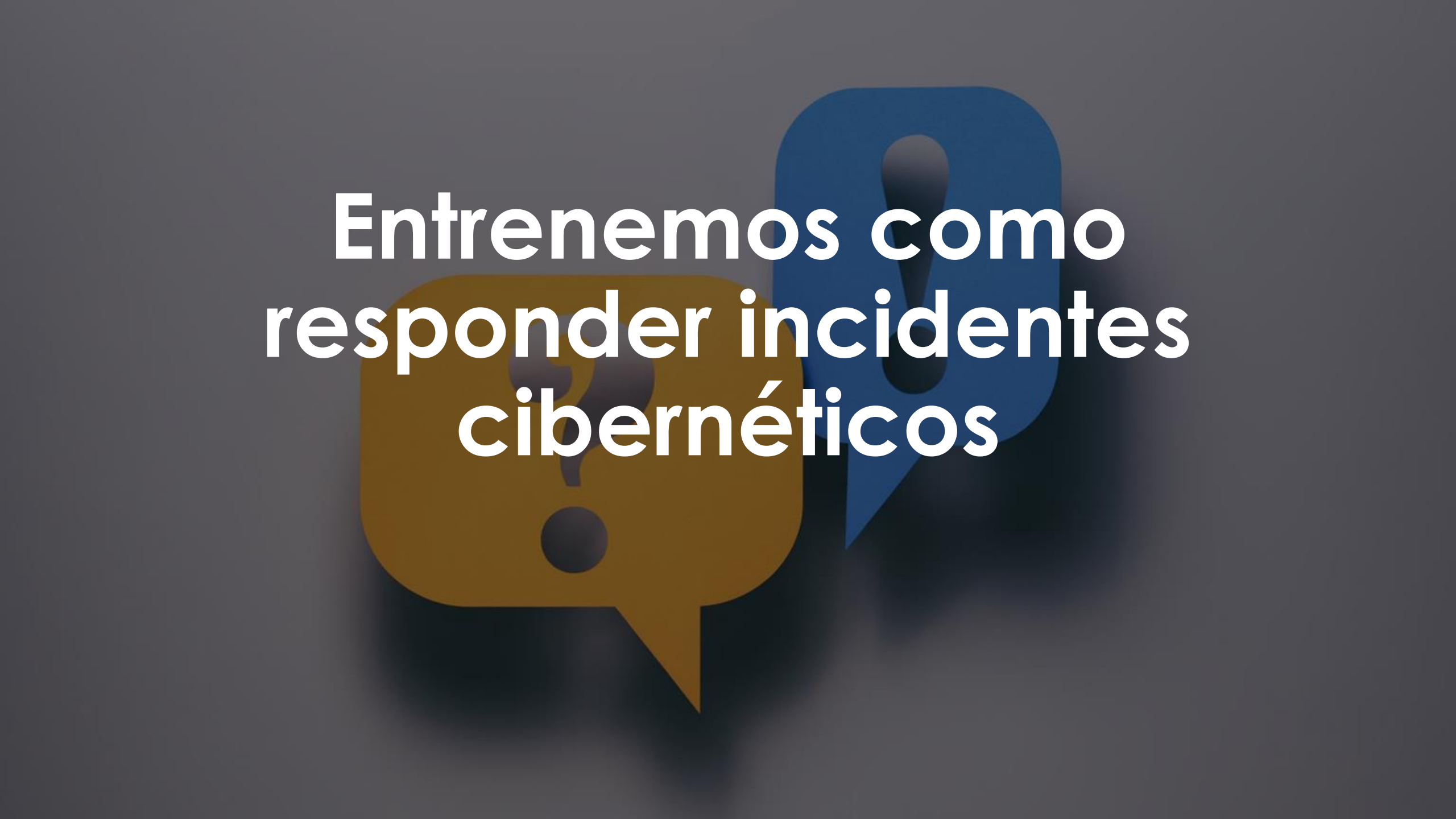

Entrenemos como
responder incidentes
cibernéticos

Diego Samuel Espitia

Ingeniero electrónico por profesión,
hacker por pasión

@dsespitia

Contexto

Ransomware By Geographic Region

2022

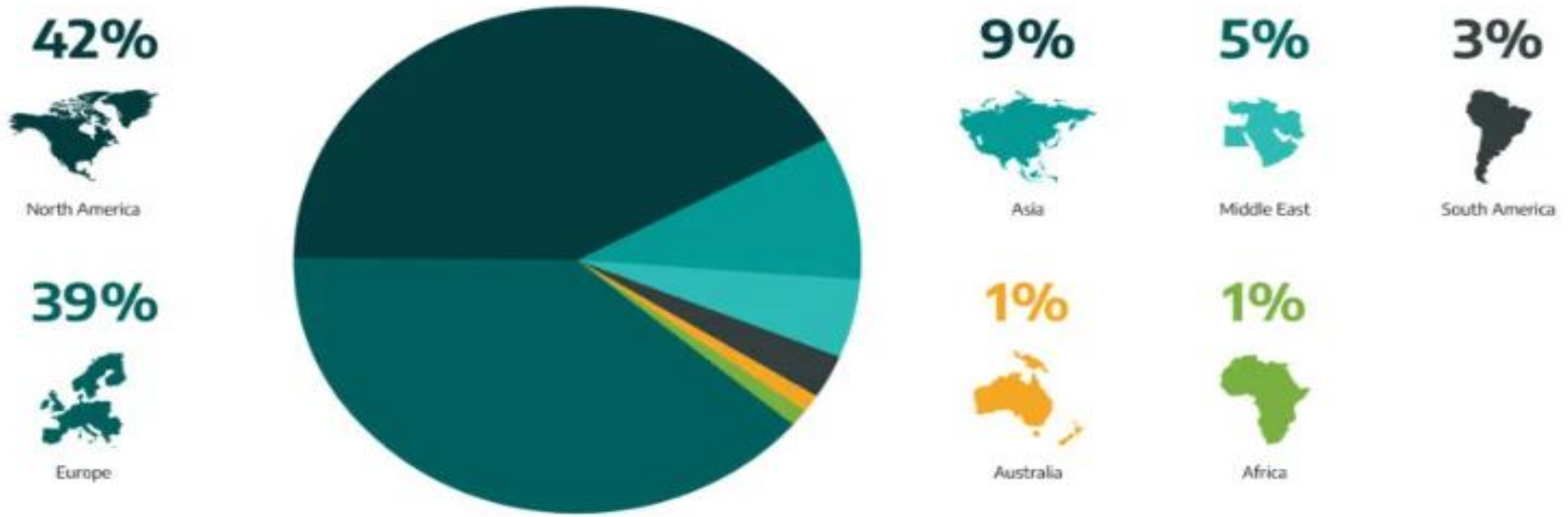
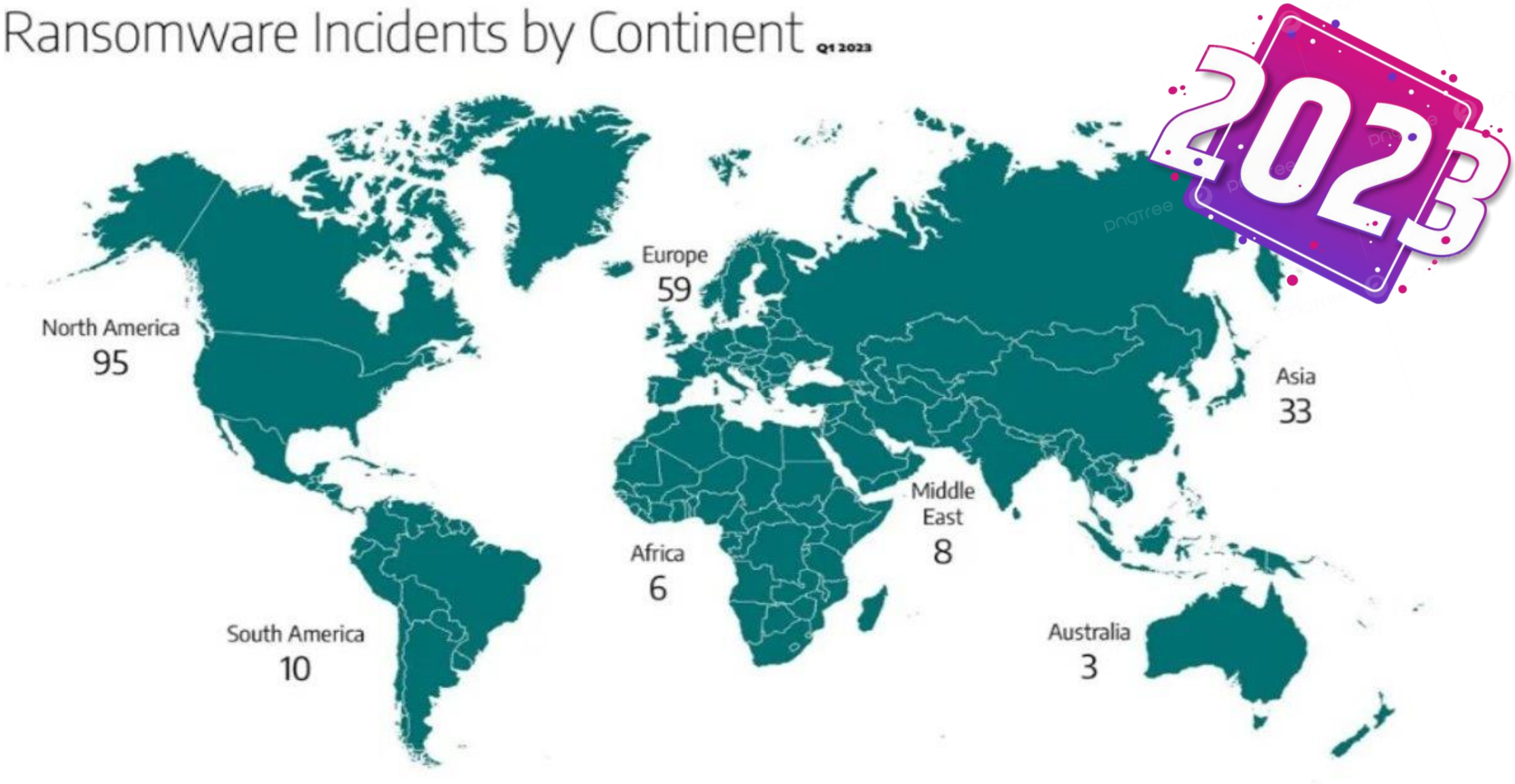


Figure 1: Ransomware Targets By Continent

https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q1-2022/



https://www.dragos.com/blog/ransomware-attack-analysis-q1-2023/

Figure 1: Ransomware Incidents by Continent

Can you quickly tell which of the URLs below is legitimate and which one is a malicious phish that drops evil.exe?

https://github.com/kubernetes/kubernetes/archive/refs/tags/@v1271.zip

https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip

BLEEPINGCOMPUTER

NEWS ▾ DOWNLOADS ▾ VPNS ▾ VIRUS REMOVA

Canadian mining firm shuts down

By Bill Toulas

The Canadian Copper Mountain Mining Corporation (CMMC) in British Columbia has ann

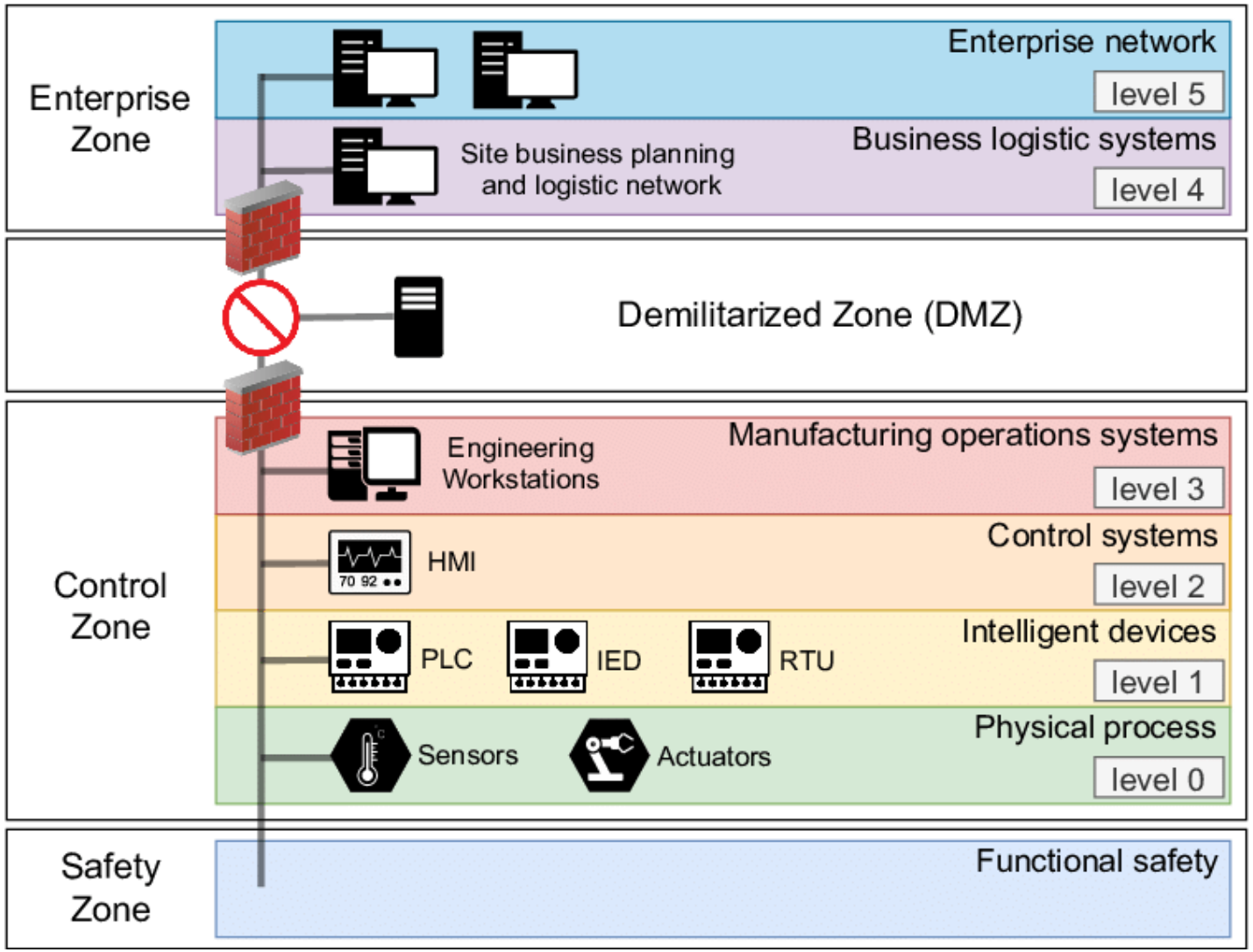
The image can represent a variety of threats in the digital world: data theft, data leak, security breach, intrusion, etc... Cyber-crime is growing exponentially. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025. 5 mar 2023

forbes.com
https://www.forbes.com › chuckbrooks › 2023/03/05 › c...

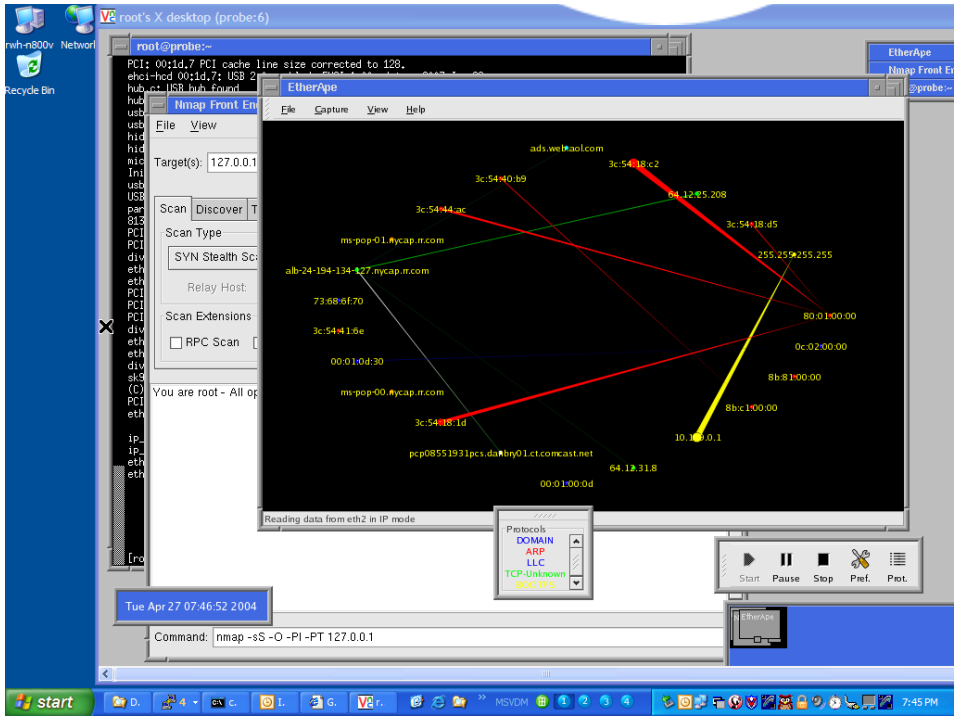
Cybersecurity Trends & Statistics For 2023; What You ... - Forbes

Medidas Empresariales

Sector OT

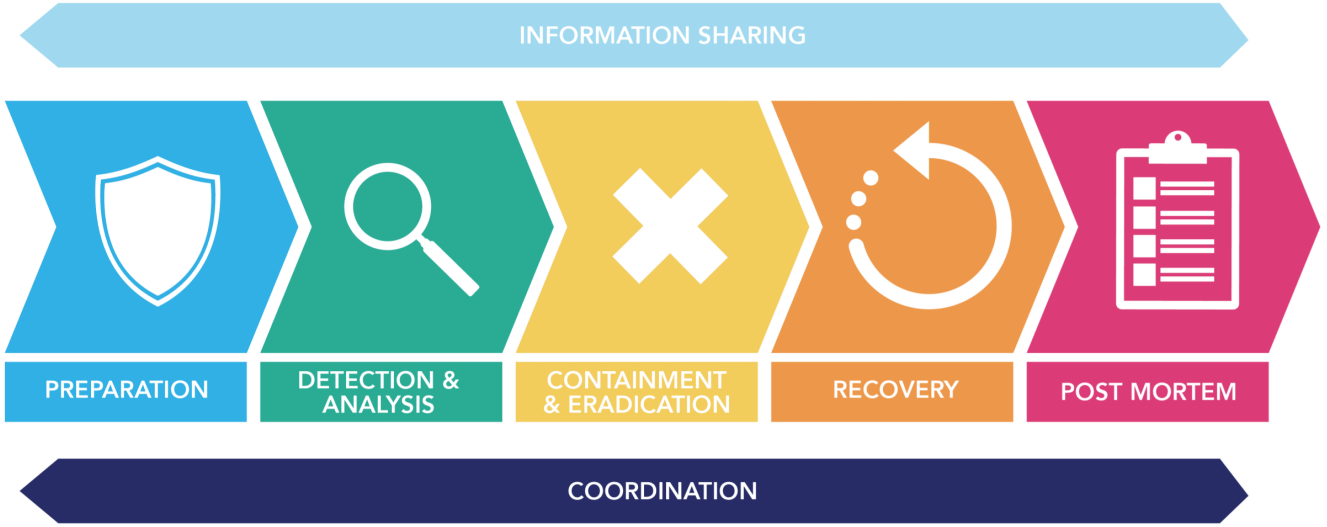

Enterprise Zone
Enterprise network
level 5
Site business planning and logistic network
Business logistic systems
level 4
Demilitarized Zone (DMZ)
Control Zone
Engineering Workstations
Manufacturing operations systems
level 3
HMI
Control systems
level 2
PLC
IED
RTU
Intelligent devices
level 1
Sensors
Actuators
Physical process
level 0
Safety Zone
Functional safety


ANTIVIRUS


root's X desktop (probe:6)
root@probe:~
EtherApe
Nmap Front End
Target(s): 127.0.0.1
Scan Type
SYN Stealth Sc
Relay Host:
Scan Extensions
RPC Scan
You are root - All op
Command: nmap -sS -O -PI -PT 127.0.0.1
Tue Apr 27 07:46:52 2004
Protocols
DOMAIN
ARP
LLC
TCP-Unknown
Start
Pause
Stop
Pref.
Prot.
start
7:45 PM

Sector IT

CISO



RED TEAM

OFFENSIVE ATTACK TEAM

Tasks include:

- Ethical hacking
- Penentration testing
- Black box testing
- Social engineering
- Web app scanning
- Vulernability exploitation

PURPLE TEAM

DATA COLLECTION & IMPLEMENTATION TEAM

Tasks include:

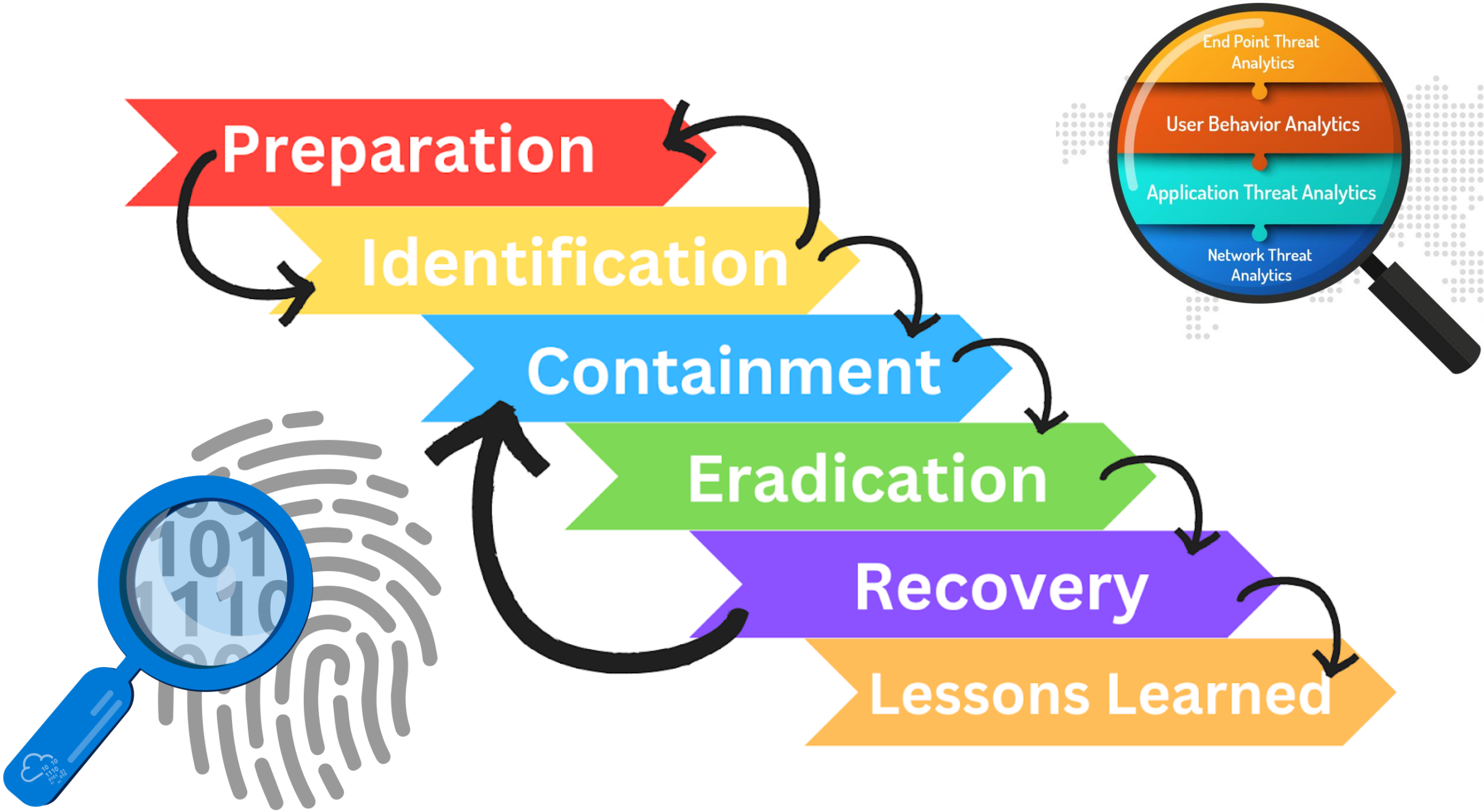
- Improvement facilitation
- Data analytics
- Gap analysis
- Red vs Blue skill testing
- System improvements
- Collaborative security

BLUE TEAM

DEFENSIVE PROTECT TEAM

Tasks include:

- Infrastructure security
- Damage control
- Incident response (IR)
- Operational security
- Threat hunting
- Digital forensics


Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned
End Point Threat Analytics
User Behavior Analytics
Application Threat Analytics
Network Threat Analytics

CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

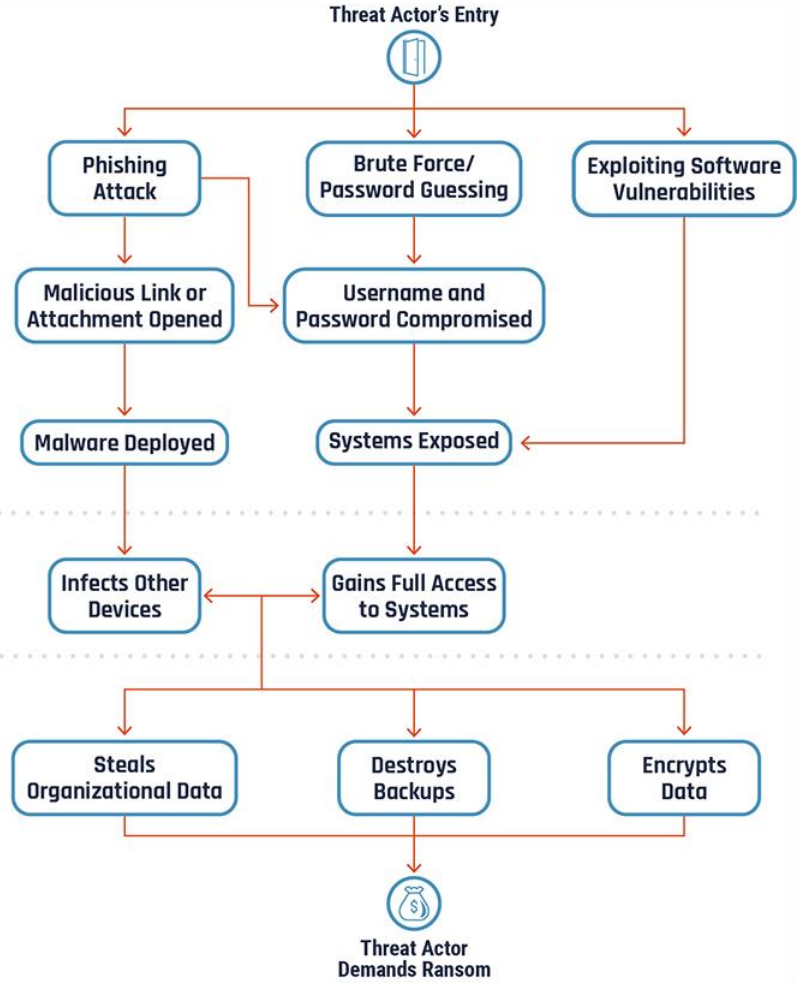
Ransomware Playbook

How to prepare for, respond to, and recover from a ransomware attack

GAINS ACCESS
Threat actor finds a way into your network.

TAKES CONTROL
Threat actor gains access of connected systems and devices.

IMPACTS ORGANIZATION
Threat actor encrypts and copies your data, deletes connected backups, and demands a ransom.



Llego el momento de la verdad

Restore Only

Destination corrupted (Error report)

Last successful backup: 2022-03-12 01:04

Next scheduled backup time: 2022-03-21 01:00

Target - On-line

Server address: gateway.eu1.storj...

Task Settings

Shared Folder:

Preparemonos

Table Top

Simulaciones

Emulaciones

Table Top

- Historias reales adaptadas a la infraestructura e IRP que se requiere probar.
- Probar toma de decisiones y conocimiento de los planes.
- Detectar posibles falencias o debilidades en personas, procesos o tecnología.

National Cyber Security Centre

Cyber Exercising

Creating your own exercises

The following tips can help organisations create their own cyber incident response exercises. They are intended for IT staff, cyber risk management teams, and business continuity teams in small-to-medium sized organisations. For more information refer to **www.ncsc.gov.uk/exercising**

Why run cyber incident exercises?

Cyber incident exercising helps organisations to establish how resilient they are to cyber attack, and to practice their response in a safe environment.

Exercising also helps create a culture of learning within an organisation, and provides an opportunity for relevant teams and individuals to maximise their effectiveness during an incident.

Creating **bespoke** exercises allows you to tailor these to reflect **your organisation's values**, and the unique **challenges**, **constraints**, and **threats** you face.

1. Define what you want to exercise

Having clear objectives set from the start will ensure your approach remains focused.

2. Secure senior level endorsement

Strong buy-in from seniors will encourage participation and ensure any recommendations can be more easily put in place.

3. Select the most effective approach

There are broadly two types: **tabletop** (i.e. discussion-based) or **live play** exercises.

4. Create a team & agree participants

A dedicated exercise team can ensure the exercise is realistic, and that lessons are learned.

5. Create & agree metrics

Metrics should be defined that allow you to identify both areas that worked well, and ones that need improving.

6. Create & develop exercise scenarios

Provide a background story with real-world events to make the exercise more realistic.

7. Create & develop the exercise injects

Create the information that participants will receive (and respond to) during the exercise.

8. Develop guidance for participants

Distribute guidance to participants a few days ahead of the exercise so they come adequately prepared for it.

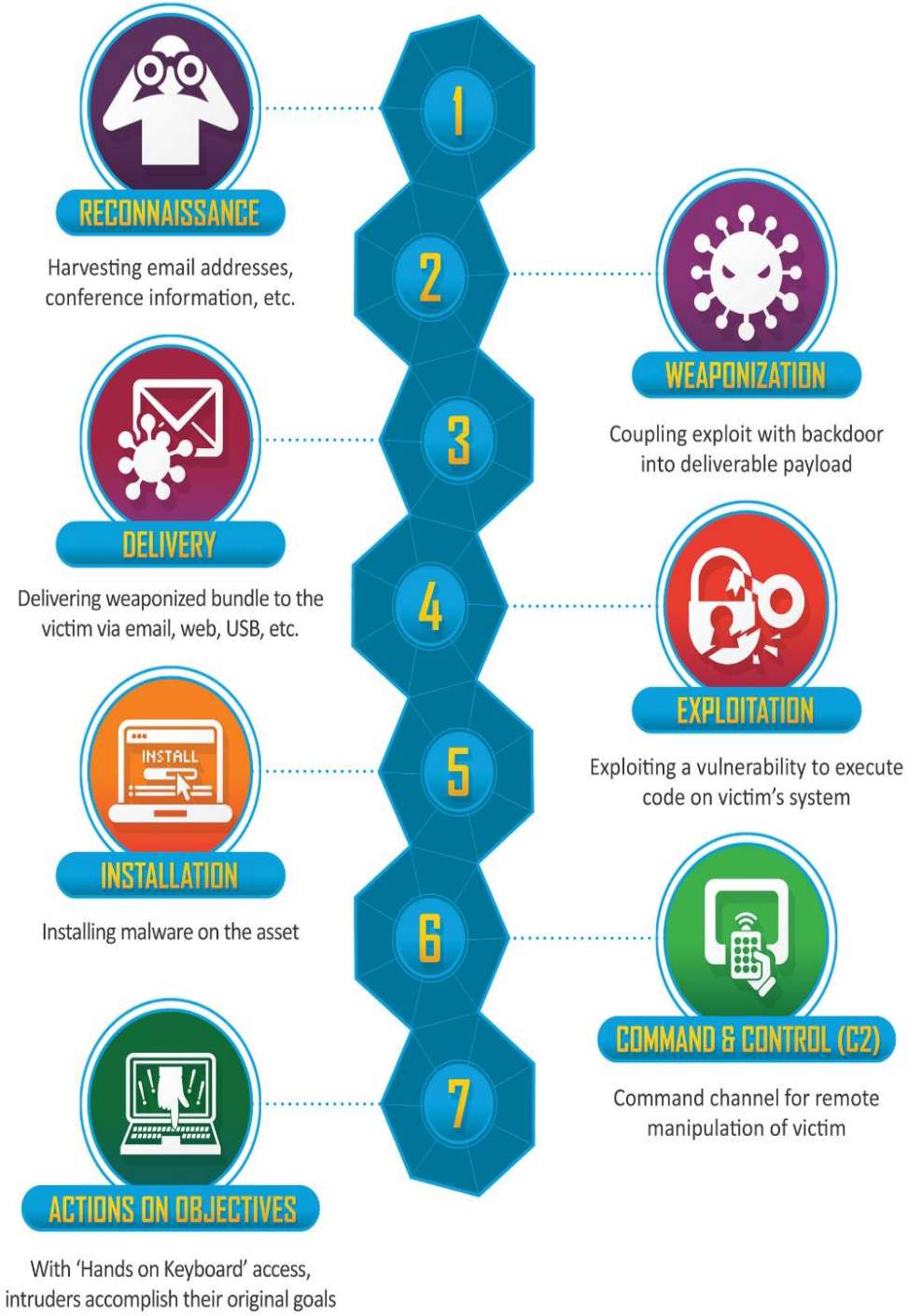
Run the exercise

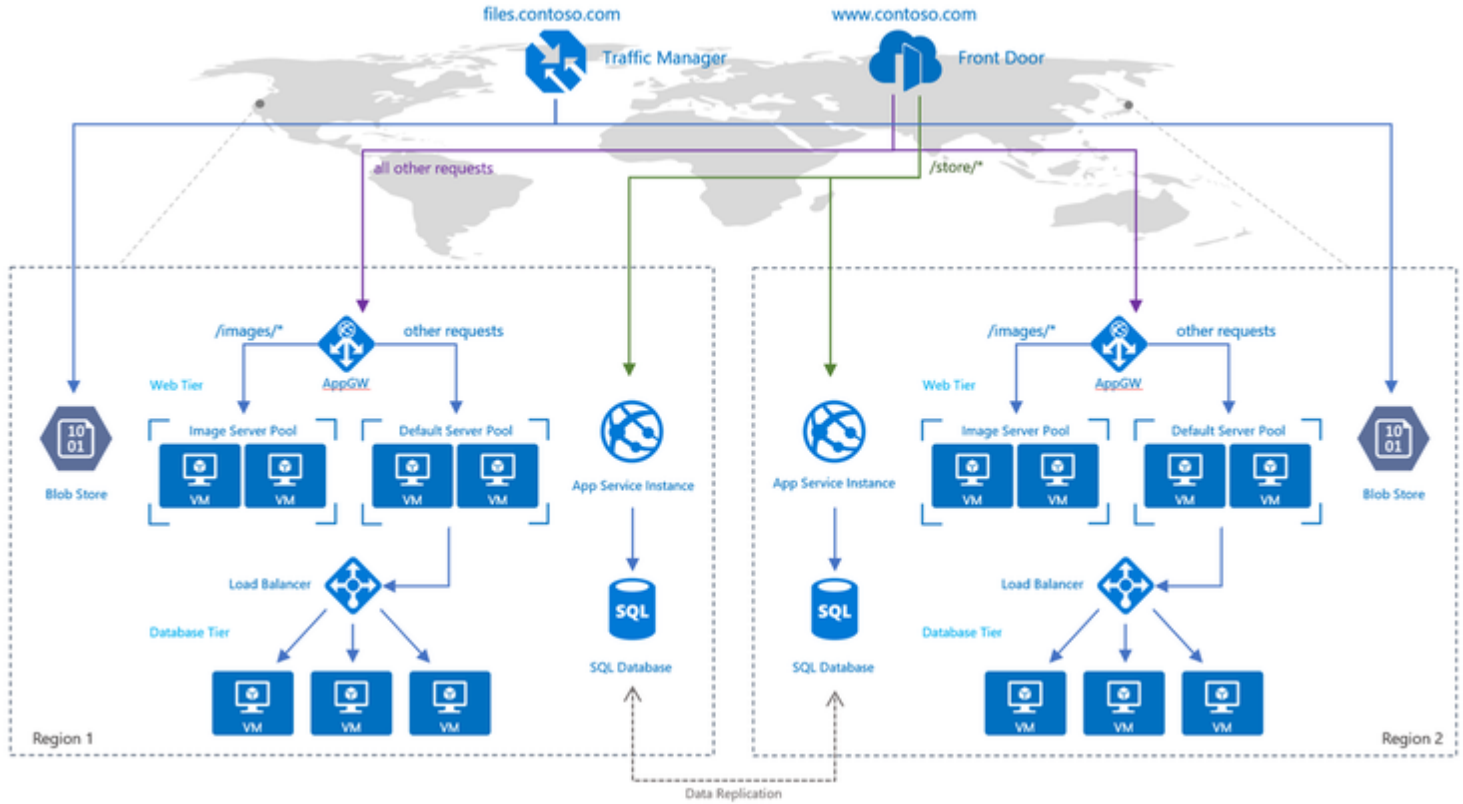
9. Capture feedback & identify lessons

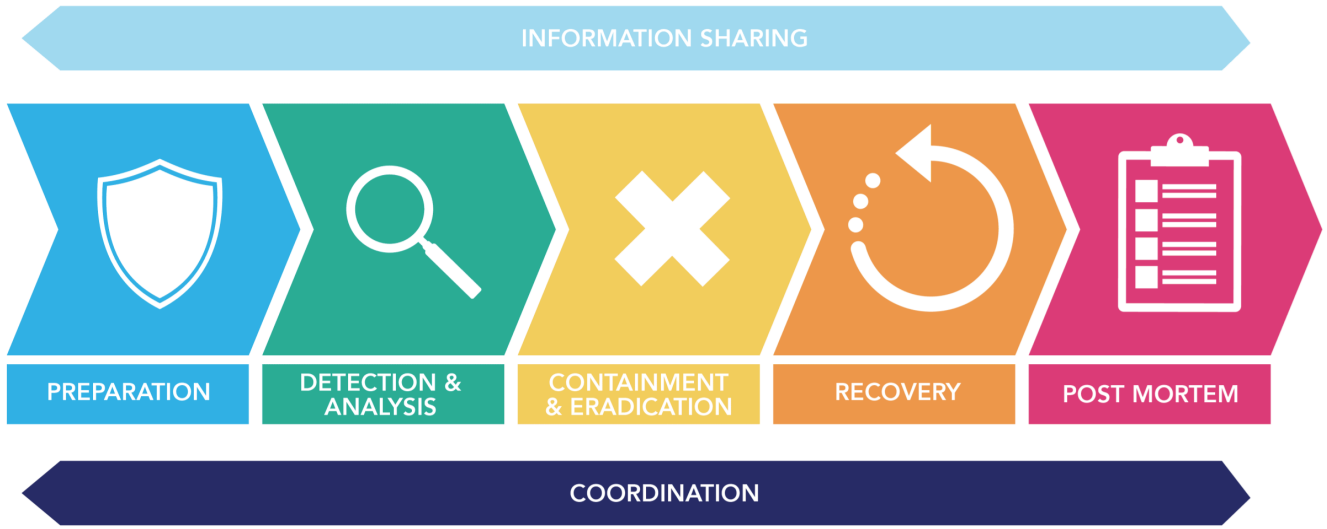
Make sure that any recommendations are allocated to business owners to ensure action is taken.

Simulación

- Arquitecturas virtualizadas, que permiten entrenar.
- Validación técnica de la respuesta de incidentes.
- Calificación de equipos tecnicos.

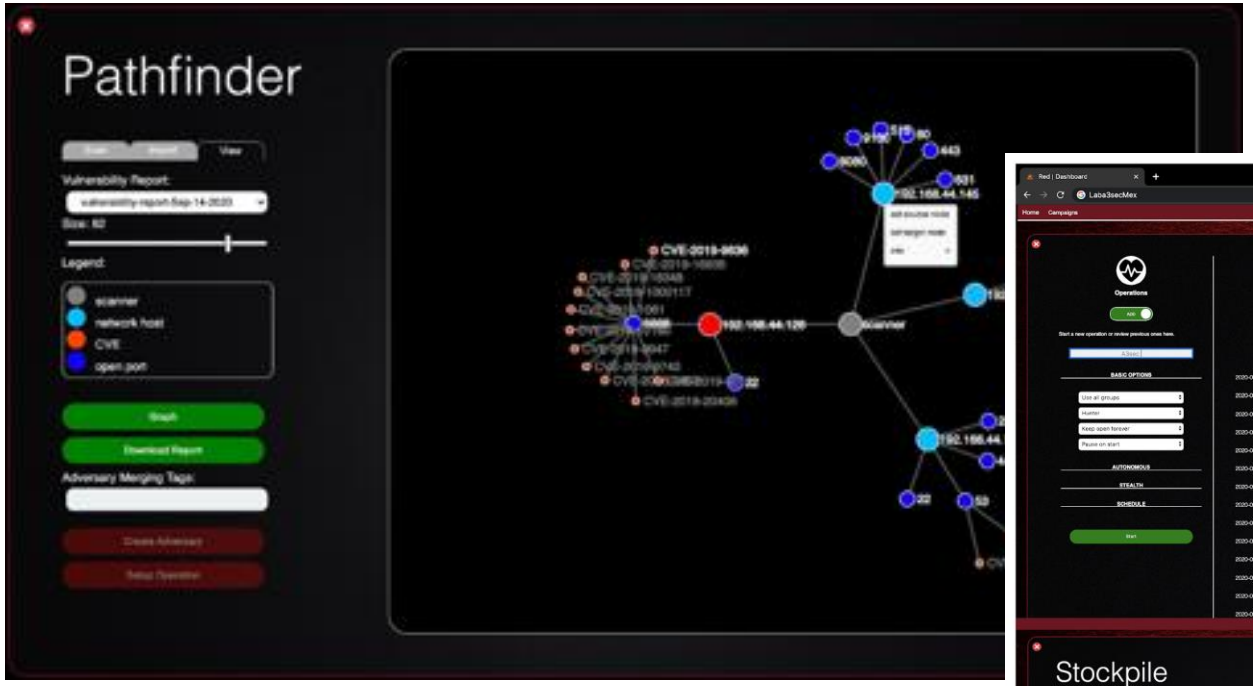

1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

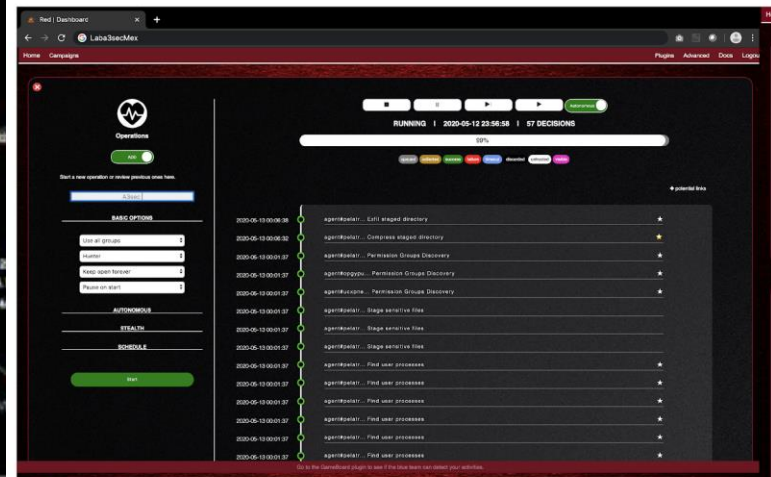

files.contoso.com
Traffic Manager
www.contoso.com
Front Door
all other requests
/store/*
/images/*
other requests
AppGW
Web Tier
Image Server Pool
Default Server Pool
VM
Blob Store
App Service Instance
Load Balancer
Database Tier
SQL
SQL Database
Region 1
Region 2
Data Replication


INFORMATION SHARING
PREPARATION
DETECTION & ANALYSIS
CONTAINMENT & ERADICATION
RECOVERY
POST MORTEM
COORDINATION

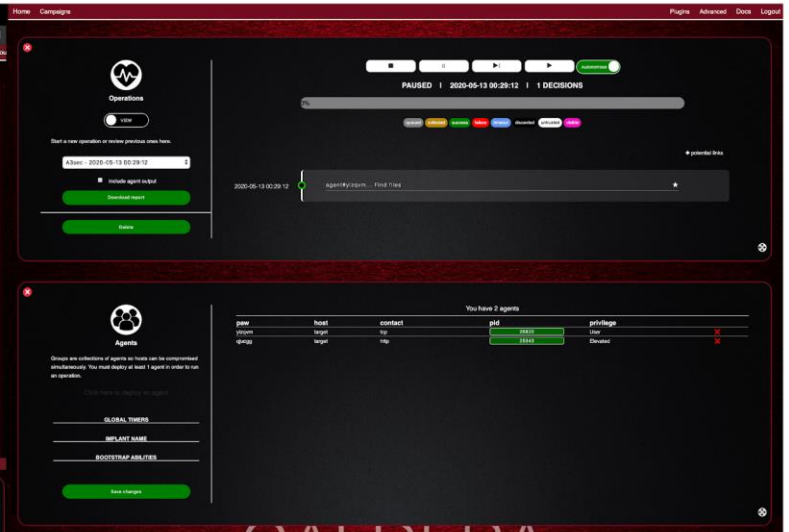
Emulación

- Se ejecuta TTP en infraestructura real.
- Se valida respuesta de arquitectura de seguridad.
- Entrenamiento "real".
- Se requiere un conciencia muy alta de ciberseguridad.

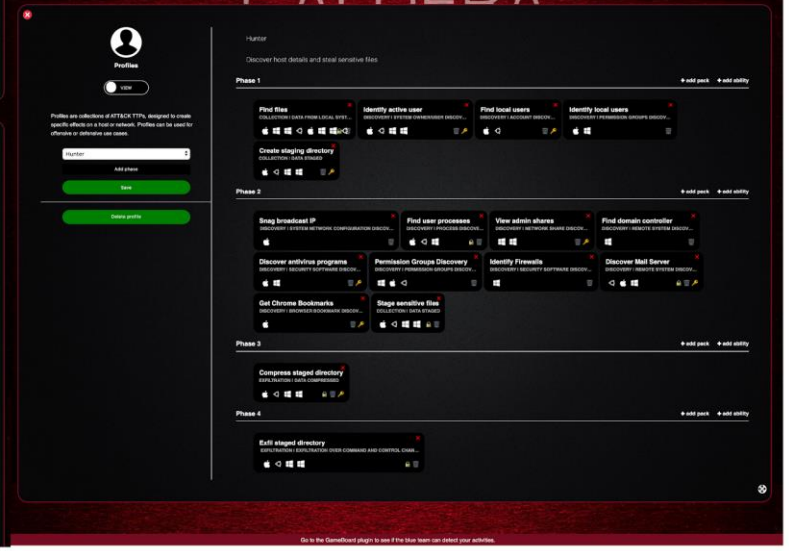

Pathfinder
Vulnerability Report:
Legend:
scanner
network host
CVE
open port
Adversary Merging Tags:


Operations
RUNNING | 2020-05-12 23:56:58 | 57 DECISIONS


Stockpile
a database of abilities
ABILITIES
219
ADVERSARIES
16


Operations
PAUSED | 2020-05-13 00:29:12 | 1 DECISIONS

Agents
You have 2 agents


Profiles
Hunter
Discover host details and steal sensitive files


Adversary Profiles
VIEW
Adversary Profiles are collections of ATT&CK TTPs, designed to create specific effects on a host or network. Profiles can be used for offensive or defensive use cases.
Adversary Profile
Discovery
Save
Delete
Discovery
Adversary Profile Name
A discovery adversary
Adversary Profile Description
Ordering
Adversary Profile Abilities
+ link objective | + add adv
Identify active user
DISCOVERY | SYSTEM OWNER/USER DIS...
Find local users
DISCOVERY | ACCOUNT DISCOVERY: LO...
Identify local users
DISCOVERY | ACCOUNT DISCOVERY: LO...
Snag broadcast IP
DISCOVERY | SYSTEM NETWORK CONFI...
Find user processes
DISCOVERY | PROCESS DISCOVERY
View admin shares
DISCOVERY | NETWORK SHARE DISCOV...
Discover domain controller
DISCOVERY | REMOTE SYSTEM DISCOV...
Discover antivirus progra...
DISCOVERY | SOFTWARE DISCOVERY: S...
Permission Groups Disco...
DISCOVERY | PERMISSION GROUPS DIS...
Identify Firewalls
DISCOVERY | SOFTWARE DISCOVERY: S...
Discover Mail Server
DISCOVERY | REMOTE SYSTEM DISCOV...
Get Chrome Bookmarks
DISCOVERY | BROWSER BOOKMARK DI...


Gracias
Ngiyabonga
Hvala
Merci
Moltes
Dankon
Maraba
Xié
Barka
olun
rhât
Paldies
Maketai
Tānan
Mantiox
Murakoze
Tack
qūi
pai
Grazzie
Ntyox
Grazias
Bedankt
Thanks
leibh
ederim
dimo
Kommol
Shokrán
Dannaba
Mwebare
Kaigai
teru
Kulo
Dekoju
Ka
Khawp
Arigato
Shukuriyyaa
Emitekati
Tesekkür
Matóndo
Tsin'aen
Fa'afetai
gràcies
agaibh
Sag
jai
Dakujem
Trugarez
Ashoge
so
Merçi
Tinotenda
Spaisíva
ek
Multumesc
Aalghïstapcham
Syaabaas
magah
GyalailaaThai
Takk
Tak
Marahaba
chawe
Yuspagara
Néá'eshe
dziekuje
Blagodaram
òn
Faleminderit
Dyakooyu
Matu
Cám
Blagodarya
Dyuspagrasunki
Kili
Ngeyabonga
Xie
Evgaristó
maluhlap
Mahalo
Gunasakulila
Shterakravetsun
Dziakuju
TashakkurBulgaro
Tapaidh
Webale
Rakhmat
Go
Khrap
Alla
Imela
Gmadlob
Obrigado
Doh
maith
suksama
Eskerrik
Fafetai
Dêkuji
Ha'evete
Uzbezco
Rahmet
Danke
asko
mamexes
Kiitos
Gratias
Netjer
Dios
raibh
blu
Puno
todá
Ah
hvala
Ashi