

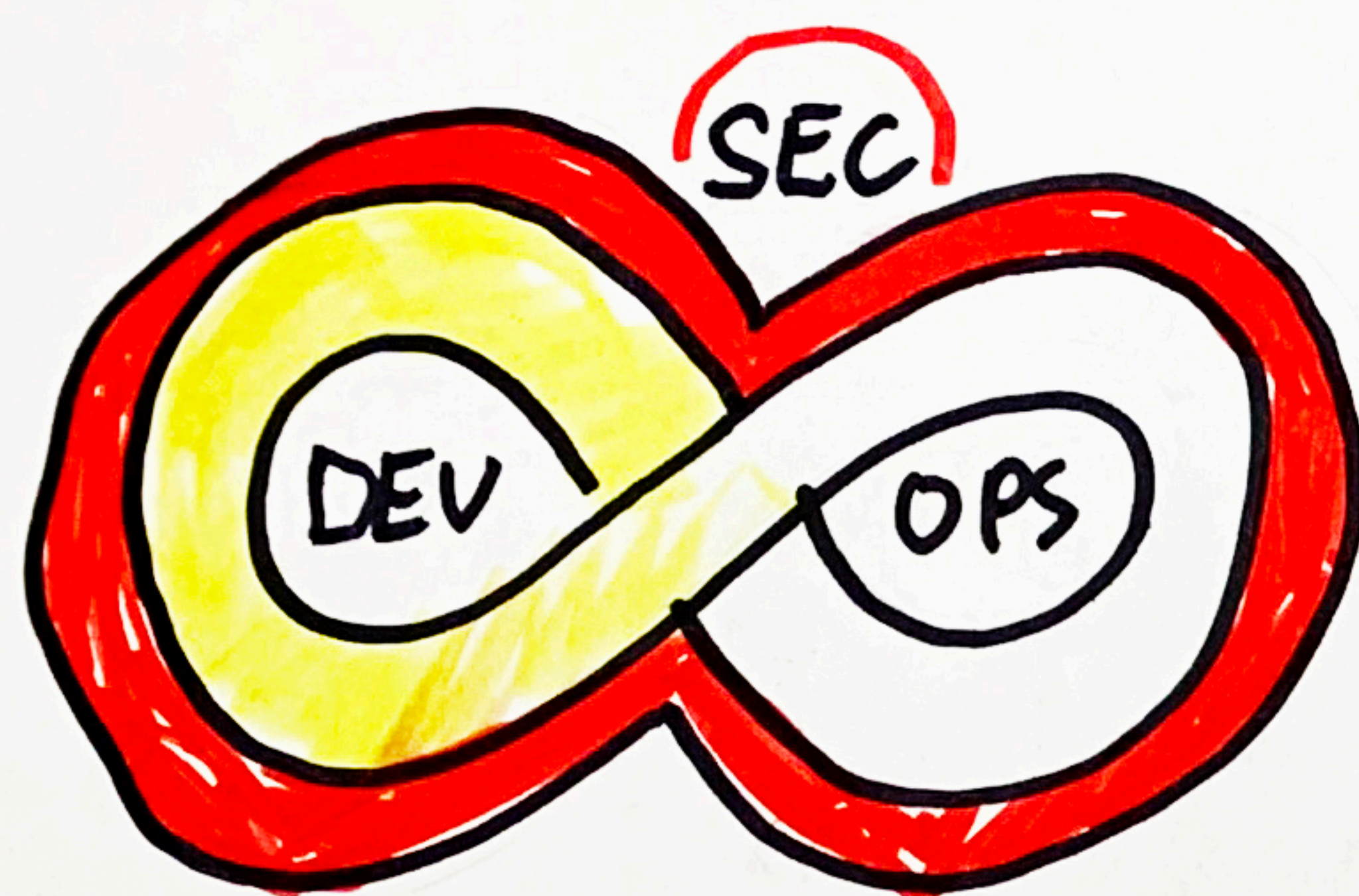
ENHANCE APPSEC MATURITY AND OUTCOMES USING DEVSECOPS METRICS

SURESH CHANDRA BOSE GANESH BOSE

RELEASE ON DEMAND = CONTINUOUS SECURITY MODELING USING S.I.E.M.

USE GARTNER BEST PRACTICES (+ OTHERS) ACROSS LIFE CYCLE

METRICS ARE KEY TO DSO



WHY DEVSECOPS? EVEN MOBILE PHONES ARE VULNERABLE TO HACKS!

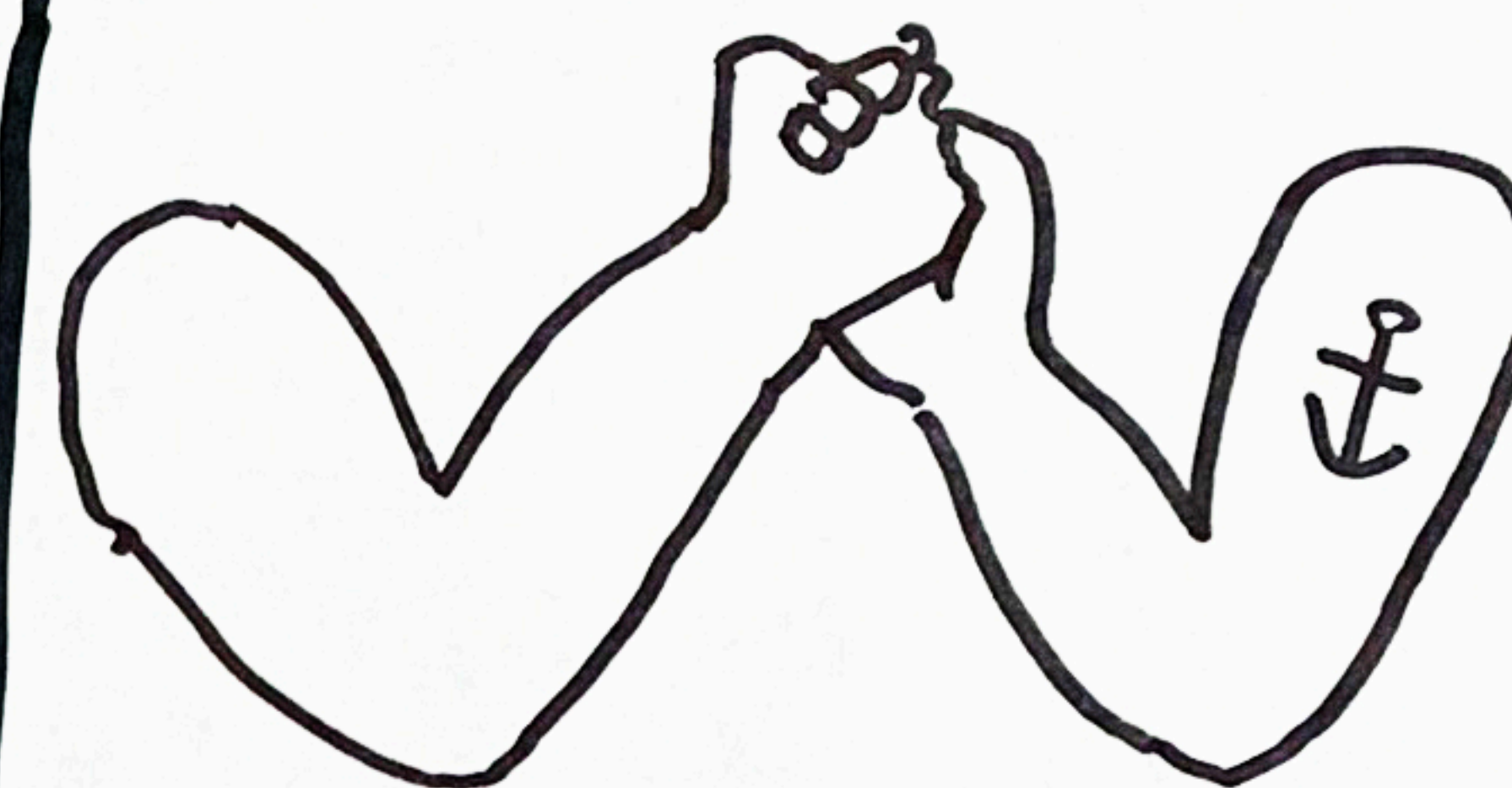
CE: BENEFITS FROM THREAT MODELING

CI: WHERE THE DEV HAPPENS

FOUR STEPS OF THREAT MODELING

- 1) WHAT ARE YOU BUILDING?
- 2) IDENTIFY THREATS
- 3) MITIGATE
- 4) VALIDATE

ALL FOUR REQUIRE MORE SECURITY SUPPORT

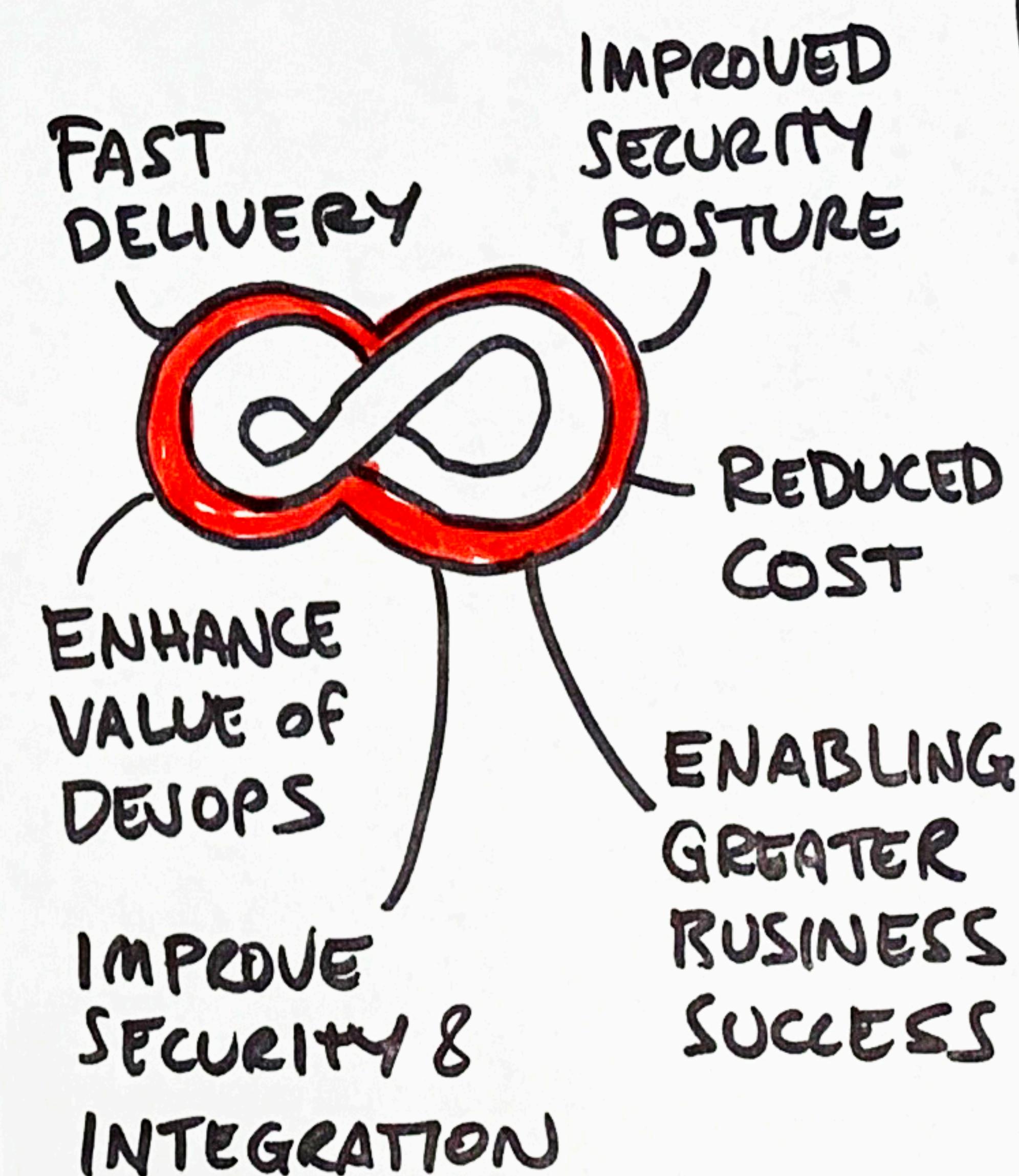


STRONG COLLABORATION ACROSS DEVSECOPS TEAM

SECURITY IDE PLUG-INS CODE REVIEW PAIR WORK

- STATIC CODE ANALYSIS
- 3rd PART SCANS
- FUZZ TESTING
- CODE SIGNING
- INFRA SCANS
- MALWARE SCANS
- DYNAMIC SCANS

MEET BUSINESS OUTCOME



METRICS GOALS:

- REDUCED TOTAL SECURITY TICKETS OPENED
- REDUCED TIME TO DEPLOY
- DISCOVERY OF PREPRODUCTION VULNERABILITIES
- REDUCE TIME TO MEDIATE
- % OF SECURITY PASSED
- REDUCED FAILED SECURITY TESTS