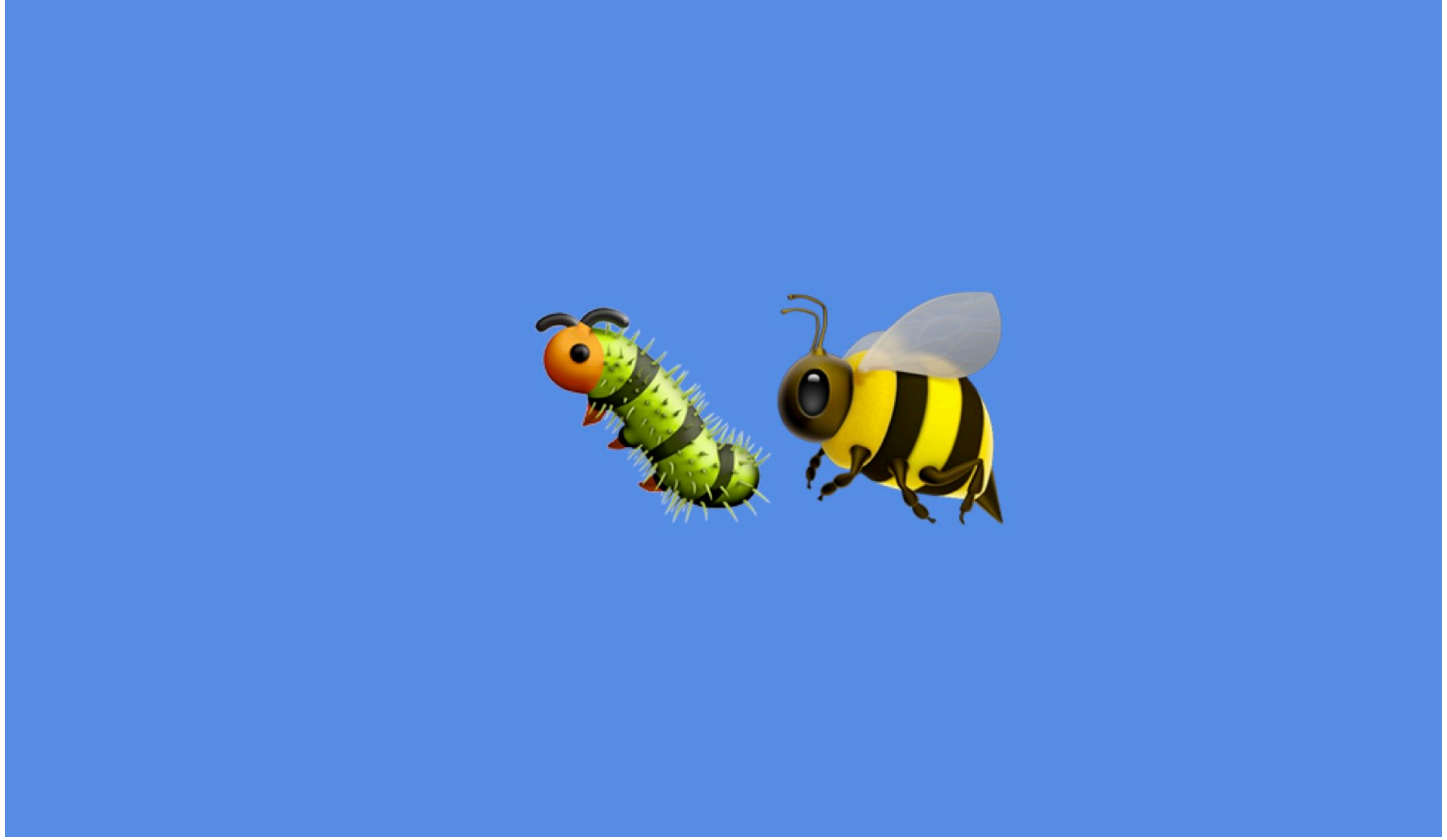
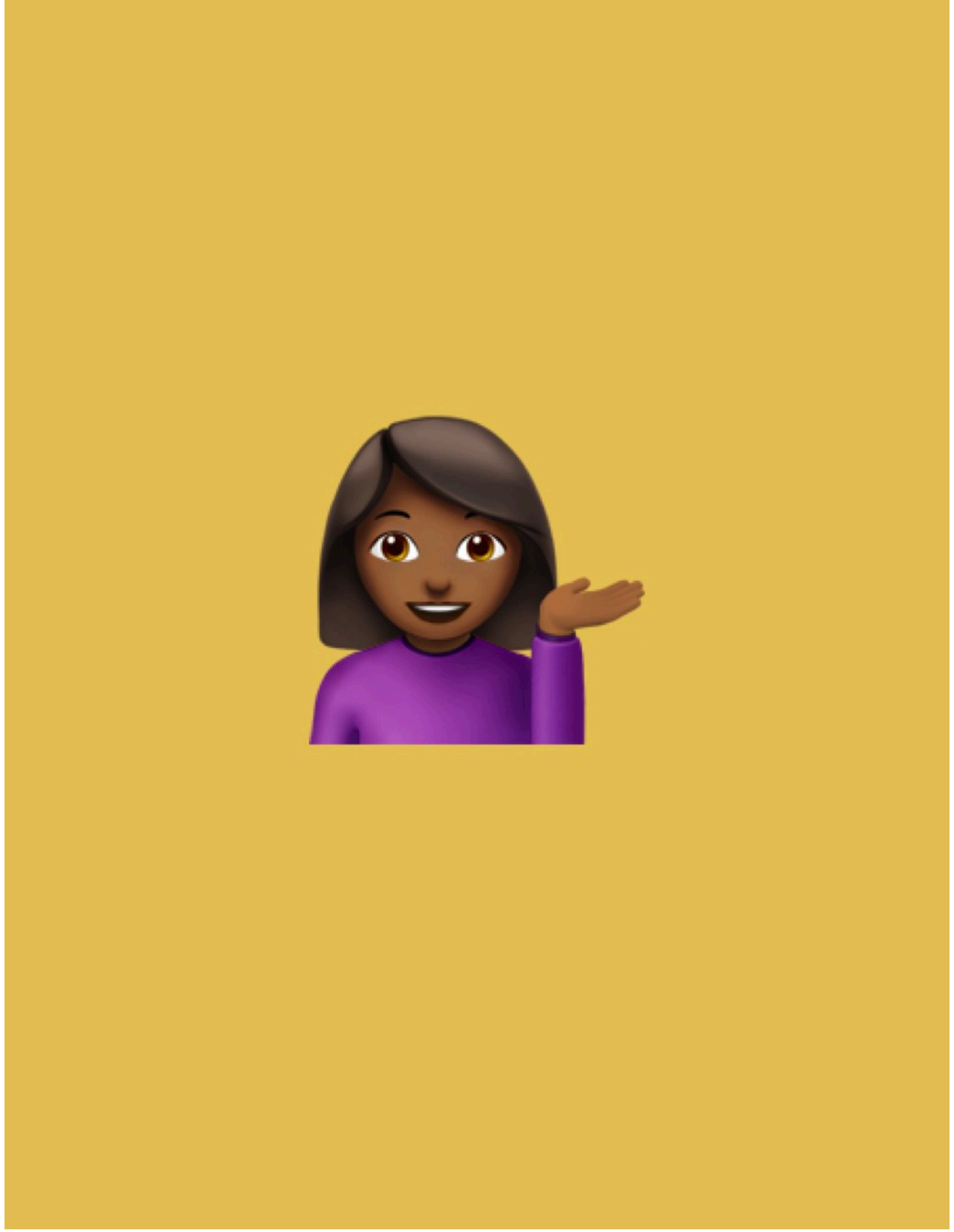
WIKTORIA DALACH (SHE/HER) @WDALACH

SECURITY DOESN'T HAVE TO BE A NIGHTMARE (CLOUD EDITION)

Conf42: Cloud Native 2023



Here's to the crazy ones.
The misfits. The rebels.
The troublemakers. The
round pegs in the
holes.
The ones w
differentl
fond of



WIKTORIA DALACH

- Born in Kraków, Poland, based in Berlin, Germany
- Over a decade in tech
- Mostly backend
- 👩🏻‍💻 🤝 🔐

WIKTORIADALACH.COM/SECURITY

🍓 PAY ATTENTION TO ACCESS CONTROL

🫐 SECURE APIS

🍇 MISCONFIGURATION HURTS

🍐 LET THE MACHINES WORK FOR YOU 🤖

DAST - DYNAMIC APPLICATION SECURITY TESTING

🤖

SAST - STATIC APPLICATION SECURITY TESTING

🤖

🤯

ENGINEERING VS. NICE-TO-HAVE

Hope St

THERE IS AN INFINITE AMOUNT OF THREATS BUT...

...ALL OF THEM CAN BE ASSIGNED TO 1 OF 3 CATEGORIES

CONFIDENTIALITY, INTEGRITY, AVAILABILITY

THE CIA TRIAD

CONFIDENTIALITY

WE WANT SECRETS TO BE SECRET

INTEGRITY

WE GET WHAT WE EXPECT

AVAILABILITY

WE CAN ALWAYS ACCESS THE INFORMATION

HOW IS IT HELPFUL?

THE QUESTION

HOW CAN THE CIA OF THIS PROJECT BE BROKEN?

CONFIDENTIALITY:

- WHO CAN SEE THIS RESOURCE?
- HOW DO WE STORE CREDENTIALS?
- DO WE LOG SENSITIVE DATA?

INTEGRITY:

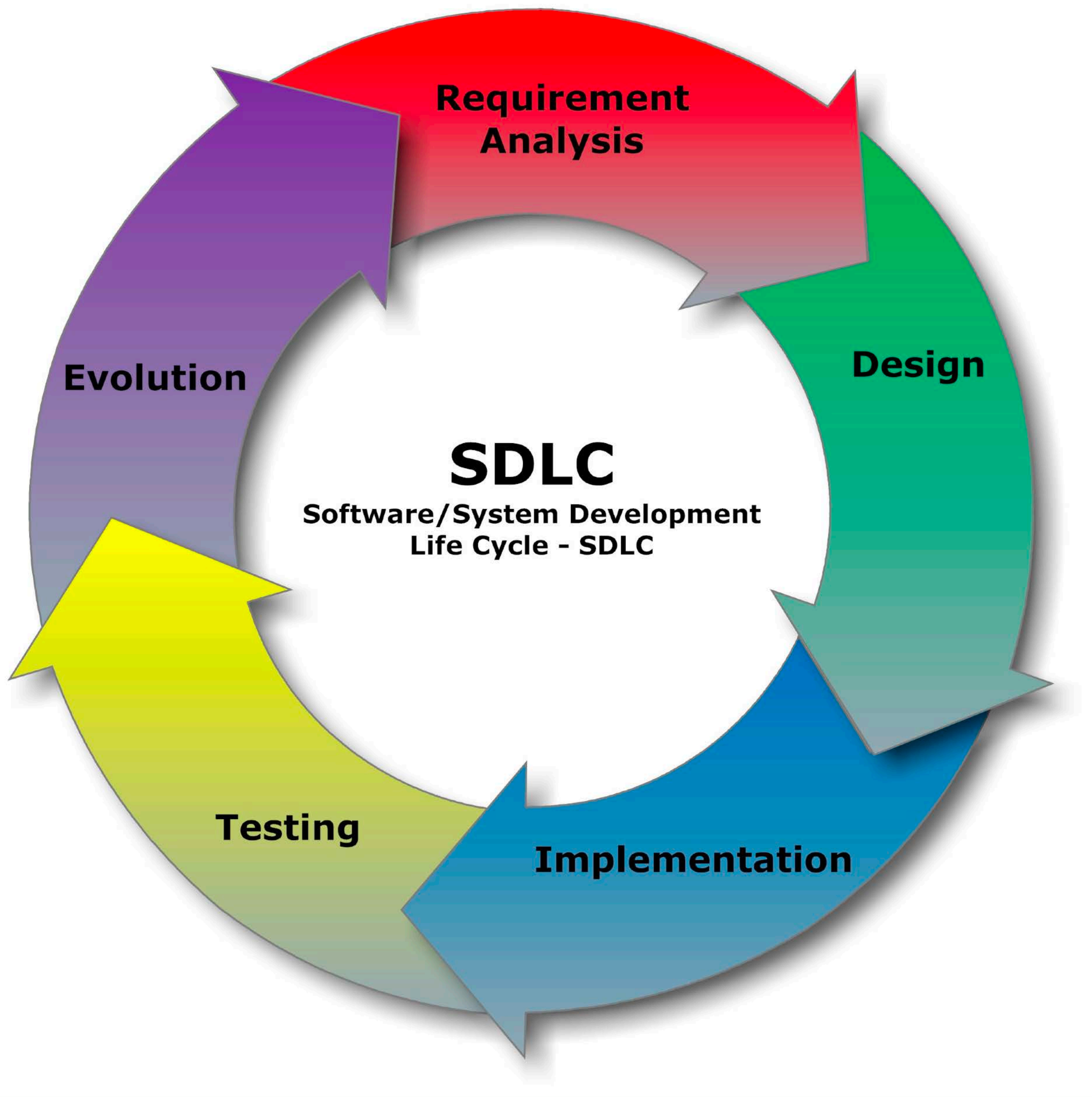
- WHO CAN CREATE, UPDATE AND REMOVE A RESOURCE?
- IS THERE A WAY TO SEE A MALICIOUS ACTOR DELETING ALL RESOURCES?
- WHAT HAPPENS WHEN MALICIOUS DATA IS SENT VIA A FORM?

AVAILABILITY:

- IS THIS ENDPOINT RATE-LIMITED?
- WHAT HAPPENS WHEN EXTERNAL PRODUCT IS DOWN?
- HOW MUCH TIME DOES A DATABASE MIGRATION TAKE?

WHEN SHOULD YOU DO THIS?

🍅 SHIFT SECURITY LEFT

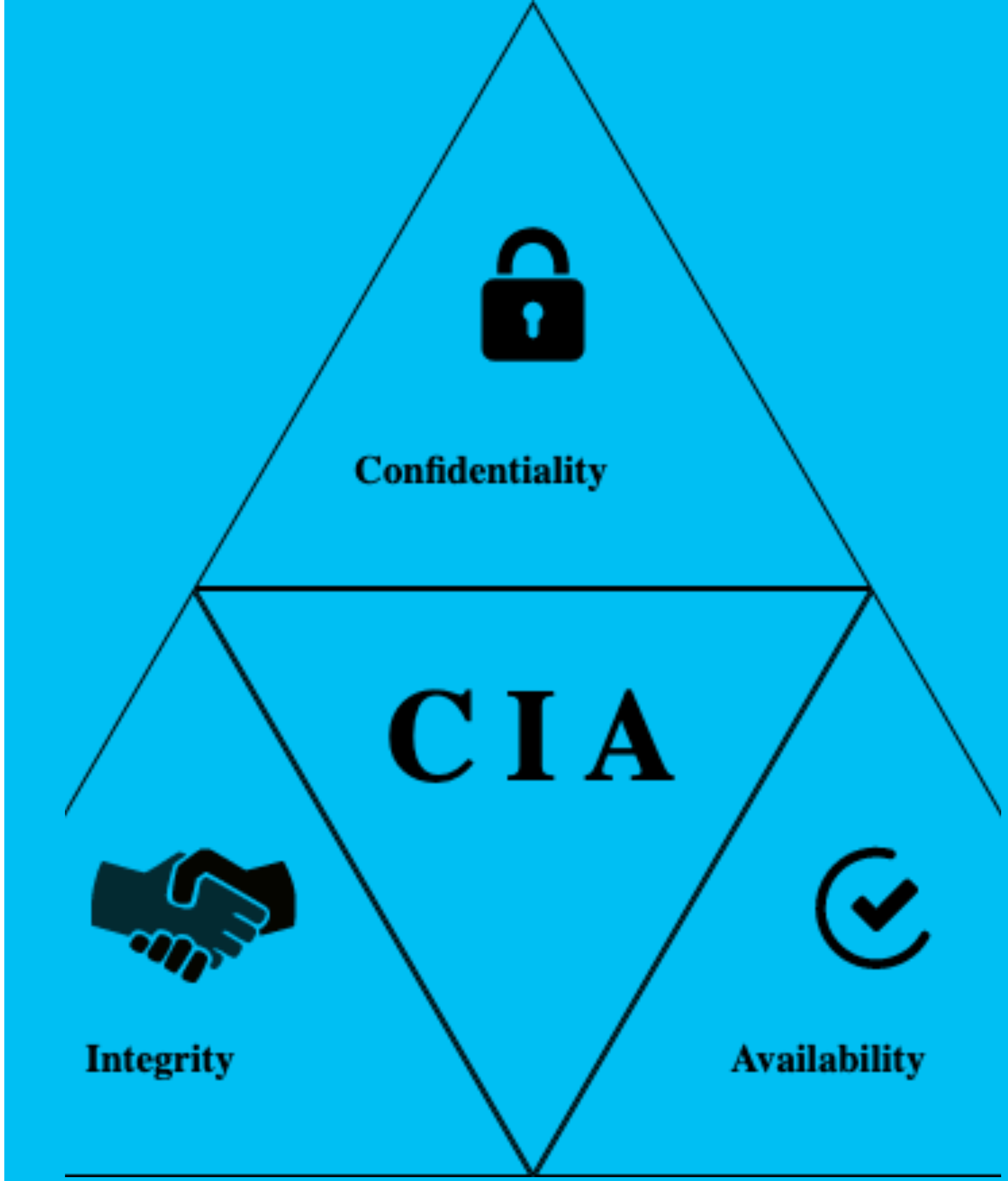

Requirement Analysis
Design
Implementation
Testing
Evolution
SDLC
Software/System Development Life Cycle - SDLC

ANALYSE → DESIGN → DEVELOP → TEST → MAINTAIN

INJECT IT!

HOW TO IMPLEMENT THE CIA TRIAD?

- Present it to your peers,
- Discuss it with your team,
- Make it part of your process,
- Add it to doc templates:
  - Solution Briefs,
  - Enhancement Proposals,
  - Request for Comments.



MOVE FAST AND BREAK THINGS IS OVER