BLAZE

INFORMATION SECURITY

BC
SB
2019

BLAZE CYBER SECURITY BRIEFING 2019

Willian Mayan

Security Engineer
at Blaze Information Security

Automating red team infrastructure

BLAZE

Summary

BLAZE

SUMMARY

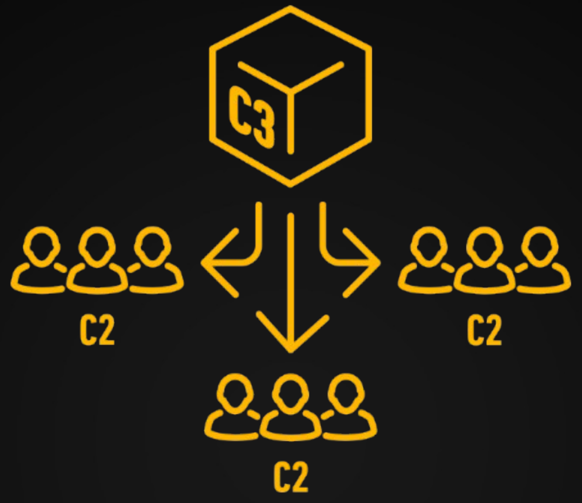
WILDFIRE
LABS

This presentation intends to serve as **an introductory basis for a research that is currently being held at Blaze’s WILDFIRE LABS**

SUMMARY

Here **we will address a disposal architecture for Command Control Center (C3)** in which the resources are created and disposed in their stages of use

SUMMARY



C3 aims to secure resources for multiple teams during testing steps, provisioning resources for the C2 environments

Agenda

BLAZE

Red Team

Problems

Automating

Proof of concept

BLAZE

RED TEAM #1

In possession of the objectives to be achieved by the team during the mission responsibiles are scaled for task creation and activity execution

RED TEAM #2

From this first stage, extremely relevant information for the creation of the necessary infrastructure is already extracted

RED TEAM #3

As exemplified here, we will have a test with no information whatsoever, from physical tests to tests that make use of social engineering

SCOPE EXAMPLE

Type

☐ White Box
☐ Gray Box
☑ Black Box

Scope

☑ Physical
☑ Remote
☐ Wireless
☑ Web-App
☐ App
☐ Social Engineering
  ☑ Phising
☐ Rogue-devices
☑ Insider
☐ DoS

RED TEAM SOLDIER SELECTION

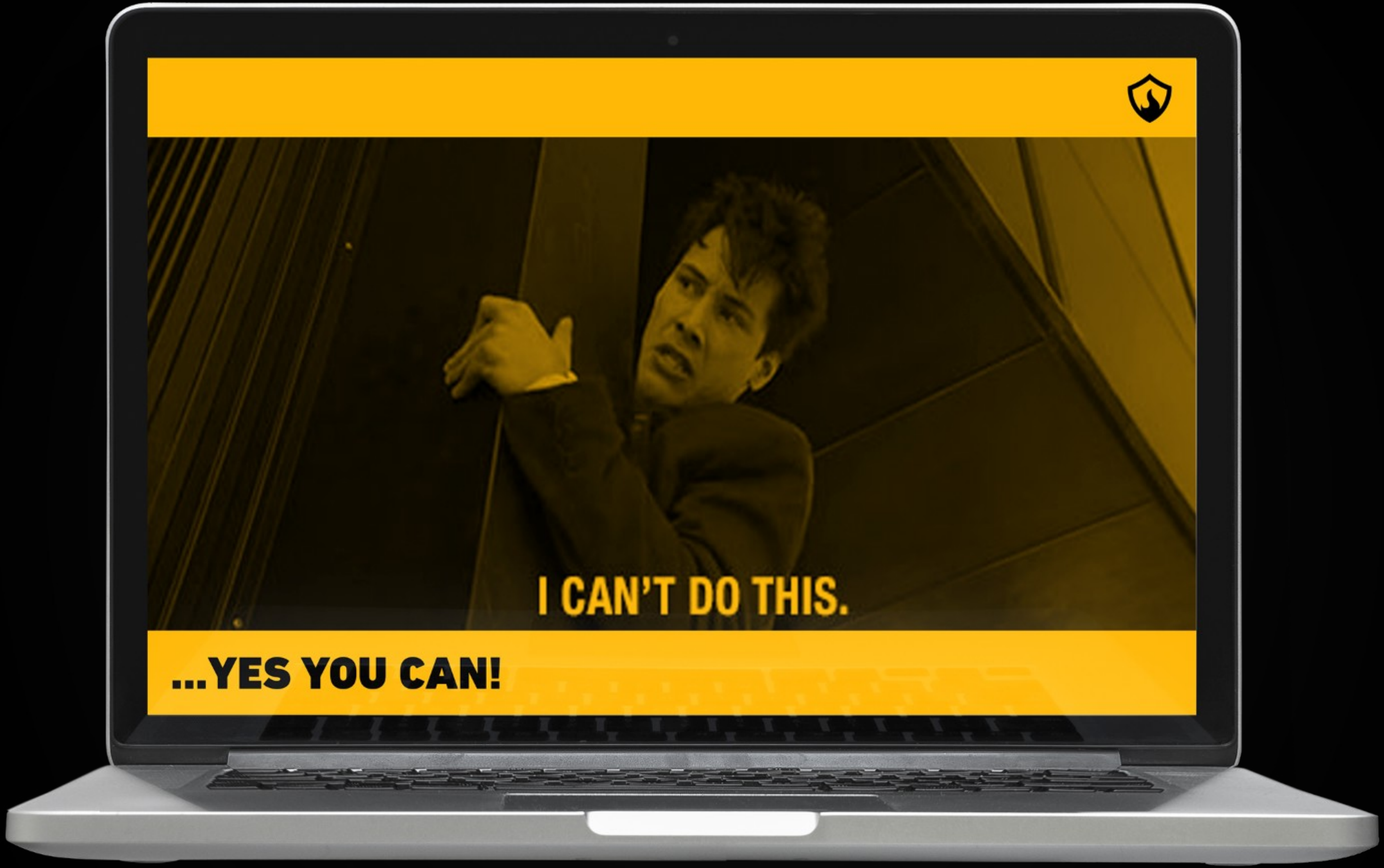
SOLDIERS:

○ Malware Engineer
○ Security Engineer
○ Network Engineer
○ Cloud Engineer
○ Insider

BLAZE

Problems

BLAZE



...YES YOU CAN!

Image credit: The Matrix (1999, Warner Bros.)

PROBLEMS BEGIN

YOU NEED QUICK SOLUTIONS FOR THE PROBLEMS LIKE:

- Rework
- Multiple people working on the project
- Blue team drops C2’s IP
- Setting up services during mission time
- Physical attacks need an internet exit
- Structure Exposure Time
- Every other problem that surfaces during the project
- Etc.

CALL ME...

...THE TELEPHONIST!

Image credit: The Matrix (1999, Warner Bros.)

Automating

BLAZE

AUTOMATING

C3 – TECHNOLOGIES

ANSIBLE

CLIENT ONLY
SIMPLE CONFS YAML
EASY SETUP / MANAGEMENT
SCALABLE

docker

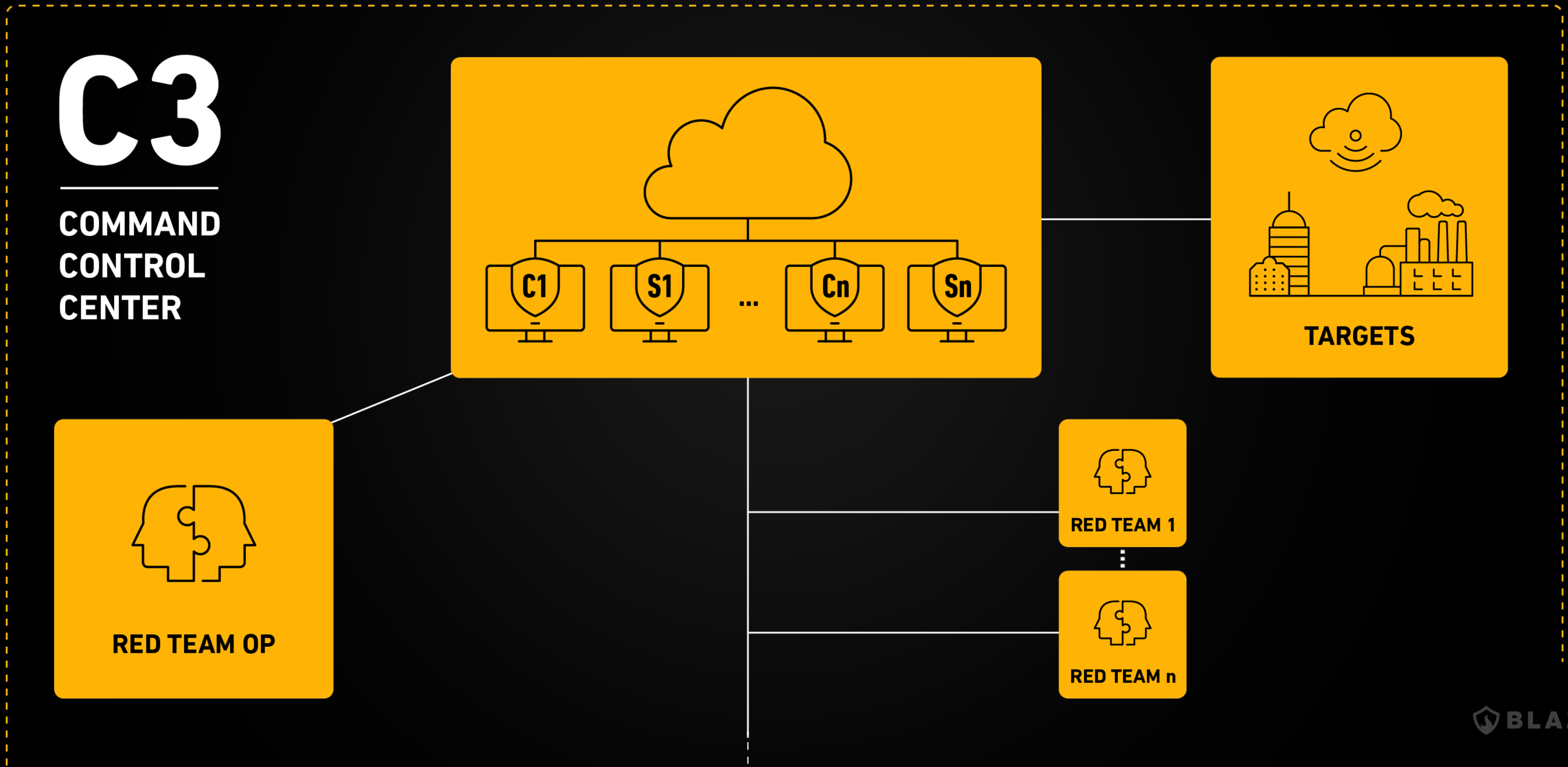
DOCKER COMPOSE
CUSTOM IMAGES AND SERVICES

{ api }

VARIOUS APIs

HashiCorp
Terraform

AUTOMATING


C3
COMMAND
CONTROL
CENTER
C1
S1
...
Cn
Sn
TARGETS
RED TEAM OP
RED TEAM 1
RED TEAM n

Proof of concept

BLAZE

PROOF OF CONCEPT

Image credit: The Matrix (1999, Warner Bros.)

Questions?

BLAZE

Be secure. Be ahead. Be Blaze.

THANK YOU!

BLAZE

www.blazeinfosec.com

info@blazeinfosec.com

Brazil
Rua Visconde de Jequitinhonha
279. Office 701. Recife

Portugal
Praça Bom Sucesso 131
Península, Office 206, Porto

Poland
Rynek Główny 28
33-332, Kraków

BR: +55 81 3071 7148
PT: +351 222 463 641
PL: +48 792 436 755

BLAZE