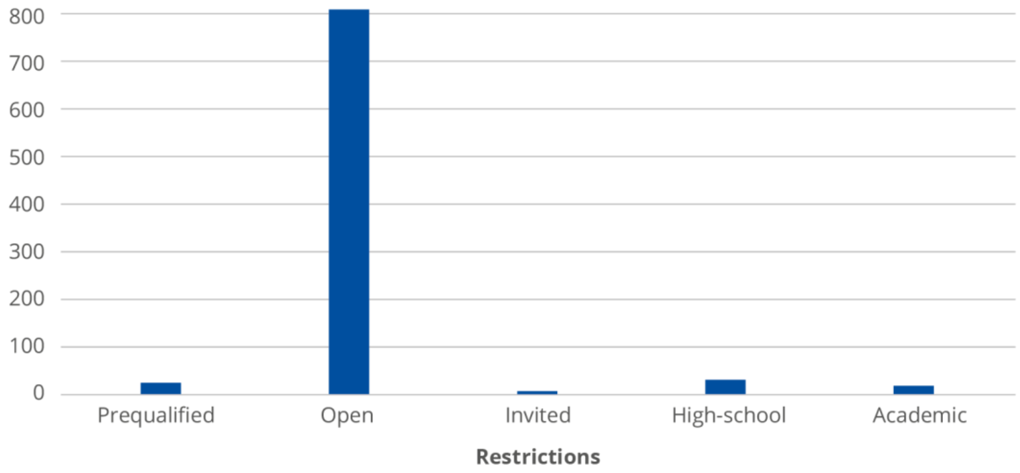
As with the events studied in the manual analysis, the vast majority of competitions from the CTF Time dataset use a Jeopardy format (>87%), over Attack-Defence or Hack Quest formats (see **Figure 36**). Again however, Attack-Defence is more popular for in-person events; accounting for nearly 25% of the total events, while online competitions only use an Attack-Defence format approximately 5% of the time.

Figure 36: Competitions by Format



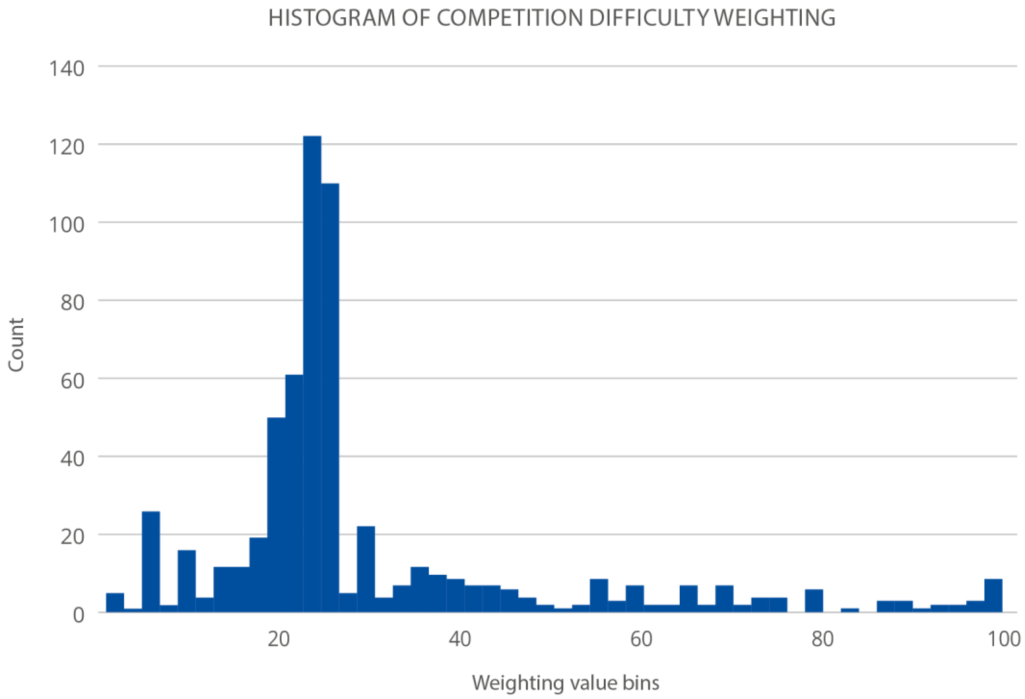
The competitions listed on CTF Time overwhelmingly specify no entry criteria; with all teams welcome to apply (see **Figure 37**). A small number are restricted to (high-) schoolchildren or university teams, but this is less common than in the manual analysis. A handful of competitions, usually larger and more renowned events, apply a prequalification criterion. This is typically an initial public competition, from which the best-placing teams are selected for invitation to the main competition. Alternatively, teams may be scouted among other notable competitions and invited without a direct qualification round. While the use of qualification rounds was seen often in the manual analysis, it is far rarer in the full CTF Time data, likely due to the logistical effort required and the focus on accessibility, over exclusivity and performance, that is common of community events.

Figure 37: Competitions by Entry Restriction



In the CTF Time difficulty weighting, events were significantly clustered around a low-to-medium difficulty level (approx. 25), although with instances of events having nearly every difficulty weighting. This is visualised as a histogram of weightings in **Figure 38**. This is consistent with the focus on accessible challenges that can be enjoyed by a range of participants, along with the likelihood that many community organisers cannot devote sufficient resources to create very challenging tasks as part of their events. Many events included in the manual analysis do not appear on CTF Time (particularly government events), however those that do have an average weighting of 53.05 and include DEF CON CTF, HITCON CTF and PlaidCTF, which all have weightings over 90 in recent years.

Figure 38: Histogram of Competitions by Weighting



5. DISCUSSION

This section contains a discussion of the results found in the course of this report and their relevant for organisers of future events.

5.1 PARTICIPATION AND INVOLVEMENT

5.1.1 Popularity

The data gathered in this report shows that CTFs are a hugely, and increasingly, popular event format. CTF events are carried out all over the world, with participants from a range of age groups and skill levels. The number of events has consistently grown year-on-year since the earliest year in the data gathered. Recommendations of the educational benefits of security competitions[2] have resonance with the success of events aimed at school- and university-age groups. The data gathered in this report suggests that there are more events targeted at these groups than at professionals; which suggests the value of CTFs as introductory and skill-building opportunities. CTFs have also been used to encourage the traditionally-underrepresented group of female participants. Some events were seen to offer benefits to teams with female members, although this was not a popular approach. Indeed, in the authors' experience of one such event, their female colleagues felt this practice commented negatively on their contribution. In other cases, gender diversity measures focused on providing access to role models and tailored mentorship as peripheral activities, rather than employing measures that altered the competition.

5.1.2 Online and in-person

While the CTF format lends itself well to online participation, half of the significant events that data was gathered on were in-person. Some events supplemented an in-person competition with online components in order to allow greater participation; this was found in both high-tier events such as DEF CON (which allows remote participants to assist a size-limited in-person team) and events focused on education and outreach (with some events holding open-access online events concurrent to invitation- or qualification-only in-person events). Where these parallel contests occurred, they had a range of purposes; concurrent events were found that targeted a different audience, provided challenges on a different theme (such as a set of challenges about hacking into wireless networks), or simply provided extra challenges on the same theme.

5.1.3 Mentors and coaches

Events, particularly those targeted at minors, often invited teams to participate under a mentor or coach. In many cases, this was an adult or teacher, presumably for the purpose of taking responsibility for child participants. Beyond this, some events allocate teams a mentor from one of the sponsoring organisations, and in one case previous competitors were selected to mentor later teams. Mentorship in this way offers a range of benefits, including allowing sponsoring organisations to work with potential job applicants in a close fashion and allowing teams to benefit from professional input and experience. Previous competitors, particularly those who are no longer able to compete, may enjoy mentoring and coaching as an opportunity to continue to be involved, and their input to teams provides teams with experienced guidance. In the experience of the authors, providing new participants with close guidance during their

[2] Chothia and Novakovic, 'An Offline Capture the Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education'.

introduction to the CTF format is highly productive and can enable participants to gain experience from avenue that they may be otherwise have been dissuaded from using.

5.2 COMPETITION AND CHALLENGE

5.2.1 Format

While Jeopardy is the dominant format both online and in-person, Attack-Defence events have had a persistent presence since the earliest events. Mixed-format events, containing both Jeopardy challenges and Attack-Defence targets provides a middle-ground that combines the benefits of both styles. In the manually-gathered dataset, only one of the events surveyed was purely Attack-Defence without any Jeopardy components. The considerably higher costs associated with setting up and managing Attack-Defence infrastructure may be a considerable factor in the decisions of event organisers. Further, the comparative difficulty of scaling-up Attack-Defence contests may further explain their lack of use in online formats, which typically have larger participant numbers. Attack-Defence may also be associated with higher skill requirements for participants, as their less-gamified structure may increase the knowledge and tools needed to successfully perform compromises. This is somewhat supported by the participant-perceived difficulty of the events, with Attack-Defence events having the highest average difficulty, followed by Jeopardy. Hack Quests, were on average considered to be significantly easier than standard Jeopardy, suggesting their typical use as highly-structured introductory events for new players.

5.2.2 Challenge categories

The strength of CTFs, and in particular Jeopardy formats, comes from their flexibility and inclusion of many types of distinct tasks for participants. The events surveyed covered a wide variety of areas; forming 26 distinct categories in this report. The most popular categories -- in terms of presence at most events -- are unsurprising to seasoned CTF participants, with Crypto, Forensics, Re, Web and Exploit forming the top five. Other, more unusual challenge themes found included Human Factors, Privacy, Hardware, and Hash-Breaking.

Challenges are predominantly technical, and while some events mentioned non-technical categories, the survey was not able to find any specific instances of non-technical challenges. Some examples from prior experience include social engineering challenges, such as interacting with an automated email service to send it phishing emails, lockpicking and interacting with other teams to gather all the parts of a flag. Physical security challenges such as lockpicking are sometimes incorporated into the main, scored competition, while others are conducted as an unscored peripheral activity (such as a guided exercise, from the authors' experience, in which participants performed a physical wiretap of a network cable).

5.2.3 Challenge sources

Challenges came from a variety of sources, although they were predominantly provided by the organisers directly. In some cases, participants themselves were required to provide challenges in order to compete. These submitted challenges were then vetted and modified by organisers before inclusion. In one instance this formed the basis for a secondary prize, where the team with the best challenge received an award. Participant-submitted challenges were observed in two Jeopardy contests; in one case, the participants were required to submit a vulnerable virtual machine containing weaknesses. Some events also included sponsor-provided challenges. These would could cover a similar theme to the sponsor, or even explicitly involve the use of the sponsor's product. In one event, sponsor challenges acted as a separate competition, with participants being awarded individual prizes for the best performance in the sponsor challenge. In some cases, the event was hosted by an existing CTF provider and may have used the existing challenges produced by that provider.

5.2.4 Jeopardy variants

Within the Jeopardy format, there was considerable variation. While the standard format of individual challenges with automatically-scored flags was the most prevalent, many events provided further interest with alternative scoring or challenge formats. There was relatively little consensus -- the most popular non-standard variation was only found in three of the events -- but almost all in-person events included some variant. The most popular was quiz- or question-based scoring, where participants were required to answer further information about the challenges they were performing. This may take the form of multiple-choice questions or through written submissions that were evaluated by a jury. As opposed to the standard CTF platform infrastructure, some events opted to distribute challenges via vulnerable virtual machine images, in a manner similar to Attack-Defence. Points were rewarded for participants primarily based on a fixed-per-solve basis, although events also included points that scaled according to the number of solves, and extra points for the first solves of a challenge. Four events also explicitly mentioned providing points for other, miscellaneous, non-challenge activities.

5.3 STRUCTURE AND ORGANISATION

5.3.1 Event length

Event length varied considerably in the larger dataset; events most often lasted a day or two but many took place over up to a week and some considerably longer. Conversely, almost all the events in the manually-gathered dataset took a few days or less, with half of them taking one day. Only one event, PicoCTF, took place over a longer period (two weeks). Actual competition time was often shorter; some events took place for a few hours on a single day and included time for other activities. Conversely, some events took place over a few days and enabled participants to continue working "out of hours"; this is primarily the case for online events but also seen in some in-person events. In these instances, scoreboards and submission systems may be disabled while participants are not in the venue.

5.3.2 Peripheral activities

In-person events frequently advertised other activities planned during the competition period. These included briefings, meals, and other social activities. Events also included activities led by or including sponsors; particularly job fairs, career advice sessions and other recruitment activities. In many cases these were disconnected from the competition, in a few instances they were connected to the scoring of the competition (for instance, sponsor booths that allowed participants to score points by engaging with an activity). Many events explicitly mentioned providing catering, including one online event which offered to deliver pizza to competitors. Fewer events mentioned covering travel or accommodation costs, although the nature of the data sources used made this data difficult to gather with confidence.

5.3.3 Organiser communication

Organisers communicated with their participants through a variety of media, both before and during the event. Almost (but, notably, not all) events had an event-specific webpage that provided details and (normally) a means of participants to register. Twitter and Facebook were both commonly used by a significant number of events, and other social media such as LinkedIn, Instagram and Flickr were also utilised. Chat-based platforms, such as IRC, Discord and Telegram were also seen, with Discord proving the most widely-used (although still only found in a small number of events). In particular, some events used Discord both as a communication means and as a challenge-distribution platform, where participants were able to download challenges directly from Discord channels. Some events reported that organisers would provide hints and help during the competition, although this was unusual. While live streaming of screens, scoreboards and judging processes was witnessed in some cases, it was rare for events to fully embrace the medium. Pwn2Own is a notable counterexample, however, with day-long streams and live commentary.

5.4 QUALIFICATION AND POST-EVENT

5.4.1 Qualification

Few CTF events had explicit requirements on who could compete, aside from educational status; one event required participants to pass a short online test that examined technical skills and English-language proficiency. One event, which was on the borderline between a wargame exercise and a CTF, was invitational and only included participants who worked professionally as cyber incident responders. Roughly half the events used a qualification round to filter participants down for final events. In most cases, qualification rounds were run by the same organisers and were often online or run in a decentralised fashion, with individual schools or universities hosting qualifiers. In some cases, events that are significant in themselves are used as qualifiers to a future event, and successful winners of the main event go on to participate in a further competition. This was particularly prevalent in the dataset due to selection biases, and many surveyed events act as national qualifiers for the ECSC. In the case of DEF CON, participant teams were able to join from successful participation in the DEF CON qualification round or by winning other selected other events (including the previous year).

5.4.2 Team allocation

Participants almost always participated in teams in main events, although many events allow participation in teams of one. In some cases, participants qualified individually and were then sorted into teams by the organisers. In the Cambridge2Cambridge event, this was performed by sorting participants by qualification score and assembling teams of equal skill. Teams occasionally had further requirements: in one case, teams needed to contain participants from different age groups; in two, teams were encouraged to include female members by providing benefits in the rules (for instance, by allowing teams to have one additional member if they were female).

5.4.3 Resultant publications

There are many papers in academic literature relating to both the organisational processes, and to the education and training benefits. Experience of running events is a frequent basis of this work and consequently many events led directly to publications. For instance, the organisers of PicoCTF list a collection of papers and research work they have performed around the competition, on topics such as how to encourage participation, how to generate challenges automatically (with a view to overcoming flag-sharing), and more generally on the running of PicoCTF itself.

5.4.4 Data Sharing

Some events also release detailed statistics about the event. DEF CON release considerable information, including raw packet captures, that provide detailed insight both to the event itself and to the exploits and vulnerabilities that were used during the competition. Other events release demographic statistics; Cyber Challenge Italia release such statistics both for their final event and broken down by individual qualifier events. In total, detailed data was found for six of the events.

5.4.5 Writeups

CTF culture places significant importance of the creation, study and dissemination of post-event writeups. Each writeup explains the details of a challenge and its solution from the perspective of a participant or team. These are widely shared and repositories exist that collect them together (for instance, CTFTime allows users to submit writeups for challenges once a contest is ended). This is reinforced by some event organisers, who encourage (and sometimes reward) participants who submit high-quality writeups to them. In some instances, teams must supply writeups to challenges they solve in order to be presented with their prizes. This may act as a deterrent to cheats, or may ensure winning teams have a thorough understanding of the challenges they have solved. Organisers may also release solutions to their challenges themselves so that participants can understand the technicalities behind the challenges after the event. On the other end of the spectrum, some competitions explicitly forbid the release of writeups or the sharing of challenge files after the event. This may be intended to enable them to re-use challenges in later years, although it is unlikely that determined participants would be unable to find copies of the solutions to previous years. In the manual dataset, we found no direct evidence that any of the events surveyed forbade sharing of either challenges or writeups.

6. CONCLUSIONS

In this section, we provide the following recommendations for organisers of future competitions. These conclusions are informed by the analysis and discussions presented in this report. These recommendations are made in the context of the survey results. Our conclusions are as follows:

6.1 COMPETITION FORMAT

Jeopardy is heavily favoured in both online and in-person event formats. This is likely due to a range of factors, including accessibility, lower deployment costs, and scalability. Despite this, the continued prevalence of Attack-Defence (particularly in the well-respected DEF CON CTF), and its similarity to the wargame formats preferred by professional training exercises, indicates the value of this format. We suggest that events designed to be accessible to non-professional audiences are based on the Jeopardy format, and follow the trend of other events and include Attack-Defence elements if desired. Structuring in this way gives the benefits of both formats and reduces the drawbacks of either.

6.2 TEAM REQUIREMENTS

We found that many events are deliberately targeted to specific age groups, or specifically to students. Further, we found evidence that some events attempt to create a more even gender balance. We found little evidence of events requiring specific degrees or certifications, except implicitly in professional competitions. We suggest that attempts to encourage gender balance through team composition are unlikely to have significant impact, particularly for top-tier events where participants are likely to have needed to be preparing for (and attempting qualify for) the event for a long period.

Teams may expect to have a mentor or coach present, particular when younger participants are involved. In cases where a mentor is involved, it may be important to provide clear rules and roles for them. In particular, their communication with their team during the event may give an unfair advantage to competitors based on the expertise and willingness of their mentor. As a result, we suggest that mentor roles are clearly defined, if included at all.

6.3 TEAM SIZES

The greatest division between the results of our analysis and the survey results are in team size, where the ideal size suggested in the survey was approximately twice as large as the expected team size in the events surveyed. We believe this is due to the nature of ECSC as an international event with national qualifiers; as participant teams are likely to be created out of the top-performing teams from individual qualifying events, it is natural that large team sizes would be more suitable and preferred by participants. It may be worth drawing a parallel to DEF CON, which equally represents the culmination of a number of events and, equally, is typically attended by teams of a larger size. It may be worth considering that DEF CON places a limit on the in-person team size, presumably for logistical reasons, while placing no limit on the size of the remote team -- limiting the size of a remote team is impossible to enforce and therefore unlikely to be suitable to a competitive environment.

6.4 SCORING AND RULES

For Jeopardy formats, it is anticipated that participants would expect the primary scoring mechanism to follow traditional Jeopardy fixed-per-challenge or scoring based on the number of solves. Many events provide some deviation from this, and in particular some events provide subjective or jury-evaluated questions alongside challenges. We believe these are less likely to scale well into larger competitions with higher skill levels and suggest that objective scoring systems have higher integrity.

Equally, while some events include participant-submitted challenges, these require a distinct skillset to that of typical CTF participation. Including participant-submitted challenges also creates an uneven playing field, where each team has a different set of challenges to solve and consequently this may somewhat dilute the competitive aspect. Sponsor-provided challenges provide a potential opportunity for more competitive challenge variety. In these instances, care should be taken that challenges fit with the format and style of the rest of the competition; in our experience, unrestricted sponsor challenges can fit poorly with the rest of the competition, possibly due to sponsor inexperience with the format.

6.5 PARALLEL COMPETITIONS

Including a parallel competition may be a valuable way to increase engagement beyond core participants. Of particular note, Google CTF's Beginner's Quest offered interested non-participants an opportunity to experience the event without requiring the (relatively high) skills necessary to participate in the full event. Hack Quests in particular offer an enjoyable and engaging way to bring new participants into later competitions and build interest in the CTF scene. It may also be appropriate, in some events, to run specialist parallel competitions that focus specifically on one aspect of the competition that may not be a good fit for general participants. For instance, it may be the case that few participants have experience of hardware challenges, and inclusion in the main event may give a disproportionate advantage to those with prior experience.

6.6 CHALLENGE FORMATS

The "typical" range of Jeopardy CTF challenges is extremely broad. While there are standard categories that most challenges are drawn from (specifically reverse engineering, exploitation, web-based exploits, forensics, and cryptography), there is a wide variety of alternative categories that may be suitable for inclusion. In particular, challenges that benefit from the physical, in-person nature of the event, such as snooping on wireless traffic, may be well-received, particularly as they are less likely to have been experienced previously. There is some evidence of increased interest in non-technical challenges, and the interdisciplinary nature of cybersecurity may be encouraged by including challenges of this form. Particularly, there has been some evidence of automated social engineering challenges. Events which utilise jury-based evaluation may find greater success with challenges of this form, which may require more subjective analysis, but care should be taken not to deviate too greatly from the established and successful CTF format.

6.7 COMMUNICATION AND MEDIA

Web and social media presence is generally consistent across all events, with almost every event (and every open event) maintaining a website and some social media presence. Facebook and Twitter were the most common, and some degree of engagement with these platforms is likely anticipated by participants. We further recommend the consideration of chat-based platforms, such as Discord, IRC, or Slack, which offer an excellent opportunity for general communication, announcements, challenge and platform support. Further, community-led platforms such as these offer a chance for engagement beyond the competition. In the Discord servers we surveyed, we found evidence that participants were still engaged with each other, with discussions of both security and general interests.

6.8 POST-EVENT

To further encourage and engage the community beyond the event itself, organisers may wish to support participants (and non-participants) who wish to go over the challenges in their own time. This has two primary avenues; firstly, making challenges available after the event, and secondly, ensuring that writeups or solutions for challenges are available. Organisers may not need to do a great deal to facilitate this, as the community has a strong tradition of publishing writeups for most events. However, organisers who go further to facilitate this, such as by amplifying or sharing participant writeups, or by providing awards to the best writeups, may compound the benefits. Releasing challenges after the event is also beneficial as they can be used as a training and teaching tool, particularly for participants seeking to prepare for future iterations of the event. Some thought may need to be given to this in cases where challenges involve servers, and this may not be possible in cases where hardware is involved.

In addition to supporting the spread of challenges and writeups, organisers should consider the beneficial impact they can have on the academic community. This could be performed indirectly, by sharing data about the competition, such as demographic data on participants, or about the challenges themselves. Such data is of particular interest in Attack-Defence formats, where attack traffic data may closely mirror real-world attack traffic. Further, organisers may wish to follow the example of other events and directly publish their conclusions that follow from their own experience running an event.

7. BIBLIOGRAPHY

[1] L. McDaniel, E. Talvi and B. Hay, “Capture the Flag as Cyber Security Introduction,” in *Hawaii International Conference on System Sciences*, 2016.

[2] T. Chothia and C. Novakovic, “An Offline Capture the Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education,” in *USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2015.

[3] CTFTime.org, “What Is Capture The Flag?,” 13 12 2020. [Online]. Available: https://ctftime.org/ctf-wtf/.

[4] J. Burket, P. Chapman and T. Becker, “Automatic Problem Generation for Capture-the-Flag Competitions,” in *USENIX Summit on Gaming, Games and Gamification in Security Education*, 2015.

[5] K. Chung, “Lowering the Barriers to Capture The Flag Administration and Participation,” in *USENIX Workshop on Advances in Security Education*, 2017.

[6] P. Prinetto, G. Roascio and A. Varriale, “Hardware-Based Capture-The-Flag Challenges,” in *IEEE East-West Design Test Symposium*, 2020.

[7] C. Cowan, S. Arnold, S. Beattie, C. Wright and J. Viega, “Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack,” in *DARPA Information Survivability Conference and Exposition*, 2003.

[8] V. Braun and V. Clarke, “Using Thematic Analysis in Psychology,” *Qualitative Research in Psychology,* vol. 2, no. 3, pp. 77-101, 2006.

A ANNEX: CTF EVENT PROFILES

This annex provides short profiles on each capture-the-flag event included in the manual analysis:

European Cyber Security Challenge
URL: https://europeancybersecuritychallenge.eu
Organiser Type: Government
Pan-European event organised by ENISA. Included as comparative baseline.

CyberCenturion - Cyber Security Challenge UK
URL: https://www.cybersecuritychallenge.org.uk
Organiser Type: Government
Competition for young people in the UK, intended to promote cybersecurity education.

Cyber Security Challenge Canada
URL: https://cybersecuritychallenge.ca
Organiser Type: Government
University-focused competition run by Canadian government, intended to promote skills training and connect students with potential employers.

Cyber Security Challenge Germany
URL: https://www.cscg.de
Organiser Type: Government
German competition targeting children and young adults to promote cybersecurity education and careers.

Cyber Challenge Italia
URL: https://cyberchallenge.it
Organiser Type: Government
Italian competition focusing on school- and university-aged students with the intent to promote cybersecurity education and careers. CTF is part of a wider training programme covering technical skills, attack/defence and ethics.

US Cyber Challenge
URL: https://www.uscyberchallenge.org
Organiser Type: Government
National US programme designed "to identify, attract, train and recruit the next generation of cybersecurity professionals". Run as a public-private partnership.

Cyber Security Challenge SA
URL: https://cybersecuritychallenge.ac.za/
Organiser Type: Government
South African competition intended to "stimulate interest in Cyber Security in general and specifically in the field of Network Security within South African Tertiary institutions".

ACSC-ASEAN
URL: https://www.cyber.gov.au/acsc/view-all-content/news/acsc-asean-strengthening-regional-cyber-security
Organiser Type: Government
Australian-organised event, inviting competitors from the Association of South East Asian Nations (ASEAN), with a specific focus on cybersecurity professionals and a stated intention to promote collaboration.

DEF CON CTF
URL: https://www.defcon.org
Organiser Type: Community
Long-running and renowned community CTF, attached to the annual DEF CON security conference. Often considered the premiere event in the public domain.

PicoCTF
URL: https://picoctf.com
Organiser Type: University
US online competition with focus on school-age children, intended to promote cybersecurity education. Also used as a research platform to develop effective skills training.

Pwn2Own
URL: https://cansecwest.com
Organiser Type: Community
Exploit-finding competition for popular consumer software and products; essentially a live bug-bounty programme. Attached to the CanSecWest conference.

Cambridge 2 Cambridge Cyber Competition
URL: https://cambridge2cambridge.mit.edu (defunct)
Organiser Type: University
Joint MIT-CSAIL/Cambridge University collaborative event designed to develop cybersecurity skills in university students, encourage collaboration between countries and promote interest in cyber-related careers among schoolchildren.

Country 2 Country
URL: https://www.c2c-ctf.org/
Organiser Type: University
Joint event organised by InterNational Cyber Security Center of Excellence (INCS-CoE) members, aiming to host five CTFs over five years (in the UK, Israel, USA, Japan and Australia). Developed from the Cambridge2Cambridge events. Intended to promote international collaboration and develop cybersecurity skills in university students.

Midnight Sun Capture the Flag (AFCEA Sweden)
URL: https://www.midnightsunctf.se/
Organiser Type: Community
CTF attached to the CyberSecurity and Privacy (CySeP) summer school, but open publicly. Developed by KTH university and HackingForSoju CTF team with the stated goal "to promote the cyber security eco-system in the region".

WCTF (Qihoo 360)
URL: https://ctf.360.com
Organiser Type: Commercial
Public CTF run by internet security company Qihoo 360 Technology Co. Ltd.

CyberTalents Arab and Africa Regional CTF

URL: https://cybertalents.com/competitions/arab-africa-regional-cyber-security-ctf-2020
Organiser Type: Commercial
Regional CTF covering a wide area including Africa & Arab countries ("Saudi Arabia, Oman, Nigeria, Uganda, UAE, Sudan, Kuwait, Algeria, Morocco, Lebanon, Jordan, Tunisia, and Egypt, etc."). Organised by recruitement firm CyberTalents.

National Collegiate Cyber Defense Competition

URL: https://www.nationalccdc.org/
Organiser Type: University
League-based US competition with 14 year history. Intended to serve as a training and testing platform for institutions teaching cybersecurity skills.

International Collegiate Cyber Defense Competition

URL: https://iccdi.org/
Organiser Type: University
Internationally-focused event derived from the US CCDC, incorporating participants from other countries.

Global Cyberlympics

URL: https://www.cyberlympics.org/
Organiser Type: Commercial
International competition run by the EC-Council Foundation, with stated goals of: "Capacity Building, Raising Awareness, Global Peace & Child Online Protection".

PlaidCTF

URL: https://play.plaidctf.com
Organiser Type: Community
Public CTF run by the PPP CTF team attached to Carnegie Mellon University

HITCON

URL: https://ctf2020.hitcon.org/
Organiser Type: Community
Public CTF organised by Hacking-in-Taiwan. Attached to the HITCON conference.

Google CTF

URL: https://capturetheflag.withgoogle.com/
Organiser Type: Commercial
Public CTF run by internet company Google Inc.

B ANNEX: MANUAL ANALYSIS DATA TABLES

B.1 ORGANISING ENTITY

Event Name	Commercial	Community	Government	University
European Cyber Security Challenge			√	
Cyber Centurion - CSC UK			√	
ACSC-ASEAN			√	
Cambridge 2 Cambridge Cyber Competition				√
Country 2 Country				√
Cyber Challenge Italia			√	
Cyber Security Challenge Canada			√	
Cyber Security Challenge Germany			√	
Cyber Security Challenge SA			√	
DEF CON CTF		√		
Midnight Sun Capture the Flag (AFCEA Sweden)		√		
PicoCTF				√
Pwn2Own		√		
US Cyber Challenge			√	
WCTF (Qihoo 360)	√			
CyberTalents Arab and Africa Regional CTF	√			
National Collegiate Cyber Defense Competition				√
International Collegiate Cyber Defense Competition				√
Global Cyberlympics	√			
PlaidCTF		√		
HITCON		√		
Google CTF	√			

B.2 INTENDED AUDIENCE

Event Name	Children	Professional	Public	University	Unknown
European Cyber Security Challenge	✓			✓	
Cyber Centurion - CSC UK	✓				
ACSC-ASEAN		✓			
Cambridge 2 Cambridge Cyber Competition				✓	
Country 2 Country				✓	
Cyber Challenge Italia				✓	
Cyber Security Challenge Canada				✓	
Cyber Security Challenge Germany			✓		
Cyber Security Challenge SA				✓	
DEF CON CTF		✓	✓		
Midnight Sun Capture the Flag (AFCEA Sweden)					✓
PicoCTF	✓				
Pwn2Own		✓	✓		
US Cyber Challenge					✓
WCTF (Qihoo 360)		✓	✓		
CyberTalents Arab and Africa Regional CTF			✓		
National Collegiate Cyber Defense Competition				✓	
International Collegiate Cyber Defense Competition				✓	
Global Cyberlympics					✓
PlaidCTF			✓		
HITCON			✓		
Google CTF			✓		

B.3 AGE

Event Name	Adult	Elder Teen	Young Adult	Young Teen	Unknown
European Cyber Security Challenge		✓	✓		
Cyber Centurion - CSC UK		✓		✓	
ACSC-ASEAN	✓				
Cambridge 2 Cambridge Cyber Competition					✓
Country 2 Country					✓
Cyber Challenge Italia			✓		
Cyber Security Challenge Canada			✓		
Cyber Security Challenge Germany		✓	✓	✓	
Cyber Security Challenge SA					✓
DEF CON CTF					✓
Midnight Sun Capture the Flag (AFCEA Sweden)					✓
PicoCTF	✓	✓	✓	✓	
Pwn2Own					✓
US Cyber Challenge	✓		✓		
WCTF (Qihoo 360)					✓
CyberTalents Arab and Africa Regional CTF	✓	✓	✓	✓	
National Collegiate Cyber Defense Competition					✓
International Collegiate Cyber Defense Competition					✓
Global Cyberlympics	✓		✓		
PlaidCTF					✓
HITCON					✓
Google CTF					✓

B.4 ORGANISING ENTITY PARTICIPANT TYPES

Event Name	Children	Cyber Professionals	Invitation	No restriction	Students	Unknown
European Cyber Security Challenge	✓				✓	
Cyber Centurion - CSC UK	✓					
ACSC-ASEAN		✓				
Cambridge 2 Cambridge Cyber Competition					✓	
Country 2 Country					✓	
Cyber Challenge Italia					✓	
Cyber Security Challenge Canada			✓			
Cyber Security Challenge Germany				✓		
Cyber Security Challenge SA					✓	
DEF CON CTF			✓			
Midnight Sun Capture the Flag (AFCEA Sweden)				✓	✓	
PicoCTF				✓		
Pwn2Own				✓		
US Cyber Challenge						✓
WCTF (Qihoo 360)			✓			
CyberTalents Arab and Africa Regional CTF				✓		
National Collegiate Cyber Defense Competition				✓		
International Collegiate Cyber Defense Competition					✓	
Global Cyberlympics				✓		
PlaidCTF				✓		
HITCON				✓		
Google CTF				✓		

B.5 QUALIFICATIONS REQUIRED

Event Name	CyberSec Expert	Language Skills	No restriction	Technical Skills
European Cyber Security Challenge			✓	
Cyber Centurion - CSC UK			✓	
ACSC-ASEAN	✓			
Cambridge 2 Cambridge Cyber Competition			✓	
Country 2 Country			✓	
Cyber Challenge Italia		✓		✓
Cyber Security Challenge Canada			✓	
Cyber Security Challenge Germany			✓	
Cyber Security Challenge SA			✓	
DEF CON CTF			✓	
Midnight Sun Capture the Flag (AFCEA Sweden)			✓	
PicoCTF			✓	
Pwn2Own			✓	
US Cyber Challenge			✓	
WCTF (Qihoo 360)			✓	
CyberTalents Arab and Africa Regional CTF			✓	
National Collegiate Cyber Defense Competition			✓	
International Collegiate Cyber Defense Competition			✓	
Global Cyberlympics			✓	
PlaidCTF			✓	
HITCON			✓	
Google CTF			✓	

B.6 ORGANISING ENTITY LOCATIONS

Event Name	Country	Multiple Countries	No restriction	Region Within Country
European Cyber Security Challenge	✓			
Cyber Centurion - CSC UK	✓			
ACSC-ASEAN		✓		
Cambridge 2 Cambridge Cyber Competition	✓			
Country 2 Country		✓		
Cyber Challenge Italia	✓			
Cyber Security Challenge Canada				✓
Cyber Security Challenge Germany	✓			
Cyber Security Challenge SA		✓		
DEF CON CTF			✓	
Midnight Sun Capture the Flag (AFCEA Sweden)		✓		
PicoCTF			✓	
Pwn2Own			✓	
US Cyber Challenge				✓
WCTF (Qihoo 360)			✓	
CyberTalents Arab and Africa Regional CTF		✓		
National Collegiate Cyber Defense Competition	✓			
International Collegiate Cyber Defense Competition		✓		
Global Cyberlympics	✓			
PlaidCTF			✓	
HITCON			✓	
Google CTF			✓	

B.7 GENDER

Event Name	Female Participation Benefit	Gender Categorisation	No restriction
European Cyber Security Challenge			✓
Cyber Centurion - CSC UK		✓	
ACSC-ASEAN			✓
Cambridge 2 Cambridge Cyber Competition	✓		
Country 2 Country			✓
Cyber Challenge Italia			✓
Cyber Security Challenge Canada			✓
Cyber Security Challenge Germany			✓
Cyber Security Challenge SA	✓		
DEF CON CTF			✓
Midnight Sun Capture the Flag (AFCEA Sweden)			✓
PicoCTF			✓
Pwn2Own			✓
US Cyber Challenge			✓
WCTF (Qihoo 360)			✓
CyberTalents Arab and Africa Regional CTF			✓
National Collegiate Cyber Defense Competition			✓
International Collegiate Cyber Defense Competition			✓
Global Cyberlympics			✓
PlaidCTF			✓
HITCON			✓
Google CTF			✓

B.8 SOCIO-ECONOMIC

Event Name	Considerations made	No restriction
European Cyber Security Challenge		✓
Cyber Centurion - CSC UK		✓
ACSC-ASEAN		✓
Cambridge 2 Cambridge Cyber Competition		✓
Country 2 Country		✓
Cyber Challenge Italia		✓
Cyber Security Challenge Canada		✓
Cyber Security Challenge Germany		✓
Cyber Security Challenge SA		✓
DEF CON CTF		✓
Midnight Sun Capture the Flag (AFCEA Sweden)		✓
PicoCTF	✓	
Pwn2Own		✓
US Cyber Challenge		✓
WCTF (Qihoo 360)		✓
CyberTalents Arab and Africa Regional CTF		✓
National Collegiate Cyber Defense Competition		✓
International Collegiate Cyber Defense Competition		✓
Global Cyberlympics		✓
PlaidCTF		✓
HITCON		✓
Google CTF		✓

B.9 ETHNICITY

Event Name	No restriction	Unknown
European Cyber Security Challenge	✓	
Cyber Centurion - CSC UK		✓
ACSC-ASEAN		✓
Cambridge 2 Cambridge Cyber Competition		✓
Country 2 Country		✓
Cyber Challenge Italia		✓
Cyber Security Challenge Canada		✓
Cyber Security Challenge Germany		✓
Cyber Security Challenge SA		✓
DEF CON CTF		✓
Midnight Sun Capture the Flag (AFCEA Sweden)		✓
PicoCTF		✓
Pwn2Own		✓
US Cyber Challenge		✓
WCTF (Qihoo 360)		✓
CyberTalents Arab and Africa Regional CTF	✓	
National Collegiate Cyber Defense Competition	✓	
International Collegiate Cyber Defense Competition	✓	
Global Cyberlympics	✓	
PlaidCTF	✓	
HITCON	✓	
Google CTF	✓	

B.10 ORGANISING ENTITY FORMAT

Event Name	Artifact Analysis	Attack/Defence	Defence	Exploit Finding	Jeopardy	Jury Evaluation	Patching	Questions	Vulnerable VM	Unknown
European Cyber Security Challenge					✓	✓				
Cyber Centurion - CSC UK							✓	✓		
ACSC-ASEAN	✓				✓					
Cambridge 2 Cambridge Cyber Competition		✓			✓				✓	
Country 2 Country					✓					
Cyber Challenge Italia										✓
Cyber Security Challenge Canada									✓	
Cyber Security Challenge Germany					✓			✓		
Cyber Security Challenge SA		✓			✓					
DEF CON CTF		✓								
Midnight Sun Capture the Flag (AFCEA Sweden)					✓					
PicoCTF					✓					
Pwn2Own				✓						
US Cyber Challenge	✓							✓		
WCTF (Qihoo 360)					✓	✓				
CyberTalents Arab and Africa Regional CTF					✓					
National Collegiate Cyber Defense Competition			✓							
International Collegiate Cyber Defense Competition			✓							
Global Cyberlympics					✓					
PlaidCTF					✓					
HITCON					✓					
Google CTF					✓					

B.11 CHALLENGE CATEGORY

Event Name	Administration	Attack	Automation	Crypto	Defence	Exploit	Forensics	Hardware	Hash-breaking	Human Factors	IoT	Malware	Misc	Mobile	Networks	OS	Patching	Pen Testing	Physical Security	Privacy	Programming	Re	Recon/Opsec/Intel	User-Submitted	Virtualization	Web
European Cyber Security Challenge				✓			✓	✓		✓	✓	✓	✓	✓	✓	✓		✓		✓			✓			✓
Cyber Centurion - CSC UK							✓			✓							✓									
ACSC-ASEAN					✓		✓																			
Cambridge 2 Cambridge Cyber Competition				✓			✓								✓						✓	✓				✓
Country 2 Country				✓		✓	✓														✓	✓				
Cyber Challenge Italia					✓							✓					✓									
Cyber Security Challenge Canada																								✓		
Cyber Security Challenge Germany				✓			✓					✓		✓	✓	✓					✓	✓				✓
Cyber Security Challenge SA		✓		✓	✓		✓		✓									✓								
DEF CON CTF		✓			✓																					
Midnight Sun Capture the Flag (AFCEA Sweden)				✓		✓																✓				✓
PicoCTF				✓		✓	✓						✓									✓				✓
Pwn2Own			✓			✓										✓		✓							✓	✓
US Cyber Challenge						✓	✓								✓											✓
WCTF (Qihoo 360)																								✓		
CyberTalents Arab and Africa Regional CTF				✓			✓					✓	✓									✓	✓			✓
National Collegiate Cyber Defense Competition	✓																									
International Collegiate Cyber Defense Competition	✓				✓																					
Global Cyberlympics				✓		✓	✓					✓			✓				✓			✓				✓
PlaidCTF				✓		✓							✓									✓				✓
HITCON				✓		✓	✓						✓									✓				✓
Google CTF						✓							✓									✓				✓

B.12 PLATFORM

Event Name	Custom	Hosted Service	Unknown
European Cyber Security Challenge	√		
Cyber Centurion - CSC UK	√		
ACSC-ASEAN			√
Cambridge 2 Cambridge Cyber Competition	√		
Country 2 Country	√		
Cyber Challenge Italia			√
Cyber Security Challenge Canada		√	
Cyber Security Challenge Germany	√		
Cyber Security Challenge SA		√	
DEF CON CTF	√		
Midnight Sun Capture the Flag (AFCEA Sweden)	√		
PicoCTF			√
Pwn2Own			√
US Cyber Challenge	√		
WCTF (Qihoo 360)			√
CyberTalents Arab and Africa Regional CTF	√		
National Collegiate Cyber Defense Competition	√		
International Collegiate Cyber Defense Competition	√		
Global Cyberlympics		√	
PlaidCTF	√		
HITCON	√		
Google CTF	√		

B.13 SCORING

Event Name	Attack Points	Based on Solve Count	Defence Points	First Blood	Fixed Per Solve	KoTH Points	Manual Grading	Miscellaneous	Unknown
European Cyber Security Challenge		✓					✓		
Cyber Centurion - CSC UK					✓				
ACSC-ASEAN					✓				
Cambridge 2 Cambridge Cyber Competition					✓			✓	
Country 2 Country									✓
Cyber Challenge Italia									✓
Cyber Security Challenge Canada									✓
Cyber Security Challenge Germany					✓				
Cyber Security Challenge SA							✓		
DEF CON CTF	✓		✓			✓			
Midnight Sun Capture the Flag (AFCEA Sweden)		✓							
PicoCTF					✓				
Pwn2Own					✓			✓	
US Cyber Challenge								✓	
WCTF (Qihoo 360)				✓	✓		✓		
CyberTalents Arab and Africa Regional CTF					✓				
National Collegiate Cyber Defense Competition			✓				✓		
International Collegiate Cyber Defense Competition							✓	✓	
Global Cyberlympics					✓			✓	
PlaidCTF					✓				
HITCON		✓							
Google CTF					✓				

B.14 WINNER PRIZES

Event Name	Invitation	Sponsor-related	Yes	No	Unknown
European Cyber Security Challenge					✓
Cyber Centurion - CSC UK		✓			
ACSC-ASEAN				✓	
Cambridge 2 Cambridge Cyber Competition			✓		
Country 2 Country			✓		
Cyber Challenge Italia	✓		✓		
Cyber Security Challenge Canada			✓		
Cyber Security Challenge Germany	✓		✓		
Cyber Security Challenge SA			✓		
DEF CON CTF			✓		
Midnight Sun Capture the Flag (AFCEA Sweden)			✓		
PicoCTF			✓		
Pwn2Own			✓		
US Cyber Challenge	✓				
WCTF (Qihoo 360)			✓		
CyberTalents Arab and Africa Regional CTF	✓				
National Collegiate Cyber Defense Competition				✓	
International Collegiate Cyber Defense Competition				✓	
Global Cyberlympics			✓		
PlaidCTF			✓		
HITCON	✓		✓		
Google CTF			✓		

B.15 OTHER PRIZES

Event Name	Best Submitted Challenge	Other	No	Unknown
European Cyber Security Challenge				✓
Cyber Centurion - CSC UK			✓	
ACSC-ASEAN			✓	
Cambridge 2 Cambridge Cyber Competition			✓	
Country 2 Country			✓	
Cyber Challenge Italia				✓
Cyber Security Challenge Canada	✓			
Cyber Security Challenge Germany			✓	
Cyber Security Challenge SA			✓	
DEF CON CTF			✓	
Midnight Sun Capture the Flag (AFCEA Sweden)			✓	
PicoCTF			✓	
Pwn2Own		✓		
US Cyber Challenge				✓
WCTF (Qihoo 360)				✓
CyberTalents Arab and Africa Regional CTF			✓	
National Collegiate Cyber Defense Competition			✓	
International Collegiate Cyber Defense Competition			✓	
Global Cyberlympics			✓	
PlaidCTF			✓	
HITCON			✓	
Google CTF		✓		

B.16 EVENT LENGTH

Event Name	Few Days	Single Day	Weeks or Longer
European Cyber Security Challenge	✓		
Cyber Centurion - CSC UK		✓	
ACSC-ASEAN	✓		
Cambridge 2 Cambridge Cyber Competition	✓		
Country 2 Country		✓	
Cyber Challenge Italia		✓	
Cyber Security Challenge Canada		✓	
Cyber Security Challenge Germany		✓	
Cyber Security Challenge SA	✓		
DEF CON CTF	✓		
Midnight Sun Capture the Flag (AFCEA Sweden)		✓	
PicoCTF			✓
Pwn2Own	✓		
US Cyber Challenge		✓	
WCTF (Qihoo 360)	✓		
CyberTalents Arab and Africa Regional CTF		✓	
National Collegiate Cyber Defense Competition	✓		
International Collegiate Cyber Defense Competition	✓		
Global Cyberlympics		✓	
PlaidCTF	✓		
HITCON	✓		
Google CTF	✓		

B.17 TEAM SIZE

Minimum

Event Name	1.0	2.0	3.0	4.0	5.0	6.0	Unknown
European Cyber Security Challenge					✓		
Cyber Centurion - CSC UK				✓			
ACSC-ASEAN	✓						
Cambridge 2 Cambridge Cyber Competition					✓		
Country 2 Country	✓						
Cyber Challenge Italia	✓						
Cyber Security Challenge Canada	✓						
Cyber Security Challenge Germany	✓						
Cyber Security Challenge SA			✓				
DEF CON CTF	✓						
Midnight Sun Capture the Flag (AFCEA Sweden)							✓
PicoCTF	✓						
Pwn2Own	✓						
US Cyber Challenge	✓						
WCTF (Qihoo 360)							✓
CyberTalents Arab and Africa Regional CTF		✓					
National Collegiate Cyber Defense Competition	✓						
International Collegiate Cyber Defense Competition						✓	
Global Cyberlympics				✓			
PlaidCTF	✓						
HITCON	✓						
Google CTF	✓						

Maximum

Event Name	1.0	10.0	3.0	4.0	5.0	6.0	8.0	Unknown
European Cyber Security Challenge		✓						
Cyber Centurion - CSC UK				✓				
ACSC-ASEAN			✓					
Cambridge 2 Cambridge Cyber Competition					✓			
Country 2 Country	✓							
Cyber Challenge Italia	✓							
Cyber Security Challenge Canada				✓				
Cyber Security Challenge Germany					✓			
Cyber Security Challenge SA				✓				
DEF CON CTF								✓
Midnight Sun Capture the Flag (AFCEA Sweden)								✓
PicoCTF	✓							
Pwn2Own								✓
US Cyber Challenge	✓							
WCTF (Qihoo 360)								✓
CyberTalents Arab and Africa Regional CTF				✓				
National Collegiate Cyber Defense Competition							✓	
International Collegiate Cyber Defense Competition							✓	
Global Cyberlympics						✓		
PlaidCTF								✓
HITCON								✓
Google CTF								✓

B.18 QUALIFIERS

Event Name	Invitational	Other Contests	Yes	No
European Cyber Security Challenge			✓	
Cyber Centurion - CSC UK			✓	
ACSC-ASEAN	✓			
Cambridge 2 Cambridge Cyber Competition				✓
Country 2 Country			✓	
Cyber Challenge Italia			✓	
Cyber Security Challenge Canada		✓		
Cyber Security Challenge Germany			✓	
Cyber Security Challenge SA			✓	
DEF CON CTF			✓	
Midnight Sun Capture the Flag (AFCEA Sweden)			✓	
PicoCTF				✓
Pwn2Own				✓
US Cyber Challenge				✓
WCTF (Qihoo 360)			✓	
CyberTalents Arab and Africa Regional CTF				✓
National Collegiate Cyber Defense Competition			✓	
International Collegiate Cyber Defense Competition				✓
Global Cyberlympics			✓	
PlaidCTF				✓
HITCON				✓
Google CTF				✓

B.19 ONLINE OR IN-PERSON

Event Name	COVID-Affected	In-Person	Online
European Cyber Security Challenge		✓	
Cyber Centurion - CSC UK		✓	
ACSC-ASEAN		✓	
Cambridge 2 Cambridge Cyber Competition		✓	
Country 2 Country			✓
Cyber Challenge Italia		✓	
Cyber Security Challenge Canada	✓		✓
Cyber Security Challenge Germany		✓	
Cyber Security Challenge SA		✓	
DEF CON CTF		✓	✓
Midnight Sun Capture the Flag (AFCEA Sweden)	✓	✓	✓
PicoCTF			✓
Pwn2Own		✓	✓
US Cyber Challenge			✓
WCTF (Qihoo 360)		✓	
CyberTalents Arab and Africa Regional CTF			✓
National Collegiate Cyber Defense Competition		✓	
International Collegiate Cyber Defense Competition			✓
Global Cyberlympics		✓	✓
PlaidCTF			✓
HITCON			✓
Google CTF			✓

B.20 MENTOR/COACH

Event Name	Adult/Teacher	Employer	Previous Competitors	No	Unknown
European Cyber Security Challenge	✓				
Cyber Centurion - CSC UK	✓				
ACSC-ASEAN				✓	
Cambridge 2 Cambridge Cyber Competition	✓				
Country 2 Country				✓	
Cyber Challenge Italia					✓
Cyber Security Challenge Canada		✓			
Cyber Security Challenge Germany				✓	
Cyber Security Challenge SA			✓		
DEF CON CTF				✓	
Midnight Sun Capture the Flag (AFCEA Sweden)	✓				
PicoCTF				✓	
Pwn2Own				✓	
US Cyber Challenge				✓	
WCTF (Qihoo 360)				✓	
CyberTalents Arab and Africa Regional CTF				✓	
National Collegiate Cyber Defense Competition	✓				
International Collegiate Cyber Defense Competition	✓				
Global Cyberlympics	✓	✓			
PlaidCTF				✓	
HITCON				✓	
Google CTF				✓	

B.21 PARALLEL CONTESTS

Event Name	Different Audience	Different Theme	Extra Challenges	No
European Cyber Security Challenge			✓	
Cyber Centurion - CSC UK				✓
ACSC-ASEAN				✓
Cambridge 2 Cambridge Cyber Competition				✓
Country 2 Country				✓
Cyber Challenge Italia				✓
Cyber Security Challenge Canada				✓
Cyber Security Challenge Germany				✓
Cyber Security Challenge SA				✓
DEF CON CTF		✓		
Midnight Sun Capture the Flag (AFCEA Sweden)				✓
PicoCTF				✓
Pwn2Own				✓
US Cyber Challenge				✓
WCTF (Qihoo 360)	✓		✓	
CyberTalents Arab and Africa Regional CTF				✓
National Collegiate Cyber Defense Competition				✓
International Collegiate Cyber Defense Competition				✓
Global Cyberlympics			✓	
PlaidCTF				✓
HITCON				✓
Google CTF				✓

B.22 ORGANISER COMMUNICATION

Event Name	Help	Hints	Platform Support	Unknown
European Cyber Security Challenge				✓
Cyber Centurion - CSC UK				✓
ACSC-ASEAN				✓
Cambridge 2 Cambridge Cyber Competition		✓		
Country 2 Country			✓	
Cyber Challenge Italia				✓
Cyber Security Challenge Canada				✓
Cyber Security Challenge Germany			✓	
Cyber Security Challenge SA	✓			
DEF CON CTF	✓		✓	
Midnight Sun Capture the Flag (AFCEA Sweden)				✓
PicoCTF				✓
Pwn2Own				✓
US Cyber Challenge				✓
WCTF (Qihoo 360)				✓
CyberTalents Arab and Africa Regional CTF				✓
National Collegiate Cyber Defense Competition				✓
International Collegiate Cyber Defense Competition				✓
Global Cyberlympics		✓		
PlaidCTF				✓
HITCON				✓
Google CTF			✓	

B.23 OTHER ACTIVITIES

Event Name	Briefings	Career Advice	Meals	Recruitment	Social	Unknown
European Cyber Security Challenge			✓		✓	
Cyber Centurion - CSC UK						✓
ACSC-ASEAN					✓	
Cambridge 2 Cambridge Cyber Competition		✓			✓	
Country 2 Country						✓
Cyber Challenge Italia				✓		
Cyber Security Challenge Canada				✓		
Cyber Security Challenge Germany				✓	✓	
Cyber Security Challenge SA	✓		✓			
DEF CON CTF						✓
Midnight Sun Capture the Flag (AFCEA Sweden)						✓
PicoCTF						✓
Pwn2Own						✓
US Cyber Challenge		✓		✓		
WCTF (Qihoo 360)						✓
CyberTalents Arab and Africa Regional CTF						✓
National Collegiate Cyber Defense Competition						✓
International Collegiate Cyber Defense Competition						✓
Global Cyberlympics			✓		✓	
PlaidCTF						✓
HITCON						✓
Google CTF						✓

B.24 CATERING

Event Name	Yes	No	Unknown
European Cyber Security Challenge	✓		
Cyber Centurion - CSC UK			✓
ACSC-ASEAN			✓
Cambridge 2 Cambridge Cyber Competition	✓		
Country 2 Country			✓
Cyber Challenge Italia			✓
Cyber Security Challenge Canada	✓		
Cyber Security Challenge Germany	✓		
Cyber Security Challenge SA	✓		
DEF CON CTF		✓	
Midnight Sun Capture the Flag (AFCEA Sweden)	✓		
PicoCTF			✓
Pwn2Own		✓	
US Cyber Challenge			✓
WCTF (Qihoo 360)	✓		
CyberTalents Arab and Africa Regional CTF			✓
National Collegiate Cyber Defense Competition	✓		
International Collegiate Cyber Defense Competition		✓	
Global Cyberlympics	✓		
PlaidCTF		✓	
HITCON		✓	
Google CTF		✓	

B.25 TRANSPORT

Event Name	Yes	No	Unknown
European Cyber Security Challenge	✓		
Cyber Centurion - CSC UK			✓
ACSC-ASEAN			✓
Cambridge 2 Cambridge Cyber Competition	✓		
Country 2 Country			✓
Cyber Challenge Italia			✓
Cyber Security Challenge Canada			✓
Cyber Security Challenge Germany			✓
Cyber Security Challenge SA			✓
DEF CON CTF		✓	
Midnight Sun Capture the Flag (AFCEA Sweden)	✓		
PicoCTF			✓
Pwn2Own		✓	
US Cyber Challenge			✓
WCTF (Qihoo 360)			✓
CyberTalents Arab and Africa Regional CTF			✓
National Collegiate Cyber Defense Competition			✓
International Collegiate Cyber Defense Competition		✓	
Global Cyberlympics		✓	
PlaidCTF		✓	
HITCON		✓	
Google CTF		✓	

B.26 CHALLENGE SOURCE

Event Name	Organisers	Participant-Provided	Platform-Provided	Sponsor-Provided	Unknown
European Cyber Security Challenge	✓				
Cyber Centurion - CSC UK					✓
ACSC-ASEAN					✓
Cambridge 2 Cambridge Cyber Competition	✓			✓	
Country 2 Country					✓
Cyber Challenge Italia					✓
Cyber Security Challenge Canada		✓			
Cyber Security Challenge Germany					✓
Cyber Security Challenge SA	✓		✓		
DEF CON CTF	✓				
Midnight Sun Capture the Flag (AFCEA Sweden)	✓				
PicoCTF	✓				
Pwn2Own				✓	
US Cyber Challenge					✓
WCTF (Qihoo 360)		✓			
CyberTalents Arab and Africa Regional CTF	✓				
National Collegiate Cyber Defense Competition	✓			✓	
International Collegiate Cyber Defense Competition	✓			✓	
Global Cyberlympics					✓
PlaidCTF	✓				
HITCON	✓				
Google CTF	✓				

B.27 COMMUNICATION CHANNELS

Event Name	Blog	CTFTime	Discord	Facebook	Flickr	IRC	Instagram	LinkedIn	Livestream	Telegram	Twitter	Website
European Cyber Security Challenge				✓							✓	✓
Cyber Centurion - CSC UK	✓						✓	✓			✓	
ACSC-ASEAN											✓	
Cambridge 2 Cambridge Cyber Competition				✓								
Country 2 Country			✓									✓
Cyber Challenge Italia				✓			✓	✓			✓	✓
Cyber Security Challenge Canada			✓									✓
Cyber Security Challenge Germany			✓								✓	✓
Cyber Security Challenge SA											✓	✓
DEF CON CTF		✓	✓								✓	
Midnight Sun Capture the Flag (AFCEA Sweden)		✓										✓
PicoCTF		✓	✓	✓			✓				✓	✓
Pwn2Own	✓										✓	
US Cyber Challenge				✓							✓	✓
WCTF (Qihoo 360)		✓							✓			✓
CyberTalents Arab and Africa Regional CTF				✓							✓	✓
National Collegiate Cyber Defense Competition								✓	✓		✓	✓
International Collegiate Cyber Defense Competition				✓							✓	✓
Global Cyberlympics	✓			✓				✓			✓	✓
PlaidCTF		✓				✓					✓	✓
HITCON		✓		✓	✓					✓	✓	✓
Google CTF		✓				✓			✓			✓

B.28 SOLUTIONS RELEASED

Event Name	Yes	No	Unknown
European Cyber Security Challenge		√	
Cyber Centurion - CSC UK		√	
ACSC-ASEAN		√	
Cambridge 2 Cambridge Cyber Competition		√	
Country 2 Country			√
Cyber Challenge Italia		√	
Cyber Security Challenge Canada		√	
Cyber Security Challenge Germany	√		
Cyber Security Challenge SA		√	
DEF CON CTF	√		
Midnight Sun Capture the Flag (AFCEA Sweden)	√		
PicoCTF		√	
Pwn2Own			√
US Cyber Challenge		√	
WCTF (Qihoo 360)		√	
CyberTalents Arab and Africa Regional CTF			√
National Collegiate Cyber Defense Competition			√
International Collegiate Cyber Defense Competition			√
Global Cyberlympics			√
PlaidCTF	√		
HITCON			√
Google CTF	√		

B.29 CHALLENGES RELEASED

Event Name	Yes	No	Unknown
European Cyber Security Challenge		√	
Cyber Centurion - CSC UK		√	
ACSC-ASEAN		√	
Cambridge 2 Cambridge Cyber Competition		√	
Country 2 Country			√
Cyber Challenge Italia		√	
Cyber Security Challenge Canada		√	
Cyber Security Challenge Germany	√		
Cyber Security Challenge SA			√
DEF CON CTF	√		
Midnight Sun Capture the Flag (AFCEA Sweden)		√	
PicoCTF	√		
Pwn2Own			√
US Cyber Challenge		√	
WCTF (Qihoo 360)		√	
CyberTalents Arab and Africa Regional CTF	√		
National Collegiate Cyber Defense Competition			√
International Collegiate Cyber Defense Competition			√
Global Cyberlympics			√
PlaidCTF	√		
HITCON	√		
Google CTF		√	

B.30 DATA RELEASED

Event Name	Yes	No	Unknown
European Cyber Security Challenge			√
Cyber Centurion - CSC UK			√
ACSC-ASEAN			√
Cambridge 2 Cambridge Cyber Competition			√
Country 2 Country			√
Cyber Challenge Italia	√		
Cyber Security Challenge Canada			√
Cyber Security Challenge Germany			√
Cyber Security Challenge SA			√
DEF CON CTF	√		
Midnight Sun Capture the Flag (AFCEA Sweden)			√
PicoCTF		√	
Pwn2Own		√	
US Cyber Challenge			√
WCTF (Qihoo 360)		√	
CyberTalents Arab and Africa Regional CTF	√		
National Collegiate Cyber Defense Competition			√
International Collegiate Cyber Defense Competition			√
Global Cyberlympics	√		
PlaidCTF	√		
HITCON	√		
Google CTF			√

B.31 PAPERS RELEASED

Event Name	Yes	No	Unknown
European Cyber Security Challenge	√		
Cyber Centurion - CSC UK			√
ACSC-ASEAN			√
Cambridge 2 Cambridge Cyber Competition			√
Country 2 Country		√	
Cyber Challenge Italia			√
Cyber Security Challenge Canada			√
Cyber Security Challenge Germany			√
Cyber Security Challenge SA			√
DEF CON CTF			√
Midnight Sun Capture the Flag (AFCEA Sweden)			√
PicoCTF	√		
Pwn2Own			√
US Cyber Challenge			√
WCTF (Qihoo 360)			√
CyberTalents Arab and Africa Regional CTF			√
National Collegiate Cyber Defense Competition			√
International Collegiate Cyber Defense Competition			√
Global Cyberlympics			√
PlaidCTF			√
HITCON			√
Google CTF			√

TP-02-21-396-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-501-2
DOI: 10.2824/313553