A new approach to Cybersecurity Education gives hope to the Next Generation of Cybersecurity Leaders

By: **Waymon Ho, Director of Content Development**
Simeon Kakpovi, President and Founder
Greg Schloemer, Vice President

In June 2023, the KC7 Foundation piloted a curriculum that brought real-world cybersecurity analysis to a group of fourth through seventh graders from underserved communities in Central Kentucky. Although students who participated in the Summer camp had no prior experience in cyber security, data analysis, or computer science, over the course of five days, the students investigated a realistic, complex, and multi-pronged cyber incident. At the end of the camp, students synthesized their analysis and conclusions, demonstrating their grasp of the fundamental concepts covered in the curriculum. In some cases, the strength of the analysis they presented rivaled the work of more experienced analysts in the field.

In just five days, the students were able to:

- analyze end-to-end intrusions using real data via a technical query language
- attribute intrusions to the people/entities responsible
- communicate their findings at a high level to a technical audience

We observed the following changes in the students over the course of the week:

- **Increased engagement:** At the beginning of the week, most of the students did not want to attend the camp. By Friday afternoon, they were so engaged we had to force them to close their laptops and make them walk away.
- **Improved ability to identify core analytic questions:** Students went from asking broad undirected questions, to asking specific and purposeful questions that would further their investigations
- **New ability to conduct cross-source analysis:** Students developed the ability to use disparate sources of information (5-8) to build evidence-based analytical assessments

We accomplished this by (1) redefining cybersecurity "fundamentals" not as disparate technical skills, but as highly transferable, cross-disciplinary skills that help students learn how to think, reason, and communicate and (2) creating experiential learning opportunities that promote student agency and allow students to develop these skills independently. Using this model, we can make cybersecurity training approachable to millions of people around the word regardless of their background or prior knowledge.

About the camp

In June of 2023, the KC7 Foundation held a week-long Cyber Summer Camp in partnership with Fayette County Public Schools (FCPS) in Lexington, Kentucky. The summer camp consisted of 4th to 7th grade students, primarily from **underserved and underrepresented communities.** This camp was provided free of charge to students and their families, with the intention of reaching students who may never otherwise get exposure to the cybersecurity industry. Consequently, most of the student participants had never been exposed to computer science or cybersecurity concepts before.

Source: Youtube (https://www.youtube.com/watch?v=H-lKiHsctTQ) – FOX56 News

"At first I didn't want to be here and now I'm enjoying the camp. [They're] teaching a whole bunch of things, things I've never heard [of], things I've never learned.." (Camp participant, 7th grade)

After just five days of camp, the students learned to use Kusto Query Language (KQL) and Azure Data Explorer (ADX) to analyze various types of log data, investigate simulated computer intrusions, and formulate and present assessments of what occurred. All the while, they developed investigative and critical thinking skills by asking good questions, paying attention to details, and linking threat indicators across various mediums of data, like news articles, social media posts and business records. Further, they used the data they analyzed to perform attribution of threat actors to (fictitious) people, an opportunity that even most cybersecurity professionals never have.

Our Approach

We started with a focus on using data to make analytical assessments

Source: students investigate a museum heist by interviewing several museum staff.

Every day at Cyber Summer Camp, the KC7 team had campers recite the three key tenants of a good cybersecurity analyst:

1. *Pay attention to details*
2. *Ask good questions*
3. *Be good with data*

Students started their week with an investigation into a fictional museum heist. The key to solving the mystery lay with the museum staff (witnesses), each possessing valuable information that, when combined, would unveil the complete picture of the heist. The campers had to ask witnesses targeted questions to get clues that could help them solve the mystery.

At the beginning of the exercise, students were asking broad, undirected questions like:

- “Did you see who stole the amulet?”
- “Who is the thief?”
- “Did you steal it?” (directed even at people who were not part of the exercise)

These generic questions yielded no information. The students quickly adapted and learned how to ask better, more specific questions, like:

- “What was the color of the person’s [suspect’s] hair?”
- “What were they wearing?”
- “Do you have any ticket logs or sales receipts?”
- “Do you have any parking information?”

As the students iterated on their questions and learned to be more specific, they built better mental models that would help them solve the problem. They were not only answering the question of “who did it?”, but were learning how to break a complex investigation into smaller, more manageable pieces and to understand the relationships between different pieces of information.

Not all of the clues lead students to straightforward conclusions. Some students jumped too quickly to accuse a particular suspect without fully considering all the evidence available to them. This enabled us to have rich conversations about analytical biases and how they can detrimentally impact investigations.

Ultimately, the students learned how disparate sources of information can connect to tell a cohesive story. This activity also instilled in students an investigative mindset and curiosity which they would apply to cybersecurity investigations during the rest of the week.

Tabular data and query languages

After completing the museum heist exercise, we introduced students to tabular data (data in tables) and showed them a new way to ask questions about data.

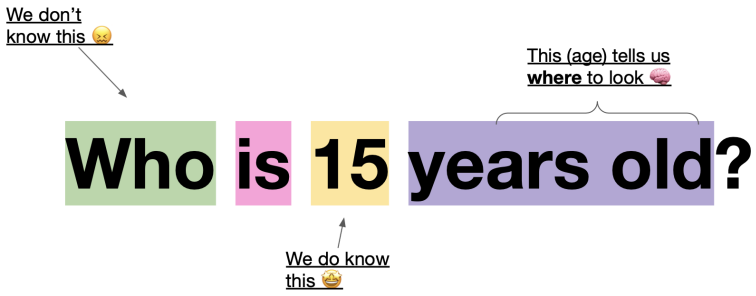
The goal, ultimately, was to teach students how to use Kusto Query Language (KQL), a data query language developed by Microsoft that is used by cybersecurity professionals to analyze large, tabular datasets. Since most of the students had little to no experience with programming or the syntax complexities that come with it, we had to take a unique approach to building KQL proficiency.

We began with a simple data table that presented some information about a few people. We asked students basic questions about the data, like “Who is 15 years old?”

Who is 15 years old?

Name	Age	Height	Favorite Color	Favorite Food
Benjamin	55	6'2"	Blue	Cheese pizza
Sophia	8	3'11"	Green	Pepperoni pizza
Olivia	17	5'6"	Red	Sushi
Ethan	15	4'9"	Blue	Ice cream
Ava	29	5'4"	Yellow	Sushi
Hagatha	19	5'10"	Orange	Sushi

Once they were comfortable answering questions by looking at columns and rows, we asked them to think about the questions we were asking them in a different way.



Students took the questions we asked them, and broke them down into a few parts:

- What don't we know?
- What do we know?
- Where do we need to look to find the answer?

Next, students were introduced to KQL operators using physical, color-coded cards. They used these cards to convert our questions into a corresponding KQL query equivalent.

Source: Students using flash cards to craft queries in KQL.

Once they had gained familiarity with KQL syntax and the operators that could be used in the language, we transitioned students from building cards on the table to writing KQL queries in Azure Data Explorer (ADX), Microsoft's cloud-based data analytics platform.

Why it worked

Had we taken these students, who had no prior experience writing code, and asked them to jump directly into ADX, they almost certainly would have failed. Instead, we built a supportive learning environment and offered accessible, hands-on learning opportunities that helped students feel successful and quickly master a highly technical concept.

Bringing it all together

With an understanding of how to ask good questions, how to use multiple sources of information (data) to tell a story, and how to challenge assumptions (biases) and make good assessments, the students were ready to investigate their first cyber intrusion.

The task: The students were informed they had been hired to investigate a cyber attack against the Spider Society, a fictional organization related to Marvel's Spiderman. Students had to work

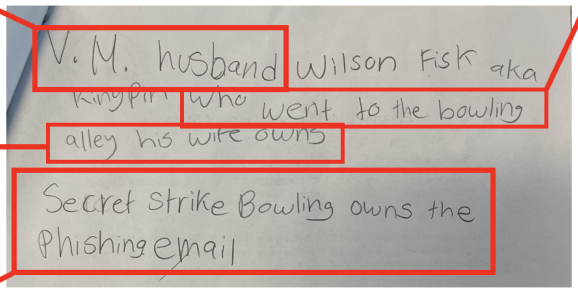
collaboratively with their peers to investigate the intrusion, find out who was responsible for it, and report what they'd learned.

The roles: In their teams, students were assigned unique roles. The *analysts* were hands-on in ADX, analyzing log data and drawing conclusions from it. The *investigators* had to compile various types of evidence (from human sources, social media, business filings, etc) and ask pointed questions to gain more insight. *Case managers* were responsible for documenting the team's findings and directing each of the team's members to ensure they were working together and aligning on goals. And each team's *CFO (Chief Financial Officer)* tracked the team's financial performance and helped the team make risk-based decisions. Students learned the value of each team members' role and helped support their peers and the work they were doing.

Real-world example (1) Below is an example of a student (a 6th grader) summary of how she would attribute the phishing attack that targeted the Spider Society. Note that the student correlates multiple sources of data, and "pivots" on indicators to discover new sources of evidence during the attribution process.

4. The student conducted OSINT research on an individual named "Vanessa Mariana" and realized this was the maiden name of a woman named "Vanessa Fisk." Vanessa Fisk is a wife of supervillain Wilson Fisk who is also known as "Kingpin"

5. The students identified a social media post in which someone sighted the "Kingpin" at the Secret Strike bowling alley

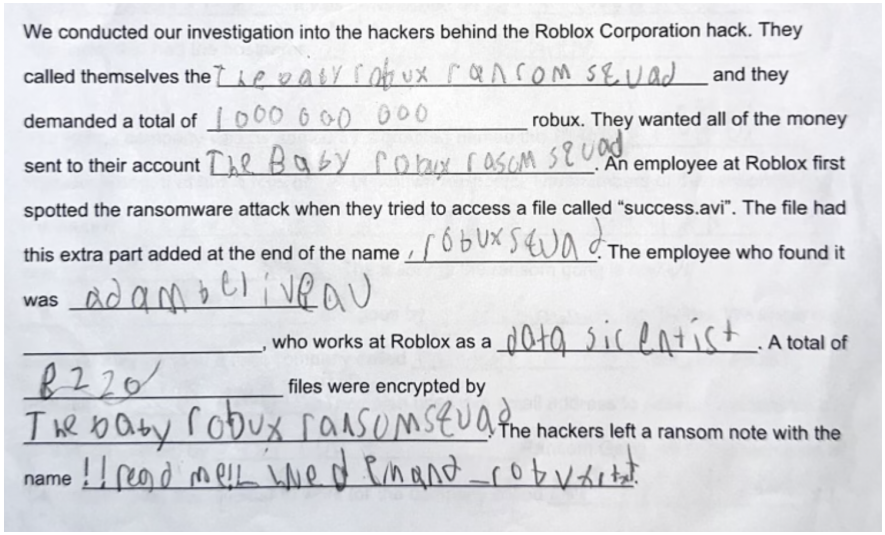


3. Student requested business records for the Secret Strike Bowling Alley and discovered it was registered to "Vanessa Mariana"

2. The student observed a newspaper article in which the Secret Strike Bowling alley used email address underground[@]aol.com as a contact email

1. The student observed email address underground[@]aol.com used to send phishing emails to targets

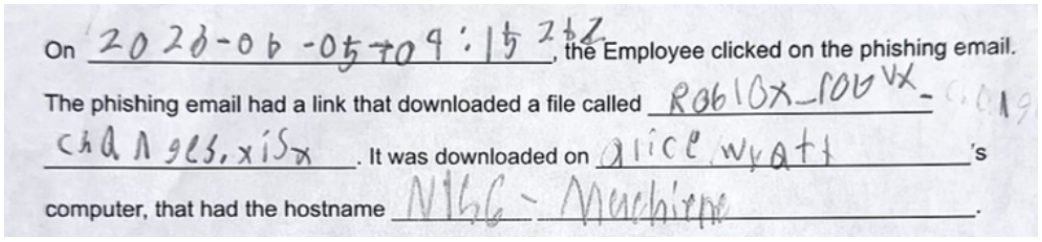
Real-world example (2): Here's another example of how students applied what they learned to investigate the final challenge intrusion, a ransomware attack against a video game development company:



We conducted our investigation into the hackers behind the Roblox Corporation hack. They called themselves the The baby robux ransom squad and they demanded a total of 1000 000 000 robux. They wanted all of the money sent to their account The Baby robux ransom squad. An employee at Roblox first spotted the ransomware attack when they tried to access a file called "success.avi". The file had this extra part added at the end of the name .robuxsquad. The employee who found it was adam bilibau, who works at Roblox as a data scientist. A total of 8220 files were encrypted by The baby robux ransomsquad. The hackers left a ransom note with the name !!read me!! the baby robux ransomsquad.

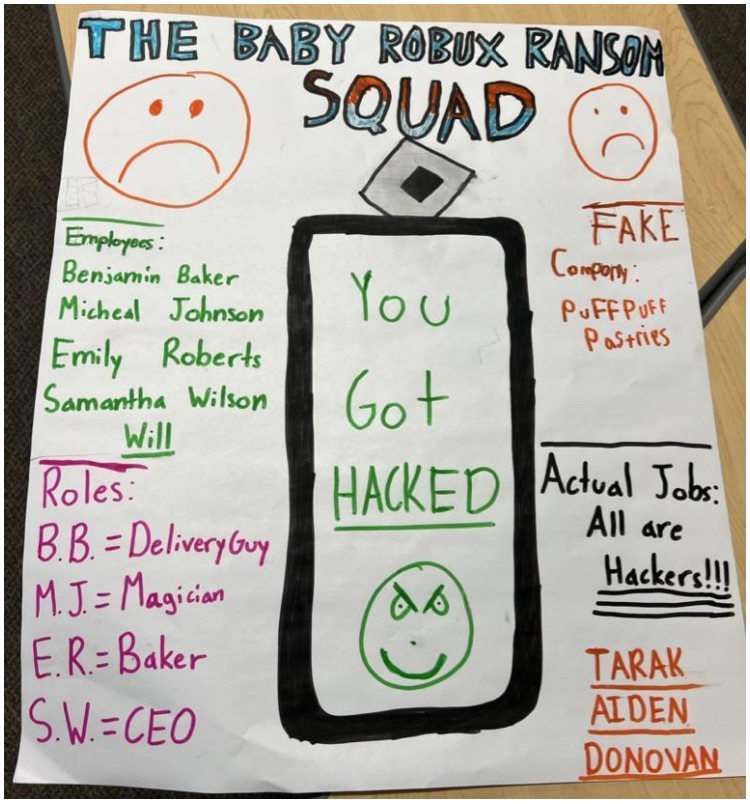
Source: Students analyzed data including text files, social media posts, and data derived from tables in ADX using KQL to answer questions in a summary sheet.

Students used multiple investigative techniques to generate leads on their case. They questioned witnesses to solicit information that could then be used to find indications of compromise within the compromised environment. Working together, they were able to create a timeline of the intrusion and attribute it to the threat actors responsible.



On 2020-06-05T09:15:22Z, the Employee clicked on the phishing email. The phishing email had a link that downloaded a file called ROBLOX_ROBUX_CHANGES.ISO. It was downloaded on alice wyatt's computer, that had the hostname NHG-Machine.

Source: Students used KQL and ADX to extract evidence from data and answered questions pertaining to the timeline and victims.



Source: Students created visuals like this poster to help present their technical findings to a wider audience.

Outcomes

All 35 students finished the camp with a set of new skills and abilities. They learned:

- How to ask targeted questions to derive information from multiple sources and types of data
- How to use KQL and ADX to analyze log data and synthesize results
- How to understand and apply technical terms and details derived from various data sources
- How to present findings clearly and concisely to a team of stakeholders
- How to attribute cyber threat activity to a persona, individual, or entity
- How to work in a team and collaborate with teammates of different skill sets to accomplish a mission

But most importantly, over the course of the week, students grew excited about cybersecurity, and about learning in general. They came in each day more excited to get started than they were the day before. They each experienced success and felt empowered to continue learning and to share what they had learned with their peers.

"…I feel smart in something that I didn't know [before]."

Some of the FCPS Educators mentioned that many of these students would be overlooked if teachers exclusively provided opportunities based on students' reading levels. The Cyber Summer Camp helped students identify critical abilities and skills. It also provided them with the opportunity to learn about a career pathway they can start pursuing immediately.

If we had 4th graders excited about and capable of investigating, attributing, and reporting on intrusions in just five days, then how are we facing a shortage of 3.5 million cybersecurity professionals in the next two years? The problem lies in the way we've always taught cybersecurity.

Our Philosophy

Traditional cybersecurity training is flawed, especially formal cybersecurity education that takes place in K-12 and post-secondary classrooms. Cybersecurity classes have historically started with *the "fundamentals"*: networking, operating systems, and cryptography. With this approach, students spend the first few years reading textbooks and listening to lectures that discuss deeply technical, yet disjointed concepts. Without scaffolding upon which they can apply and retain these skills, students forget what they've studied and/or completely lose interest in the field before they ever have a chance to see the more fun and interesting parts of cyber.

KC7 challenges this traditional approach. We've redefined "fundamentals" not as disparate technical skills, but as highly transferable, cross-disciplinary skills that help students learn how to think, reason, and communicate. With KC7, students begin their cybersecurity learning journey by building and reinforcing skills in critical thinking, teamwork, written and verbal communication, and application of geopolitical context.

How we do it?

With KC7, there aren't any textbooks to read, lectures to listen to, or papers to write. **Students step straight into the role of a cybersecurity analyst and get hands-on experience analyzing realistic cybersecurity intrusion data and investigating simulated cyber attacks.** At first, students encounter many concepts they aren't familiar with, leaving them wondering: *what's an IP address? What is a file hash? How does a process work?* But, instead of frontloading instruction by introducing these concepts through lecture, we push students to interact with and apply deeply technical knowledge without fully understanding how it works. **We are creating experiential learning opportunities that promote student agency and allow students to develop these skills independently**

KC7's approach to teaching cyber inspires students' natural curiosity, which often leads students to learn more about the concepts they encounter on their own. Most importantly, this approach builds the scaffolding which will enable future, more rigorous instruction. Later, when students learn what an IP address is and how network routing works, they aren't left wondering *"but why does this matter?"* Instead, they've seen and worked with IP addresses and domains before, and can better understand and appreciate the technical underpinnings of those concepts.

We've employed this approach, with great success, when teaching cybersecurity to students at all levels, from elementary students to senior cybersecurity analysts to executives at top cybersecurity firms. While the content developed for these different audiences may vary slightly, the core of our approach is always focused on hands-on experience and building transferable skills that will prepare learners for careers in cybersecurity, but will also support them in any field they may choose to learn and work in.

About the KC7 Foundation

The KC7 Foundation is a 501(c)(3) nonprofit organization whose mission is to empower everyone to succeed in tomorrow's diverse cybersecurity workforce. We realize this mission by developing cybersecurity training and educational content that is accessible to everyone. The KC7 Foundation aims primarily to provide equitable training to several key groups: K-12 students, post-secondary students, transitioning professionals looking to reskill into cyber roles, and current cybersecurity professionals looking to upskill.

The KC7 Foundation considers K-12 cybersecurity education to be one of its key focus areas. To ensure that we build the next generation of cybersecurity leaders, we must provide engaging and accessible opportunities that will help young students build interest in and excitement about cybersecurity. Then, we must support and nurture that curiosity by providing dynamic and comprehensive learning opportunities for all grade levels. In order to do that, we must bring together industry professionals with K-12 educators to provide students hands-on, real-world training that will teach them the foundations of cybersecurity and help spark an interest in this career field.

Funds obtained from donations, grants, and sponsors support our mission and are used to provide cybersecurity training and workshops **at no cost** to underserved communities and populations.

References:

The KC7 Foundation
- https://www.kc7cyber.com

News Broadcast on FCPS Cyber Summer Camp
- https://youtu.be/H-lKiHsctTQ

Twitter Post on another News Broadcast of the FCPS Summer Camp
- https://twitter.com/KC7cyber/status/1674176230780813319