SECURITY FORUM

5 avril 2022
CITE INTERNATIONALE UNIVERSITAIRE
17 boulevard Jourdan 75014 PARIS

CYBER RESILIENCE 360°

par

Gérard PAZUELO
Directeur Cybersécurité, ISE SYSTEMS
gerard.pazuelo@ise-systems.fr

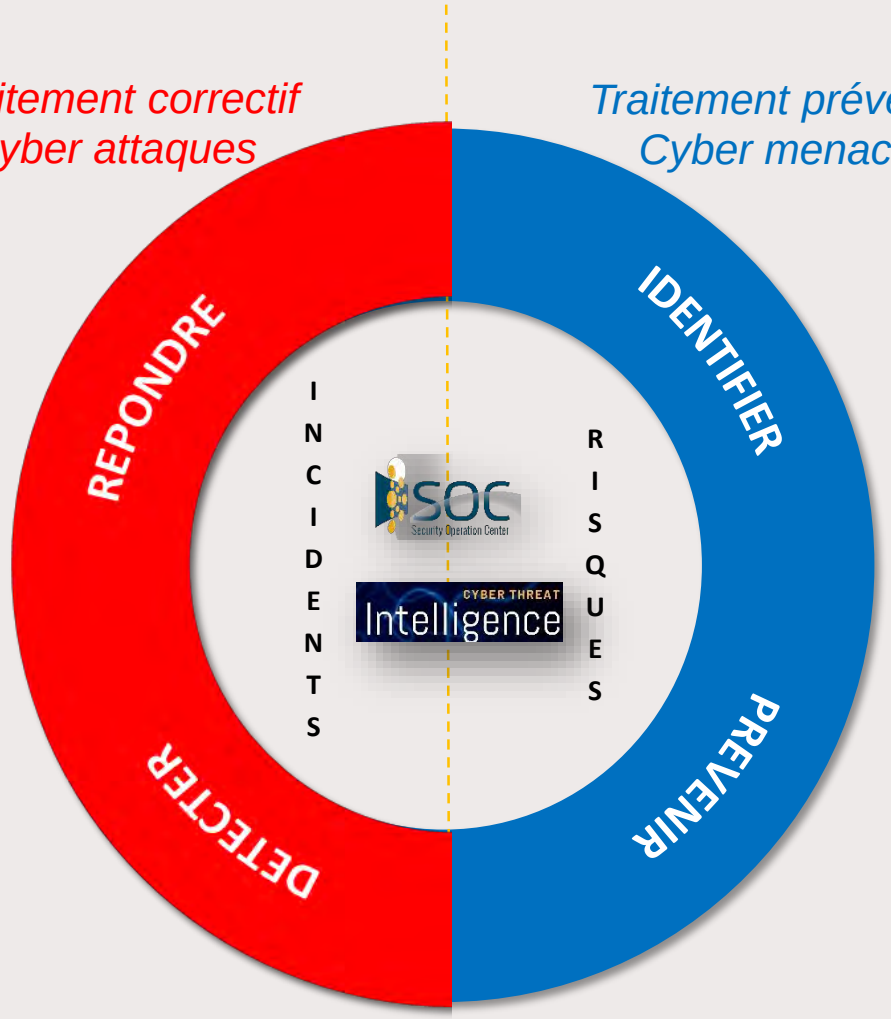
ISE SYSTEMS

Cyber Résilience

La capacité d'une entreprise à **identifier**, **prévenir**, **détecter** et **répondre** aux défaillances technologiques ou de process et à se rétablir en réduisant au **minimum les impacts négatifs** pour ses clients, les préjudices en matière de réputation et les pertes financières*.

Source Accenture

Intégration continue de la gestion des risques dans le management et la mise de œuvre de la cybersécurité



Risque = Vulnérabilité x Menace

Analyse de risque

PCA/PRA

Cybersécurité Opérationnelle

Cyber Threat Intelligence

CYBER RESILIENCE 360°

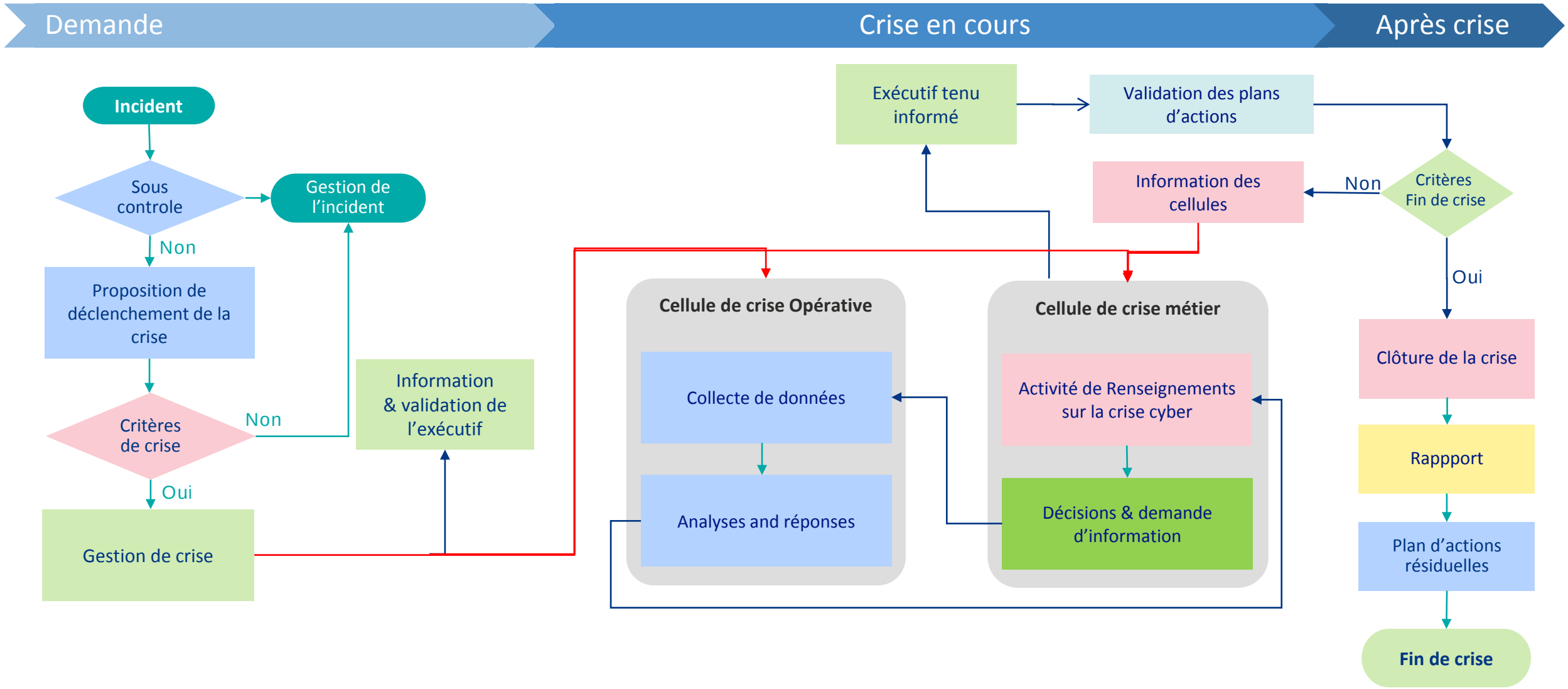
Exercice de crise cyber

Entrainement Cyber

Sensibilisation Cyber

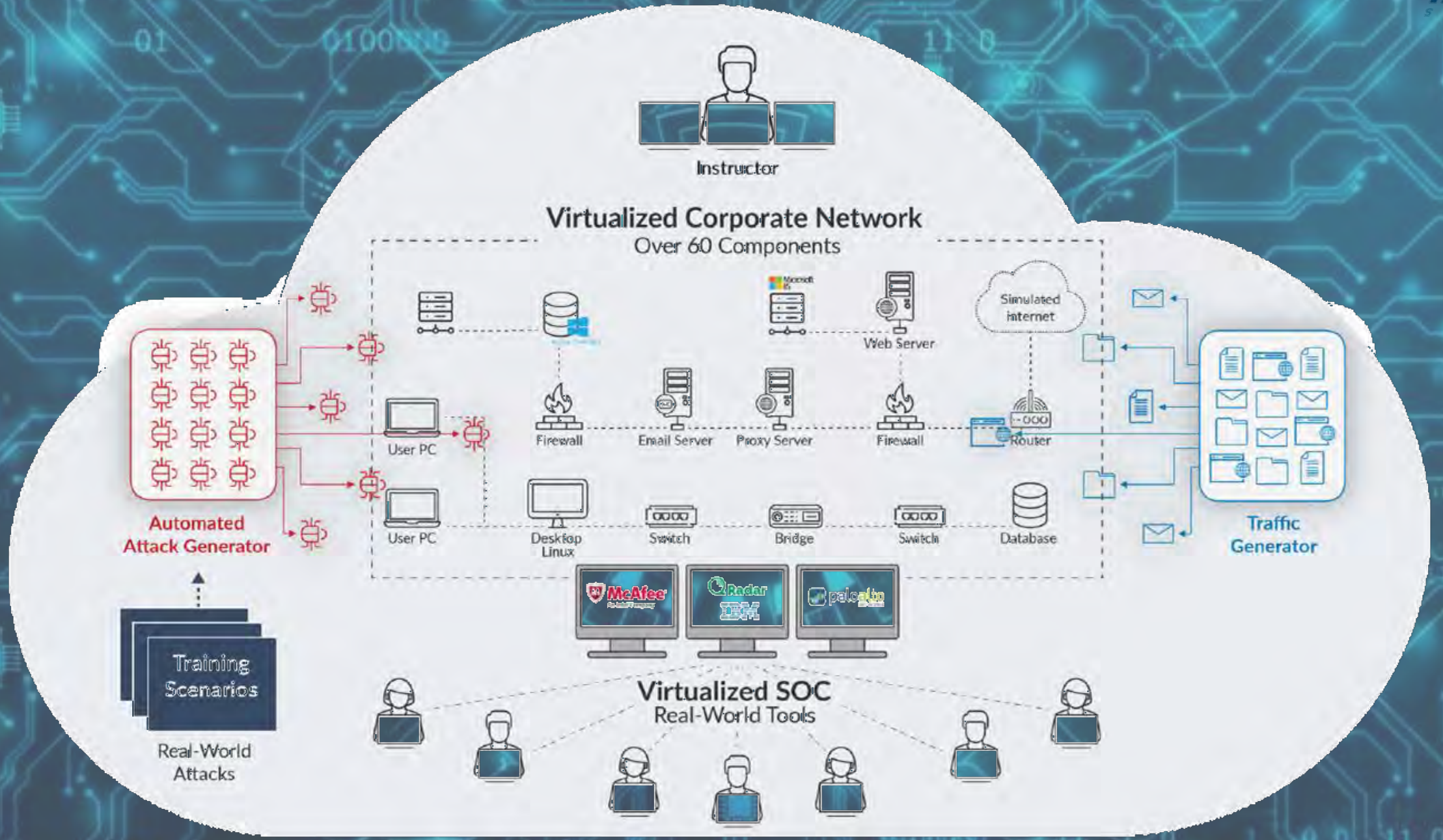
Plan de gestion de crise cyber

Exemple de processus synthétique



Transformer le comportement des collaborateurs, en assurant une préparation continue contre les menaces de phishing et une sensibilisation à la cyber sécurité


ACTIVE MISSION
Malicious Server
Follow the Tracks
You track the commands to the car as coming from the following IP: http://1371171511161/getaway/?id=0. If you can find a way to login maybe you will be able to figure out what's really going on. There's a table residing on the server. What is its name?
Hint 1: Sometimes you just gotta go in blind...
All Hints Taken (-50)
TYPE THE ANSWER
SUBMIT
TARGETS / MISSIONS
Acropolis Casino 0 / 1200
The Smoking Barrel 400
A Trail of Smoke 500
Locked 300
Locked 0 / 650
Locked 200
Locked 200
Locked 250
Locked 0 / 800
Locked 200
Locked 600
BRIEF
2nd
Of 2
0pts
A-TEAM
+4
47 : 58 : 57
COMM
No Notifications Yet
Campaign Master
Hi, I'm the Campaign Master. Text me here if you have any private questions. Good luck!
16:02
TYPE A MESSAGE
SEND


Instructor
Virtualized Corporate Network
Over 60 Components
Simulated Internet
Web Server
Firewall
Email Server
Proxy Server
Firewall
Router
User PC
User PC
Desktop Linux
Switch
Bridge
Switch
Database
Automated Attack Generator
Traffic Generator
Training Scenarios
Real-World Attacks
McAfee
Radar
paloalto
Virtualized SOC
Real-World Tools

CYBER RANGE

Training Categories

New Training

Tier 1 SOC Analysis

Tier 2 SOC Analysis

Advanced Incident Response

Malware Analysis

Network Forensics

Industrial Control Systems

Penetration Testing

Windows Forensics

Linux Forensics

CYBER RÉSILIENCE

CELLULE STRATEGIQUE (COMEX)

CELLULE BUSINESS

CELLULE OPERATIVE

CELLULE TECHNIQUE

SYSTÈME DE SECURITE DE L'INFORMATION

CELLULE STRATEGIQUE (COMEX)

CELLULE BUSINESS

CELLULE OPERATIVE

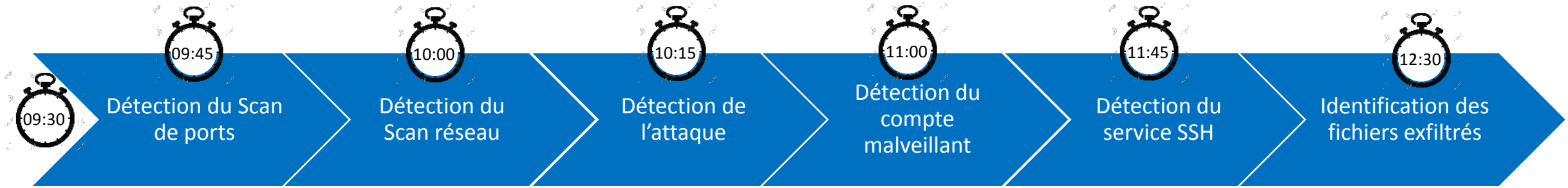
CELLULE TECHNIQUE

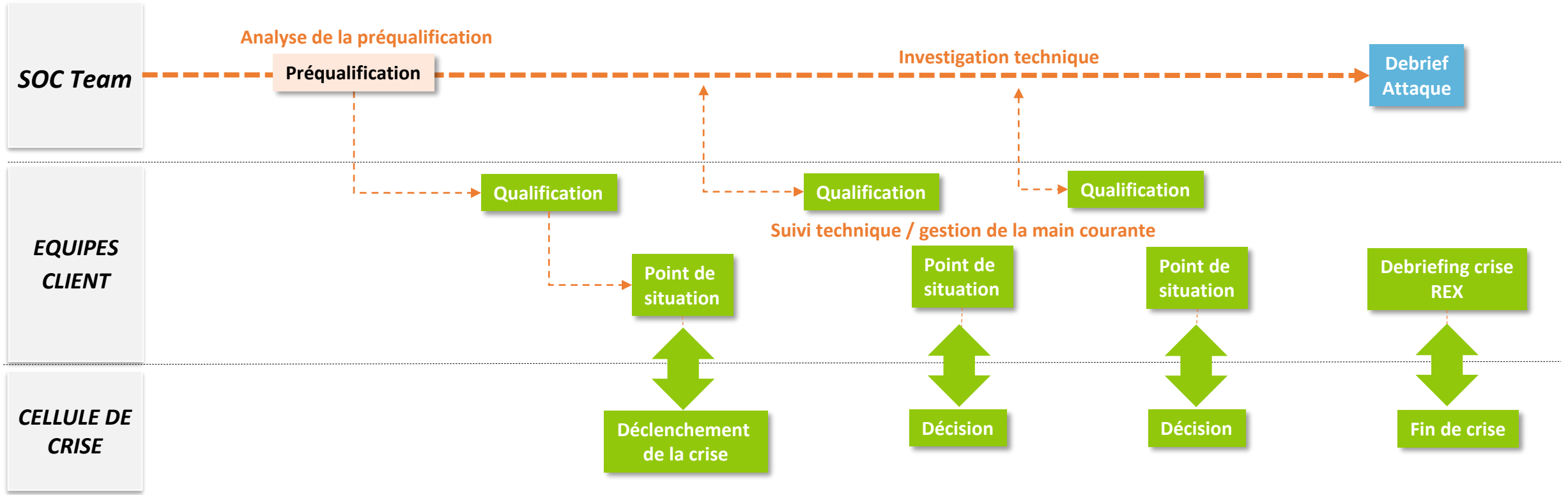
SYSTÈME DE SECURITE DE L'INFORMATION

CYBER RÉSILIENCE

Simulation de crise

Exercice de crise

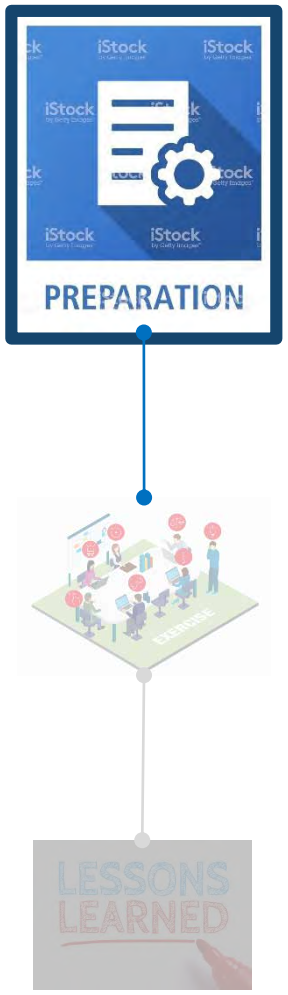

09:30
09:45
Détection du Scan de ports
10:00
Détection du Scan réseau
10:15
Détection de l'attaque
11:00
Détection du compte malveillant
11:45
Détection du service SSH
12:30
Identification des fichiers exfiltrés

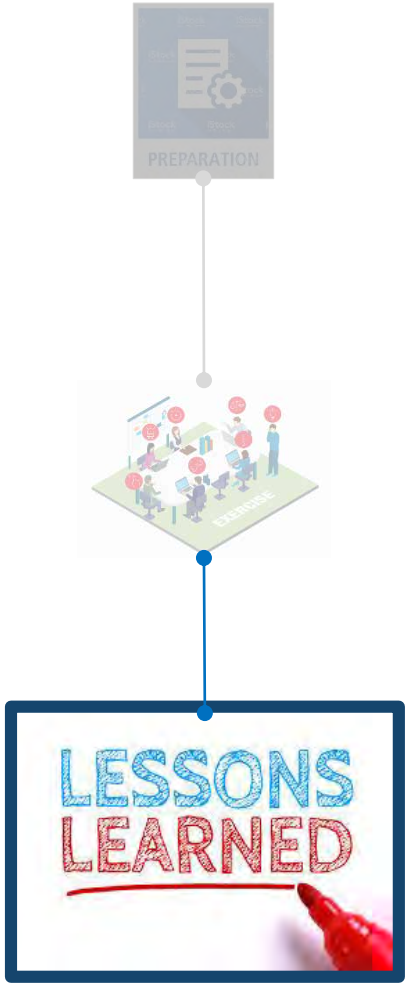

SOC Team
EQUIPES CLIENT
CELLULE DE CRISE
Analyse de la préqualification
Préqualification
Investigation technique
Debrief Attaque
Qualification
Qualification
Qualification
Suivi technique / gestion de la main courante
Point de situation
Point de situation
Point de situation
Debriefing crise REX
Déclenchement de la crise
Décision
Décision
Fin de crise

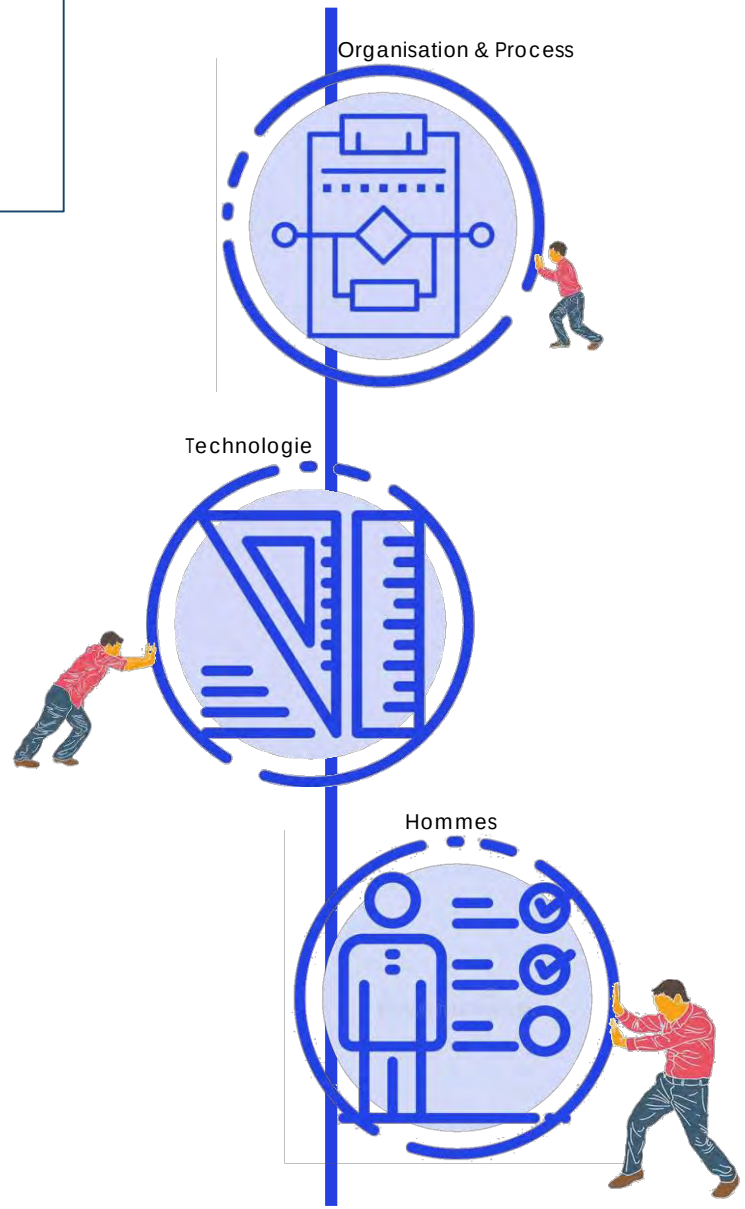
- ✓ Audit des Plans et Documents
- ✓ Périmètre
- ✓ Scénario
- ✓ Eléments de réalité
- ✓ Niveau d'effet de surprise
- ✓ Calendrier

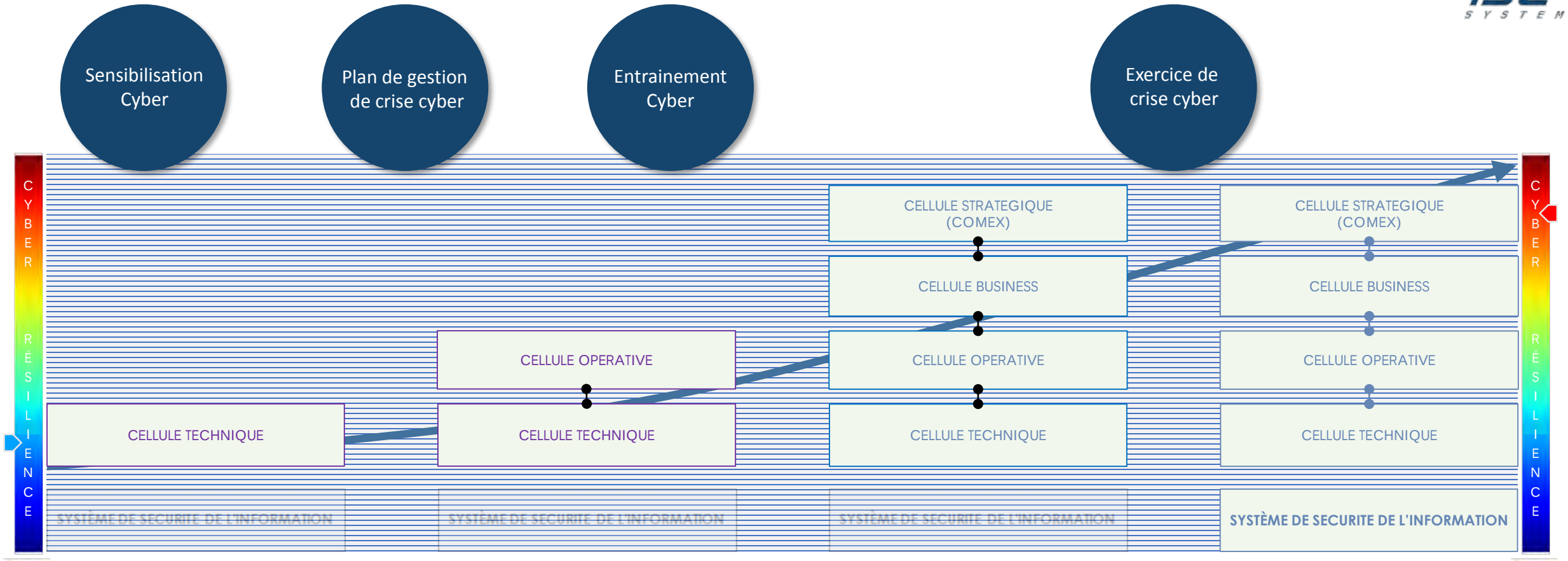
- ✓ Respect des plans / Réactivité
- ✓ Gestion des prises de décision
- ✓ Gestion de la communication
- ✓ Gestion du temps

- ✓ Retour à chaud
- ✓ Rapports
- ✓ Restitution
- ✓ Plan d'action
- ✓ Trajectoire









Entrainement individuel

Compétences techniques

Entrainement des équipes

Compétences techniques
Efficience collective

Simulation de crise

Compétences techniques
Efficience collective
Organisation & communication

Exercice de crise

Compétences techniques
Efficience collective
Organisation & communication
Système de sécurité de l'information

ISE SYSTEMS

Gérard PAZUELO
Directeur Cybersécurité, ISE SYSTEMS
gerard.pazuelo@ise-systems.fr