Threat Modeling in the ☁

Paige Cruz
@paigerduty

chronosphere

What threats are *likely* for a vending machine?

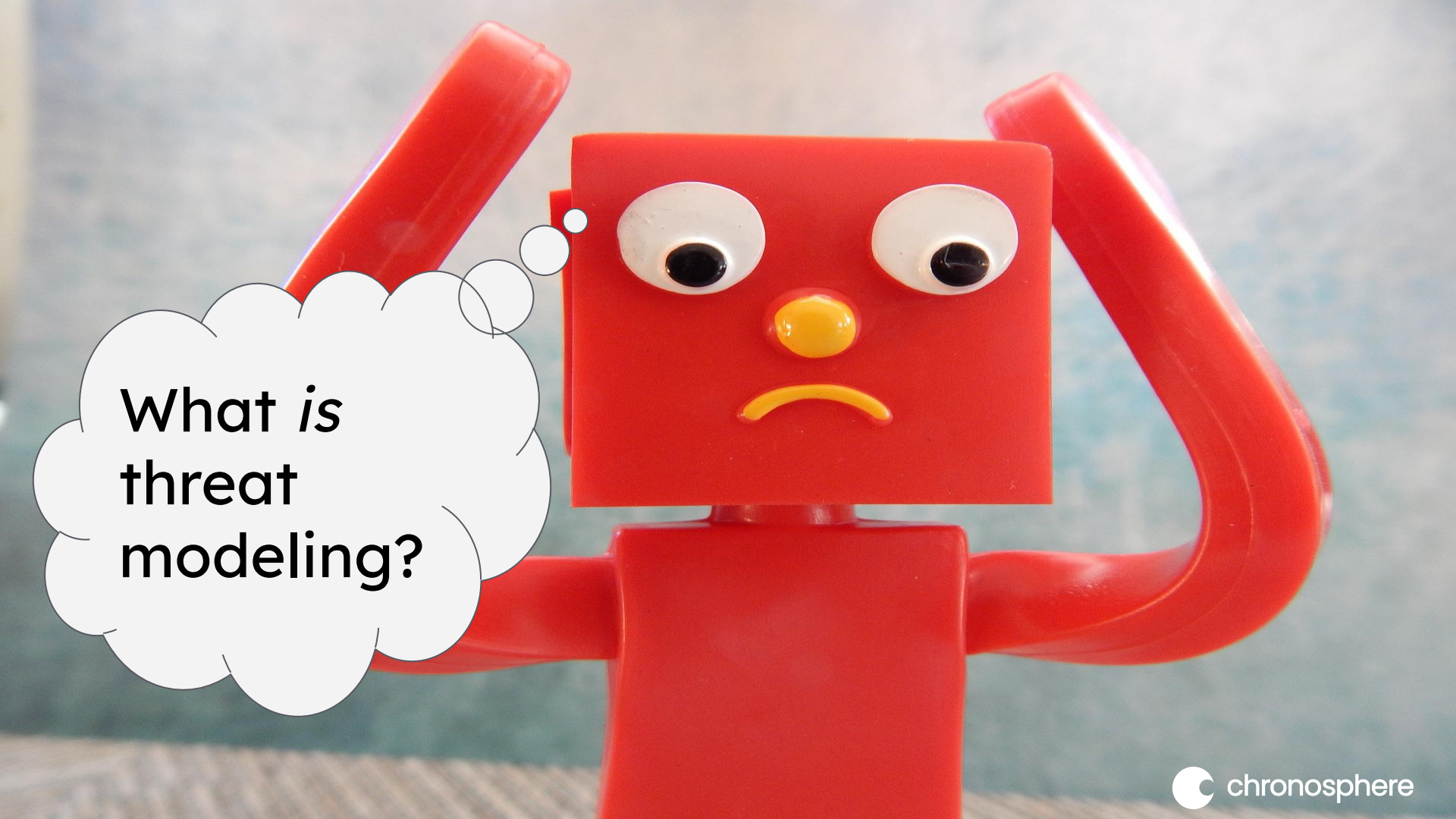
chronosphere

Your threat model is not my threat model: **Hospital edition**

chronosphere

Warning

Do not use endoscopy equipment to steal chocolate from this vending machine.


What *is* threat modeling?
chronosphere

The Official ™ Definition

*A structured process to **identify** security requirements, pinpoint threats and potential vulnerabilities, **quantify** threat and vulnerability criticality and **prioritize** remediation methods.*

Real World Definition

“

Threat modeling is a *conversation.*

- Matthew Coles

  Sr Principal Product Security Eng @ Dell

Guiding Questions

What are we working on?

Guiding Questions

What are we working on?

What can go wrong?

Guiding Questions

What are we working on?

What can go wrong?

What are we going to do about it?

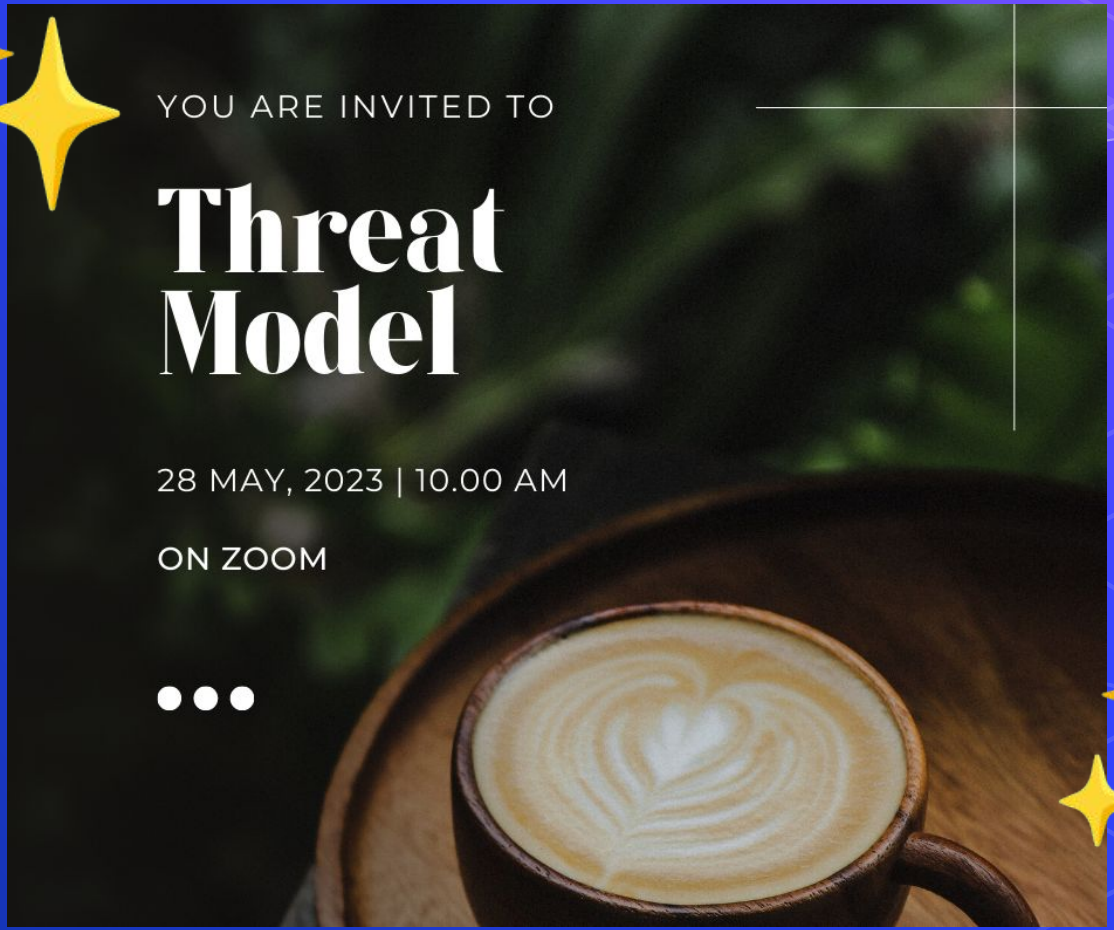
Guiding Questions

What are we working on?

What can go wrong?

What are we going to do about it?

Did we do a good enough job?



chronosphere13

Architect

Software Developer

Architect

Software Developer

Customer Support

Architect

chronosphere16

Architect

Software Developer

Customer Support

Quality Assurance (QA)

Architect

Software Developer

Customer Support

Quality Assurance (QA)

Tech Writer


chronosphere19

Threat Modeling in the *Cloud*

chronosphere

Which make up the top 3 cloud threats?

- Weak Control Plane
- Account Hijacking
- Data Breaches
- Insufficient IAM and Key Management
- Metastructure + Applistructure Failures
- Abuse + Nefarious Use of Cloud Services
- Insecure Interfaces + APIs
- Insider Threat
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture + Strategy
- Limited Cloud Usage Visibility

Which make up the top 3 cloud threats?

- Weak Control Plane
- Account Hijacking
- Data Breaches
- Insufficient IAM and Key Management
- Metastructure + Applistructure Failures
- Abuse + Nefarious Use of Cloud Services
- Insecure Interfaces + APIs
- Insider Threat
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture + Strategy
- Limited Cloud Usage Visibility

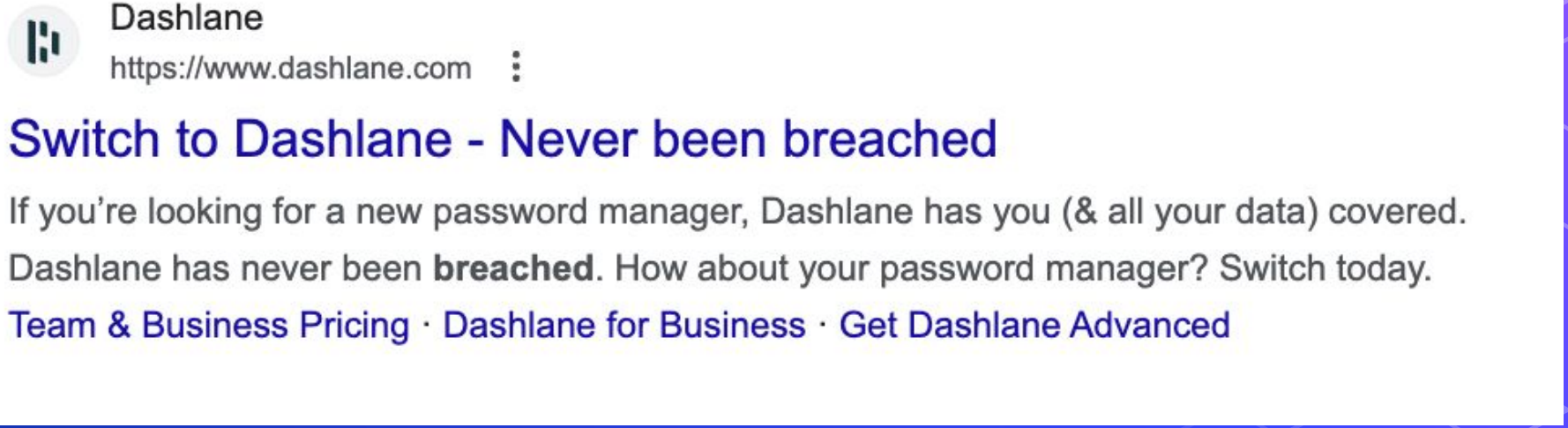
Which make up the top 3 cloud threats?

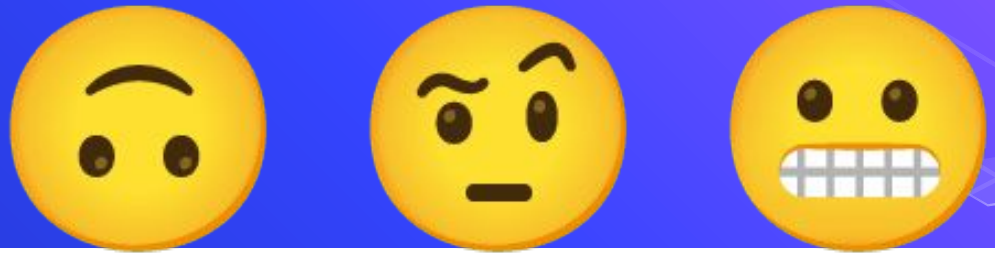
- Weak Control Plane
- Account Hijacking
- Data Breaches
- Insufficient IAM and Key Management
- Metastructure + Applistructure Failures
- Abuse + Nefarious Use of Cloud Services
- Insecure Interfaces + APIs
- Insider Threat
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture + Strategy
- Limited Cloud Usage Visibility

Which make up the top 3 cloud threats?

- Weak Control Plane
- Account Hijacking
- Data Breaches
- Insufficient IAM and Key Management
- Metastructure + Applistructure Failures
- Abuse + Nefarious Use of Cloud Services
- Insecure Interfaces + APIs
- Insider Threat
- Misconfiguration and Inadequate Change Control
- Lack of Cloud Security Architecture + Strategy
- Limited Cloud Usage Visibility


IT'S NOT A DATA BREACH
IT'S A SURPRISE BACKUP


Dashlane
https://www.dashlane.com
Switch to Dashlane - Never been breached
If you're looking for a new password manager, Dashlane has you (& all your data) covered.
Dashlane has never been **breached**. How about your password manager? Switch today.
Team & Business Pricing · Dashlane for Business · Get Dashlane Advanced



Dashlane

https://www.dashlane.com

Switch to Dashlane - Never been breached

If you're looking for a new password manager, Dashlane has you (& all your data) covered. Dashlane has never been **breached**. How about your password manager? Switch today.

Team & Business Pricing · Dashlane for Business · Get Dashlane Advanced

“If Defendant had disclosed the full extent of the breach in August **instead of waiting months**, Plaintiff/Class would have been on heightened alert and changed passwords to avoid theft that ensued.”


A MISCONFIGURED FIREWALL
imgflip.com

rsync

chronosphere30


I DON'T ALWAYS THINK ABOUT CYBERSECURITY
BUT WHEN I DO, IT'S USUALLY TOO LATE
memegenerator.net

accenture

chronosphere32


Egregious Eleven
chronosphere33

Case Study

chronosphere

> While Argo services often support various risk or threat prevention methods, these are frequently **under-documented** or are provided on an **opt-in** basis rather than default

- Argo Project Threat Model

README.md

example

an example GitHub repository

chronosphere37

Minimal Service Documentation: Argo

Argo Workflows Findings

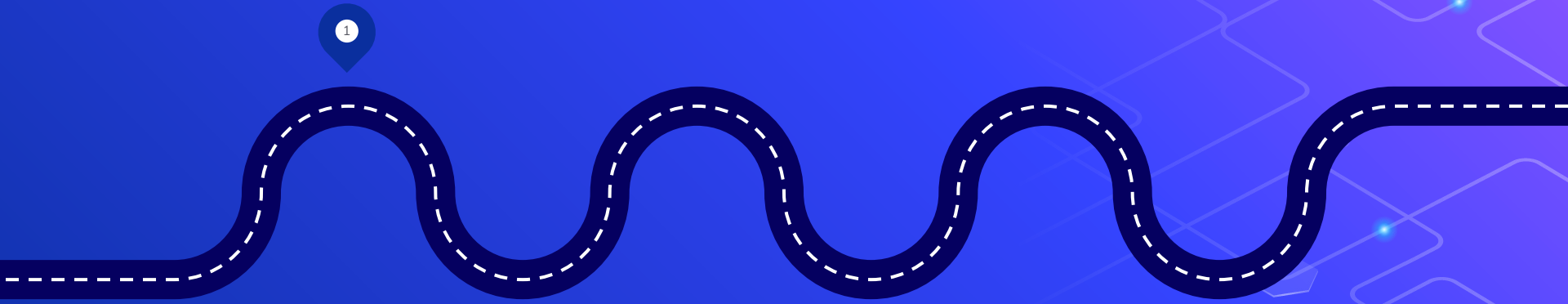
Argo Workflows is an engine for creating and managing multi-step workflows. Workflow steps are defined in their own containers. Like Argo CD, Argo Workflows depends on an API server that users access via a Web UI or CLI utility for creating and managing workflows. The API also serves as an authentication endpoint.

Within Kubernetes, Argo Workflows is defined as a set of Kubernetes CRDs, and each workflow is a custom Kubernetes resource that resides in the user namespace. Workflows can be started via API requests, webhooks, or cron jobs. Requests are then forwarded to the workflow-controller, which monitors the workflow namespace for changes and executes tasks accordingly. After a workflow has been completed, a copy of the workflow is made and stored in an SQL database. Produced artifacts are stored in services like s3 and MinIO.

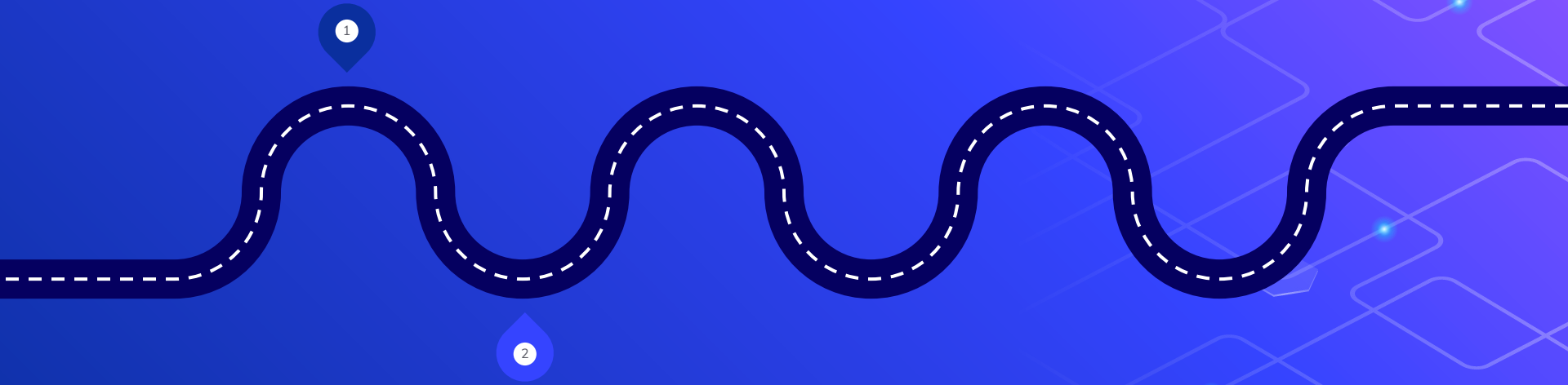
Threat Modeling and You ✨

chronosphere

Identify 1 feature or service to begin threat modeling



Identify 1 feature or service to begin threat modeling

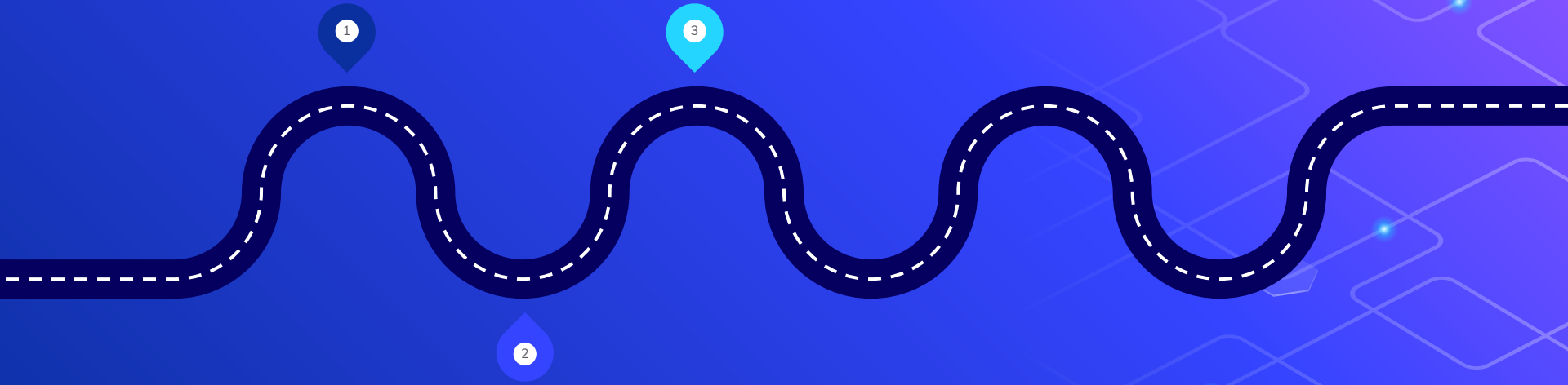


Schedule a meeting. Agenda: The 4 Guiding Questions

chronosphere41

Identify 1 feature or service to begin threat modeling

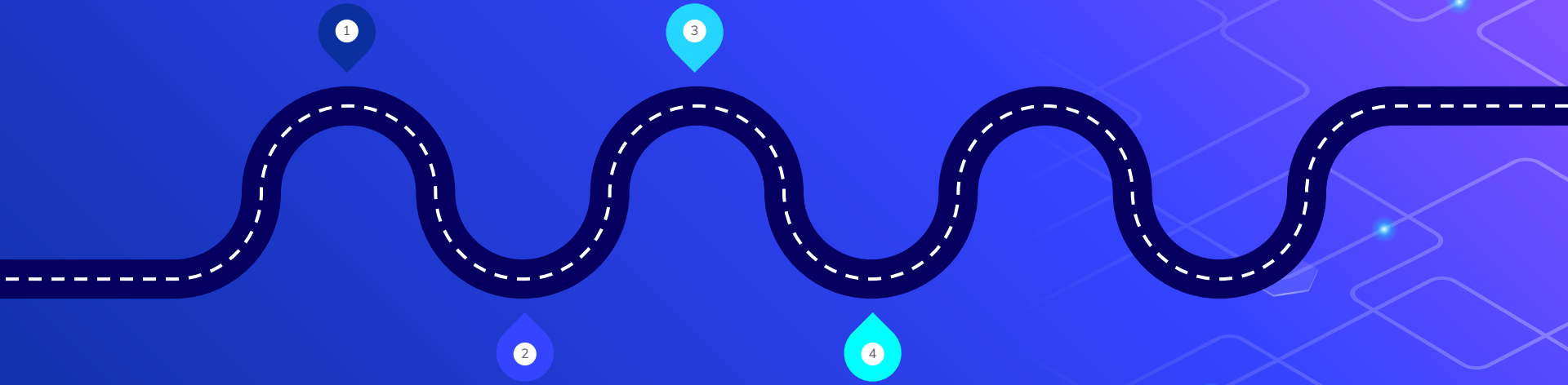
Send pre-read of the Threat Modeling Manifesto



Schedule a meeting. Agenda: The 4 Guiding Questions

Identify 1 feature or service to begin threat modeling

Send pre-read of the Threat Modeling Manifesto



Schedule a meeting. Agenda: The 4 Guiding Questions

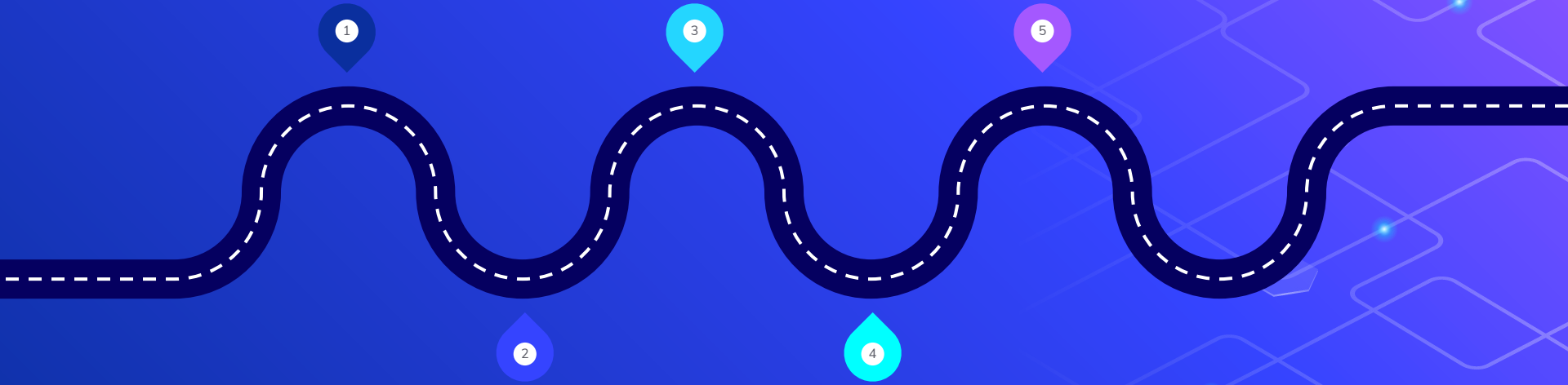
Ensure minimal service documentation

chronosphere43

Identify 1 feature or service to begin threat modeling

Send pre-read of the Threat Modeling Manifesto

Assign a scribe and facilitator for the meeting



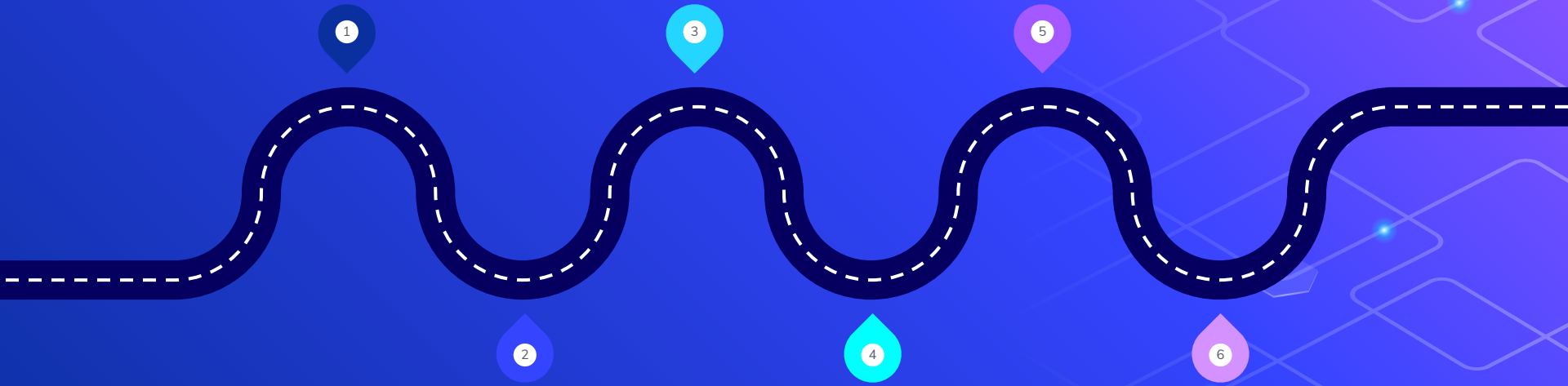
Schedule a meeting. Agenda: The 4 Guiding Questions

Ensure minimal service documentation

Identify 1 feature or service to begin threat modeling

Send pre-read of the Threat Modeling Manifesto

Assign a scribe and facilitator for the meeting



Schedule a meeting. Agenda: The 4 Guiding Questions

Ensure minimal service documentation

Rinse and repeat

chronosphere45

Case Study

chronosphere

2019 Data Exposure

Threat Modeling is a *conversation*

chronosphere

Further Resources

- Threat Modeling Manifesto
- OWASP Top Ten Web App Security Risks
- Hiding Malware in Docker Desktop <- srsly a hilarious and informative read
- MITRE ATT&CK adversarial knowledge base 101 blog post

Minimal Service Documentation

- How does the service work?
- Are there any subcomponents or shared boundaries?
- What communication protocols does it use?
- Where does it store data?
- What is the most sensitive data it stores?

Egregious Eleven

1. **Data Breaches**
2. **Misconfiguration and Inadequate Change Control**
3. **Lack of Cloud Security Architecture + Strategy**
4. Insufficient IAM and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces + APIs
8. Weak Control Plane
9. Metastructure + Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse + Nefarious Use of Cloud Services

Let’s Chat

@ CNCF Booth G3

Friday, 2:20 - 3:20

paigerduty.com

- @chronosphere.io
- @hachyderm.io

chronosphere52