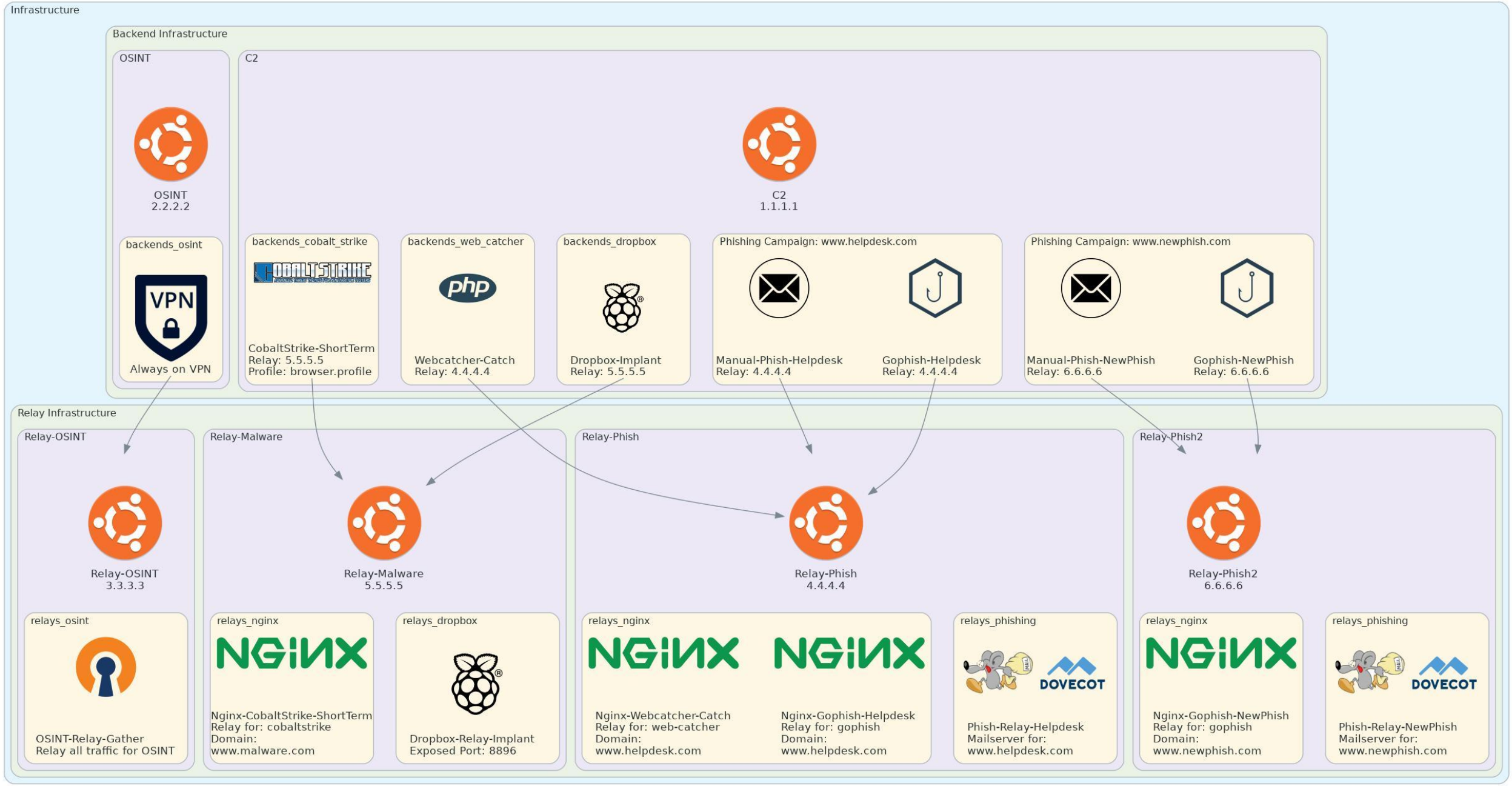
Red Wizard

User friendly, automated RT infrastructure

https://github.com/SecuraBV/RedWizard

Secura

Goal for today:
Publish the Red Wizard tool and show you its capabilities



Infra Deployment

Agenda

- (Short) Intro to Red Teaming
- Red Teaming and infrastructure
- Red Wizard: Introduction
- Red Wizard: Basic Building Blocks
- Red Wizard: Demo Time
- Closing thoughts

Secura

Welcome! Who am I?

Ben Brücker

Domain Manager: Red Teaming
@Secura since 2014

Trained Penetration Tester /
Social Engineer / Trainer
OSCP, GXPN, GMOB, MLSE

Secura

(Short) Intro to Red Teaming

A realistic cyber attack simulation to test the detection, response and mitigation capabilities of the defenders.

Full-Spectrum Operations

Physical Access

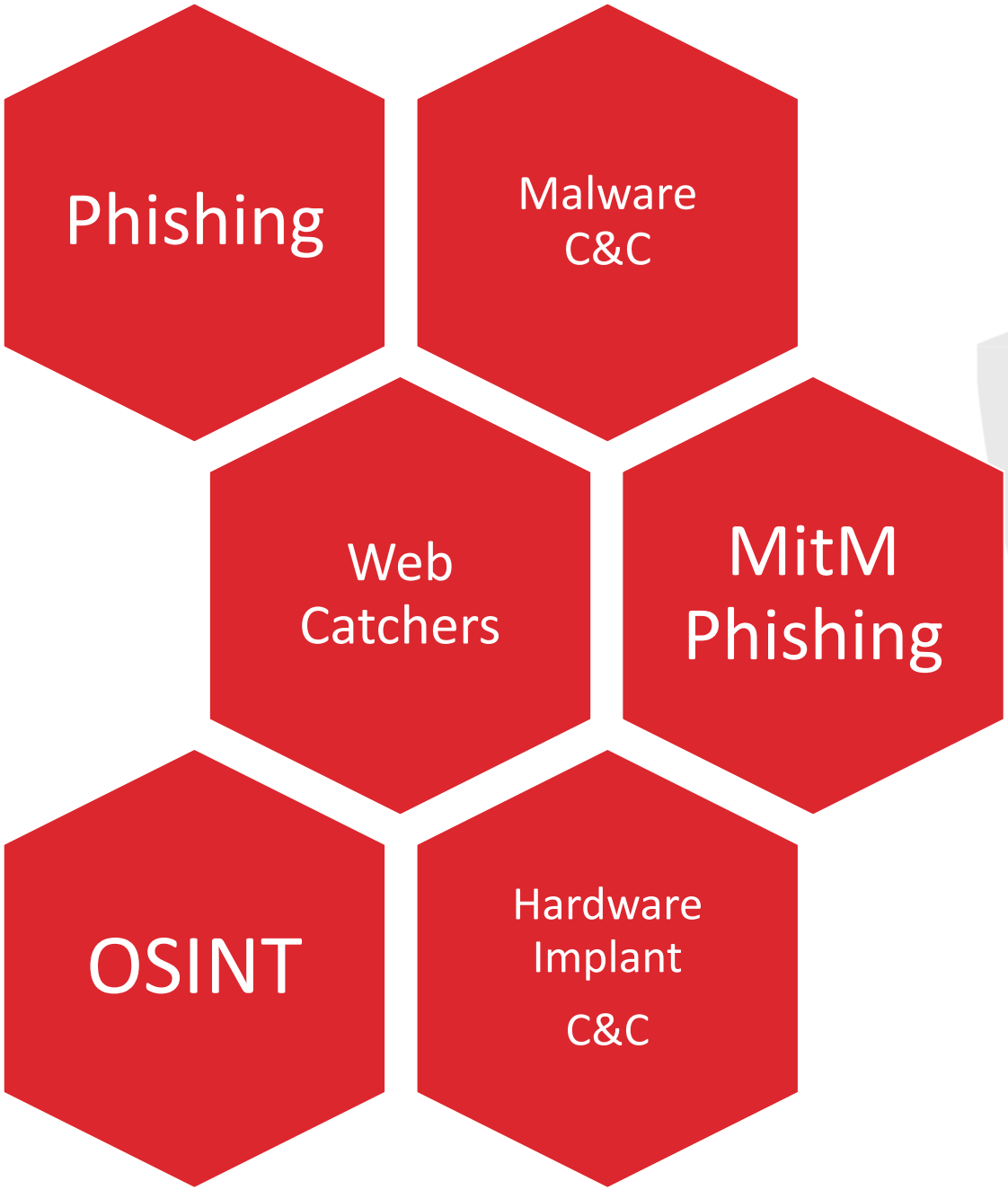
Social Engineering

Rogue Devices

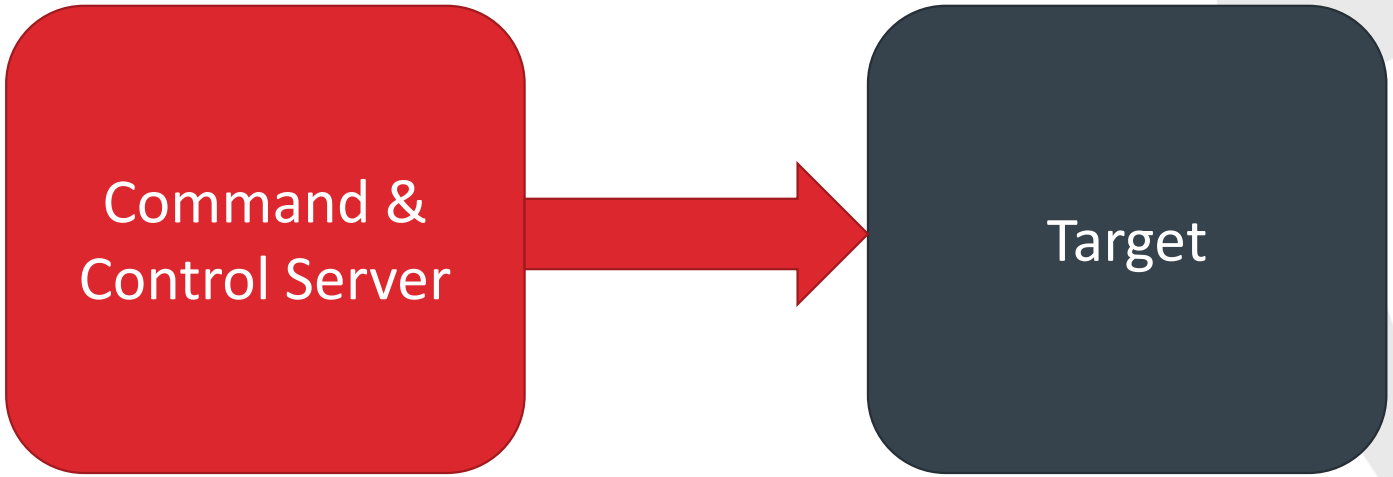
(Remote) Network Compromise

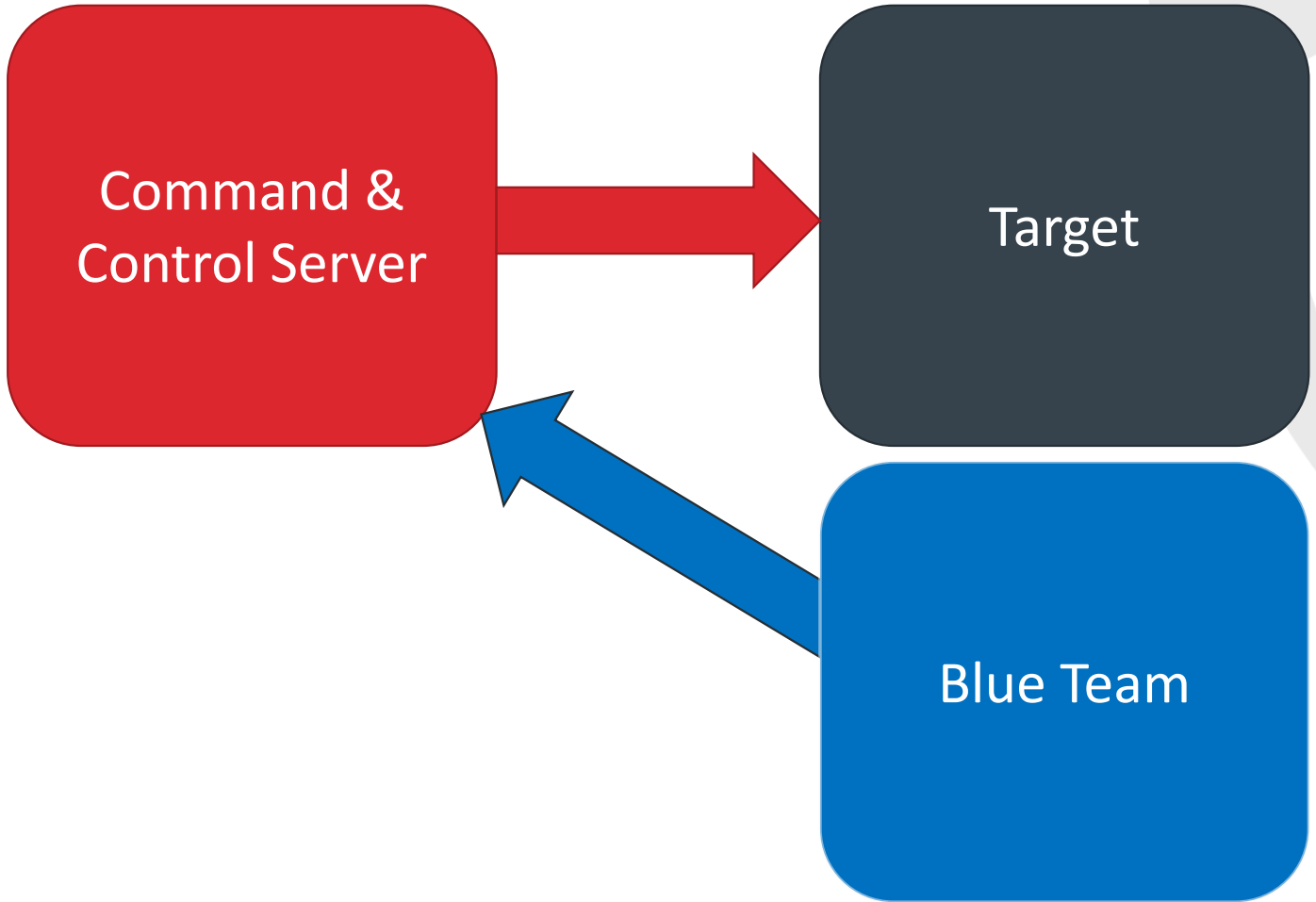
Red Teaming is unforgiving.

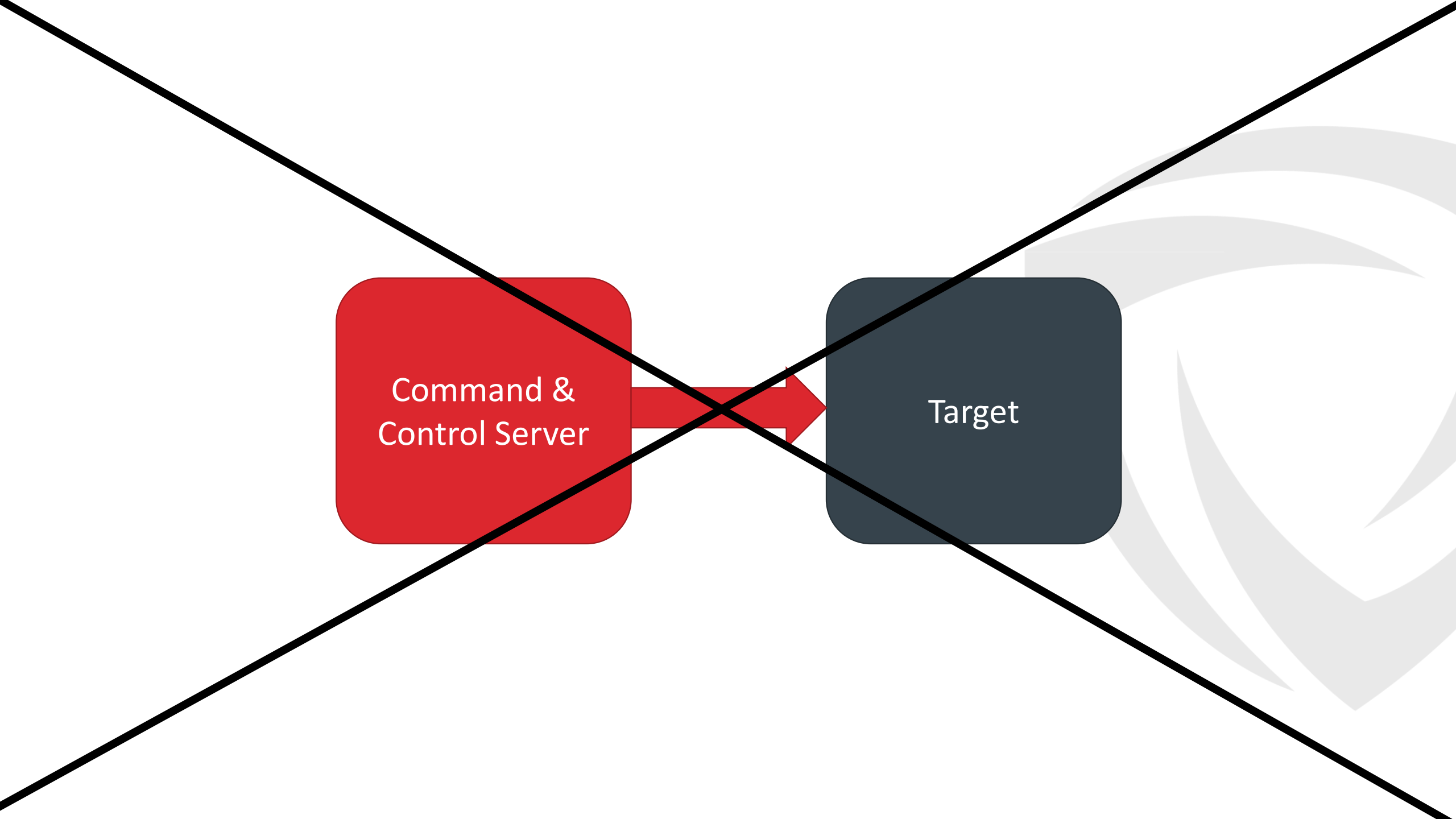
Red Teaming and infrastructure


Phishing
Malware C&C
Web Catchers
MitM Phishing
OSINT
Hardware Implant C&C

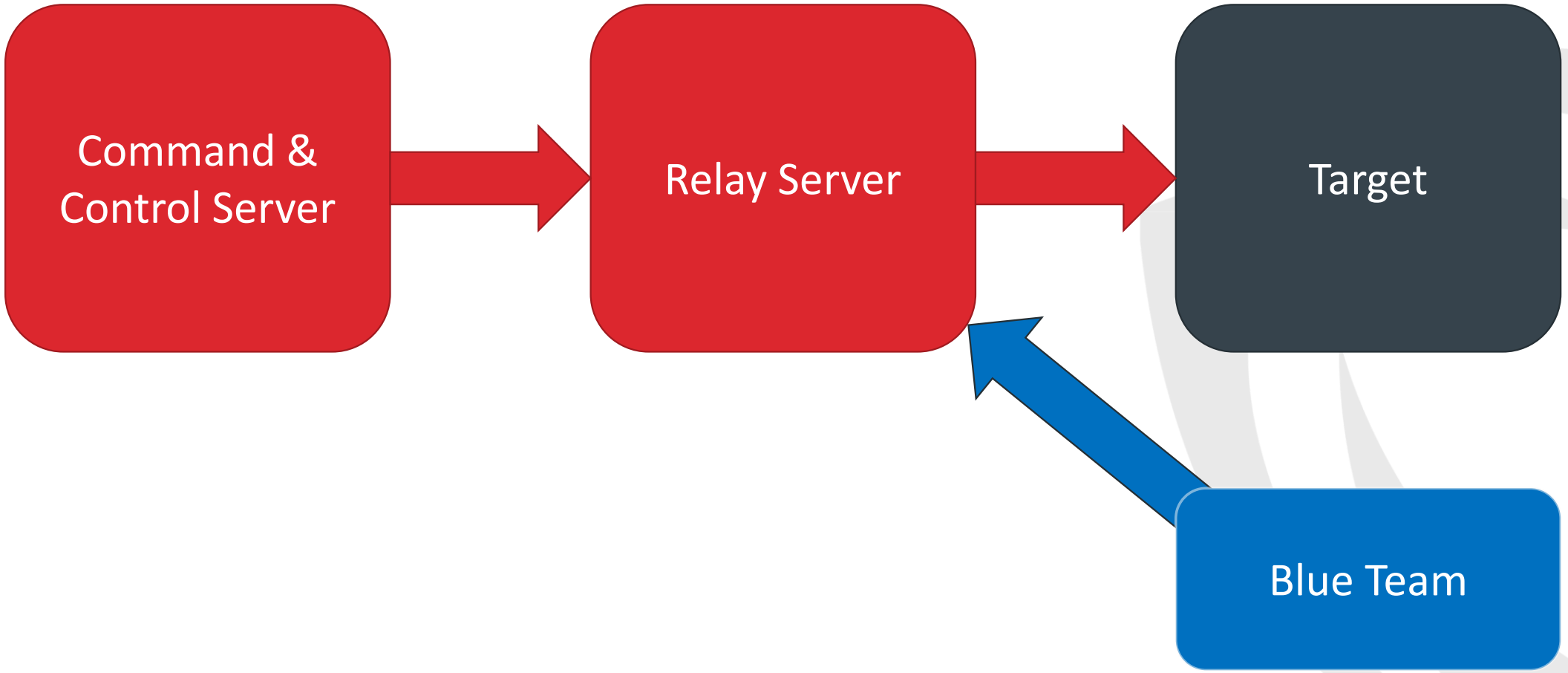
Red vs. Blue

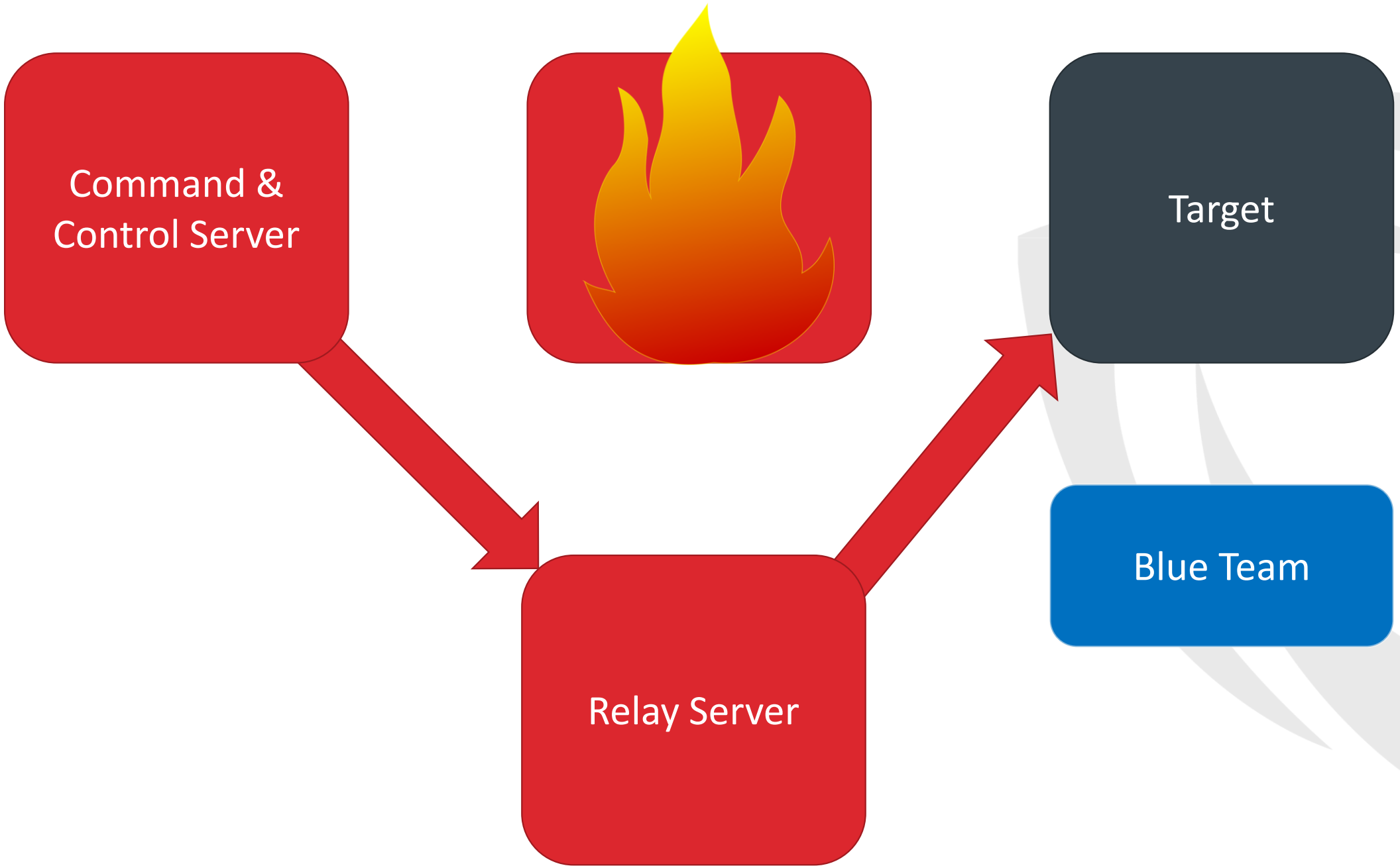

Command &
Control Server
Target


Command &
Control Server
Target
Blue Team


Command &
Control Server
Target


Command &
Control Server
Relay Server
Target


Command &
Control Server
Relay Server
Target
Blue Team


Command &
Control Server
Target
Relay Server
Blue Team

You have to do this a lot

Introducing:
Red Wizard

What is Red Wizard?

Why did we make it?

- Deploying stuff manually is painful
- Must be easily explainable to new team members
- Infrastructure deployer is not always the operator
- Information sharing on how to use an infra costs time
- Spending less time on infra deployment results in more time for our customers

Secura

Is it unique? Is it rocket science?

Red Wizard Design Principles

- Simplicity trumps fanciness
- Operational Security (OPSEC)
- Must be robust
- No magical Black Boxes
- Everything must be self-documenting
- Easily extendable
- Preconfigured listeners / phishing profiles
- Log everything

Secura

Maturity of the tool?

Technology behind Red Wizard?

Step 1	• Create a base configuration for all your deployments
Step 2	• Create a configuration for a new RT campaign
Step 3	• Create an inventory of systems
Step 4	• Deploy your infrastructure

Secura

Deployment Requirements

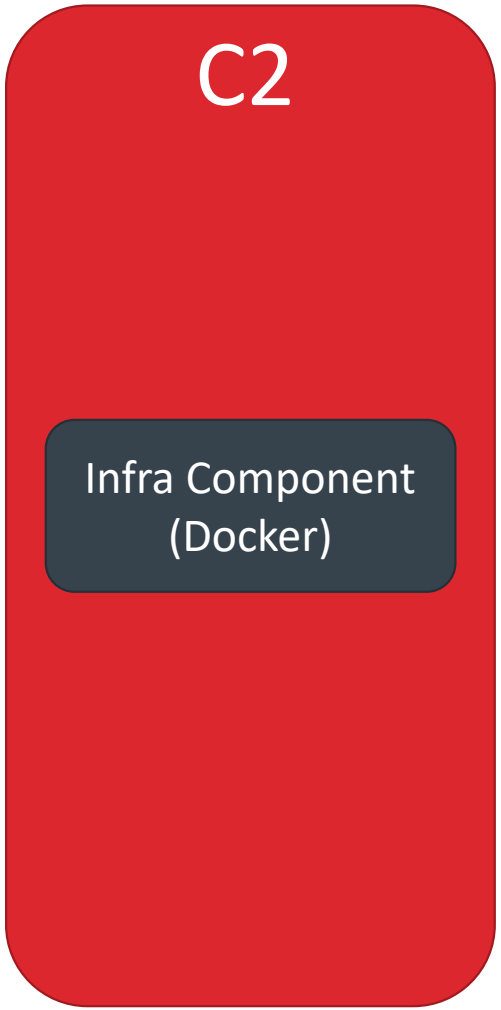
- Ubuntu 22.04 on the deployment system
  - (Your laptop or a VM is fine)
- Clean Ubuntu 20.04 on all target machines
  - (Will support 22.04 in the near future)
- 1 deployment user
  - (Configured for key-based SSH access on all machines)
- Deployment user has identical sudo password on all machines

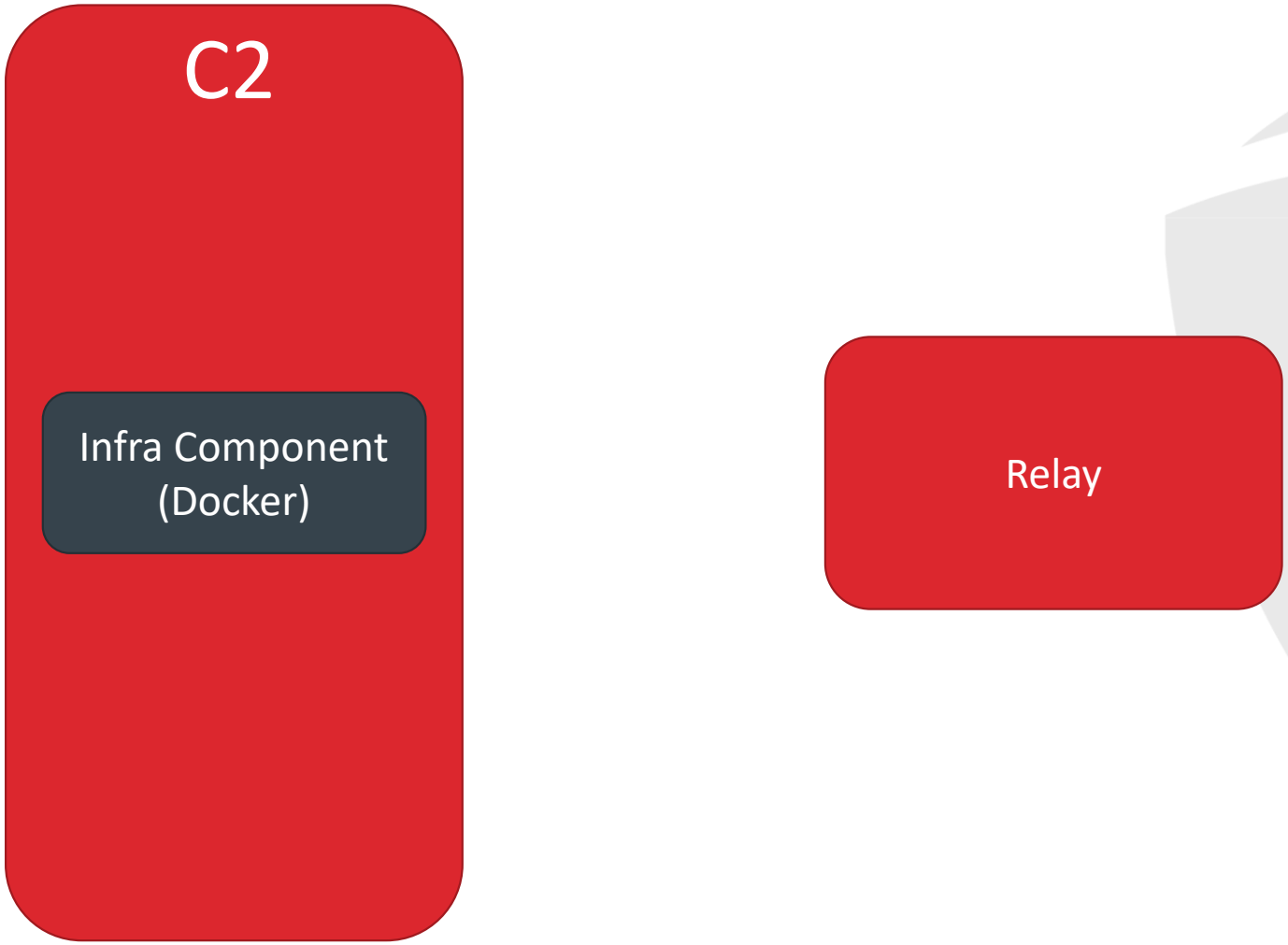
Secura

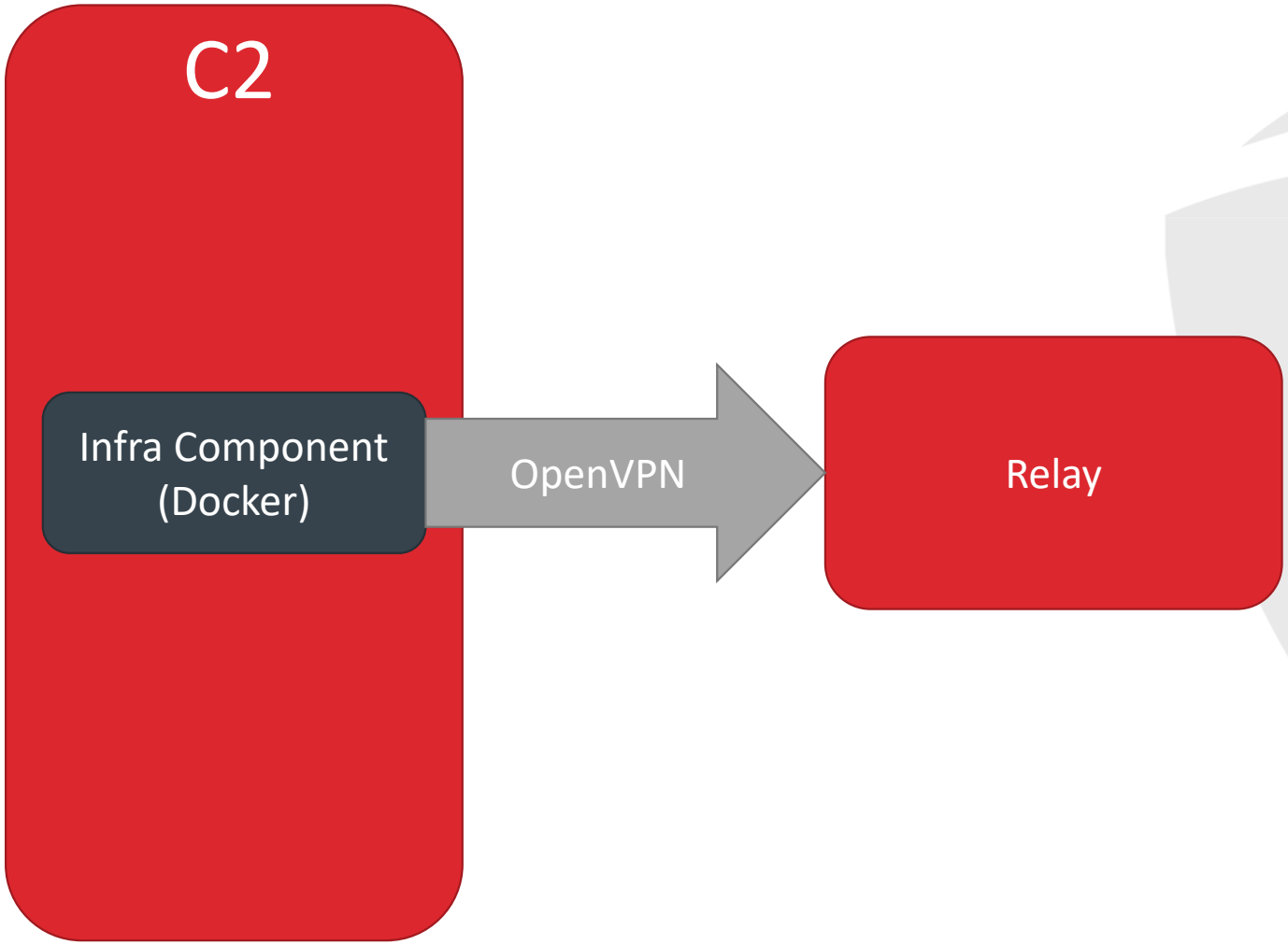
Red Wizard

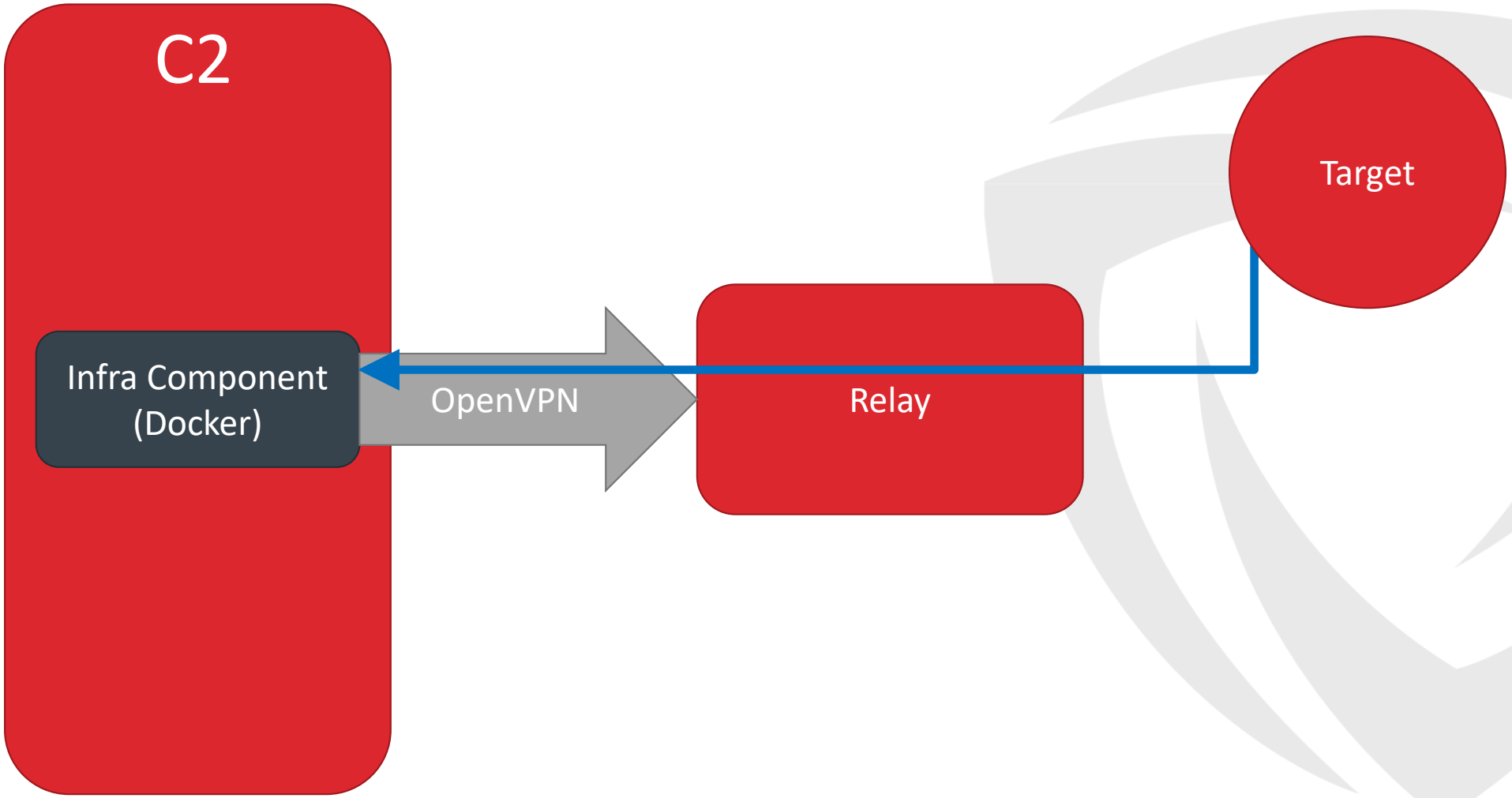
Basic Building Blocks

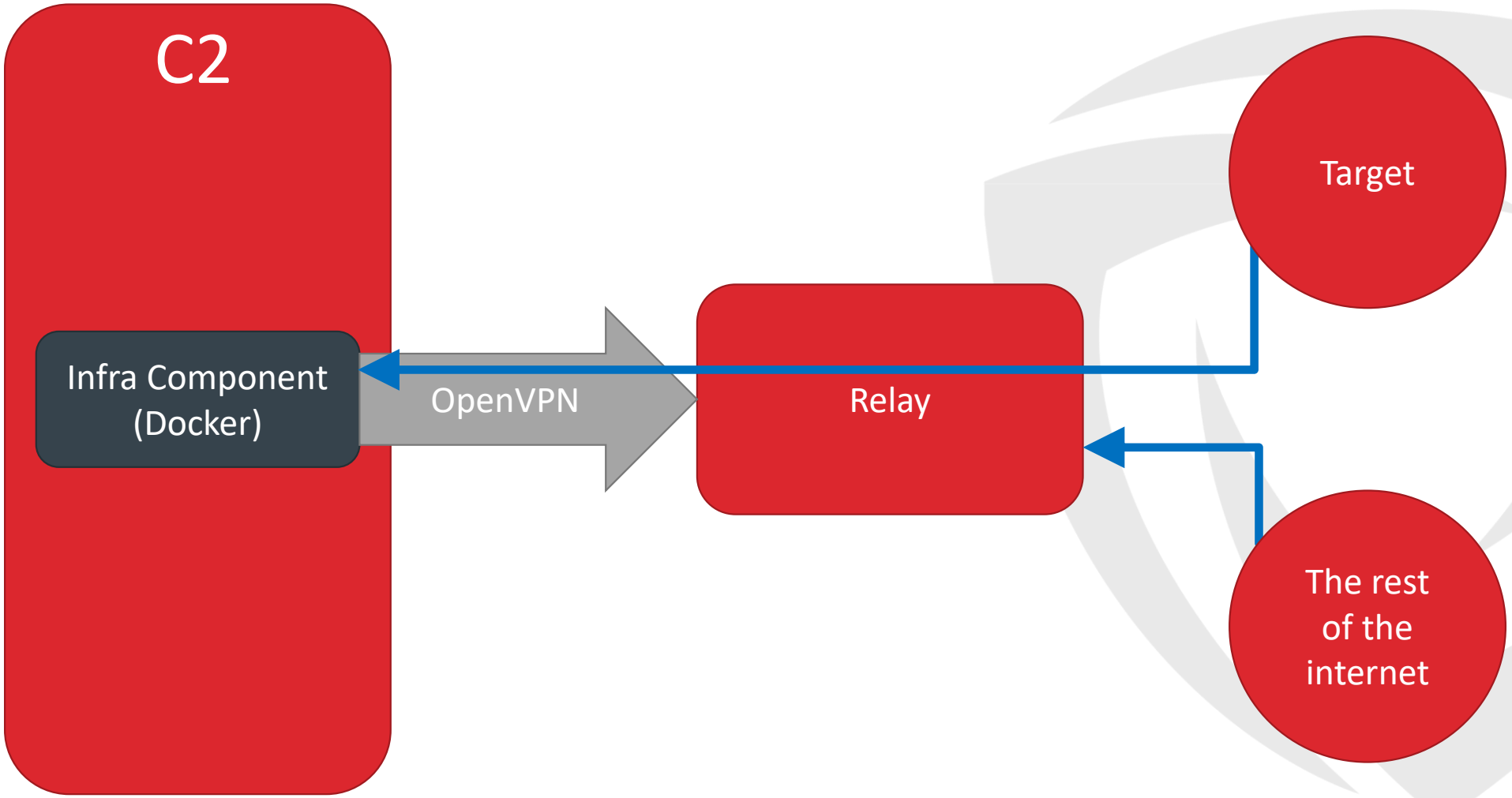

C2

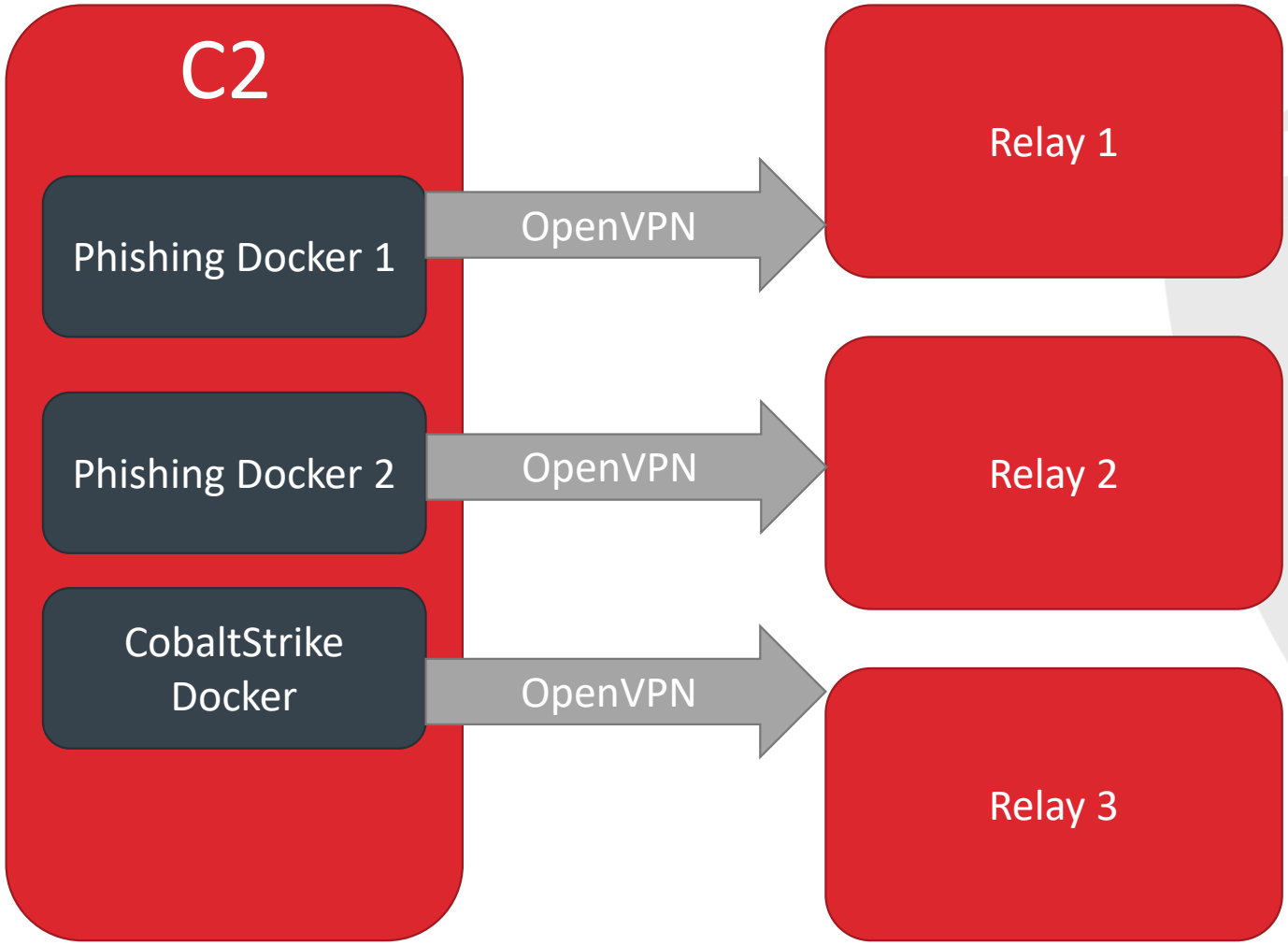

C2
Infra Component
(Docker)

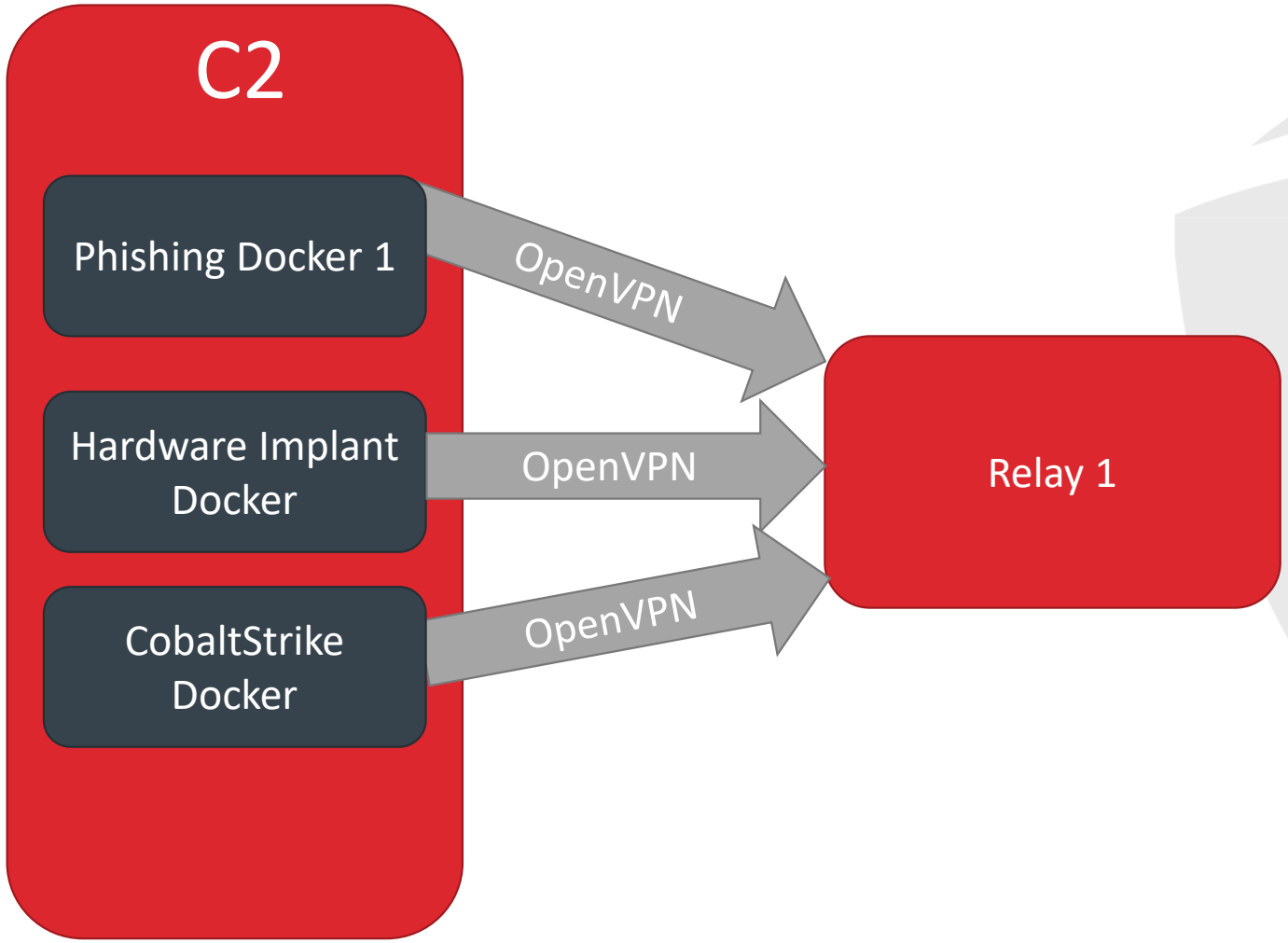

C2
Infra Component
(Docker)
Relay

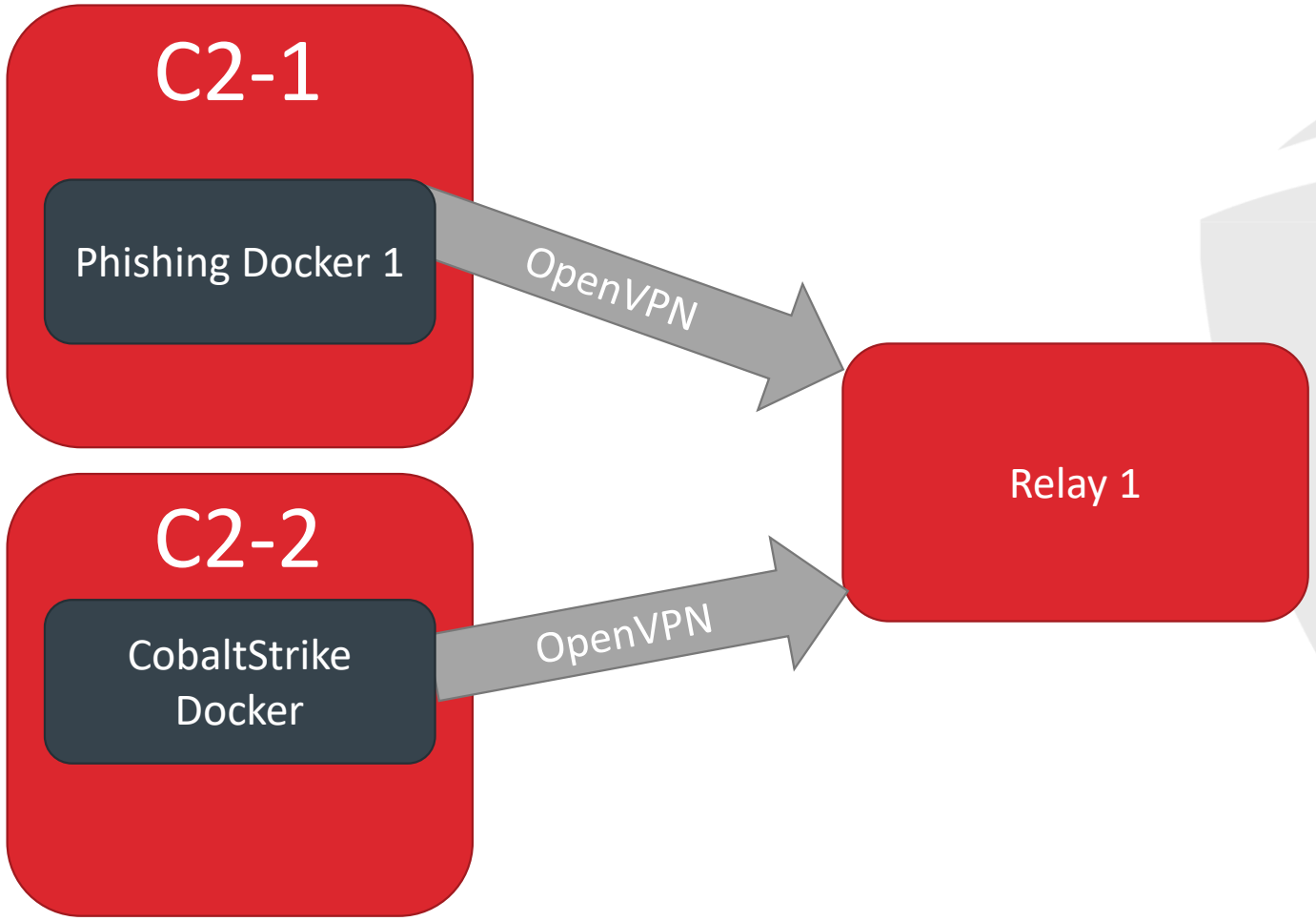

C2
Infra Component
(Docker)
OpenVPN
Relay


C2
Infra Component
(Docker)
OpenVPN
Relay
Target

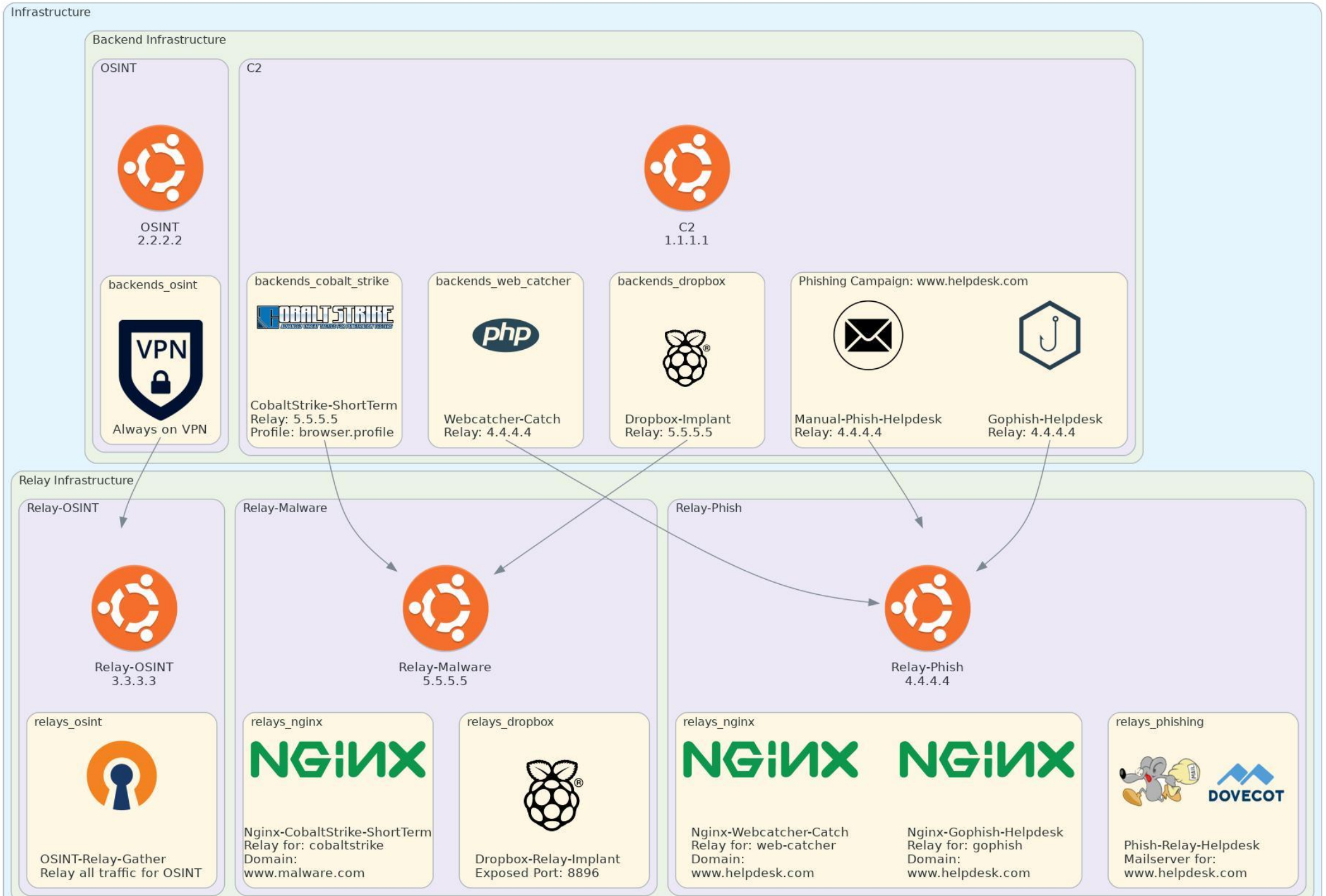

C2
Infra Component
(Docker)
OpenVPN
Relay
Target
The rest
of the
internet


C2
Phishing Docker 1
Phishing Docker 2
CobaltStrike Docker
OpenVPN
OpenVPN
OpenVPN
Relay 1
Relay 2
Relay 3


C2
Phishing Docker 1
Hardware Implant Docker
CobaltStrike Docker
OpenVPN
OpenVPN
OpenVPN
Relay 1


C2-1
Phishing Docker 1
OpenVPN
C2-2
CobaltStrike
Docker
OpenVPN
Relay 1

Red Wizard
Demo Time


Infrastructure
Backend Infrastructure
OSINT
OSINT
2.2.2.2
backends_osint
VPN
Always on VPN
C2
C2
1.1.1.1
backends_cobalt_strike
CobaltStrike-ShortTerm
Relay: 5.5.5.5
Profile: browser.profile
backends_web_catcher
Webcatcher-Catch
Relay: 4.4.4.4
backends_dropbox
Dropbox-Implant
Relay: 5.5.5.5
Phishing Campaign: www.helpdesk.com
Manual-Phish-Helpdesk
Relay: 4.4.4.4
Gophish-Helpdesk
Relay: 4.4.4.4
Relay Infrastructure
Relay-OSINT
Relay-OSINT
3.3.3.3
relays_osint
OSINT-Relay-Gather
Relay all traffic for OSINT
Relay-Malware
Relay-Malware
5.5.5.5
relays_nginx
Nginx-CobaltStrike-ShortTerm
Relay for: cobaltstrike
Domain:
www.malware.com
relays_dropbox
Dropbox-Relay-Implant
Exposed Port: 8896
Relay-Phish
Relay-Phish
4.4.4.4
relays_nginx
Nginx-Webcatcher-Catch
Relay for: web-catcher
Domain:
www.helpdesk.com
Nginx-Gophish-Helpdesk
Relay for: gophish
Domain:
www.helpdesk.com
relays_phishing
Phish-Relay-Helpdesk
Mailserver for:
www.helpdesk.com

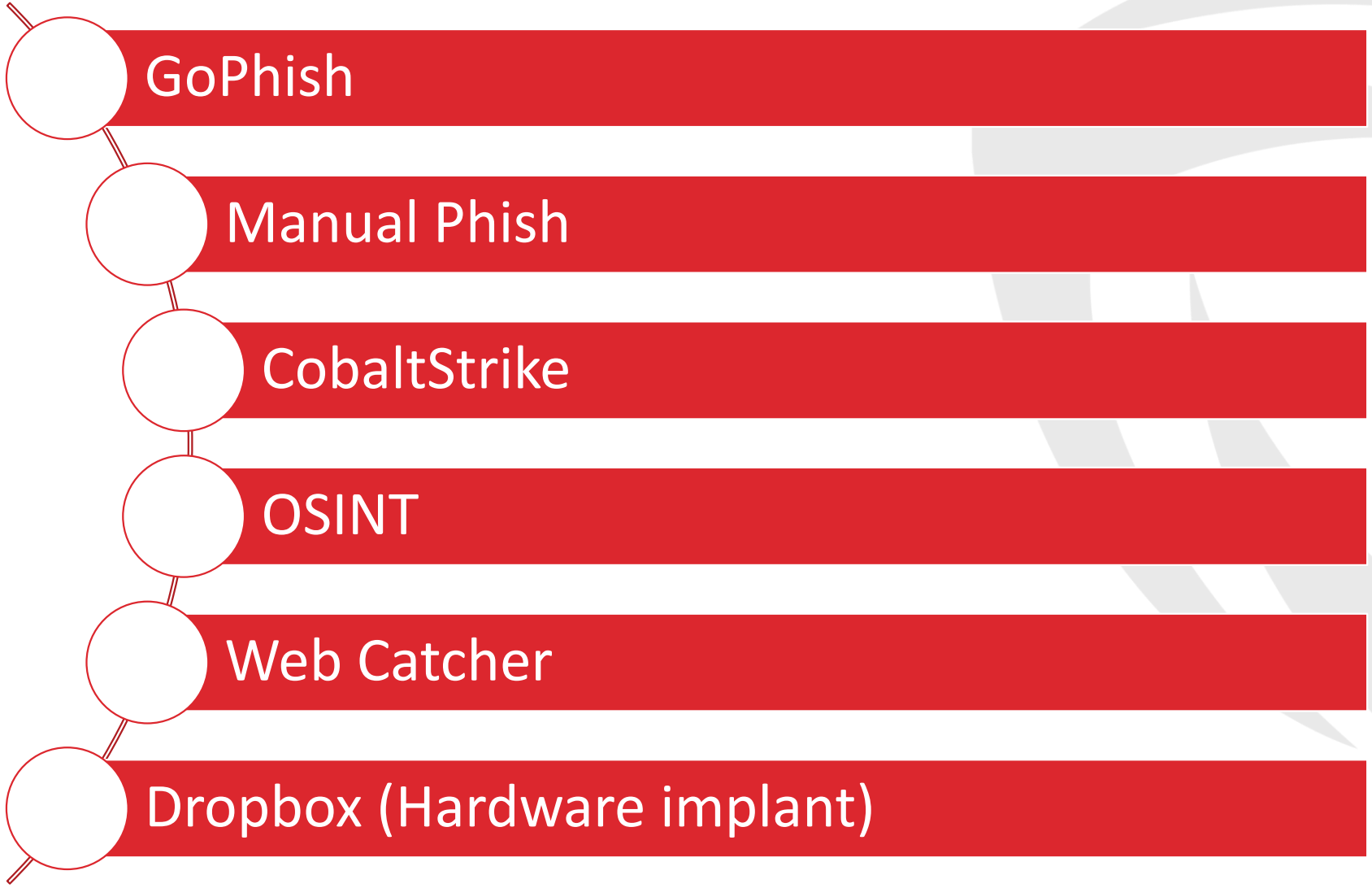
Red Wizard
Closing thoughts

Where to get it?

https://github.com/SecuraBV/RedWizard

Will there be bugs?

Publicly released components



Secura

What did we not release? What do you have to do yourself?

- Secura's Red Teaming secret sauce
  - OPSEC patches to GoPhish / Cobaltstrike etc
  - Malleable Profiles
- Other components for proprietary software
- Not all hardenings for our environments
- Relay website-generators
- Server deployment

Secura

Future public releases?

- RedElk integration (Red Team SIEM by Outflank)
- MitM Phishing (EvilGinx / Modlishka)
- Support for non-standard relays (domain fronting etc)
- Hardware implants?

Secura

Thank you!

https://github.com/SecuraBV/RedWizard

Ben Brücker
ben.brucker@secura.com

Secura