THE

SOCIAL ENGINEERING COMMUNITY

PRESENTS

2024 VISHING COMPETITION REPORT

AT DEF CON 32

Aunshul Rege

Rachel Bleiman

JC Carruthers

Stephanie Carruthers

January 18, 2025

Table of Contents

Introduction

WELCOME TO THE 2024 SECVC REPORT

Exploring the Art and Impact of Social Engineering

Welcome to the 2024 Social Engineering Community Vishing Competition (SECVC) Report! Now in its third year, this report provides a detailed look into the strategies, tactics, and lessons learned from the competition at DEF CON 32. Our goal is to offer a resource that professional and aspiring social engineers will find insightful and full of actionable tips. At the same time, we hope organizations can use these insights to better understand the tactics being used against them and strengthen their defenses against vishing attacks.

We want to give a huge shout-out to our incredible research team, Aunshul Rege and Rachel Bleiman, for their invaluable contributions. Their time, expertise, and dedication in gathering and analyzing the competition data have made this report possible. We are so grateful for their insights and the depth they bring.

Of course, none of this would be possible without the support of our amazing community. From the competitors and volunteers to the audience members who waited hours in line just to hear live calls at DEF CON—your enthusiasm fuels us! We're thrilled to have the opportunity to run the village and competition for a third year, and we can't wait to see how we continue to grow together.

See you next year,
JC & Snow

JC and Snow placing calls in the soundproof booth (2024)
Photo taken by: WiK's Pix

Competition Overview

SECVC Trophy and Dundie Awards (2024)
Photo taken by: WiK's Pix

Competition Overview

HOW THE COMPETITION WORKS

Introduction

In the Social Engineering Community's Vishing Competition (SECVC), participants engage in live phone calls in front of the SE Community audience at DEF CON, demonstrating both the challenges and simplicity of the craft while testing the varying levels of preparedness and defenses of real-world companies.

Purpose

This competition creates a safe space for participants to develop their social engineering skills while offering the audience valuable lessons, highlighting the critical role awareness training plays in modern business security.

Code of Ethics

Maintaining ethical standards is a top priority for the SEC. We have established a Code of Ethics that every individual making a phone call from our booth is required to agree to before placing any phone calls..

Competition Phases

Call for Competitors

We invite individuals and teams of 1, 2, or 3 people to take part in the competition. To apply, competitors must submit an application along with a 2-minute video. This helps our review board gain a better understanding of each applicant and their approach.

Company and Objectives Assignment

Once acceptance, competitors will receive a target company to conduct open-source intelligence ("OSINT"), develop pretexts, and execute calls during DEF CON against their target company. They will also be provided with a list of objectives and their corresponding OSINT and Vishing Call point values.

OSINT and Pretext Plan Reports

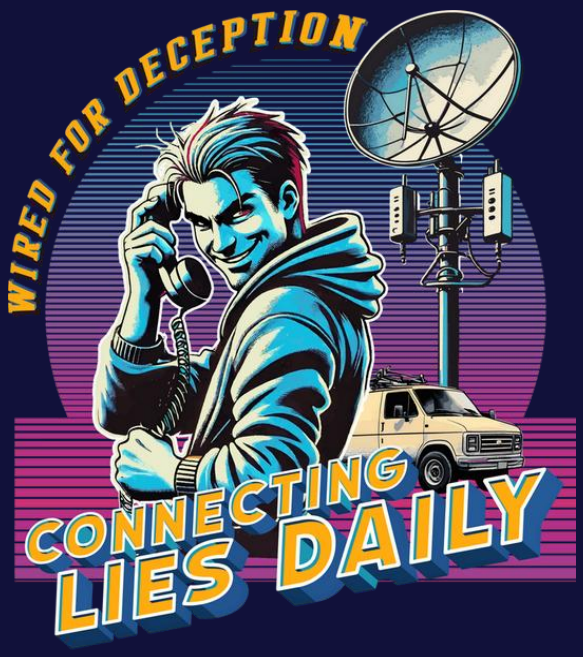
Upon receiving their target company, competitors are allotted a specific timeframe to perform OSINT gathering, aiming to discover and document objectives for point accumulation. calls. This period is also crucial for teams to prepare their strategy by writing their Pretext Plans for the live phone

Live Calls

Competitors will be assigned a specific day and time to conduct their live calls from a soundproof booth in the SEC village during DEF CON. They will have 22 minutes to make calls and accumulate as many objectives as they can. During this phase, judges will score the calls.

2024 Theme

WIRED FOR DECEPTION



Every year, the Social Engineering Community ties its Vishing Competition theme to the broader DEF CON theme, and let me tell you, choosing the right theme is no small task. It needs to align with DEF CON's overarching message, make sense for the competition, and give us something that sparks conversation and engagement. This year's DEF CON theme, "Engage," challenged us to think about the internet's centralization and what it means to take back control of our digital world. After many sleepless nights (and probably too much coffee), we landed on the perfect fit: Internet Service Providers (ISPs).

Why ISPs? Because they're the forgotten gatekeepers of our connected lives. Out of sight, out of mind—you only think about them when the internet goes down or it's time to pay the bill. Today, they control access to everything from Netflix binges to work Zoom calls, creating a universal dependence that makes their ability to respond to and prevent vishing calls a vital lesson. Watching ISPs through this lens provided not just a fair competition but insights for the audience to take back and strengthen their security awareness programs.

This year, we paid tribute to The Cable Guy, Jim Carrey's 1996 dark comedy about a cable installer whose "customer service" takes a chaotic turn. The movie's parallels to today's ISPs were too good to pass up: both hold the keys to access, and both can make or break your day.

In this report, we made a conscious decision not to name companies or tie any team's success to specific organizational shortcomings. The focus wasn't on shaming ISPs but on providing a platform for competitors to showcase their skills and for the audience to observe real-world social engineering techniques in action. Whether it's improving a security awareness program, adapting defensive measures, or recognizing strong security practices when a competitor's pretext gets shut down, there's something here for everyone.

So yeah, ISPs were the theme this year. We aligned with DEF CON's broader message, challenged competitors, and gave the audience a front-row seat to real social engineering in action. And if I lost some sleep obsessing over getting the theme *just* right? Worth it.

— JC

Competitor Selection Process

BUILDING A STRONG LINEUP

Call For Competitors

We opened the CFC months before DEF CON, allowing ample time to review submissions, make decisions, and give selected teams time to perform OSINT in preparation for their calls at DEF CON in August. This year, as is our tradition, the 2nd place team from the previous year was invited back, leaving space for 13 new teams. In 2023, we received 28 complete submissions; this year, we saw a significant increase, with 39 submissions!

How Teams Are Chosen

Selecting competitors for this year involved a rigorous process led by a four-person review board. Teams could consist of 1, 2, or 3 members, allowing for greater flexibility and diversity among participants.

How we chose the teams:

1. Submissions were evaluated based on their response to the prompt: "Why should your team be chosen to compete?" Reviewers prioritized responses that were heartfelt, unique, and relevant to the competition's goals.
2. Videos accompanying the submissions were analyzed for their ability to convey the team's passion and ideas clearly. Polished production wasn't necessary, but the content had to feel authentic and align with the written submission.

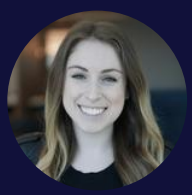
From a pool of competitive entries, 13 teams were selected to join last year's 2nd place team, completing this year's roster of 14 teams. However, last year's 2nd place winner could not make the event, so the top 14 team were selected.

Call for Competitor Review Board

Jennifer

Jamie

Matt



Rachel

39	4	14
Total Submissions	**Reviewers**	**Teams Chosen**

Ready, Set, Coach!

COACHING SESSIONS TO BOOST COMPETITOR SKILLS AND CONFIDENCE

2024 Coaches

Jennifer

JC

Jason
2023 SECVC Winner

How Does Coaching Work?

The SECVC includes a unique opportunity for competitors to gain valuable insights through personalized coaching sessions. Each team had the chance to meet with multiple coaches, all of whom brought firsthand experience in vishing or similar competition formats. These coaching sessions provided a platform for teams to refine their strategies, enhance their skills, and gain confidence ahead of the big event.

We were fortunate to have three dedicated coaches this year, including two former SECVC champions, a tradition that allows previous winners to give back to the community. Their expertise and familiarity with the challenges of the competition offered competitors a rare opportunity to learn from the best.

Coaching sessions were tailored to the needs of each team and covered a variety of topics, such as OSINT techniques, crafting compelling pretexts, and even practicing calls through roleplaying. While coaches were generous with their time and guidance, they adhered strictly to competition rules—offering no shortcuts or direct answers to ensure the integrity of the event.

58
Total Coaching Sessions

29
Total Hours of Coaching

2
Teams Skipped Coaching

Competitor Performance

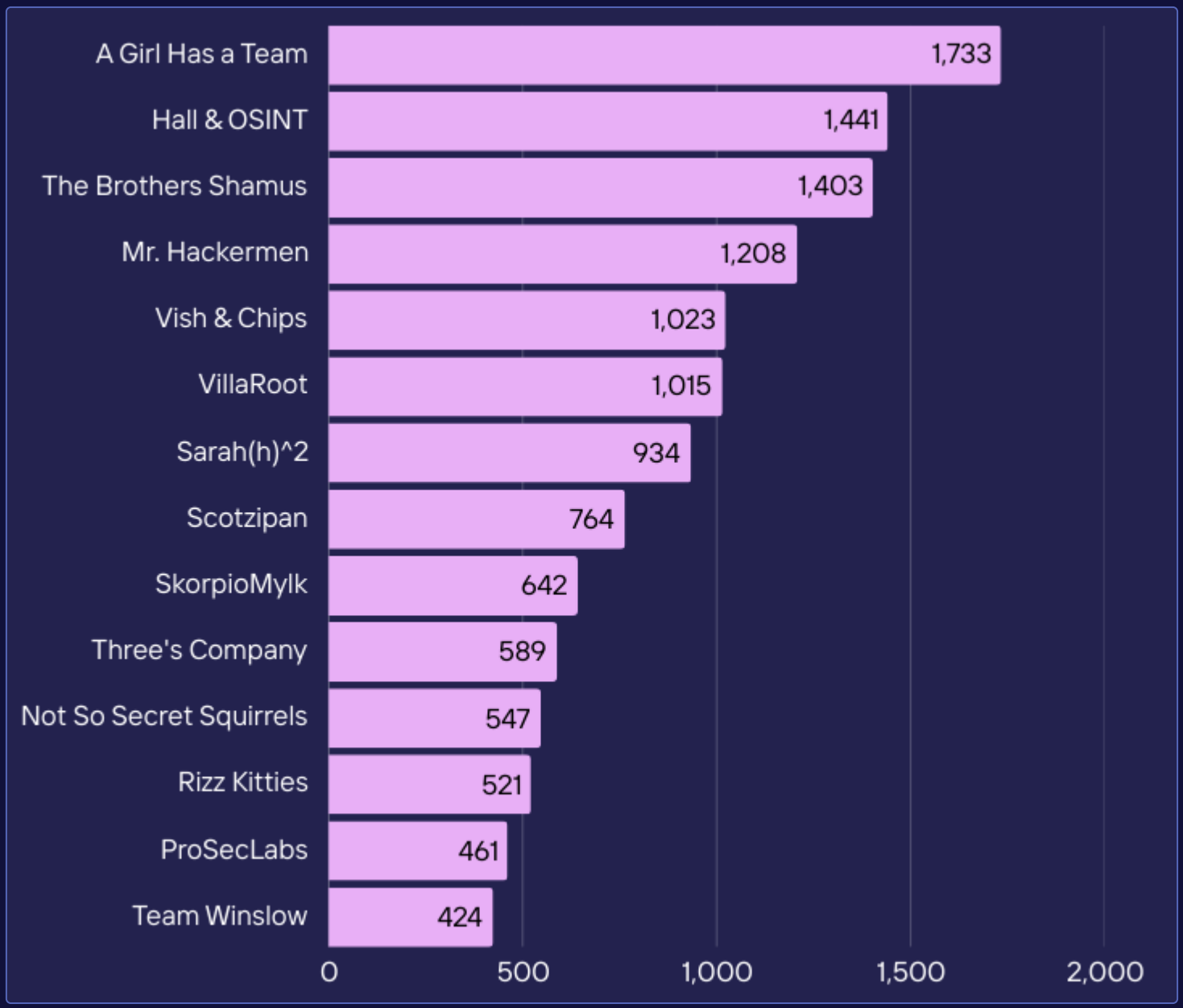
Team Rizz Kitties (2024)
Photo taken by: WiK's Pix

Final Scores

ALL POINTS COMBINED

How Teams Performed

The points below represent the total scores earned by competitors across all phases of the competition. Each phase tested a unique aspect of the competitors' skills, from research and strategy development to real-time execution under pressure. By combining the results from all phases, the final scores reflect a comprehensive evaluation of each team's performance.



Winning the SECVC

A BLACK BADGE EVENT

Being a Black Badge Competition

At DEF CON, awarding a black badge is the ultimate mark of distinction for any competition. This honor is rigorously evaluated each year, with only the most intense and engaging events earning the privilege—there's no automatic qualification. The expectation is that participants are so immersed in the challenge that they barely have time for anything else during the conference. With that in mind, we are thrilled to announce that, for the third consecutive year, our competition has achieved the prestigious status of being a black badge event!

Winning Team

This year's winning team, "A Girl Has a Team," brought both skill and humor to the competition. The name is a playful nod to Andi's solo effort in 2023, when she competed as "A Girl Has No Team." In 2024, Andi joined forces with James and Jace to take on the challenge together. Although Jace couldn't attend DEF CON in person, the trio's collaboration was unstoppable. Their exceptional teamwork and expertise led them to a well-deserved victory in this year's competition.

Partial Team "A Girl Has A Team" (James and Andi) with their black badge and SECVC trophy.

OSINT Scores

TURNING OBJECTIVES INTO ACTIONABLE INTELLIGENCE

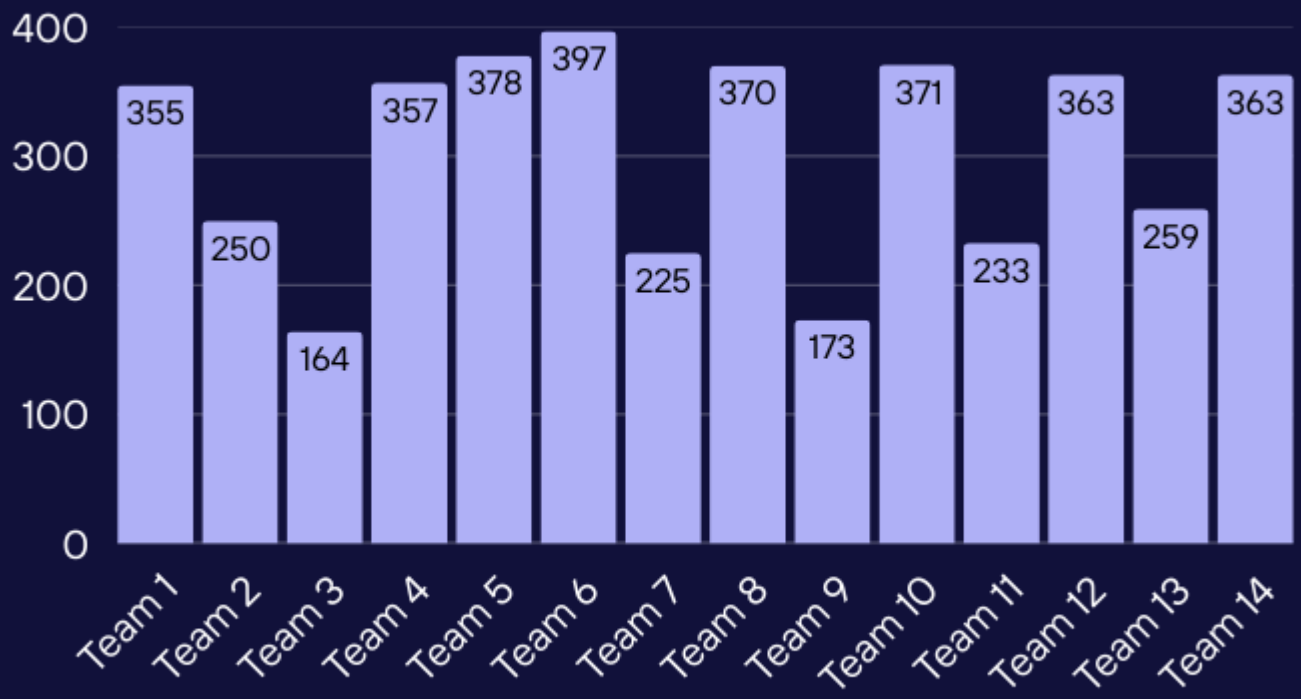
The OSINT Phase

Once teams were assigned their target company, their initial task was to create an Open-Source Intelligence (OSINT) report. Using a list of objectives provided by the SEC, teams gathered and documented information to earn points. The report was evaluated in two ways: individual objectives were scored if at least two out of three judges approved them, and the overall report was given an average score based on each judge's assessment. Teams could earn up to 400 points total during this phase.

Score Composition

#	Section	Description	Points Possible
1.	Objectives	Each team has a list of 25 OSINT objectives to idenitfy and each objective was assigned a point value.	300
2.	Report Score	The report rubric encompasses an executive summary, documentation, recommendations, grammar, among other criteria.	100

Total OSINT Report Scores by Team



Pretext Plan Scores

CRAFTING THE PERFECT PLAYBOOK FOR VISHING CALLS

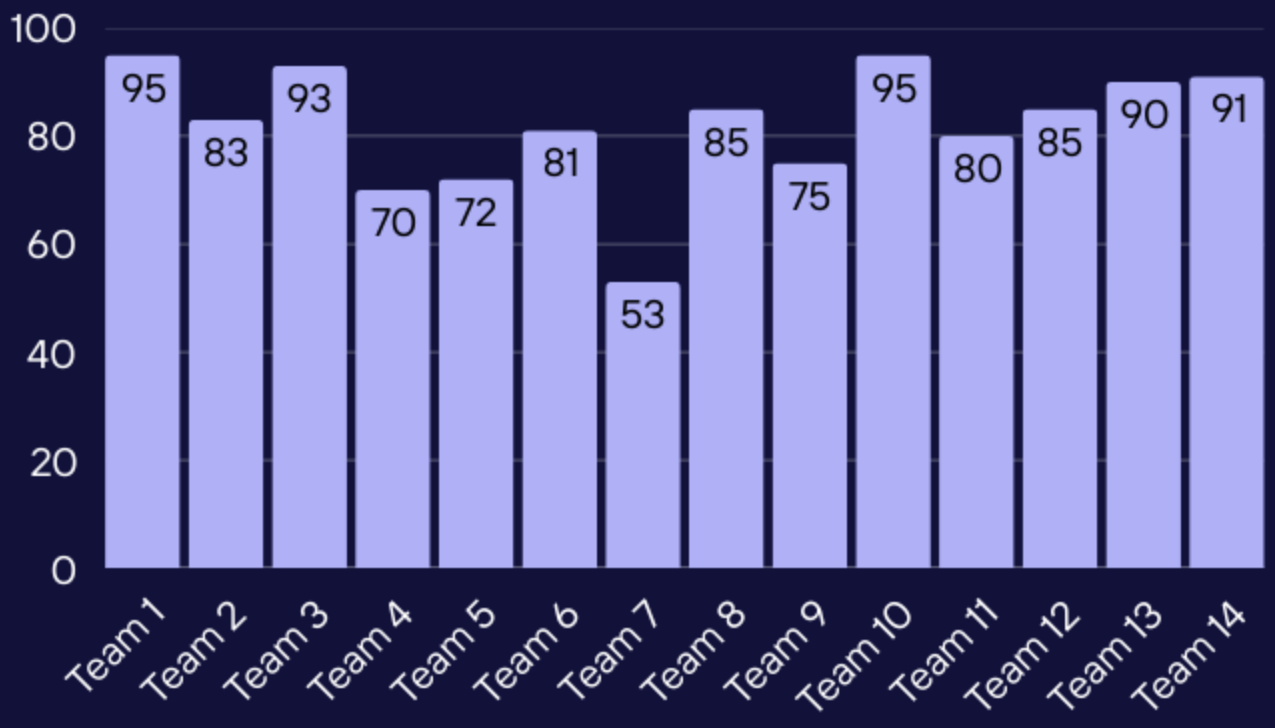
The Pretext Plan Phase

Following the OSINT phase, competitors were tasked with creating a comprehensive Pretext Plan Report prior to arriving at DEF CON. This report needed to outline at least three distinct pretexts the team planned to use to achieve their objectives, as well as the specific phone numbers they intended to target. To ensure fairness, the SEC team mandated that no other numbers could be contacted during the live call phase. SEC also thoroughly verified that all submitted phone numbers belonged to the intended targets.

Score Composition

#	Type	Description	Points Possible
1.	Report Score	The scoring rubric included points for competitors who provided at least three documented pretexts, with additional emphasis on the quality of these pretexts, as well as the quality and quantity of submitted phone numbers, among other factors.	100

Pretext Plan Scores by Team



Live Calls Scores

RING, RING...

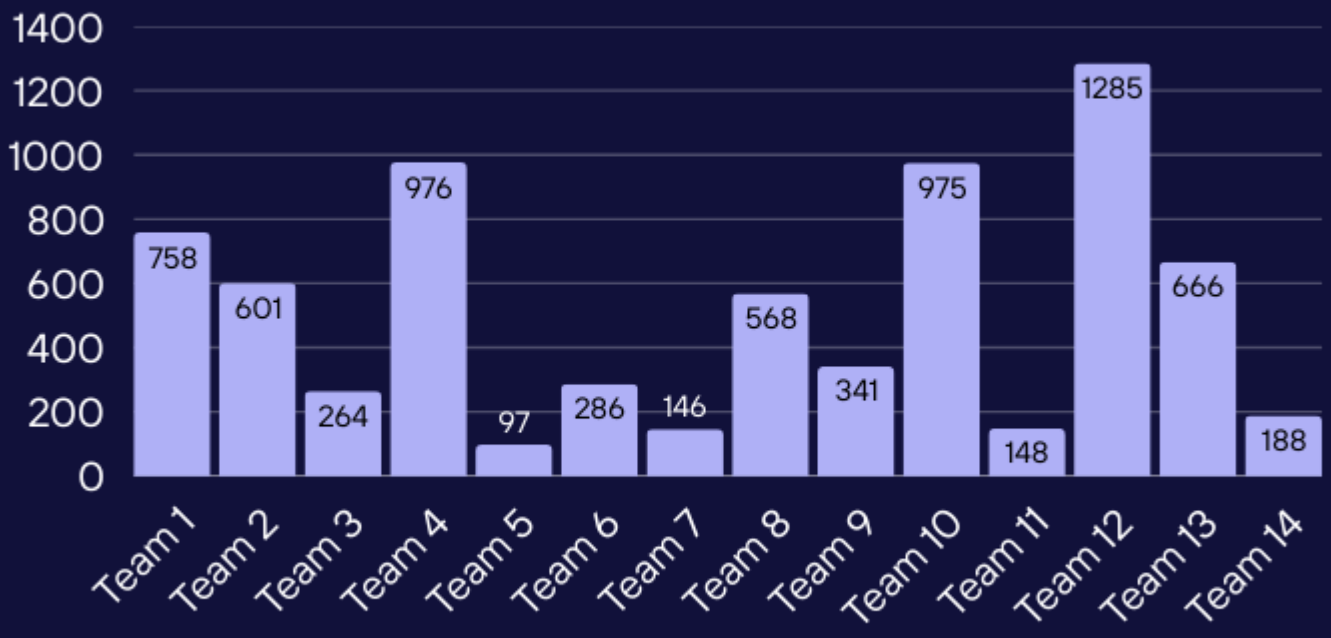
The Live Calls Phase

The live call phase at DEF CON marked the final test of each team's preparation. Teams had 22 minutes to make as many calls as they chose, strategically using pretexts to achieve their objectives. Points were awarded only with agreement from two of the three judges. Each objective had a different amount of times team could capture it, making them plan which objectives they would attempt for each call. Additional style points were available for creativity, such as costume changes, varied pretexts, background sounds, and completing the Crowd Picked objective.

Score Composition

#	Type	Description	Points Possible
1.	Objectives Captured	Each team is provided with a list of 28 objectives. Each objective's point value is different and has a capture limit from one up to four times.	1,600
2.	Style Points	There are a total of eight style point objectives that range from using background noise during calls to wardrobe changes.	400

Live Call Scores by Team

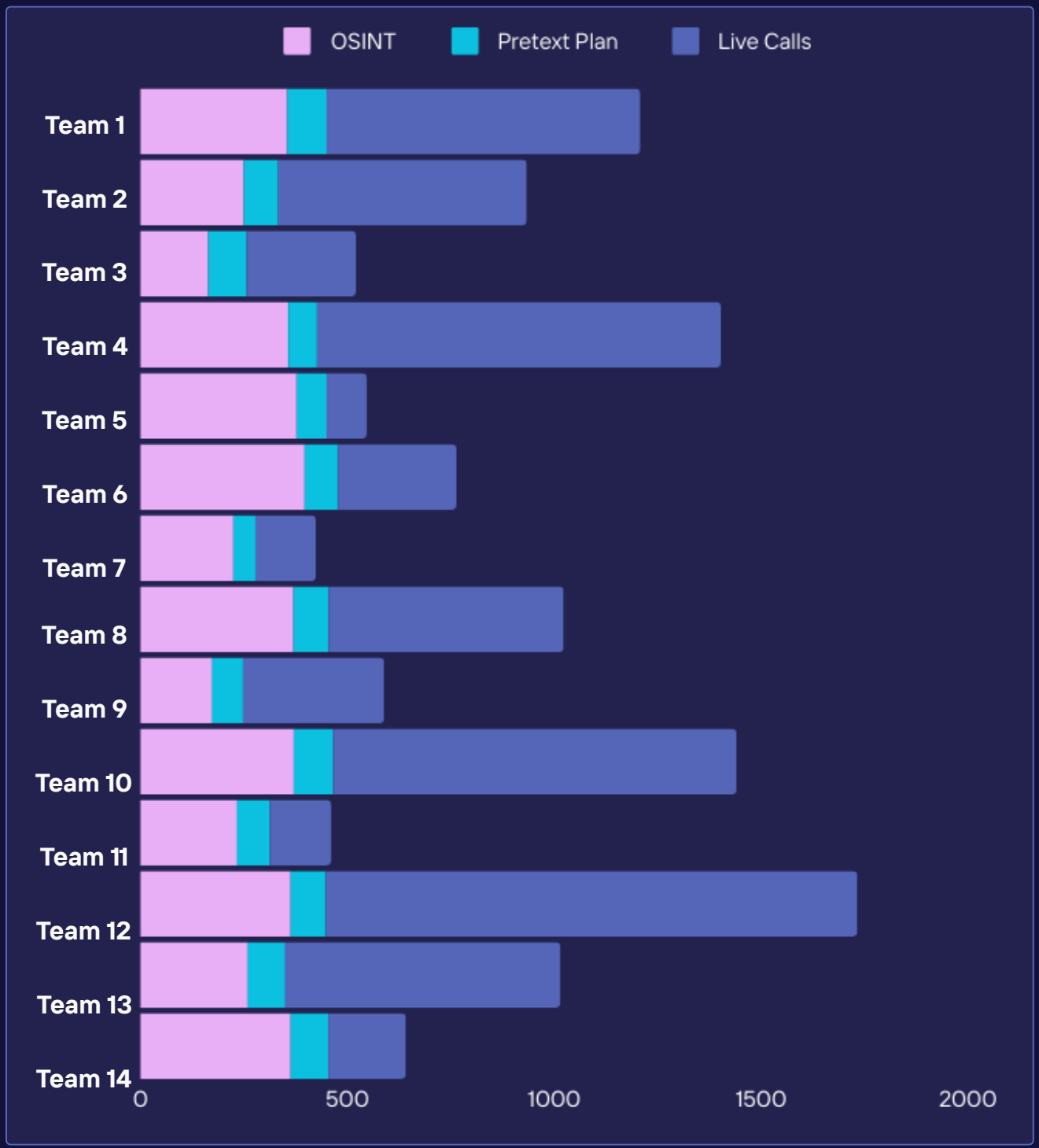


Total Score Summary

CONSOLIDATED TEAM SCORES

Total Score Breakdown

The following table shows how each phase contributed to the team's overall success.



OSINT Results and Analysis

Team Sara(h)^2 (2024)
Photo taken by: WiK's Pix

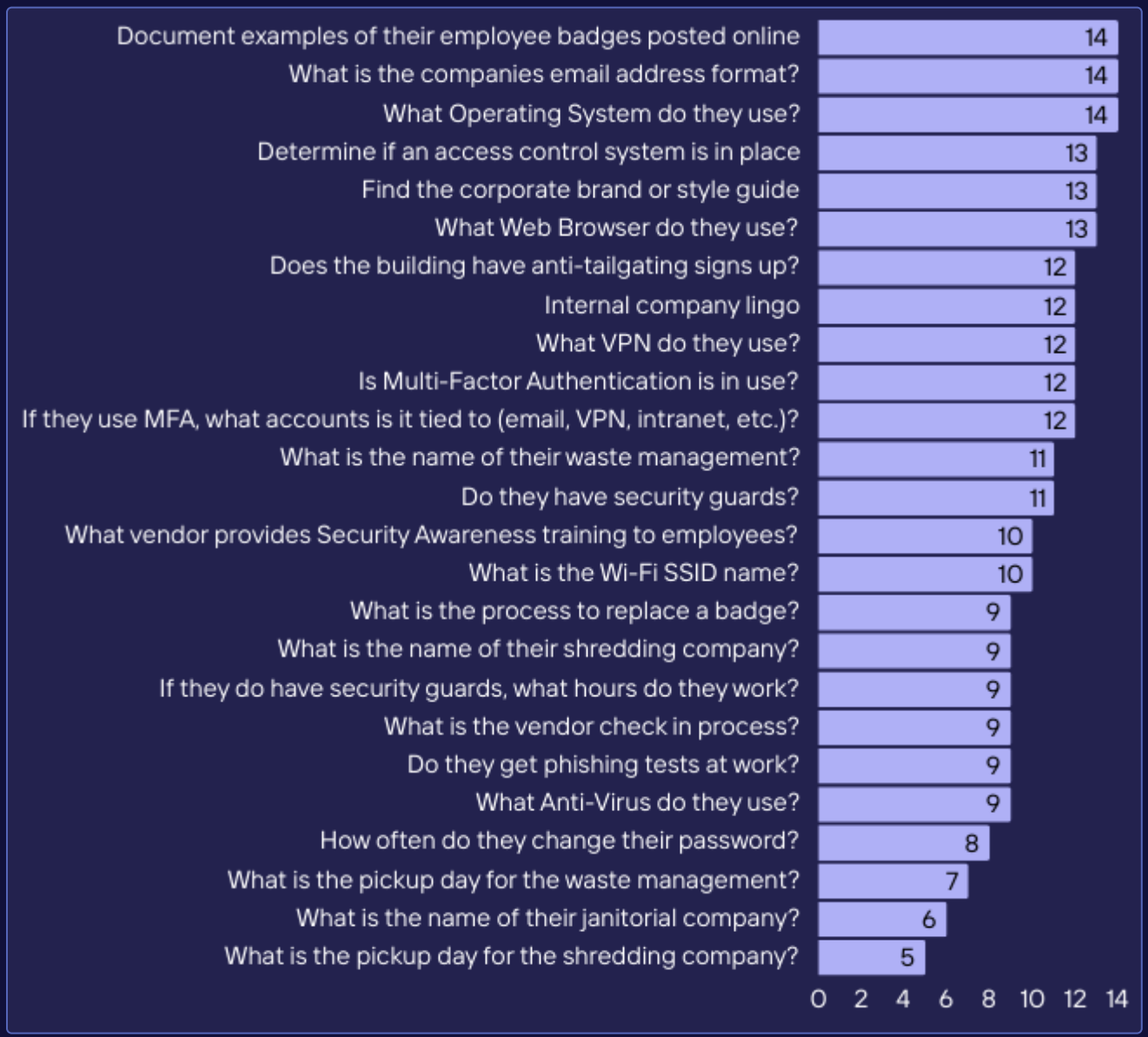
OSINT Objectives

OSINT OBJECTIVE CAPTURES

Capture Rates

During the OSINT phase, teams worked to identify specific objectives outlined by the SEC. The table below shows the objectives and the number of teams which captured them. All reconnaissance had to be passive and remote, with no contact allowed with the target location or its employees.

To earn points, teams had to document their findings and provide steps to replicate the discovery. At least two of the three judges had to validate each objective. This year, every single objective on the list was successfully identified by at least one team.



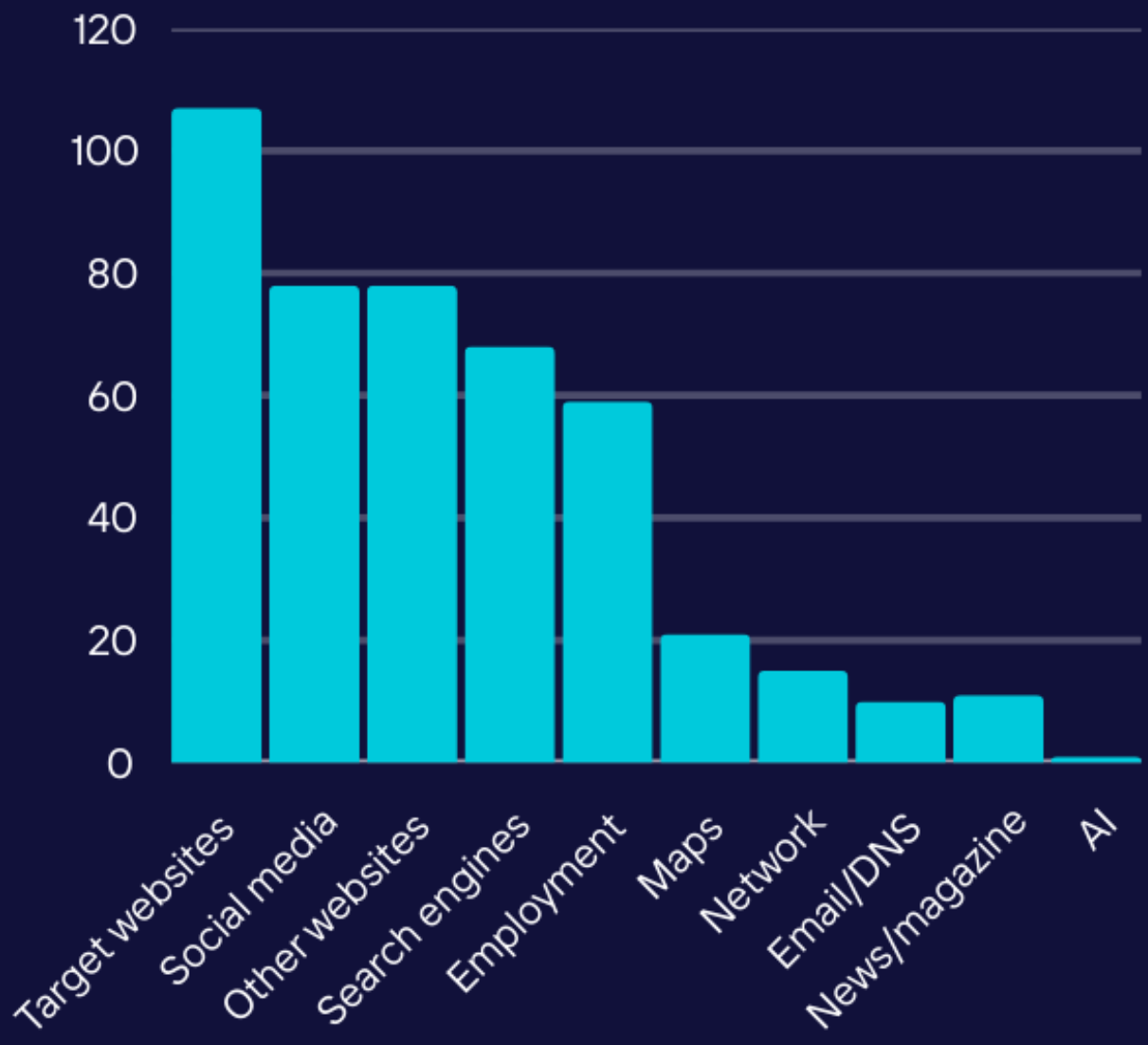
OSINT Sources

OVERALL SOURCE CATEGORIZATION

OSINT Source Data

The most frequently used resources during the OSINT phase were the target company's website, other websites, LinkedIn, YouTube, TikTok, and Instagram, as detailed in the following section. While teams often used resources multiple times, each resource was counted only once per team per objective for this report.

This report focuses on where evidence was ultimately found rather than the methods used to discover it. For instance, while Google Dorking may have been employed, only the platform where the final evidence was located (e.g., Instagram) was recorded. This approach highlights the locations of where information was discovered.



OSINT Sources

OVERALL SOURCE CATEGORIZATION

OSINT Source Data Breakdown

The tables below showcase specific websites or tools that were used under it's assigned category along with the count of how many times it was used to capture an objective during the OSINT phase.

MAPS	
Google Maps	16
Google Street View	4
Google Earth	1

EMPLOYMENT	
LinkedIn	47
Glassdoor	4
Indeed	3
Salary	2
ZipRecruiter	1
Dice	1
BuiltIn	1

WEBSITES	
Target Company Website	107
Other Company Website	78

SOCIAL MEDIA	
YouTube	25
TikTok	18
Instagram	14
X	8
Reddit	5
Facebook	4
Flickr	2
Vimeo	2

NETWORK	
Wigle	10
Pentest-tools.com	2
WhatIsMYIPAddress	1
Urlscan.io	1
Subdomain finder	1

SEARCH ENGINES	
Google	42
Google Dorking	20
Google Images	5
Bing	1

EMAIL/DNS	
RocketReach	5
MX Toolbox	2
LeadiQ	1
Elliot.org	1
HaveIBeenPwnd	1

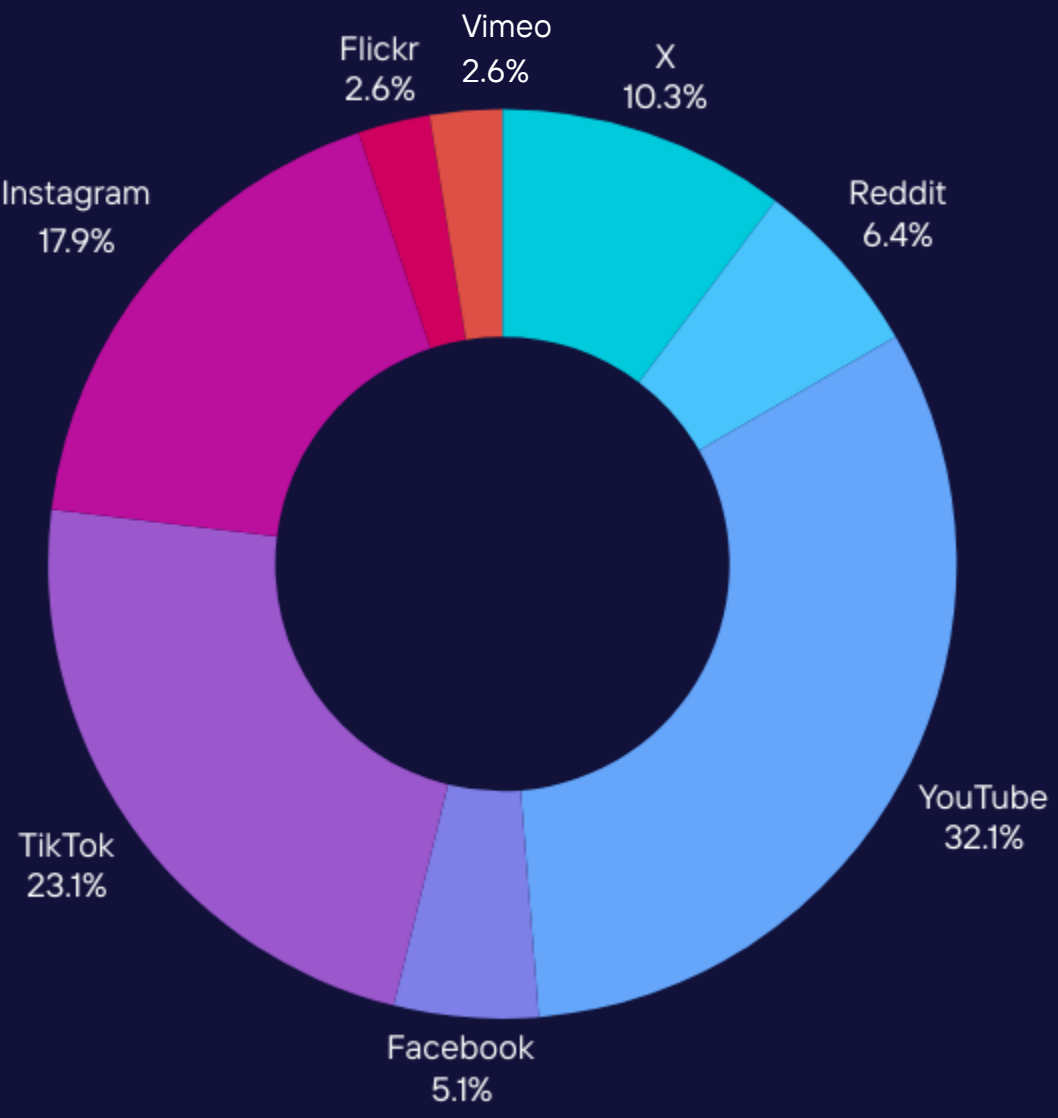
AI	
ChatGPT	1

OSINT Sources

SOCIAL MEDIA CATEGORY BREAKDOWN

Sources

The pie chart below visually represents the social media platforms that contributed most significantly to the identification of objectives.



151%

Increase from 2023

TikTok

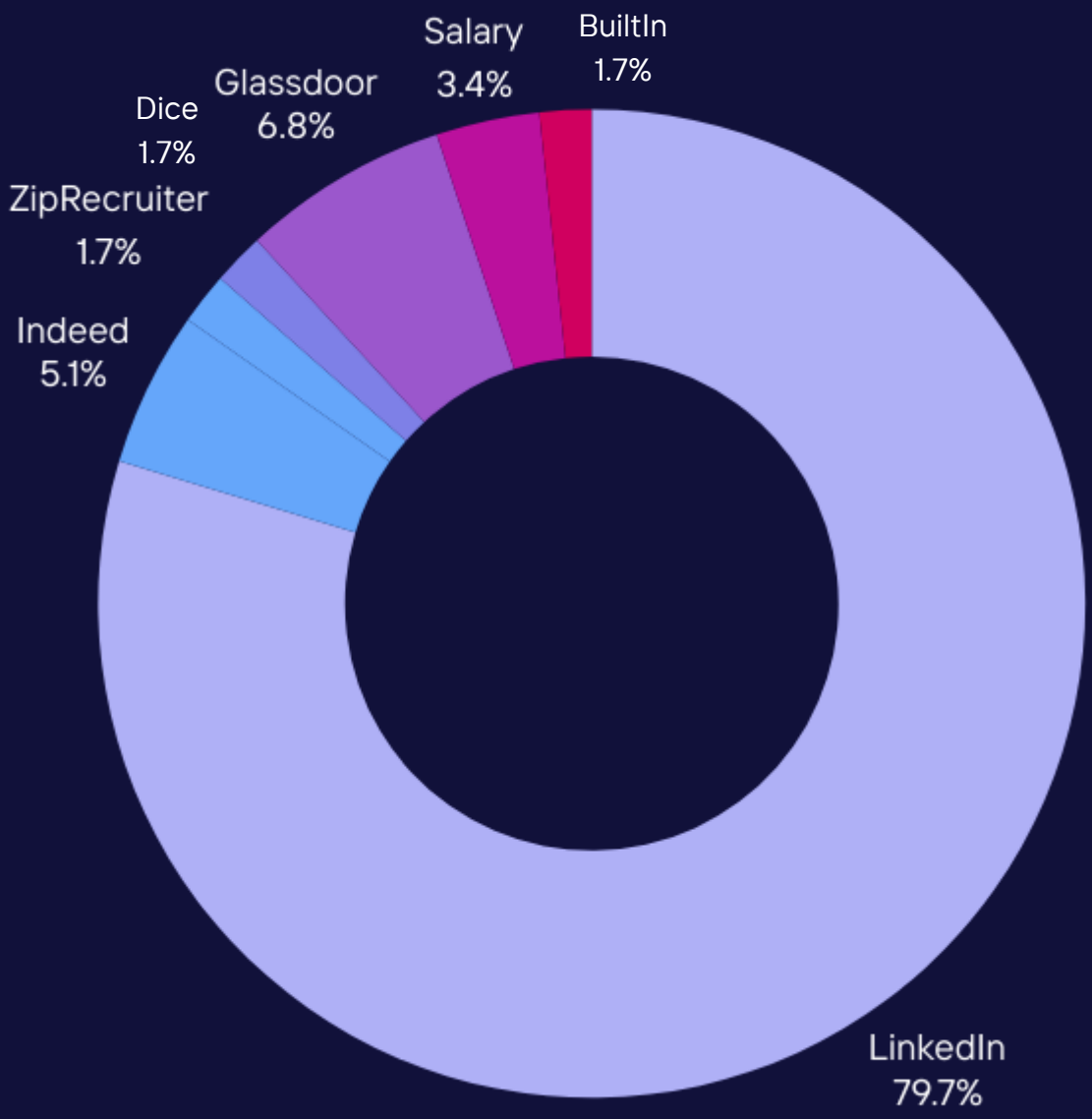
This year there was a huge increase in the use of TikTok, which lead to OSINT objectives identified.

OSINT Sources

EMPLOYMENT CATEGORY BREAKDOWN

Sources

The pie chart below visually represents the employment sources that contributed most significantly to the identification of objectives.



5

New Sources

New Employment Source

In 2023, we saw only two sources (LinkedIn and Indeed) were used by teams. However, in 2024 we saw five new sources utilized.

Vishing Results and Analysis

Team SkorpioMylk (2024)
Photo taken by: WiK's Pix

Judges

THE MINDS BEHIND THE SCORES

2024

Every year, two esteemed guest judges are invited to partner with Snow in the critical task of evaluating the competition. Their role involves dedicating countless hours to carefully reviewing all submitted reports and scoring of the live calls conducted during DEF CON.

John Hammond

Ibetika

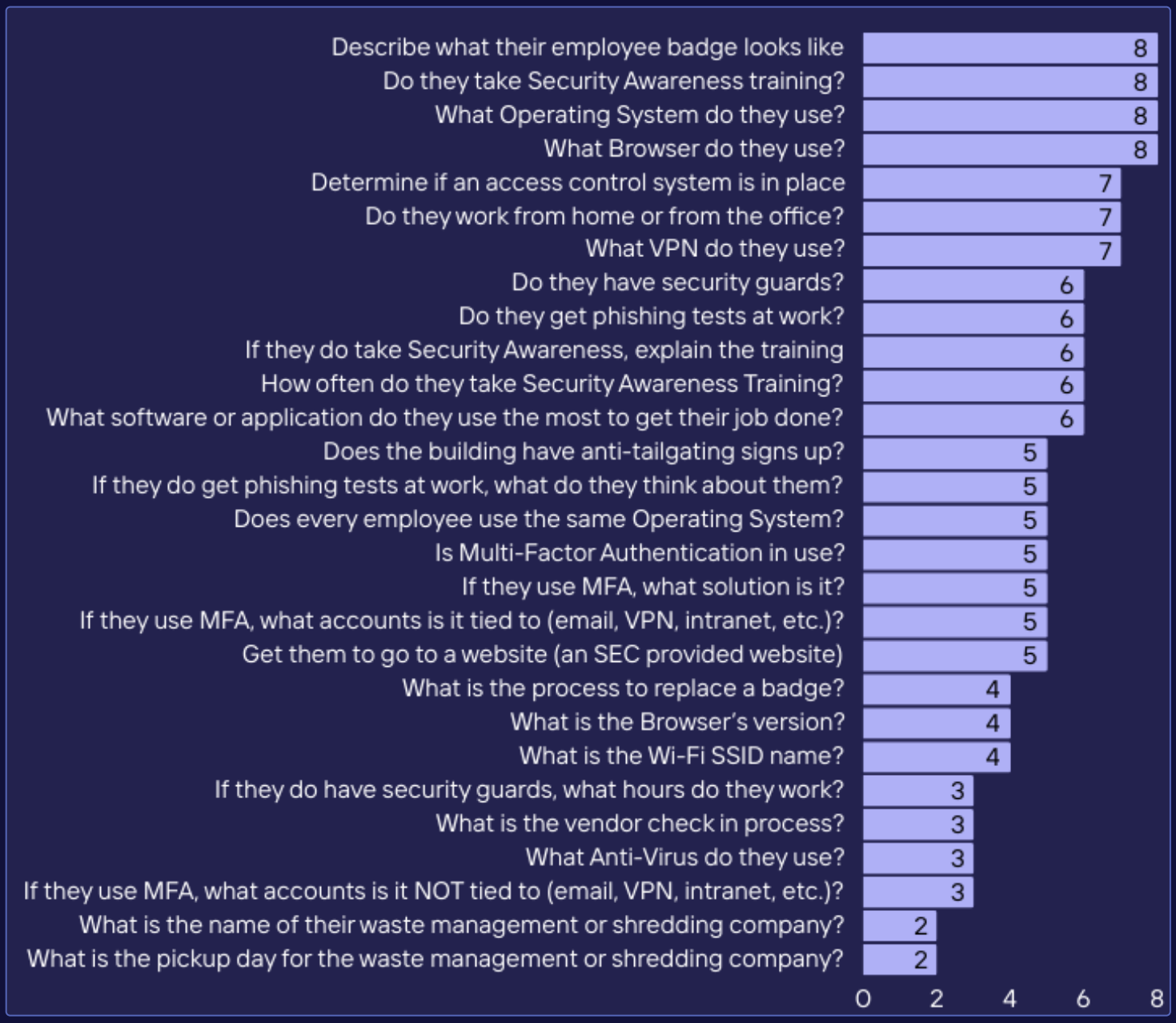
Snow

Vishing Results and Analysis

LIVE CALL OBJECTIVE CAPTURES

Capture Rates

The table below highlights two key aspects: "Objectives," which outlines the specific goals teams aimed to achieve during their calls, and the number of teams that successfully captured each one. Points were awarded only when at least two of the three judges confirmed the objective had been met, ensuring consistency and fairness in scoring.



Vishing Results and Analysis

PRETEXTS AND PERSONAS

Crafting Convincing Characters and Scenarios

In social engineering, pretexts and personas are essential tools used to build credibility and influence targets. Pretexts, or the scenarios and justifications crafted to engage with a target, ranged widely among competitors, with audits and corporate IT/help desk scenarios being the most frequently employed. Personas, or the roles assumed by competitors, often complemented these pretexts; the most popular personas included new or existing employees seeking assistance and IT/help desk staff conducting system checks. Together, these carefully chosen pretexts and personas allowed competitors to gain trust and achieve their objectives effectively.

Pretext	Usage Count
Audit	17
Corporate IT/Help Desk	15
(Cyber) Security	11
Marketing/promotion	7
New Customer Recruitment	6
New employee/intern onboarding	4
Employee Feedback	4
(Security) Training	3
Customer Support	2
Events	2
Partner Company Support	1
Delivery	1

Persona	Usage Count
(New) Employee	15
IT/Help Desk	14
Auditor	12
Customer	8
Marketers	5
General Public	5
Corporate vendor	4
Contractor	4
Student/Intern	3
Human Resources	3

Vishing Results and Analysis

PERSUASION TECHNIQUES

Breaking Down the Seven Core Methods

Persuasion techniques play a critical role in effective social engineering and utilizing them can make all the difference. In this section, we delve into techniques used by competitors, breaking down their definitions and metrics. There are several principles of persuasion, such as authority, commitment, consistency, reciprocity, likeness or commonality, scarcity, social proof, and a natural inclination to help[1, 2].

Persuasion Technique Definitions

Attackers who utilize **authority** as a principle of persuasion rely on the victim's willingness to comply with authorities, despite their own personal ethics.

Commitment is used to persuade victims by targeting their beliefs and commitments, and **consistency** relies on the fact that people act and behave in a manner consistent with their beliefs.

Reciprocity relies on the fact that people are likely to return favors when one is given to them.

Likeness or **commonality** is used when perceived similarities between the attacker and victim enhances the victim's compliance.

Scarcity persuades people through offering opportunities or objects that are seen as less available or highly valuable

Social proof exploits the tendency that people are more likely to comply with a request if others have already done the same.

Lastly, attackers can persuade their targets to help them execute their attack by posing as someone in need of assistance, as people have a **natural inclination to help** others who are in need.

[1] Cialdini, R. B. (2007). Influence: The psychology of persuasion (Vol. 55, p. 339). New York: Collins.

[2] Philpot, R., Liebst, L. S., Levine, M., Bernasco, W., & Lindegaard, M. R. (2020). Would I be helped? Cross-national CCTV footage shows that intervention is the norm in public conflicts. American Psychologist, 75(1), 66.

Vishing Results and Analysis

PERSUASION TECHNIQUES

Effective Strategies for Influencing Targets

The most frequently employed persuasion principle was authority, which aligns with the popularity of audit and corporate IT/helpdesk pretexts. Several teams used rapport building in their calls, which manifested as being polite, helpful, calm, friendly, appreciative, reassuring, using praise/flattery, affirmation, southern accents, slang/lingo, humor, and engaging in small talk.

Persuasion Technique	Usage Count
Authority	19
Natural inclination to help	13
Quid pro quo/reciprocity	13
Likeness/commonality	9
Commitment/consistency	5
Social proof	5
Scarcity/urgency	3

Supporting Technique	Usage Count
Building rapport/small talk	17
Polite/courteous	16
Reassuring	15
Friendly	12
Helpful	10
Humor/laughter	8
Praise/flattery/compliments	8
Appreciative	6
Accent/slang/lingo	4
Novice/nervous/acting dumb	3

Vishing Results and Analysis

PRETEXT, PERSUASION, AND PERSONAS... OH MY!

How Teams Put Them into Practice

Below we highlight examples from two standout teams that skillfully combined multiple techniques during their successful vishing calls. By analyzing their approaches, we gain insight into how these strategies were effectively applied to achieve their objectives.

Team 12 had one of the most successful calls, which utilized a pretext centered around an Olympics-themed quiz from the new hire experience team. The team utilized numerous OSINT findings on an individual (who had left the organization and just came back to work there again) then used that information to build rapport in the first 30 seconds because the target believed everything they said. Throughout the call they demonstrated operant conditioning ("you're doing great; still in gold zone here; you killed it") and urgency (they had an opportunity to be entered intro a drawing which then might have a chance to win the swag bag only if they answered questions quickly). The potential to win a swag bag reward for answering questions also utilized the principle of reciprocity, which was also used throughout the call (e.g., the competitor telling the caller, "I'll give you credit for it," when they weren't confident about their answer).

Team 9 posed as a nervous new hire. They made themselves seem credible by using lingo that matched the persona of a young employee new to the corporate world. They purposefully used filler words ("like") and slang such as "lowkey" to fit the expectations of how Generation Z speaks. The same team demonstrated the art of 'flexibility' in another authority-based pretext. The target was busy and out walking their dog, and so the team built rapport by saying they liked dogs (commonality/likeness) and would allow the target to continue their task while answering the objective questions.

Vishing Results and Analysis

ADJUSTING STRATEGIES FOR MAXIMUM IMPACT

How Teams Evolved to Overcome Challenges

Throughout the live calls, competitors used an assortment of techniques to adapt and persist in their objectives. Some techniques used are listed below.

Adaptation	
Assisting Targets with Difficulties	Competitors helped targets by explaining processes, such as MFA, to gain trust and extract information.
Providing Expected Answers	Suggested likely answers to jog targets' memory, building credibility and prompting confirmation.
Clarifying Identity/Pretext	Used OSINT details or reinforced pretexts with persuasive techniques to build trust and reduce suspicion.
Maximizing Downtime	Asked additional questions during lulls, like while targets booted devices, to save time and extract more information.
Persistence	Continued questioning despite hesitation, supervisor referrals, or targets being too busy.
Avoiding Call Transfers	Avoided losing rapport by declining transfers, reinforcing urgency, or convincing targets they were the right person to help.

Team Dynamics and Social Engineering Performance

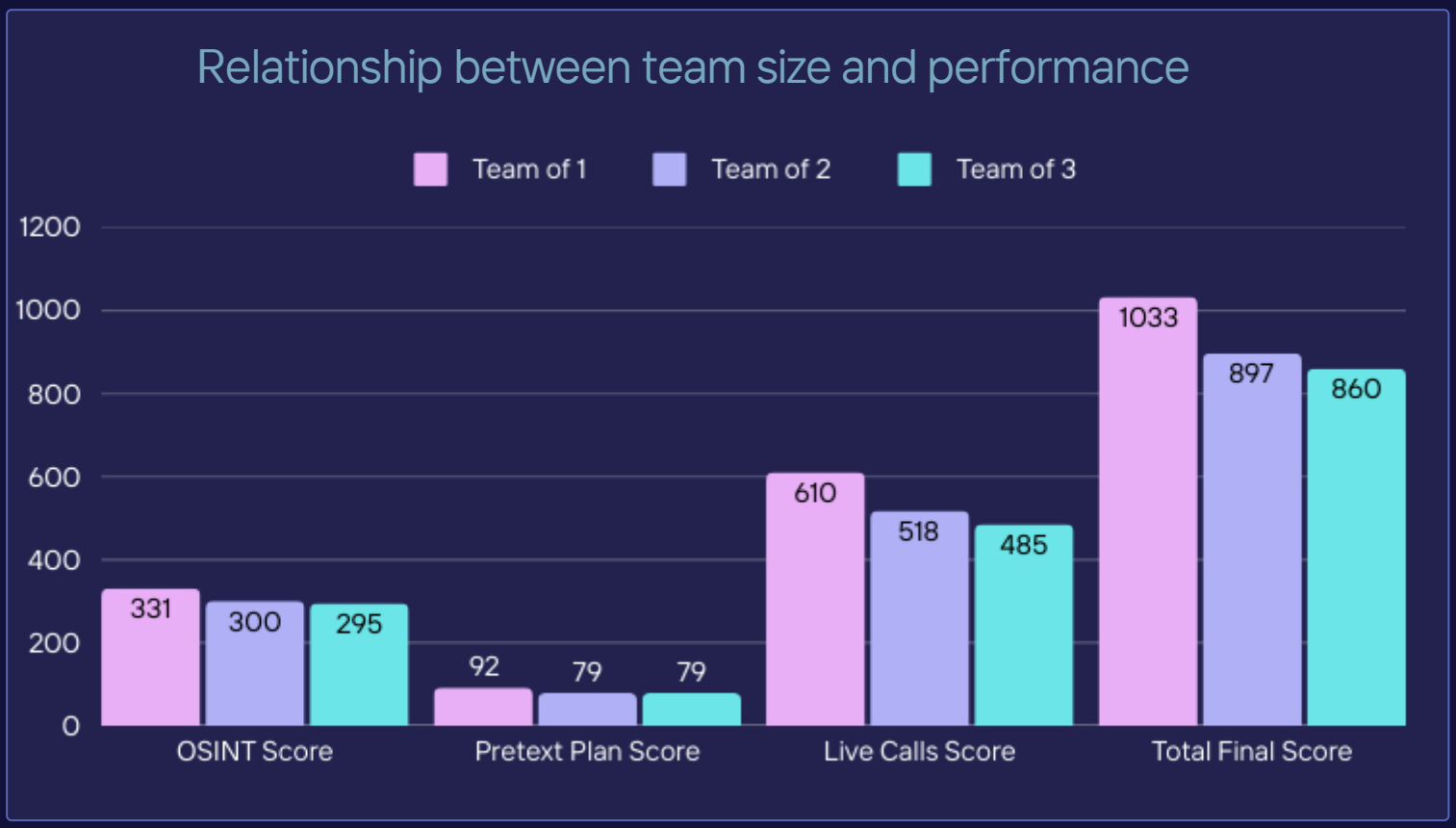
Team Scotzipan (2024)
Photo taken by: WiK's Pix

Team Dynamics & Performance

IMPACT OF TEAM SIZE ON OUTCOMES

Relationship between team size and performance

According to the literature on group dynamics and performance[3], many factors come together to determine the success and efficacy of a social engineering engagement: team size and cohesion, skill experience, disciplinary background, research and preparation, and adaptation ability. This report attempts to address these factors but reminds the reader to cautiously interpret these findings given that 14 teams competed and as such the findings are not intended to be generalizable.



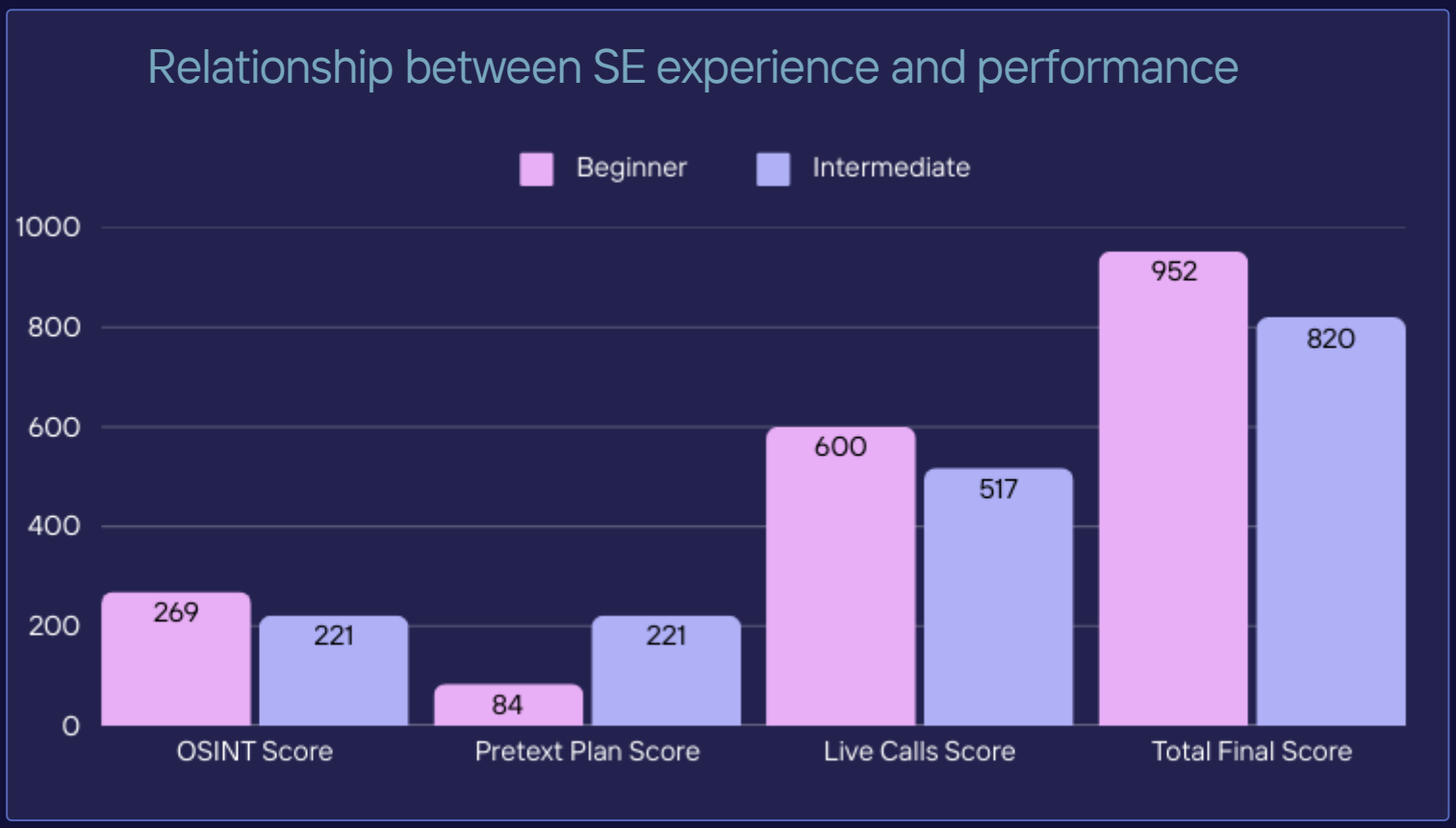
[3] Forsyth, D. R. (2014). Group dynamics. Wadsworth Cengage Learning.

Team Dynamics & Performance

HOW EXPERIENCE LEVELS INFLUENCED SUCCESS

Relationship between SE experience and performance

This section examines the connection between competitors' self-assessed social engineering experience levels, categorized as beginner, intermediate, and advanced. Interestingly, no participants identified as advanced. Notably, beginners excelled across all phases except the pretext plan phase, where we observed that a background skill set likely played a key role in report writing and the ability to effectively select and develop pretexts.

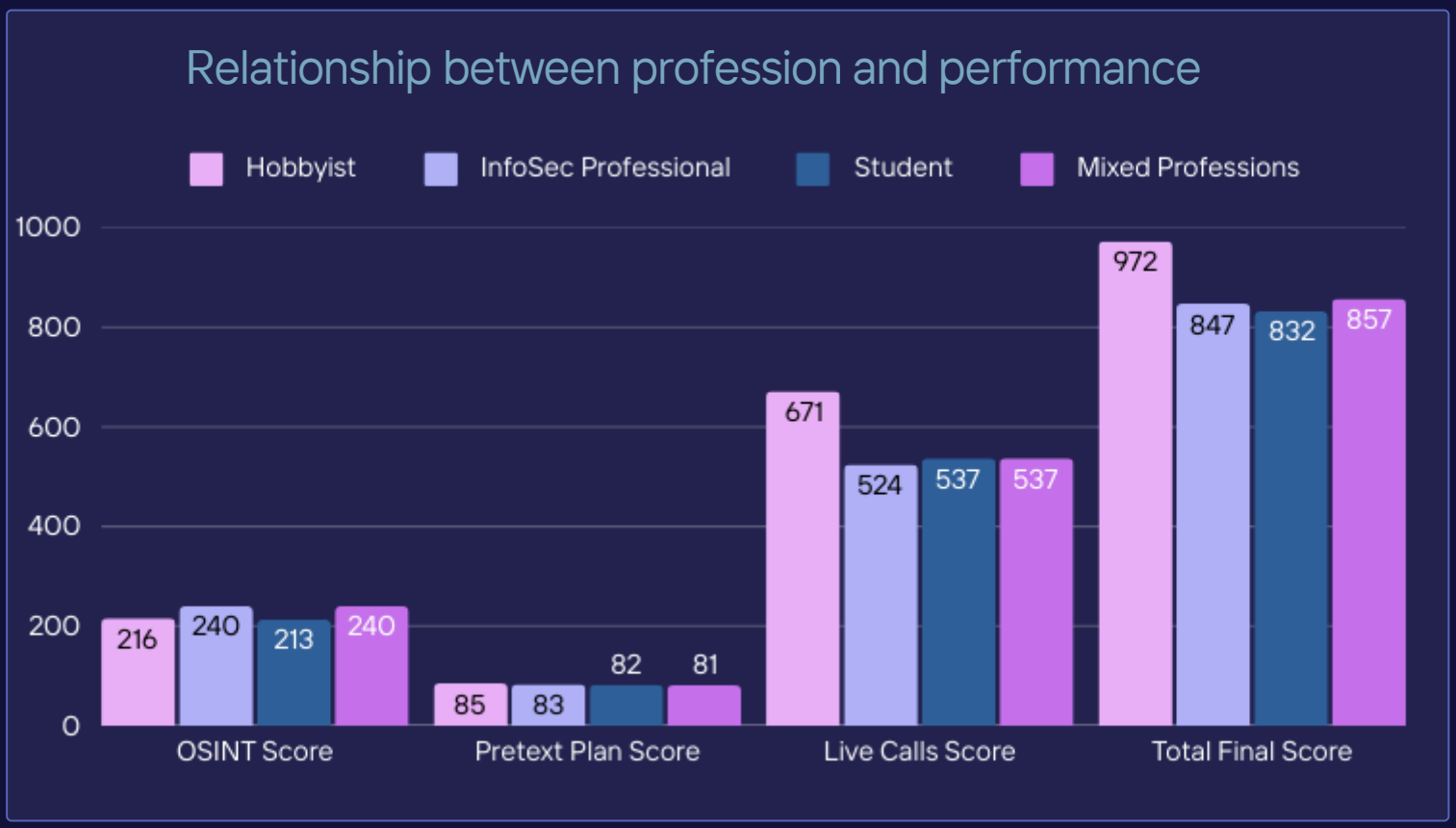


Team Dynamics & Performance

HOW BACKGROUNDS SHAPED RESULTS

Relationship between profession and performance

For teams with more than one member, establishing a connection to performance becomes tricky. For instance, a team of 2 members selected five professions (Student, Hobbyist, InfoSec Professional, Sales, Marketing) making it impossible to determine which of these professions contributed to their experience and in what capacity. Where there was a 1:1 mapping between size and number of professions, it was also difficult to determine which profession contributed more and/or had greater influence in the team's strategy. For instance, one 2-person team was a mix of Hobbyist and Infosec Professional, but we cannot determine member role, division of labor, effort, contribution, etc. Despite this limitation, comparisons can still be made between solo teams that were composed of Hobbyists, Infosec Professionals, and Students. For the most part, all professions had a similar performance for OSINT and Vish plans/pretext development. However, during the Live Vish, the hobbyist did better, which resulted in an overall higher score. We are cautious with this analysis as there was only 1 solo team identify as a hobbyist and 1 solo team identify as student. More data points would be needed to identify any patterns or relationships between profession and performance.



Summary of Vishing Threat Landscape

Team Hall & OSINT (2024)
Photo taken by: WiK's Pix

Vishing Threat Landscape

2024

Emerging Trends and Evolving Risks

The SECVC highlighted the critical role of social engineering, particularly OSINT and vishing, in the 2024 competition. While company websites revealed expected information, platforms like LinkedIn, YouTube, TikTok, and Instagram provided a wealth of data, including access control measures, employee badges, internal lingo, operating systems, VPNs, and MFA setups. This information could easily be exploited for phishing, impersonation, and network access. Many targets, despite phishing training, fell for vishing attempts and escalated calls to supervisors when unable to provide answers, often sharing private numbers. This escalation is especially dangerous, as it sets up another employee for potential failure while also increasing the adversary's access to information.

An interesting observation during the competition was that many targets readily divulged information but became hesitant or suspicious when asked to take specific actions, such as visiting a URL. Adversaries often take advantage of employees experiencing burnout, distraction, or stress, making them more susceptible to social engineering attacks[4]. These risks are further exacerbated in remote work environments, emphasizing the need for holistic training that addresses OSINT, phishing, and vishing collectively. Additionally, while companies encourage social media use to promote corporate culture, this practice can inadvertently aid adversaries conducting OSINT, as employees unknowingly share exploitable details.

This year also demonstrated the rising impact of AI in social engineering. OSINT reports revealed that tools like ChatGPT were used to uncover details, such as password change frequencies. Moreover, the SEC's inaugural John Henry: AI vs. Human competition underscored AI's effectiveness in deceiving human targets. As technologies like ChatGPT, deepfakes, and voice cloning advance, companies must adapt their training and awareness programs to counter these threats. Security measures should be designed with the assumption that internal knowledge may already be public, ensuring organizations remain proactive against evolving risks.

[4] Hancock, J. (2022). Understand The Mistakes That Compromise Your Company's Cybersecurity.

Research Sponsor

POWERING OUR RESEARCH TEAM... AND THIS REPORT!

We are proud to announce that Microsoft Threat Intelligence sponsored the Social Engineering Community (SEC) as the first ever Research Sponsor. Their generous support enables us to foster a collaborative environment where security professionals and enthusiasts can come together to share knowledge and drive innovation. We are grateful for their partnership and the valuable resources they bring to our community. Learn more about our sponsor and gain more threat intelligence guidance and insights from Microsoft security experts by visiting Security Insider at https://www.microsoft.com/en-us/security/security-insider.

Sponsors

THANK YOU FOR HELPING MAKE THE VILLAGE HAPPEN!

Platinum Sponsors

Gold Sponsor

Booth Sponsor

Authors

DR. AUNSHUL REGE

Full Professor and Director of CARE Lab

Dr. Aunshul Rege is an Associate Professor in the Department of Criminal Justice and Director of the Cybersecurity in Application, Research, and Education (CARE) Lab at Temple. Her research has been funded by several National Science Foundation (NSF CAREER, NSF EAGER, NSF CPS, NSF SaTC EDU) and Department of Energy/Idaho National Lab grants. Her work focuses on critical infrastructure and cybersecurity, cyberadversarial decision-making and adaptation, ransomware, social engineering, and cybersecurity education. She is the organizer and host of the summer social engineering competitions for high school, undergraduate, and graduate students. Her cybersecurity awareness and training efforts extend beyond higher education to include working with youth, elderly, and previously incarcerated individuals via partnerships with local nonprofits.

Dr. Rege has a B.Sc.(2002) in Computer Science from the University of British Columbia and worked for two years as a software engineer. She also holds a B.A. (hons.) (2006) and M.A. (2008) in Criminology from Saint Mary's University in Halifax, Nova Scotia. She completed her M.A. (2010) and Ph.D. (2012) in Criminal Justice from the Rutgers School of Criminal Justice. She has been featured on BBC World Service, WHYY/ PBS/NPR's Studio 2, the David Bombal's show, Technical.ly, and the BBC/CBC Podcast "Love, Janessa", and her work has been recognized in Security News, Dark Reading, and AARP to name a few. She currently serves as the Research Lead for the Social Engineering Community at Defcon. She also serves on the Advisory Board of Raices Cyber and Black Girls Hack.

Authors

RACHEL BLEIMAN

PhD Candidate and Graduate Research Assistant

Rachel Bleiman is a Ph.D. candidate in the Department of Criminal Justice at Temple University, where she previously received her B.A. (2020) and M.A. (2022) in Criminal Justice. She is an NSF graduate research assistant and a member of the Cybersecurity in Application, Research, and Education (CARE) LAB. As a research assistant, Rachel maintains a critical infrastructure ransomware dataset, assists in organizing social engineering competitions and awareness programs, and hosts the CARE Pod.

Rachel's research areas of interest include cybercrime, mis/disinformation, AI and deepfakes, online privacy, ransomware, and social engineering. She is currently working on her doctoral dissertation examining the human decision-making process of deepfake detection.

Authors

JC Carruthers

Social Engineering Community Co-founder

JC Carruthers is a U.S. Marine Corps veteran and President at Snowfensive. With over two decades of experience in IT and cybersecurity, JC has a wide range of skill that include digital forensics and incident response, offensive security, and he enjoys focusing on providing value to his clients. JC is the co-founder of the Social Engineering Community, a DEF CON village, as well as an annual trainer at Black Hat US. When JC isn't hacking the planet, he's probably watching 80's movies with his family, hanging out with his birds, or learning a new hobby he'll use only once.

Stephanie (Snow) Carruthers

Social Engineering Community Co-founder

Stephanie "Snow" Carruthers, Chief People Hacker and Global Lead of Cyber Ranges on IBM's X-Force team. She is a seasoned presenter and trainer at global security events since 2014, a black badge winner at DEF CON and SAINTCON, co-founder of the SE Community, and a mentor passionate about guiding aspiring social engineers—all while traveling the world to meet fascinating people, like Larry, who just let her into your data center.

Closing Thoughts

Time to Say Goodbye ...

Success like this doesn't happen without the hard work and dedication of an entire community. Kudos to our incredible volunteers, sponsors, competitors, and DEF CON for making this year's village a true standout event. Creativity was on full display, with the John Henry competition showcasing how human ingenuity and AI innovation can push the boundaries of social engineering. Unforgettable moments filled the event, from jaw-dropping vishing performances to insightful discussions in the hallways. Support from every corner of the community continues to help transform this event from an idea into an unforgettable experience. Seeing the enthusiasm and talent here reminds us why this village continues to thrive and grow year after year. Innovation is the heartbeat of what we do, and this year set a new bar for creativity and experimentation in our field. Reflecting on this event, we are inspired by the passion and commitment of everyone involved. Here's to 2025—another year to learn, compete, and celebrate what makes this community great.

Can't wait to see you all there,
JC & Snow

SOCIAL ENGINEERING COMMUNITY

*** END OF REPORT ***