Google's Gamified Threat Model Colony Has Engineers Working Together to Fight Threats

Google and Plum eLearning

Best Unique or Innovative Learning and Development Program

November 2021

Company Background

Company-at-a-Glance	Google
Headquarters	Mountain View, CA
Year Founded	1998
Revenue	$180 billion
Employees	135,000+
Global Scale	Global
Customers/Output, etc.	Online advertisers, cloud software and services
Industry	all
Stock Symbol	GOOGL
Website	www.google.com/about

Company Background

Company-at-a-Glance	Plum eLearning
Headquarters	Encinitas, CA
Year Founded	1999
Global Scale	Primarily the US and the UK
Customers/Output, etc.	Plum eLearning designs and develops eLearning courses for corporate, government and nonprofit clients. Plum's services include training needs analysis, instructional design and eLearning authoring.
Industry	Training
Website	www.plumelearning.com

Budget and Timeframe

Overall budget	$180,000
Number of (HR, Learning, Talent) employees involved with the implementation?	One
Number of Operations or Subject Matter Expert employees involved with the implementation?	Six
Timeframe to implement	Eight months
Start date of the program	April 1, 2020

Business Conditions and Business Needs

Google's Security Education team wanted to reduce potential software vulnerabilities through use of a process called Threat Modeling. Threat Modeling is an industry practice whereby software developers and project managers analyze the flow of data through products and services, creatively think about what could go wrong and come up with mitigation strategies. Threat Modeling is not a process that can be done solo; it is best conducted with teams in a live discussion.

Overview

The team started its mission by recruiting facilitators to conduct instructor-led training (ILT) sessions. They quickly realized that this approach was limited, for several reasons:

- **Scalability.** Coordinating dozens of training sessions for hundreds of engineers across the country proved to be a daunting task.
- **Facilitation skills.** This would probably not surprise experienced trainers, but it turned out that subject-matter experts (SMEs) recruited as facilitators weren't necessarily capable of producing the kind of robust, collaborative discussion that a productive Threat Modeling session requires.
- **Participation.** Participants weren't always taking ownership of the brainstorming process, but rather seemed to be waiting to be told the answers. Or, one or two people might dominate the discussion while others stay silent.

Pivoting to virtual training (VILT), as so many organizations have done during the pandemic, could help with scalability but it wouldn't improve the quality of the threat models produced during these sessions. So, the Security Education team came to Plum eLearning with a proposed solution: They had designed an online game. In the game, teams would have to develop their project while also fortifying their defenses against common threats and vulnerabilities. Just like in the real world, only more fun.

The game is designed to be conducted either in person and/or over videoconference (VC), so teams with geographically distributed members or members who are working from home can all play together.

The game was effective because it addressed each of the issues that were presented with the ILT:

- **Scalability.** Teams could play the game any time they could schedule a couple of hours together and there would no longer be any travel costs.

- **Facilitation skills.** Facilitators are no longer needed; the game walks players through the threat model process step by step.
- **Participation.** Players register so that the game can prompt each player, balancing participation with questions relevant to their role.

Design of the Program

The following were the key design considerations:

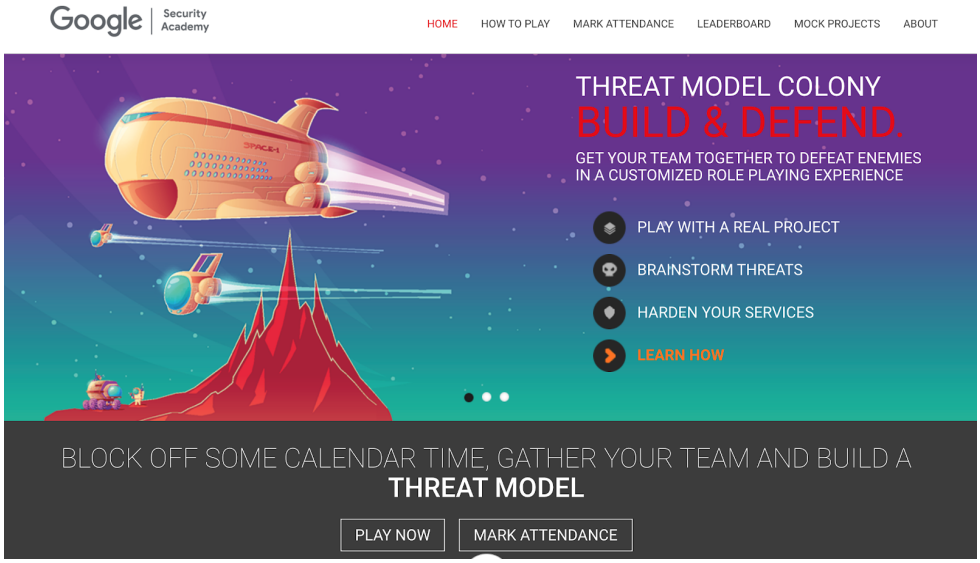
- The Security EDU team wanted players to bring their real-life engineering projects to the game. These projects would become the focus of the gameplay. In this manner, players learn threat modeling by doing it in real-time with a project they already know intimately. This is unique in that most education programs are based on hypothetical decision-making about fictionalized scenarios.
- The game would need to capture all the players' discussion items and notes and effectively produce a "threat model" document the employees could save at the end of each session and use to address the vulnerabilities they uncovered.
- The game needed to create a psychologically safe place for hard discussion and be fun enough for people to enjoy so they would recommend others and play again. It is rare that training programs are considered fun!
- The game would need to be flexible by both customizing itself in difficulty level based on the characteristics of the project the players brought and by giving players control over what security, privacy and abuse topics they felt most relevant to their work.
- The experience needed to be effective for two very divergent groups of employees:
  - Brand-new (week 2) employees going through the onboarding process with assigned starter projects
  - Standing engineering teams, working across fields as distinct as Android phones and self-driving cars, to Google Maps and Search
- The game had to serve employees with both technical and non-technical roles (e.g., engineers and non-engineering program managers or designers).

To achieve these goals, the design team focused on these requirements:

Easy to play. While the game's goals from the Security Education team were ambitious, the experience had to be simple and easy-to-use right out of the box for players. Players need only to navigate to the game's homepage and click "Play Now." A quick onboarding flow then instructs them that the game is played by one person presenting their screen

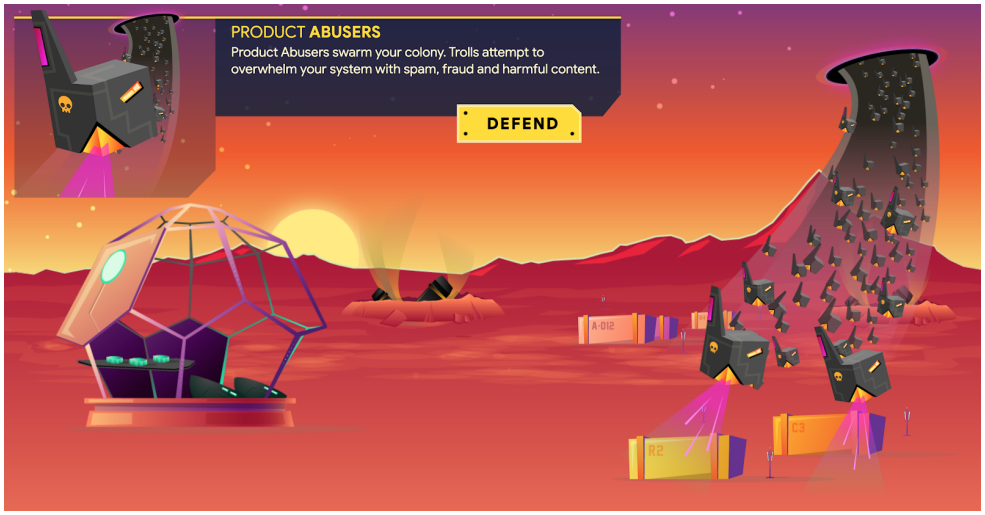
over VC so everyone else in the virtual meeting or in-person can watch and contribute. The game takes roughly 90 minutes.

Figure 1: Google Security Academy's Threat Model Colony: Build and Defend



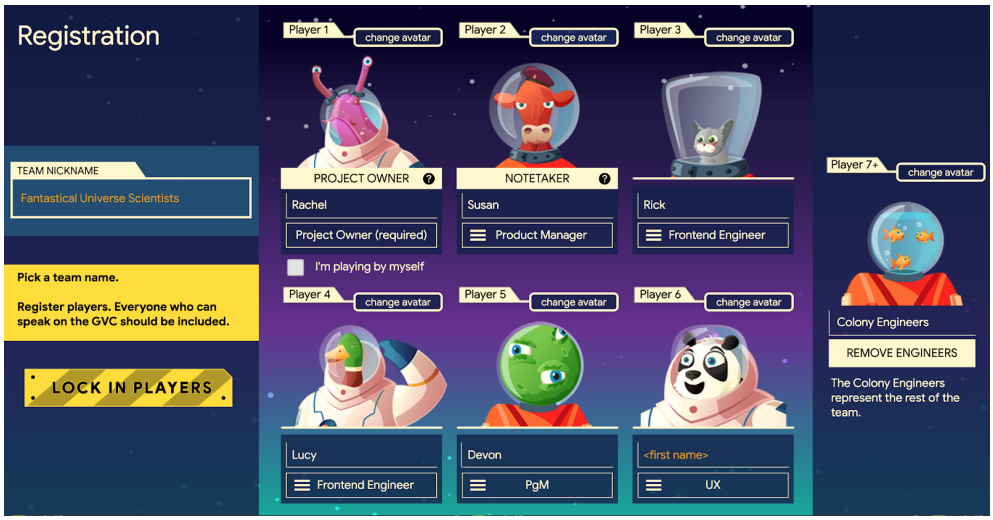
Theme. While the game employs a colorful Mars colony analogy where players assume the role of a team of robots, the analogy is intentionally "thin." While maximizing the fun, all the textual content describing the attackers emulates real-life threats and issues. This way players never lose sight of the fact they are playing the game to fortify their real-life engineering project.

Figure 2: Theme



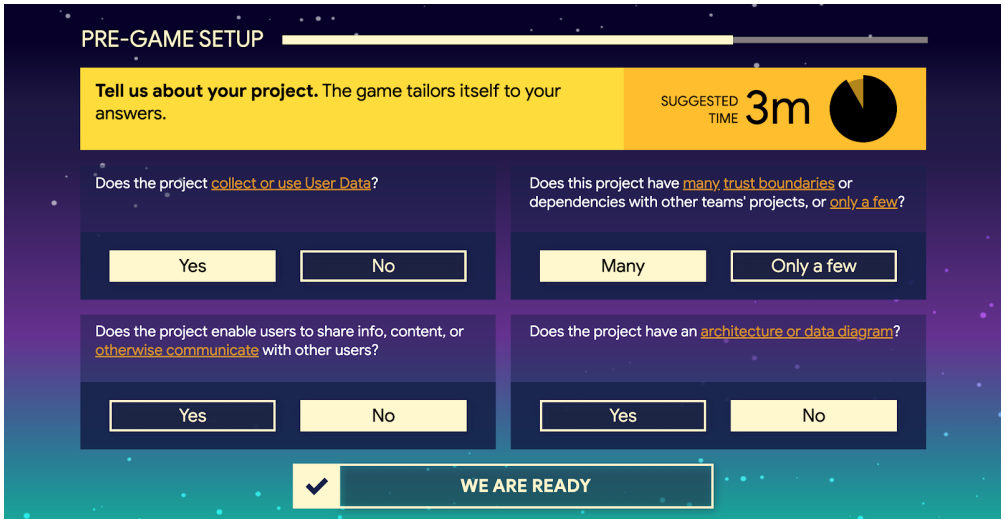
Inclusive players. Players choose not only their avatar but also identify themselves as technically or non-technically skilled employees by selecting from a dropdown of job roles. This way, the game will later customize questions that are a better fit for their skillset and knowledge level. Assigning players also has the benefit of ensuring that everyone in the team is called on at some point to contribute and one or two more vocal participants cannot dominate a session.

Figure 3: Registration



Flexibility and relevance. At Google, there's no "one size fits all" education treatment that can work across all its diverse teams and products. So the game asks a few questions and then customizes the enemy profile, game duration, and the question list for the actual project the players have brought. The game also offers mock projects for teams that want to play but have no project on hand.

Figure 4: Pre-Game Setup

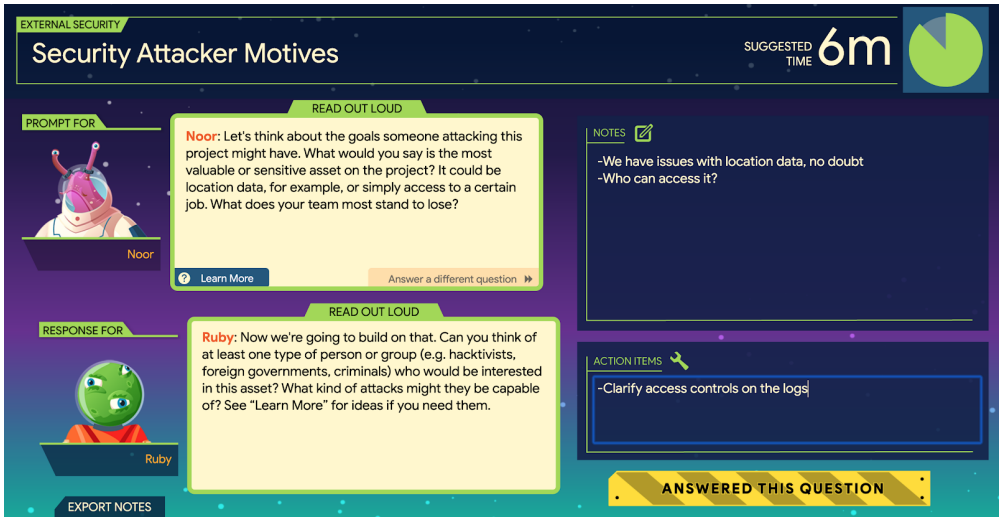


Tooltips and walkthroughs. New games with new rules take time to learn. After extensive testing, to ensure players never get stuck or waste time trying to figure out how to win, the development team built extensive overflows and tooltips to keep players on track.

Figure 5: Tutorial

Winning the game through discussion. The game has a resource allocation element where players must invest robots across their colony to ensure its survival but the core of the game is in the prompt-and-response sections where players are called on to read questions out loud and talk through potential problems. In the process, the person in the notetaker role takes notes and captures the "aha!" moments where players realize they have an issue they need to resolve. Those moments go in the "Action Items" section and are exported to their document at the end of gameplay.

Figure 6: Prompt



Engagement. To help spread the game virally, the game encourages players to submit their scores to the leaderboard and collect an internal employee badge at game end. While not required, most players do submit their scores and fill out an optional survey to collect a profile badge.

Figure 7: Leaderboard

	TEAM NAME	SCORE	EXTERNAL SECURITY	PRIVACY POSTURE	ABUSE MITIGATIONS	INTERNAL SECURITY	LAUNCH DATE	FEATURE PROGRESS
1	Not Adobe	68880	Pass	Pass	Pass	Pass	On Time	100%
2	BackToOffice	68757	Pass	Pass	Pass	Pass	On Time	100%
3	The Privacy Catastrophe	68511	Pass	Pass	Pass	Pass	On Time	100%
4	Crystal Cloud	67896	Pass	Pass	Pass	Pass	On Time	100%
5	Heroic Universe Guardians	67748	Pass	Pass	Pass	Pass	1 Week Delay	100%
6	The APJs	67650	Pass	Pass	Pass	Pass	On Time	100%
7	Heroic Asteroid Scientists	67404	Pass	Pass	Pass	Pass	On Time	100%
8	Heroic Planet Terrafarmers	66752	Pass	Pass	Pass	Pass	1 Week Delay	100%
9	Unpredictable Cosmos Pilots	66666	Pass	Pass	Pass	Pass	On Time	100%
10	Heroic Quasar Settlers	66420	Pass	Pass	Pass	Pass	On Time	100%
11	Uncanny Cosmos Explorers	66420	Pass	Pass	Pass	Pass	On Time	100%
12	Thrilling Quasar	66174	Pass	Pass	Pass	Pass	On Time	100%

All illustrations provided by Google and Plum eLearning

Delivery of the Program

Two versions of Colony were designed: one for new employees, who would be required to play, and the other for standing software engineer teams. For new employees, the EDU team performed numerous user tests to ensure a smooth delivery, employing calendar invites, pre-game emails and a tiered-badge system to encourage employees to both get excited to play and ultimately mark their attendance. For standing engineer teams, Colony was positioned as more than just an educational program — but rather as a remote team-building exercise that helps reduce the real-life pain of required security reviews for new launches. As a result, there has been a consistent amount of gameplays (about 20%) coming from standing engineer teams.

No updates or changes were made to the program in the first year; an enhancement was recently completed to facilitate the export of action items directly into Google's internal bug tracking tool (vs. copying and pasting notes into a doc for later retrieval). The goal of this enhancement was to ensure that teams follow up on action items, and thus generate even more tangible business benefits from the game.

Measurable Benefits

To date, after just under one year since launch:

- 8,720 players from 1,744 project teams at Google played the game
- 40% of teams voluntarily extended gameplay to continue their threat model sessions
- 14,424 actions items or bugs were generated to decrease or mitigate real-world software vulnerabilities.

One of most exciting elements for Google's Security EDU team is that this program measures real-life actions as a result of their education. Because players are learning by doing, they ultimately walk away with a series of action items or bugs they need to address — potentially disastrous bugs that could have cost Google millions if they had later been exploited. While the metrics show growth and excitement among employees, and survey feedback indicates players are enjoying the competitive nature of the experience and the psychological safety of poking holes in their own software behind a game narrative, what Google is most excited about is that this learning experience is reducing tangible risk by helping catch almost 15,000 (and counting) potential bugs in products through employee discussion and gameplay.

Overall

Threat Modeling was a practice that Google's internal research strongly suggested could improve the security posture of the company and reduce costly vulnerabilities. But no other approach — conventional use of facilitators, documentation, etc. — was able to integrate Modeling into Google's culture in a meaningful way. Threat Model Colony started as a moonshot, back-of-a-napkin idea to break that impasse. The program has gone on to be hailed as a groundbreaking success and has in turn up-leveled the approach even other teams at Google take toward educating employees, especially during work from home. Google has learned to take risks on unique and innovative experiences, especially for proposals that make use of social and interactive elements. And learning by doing is a huge value-add for teams that otherwise wouldn't take the time to play a game or engage with a "merely" educational exercise. By integrating the learning into an activity tied to their business objectives, the barrier to spend time playing the game was lowered and Colony attracted employees it otherwise would not have reached.

Threat Model Colony was ultimately more successful than the Security EDU team planned and they continue to plan its future as more teams play and use it. The game only recently unveiled the ability to export action items for players but there are also opportunities to

potentially externalize the game to customers, to build new skins and themes, and offer custom versions for different product teams. The EDU team is in multiple talks to do all these things and is incredibly excited to see what comes next.

About Brandon Hall Group

With more than 10,000 clients globally and 27 years of delivering world-class research and advisory services, Brandon Hall Group is focused on developing research that drives performance in emerging and large organizations, and provides strategic insights for executives and practitioners responsible for growth and business results.

Some ways we can help…

MEMBERSHIP PACKAGE

Includes research library access, events, advisory support, a client success plan and more.

ADVISORY OFFERINGS

Custom Research Projects, including surveys and focus groups interviews. Organization Needs Assessment for Transformation, Technology Selection and Strategy.

EXCELLENCE AWARDS

Global recognition showcasing leading programs and practices with a library of case studies.

PROFESSIONAL DEVELOPMENT

Virtual and on-site certification programs, workshops and webinars supplemented with research-driven assessments and tools.

ORGANIZATIONAL EXCELLENCE CERTIFICATION PROGRAM

recognizes world-class HCM programs that transform their organization and achieve breakthrough results. This designation is the next step beyond the HCM Excellence Awards, which focus on a single program, and looks at the department as a whole.

SMARTCHOICE® PREFERRED PROVIDER PROGRAM

uniquely places HCM service and technology companies at the top of organizations' consideration list of vendors. It adds an unmatched level of credibility based on BHG's quarter of a century's experience in evaluating and selecting the best solution providers for leading organizations around the world.

HCMA PROFESSIONAL CERTIFICATIONS

are comprehensive educational programs that center around a multiphase knowledge test.