*image credits goes to https://tacticaladversary.io/

TACTICAL ADVERSARY: BUILDING A PRACTICAL INTERNAL RED TEAM

ABHIJITH B R [Abx]

DEFCON 28 SAFE MODE DCG VILLAGE 2020, AUG 7TH

tacticaladversary.io

ABHIJITH B R [Abx]

- Leading Offensive security operations in a global FinTech company
- Former Deputy Manager cyber security at Nissan motor corporation, previously with EY
- A decade of experience in the security domain
- Founder of https://RedTeamVillage.org community
  [No, It is not associated with DC]
- Lead at DEFCON Group Trivandrum (https://dc0471.org/)
- Started running https://tacticaladversary.io blog this year

@abhijithbr

LET'S MAKE IT CLEAR!

VULNERABILITY ASSESSMENT IS NOT RED TEAMING.

PENETRATION TESTING IS ALSO NOT RED TEAMING.

WHAT IS RED TEAM

Historically, a red team was a group of military personnel playing the role of adversaries, the role of the enemy or opposing force team ("RED"), as opposed to the friendly forces team ("BLUE"). With time, the red teams mission and capabilities evolved and they turned into a force tasked with challenging the security posture of military bases, outposts and other "targets".

[Redteams.net]

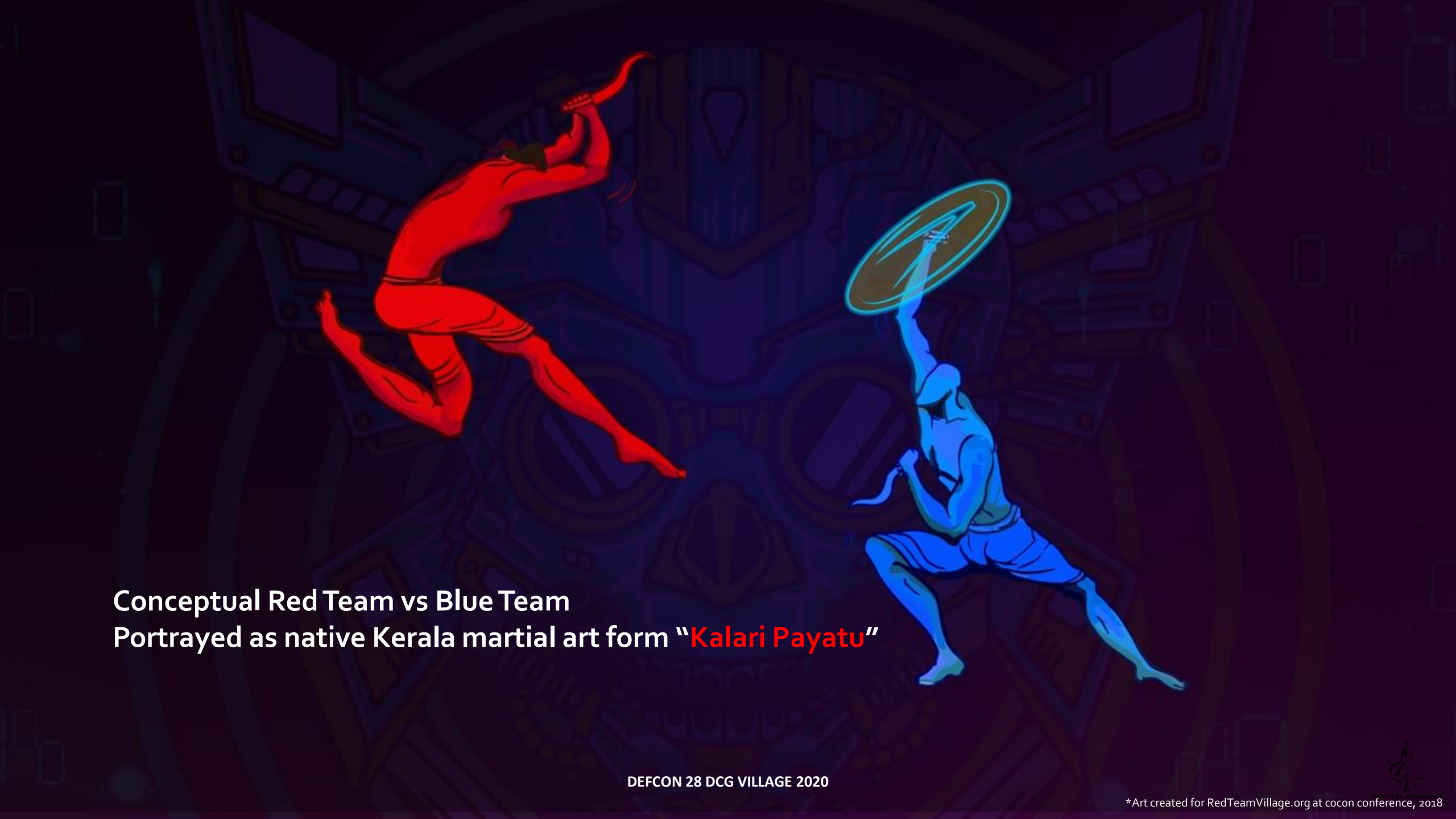
WHAT IS RED TEAM

A **RED TEAM** IS A GROUP OF HIGHLY SKILLED PEOPLE THAT CONTINUOUSLY CHALLENGE THE PLANS, DEFENSIVE MEASURES AND SECURITY CONCEPTS.

[Redteams.net]

Our **Red Team** will be doing pentest and vuln scanning for the clients.

Security sales guy
from Security company XYZ



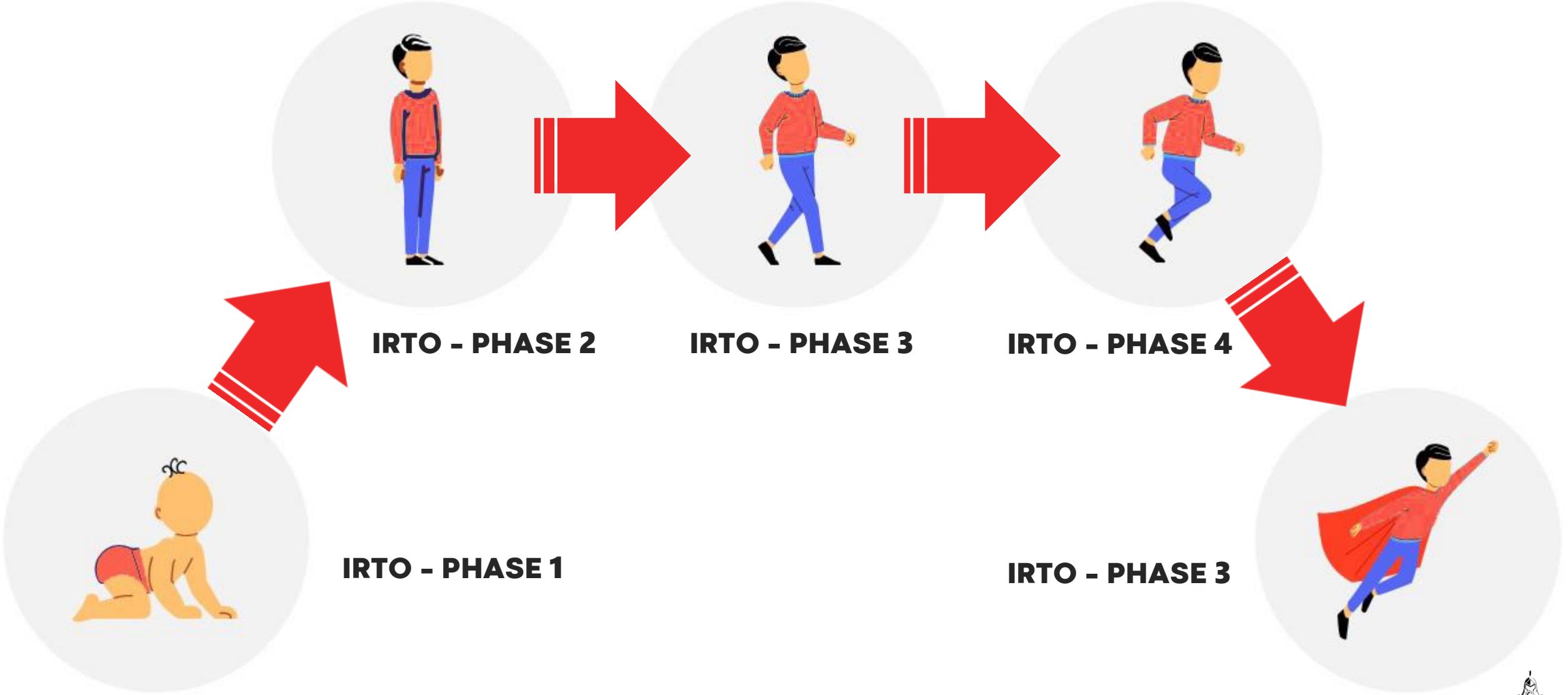
Conceptual Red Team vs Blue Team
Portrayed as native Kerala martial art form "Kalari Payatu"

*Art created for RedTeamVillage.org at cocon conference, 2018

BUILDING AN INTERNAL RED TEAM.

[ADVERSARIAL SIMULATION]

INTERNAL RED TEAM OPERATIONS FRAMEWORK*



this is still a work in progress.

*image credits goes to respective owners.

TACTICAL ADVERSARY

IRTO – PHASE 1 CRAWLING

- Get the budget approval
- Define the practical goals, objectives
- Identify the crown jewels and people
- Rules of engagement (ROE), reporting and other process documentation
- Assistance from the Management and Legal department
- Understand the security posture of the organization
- Hire the talent – The Red Team

THE ~~A~~ TEAM RED

DEFCON 28 DCG VILLAGE 2020

*image credits goes to respective owners.

IRTO – PHASE 2 GET ON YOUR FEET

- Red Team external infrastructure (Digital ocean, GCP, AWS)
- Corp. tools, Improvised open source tooling capabilities
- Identifying the business specific risks
- Be friends with your organization's Blue Team
- Adversarial Emulation (Atomic red team, Caldera etc)
- Manual campaigns against the organization and employees
- Validate current defense mechanisms with blue team (MITRE)
- External attack surface discovery and mapping
- Designing a remediation process to address issues

IRTO – PHASE 3 START WALKING

- Improved Tools, techniques and procedures (TTP's) based on current security posture
- Identify and eradicate findings 1, 2 - crown jewels and people*
- Evaluation of Incident response process*
- Automated Adversary Emulation
- Automated campaigns
- Targeted APT emulation based on Threat Intel
- Improvised RTO process documentation

IRTO – PHASE 4 START RUNNING

- Collaborative and continuous Purple team exercises
- Enterprise tooling capabilities
- Targeted campaigns against the Crown jewels and key people
- Overt physical security assessments
- Continuous awareness programme for employees and key people
- Continuous training process for operators and defenders
- Proactive remediation process and plans

IRTO – PHASE 5 TIME TO FLY

- Matured red team operations
- Significant improvement of organizational security posture
- Highly skilled operators
- Covert physical security assessments
- Custom tooling capabilities
- Continuous Adversary simulation to keep the defenders on their toes.
- Continuous RTO with well defined process

PLANS: STRATEGIC AND TACTICAL

STRATEGIC PLAN = **TACTICAL PLAN 1** + **TACTICAL PLAN 2** + **TACTICAL PLAN N**

[Long term objective]

[Divided into short term tactical engagements]

**The management always need updates*

Q&A

Reach me on Discord **Abx#1474**

twitter: **@abhijithbr**

THANK YOU ☺

Special thanks to,

Jayson E Street

DEF CON Groups

TX and DEF CON Group Delhi

DEF CON Group Trivandrum members

*image credits goes to https://tacticaladversary.io/