SECURING THE DEVELOPMENT & SUPPLY CHAIN OF OPEN-SOURCE S.W.

DEREK WEEKS, LINUX FOUNDATION

STORY: NATIONAL ONION RECALL

ON RADIO

- ECOLI OUTBREAK
- 37 STATES
- FROM MEXICO

⇒ ABLE TO RECALL
- SOURCE
- SUPPLY CHAIN
- CONSUMERS

TAKATA AIRBAGS
- PIECES OF METAL
- TOYOTA KNEW WHERE CARS WERE + BUYERS
- ABLE TO DO BECAUSE OF MANAGED SUPPLY CHAIN

SW CHAIN IS NOT LIKE FOOD/AUTO

MFG. HAVE KNOWLEDGE + VISIBILITY ON PARTS
- THEY CAN FIND + FIX DEFECTS

OPEN SOURCE SW DEV.

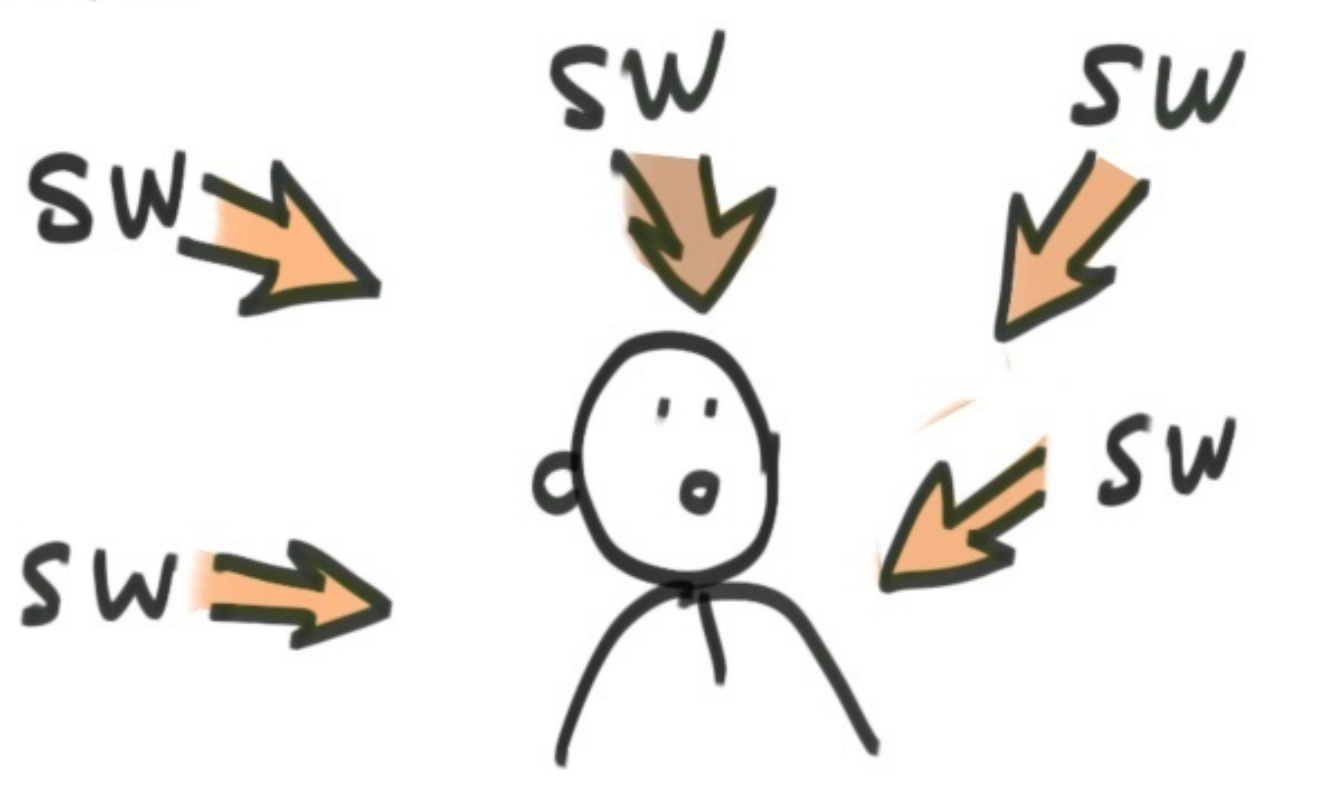
40M	420M	2T
OSS COMPONENTS	OSS RELEASES by 2026	PACKAGE ↓ PER YR.

OSS – OPEN SOURCE SW

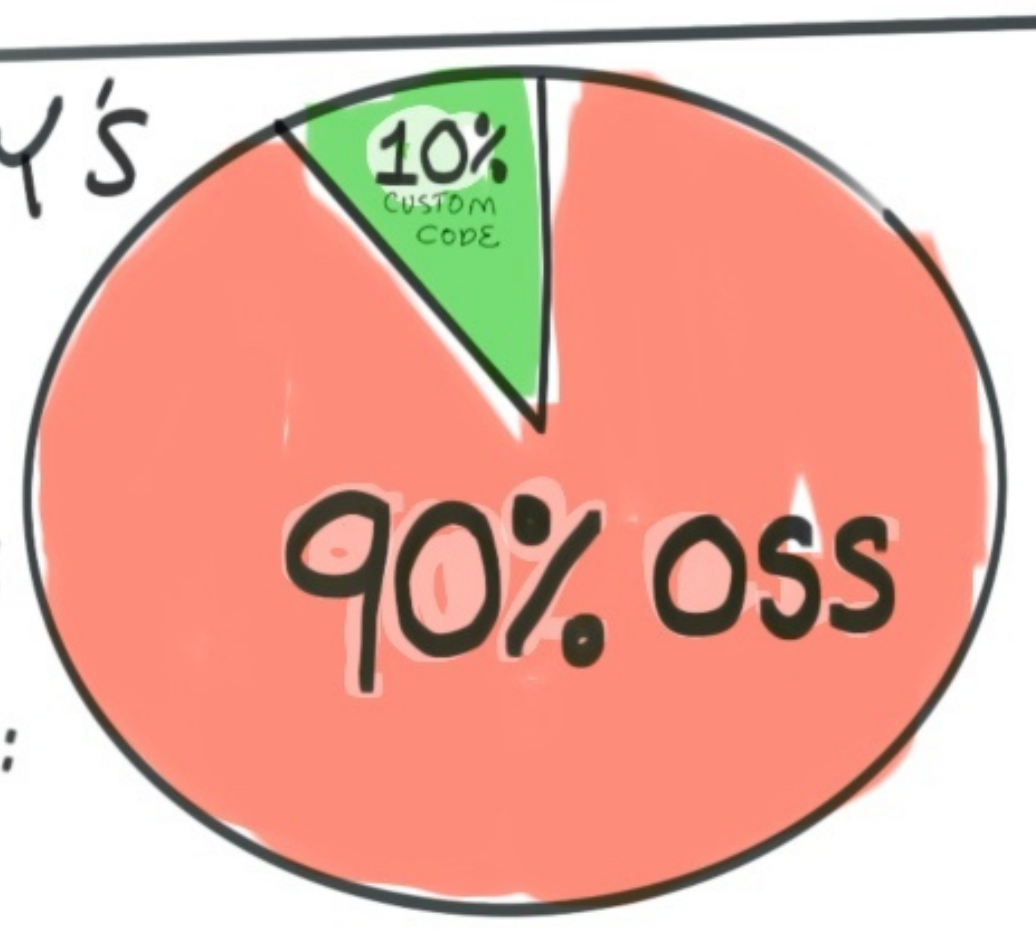
- TODAY, APPS NO LONGER WRITTEN FROM SCRATCH
- DEVELOPERS ARE LEVERAGING OPEN SOURCE TO BUILD S.W.

⇒ MADE BY DEVELOPERS FOR DEVELOPERS

YOU HAVE MORE THAN ONE S.W. SUPPLY CHAIN.



TODAY'S MODERN APP CODE BASE IS MADE OF:



WE'RE ABLE TO BUILD + DEPLOY FASTER W/OSS

BUT

NOT ALL OSS ARE CREATED EQUAL

30% HAVE KNOWN VULNERABILITIES

TRADITIONAL MFG., THE PROCUREMENT DEPT. VETS THE SUPPLIERS FOR THEIR MFG.

IN OSS PROCUREMENT, EACH DEVELOPER, IS A PROCUREMENT OFFICER

SW SUPPLY CHAIN BREACHES UP

6507

BAD SW IS BAD FOR BUSINESS

VOLVO EXAMPLE. EARLY LEADER IN SAFE AUTOS

SOON SW SECURITY IN CONSUMER PRODUCTS + BUSINESS WILL BE HOW COMPANIES COMPETE

WHAT CAN BE DONE?
- OSS IS AT CENTER
- SECURITY IS CRITICAL
- ADVESARIS WINNING
- GOVTS. DEMAND ACTION

ACKNOWLEDG DEPENDENCIES ON OSS

- FIX KNOWN VULS.
- TRACK + TRACE NEW OSS VULS
- LINUX ISO STANDARD SPDX

THE OLD ADVERSARY GAME

WAIT | DISCOVERY | PREY

THE NEW ADVERSARY GAME

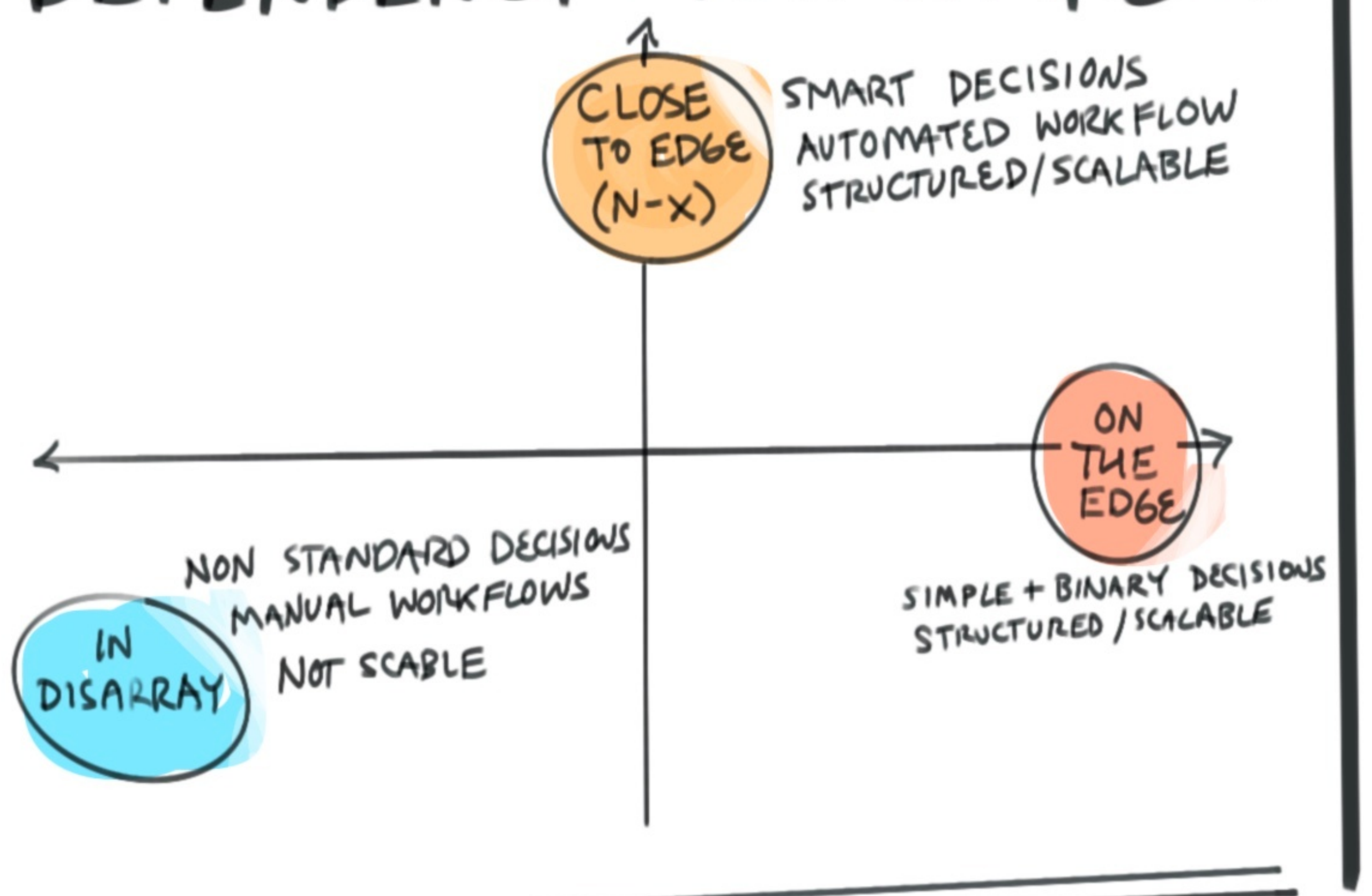
DEVELOP | SHARE | DISTRIBUTE | PREY

ADVERSARIES, ARE BECOMING DEVELOPERS!

INJECTING ZERO DAY AT THE INCEPTION OF CODE!

ADVERSARIES ARE LOOKING AT EVERY STEP ALONG THE WAY.
- SOURCE
- PACKAGE
- BUILD
- DEPENDENCIES

DEPENDENCY MGT. STRATEGY


CLOSE TO EDGE (N-X)
SMART DECISIONS
AUTOMATED WORKFLOW
STRUCTURED/SCALABLE
ON THE EDGE
SIMPLE + BINARY DECISIONS
STRUCTURED/SCALABLE
IN DISARRAY
NON STANDARD DECISIONS
MANUAL WORKFLOWS
NOT SCABLE