Cyber Grand Challenge - Visualization

This document is intended to describe in detail the visualizations we are providing for CGC. If you have questions on any of the details, please contact Matthew Wynne (matthew.wynne@voidalpha.com).

The seven main visualization views available to us are as follows:

1. Arena View
2. Scoreboard View
3. Graph View
4. CS View
5. Filament View
6. Memory View
7. Cube View

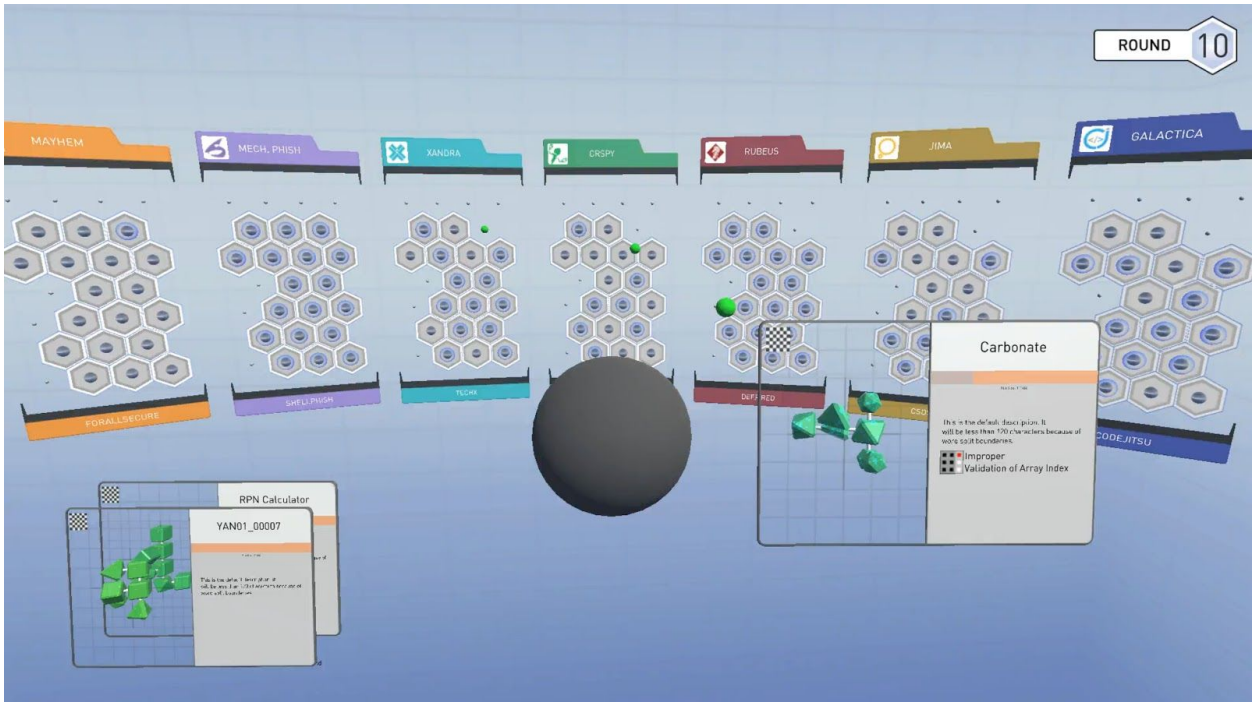
#1 Arena View

General

Arena View always focuses on a single round of play. In this view, Challenge Sets (CSs) or “services” are represented by hexagons (hexes) on a grid. Each Cyber Reasoning System (CRS) has a CRS Card in the Arena, and that card reflects all of the activity for the CRS in a round of play. The same CSs appear in the same relative locations on each CRS’s Card. So for example the top left hex on each CRS Card will represent the same CS as presented by the game. As a round of play progresses, the viewer can discern various details about how a CRS is playing and performing by comparing the visual state of a CS hexes in the same locations on different CRS’s cards.

Round Intro

Before we show the activity that takes place during a round, we can set the scene by showing the Arena View Round Intro sequence. In this view, we retire any CSs that will not be present in the game going forward, and we introduce any new CSs that are appearing for the first time in the coming round. When retiring a CS that will no longer be appearing in the game, we invoke CS View to remind viewers of that CSs properties. If one of the Cyber Reasoning Systems (CRSs) has done particularly well or poorly against a CS that is being retired, we might expect to see a change in that CRS’s scoring for the coming round. Likewise, we use CS View to give an overview of any new CSs that are appearing in the game for the first time in the coming round.



Round Replay

This view shows just about every event that happens during a round, though generally no one event is shown in any great detail. Think of it as a 3-ring (or more accurately 7-ring) circus, where no one could possibly take in every detail. It shows a big-picture view of what happened during the round. Someone in the audience focusing on a particular CRS’s Card... or some other particular detail of this view... should be able to glean some general information (e.g., a CRS is doing well/poorly overall for the round, a CRS is scoring well against one adversary but not well against others, a CRS is doing well in one aspect of the game but not in another, etc.). However, a viewer almost certainly wouldn’t be able to discern the complete outcome of

the round until the scores are revealed in the Arena View Score Tabulation Sequence. Neither would a viewer be able to tell the overall status of the game from Arena View, as Arena View always focuses on one round of play.

As Round Replay progresses, the visual state of each CS hex will change to reflect how the CRS is scoring for Availability, Security, and Evaluation, which are the 3 components of the overall score for the game. The video **CGC_Explainer_ArenaView_ASE_Scoring.mp4** shows a visual deconstruction of our per-CS representation of scoring in Arena View. The constituent parts of the overall score for a CS on a CRS Card are represented in Arena View as follows:

- **Availability (A)** is represented by the hex's scale, color value, and the speed of the center sphere's rotation – larger, lighter, and faster spin means a higher "A" score; smaller, darker and slower spin means a lower "A" score.
- **Security (S)** is represented by a white outline with a blue pinstripe around the hex – its presence means security has not been breached for the CS, it's absence means security has been breached.
- **Evaluation (E)** is represented by colored wedges radiating around the internal area of a hex. When the CRS being viewed has scored against an opponent, a wedge of the opponent CRS's color will appear over the scoring CRS's CS hex.

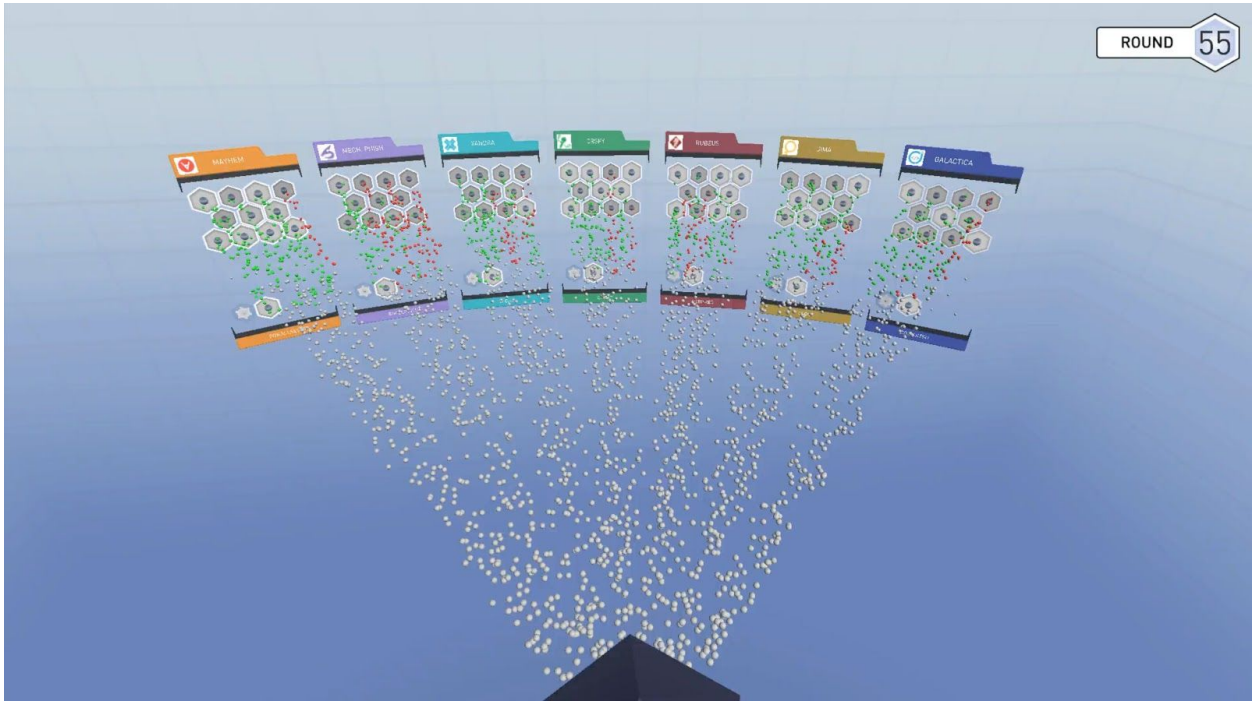
Scoring: Per round, for each CS a CRS is given a score from 0.00-1 for Availability; a score of 1 or 2 for Security; and a score from 1.00-2 for Evaluation. Those three numbers are multiplied together and the result is then multiplied by 100 to ensure that the total score for the CS for that round is an integer. So the maximum score a CRS can get per CS per round is 400 [=(1 x 2 x 2) x 100]. Since Availability can be zero, the minimum score a CRS can get per round for a CS is zero [=(0 x 1 x 1 x 100].

Other representations during Round Replay include:

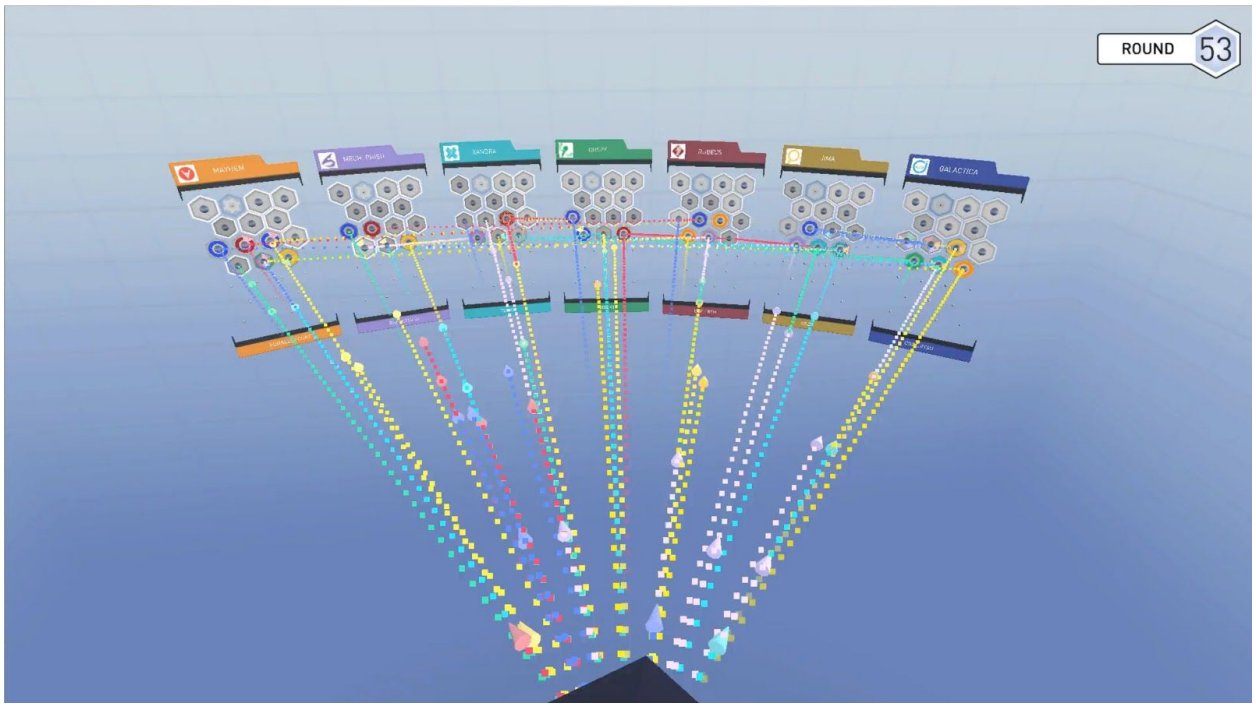
- **Thrown PoVs** (cones, color coordinated with the attacking CRS) emanate from a central Warden object (a black, spinning dodecahedron). For an unsuccessful attack, the cone will simply disappear. For a successful attack, a ring of the attacking CRS's color will appear on the attacked CS hex and the Security outline will disappear on the CS hex if the hex has not previously been successfully attacked (see "Security" above); Haxxis then draws a dotted line from the attacked CRS's CS hex to the corresponding CS hex on the attacking CRS's Card, where a colored wedge of the attacked CRS's color appears.

· **Polls** (white spheres) emanate from a central Warden object. Before a Poll reaches the CS hex, it will turn green if the CS handles it successfully and red if the CS fails to handle it successfully. Unsuccessful Poll handling affects Availability score negatively.
· **Network Defenses**, when present, are represented by a light blue, semi-transparent hemisphere over the CS hex.
· **CS down for patching -** when a CRS submits a patched Replacement CS (RCS) during a round, it will be down for that CRS for the following round to allow for “Consensus Evaluation” of the patch. During the round for which the CS is down, we will show a slowly spinning gear icon in the hex corresponding to that CS on that CRS’s Card.
· **Network Defense Rules submitted for Consensus Evaluation:** As with CSs, Network Defense Rules can be submitted by a CRS but must undergo Consensus Evaluation for a round. During the round for which the Network Defense Rules are being Consensus Evaluated, we will show a smaller spinning gear icon in the upper-right corner of the corresponding hex.

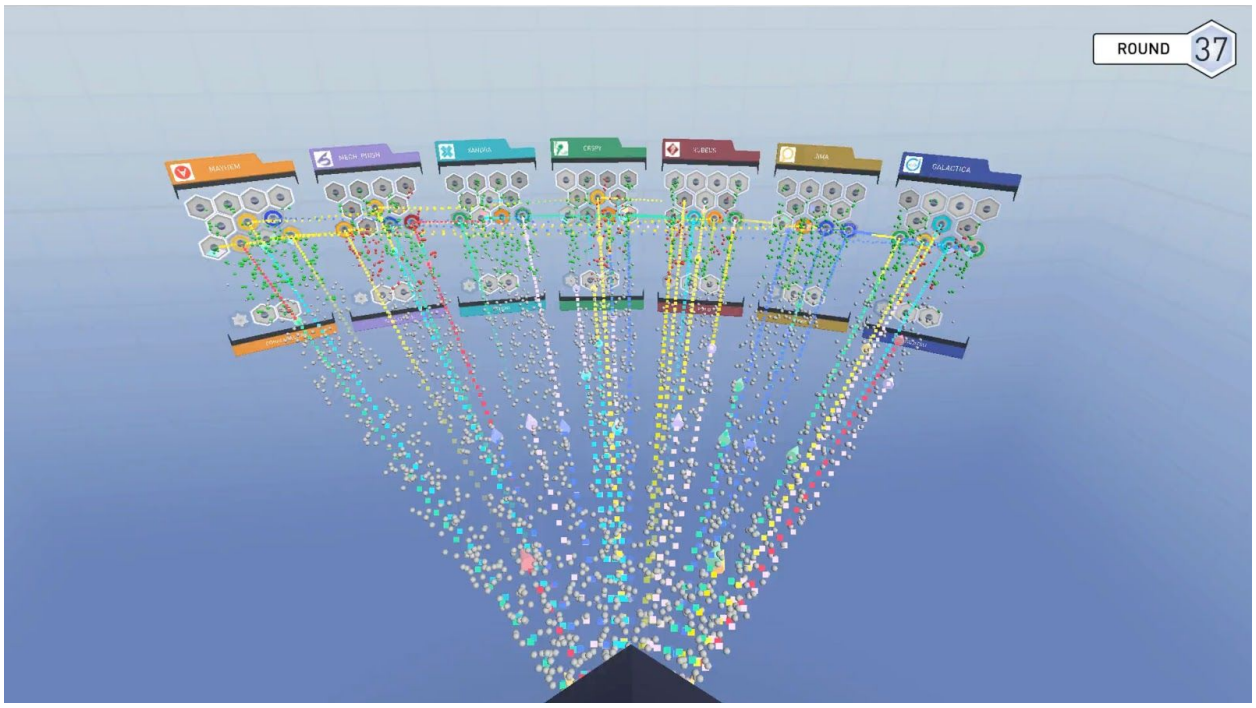
Polls:



PoVs:

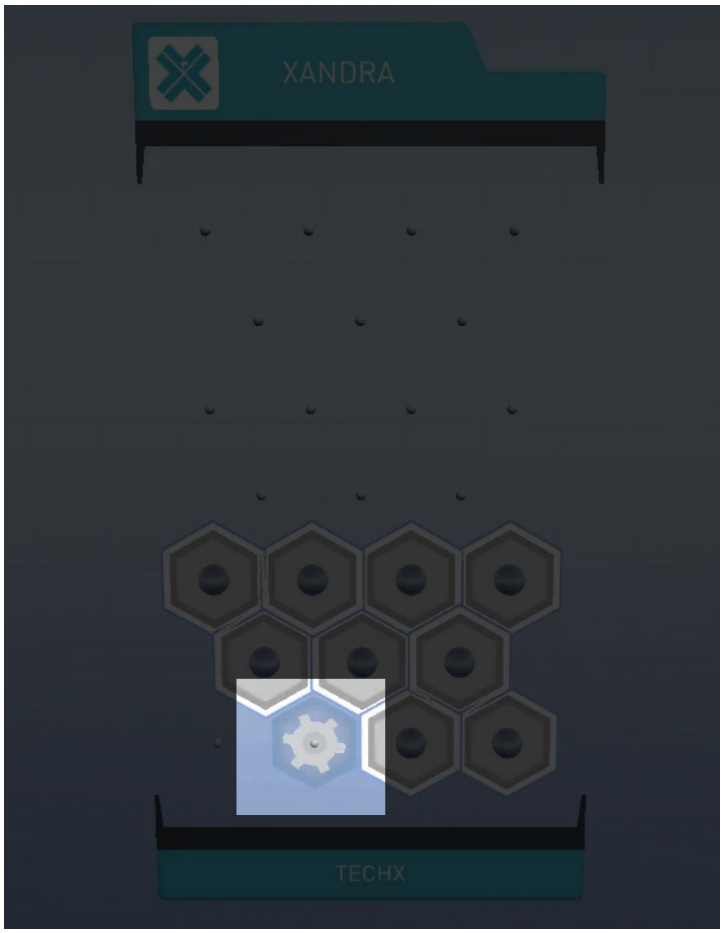


All Events:



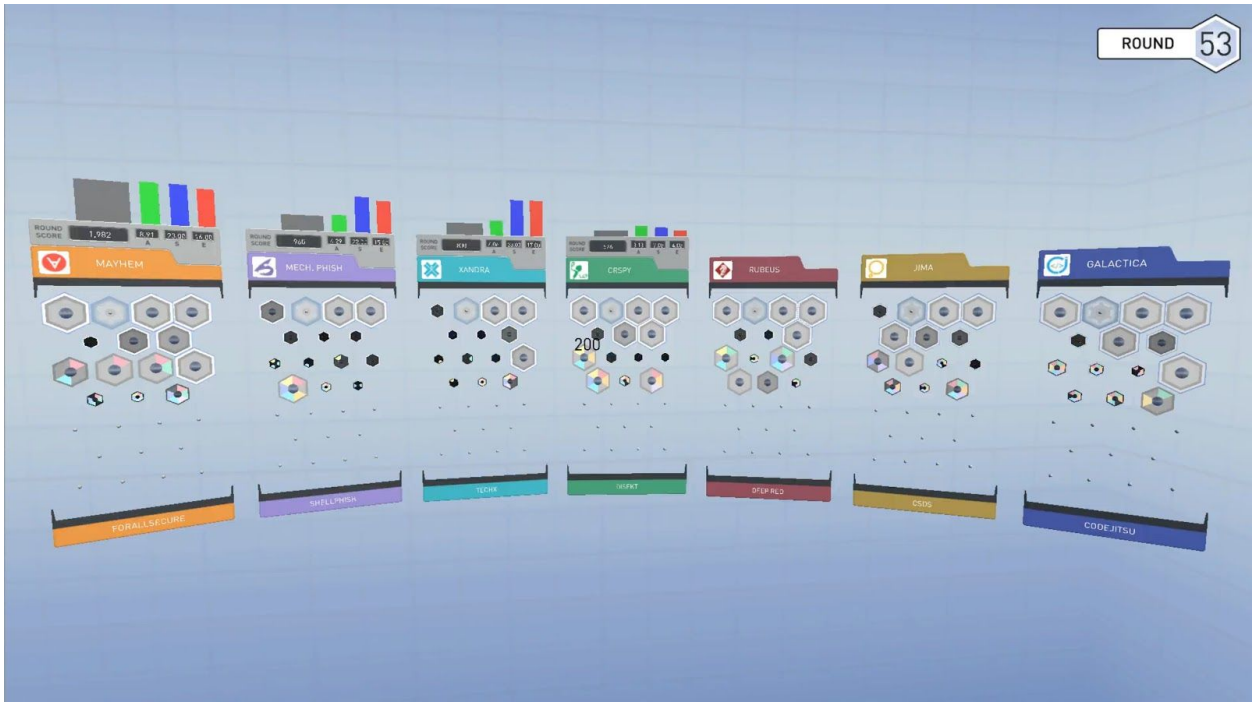
Network Defense Rules Present:

Service Down for Software Update:



Score Tabulation Sequence

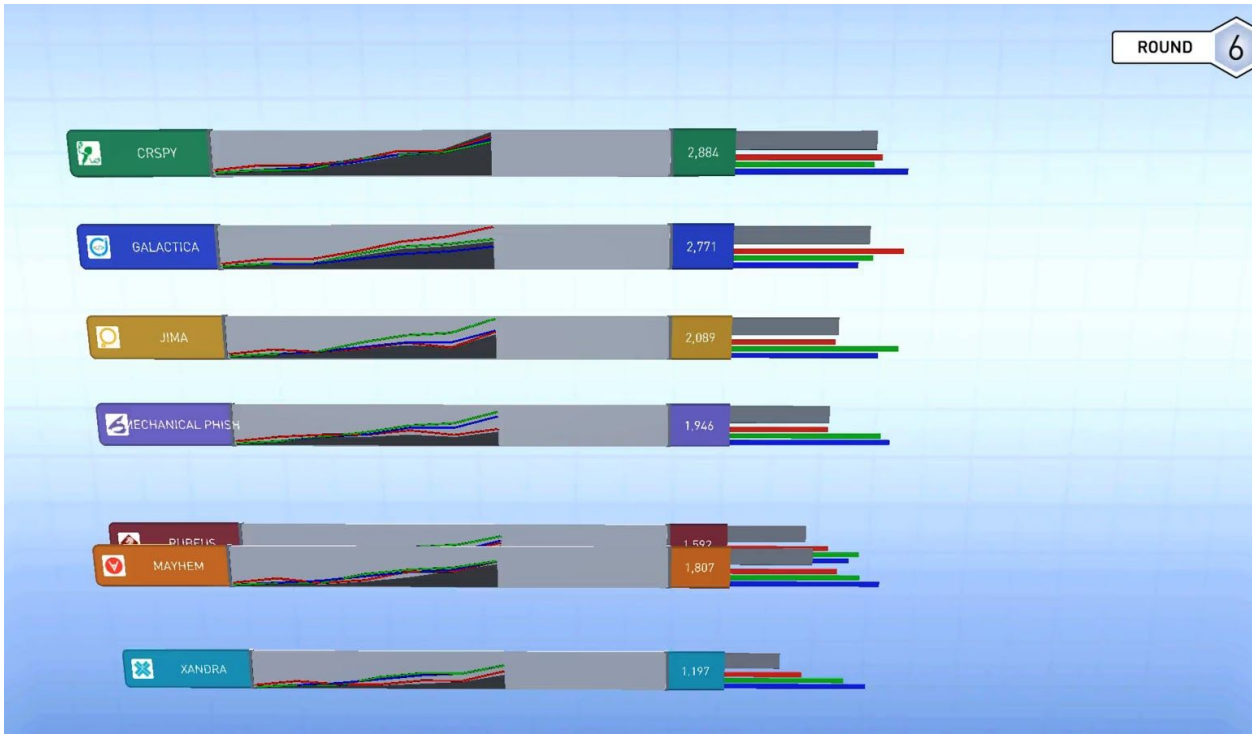
The Score Tabulation Sequence happens at the end of the Arena View Round Replay. Here, after a round's activity has completed, we tally up the results of the round for each CRS. First we convert the results of the Round Replay into a total score per CS. Then we sum the scores for all the individual CSs to get a total score for the round. We also tabulate totals for the A, S, and E scores individually. Total Overall Score is represented by a number and by a gray bar graph. The CRS with the largest score for the round has a gray bar graph of maximum size, and the other CRSs' gray bar graphs are scaled to match the proportion of their scores to the round winner's score. Total E, A, and S scores are displayed by numbers and by red, green, and blue bars respectively. Again, the CRSs with the largest E, A, and S scores will show maximum sized red, green and blue bars, and the other CRSs' bars will be scaled down to match the proportion of their scores to the round winners' scores.



#2 Scoreboard

Score Bars

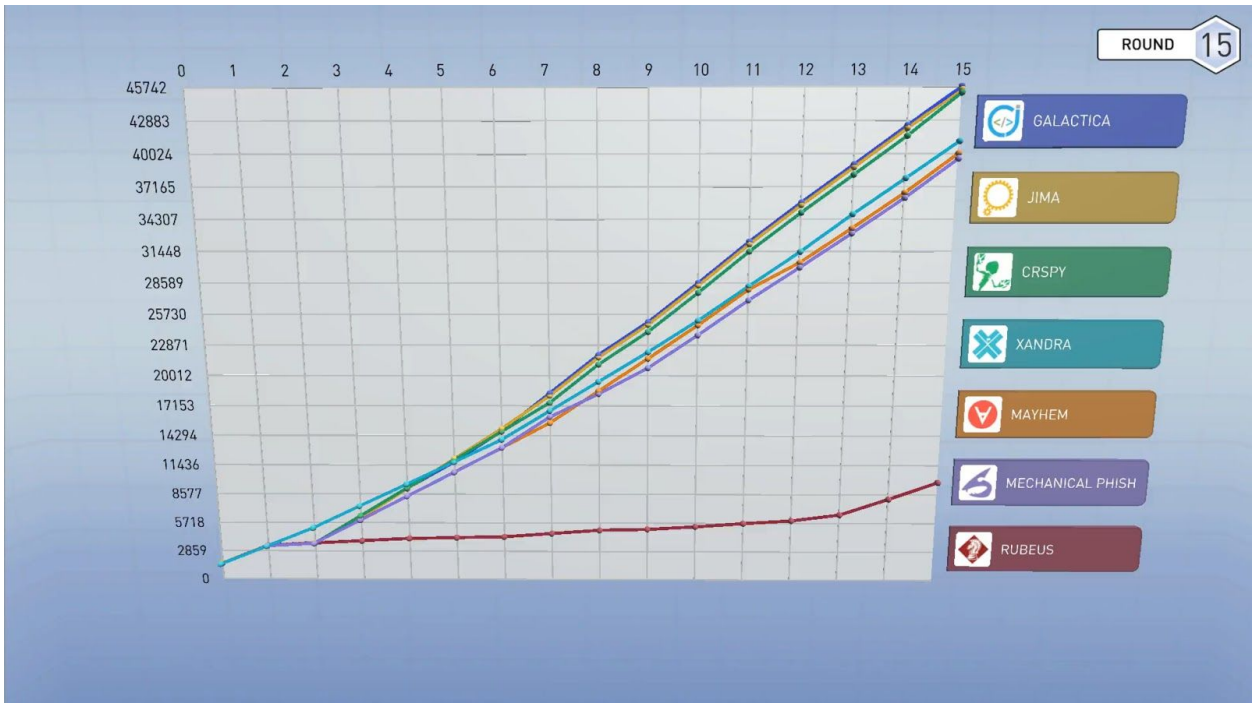
This view shows the overall score of the game. We intend to automatically generate a new score bar sequence video for each round. In each of these auto-generated videos, we will start with the score up to that round, add the scores for the round that just finished, and show changes in rank if they occur. To the right, we see bars whose length correspond to total Overall Score (gray), total E score (red), total A score (green), and total S score (blue) to this point in the game. The line graphs in between the ends of the score bar shows total score per round as a gray filled line graph and total A, S, & E scores per round as colored lines. We can also generate on demand a Score Bar Sequence from any round to any round.



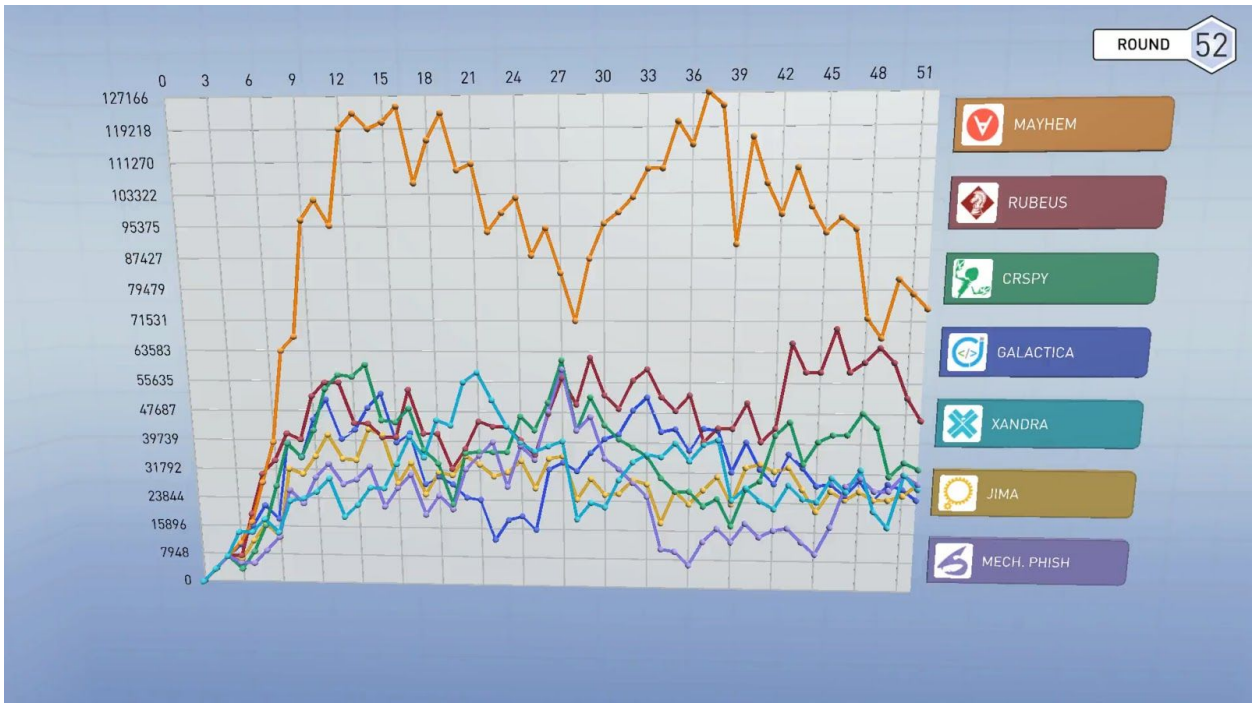
Graph Views

This easy to understand view is generated after each round and shows

a) Cumulative score as the game progresses



b) Per round scores as the game progresses



#3 CS Card View

This view is comprised of a cluster of shapes that is procedurally generated based on a series of properties inherent to a Challenge Set. We've set this up such that CSs which are similar (e.g., a CS and a replacement to the same CS) are guaranteed to retain similarities, but will also differ in some ways. We are currently using file size to determine the number of components of a shape; a bit stream created from a combination of the CS name (95%) and the file hash (5%) determines the arrangement of shapes within a cluster and the base color of the cluster; the opcode histogram determines a color pattern that translates across the surface of the shape cluster; and the entropy determines the sharpness (low) or roughness (high) of noise applied to that color pattern and the density of the black and white checkerboard pattern in the upper left corner. Using these properties ensures that the overall silhouette and color of a CS and its replacements will remain similar while other features will differ enough to be noticeable.

The "card" part of the view is a UI housing that presents various details about the CS in question:

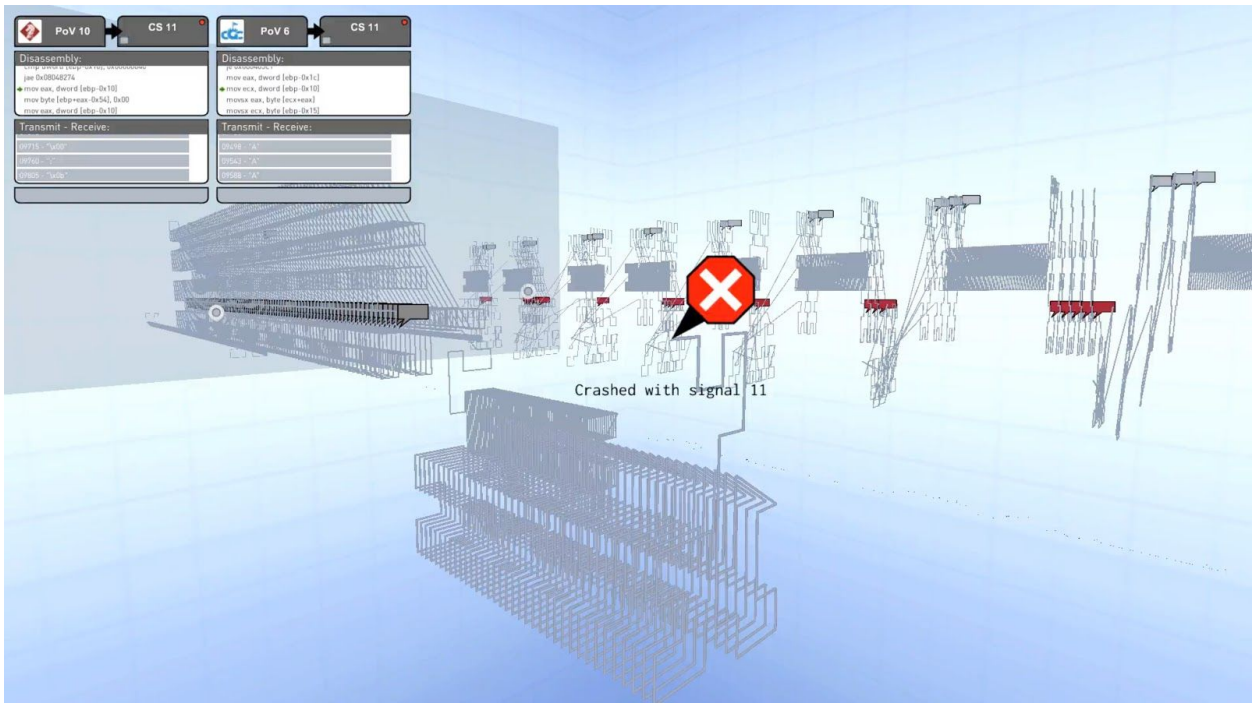
- Short Name
- Short Description
- Binary Section Types and Flags
- Filesize
- CWEs present in reference CS

This view will be used to introduce and compare the CSs used in the event. A CS Card can be visualized alone or within another visualization (e.g. in Arena View during the Inter-Round Sequence when CSs are introduced for the first time or in Filament View to describe the CS being visualized handling requests).

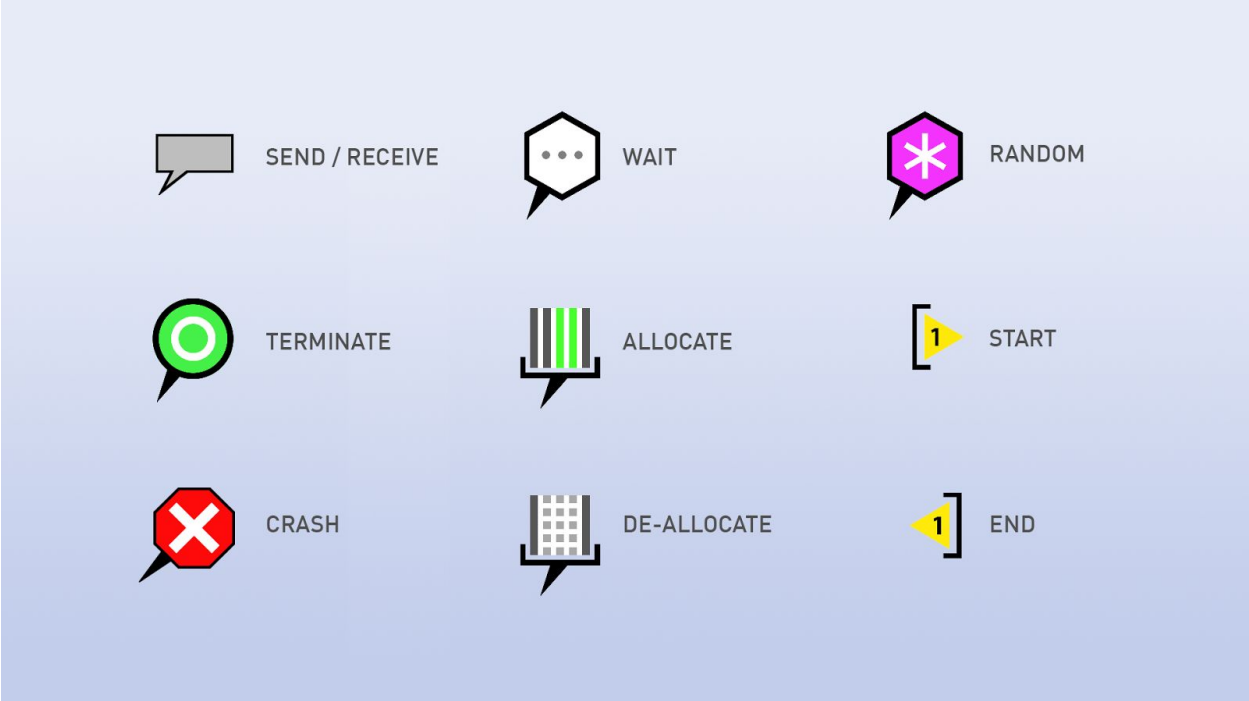
#4 Filament View

This is the view we use most often to illustrate stories that we find in the Story Finder tool. In Filament View, we show a representation of the instruction pointer crawling through an execution of a binary thereby "tracing" a "filament" in 3D space. So for example, we might compare a CS that has been replaced by a CRS to the original CS that was presented by the game as the author wrote it. Both CSs might try to handle a PoV, and perhaps one crashes against the PoV and the other successfully handles the PoV and avoids the crash. We can support comparing up to 4 traces at a time, which allows us to compare a 2-binary CS with a replacement to the same CS. We also have several tools for pointing out interesting happenings within the trace:

- Annotation icons call out specific events within the trace
- A Dis-assembly Window shows a text output of what the binary is doing instruction by instruction
- A Communications Window specifically focuses on Transmit and Receive events resulting in a "communication" between the CS and a request (i.e., a Poll or PoV).

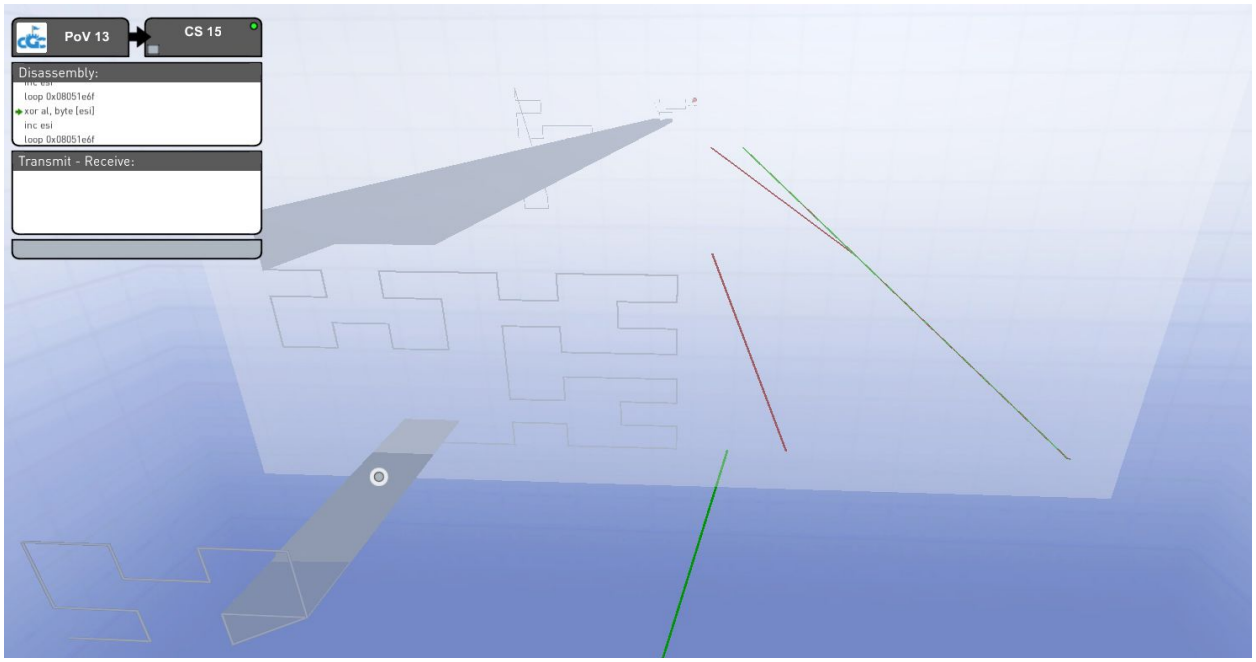


Annotations:



#5 Memory View

Memory View illustrates memory allocations, de-allocations, reads, and writes made by the binary as it handles a request. It appears alongside an instruction trace in Filament View. Allocations are shown as strips of colored space that appear next to a filament as the cursor (a plane with a highlighted dot on the trace itself) moves from one end to the other. Each new allocation is assigned a different color. Specific colors do not signify anything in and of themselves; they are only meant to distinguish one allocation from another. Reads and writes appear within the allocated memory as white or black blocks as the cursor moves along the trace.



#6 Cube View

In this view we can map any three properties to the three axes of a cube. Most commonly we use A, S, and E scores. We then show a series of these cubes mapped in a grid whose X and Y axes can be any elemets of the game, such as teams and CSs for a round.