

FIVE PHASES OF IRTOF: KICK-STARTING YOUR ORGANIZATION'S INTERNAL **RED TEAM OPERATIONS PROGRAMME**

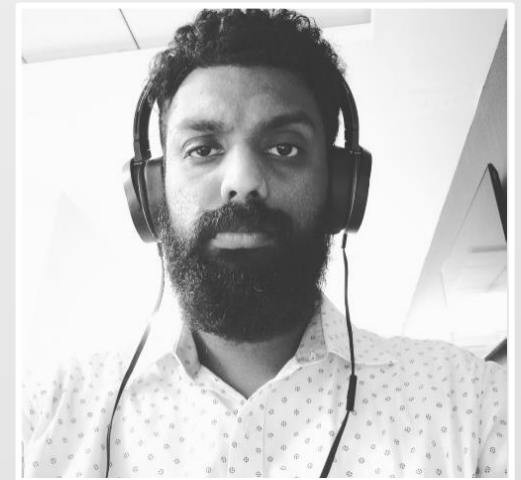
ABHIJITH B R [Abx]

BSIDES DELHI, OCT 18, 2020



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
- Started running <https://tacticaladversary.io> blog this year
- Founder of <https://RedTeamVillage.org> community
[No, It is not associated with DC]
- Lead at DEFCON Group (<https://dco471.org/>)



@abhijithbr

DEFINITIONS?
WE STILL NEED TO DO THIS.

**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*



ADVERSARY EMULATION.

ADVERSARY SIMULATION.

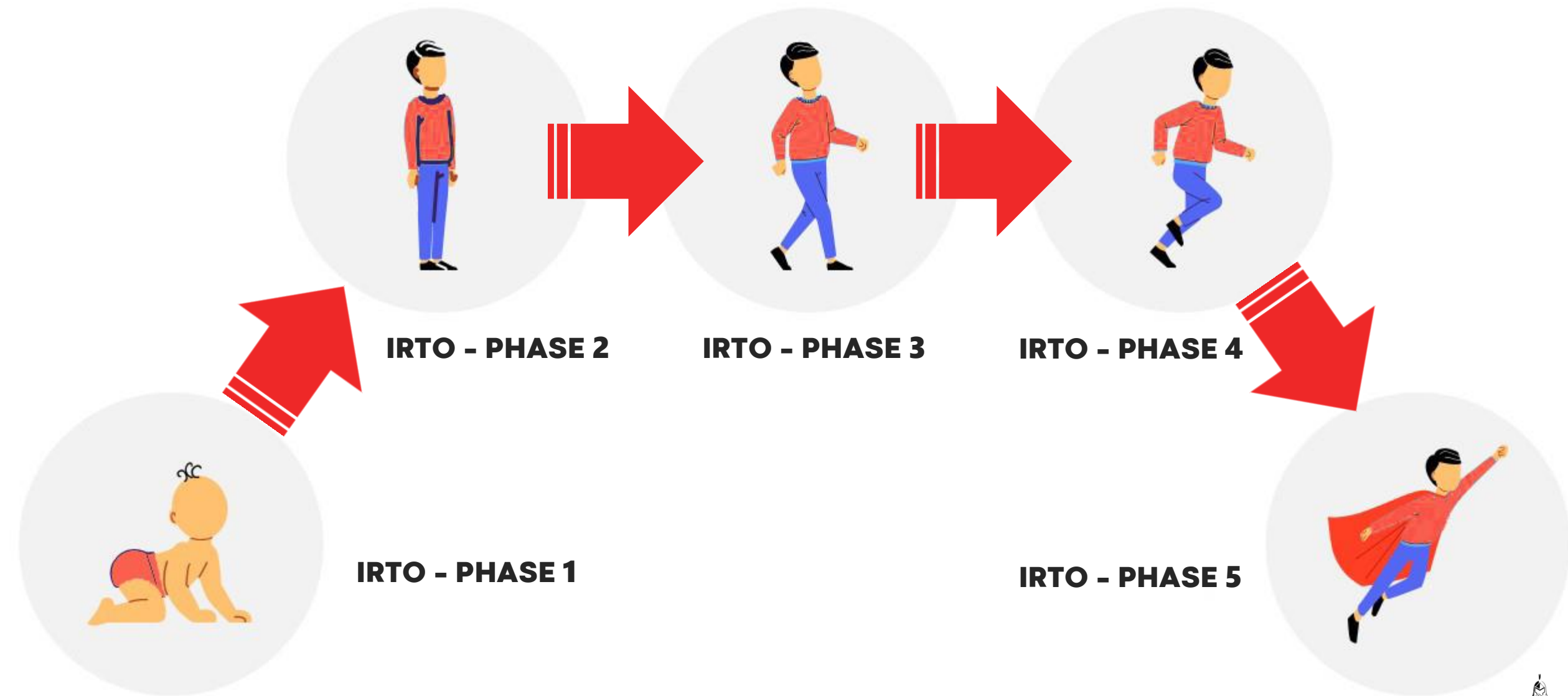
[ADVERSARIAL SIMULATION]

[FULL SCOPE ADVERSARIAL ASSESSMENT]

BUILDING AN INTERNAL RED TEAM.

[ADVERSARIAL SIMULATION and FULL SCOPE]

INTERNAL **RED TEAM** OPERATIONS FRAMEWORK [IRTOF]*



**this is still a work in progress.*

BSIDES DELHI 2020

**image credits goes to respective owners.*



TACTICAL ADVERSARY

IRTO - PHASE 1 CRAWLING

- Define the practical goals, objectives
- Get the budget approval
- Identify the crown jewels and people
- Rules of engagement (ROE), reporting and other process documentation
- Assistance from the Management and Legal department
- Understand the technologies in use – On premise infra, Cloud, Active Directory, Devices etc
- Understand the security posture of the organization
- Hire the talent – The Red Team

A FAIR WARNING - COALFIRE SECURITY CONSULTANTS CHARGED

These photos, provided by the Dallas County Jail, show Justin Wynn and Gary Demercurio. Court officials in central Iowa say they're behind the hiring of two men who were arrested after breaking into the Dallas County Courthouse. Demercurio, 43, of Seattle and Justin Wynn, 29, of Naples, Florida, were found in the courthouse early Wednesday, Sept. 11, 2019, after an alarm was tripped. Both face burglary charges and are being held on \$50,000 bond apiece. (Photo: Dallas County Jail via AP)

THE COURTHOUSE:

<https://darknetdiaries.com/episode/59/>

PHYSICAL SECURITY LEGAL DOCS FROM TRUSTEDSEC:

<https://github.com/trustedsec/physical-docs>

- <https://www.trustedsec.com/blog/a-message-of-support-coalfire-consultants-charged/>
- <https://www.coalfire.com/News-and-Events/Press-Releases/Coalfire-CEO-Tom-McAndrew-statement>
- Proper escalation
- Points of contact
- Strong Legal documentation, ROE

THE ~~A~~ TEAM RED



BSIDES DELHI 2020

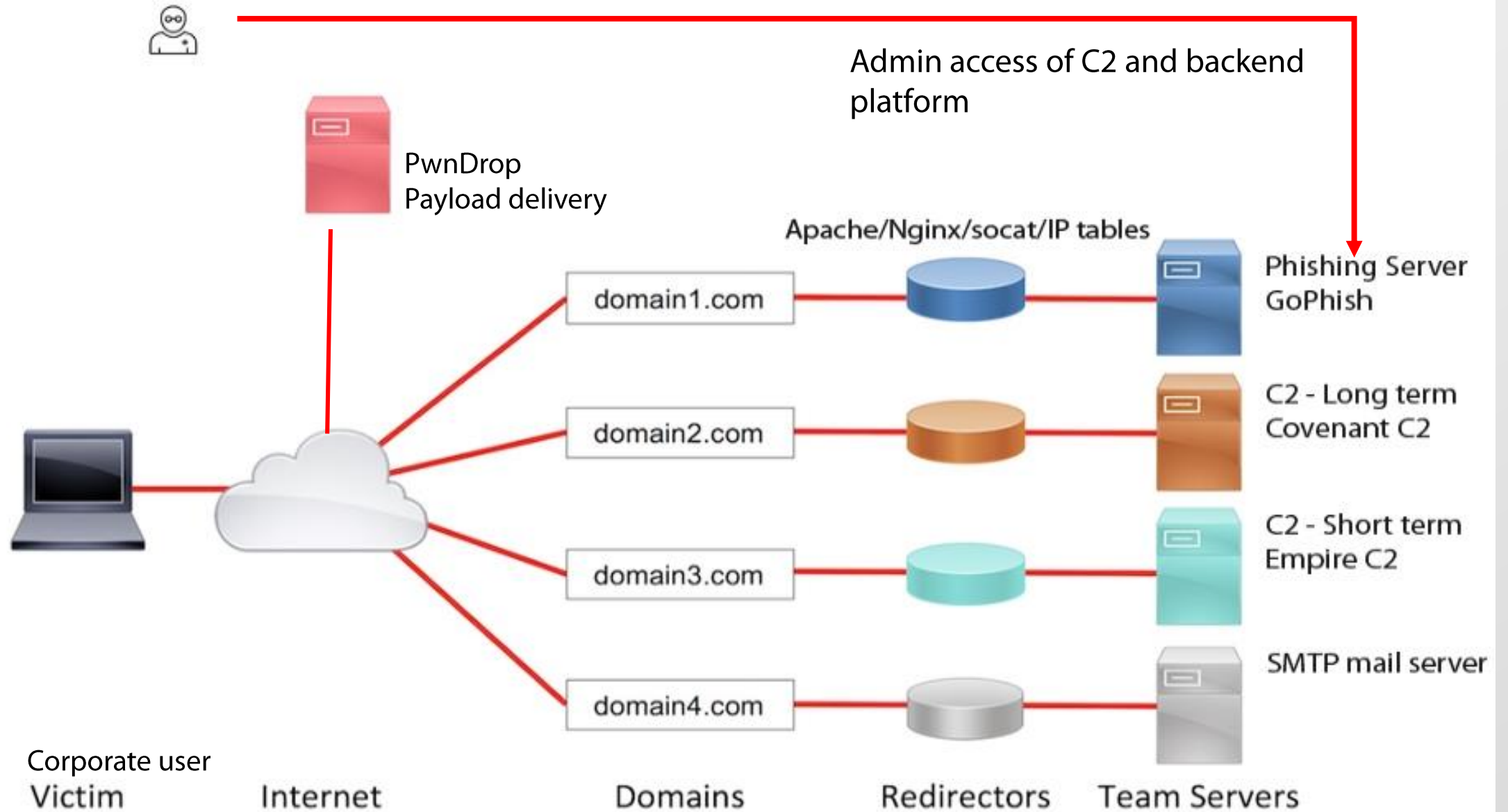
*image credits goes to respective owners.



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)
- Validate current defense mechanisms with **blue team** (MITRE)
- Manual campaigns against the organization and employees
- External attack surface discovery and mapping
- Designing a remediation process to address issues

- Basic **Red Team** external infrastructure (Digital ocean, GCP, AWS)



IRTO - PHASE 3 START WALKING

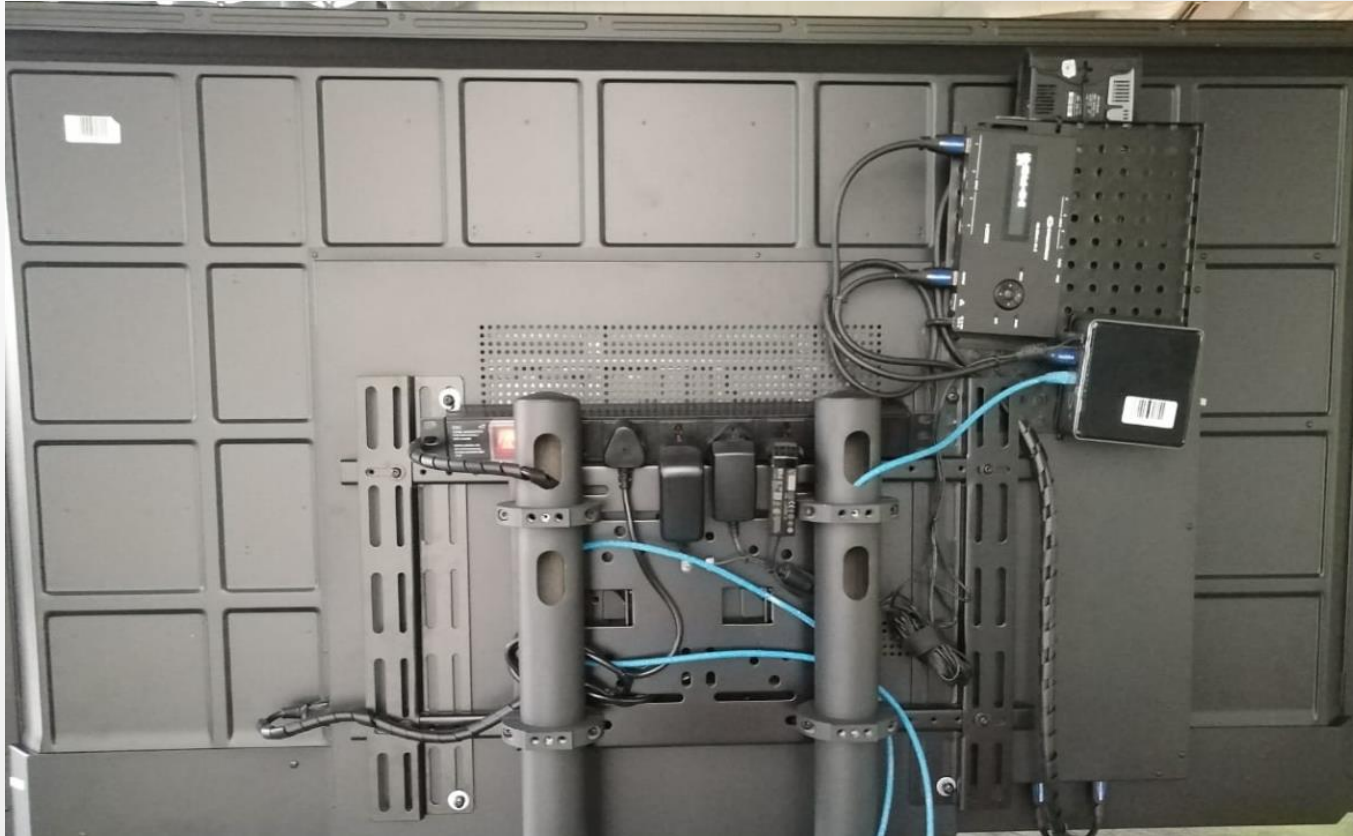
- Improved Tools, techniques and procedures (TTP's) based on current security posture
- Identify and eradicate findings 1, 2 - crown jewels and people*
- Evaluation of Incident response process*
- Automated Adversary Emulation
- Automated campaigns
- Targeted APT emulation based on Threat Intel
- Improvised 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 4 START RUNNING

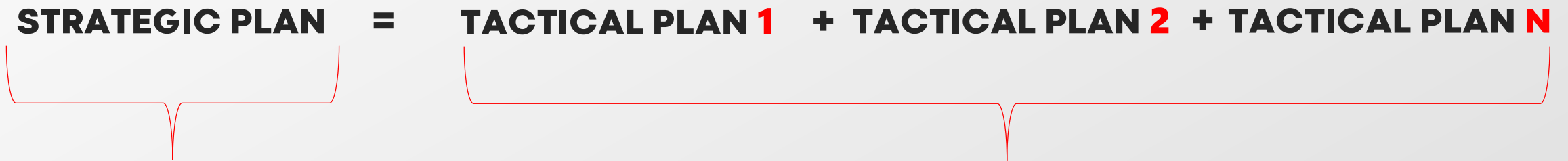
- Overt physical security assessments



IRTO - PHASE 5 TIME TO FLY

- Matured **red team** operations
- Significant improvement of organizational security posture
- Highly skilled operators
- Well defined **Purple team** model to measure the progress of **Red** and **Blue** team capabilities.
- 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

$$\text{STRATEGIC PLAN} = \text{TACTICAL PLAN 1} + \text{TACTICAL PLAN 2} + \text{TACTICAL PLAN N}$$


[Long term objective]

[Divided into short term tactical engagements]

**The management always need updates*



Conceptual **Red Team** vs **Blue Team**
Portrayed as native Kerala (India) martial art form "**Kalari Payatu**"



Q&A

Reach me on Discord **Abx#1474**

twitter: **@abhijithbr**

THANK YOU 😊
BSIDES DELHI

