MetaCTF

A Comprehensive Guide to Hosting a Capture the Flag Competition

For Businesses, Organizations, and Conferences

www.metactf.com

contact@metactf.com

Table of Contents

Introduction 03

Setting up for Success 05

Planning the CTF 07

Running the CTF 12

Introduction

A Capture the Flag (CTF) competition is an engaging way to assess and develop cybersecurity skills through hands-on challenges. In a Jeopardy-style CTF, participants solve security puzzles across various categories to find hidden flags and earn points. This format has become increasingly popular in both educational and professional settings.

This guide provides detailed instructions for organizations looking to host their own CTF competition. It covers everything from initial planning to post-event analysis. Whether you're hosting a CTF for a corporate security team, an educational institution or a conference, this guide will help ensure the success of your CTF.

Getting Started

The decision to host a CTF competition extends beyond technical training. While organizations may consider CTFs an activity for security skills development, their value contributes to multiple aspects of organizational growth and culture. A CTF provides a unique environment where participants learn about security concepts and practice them in a safe environment. Rather than reading about vulnerabilities, they have to find and, in some instances, patch them. This practical approach helps people learn at a deeper level and understand how to apply tools or techniques to real situations. When properly executed, CTFs become powerful tools for developing security skills, fostering collaboration, and building a strong security culture within an organization.

Training and Development

Many managers make the mistake of scheduling training sessions without first building a culture that values ongoing skill development. The most effective security teams prioritize continuous learning over one-off training events. CTFs can help establish this culture by providing regular, hands-on practice with security concepts.

Security teams will gain practical experience solving realistic challenges while developers and IT professionals will learn security concepts that apply to their daily work. For organizations with Security Champions programs, CTFs provide a structured way for participants to build and demonstrate their security skills.

Organizational Benefits

CTF competitions offer key benefits beyond security training. They naturally encourage team building as participants work together across different departments and skill levels. For management, CTFs provide a practical way to assess technical talent.

Different types of organizations can leverage CTFs in unique ways. Conferences can use them to add interactive elements to their programs, giving attendees hands-on activities between talks and presentations. Higher education institutions

can integrate CTFs into their cybersecurity curriculum, helping students apply concepts they've learned in the classroom to hands-on, practical challenges. Security interest groups and professional organizations can use CTFs to bring their communities together and provide skill-building opportunities for their members.

Strategic Value

CTFs can play an integral role in developing security culture across an organization. When employees participate in security-focused events, they're more likely to consider security a part of their daily work. CTFs create natural opportunities for security teams to connect with other departments, breaking down the common perception of security as simply a compliance requirement.

These events also support diversity, equity, and inclusion initiatives in several ways. First, CTFs provide an objective way to demonstrate skills, regardless of background or traditional credentials. Additionally, teams often perform better when they include diverse perspectives and problem-solving approaches. The competitive format can help identify talented individuals who might be overlooked in traditional hiring and advancement processes.

Setting up for Success

Defining Goals

To ensure value from your CTF, it is important to clearly define what success looks like. Before diving into specific metrics, you need to clearly define goals.

Common goals for CTFs include:

- A high participation rate from specific functional teams.
- Exposing participants to new concepts, measured by number of different categories attempted by individuals and teams.
- Assessing skills across your organization.

Success Metrics

To prove the value gained from a CTF, it is important to identify success metrics to track progress on your organization's goals. These will vary based on your intended audience and organizational goals. Commonly used success metrics fall into three main categories. We recommend selecting three to five metrics (at least one from each category) to measure the effectiveness of your CTF.

01 Engagement and Activity Metrics

The following metrics provide insight into user activity and engagement:

- The number of active users.
- The number of submissions.
- The number of correct submissions.
- The number of submissions per minute/hour.

02 Individual Performance Metrics

The following metrics provide insight into user skills and performance:

- Percent of correct submissions (including by category).
- Percent of total available problems were solved (including by category).
- Average percent of total challenges solved by an individual.

03 Team Performance Metrics

Team performance metrics evaluate collaborative effectiveness and collective achievement by measuring things like the percentage of total correct team submissions, the percentage of total problems solved by the team, and the average percentage of total challenges solved by a team.

Planning Your CTF

Budget Considerations

A successful CTF requires careful budget planning. Consider allocations for training resources, platform fees for hosting the competition, and event costs if you're including an in-person component. Additional costs might include marketing materials to help drive participation and prizes to help boost engagement. To build, host, and manage a CTF internally, you will likely invest at least $20,000 including labor costs.

Event Timing and Duration

When, where, and for how long you host your CTF can impact its success. There is no one-size-fits-all solution. Here are some common approaches:

Annual

Annual CTFs typically coincide with Cybersecurity Awareness Month or team offsites. They offer flexible durations — from two hours to a month for virtual events. Longer competitions show participation spikes at the start and the end, requiring mid-event checkpoints. Virtual month-long events need strategic reminders to maintain engagement.

Annual CTFs are easy to plan and market, generating high engagement when aligned with existing security initiatives. However, the yearly gap severely limits knowledge retention. Participants who miss the event lose their only opportunity to participate in a CTF that year, undermining training goals. Annual CTFs are best for organizations with limited resources seeking maximum flexibility.

Biannual

Bi-annual CTFs balance skill development with manageable resource commitments. Space these events evenly throughout the year — if one falls in

October (Cybersecurity Awareness Month), schedule the second in April. When planning, consider company fiscal cycles, employee availability, and major security conferences. Avoid scheduling your CTF during vacation periods (August in EMEA) or conferences like DEFCON, Black Hat, and RSA. Biannual CTFs provide consistent opportunities to build on previous learnings while maintaining reasonable resource requirements.

Quarterly / Monthly

Quarterly/monthly CTFs deliver optimal learning outcomes but require a strong training culture. These events work best as short two-hour sessions to minimize workplace disruption. Quarterly reinforcement significantly improves knowledge retention compared to less frequent approaches. These events provide valuable point-in-time talent assessments, allowing skill development to be tracked over time. The primary challenge is resource intensity — dedicated program management is essential for configurations, logistics, and marketing. Without an established training culture, organizations struggle to maintain this cadence. Quarterly CTFs are best for companies serious about security skill development as a continuous process with the resources to support frequent events.

Content Design

The content for your CTF largely depends on your target audience. Choosing the right mix of challenges is critical to success. One primary reason CTFs fail is a mismatch between content difficulty and participant skill levels. Your first step should be identifying which of the three main audiences you're targeting.

General Audience

When designing a CTF for a general audience with varying technical backgrounds, it is important to build confidence. This is especially important for individuals who have never participated in a CTF before. The biggest mistake organizers make with general audience CTFs is jumping straight into technical challenges. Instead, start with basic security awareness questions that any participant can solve. Simple trivia about password etiquette or common security best practices gives participants early wins and encourages them to continue.

Company-specific content can be particularly effective for a general audience. Questions based on internal data privacy policies or security procedures not only test knowledge but reinforce important organizational guidelines. As participants gain confidence, you can introduce them to basic versions of traditional CTF categories like reconnaissance or simple cryptography puzzles.

You'll likely have some technically skilled participants, even in a general audience. To keep these participants engaged, include a selection of more challenging problems but align most of the content at the beginner level.

Technical Audience

For audiences with technical backgrounds but varying cybersecurity experience, focus on practical challenges that connect to their daily work. Software developers do well with secure coding challenges, and IT pros can engage with system hardening and network security scenarios. Create challenges that build on existing technical knowledge while introducing security concepts.

Cybersecurity Pros

Depth and complexity are important when designing CTFs for security professionals. These participants expect challenges that test both their theoretical knowledge and practical skills. Consider creating multi-stage challenges in which solving one problem reveals components of another.

When designing for security professionals, focus on six core topic areas: forensics challenges incorporating memory analysis, disk forensics, and network traffic analysis; cryptography challenges ranging from classic ciphers to modern encryption with emphasis on implementation weaknesses; web exploitation covering everything from injection flaws to attacks against modern frameworks; binary exploitation testing the ability to identify and exploit attacks against compiled binaries; reconnaissance/OSINT simulating realistic intelligence gathering from public sources; and reverse engineering including various platforms and obfuscation techniques to challenge participants' understanding of complex software behaviors.

Technical Requirements

Setting up the technical infrastructure for a CTF requires careful planning and consideration of multiple components. Many first-time organizers underestimate the complexity of the technical setup, resulting in last-minute scrambles or day-of issues that can derail an otherwise well-planned event.

Communicate clear hardware and software requirements to participants at least one week an advance. They'll need personal computers with administrator/sudo access to install specialized tools during the event. Advise participants to prepare virtual machines (Kali Linux or Windows VM) to avoid cluttering their main systems and to allocate dedicated storage space for competition files.

Recommend essential tools, including Wireshark for network analysis, Ghidra for reverse engineering, netcat for forming and listening to network connections, password crackers like Hashcat, forensics tools like Volatility and Autopsy, and web testing frameworks such as browser developer tools or BurpSuite. Multi-purpose utilities like CyberChef are particularly valuable, as are free services like Webhook.site for challenges requiring external web endpoints. Consider providing browser-accessible VMs for participants facing hardware limitations or corporate policy restrictions.

Platform Requirements

Your CTF platform serves as the foundation of the entire competition. It must be able to handle user registration, authentication, team management, scoring, and real-time flag validation. More complex challenges may require deploying virtual machines to ensure a controlled environment where nothing has to be installed locally. You can use open-source platforms, but they require time for setup and maintenance.

Security is essential in the platform setup. Corporate firewalls often block downloads required for traditional CTFs, so consider using browser-based VMs. This approach allows participants to access all necessary tools through their web browser while maintaining security standards. The platform should also include robust logging and monitoring capabilities to track participation and quickly identify any technical issues.

Project Management and Staffing

Running a CTF requires a dedicated team with clearly defined responsibilities. Note that the following roles can be consolidated in many circumstances.

Project Manager

The project manager serves as the central coordinator, overseeing all aspects of the competition from planning through execution. They need both technical understanding and strong organizational skills to effectively manage timelines, resources, and stakeholder communications.

Technical Subject Matter Experts (SMEs)

Technical SMEs play a crucial role in testing the platform and ideating & writing challenges before the event. They should verify that each challenge works as intended, assess difficulty levels, and ensure clear documentation exists for all components. During the event, these SMEs transition into a support role, helping participants who encounter technical issues or need guidance. Someone must be available at all times to answer participant questions to ensure the success of the event.

Communications Lead

A “Communications Lead” manages all participant interactions, from initial announcements through final results. They create and distribute participation instructions, monitor non-support communication channels during the event, and ensure participants receive timely updates about new challenges or technical issues.

Executive support is essential for both resourcing and organizational buy-in. Having a senior sponsor who understands the value of the CTF can help secure necessary funding and participation. Additionally, ensure you have clear budget ownership for both immediate costs like platform fees and prizes, as well as longer-term investments in content development and infrastructure.

However, even with a smaller team, each responsibility area needs

clear ownership and backup plans for critical functions.

Running the CTF

Before the Event

The success of your CTF relies largely on preparation. The weeks leading up to the competition are crucial for developing challenges, testing the platform, and creating a robust support infrastructure.

Challenge development requires deep technical expertise. Subject matter experts invest significant time designing scenarios that will effectively test participants' skills while remaining fair and educational. Test each challenge multiple times under different conditions. Document common issues and their solutions to help the support team respond quickly during the event. Create clear, step-by-step participation instructions that include platform access, challenge submission procedures, and support contact information.

During the Event

During the event, real-time monitoring for support issues should be the primary focus. Maintain open communication channels for participants to seek guidance and report issues. Because events are timed, support needs to be available for immediate response at all times during the competition.

Even with thorough preparation, unexpected issues can arise during a CTF. A well-structured response plan ensures that disruptions are handled efficiently, maintaining fairness and participant engagement.

One of the most common challenges for administrators is dealing with technical issues in challenges themselves. Despite rigorous testing, bugs or unintended solutions can emerge. If a challenge is broken or unclear, organizers should communicate updates promptly and, if necessary, adjust or replace it without disrupting the competition. Flag submission errors can also frustrate participants, especially if validation scripts are too rigid. Providing clear flag formats and

allowing for slight variations in input can prevent these issues.

Technical infrastructure failures, from platform crashes to unexpected server loads, require a contingency plan. Stress testing in advance helps mitigate risks, but organizers should have backup servers and the ability to extend competition time if major disruptions occur. Security threats, such as unauthorized access or DDoS attacks, also need consideration. Implementing monitoring tools and restricting access to essential services can prevent malicious activity from impacting the event.

By preparing for these scenarios in advance, organizers can handle challenges smoothly and maintain a seamless experience for participants.

After the Event

After the CTF concludes, review your available data, including participation metrics, challenge completion rates, and performance by topic. Gather feedback from participants about challenge difficulty, platform usability, and overall event experience. Create a report for your stakeholders that directly ties outcomes to the goals you set prior to the event. Include specific examples of successful engagement and areas for improvement. You can use this information to refine your approach for future events, refining challenge difficulty, support, or platform setup.

The conclusion of a CTF should mark the beginning of deeper learning and engagement rather than an abrupt end. Participants benefit most when they have access to challenge write-ups or walkthroughs, allowing them to learn from the problems they struggled with. Organizers can further support skill development by hosting follow-up sessions, where experienced players break down solutions and share strategies.

Beyond a single event, organizations can foster a long-term security culture by creating dedicated discussion spaces, such as Slack or Discord groups, where participants can continue exchanging ideas. Running smaller, periodic challenges or “challenge of the month” competitions keeps engagement high and encourages continuous learning. Encouraging participants to explore other cybersecurity learning platforms or upcoming CTFs ensures that the event serves as a launchpad rather than an isolated experience.

A well-executed post-CTF strategy ensures that the competition has lasting impact, helping participants develop practical skills while strengthening an organization's security culture.

Special Considerations for Conferences

Running a CTF at a conference requires additional planning around logistics and marketing. The competition needs to complement rather than compete with other conference activities. For conference-based CTFs, it might be possible to offset some of your costs through sponsorship arrangements.

Marketing

Make the CTF a visible part of the conference experience. Establish a dedicated booth in a high-traffic area where staff can help with registration and answer support questions. Create eye-catching displays that show live scoreboards throughout the venue, generating interest and encouraging participation. Include QR codes on all marketing materials for easy registration access.

Integrate CTF information into the main conference registration process. Provide clear details about competition timing, prize structures, and participation requirements. Create dedicated communication channels using the conference's preferred platforms, whether that's Slack, Discord, or another tool.

Engagement Strategy

Build excitement by implementing strategic scoreboard management. Consider hiding the scoreboard during the final hours of the competition to create suspense before the awards ceremony. Plan the awards presentation for a high-visibility slot, possibly before a major keynote or during closing ceremonies. Share results on social media to create buzz and recognize participants. Always obtain permission from winners first and be prepared to use team names or aliases if participants prefer to remain anonymous.

Challenge Recommendations

Conference CTFs should be designed to accommodate various skill and participation levels. Some conference attendees will dedicate a significant amount of time to the CTF, while others may only be able to attempt a few challenges between sessions. Structure the challenge release schedule around the conference agenda, making sure to avoid scheduling over any keynotes or networking events.

Build vs. Buy

One of the most critical decisions you will make when planning your CTF is whether to build the platform and challenges and host the CTF in house or partner with a vendor that specializes in CTFs. Here are a few things to consider before making your decision.

01 The Platform

Building your own CTF platform requires technical expertise and dedicated resources. Your team needs experience in web application development, security infrastructure, and challenge creation. The development process typically takes several months, including time for security testing and platform hardening. You'll need to create or adapt scoring systems, user management interfaces, and monitoring tools. The main advantage of building your own platform is complete control over the environment and challenges. However, this control comes with ongoing maintenance responsibilities and the need for dedicated support staff during events.

02 Challenge Development

Challenge development can be difficult if you've never created challenges for a CTF before. In order to develop technically accurate challenges, you need someone with deep security knowledge and knowledge of CTFs. Plan to create 25-40 challenges across different difficulty levels and topics for a single-day CTF.

Once a challenge is created, it needs to be developed and thoroughly tested to ensure it's solvable and correctly validates flags.

There are many more considerations that go into challenge development including: Ideation, challenge creation, quality assurance testing, challenge quality and performance testing, and challenge deployment.

03 Support

Support requirements for in-house platforms are intensive and time-critical, particularly during the event itself. CTF competitions generate a constant stream of real-time support needs from knowledgeable staff. Participants get stuck and need hints, challenge infrastructure occasionally fails, flags don't validate correctly, and scoring disputes arise. Each of these issues demands immediate attention to maintain the competition's momentum and participant engagement. You'll need dedicated support staff monitoring the platform throughout the event, often requiring multiple people to work in shifts for longer competitions. Many organizations underestimate this real-time support burden and find themselves overwhelmed during the event.

04 Cost

From a financial perspective, organizations should expect significant time and expert human resources to building and hosting a CTF internally. This includes the time it takes to conduct platform development, challenge creation, infrastructure, and basic support costs. This does not account for the significant opportunity cost of pulling in-house security experts away from their primary responsibilities to develop and support the platform.

Outsourcing

Vendors like MetaCTF provide CTFs as a service so companies / organizations don't have to build their own infrastructure and content. The platform offers several key advantages that address many of the challenges outlined in this guide.

01 Technical Infrastructure

Use a vendor with a web-based platform that is accessible from any browser, eliminating the need for local installations or a complex setup. Ideally the platform will include live Windows and Linux VMs for select challenges, solving the common problem of tool accessibility in corporate environments. Infrastructure should be hosted securely to ensure reliability and performance.

02 Content and Challenge Library

Vendors should provide a broad range of challenges in both difficulty and topic. Challenge content should be customized to fit your organization's specific needs and security focus areas. Make sure that you can offer content relevant to your team's experience level and job functions.

03 Competition Management

Ideally you will be able to offer options for both individual and team-based competitions. Admins should be able to customize dashboards with competition rules, timers, FAQs and prize information. A cascading hint system is nice to have to reduce frustration, with hints available for free or at the cost of one point.

04 Support Services

Support is a highly important consideration. Some vendors provide additional support features, including:

- Live support during the CTF
- Live or recorded introduction and debrief sessions
- Office hours for CTFs longer than 24 hours

05 Scoring

Target an offering that supports customizable scoreboards that can be configured to use either fixed points or dynamic scoring based on solve rates and shown or hidden as needed. The scores should also be broken down by skill level, functional group, department, geography, or other determinants.

Outsourcing should allow your organization to focus on user engagement and learning outcomes rather than technical implementation and logistics, making it particularly valuable for first-time CTF organizers or those with limited resources.

Conclusion

Successfully hosting a CTF requires a balance of technical implementation and participant engagement. Whether building in-house or working with a vendor, make sure you clearly define your goals and have the resources to support participants before, during, and after the event. When properly executed, CTFs are engaging, powerful tools for developing skills and building a stronger security culture.