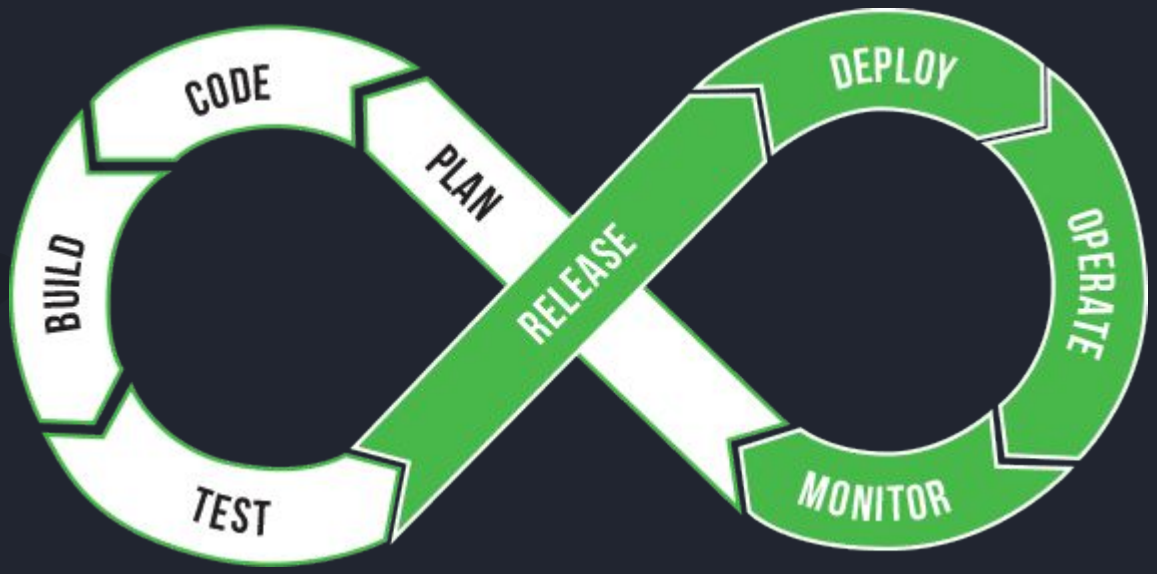
JFrog

The Liquid Software Company

You Can’t Secure Your Software Supply Chain Without a Pipeline



Lori Lorusso

Open Source Program Manager, JFrog
Marketing Outreach Committee Chair, CDF

@lorilorusso
linkedin.com/in/lorilorusso

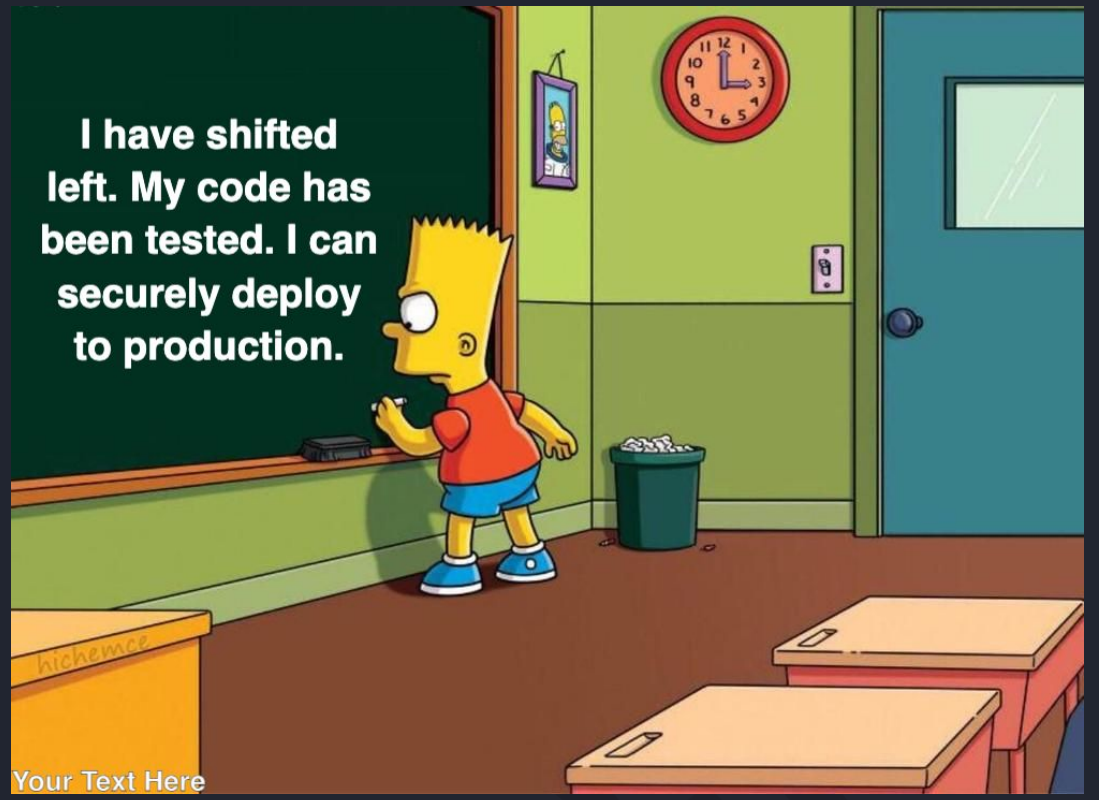
The Liquid Software Company

The Liquid Software Company

LET’S GET STARTED!

WHY CI/CD SECURITY?

The shift left has happened so our pipelines are secure… right… maybe… ugh…



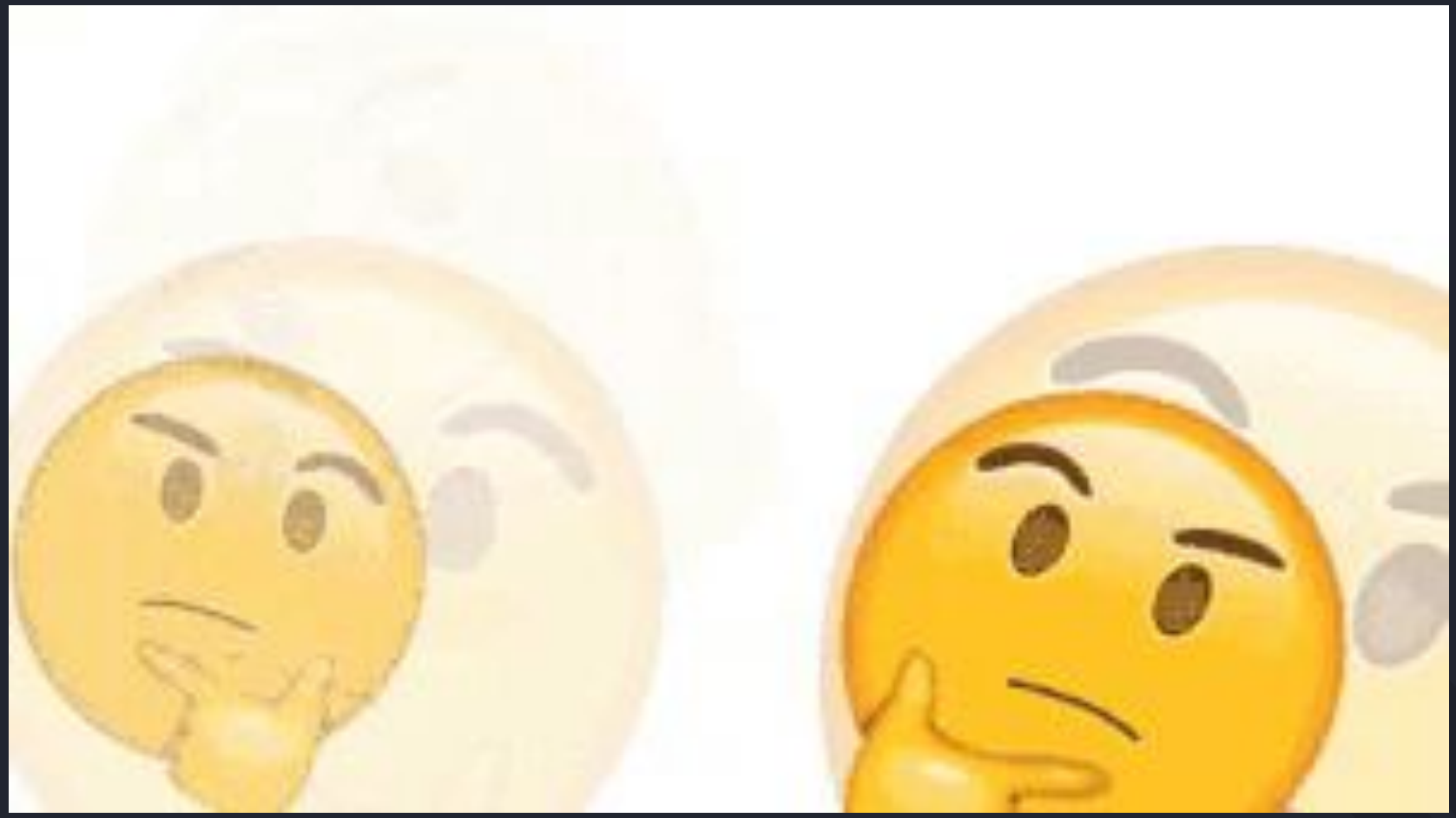
SUPPLY CHAIN SECURITY

The “New Kid On The Block…”

CREEPER WORM...

I'M THE CREEPER. CATCH ME IF YOU CAN!

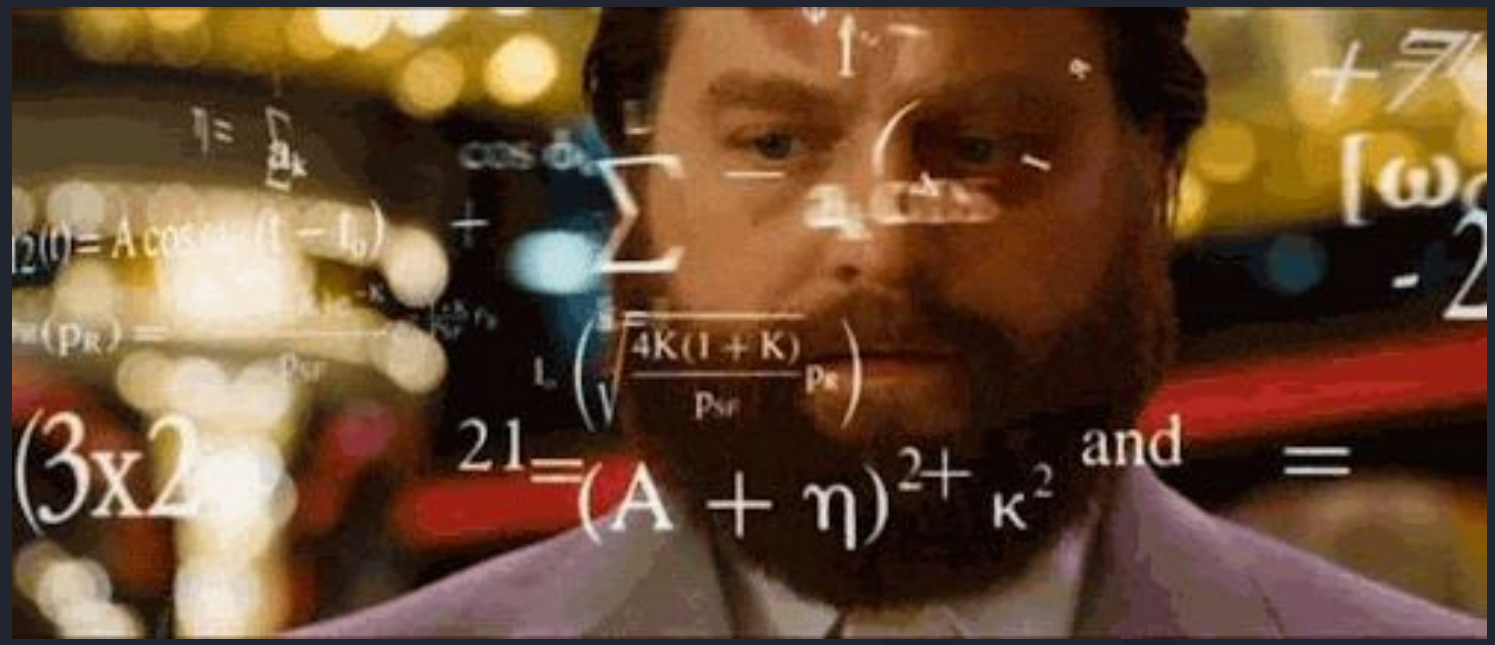
WHY ARE WE SO VULNERABLE?



LET'S DO THE MATH...

99%

85%



The Liquid Software Company

SUPPLY CHAIN SECURITY ATTACKS ARE HAPPENING

THERE WAS A BLANK% INCREASE IN SOFTWARE SUPPLY CHAIN ATTACKS IN 2021

SOFTWARE IS UNDER ATTACK!

Common Attack

VS

Supply Chain Attack

The Liquid Software Company

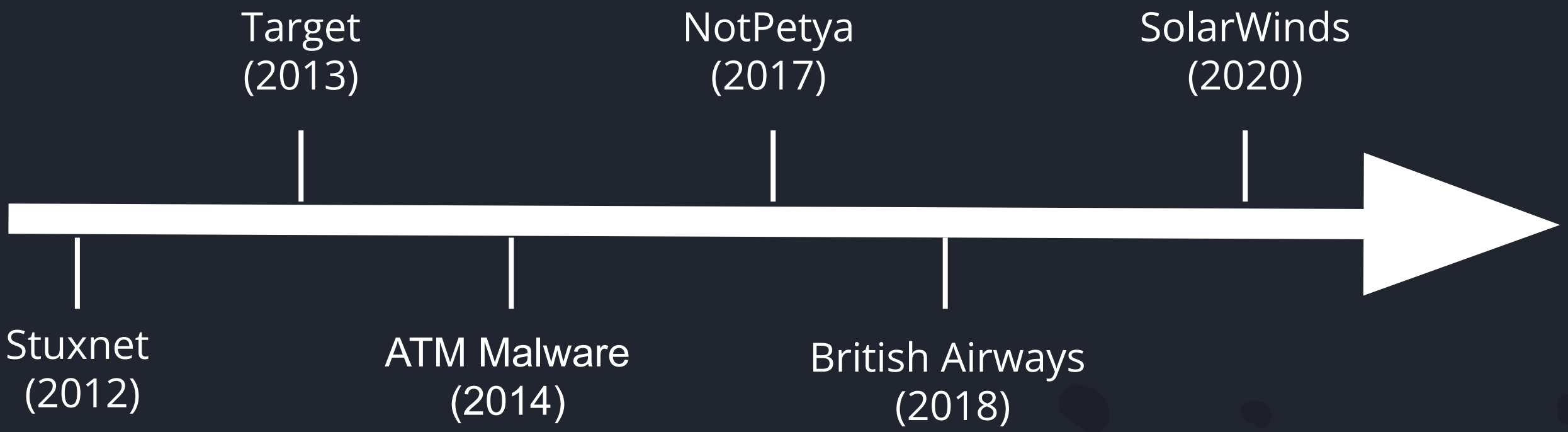
WHY ATTACK THE SUPPLY CHAIN?

JFrog
The Liquid Software Company

TYPES OF SUPPLY CHAIN SECURITY ATTACKS

- Known Vulnerabilities
  - publicly disclosed security bugs
- Unknown Vulnerablities - Zero Day Attacks
  - attack on a vulnerability that was not identfied and fixed in time to prevent the attack
- Non-Code Issues
  - human error can lead to malicious software injection attacks

10 YEARS 6 MASSIVE ATTACKS!



STUXNET 2010

- Computer worm infected over 200,000 computers
- caused 1,000 machines to physically degrade
- exploited 4 Zero Day vulnerabilities

TARGET 2013

- Malware was placed on POS (point of sale) machines through their HVAC company
- 40 million credit and debit cards details stolen
- $18.5 million in settlement claims
- Target estimates a $202 million loss

The Liquid Software Company

ATM MALWARE 2014

- Multiple varieties but all do the same thing…
- Magnetic strip can be compromised - you need an insider to put the malware on the machine
- Exploited Windows 32-Bit operating system letting attackers see how much money is in each machine and ‘withdraw’ 40 notes

NOTPETYA 2017

- Targeted Ukraine energy companies, the power grid, bus stations, gas stations, the airport, and banks!
- A patch - M.E.Doc - was used as the backdoor to infect the companies
- New iteration of Petya (2016) - a ransomware attack - Notpetya asked for low level ransom but the goal was to infect computers and not collect money

BRITISH AIRWAYS 2018

- Infected the payment screen and rerouted customers to different website where attackers stole consumer info
- 380,000 customers credit cards COMPROMISED
- £183 million fine

SOLARWINDS 2020

- Windows OS attack
- 18,000 customers infected including the United States'
  - Department of Homeland Security
  - National Nuclear Security Administration (NNSA)
  - Department of Commerce
- Average cost to companies infected - $12 Million

"Eighteen thousand [customers] was our best estimate of who may have downloaded the code between March and June of 2020."

-Sudhakar Ramakrishna, SolarWinds President & CEO

PAST, PRESENT & FUTURE

The Liquid Software Company

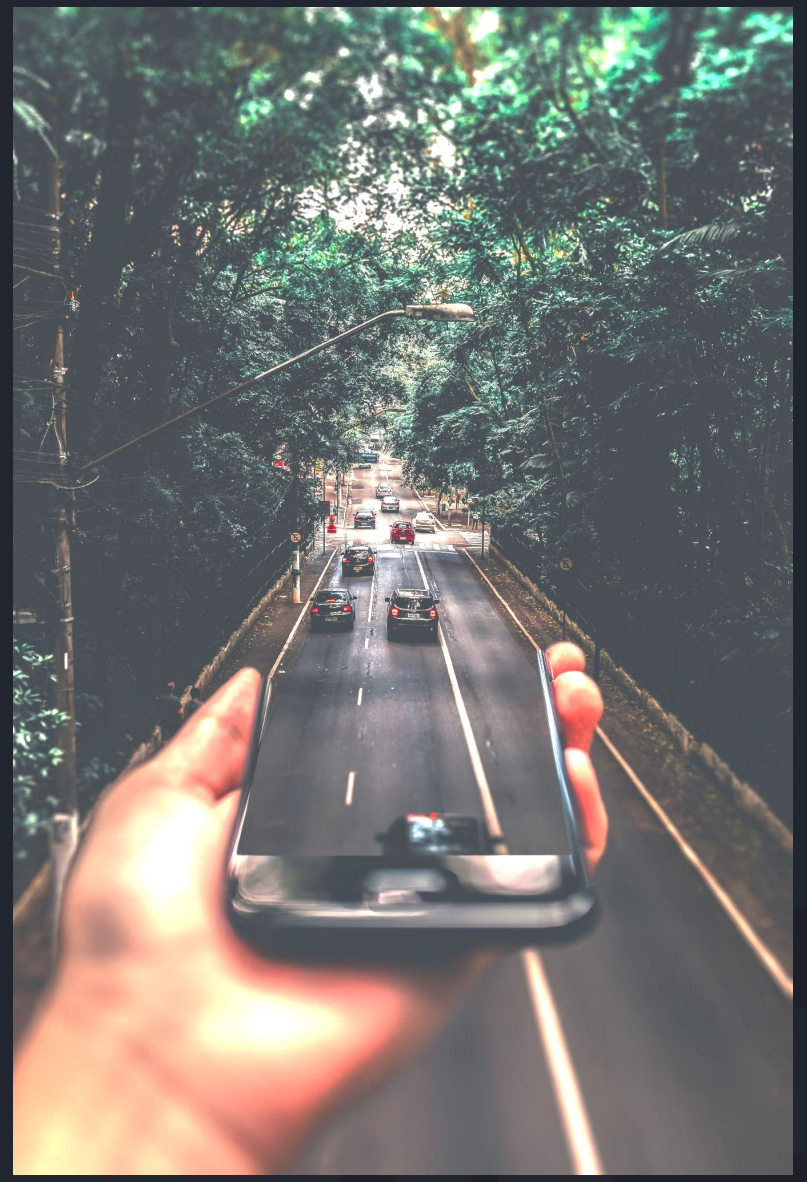
WHAT DOES THIS HAVE TO DO WITH THE CDF?

The Continuous Delivery Foundation supports various continuous delivery open source and standards projects, including infrastructure and support initiatives.

https://github.com/cdfoundation/charter/blob/main/CHARTER.md

WHAT DOES THIS HAVE TO DO WITH THE CDF?

- WHAT DO WE BELIEVE IN…
  - producing high quality software more rapidly
  - collectively addressing the whole software delivery lifecycle
- POWER OF COMMUNITY BUILDING
  - sustaining open-source, vendor neutral projects
  - collaboration among practitioners to share and improve their practices



CDF PROJECTS OVERVIEW

GRADUATED

WHERE DOES SECURITY FIT INTO THE CDF?

PYRSIA

JFrog

Pyrsia sets out to be the torch that lights up the open-source supply chain.

WHAT DO WE WANT IN OUR SUPPLY CHAIN

RELIABLE

SECURE

OPEN

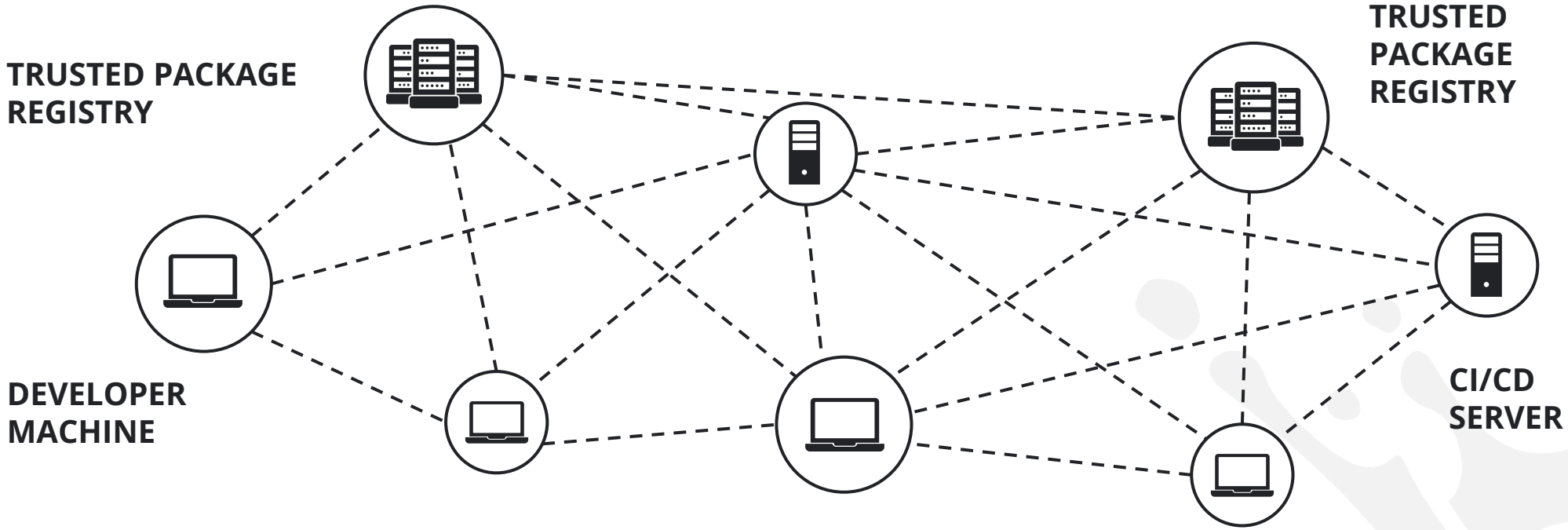
PYRSIA

JFrog

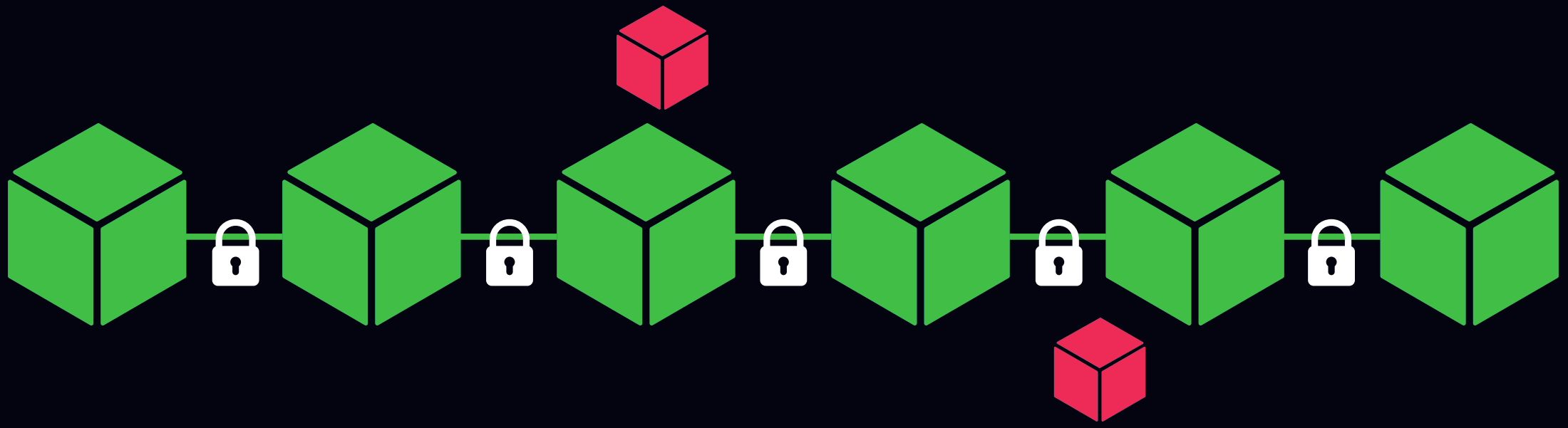
PYRSIA BINARY DISTRIBUTION NETWORK

https://github.com/pyrsia

Decentralized Package Registry
P2P Package Downloads
Multi-node Verification of Source Builds



IMMUTABLE TRANSPARENCY LEDGER



DECENTRALIZED PACKAGE NETWORK

WE NEED MORE SECURITY PROJECTS

CD.FOUNDATION

PYRSIA

JFrog

The Liquid Software Company

THANK YOU!