ISSN: 2473-4901
v11 n6402

# From Classroom to Crisis: Implementing a Collegiate Incident Response Competition for Undergraduate Students to gauge impact of Cybersecurity Education

Brandon Brown
bbrown118@coastline.edu

Tobi West
twest20@coastline.edu

Andrea Barrios
abarrios16@cccd.edu

Department of Computer & Cyber Sciences
Coastline College
Fountain Valley, CA

Joe Needleman
joe.needleman@wrccdc.org

Michael Glass
michael.glass@wrccdc.org

The Western Regional Collegiate Cyber Defense Competition
Operations Team

## Abstract

Training cybersecurity staff for the eventual breach of network and systems is crucial as it enables them to minimize the impact of these detrimental occurrences. As the cybersecurity landscape evolves, preparing undergraduate students for real-world incident response (IR) has posed challenges for instructors and institutions. This collective effort of academic and industry professionals introduces the Collegiate Incident Response Competition for Undergraduate Students (CIRCUS). This competition-based learning environment is designed to assess the skills gained in the classroom of students in both two-year and four-year institutions. The competition is a practical hands-on environment that helps gauge student learning outcomes in core areas of IR to include evidence handling, digital forensics, procedural response, analytical reporting, and professional communication.

Results show that there is a broad disparity between theory and practice without the culmination of capstone projects, and theory learned in the classroom does not always translate to understanding of practical application.

**Keywords:** cybersecurity, incident response, assessment, cyber competitions, digital forensics.

# From Classroom to Crisis: Implementing a Collegiate Incident Response Competition for Undergraduate Students to gauge impact of Cybersecurity Education

*Brandon Brown, Tobi West, Andrea Barrios, Joe Needleman, and Michael Glass*

## 1. INTRODUCTION

The focus of this paper is to provide a case for the establishment of a national cybersecurity competition that is focused on incident response for the purpose of providing two-year- and four-year education programs the vehicle to help assess their students' learning outcomes and assist with curriculum modification and enhancement. There are several precedents to the creation of such initiatives. One only needs to look at the National Cyber League, National Collegiate Cyber Defense Competition, National Centers of Academic Excellence Cyber Games, and the Global Collegiate Penetration Testing Competition (CPTC) as examples (O'Connor et. al, 2023). These core competitions set up the environments to gauge skills against established criteria such as the National Initiative on Cybersecurity Education (NICE), the Centers of Academic Excellence (CAE) knowledge units, and the Department of Defense's Cyber Workforce Framework (DCWF).

As outlined in Conklin (2005), "When we embark on the journey to develop and deploy a cyber competition, the focus is on providing a learning experience". This holds true today as it has over the past two decades since the inception of cybersecurity competitions. Over these years, we have seen the rise of several global, national, regional, and local cyber competitions where we now must compete for scheduled spots on the academic calendar. Given that competitions range from the broad range of topics such as NCL, to the specific tools and training of a single profession such as CPTC, it is hard to select and fine tune any one class to prepare students for these competitions, and their skill set requirements.

In addition to these competitions, other than CPTC, none targets any specific cybersecurity profession. Given that CPTC focuses on offensive security skill sets, there is not a competition that drives incident response and digital forensics as a core competency at a national level. Only in recent years has one come out of Baylor University in 2024 entitled the Cybersecurity Interdisciplinary Incident Response Competition (CIIRC). Given the rules, and most recent team packet of CIIRC, this competition focuses on a "real-time" response (CIIRC Team Packet, 2024).

A recent report by IBM had a key finding that on average it took organizations over 204 days to identify a breach, 73 days to contain it, and that 98% required outside assistance (IBM, 2025). Furthermore, the level adversarial use of Artificial Intelligence (AI) in breaches is on the rise and the same report showed that it had increased. (Bonnie E., 2025). Given these statistics and many others that have shown the continuing trend of complexity and occurrence, it is the question and purpose of this case to explore an alternative competition that focuses on incident response and digital forensics. The exploration of the question "Can a competition provide ways to explore impacts of classroom training and skill attainment in a DFIR competition where a more robust and stylized competition is necessary to meet the needs of firms that are overwhelmed in the market? This is a complex question that requires a robust answer that only a case study can initially provide. This competition will show that it provides market ready workers with the skills to immediately impact the workforce. Enter the CIRCUS!

## 2. A BRIEF HISTORY OF CYBER COMPETITIONS

Previous works have explored and reviewed the qualities, advantages, and challenges of the many different collegiate cyber competitions. These include Cheung et. al 2012.; Katsantonis et. al, 2017; Woszczynski and Green, 2017; Balon and Baggili, 2023; O'Connor et. al, 2023; and Anand et. al, 2023. The premises of these are rooted in the analysis of how competitions help student outcomes and touch upon the methods observed in the competitions to quantify and measure outcomes. However, they do not go into any specific area of incident response outcomes as there is no recent competition to gauge these skills.

For many years educators have used methods inside and outside of the classroom to facilitate learning cyber skills. This is outlined in detail

within Anand et. al (2023) as well as O'Connor et. al (2023). As far back as Manson and Carlin (2011) Whitman and Mattord (2008), Conklin (2006), and White and Williams (2005), the core concept was to measure skills. These came in many forms but most often tried to align with established standards of their time. The National Centers of Academic Excellence in Cybersecurity (NCAE) established in 1998 by the National Security Agency (NSA) and later joined by the Department of Homeland Security (DHC) in 2004, established different areas to facilitate the education of future cybersecurity professionals through collaboration with academic institutions.

According to their website (National Security Agency, 2014) "The purpose of the National CAE designation program is to promote higher education in IA and CD and prepare a growing number of IA/CD professionals to meet the need to reduce vulnerabilities in the Nation's networks. The initial National CAE in IA Education (CAE/IAE) program was started by NSA in 1998, with DHS joining as a partner in 2004 in response to the President's National Strategy to Secure Cyberspace. The CAE in IA Research (CAE-R) program was added in 2008 to encourage universities and students to pursue higher-level doctoral research in Cybersecurity. In 2010, the CAE in Two-Year IA Education (CAE2Y) program was established to afford two-year institutions, technical schools, and government training centers that are also teaching IA curricula, the opportunity to receive such designation". The CAE program has been the leader in curriculum and therefore the establishment for the identification of skills critical to this workforce.

Additional work over the years has validated the knowledge units, curricular, and workforce needs in cybersecurity. These include Etezady and Wang (2025) and Murphy (2018). Furthermore, the works of Oliver and Elwell (2018), Bain and Mello-Stark (2019) and Grier (2019) cover the mapping of Knowledge Units (KUs) to some of these skills. However, many of these works do not directly address Incident Response and Digital Forensics as they pertain to direct workforce skills used by forensic investigators and first responders.

These works provide the foundation for the need and opportunity to develop a cybersecurity competition that aims to provide CAE and similar programs at two and four-year institutions to leverage in gauging their programs' effectiveness for providing validation of student learning outcomes in a non-biased, best-practices framework that aligns with industry and governmental standards.

## 3. MODERN INCIDENT RESPONSE METHODOLOGY

The way that businesses, government organizations, and law enforcement approach IR depends on how the professionals are trained. In addition to this training, these groups follow the concept of continual improvement to incorporate new approaches, technologies and tactics into their practice.

These approaches and practices can best be outlined as frameworks. The three most common are from the National Institute of Standards and Technology (NIST) via their Special Publication 800-61 currently in its third revision (National Institute of Standards and Technology, 2024), the International Standards Organization / International Electrotechnical Commission (ISO/IEC) Incident Management guideline (International Organization for Standardization, 2018), and the Sysadmin, Audit, Network and Security (SANS) IR framework (SANS Institute, n.d.). Additionally, these frameworks provide guidance and practical structured processes for identifying, managing, and mitigating the effects of cybersecurity incidents to minimize damage, recover operations, and prevent future occurrences. They serve as a critical component of an organization's cybersecurity strategy, enabling a swift and efficient response to breaches, malware attacks, data theft, and other threats. Incident response involves coordinated efforts from specialized teams and the use of frameworks, tools, and processes designed to address security events effectively.

This guidance forms a core for the development of methodologies in addressing an incident. Law enforcement agencies, such as the FBI Cyber Division or Europol's EC3, tailor methodologies for evidence handling and legal admissibility. These include the focus areas for preservation of evidence, attribution of attacks, and help to collaborate with internet service providers (ISPs), computer emergency response teams (CERTs), and domestic and potentially international partners. A great example of this would be the FBI's Cyber Incident Reporting Guide which outlines how an organization would collect logs, preserve evidence in the form of disk images, and document activities prior to turnover of evidence to appropriate authorities.

## 4. INTRODUCTION TO CIRCUS

CIRCUS is an incident response competition where teams of up to six students are "contracted" to provide IR services to a fictitious business which has been compromised. This compromise is detected by the "customer" who seeks out professional assistance for recovery operations as well as initial investigative services. The students are tasked with acquiring the images, securing them, tracking their custody, examining them for evidence, and writing a report outlining to the best of their ability the sequence of events, any suspicious activity, loss of data, and kill chain evidence pertaining to system compromise.

Through CIRCUS, students can troubleshoot and practice their incident response skills in a "post-breach activity" scenario. Many other competitions focus on "active attack response" scenarios where organizations are currently under attack. However, according to a recent survey by Positive Technologies, about 60% of incidents were detected to be ongoing and not a part of an advanced persistent threat (APT) activity (Positive Technologies, 2023). Given this metric many of these breaches are therefore subject to prosecution by local, state, or federal law enforcement.

CIRCUS is comprised of two phases that are compressed timelines in the Incident Response cycle. Teams are assumed to have prepared for the engagement, and the identification and containment is already well underway. Their responsibility is to identify remaining threats, preserve evidence, propose recovery options and provide lessons learned and expert testimony for the second and final phase. In this phase, the teams provide mock testimony in a "simulated" deposition with either company counsel, law enforcement, or city, county, state, or federal departments of justice officials. Each different competition has the levity to change the scenario, and teams need to adapt to any situation.

## 5. CIRCUS & TEACHING TECHNICAL SKILLS

For many years, cybersecurity competitions have been the ideal proving ground for learning and reinforcing students' technical skills. Many students learn vast amounts of knowledge and technical acumen through the application of techniques they have accumulated in the classroom in a hands-on way and troubleshooting when coming across challenges. CIRCUS is one more competition that allows for this methodology. It focuses on theory and application of techniques in the Incident Response profession of cybersecurity by providing a holistic methodology to assess a student's skills. This is done by providing a true test of whether a student understands technical concepts as applied to IR frameworks. It also gauges their skills in working in teams, presenting findings in a professional manner.

Through competing in CIRCUS, students can apply concepts such as evidence acquisition and disk drive imaging. Even though this competition is initially virtual and systems are virtual (i.e., virtualized hard disks), there is still evidence of handling methods that need to be adhered to. Additionally, once the file system is accessed, its analysis and the cataloging of artifacts is essential for the evidence gathering process. The virtual machines also provide for the ability to examine static memory as frozen at the time of machine stoppage. This allows memory forensics to be performed.

Once the artifacts and evidence are cataloged, teams must provide an analysis of these and develop a forensics / IR report. This report falls more into the next section of providing professional skills, but it serves as a bridge between the two. The report is both technical and non-technical at the same time. Many of the artifacts located are then categorized and provided in appendices. Explanation of the attack timeline and technical detail of how the attack occurred require deep technical knowledge. This culminates in technical writing skills that are highly sought in this industry.

Students also need to provide a comprehensive list of forensic and IR tools that they leveraged during the analysis phase. These are grounds for the finalists to be queried during the deposition phase. All tools used by the competitors must be open-source or have been used during a "trial period" that aligns with the competition timeline. This is a key rule explained to the competitors and detailed in the official CIRCUS rules.

A common situation competitors come across is finding that the systems have a lot of "noise" left from the GHOSTS and CRUCIBLE applications. This is present to provide a distraction to the competitors and have them leverage tools that are used in industry for sifting through benign traffic and processing data. Tools such as Autopsy, FTK, EnCase (if allowed), X-Ways, and AXIOM are commonly seen as being used by student teams. Many of these tools provide out-of-the-box reporting. However, data provided by

these tools still needs to be analyzed and interpreted by the student teams.

Many times, students are faced with challenges and misleading paths. These are purposefully implanted to provide a challenge. Their failures and shortcomings serve as a starting point for further research after the competition ends if they get caught up in these traps. After every competition, the organizers and the red team (offensive) perform a debrief, where they provide an overview of the case and provide answers. This includes the attack chain completed by the red team for initial access and the purpose / Modus operandi of the perpetrator(s). Through this debrief, competitors learn what they missed and how to better hone their skills for future competitions and relative skills for this industry.

Competing more than once in CIRCUS provides a method for students to gauge their progress. A past competitor noted that they only were able to practice these skills in a competition environment. "Learning about forensics and IR tools in the classroom is notable but pales in comparison with doing it hands-on in a simulated environment. I would search for ways to learn to use these tools but would not have the access to viable data in terms of hard drives to put them into practice" (Student A, May 16, 2025). Cybersecurity competitions, such as CIRCUS, greatly motivate students to take the initiative to study for their own improvement. When a student can directly experience what it means to use industry tools as part of a simulation, they are motivated and compelled to further their own research into the industry. Another competitor noted; "since CIRCUS provides a comprehensive hands-on approach than provided in a class, I was able to connect the dots between theory and practicality. Additionally, because CIRCUS has a competitive flavor, it was inspiring for us as a team to perform up to our best abilities and take pride in our school and its Cybersecurity program" (Student B, May 16, 2025). Student competitors expressed that they greatly enjoyed and take great interest in the CIRCUS competition. Finally, this inspiration culminates in a desire for wider and deeper learning opportunities based on the situation they encounter during the competition.

Students excel in confidence and hone skills learned in the classroom through cyber competitions. CIRCUS is no different. Students granted the opportunity with hands-on experience are more equipped to deal with the technical demands of their future careers. Hiring managers look for people with technical experience, and cybersecurity competitions are a way for students to demonstrate what they know and what they can do. Another student disclosed that "CIRCUS was one of the many competitions I have taken part in over the past year. However, it is the only one purely focused on a single case and dedicated to forensics and incident response. It is a true mystery! You don't know what you are going to get until you open the drives" (Student C, May 16, 2025). Many competitors who participate in CIRCUS feel that they can learn much more by competing than taking a class.

## 6. CIRCUS & TEACHING PROFESSIONAL SKILLS

CIRCUS not only puts the technical skills of competitors to the test, but it also helps build critical professional skills including teamwork, communication, collaboration and presentation. These are all qualities that are much more difficult to learn in a traditional classroom setting be it in-person or virtual. CIRCUS allows students to participate in an environment that forces them to work together, divide up responsibilities, and collaborate on a final work product. This is crucial to any successful cyber competition but critical in the scope of CIRCUS.

Collaboration and team dynamic are critical parts even before the competition starts. Strong teams learn to strategize, set up their investigative environment, format reporting templates, and practice their interviewing skills. Being in a team environment can therefore result in a more successful student, as they are surrounded by others who are working towards the same goal.

During the competition, students are expected to work cohesively to dive in and complete the necessary tasks. This strongly mimics IR teams in industry and is meant to enhance learning experiences and provide an objective of teamwork. For example, competitors are given multiple machines to analyze. However, it is up to their team to decide how to divide up tasks or machines between team members. Each team may have different skill sets per member which should be taken into consideration when dividing up the work. This provides team organization skills and leadership opportunities for the team leader / faculty coach. "During the past CIRCUS competition, our team was assigned tasks appropriate with our role within the team. This allowed us to focus on the areas where we were strongest. However, we also cross checked each other's work and we all collaborated on the final

product that was submitted" (Student C, May 16, 2025).

Additionally, teams must consider other factors. These include who will cover what area during the presentation and who will answer what kinds of questions during the deposition phase. It allows for students to explore potential subject matter expertise and hone their presentation skills around the explanation of complex technical details to a degree of explaining them in layman's terms. However, every competitor takes on a leadership role in one way or another since teammates will help each other out when another teammate is unsure about how to approach a problem. The team members get a feel for how their fellow competitors will react to different situations, questions, and demands.

The statements of past student competitors emphasize the importance of having soft skills during the final phase of the competition.

One such competitor stated, "management and collaboration skills were essential to our success in the competition. There are a lot of logs and traffic to sift through, and this is very time-consuming. Having a strategy of dividing and conquering is good so that you ensure you find as many of the artifacts as possible. This led us to better understand the cause of the breach. Competing in CIRCUS is like managing a disaster after the fact. You have to piece together what happened and try, if possible, to figure out the 'why'. Approaching this with a calm, planned approach while assisting each other with our individual expertise leads to a smooth operation in the approach to the problem" (Student B, May 16, 2025).

Another student commented on the challenges presented by the mere volume of data, stating that "multiple machines were provided for analysis, and they had a multi-day timeframe to search through for artifacts. I can only imagine the complexity of a true IR engagement where professionals have to go back weeks, months or even years to find the cause of a breach" (Student B, May 16, 2025).

## 7. PERSPECTIVE OF THE ORGANIZERS

CIRCUS is a competition built by industry professionals who were once students, who bring a perspective on professional lessons. In addition, we understand that the cybersecurity technology landscape changes rapidly and is a moving target for students. Part of the goal for CIRCUS is to provide training methodology for students to adapt to these rapidly changing practices that traditional environments may lag behind. As we practice it then so do students which hopefully narrows the knowledge gap after their graduation. CIRCUS begins with the organizers developing a theme followed closely by an entire environment that will provide a foundation for the "attack" to take place. The organizers then configure various operating systems, applications, and implant materials that would be enticing to any attacker. These simulate real-world assets that include database with customer/ client information, proprietary intellectual property, and other assets that exemplify value to the fictitious organization. Even after all the planting of assets and configuration of network and systems, one key element eluded the organizers. This was the normal operating activity of real users.

The organizers leveraged several tools including SPECTRE, Shadows, GHOSTS, and to a lesser degree CRUCIBLE for user simulation. GHOSTS simulates user activity on a computer, like creating documents, browsing websites, and downloading files. It drives various popular applications on both Windows and Linux machines. Whether you're a friendly administrator or a cyber adversary, GHOSTS can replicate your expected behavior (Software Engineering Institute, 2020).

GHOSTS has many use cases in cyber experimentation, training and exercise, most notably for bringing non-player characters (NPCs) to life. However, it can also be used for other purposes requiring realistic activity on a computer. SPECTRE allowed for the GHOST agents to remember preferences such as personas mimicking human behavior. This was taken a step further by the use of Shadows, which is an agent allowing AI LLM access via API for organic appearance of natural behavior.

These simulation software frameworks were tested by the Software Engineering Institute at Carnegie Mellon University and were found to be useful in creating "noise" for the competition. Without these tools, students would have a much easier time in finding the planted artifacts left behind by the simulated attackers. One finding through the first two iterations of CIRCUS was that students identified GHOSTS' activities as malicious when they were not meant to be seen as such. This finding will be overcome in future competitions by a simple informational rule

stating that activities with certain fingerprints should be ignored.

The environment was then set up for attack. During the first two seasons of CIRCUS, the organizers also served as the attackers. A script was followed simulating an internal threat for both iterations. For future seasons, it is planned to have an outside, professional Red Team member act as a threat. This is to enact the case where advanced persistent threats (APTs) can be simulated. The end goal is to make the competition as "real-world" as possible giving students who play in multiple years of the competition the opportunity to see the major types of attacks that IR professionals come across.

The geographic scope of the competition has also grown year by year. Running from a small grant provided by the Orange County Regional Consortium (OCRC) that provided seed funds to develop the environment, craft rules, advertise to schools, and provide support services. The inaugural season consisted of only community colleges in Orange County, California. In season two, the competition expanded to two-year and four-year schools in southern California. It is the intent of the organizers to expand this in year three to include all of California and build upon a regional structure in two years. The goal is to expand into a style such as CPTC and CCDC with regional and national footprints.

In summation, throughout the development process, we have developed rules, scoring, most importantly environmental practices that provide a level playing field for student teams to compete and showcase their IR skills learned in the classrooms at their institutions. This competition's vision is to provide students with real-world experience and give outside organizations the ability to recruit top talent for their IR teams. This follows established methodologies of other successful competitions and given the prospect of the industry, only shows signs of interest and growth.

## 8. PERSPECTIVE OF THE COACHES AND PLAYERS

As aforementioned, IR and digital forensics are a continually growing and changing area of cybersecurity. CIRCUS provides the ability for educators to adapt, change and better their curriculum and teaching methods in the classroom. Students are exposed to not only technical aspects of responding to incidents, but also data collection methods and chain of custody, through a legal lens that is not highlighted in other competitions. The competition provides students with the opportunity to present their findings based on facts, not opinions, and a teaching opportunity for educators to provide mentoring and guidance to students on verbal presentation skills.

CIRCUS provides opportunities that other curricular or extracurricular activities and programs cannot through its hands-on aspect of the competition. The organizers work tirelessly to provide an environment on par with cases seen in industry and follow industry standards, frameworks, and expectations by constructing multiple competition environments each year. Moreover, as the development process is incredibly fluid and attack simulation is very nuanced, the organizers must be able to provide detailed records of the attack chain for validity purposes. For the past two competitions, we have leveraged the MITRO ATT&CK methodology while designing / documenting the attack chains to that students have a "real-world experience.

Players and coaches both expressed the unique opportunity to have a competition such as CIRCUS to test their skills. From the player's perspective, preparing for CIRCUS consisted of taking lessons learned in class and applying them to test machines. For some competitors, these were provided by class assignments or additional materials provided by the teams' faculty advisors. Teams also provided insight regarding defensive and IR related training from online sources such as TryHackMe (TryHackme.com) and Hack The Box. Hack The Box offers security operations center training that includes DFIR modules for more advanced training, including access to tools and platforms in the form of VMs to practice with. Some teams took this a step further. They reported to us that they had dedicated lab equipment in which to practice, including servers, and desktops with which they could analyze. Some teams included insight into the fact that they would split up tasks between students where one group would act as an adversary and the others would act as the responders. The adversaries would plant artifacts for the responders to find via practice with forensic and IR tools. Once the exercise was completed, they would switch roles and repeat the process.

Many teams formed through their cybersecurity clubs. This is not unlike other competitions such as CPTC or CCDC. This seems to have become the norm with training and research for undergraduate students outside of the classroom. This methodology provides a semi-structured

learning experience from which more senior students can provide training to new students. Successful teams appear to come from schools with a well-established club structure where knowledge transfer is occurring organically.

## 9. CONCLUSIONS & OPPORTUNITIES FOR FURTHER RESEARCH

This case clearly outlines and reinforces the advantage of leveraging industry specific competitions to gauge student and program strengths. This allows for the further measure of student learning outcomes provided in the classroom for digital forensics and incident response courses.

Furthermore, it surmises the links between curricula and practice. Thus, it gives educators a different lens to view, hone and improve their program's pedagogy. This provides a unique modality through the opportunity to measure skills in unique ways. Finally, it also allows for the measure to track these skills over many years to include the entire careers of participants.

Future research endeavors include the establishment of inventories of competencies and skills that relate to courses and may also offer enhanced ways to effectively measure students' knowledge, skills and abilities. This in turn can lead to more effective capabilities in offering courses in a specific curriculum set. This competition focuses on specific skill sets that are highly sought. Effective cybersecurity pathways in Digital Forensics and Incident Response (DFIR) necessitate the ability to understand and develop these skills for immediate use upon graduation making the student career ready. Finally, outreach to industry professionals as judges and volunteers can lend advisory guidance for competition enhancement. This in turn will align the competition to industry best practices.

Given these opportunities, it is proposed that further research be done with a wider populace. Driving CIRCUS to a more regional and national footprint is a logical conclusion. The measure of these skills that are so critical to aspects of cybersecurity such as incident response, digital forensics, and memory forensics.

## 10. REFERENCES

Anand, V., Bolton, N. A., Calyam, P., Chadha, R., Raj, R. K., & Mishra, S. (2023, December). Enhancing Computing Curricular Outcomes and Student Accomplishments Through Collegiate Competitions. In Proceedings of the ACM Conference on Global https://doi.org/10.1145/3576882.3617924 Computing Education Vol 1 (pp. 22-28). https://doi.org/10.1145/3576882.3617924

Bain, L. Z., & Mello-Stark, S. (2019). Reflections on security courses in CIS curriculum after attending a CAE workshop. Issues in Information Systems, 20(3). DOI:10.48009/3_iis_2019_1-10

Balon, T., & Baggili, I. (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Education and Information Technologies, 28* (9), 11759-11791. https://doi.org/10.1007/s10639-022-11451-4

Bonnie, E. (2025). *110+ of the latest data breach statistics [Updated 2025]*. IBM. https://secureframe.com/blog/data-breach-statistics

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012, January). Effectiveness of cybersecurity competitions. In Proceedings of the International Conference on Security and Management (SAM) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing. https://worldcomp-proceedings.com/proc/p2012/SAM6108.pdf?utm_source=chatgpt.com

CIIRC. (2024). *CIIRC team packet*. https://www.ecs.baylor.edu/get-involved/cybersecurity-interdisciplinary-incident-response-competition-ciirc-2024

Conklin, A. (2005, September). The use of a collegiate cyber defense competition in information security education. In Proceedings of the 2nd Annual Conference on Information Security Curriculum Development (pp. 16-18). ACM. https://doi.org/10.1145/1107622.1107627

Conklin, A. (2006, January). Cyber defense competitions and information security education: An active learning solution for a capstone course. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (Vol. 9, pp. 220b-220b). IEEE. https://doi.org/10.1109/HICSS.2006.110

Etezady, N., & Wang, P. (2025). Capstone project design for an undergraduate cybersecurity program. In Proceedings of the 22nd International Conference on Information

ISSN: 2473-4901
v11 n6402

Technology-New Generations (ITNG 2025) (pp. 84–94). Springer, Cham. https://doi.org/10.1007/978-3-031-89063-5_8

Grier, D. A. (2019). The Path Across the Great Deep. *Computer*, *52*(04), 10-11.

IBM. (2025). Cost of a Data Breach Report 2025: *The AI oversight gap*. Ponemon Institute & IBM Security. https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91

International Organization for Standardization. (2018). *ISO/IEC 27035-1:2018 — Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. https://www.iso.org/standard/78974.html

Katsantonis, M., Fouliras, P., & Mavridis, I. (2017, April). Conceptual analysis of cyber security education based on live competitions. In 2017 IEEE Global Engineering Education Conference (EDUCON) (pp. 771–779). IEEE. https://doi.org/10.1109/EDUCON.2017.7942934

Manson, D., & Carlin, A. (2011). A league of our own: The future of cyber defense competitions. *Communications of the IIMA*, *11*, 1.

Murphy, C. F. (2018). Instructional designs and the development of cybersecurity workforce readiness skills: A qualitative content analysis of cyber- or information security syllabi (Publication No. 10931804) [Doctoral dissertation, Northcentral University]. ProQuest Dissertations Publishing. https://www.proquest.com/openview/bf6d36c2d7d9dd92b3fb6829e73fb64b/1?pq-origsite=gscholar&cbl=18750&diss=y

National Institute of Standards and Technology. (2024). *Computer security incident handling guide* (Special Publication 800-61 Rev. 3). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/61/r3/final

National Security Agency. (2014, June 25). NSA and DHS announce the 2014 National Centers of Academic Excellence in Information Assurance and Cyber Defense. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1649326/nsa-and-dhs-announce-the-2014-national-centers-of-academic-excellence-in-inform/

O'Connor, T. J., Brown, D., Jackson, J., Payne, B., & Schmeelk, S. (2023). Compete to learn: Toward cybersecurity as a sport. *Journal of Cybersecurity Education, Research and Practice*, *2023*(1), 6. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/6

Oliver, J. Y., & Elwell, C. (2018, March). Effective competitions for broadening participation in cybersecurity. In 2018 ASEE Zone IV Conference. ASEE. https://peer.asee.org/29608

Positive Technologies. (2023, December 13). Results of cybersecurity incident investigations in 2021-2023. https://global.ptsecurity.com/en/research/analytics/results-of-cybersecurity-incident-investigations-in-2021-2023/

SANS Institute. (n.d.). Cybersecurity / Information Security Policies and Standards. SANS Institute. https://www.sans.org/information-security-policy

Software Engineering Institute. (2020). *Crucible and GHOSTS: Enabling realistic cyber simulations*. Carnegie Mellon University, Software Engineering Institute. https://insights.sei.cmu.edu/history-of-innovation/crucible-and-ghosts-enabling-realistic-cyber-simulations/

White, G. B., & Williams, D. (2005, October). The collegiate cyber defense competition. In *Proceedings of the 9th Colloquium for Information Systems Security Education* (pp. 26–31). https://cisse.info/e/archives/3-2005/4-papers/25-s02p02-2005

Whitman, M. E., & Mattord, H. J. (2008, September). The Southeast Collegiate Cyber Defense Competition. In Proceedings of the 5th Annual Conference on Information Security Curriculum Development (pp. 1-4). ACM. https://doi.org/10.1145/1456625.1456627

Woszczynski, A. B., & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education*, 28(1), 21.

ISSN: 2473-4901
v11 n6402

## Appendix A
## CIRCUS ATTACK CHAIN

The Attack Chain shows the path of the breach and the MITRE ATT&CK tactics employed by the adversary.

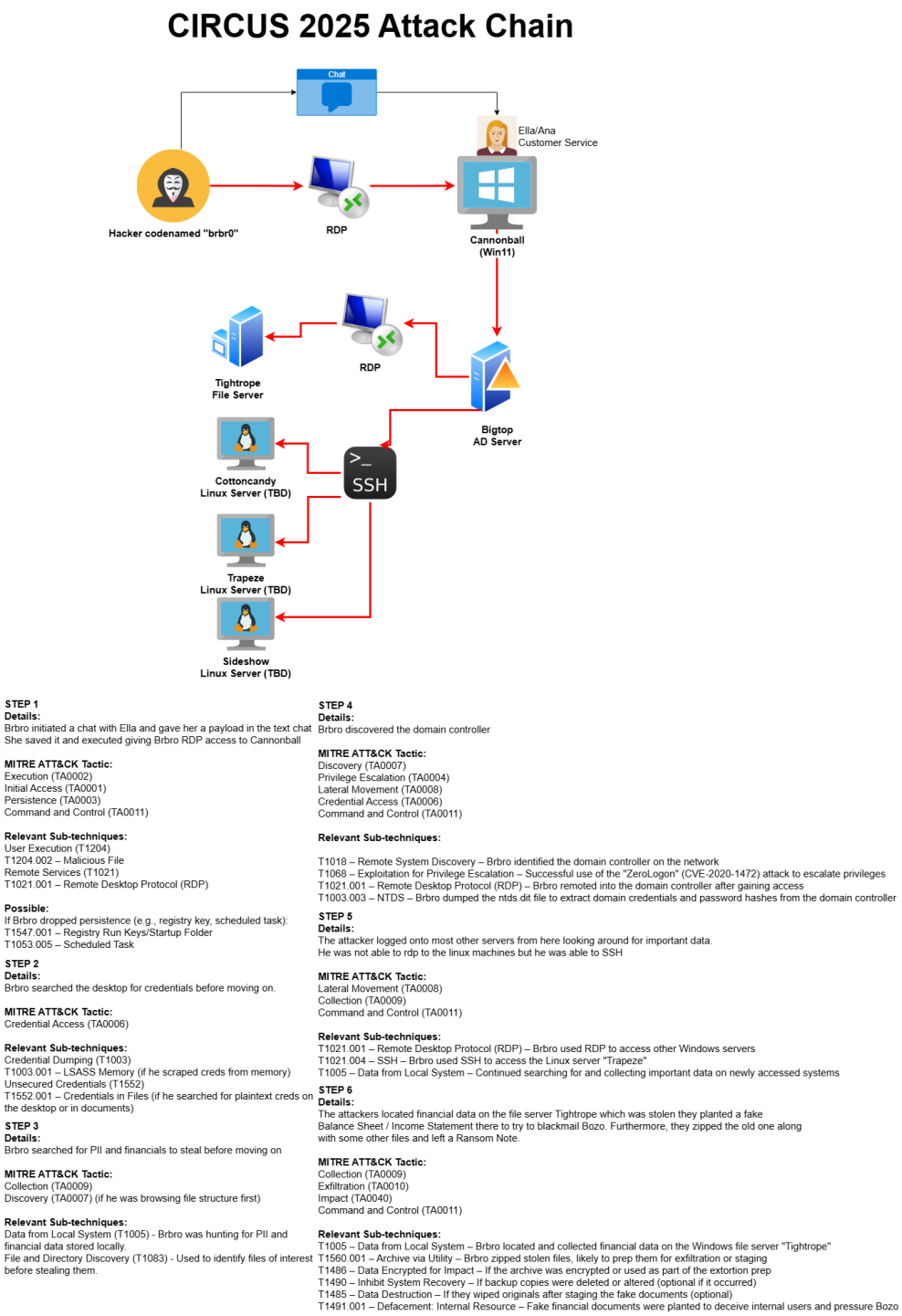


Figure 1 CIRCUS Attack Chain

Detailed Steps in Attack Chain:

**STEP 1**
**Details:**
User Brbro initiated a chat with Ella and gave her a payload in the text chat.
She saved it and executed giving Brbro RDP access to Cannonball.

**MITRE ATT&CK Tactics:**
Execution (TA0002)
Initial Access (TA0001)
Persistence (TA0003)
Command and Control (TA0011)

**Relevant Sub-techniques:**
User Execution (T1204)
T1204.002 – Malicious File
Remote Services (T1021)
T1021.001 – Remote Desktop Protocol (RDP)

**Possible Narrative of Attack**:
If Brbro dropped persistence (e.g., registry key, scheduled task):
T1547.001 – Registry Run Keys/Startup Folder
T1053.005 – Scheduled Task

**STEP 2**
**Details:**
Brbro searched the desktop for credentials before moving on.

**MITRE ATT&CK Tactic:**
Credential Access (TA0006)

**Relevant Sub-techniques:**
Credential Dumping (T1003)
T1003.001 – LSASS Memory (if he scraped creds from memory)
Unsecured Credentials (T1552)
T1552.001 – Credentials in Files (if he searched for plaintext creds on the desktop or in documents)

**STEP 3**
**Details:**
Brbro searched for PII and financials to steal before moving on.

**MITRE ATT&CK Tactic:**
Collection (TA0009)
Discovery (TA0007) (if he was browsing file structure first)

**Relevant Sub-techniques:**
Data from Local System (T1005) – Brbro was hunting for PII and financial data stored locally.
File and Directory Discovery (T1083) – Used to identify files of interest before stealing them.

**STEP 4**
**Details:**
Brbro discovered the domain controller.

**MITRE ATT&CK Tactic:**
Discovery (TA0007)
Privilege Escalation (TA0004)
Lateral Movement (TA0008)
Credential Access (TA0006)
Command and Control (TA0011)

**Relevant Sub-techniques:**
T1018 – Remote System Discovery – Brbro identified the domain controller on the network
T1068 – Exploitation for Privilege Escalation – Successful use of the "Zero-Logon" (CVE-2020-1472) attack to escalate privileges
T1021.001 – Remote Desktop Protocol (RDP) – Brbro remoted into the domain controller after gaining access.
T1003.003 – NTDS – Brbro dumped the ntds.dit file to extract domain credentials and password hashes from the domain controller

**STEP 5**
**Details:**
The attacker logged onto most other servers from here looking around for important data.
He was not able to rdp to the Linux machines, but he was able to SSH.

**MITRE ATT&CK Tactic:**
Lateral Movement (TA0008)
Collection (TA0009)
Command and Control (TA0011)

**Relevant Sub-techniques:**
T1021.001 – Remote Desktop Protocol (RDP) – Brbro used RDP to access other Windows servers
T1021.004 – SSH – Brbro used SSH to access the Linux server "Trapeze"
T1005 – Data from Local System – Continued searching for and collecting important data on newly accessed systems

**STEP 6**
**Details:**
The attackers located financial data on the file server Tightrope which was stolen they planted a fake Balance Sheet / Income Statement there to try to blackmail Bozo. Furthermore, they zipped the old one along with some other files and left a Ransom Note.

**MITRE ATT&CK Tactic:**
Collection (TA0009)
Exfiltration (TA0010)
Impact (TA0040)
Command and Control (TA0011)

**Relevant Sub-techniques:**
T1005 – Data from Local System – Brbro located and collected financial data on the Windows file server "Tightrope"
T1560.001 – Archive via Utility – Brbro zipped stolen files, likely to prep them for exfiltration or staging
T1486 – Data Encrypted for Impact – If the archive was encrypted or used as part of the extortion prep

ISSN: 2473-4901
v11 n6402

T1490 – Inhibit System Recovery – If backup copies were deleted or altered (optional if it occurred)
T1485 – Data Destruction – If they wiped originals after staging the fake documents (optional)
T1491.001 – Defacement: Internal Resource – Fake financial documents were planted to deceive internal users and pressure Bozo

ISSN: 2473-4901
v11 n6402

**Appendix B**
**Excerpt of Final Report from 2025 Competitor**

This appendix shows an example of a tool used for forensic analysis of one individual virtual machine's disk. Many teams utilized similar tools and techniques in their analysis of the breach.

Additionally, user activity was identified in the registry logs that involved the deletion of multiple security log files (shown in *Figure 3.b*) and the deletion of various user groups (shown in *Figure 3.C*).

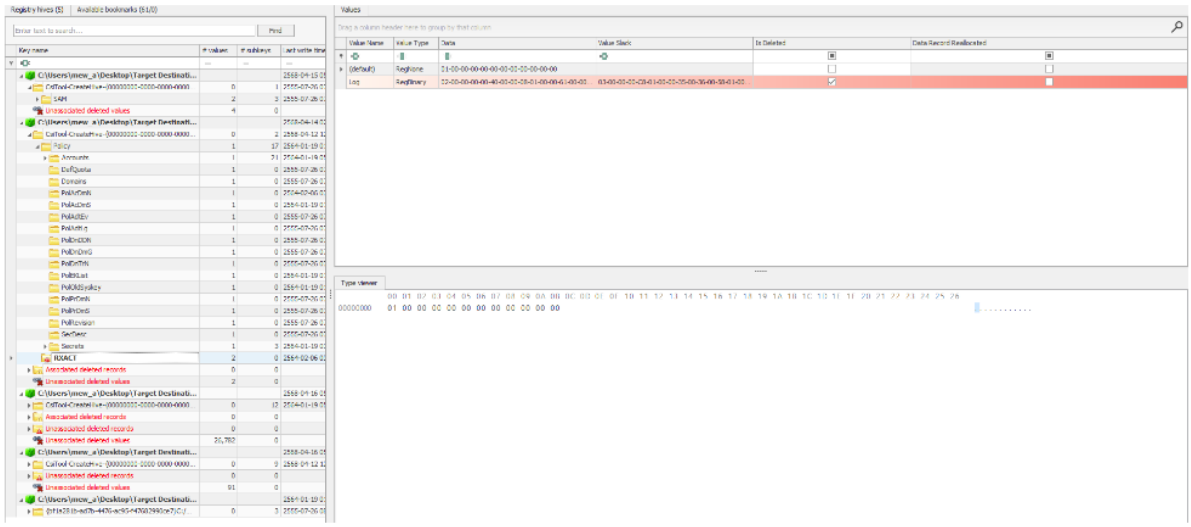

*Figure 3.b: screenshot of the deletion of security log files.*

Figure 2 Competitor Figure excerpt of Log File Analysis

ISSN: 2473-4901
v11 n6402

## Appendix C
## Judging Rubric for Competition Final Presentation

This appendix shows the list of scored areas of the report and the presentation / interview / deposition. Presentation and reporting were judged by a panel of three professionals. Scores were then averaged and calculated for each area. As the competition matures and evolves, additional and more detailed scoring and summaries are expected to coalesce.

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | CIRCUS Scoring Rubric | TeamXX | School Name | | | |
| 2 | Artifact Scoring | Description | Points | (Point Maximum) | | |
| 3 | Item | | | 250 | | Scoring Criteria |
| 4 | | | | | | |
| 5 | **Artifacts Found** | | **Between 1-5 per artifact** | | | Items are to be scored on their quality and not their frequency |
| 6 | | | **for a maximum of 250 points.** | | | Unique Artifacts are to be given priority over non-important / irrelevant ones |
| 7 | Item | | | | | Successive artifacts that "link" together that are described in such a fasion are given higher point values |
| 8 | Item | | | | | Min. 1 point per "relevant" artifact |
| 9 | Item | | | | | Max. 5 points per artifact (a score of 4 or 5 should be reserved for "linked" artifacts |
| 10 | Item | | | | | |
| 11 | Item | | | | | |
| 12 | Item | | | | | |
| 13 | Item | | | | | |
| 14 | Item | | | | | |

Figure 3 Judging Rubric