



ASSESSMENT

UNION OF EUROPEAN FOOTBALL ASSOCIATIONS (UEFA) CHAMPIONS LEAGUE FINAL

ZEROFOX INTELLIGENCE

A-2022-05-25a

TLP: Green

Criticality: High

Intelligence Requirements: Geopolitical & Physical

May 25, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 08:00 AM (EDT) on May 20, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

UEFA Champions League Final

Executive Summary

The 2022 UEFA Champions League Final (“the Final”) between Liverpool Football Club (FC) and Real Madrid will take place at 8:00 PM on May 28, 2022, at Stade de France in Paris, France. The Final’s move from Russia to France over Russia’s invasion of Ukraine increases the likelihood of Russian-affiliated cyber and political proxies finding ways to disrupt the match, amplify negative messaging, and promote more direct, violent action. Additionally, ZeroFox Intelligence assesses that major violent protests in the run-up to the Final are unlikely; however, the wave of election-related protests across Paris could exacerbate any peaceful march or protests pertaining to the most recent change to the Champions League format. Although ZeroFox Intelligence has not observed any chatter in Clear, Deep, or Dark Web platforms calling for the circumvention of security measures in place at Stade de France, ZeroFox posits that any operational systems with internet connectivity at the Stade de France venue are susceptible to a disruptive cyber attack.

Key Points

- The Final’s move from Russia to France in late February 2022 over Russia’s invasion of Ukraine makes the event a likely target of Russian cyber threat actors, who also reportedly targeted the 2018 final in Kyiv. Scenes of pro-Ukraine solidarity are expected at the event, although there are no Ukrainian or Russian players.¹ Russian-affiliated threat actor groups have recently attempted to disrupt European competitions but have not expressed intent to target the Final as of this writing.
- ZeroFox Intelligence assesses that major physical protests at the Final are unlikely; however, they are possible given the wave of election-related protests across Paris each weekend during the election cycle and recent protests across stadiums in Europe against UEFA for attempts to change the Champions League

¹ <https://twitter.com/regurgitad0r/status/1524087267035435008>



format. Liverpool supporters have been among the most vocal opponents of previous non-UEFA reforms.

- Although ZeroFox Intelligence has not observed any chatter in Clear, Deep, or Dark Web platforms calling for the circumvention of security measures in place at Stade de France, ZeroFox posits that any operational systems with internet connectivity at the Stade de France venue are susceptible to a disruptive cyber attack. A compromise of an Internet of Things (IoT)-connected lighting system has perhaps the most potential to disrupt the Final.
- Although no chatter about planned terrorist attacks has been identified, lone-wolf attackers are of the utmost concern. One form of inspiration could be the ongoing trial of Abdeslam, which attracts widespread media attention on key dates.²

Physical Security Concerns

GEOPOLITICAL TENSIONS. The Final's move from Russia to France over Russia's invasion of Ukraine increases the likelihood of Russian-affiliated cyber and political proxies finding ways to disrupt the match, amplify negative messaging, and promote more direct, violent action. The game will likely have a dedication to Ukraine, which could lead to criticism from Russia. The united European consensus against Russia and the lack of prominent Ukrainian or Russian players minimizes the risk of a major Russian escalation during the game, as most supporters will be on the same side of the conflict. Were Russia to threaten the Final, it would likely be in a way they can plausibly deny, such as a cyber attack. However, anti-Russian protesters could use the Final to protest the war, which could elicit a response from Russia after the event.

LOCAL PROTESTS. France is preparing for parliamentary elections in June, which has prompted a wave of weekly demonstrations against the high cost of living led by the Yellow Vests (Gilet Jaune). Protesters could use the Final as a means of attracting attention to their cost of living issues.³ However, the most likely protest activity will be in downtown Paris close to tourist and government locations. The Yellow Vests have announced two protests for Paris on May 28, 2022, although locations have not been identified. One protest is over COVID-19 vaccines, and the other is over the cost of

²

<https://www.france24.com/en/europe/20220419-belgium-starts-trial-of-suspected-paris-attack-accomplices>

³ <https://twitter.com/JarodGJ2022/status/1525021758935408640>



living.⁴ The increased media attention for the Final could attract Yellow Vest groups to Stade de France, but they will likely be held back by a security perimeter.

PROTESTS AGAINST UEFA. While ZeroFox Intelligence did not identify any evidence of planned activity coinciding with the Final, protests against proposed changes to the Champions League are possible due to UEFA's recently-released plans to increase the number of teams in—and thus games held during—the Champions League. Protesters allege that UEFA is seeking to maximize revenue at the expense of quality. The most criticized change would be to guarantee Champions League positions for historically powerful teams. UEFA's proposal follows a recent effort by 12 of Europe's biggest teams, including Liverpool and Real Madrid, to form their own non-UEFA competition with guaranteed entry for the signatory clubs known as the "Super League." Real Madrid is seen as the biggest proponent of the Super League, and its president, Florentino Perez, has been the least apologetic about the project, promising to resuscitate it again when the political climate is right.⁵ Since the UEFA proposals came out in April 2022, there have been similar but more muted reactions—including calls for boycotts, some stadium protests, and open letter campaigns from supporter groups. Supporters inside the stadium on May 28, 2022, may attempt a small protest that could take the form of an anti-reform banner; however, ZeroFox Intelligence has not observed any planned activity thus far, and protests outside the stadium are also possible.⁶

FIELD INVASIONS. ZeroFox Intelligence assesses that the risk of fan or player-based violence and field invasions at the Final is higher given recent disruptive activities—particularly field invasions following the games, as seen on May 17, 2022, during a semi-final play-off match in Nottingham, UK that lead to arrests. Both individuals involved were non-playing members of the losing Sheffield United team.⁷ Similar field invasions by fans that resulted in altercations with playing and coaching staff took place on May 19, 2022 at Goodison Park stadium in Liverpool—which is the home stadium of Liverpool's rival and fellow Liverpool-based team, Everton—and in Port Vale. However, security measures in place at the Final will likely mitigate such risk;

4

<https://manifestationgiletsjaunesparis.fr/samedi-28-mai-2022-manifestation-pour-une-justice-sociale-fiscale-et-climatique-pour-le-ric-contre-laugmentation-du-prix-des-produits-de-premiere-necessite-essence-electricite-pour/>

5

https://www.eurosport.com/football/liga/2021-2022/real-madrid-president-florentino-perez-insists-super-league-would-bring-financial-fair-play-to-europ_story.sto8634011/story.shtml

6

<https://www.foottheball.com/explainer/champions-league-bayern-munich-supporters-protests-new-swiss-model-reforms-andrea-agnelli-arsenal-fans>

7

<https://news.sky.com/story/cowardly-attack-during-pitch-invasion-leaves-sheffield-utds-billy-sharp-needing-stitches-12615632>



in particular, the prospect of the 20,000 vetted Liverpool or Real Madrid supporters storming the Stade de France field is unlikely given they are a minority in the stadium.

RIVAL CLASHES. While unlikely, violent clashes between rival supporters cannot be ruled out. Inside the stadium, supporters of Real Madrid and Liverpool will be kept separate. Each team has also only been given 20,000 tickets, with the remaining 50 percent going to neutrals or dignitaries. Therefore, violent clashes are unlikely. However, Liverpool supporters were blamed for the deaths of almost 40 people and injury to another 600 after attacking rival supporters at the same event in 1985 in Brussels. The violence led to the collapse of a stadium wall. Liverpool was subsequently banned from the competition for years, and major infrastructure and safety protocols have been implemented.

HOOLIGAN VIOLENCE. The prospect of widespread, premeditated hooligan violence is unlikely but could erupt outside the stadium in public areas designated for game watching. These gathering places have occasionally been the scenes of violence in the past. In 2018, a Liverpool supporter was left paralyzed after being attacked by rival supporters at a gathering before the game.⁸ Fanatical supporters of Real Madrid are known as Ultras; they have carried out acts of violence during matches before and used the media attention from games to publicize their political stances. Following disappointing performances of the Real Madrid team, Ultras have threatened players. During episodes of political tension, Ultras have also been known to use the games to make racist gestures. The more radical members are usually barred from attending or traveling to games. While Ultras do occasionally engage in acts of violence similar to that of hooligans, they are often officially affiliated with the team and engage with the club in formal capacities. A more typical role for an Ultra is to establish a good atmosphere at the games, as well as a connection between the fans, players, and the club.

Threat of Terrorism

Although no chatter about planned terrorist attacks has been identified, the most significant terror threat comes from lone-wolf attackers. One form of inspiration could be the ongoing trial of Abdeslam, which attracts widespread media attention on key dates.⁹ France's last major bout of jihadist violence came in the form of lone-wolf attackers inspired by France's supposed anti-Muslim rhetoric during the high-profile trial for the victims of the *Charlie Hebdo* massacre. *Charlie Hebdo* is a French satirical

⁸

<https://www.telegraph.co.uk/football/2019/02/28/roma-hooligan-attacked-liverpool-fan-sean-cox-jailed-three-and/>

⁹

<https://www.france24.com/en/europe/20220419-belgium-starts-trial-of-suspected-paris-attack-accomplices>



magazine, and its headquarters in Paris was attacked by al-Qaeda in January 2015 after the magazine released caricatures of the Prophet Mohamed.¹⁰ During the trial in 2020, there were several lone-wolf terror attacks in France, including the beheading of a teacher, Samuel Paty, who promoted the caricatures. The beheading in October 2020 sparked a wave of anti-Muslim legislation in France that led to an international boycott of France in many Muslim countries and included some acts of violence—particularly in Pakistan—throughout May 2021.¹¹ A similar outcome now is unlikely but cannot be ruled out given the ongoing trial and the significance of Stade de France to the 2015 Paris attacks.

On November 13, 2015, a series of coordinated attacks occurred in Paris. Three suicide bombers struck Stade de France during a football match, while another group of attackers struck cafés and restaurants in Paris. The third group of threat actors attacked the Bataclan theater during a concert. In total, 130 people were killed and 368 were injured across Paris.¹² Most of the attackers were French or Belgian nationals. All of the attackers, with the exception of two, were able to enter France after being trained by Islamic State (IS) in Syria. Abdelhamid Abaaoud, a Belgian national and ringleader of the group, was featured in an edition of the IS English-language magazine *Dabiq*. In the magazine, Abaaoud spoke about how he fled to Syria after police raided his apartment in Belgium. Despite this, authorities were unable to track Abaaoud, and he returned to Belgium and recruited several people from his childhood—including brothers Brahim and Salah Abdeslam. Brahim Abdeslam detonated himself outside a café in Paris. Salah Abdeslam was supposed to detonate himself at the Stade de France but got cold feet and went into hiding. Salah Abdeslam later went on to organize the March 2016 attacks in Brussels. He is currently participating in a high-profile trial in Paris that is expected to conclude in June 2022.¹³

The same cell responsible for the November 2015 Paris attacks also planned and executed the March 2016 attacks on Brussels Zaventem Airport (BRU) and the Maalbeek underground station. One of the participants in the Paris attacks who managed to escape, Salah Abdeslam, was arrested days before the March 2016 attack. The explosive used in the Paris and Brussels attacks, triacetone triperoxide (TATP), was also used in the IS attack at the AO arena in Manchester in 2017. These three attacks in

¹⁰

<https://www.euronews.com/2022/01/07/charlie-hebdo-attack-victims-remembered-seven-years-on>

¹¹

<https://www.rfi.fr/en/international/20210414-pakistan-forces-move-to-clear-islamists-in-anti-french-protests-prophet-mohamed-samuel-paty-charlie-hebdo>

¹²

<https://www.france24.com/en/france/20210908-paris-november-2015-attacks-a-timeline-of-the-night-that-shook-the-city>

¹³

<https://www.euronews.com/2022/05/19/paris-attacks-trial-young-son-of-bataclan-victim-calls-suspect-a-rotten-banana>



close geographic proximity demonstrate the desirability of attacking large stadiums, as well as the transportation infrastructure that supporters may use to attend events.

Since these attacks, IS has lost its territorial control in Iraq and Syria, which afforded them the logistics to plan such attacks. It is also significantly more difficult for fighters to move from Syria through Turkey across Europe. IS priorities have also shifted away from carrying out high-profile international attacks to rebuilding locally. Therefore, a sophisticated and coordinated IS or al-Qaeda linked attack on the Final is highly unlikely.

Cybersecurity Concerns

The Champions League final in 2018 was held in Kyiv, Ukraine—coincidentally, between Real Madrid and Liverpool. During that final, there was reportedly an effort by Russian cyber actors to cripple Ukrainian infrastructure, with hackers infecting IoT devices—including internet routers and storage devices—with malware called VPNFilter.¹⁴ VPNFilter has a command that renders infected routers, servers, mobile phones, and laptops unusable and could have prevented millions of viewers from watching the game. It is unclear if the attack was done to coincide with that final, but the number of infected devices did increase just ahead of the match on May 29, 2018—with the bulk of them in Ukraine.

RISK TO THE EVENT. While ZeroFox Intelligence did not identify any discussions or attack planning, given that the Final was scheduled to be held in Russia until late February, Russian threat actors could have even more incentive to target the event. A similar attack that prevents millions of viewers from watching the game would cause lasting reputational damage to UEFA. Russian threat actors could choose to prioritize the game due to UEFA's antiwar and perceived anti-Russian rhetoric. France and the wider European Union's support for Ukraine could also make them and the Final a target. Two weeks ahead of the Final, pro-Russian hackers reportedly attempted to interfere in voting for the Eurovision song contest. Ahead of the vote, Ukraine was widely expected to win the contest, and openly pro-Ukraine rhetoric was permitted. The attacks reportedly came from the Killnet and Legion groups, which attempted to add votes to other countries so Ukraine would not secure victory. This demonstrates that Russian threat actors may view displays of anti-Russian or pro-Ukrainian sentiment as an indignity warranting a response.¹⁵ However, ZeroFox Intelligence

¹⁴

<https://www.e-careers.com/connected/how-hackers-nearly-disrupted-the-champions-league-final>

¹⁵

<https://www.nme.com/news/music/pro-russian-hackers-attempted-to-interfere-with-eurovision-votes-3226437>



closely monitors these actor groups and did not identify any plans by these collectives to wage attacks against the UEFA or the Final.

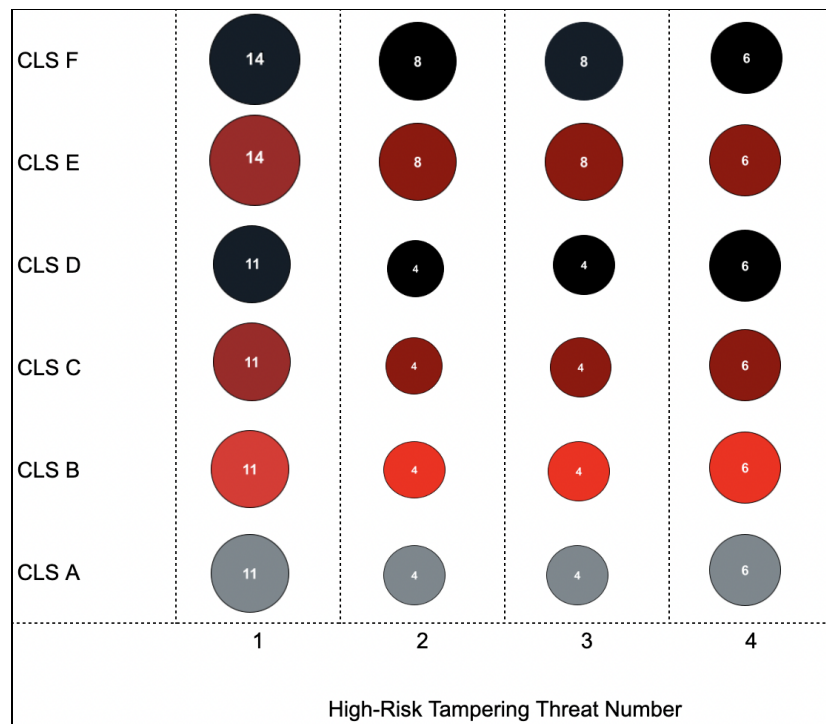
RISK TO THE INFRASTRUCTURE. Any operational systems with internet connectivity at the Stade de France venue are susceptible to attack. A compromise of an IoT-connected lighting system (CLS) has perhaps the most potential to disrupt the Final. The attack surface of a CLS will depend in large part on the extent to which associated network assets consist of on-premises equipment and software or cloud resources. For security purposes, the U.S. Department of Energy (DoE) has classified CLS according to internal versus external dependencies. The table below outlines six basic iterations of a network supporting a CLS:

System	Defining Features/ Description
CLS A	CLS comprised of a single-vendor solution using on-premise server and field gateway; Active Directory for authentication.
CLS B	CLS comprised of a single-vendor solution using cloud server and gateway; Active Directory for authentication
CLS C	CLS comprised of a single-vendor solution using on-premise server and field gateway; third-party application for authentication.
CLS D	CLS comprised of a single-vendor solution using cloud server and gateway; third-party application for authentication.
CLS E	CLS comprised of two-vendor integration using both on-premise and cloud servers and gateways; Active Directory for authentication.
CLS F	CLS comprised of two-vendor integration using both on-premise and cloud servers and gateways; third-party application for authentication.

Basic Iterations of a Network Supporting a CLS

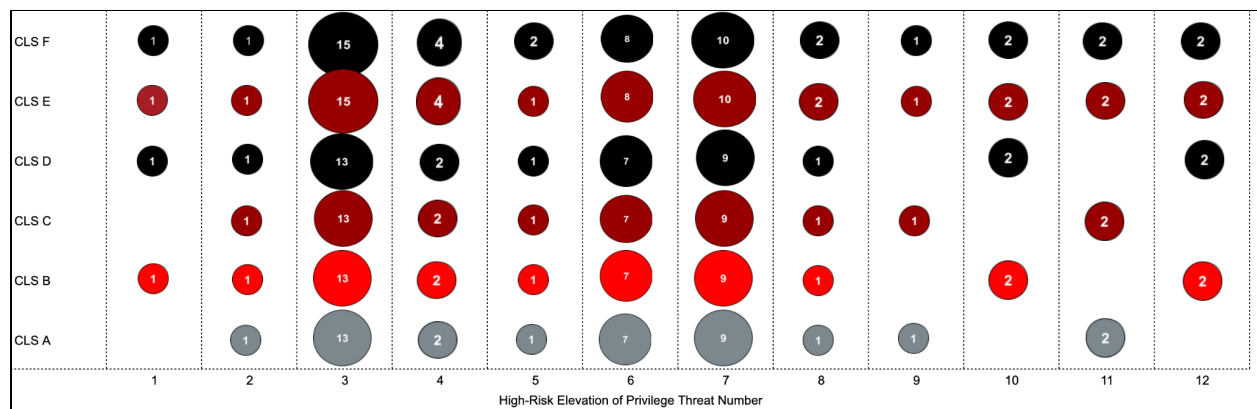
Source: U.S. Department of Energy

Of the various broad means of attacking a CLS, tampering (modifying code or data) and elevation of privileges (obtaining unauthorized capability to issue commands) are most likely to result in operational interference of lighting and disruption of the event. DoE has identified four specific high-risk threats that could result in tampering with a CLS and 12 that could enable the elevation of privileges. DoE has further quantified the various vectors or paths by which an attacker could deploy those threats for each of the six classifications of CLS, as represented in the following tables. Note that the number within each bubble represents vectors available for executing an attack rather than the resulting impact on a targeted system.



High-Risk Tampering Threats to CLS

Source: U.S. Department of Energy



High-Risk Elevation of Privilege Threats to CLS

Source: U.S. Department of Energy

Under both models, a higher number of vectors are available to an attacker for CLS that make use of both cloud and on-premises resources. For example, a CLS relying on both on-premises and cloud servers might provide an attacker both the option of compromising software pushed to a server as an update or of obtaining operationally sensitive data stored by a cloud provider. The models both show that numerous



vectors are available to an attacker—even for CLS relying primarily on on-premises services.¹⁶

One common means of attacking IoT-connected systems via tampering is reading or “sniffing” unencrypted data passing between endpoints. Information in a packet related to the lighting output value, could, for example, be modified to cause lights to turn off. Such a vulnerability can be addressed by deploying industry-standard encryption or using VLANs to secure point-to-point communications.¹⁷

To prevent elevation of privileges attacks, an asset discovery exercise to identify all equipment connected to a CLS can be conducted, followed by ensuring strong authentication requirements for each device and “hardening” connection points that are not required.

Security Measures

ZeroFox Intelligence has not observed any chatter in Clear, Deep, or Dark Web platforms calling for the circumvention of security measures in place at Stade de France; however, the Final is known to attract thousands of supporters without tickets, increasing the risk of possibly violent attempts to enter the venue. ZeroFox also notes some historical incidents associated with this event, including the 2015 explosive device detonations by suicide bombers who were unable to pass through the security.¹⁸

ENTRY SECURITY. The stadium has strict security measures, particularly at entry. Every person attending the event will be searched. Most bags are prohibited, and small items will be searched. The Stade de France is known to turn away fans who arrive at the wrong entrance.¹⁹ Entering the stadium can be a lengthy process as a result and noticeably longer than what most English fans are used to. Given the high-profile nature of the Final, which includes attendance by political dignitaries and celebrities, entering the stadium could take over an hour.

INFORMAL SUPPORTERS ZONE. To avoid attracting large crowds of supporters without tickets, the Final will not have official supporter (fan) zones. Official supporter zones are common during other football competitions, like the World Cup. During Champions League games, supporters usually establish their own informal supporter

¹⁶

<https://www.energy.gov/eere/ssl/articles/cybersecurity-threat-profile-connected-lighting-system>

¹⁷

https://betterbuildingssolutioncenter.energy.gov/sites/default/files/attachments/cyber_security_lighting.pdf

¹⁸

<https://www.msasecurity.net/security-and-counterterrorism-blog/case-study-perimeter-security-at-stade-de-france>

¹⁹ <https://www.uefa.com/uefachampionsleague/event-guide/stadium/>



zones not affiliated with UEFA. They are gathering points, usually near key landmarks, that opposition supporters go to when traveling to away games.²⁰ They have been the scenes of violence during other Champions League games; the gatherings often involve alcohol, and supporters of the host team have attacked rival supporters. In May 2021, fans of Chelsea and Manchester City clashed in the streets of Porto, Portugal, ahead of the Champions League final, for example.²¹ On May 18, 2022, Seville, Spain, hosted the 2022 UEFA Europa Cup final, which is the secondary competition to the Champions League. It was played between Rangers FC from Glasgow, Scotland, and Eintracht Frankfurt from Germany. Rangers had not been to a notable European Cup final in years, and 100,000 supporters flew to Seville—of which only 10,000 had tickets. There was widespread media coverage of clashes between the two sets of supporters ahead of the game. There were reports of drunk supporters grabbing chairs and umbrellas and fighting outside an impromptu supporters zone at a bar in Seville. Frankfurt supporters similarly clashed with West Ham supporters two weeks earlier, in the same city that was hosting the semi-final.²² In addition to the security issues, the clashes cause reputational damage.

UNTICKETED ENTRY ATTEMPTS. The Final is known to attract thousands of supporters without tickets, despite warnings to fans not to travel without them.²³ Given the close proximity of Paris, particularly for Liverpool supporters, thousands of non-ticketed fans are expected. The Eurostar train between London and Paris is also reportedly sold out leading up to the event, primarily to Liverpool supporters. This presents a risk to event security if supporters without tickets attempt to enter the venue. During the final event of the last major international football tournament, EURO 2020, which was held on July 11, 2021, thousands of England supporters without tickets were able to breach security at Wembley Stadium, England's national stadium in west London. Fans were able to overwhelm security, breach barriers, and access the event. Violent clashes between fans and stewards led to some victims being crushed but no fatalities. One breach occurred at a COVID-19 screening station two hours ahead of the game, when fans rushed the entrance.

Many of the supporters from the EURO 2020 final may be attending this game and may attempt similar tactics to enter Stade de France. A mass gathering of supporters from either side outside the stadium is also possible. The events at Wembley coincided

²⁰

<https://www.skysports.com/football/news/11945/12306162/champions-league-final-q-a-for-traveling-man-city-and-chelsea-fans>

²¹

<https://www.dailymail.co.uk/sport/sportsnews/article-9627549/Manchester-City-Chelsea-fans-involved-violent-clashes-Porto-police-other.html>

²² <https://www.mirror.co.uk/sport/football/news/rangers-fans-europa-league-final-27003074>

²³

<https://talksport.com/football/1102994/jurgen-klopp-liverpool-tickets-champions-league-real-madrid/>



with the first instances supporters were allowed back into stadiums after COVID-19 limits. The quick increase of capacity at Wembley in July 2021 from 67,000 attendees to full capacity of nearly 100,000 was partially blamed for the security breach. For the last year, supporters have been attending games with few capacity restrictions, and a breach of security by supporters is unlikely.

COVID-19

This is the first Champions League final since 2019 without COVID-19 restrictions. The 2020 final had no spectators, and there were capacity restrictions for the June 2021 final. Fans have been attending matches without restrictions or testing requirements for months, and no COVID-19 disruptions are anticipated. France has also lifted its requirement that spectators be vaccinated, and airlines are no longer requiring masks for travel as of May 16, 2022.²⁴ Vaccination requirements to enter France are still in place.²⁵

²⁴

<https://www.schengenvisainfo.com/news/today-france-lifts-covid-passport-requirement-for-access-in-most-venues-events/>

²⁵

<https://www.liverpoolecho.co.uk/news/liverpool-news/rules-liverpool-fans-travelling-champions-23850863>



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:

WHITE information without restriction, subject to copyright controls.