Let's Play AI Supply Chain Candyland

Here is where your AI supply chain adventure begins...

Rules of the Game

01.

Object

Make and save money securely using AI (time is money)

02.

Contents

1. Continuous feedback loop for AI systems
2. Lots of references to a board game about candy with an tech spin

03.

How to set up the game

Familiarize yourself with the continuous feedback loop personas and identify where you fit in

04.

How to play the game

Become aware of all the people who will participate in AI with whom you may never personally interact. *Bonus*: Think about how this might get implemented across your organization

05.

How to win the game

Build on what you already know to develop a new understanding for how people, process and technology connect in the AI supply chain

We are your guides in this adventure

Sarah Evans

Cyber Sarah, Technology Superhero

“To CICD infinity loops, and beyond!”

CRob, n, adj, and v

Pronunciation: U.S. (K-rowb)

43rd level Dungeon Master

26th level Securityologist

Pirate-enthusiast & hat-owner

01

Object

Make and save money securely using AI (time is money)

Open Source accelerates technology

Open data, open models, shared languages, shared tools, open software

Proactively Secure Open Source in AI

Components for building AI will create supply chains that must be secured, just like we learned reactively with classic open source software.

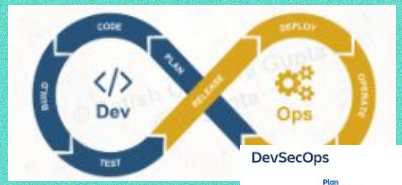
02

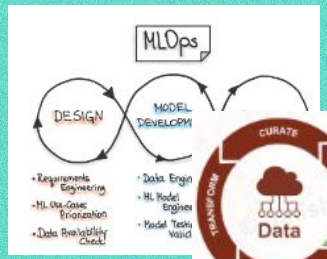
Contents

1. Continuous feedback (infinity) loop for AI systems
2. Lots of references to a board game you might have played as a child about candy…but with a tech spin.

The industry needs an aggregated view of the interaction between a variety existing examples continuous feedback loops

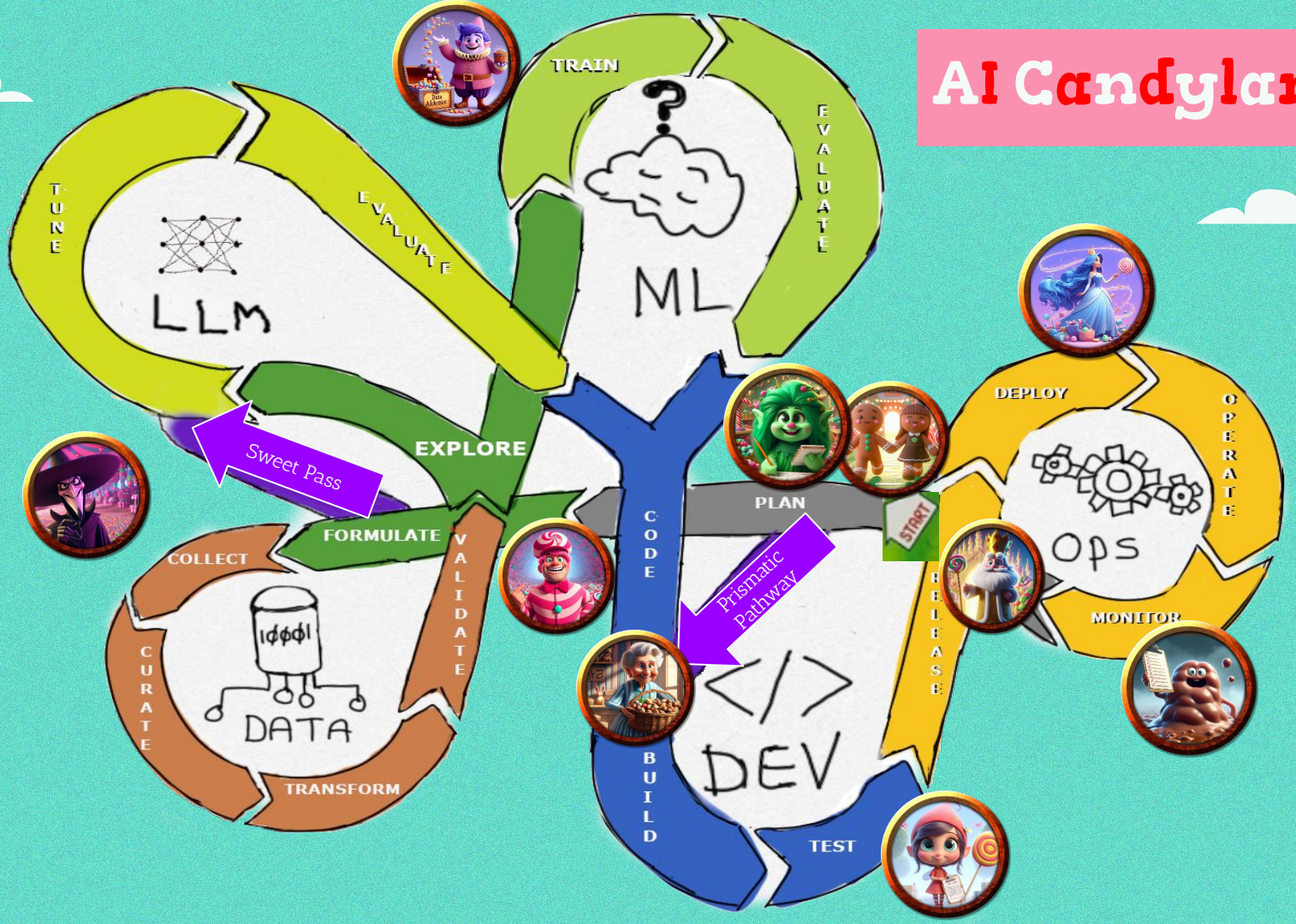
DevOps -> DevSecOps **MLOps -> MLSecOps** **LLM Ops -> LLMSecOps**





These images illustrate the challenge; subject to copyright
DevSecOps: MLOps/DevOps:MLforDevs, LLMOps: Image search

AI Candyland



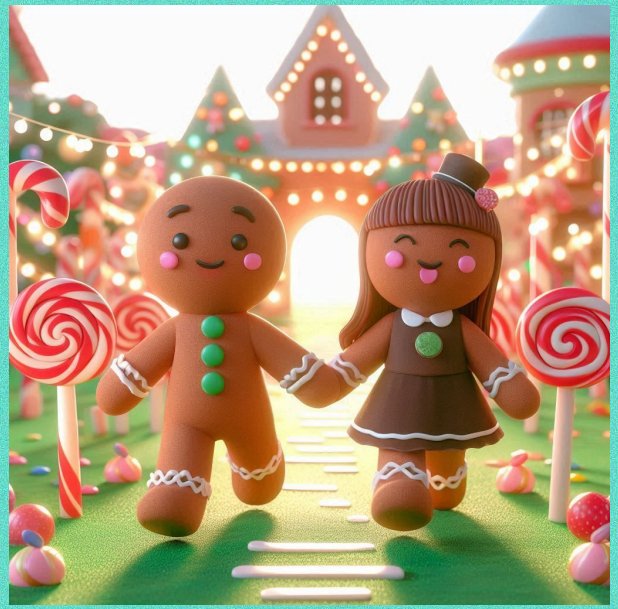
03

AI Candyland

Everyone likes candy!
Let's learn about our AI Supply Chain Personas, and their roles in the continuous feedback loop

Many of the following images are generated by AI. It's an AI talk right?? My model was still studying for its spelling test).

Secure AIML Supply Chain Trailblazers



Plan

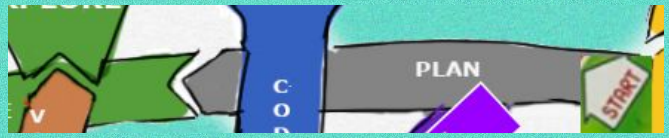
Let's go on an AI adventure, hold hands and start dreaming meeting the Sire of Secure xOps at the Sweet Success Citadel - how to use secure xOps to make or save money with software, or a combo of software + ML and LLMs.

Head toward the Confectionary Plan Orchard

Plan

Use cases.

As we take our first steps towards **Confectionary Plan Orchard** ...



What are all the amazing ways we can use AI to save time and money....and make money?

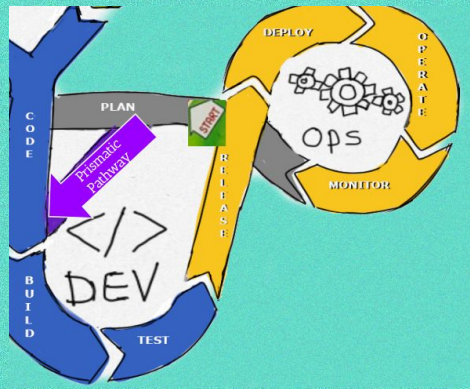
Shortcut opportunity: Prismatic Pathway

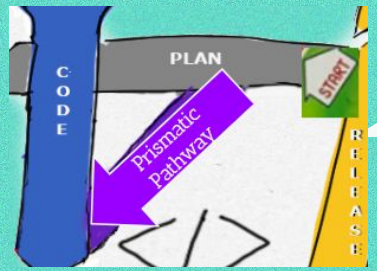
Plan

Software only: Doing classic software development PLAN *without* ML or LLMs?

Enjoy the sunshine and rainbows. Shortcut to the Prismatic Pathway for you.

Don't forget to threat model.



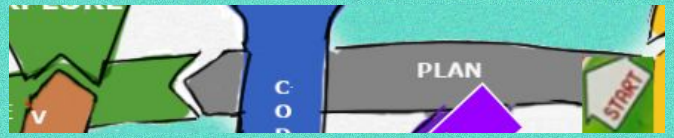


Poppy the Planning Elf

Plan

If you didn't take **Prismatic Pathway** , continue your adventure towards using AIML. Here's where you'll meet **Poppy the Planning Elf** in **Confectionary Plan Orchard**

ML Threat Model

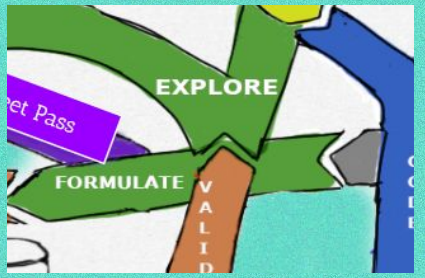


LLM LLM Model selection,
Prompt Engineering,
Threat model

The Peppermint Forest of swirly-twirly dependencies

Design

There so many dependencies to consider during the **Design/Explore** for ML/LLM. Let's continue into the **Peppermint Forest** to keep exploring.



ML Threat Model

LLM LLM Model selection, Prompt Engineering, Threat model

Peppermint Planning Engineer

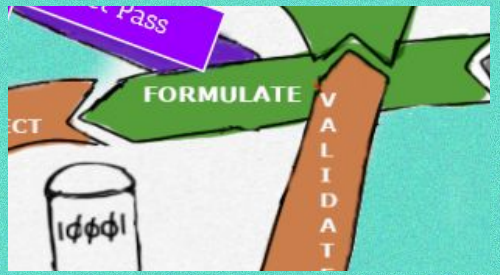
The OpenSSF's SLSA, GUAC, protobom/bomctl, Baseline, Scorecard, and BEST Practices Badges all help!

ML - Design

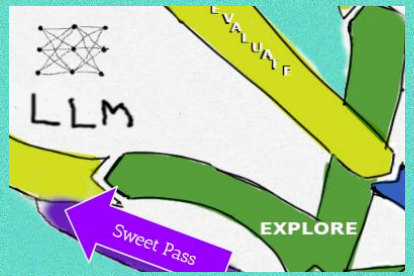
Formulate, use case prioritization, requirements engineering, data availability check

So many swirly twirly dependencies:

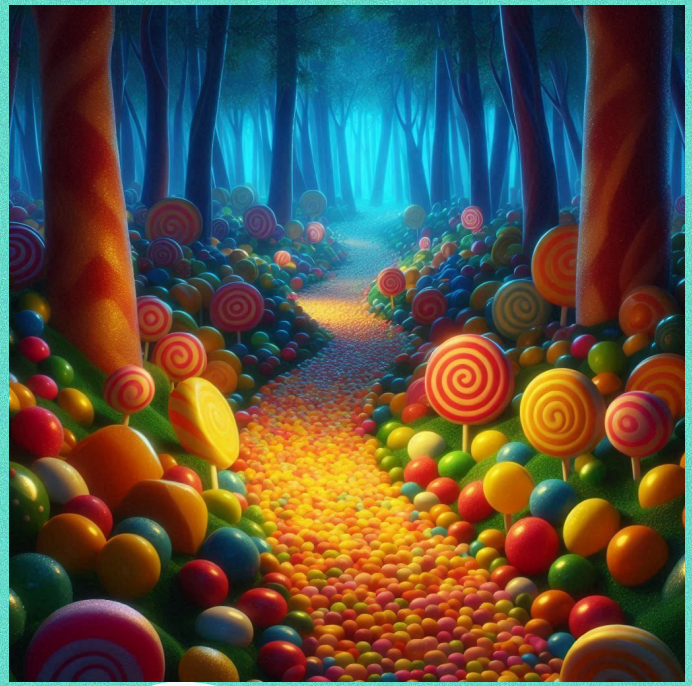
- Requirements
- Cohesion
- Traceability
- Constraints
- Algorithm choice for model **design** and methods in LLM **exploratory** analysis
- Computational resources
- Domain knowledge



LLM - Explore, Exploratory Data Analysis



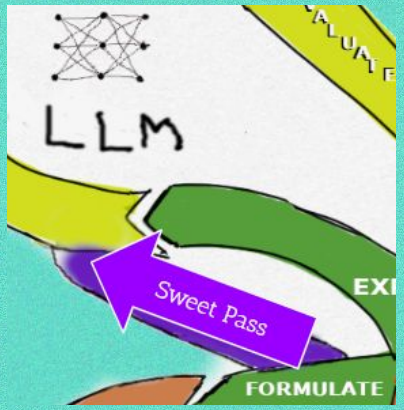
Sweet Pass



A sweet shortcut to the **LLM** loop

Take **Sweet Pass** to leverage advancements through LLMs allow some use cases to skip training a model

Move instead to the fine tuning LLM and creating RAG vector databases



Data Overlord

Can seem like a *villain-ous* experience

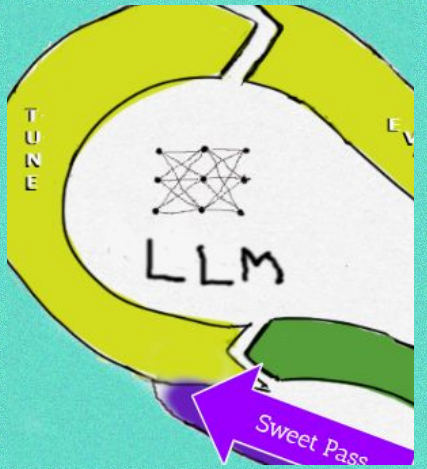
Challenges require a combination of technical skills, domain knowledge and strategic planning to overcome

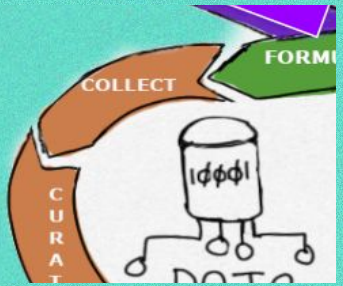
LLM Tune

The **Data Overlord** can strike also when you are even if you used the LLM **Sweet Pass** **shortcut** .

.

Data Collect, Data Engineering



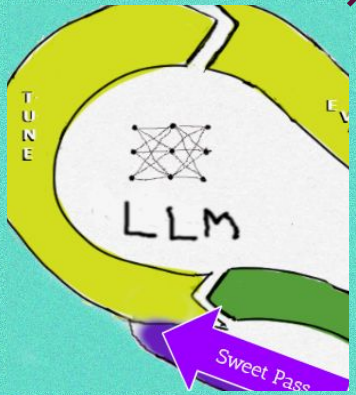


Data Silo

Beware of the **Data Silo**

Do you have the data you need? Is it clean, organized, correlated? Do you have data set provenance?

- Limited Data Access
- Inconsistent Data
- Communication Barriers
- Costs
- Compliance
- Data Integration
- Analytics

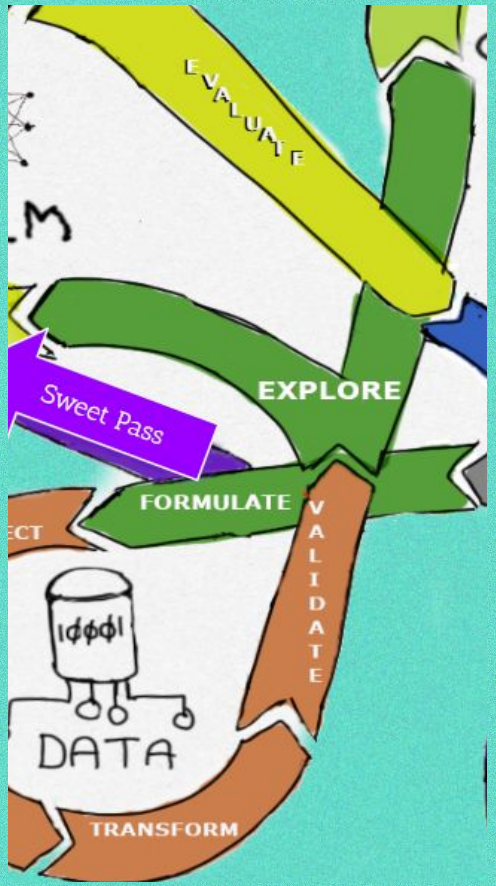


Head toward the Magical Model Mountains

Data Transform, Validate
ML Explore

This is just a *mountain* of work.

- Preprocessing,
- Data Versioning
- Storage
- Splitting
- Data Pipeline Automation
- Monitor
- Governance
- Feedback Loop



Data Alchemist

ML Model Training,

The **Data Alchemist** waves us over as he joyously turns data into models.

- Model Selection
- Model Training
- Evaluation
- Model Validation

Stuck in sticky sweets

The OpenSSF's sigstore can help with simple and fast signing

Validate

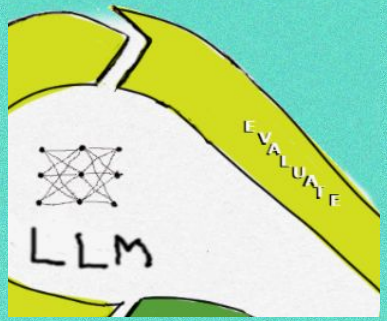
Everyone will land on this square

ML Model Validation

LLM Inference Testing

No moving on to to the next stage until your model is performing as desired.

- Deployment Readiness
- Model Signing
- Maintenance

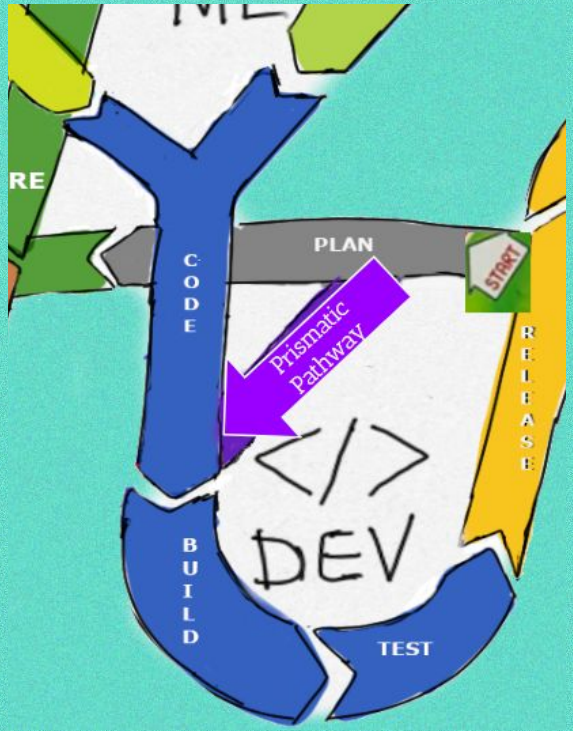


Head toward the Lead Programmer's Lodge

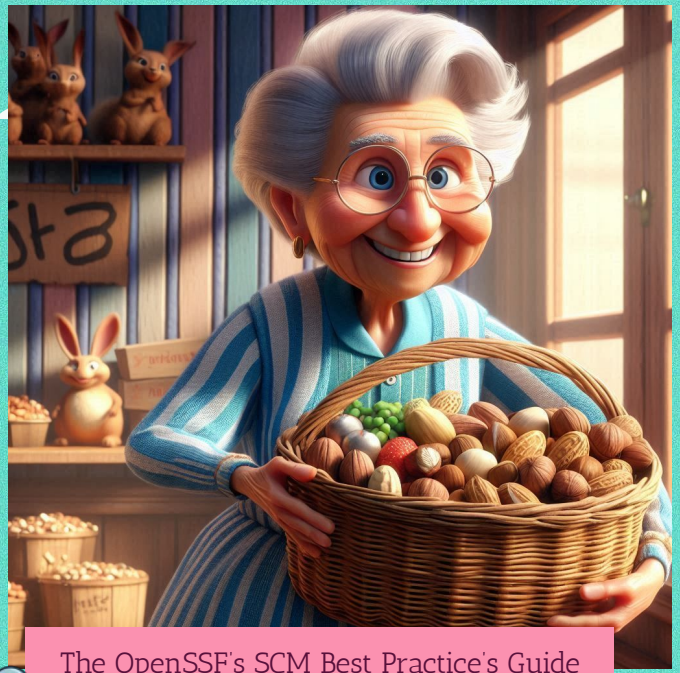
Dev code/build

Get ready to start the continuous development cycle!

Up next,: meet our software development team



Granny the Senior Software Engineer



The OpenSSF's SCM Best Practice's Guide helps with securely configuring major source code mgmt systems. Also GUAC and tools like Github's Dependabot are great for dependency mgmt

Dev Code and Build

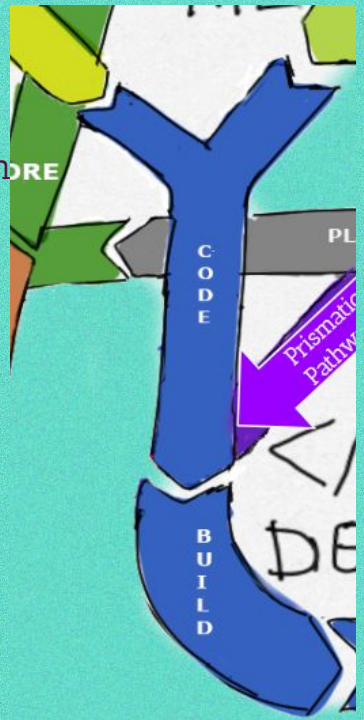
Granny the Senior Software Engineer happily awaited our arrival.. We are ready to put code around our data and model on our AI application journey.

Code

- Version Control
- Code Review
- Documentation

Build

- Automation
- Dependency management
- Compilation



Head toward Quality Assurance Forest

Dev Test

Now, let's test our functioning AI model, the data it will process, our code and build prep. Onward, to the Quality Assurance forest !

Did you get Lost in Quality Assurance Forest?

Are your CICD pipelines integrated to test ML/LLM/Dev use cases across the organization? Do your MLOps LLMOps know how to hand off to DevOps teams?

This is new for everyone operationalizing AI. It's not hard to get **Lost in Quality Assurance Forest**

- .Unit Tests
- Integration Tests
- Automated Testing

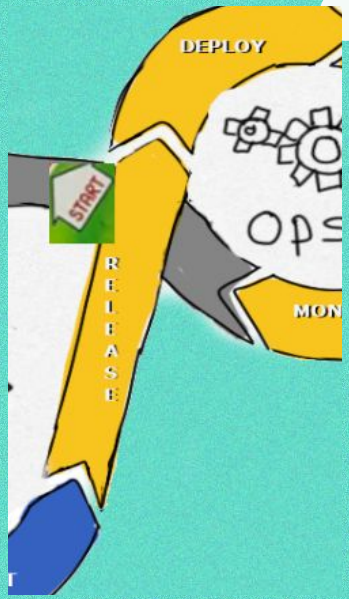
The OpenSSF's SLSA is a way to understand how to securely configure CI/CD pipelines and secure artifacts

Lollipop Code Maven

Ops Package

Lollipop Code Maven welcomes us to Package, nearing the final part of our journey. AI components (data sets, models,) should be included in Package stages that before AI only contained code artifacts.

- Artifact Creation
- Versioning
- Dependency Management
- Metadata
- Containerization
- Artifact Storage
- Security
- Distribution
- Testing
- Feedback Loop

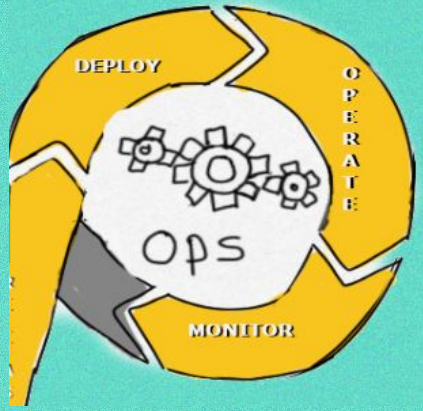


Head towards Frozen Dessert Deployment

Ops

Continue towards **Frozen Dessert Deployment** to activate the next Ops stages: Deploy and Operate.

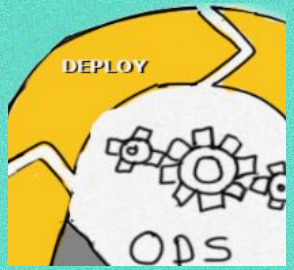
I can almost taste the sweet success!



Royal Release Manager

Ops Deploy/Release

The Royal Release Manager greets us warmly. She waves her candy scepter. Let's Deploy! Excitement fills the air.



Deploy

- Automation
- Environment Management
- Deployment Strategies
- Configuration Management

Head towards the Fudgy Swamp of Compliance

Ops Operations, Monitor

What's that smell? The last of the celebratory glitter silently lands around us.

It looks like we are headed straight into the **Fudgy Swamp of Compliance.**

Operate and Monitor

- Monitoring and Logging
- Incident Management
- Performance Management
- Security Management
- Backup and Recovery

Stuck in the Fudgy Swamp of Compliance

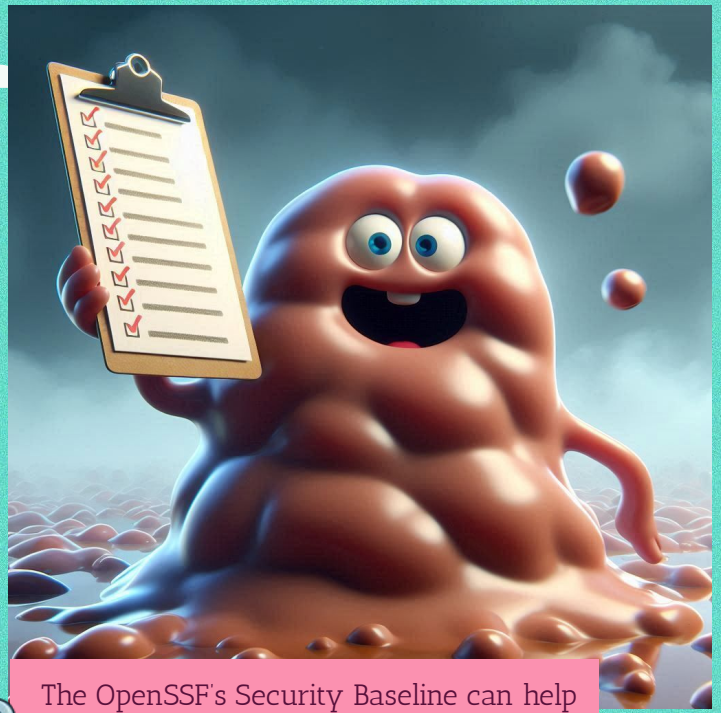
Ops

Monitor

Oh no! Our product might have used vulnerable OSS model. A popular model we deployed on a device in production to customers was poisoned with a dangerous backdoor and their legal insists they stop using it immediately.

Customers are eager to know if their device is affected and when we will have a new model/patch. Is it hot in here to you? Yes...because you are stuck in the **Fudgy Swamp of Compliance** .

Gloopy, Vulnerability Beast



The OpenSSF's Security Baseline can help give you guidance on minimum expected security practices and requirements. Minder provides a policy-based way to enforce desires security practices

Ops

Monitor

Checklist in hand, here is **Gloopy, the Vulnerability Beas** t. How can we use data from throughout the AI supply chain to effectively and efficiently provide Vulnerability Incident Response for software *and* ML/LLM components?

The **Fudgy Swamp of Compliance** steams and bubbles quietly around us. We check our dependency inventories, which we now understand should to start including data and AI components *and* with code to prepare for the inevitable AI supply chain attacks and risks.

Sire of Secure xOps Outcomes

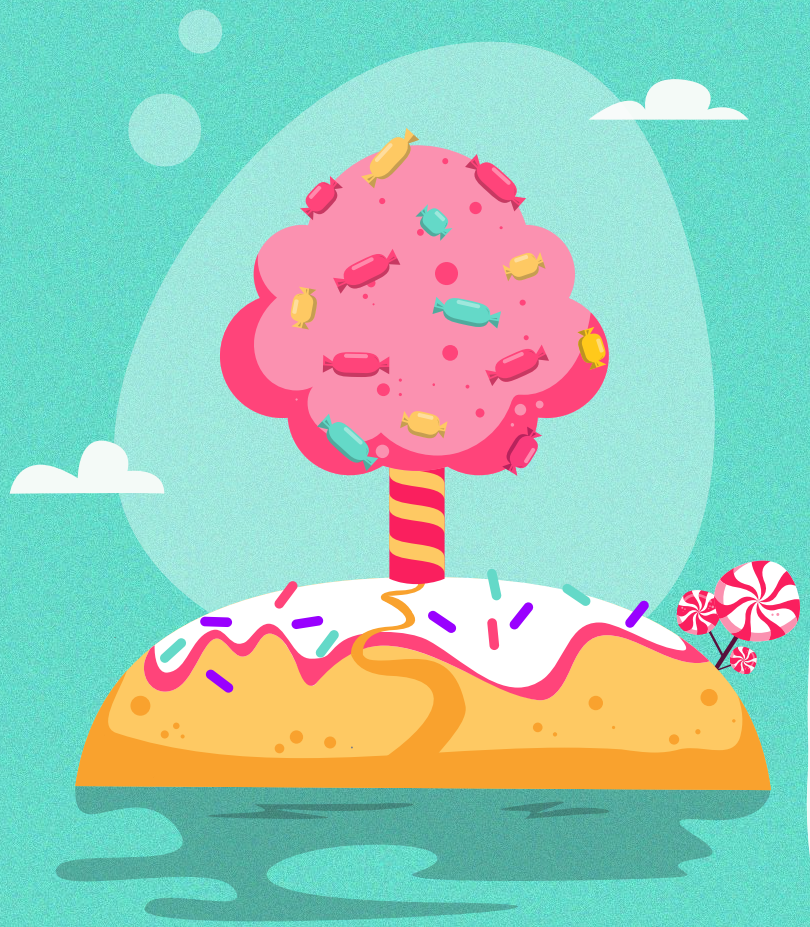
Customer Value unlocked! Making money….saving money with AI! That's sweet!

You found the **Sire of Secure xOps Outcomes** .. He lives in a citadel made of sweets.

Arrive at Sweet Success Citadel

Cheering breaks out! You've arrived at **Sweet Success Citadel** .

But guess what, our gameboard is an Infinite Loop/Eternal Knot!



04

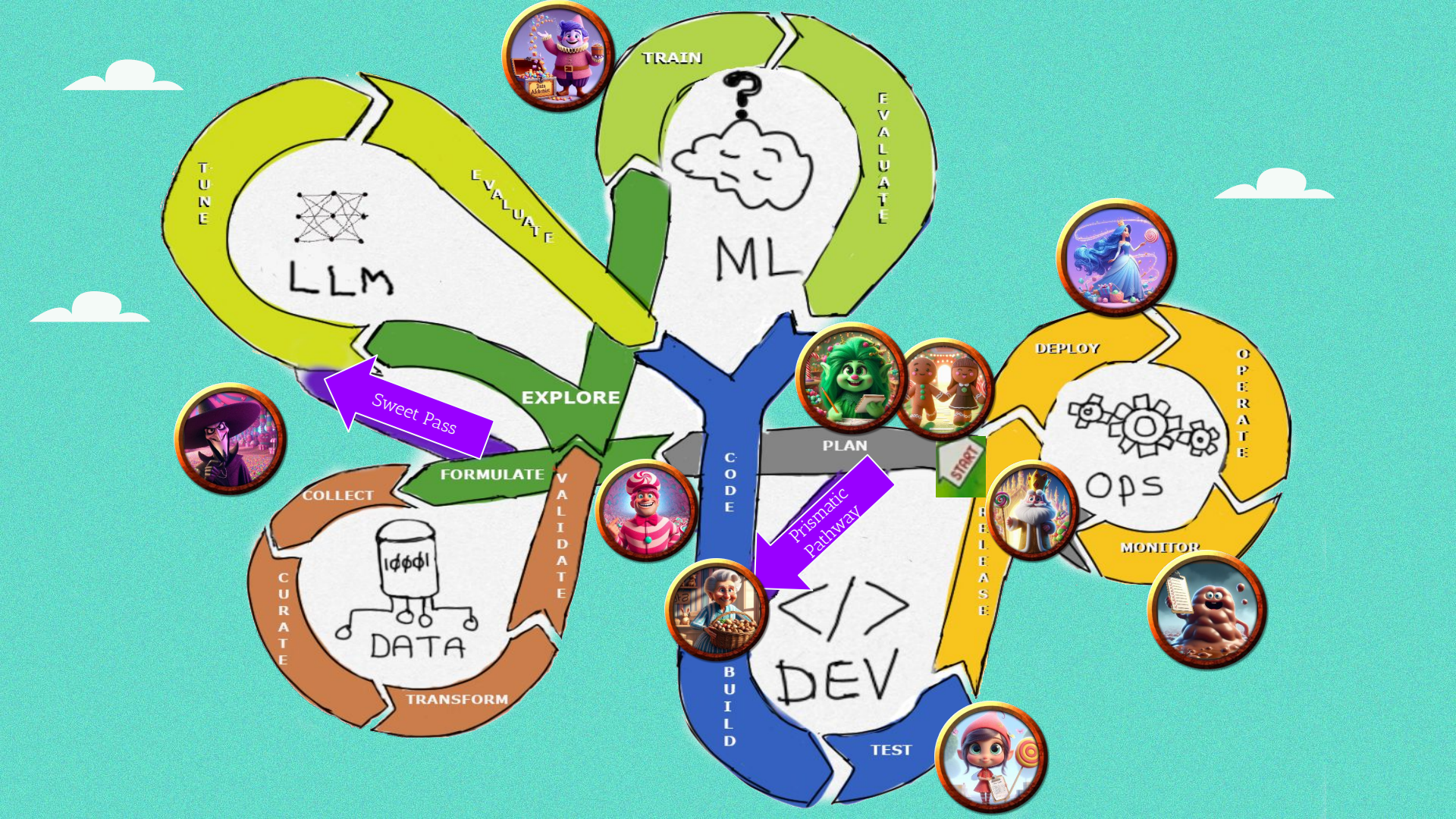
How to Play the Game

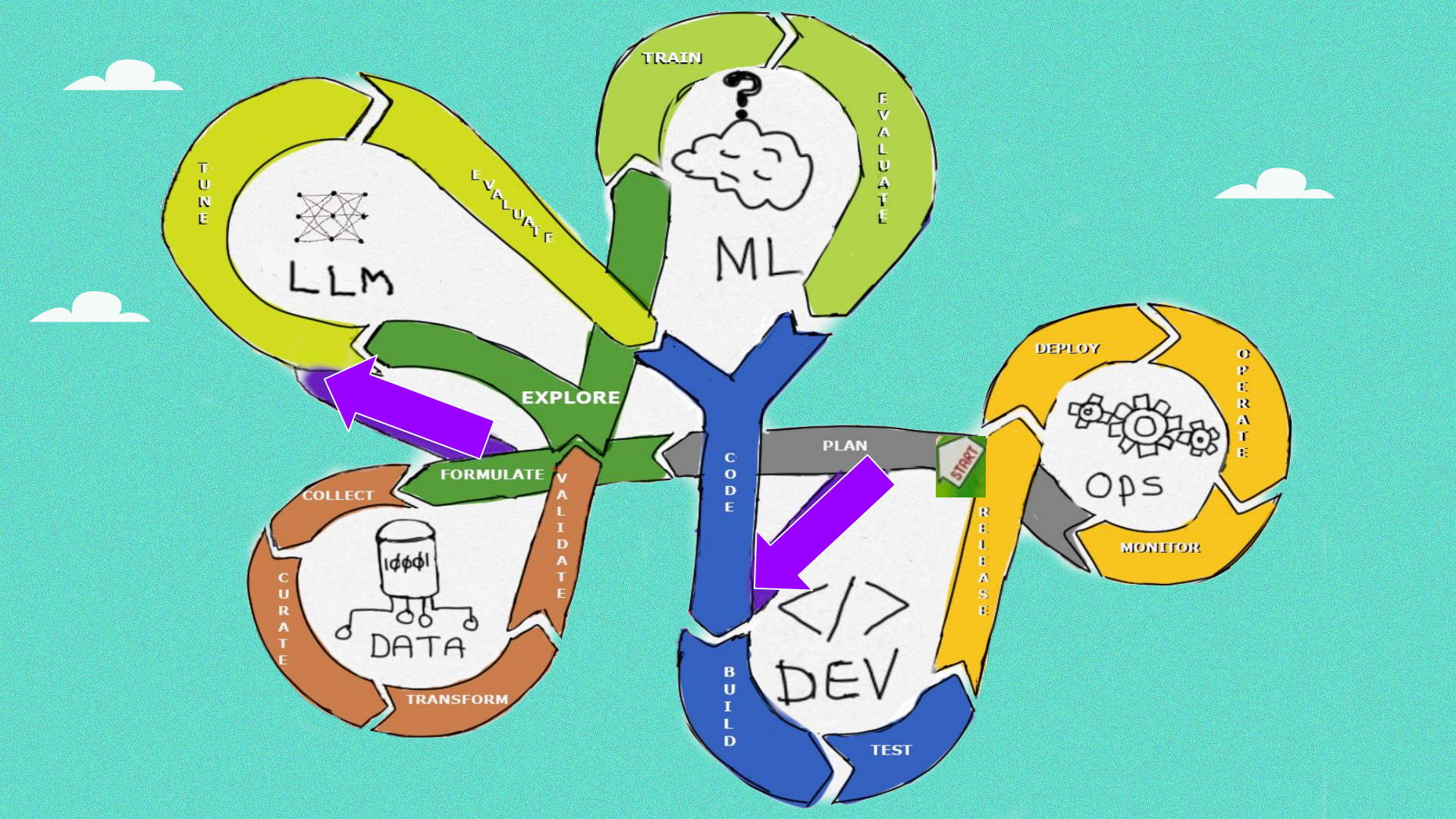
Pick your game piece: **Which persona are you?**

As you move around the board, become familiar with of all the people who will participate in AI systems with whom you may never personally interact. **What metadata should you create that supports the next step in the chain?**

Bonus: Think about how integrated CICD should get implemented across your organization

A picture is worth a thousand words


TRAIN
EVALUATE
ML
TUNE
EVALUATE
LLM
EXPLORE
Sweet Pass
FORMULATE
VALIDATE
COLLECT
CURATE
DATA
TRANSFORM
CODE
PLAN
START
Prismatic Pathway
</>
DEV
BUILD
TEST
RELEASE
DEPLOY
OPERATE
Ops
MONITOR


TRAIN
EVALUATE
ML
TUNE
EVALUATE
LLM
EXPLORE
FORMULATE
VALIDATE
COLLECT
CURATE
TRANSFORM
DATA
CODE
PLAN
START
DEPLOY
OPERATE
Ops
MONITOR
RELEASE
BUILD
TEST
DEV

05

How to Win the Game

Build on what you already know to develop a new understanding for how people, process and technology connect in the AI supply chain.

Once you know where you fit in, start contributing in OpenSSF Technical Initiatives and other foundations in which you are a member and start creating proactive security, especially with open source components.

Thanks!

Do you have any questions?

Sarah Evans

OpenSSF AIML WG

@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/

Prompts Used

Slide 11 - Two gingerbread children walking hand-in-hand through a candy playland with a colourful candy castle in the background

Slide 12 - A whimsical sign that says Confectionary Plan Orchard in a grove of Plum trees hanging with sparkling juicy fruit, and with gingerbread house with swirly icing off to the side

Slide 13- In the style of Pixar, a sparkling rainbow pathway that looks like a shortcut in a Christmas forest that says Prismatic Pathway

Slide 14 - a jolly green troll named ""poppy the planning elf" that is a project manager in a candy world

Slide 15 - a signpost made of a peppermint stick that says "The Peppermint Forest" next to a colourful candy swirly-twirly forest

Slide 16 - in the style of pixar, a tall happy man with pink hair dressing in peppermint candy-coloured clothes and a swirly driver's cap inside the swirly-twirly candy forest

Slide 17 - in the style of pixar, a secret path hidden in the candy forest with the path made of gumdrops

Slide 18 - in the style of pixar, the data overlord, who is sinister lanky figure, dressed in dark colours and a floppy hat with a long purple feather in the brim, beckoning the viewer closer in the candy playground

Slide 19 - in a candy playground, a castle made of licorice whips set against a pale yellow sky with spooky bats flying out of the towers

Slide 20 - a signpost made of a peppermint stick that is labeled "Magical Model Mountain" emerging from a gumdrop

Prompts Used, cont.

Slide 22 - in the style of pixar, two gingerbread children eating sticky sweets on a gumdrop path near a colourful candy fores

Slide 23 - a signpost made of a peppermint stick that is labeled "To the Lead Programmer's Lodge" with a small cabin made of pixie stix and licorice on a hill in the distance

Slide 24 - in the style of pixar, a kindly older woman wearing a blue-striped dress, carrying a basket of assorted nuts named Granny Nut, who is a senior developer

Slide 25 - in the style of pixar, wide-shot of two gingerbread children passing a sign made of a peppermint stick that is labeled"To the Quality Assurance Woods"

Slide 26 - in the style of pixar, wide-shot of two gingerbread children, scared and holding hands, lost in a dark Quality Assurance Woods automated tests lurk in the candy foliage

Slide 27 - in the style of pixar, a delightful young sprite girl named "Lollipop Code Maven" who is a helpful qa tester

Slide 28 - in the style of pixar, two anthropomorphic gingerbread children hold hands in the foreground looking at an ocean made of ice cream with swedish fish candies jumping out of the ice cream ocean

Slide 29 - in the style of pixar, an elegant princess, who is a software release manager, with a magical candy wand in her hand and a bright crown atop her flowing blue hair

Prompts Used, cont., cont.

Slide 30 -a signpost made of a candycane that is labeled "Fudgy Swamp of Compliance" with a bubbling fudge swamp in the distance

Slide 31 - in the style of pixar, a slightly spooky bubbling swamp made of chocolate fudge with magical candy creatures trapped inside

Slide 32 - in the style of pixar, a jolly amorphous blob with a human-like face, named Gloopy, that holds a clipboard with a long checklist on it emerging from the fudgy swamp

Slide 33 - in the style of pixar, a wise candy king with a candy scepter standing in front of a bright candy castle

Slide 34 - in the style of pixar, a wise candy king with a candy scepter standing in front of a bright candy castle greet two gingerbread children to his domain

All images generated by: https://designer.microsoft.com/image-creator