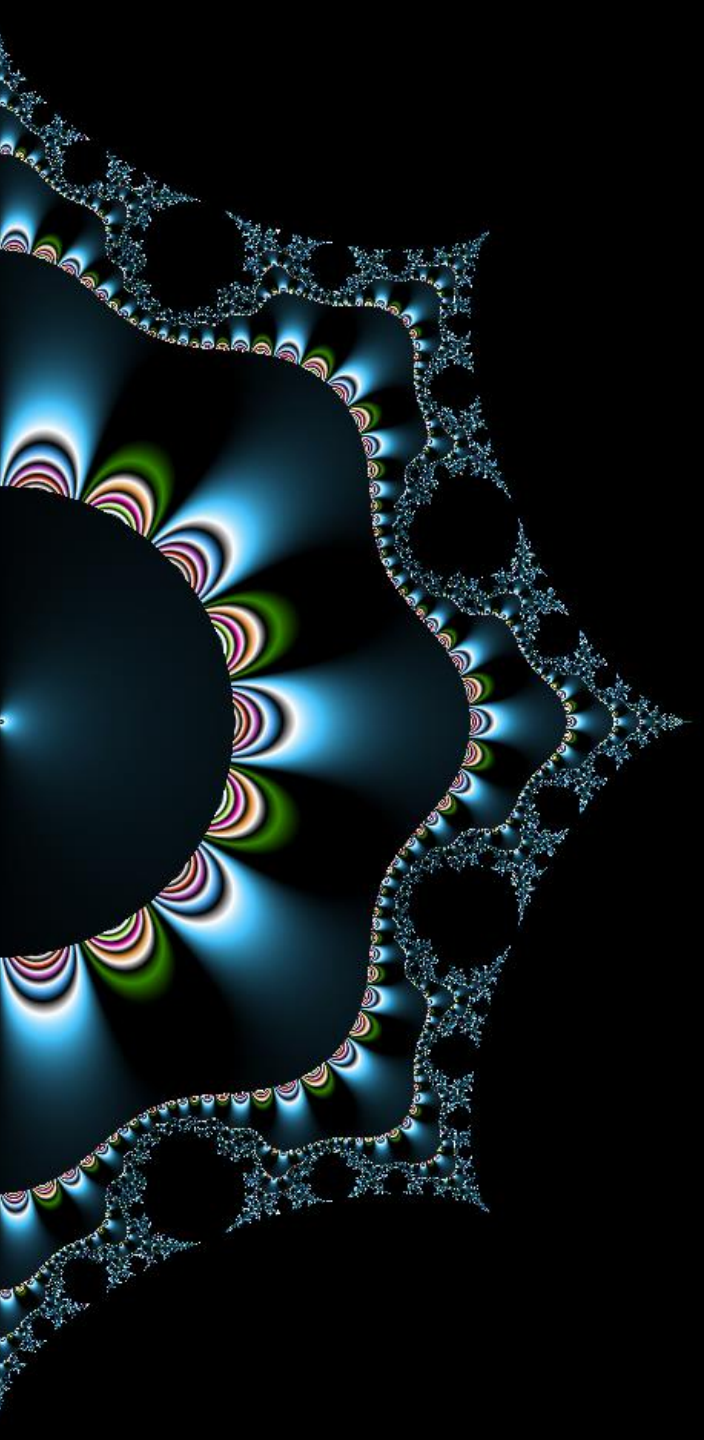


EBIOS RM

Cas Pratique, Partie 2
Ateliers 4 & 5

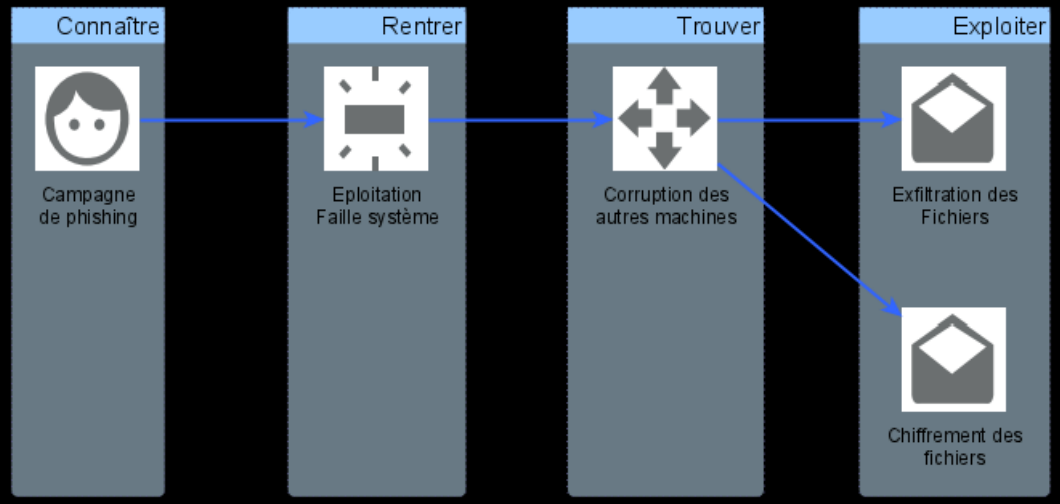
Thibaut HENIN

tbowan@arsouyes.org

Atelier 4

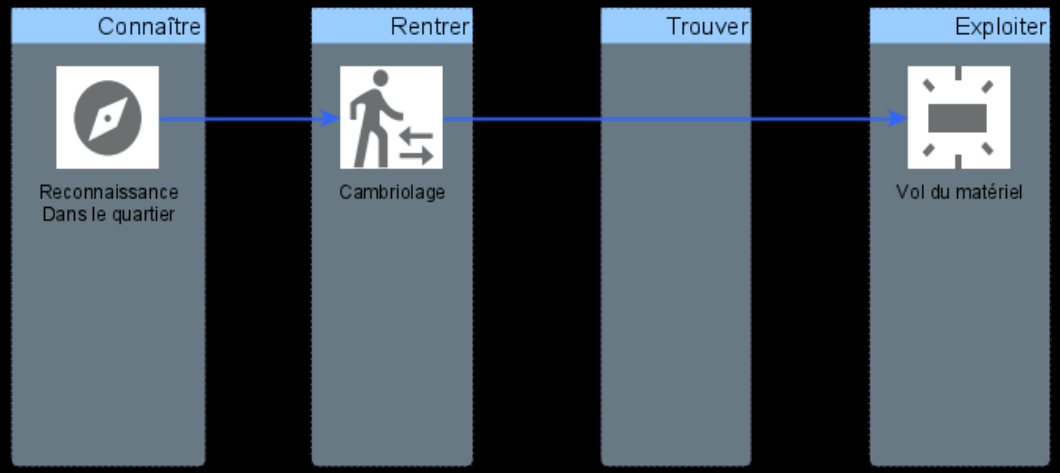
Scénarios opérationnels

Scénario 1 – Ransomware / Extorsion



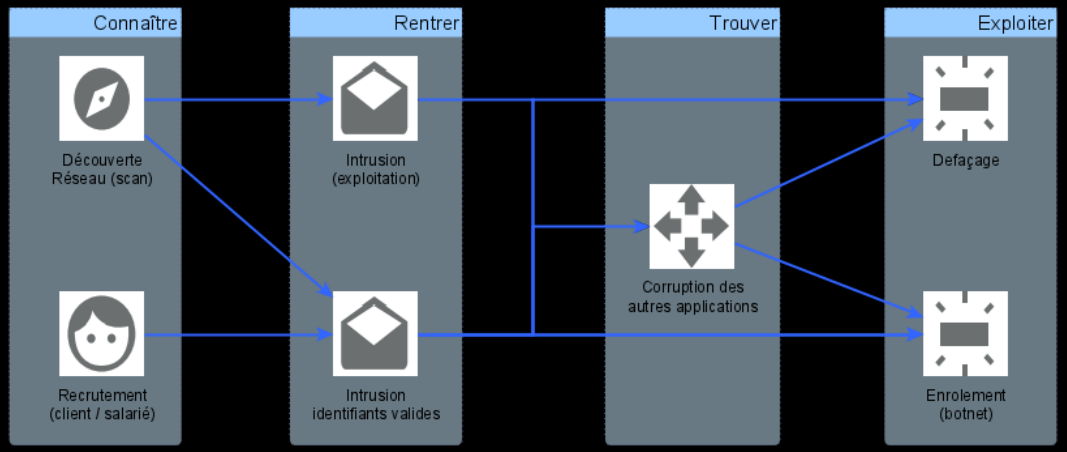
Probabilité	4
Difficulté	1
Vraisemblance	4

Scénario 2 - Cambriolage



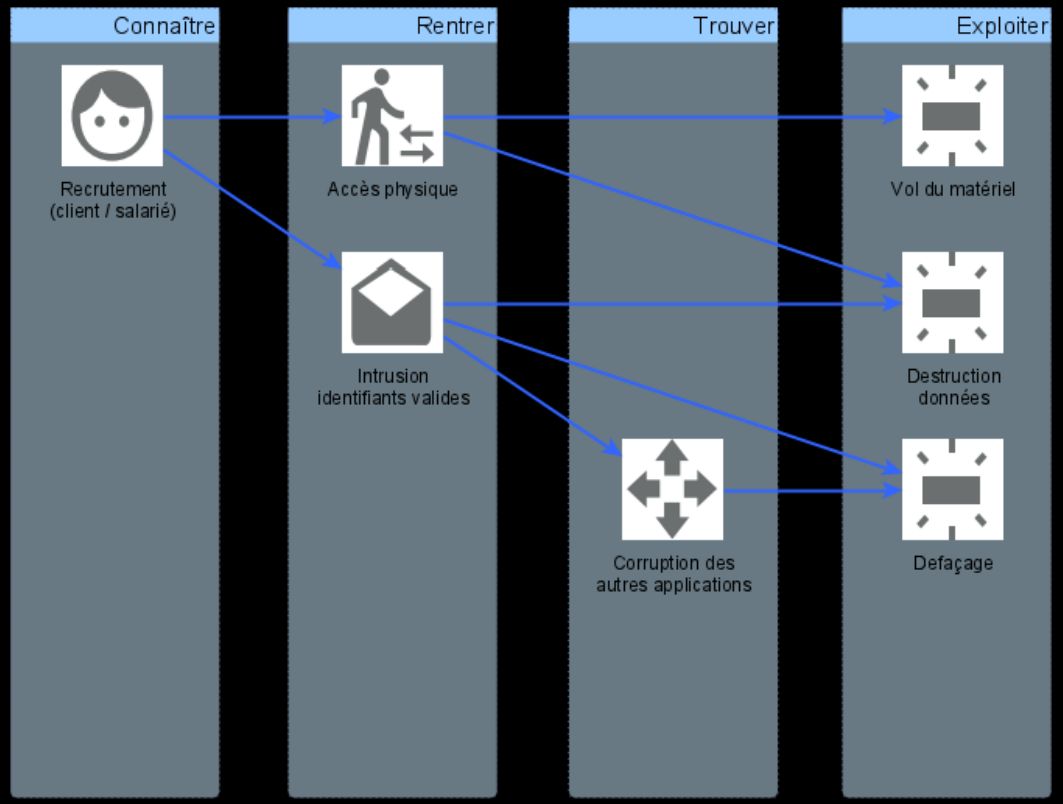
Probabilité	3
Difficulté	2
Vraisemblance	3

Scénario 3 – Defaçage / Botnet



Probabilité	3
Difficulté	2
Vraisemblance	3

Scénario 4 – Sabotage



Probabilité	1
Difficulté	3
Vraisemblance	1

Evaluation

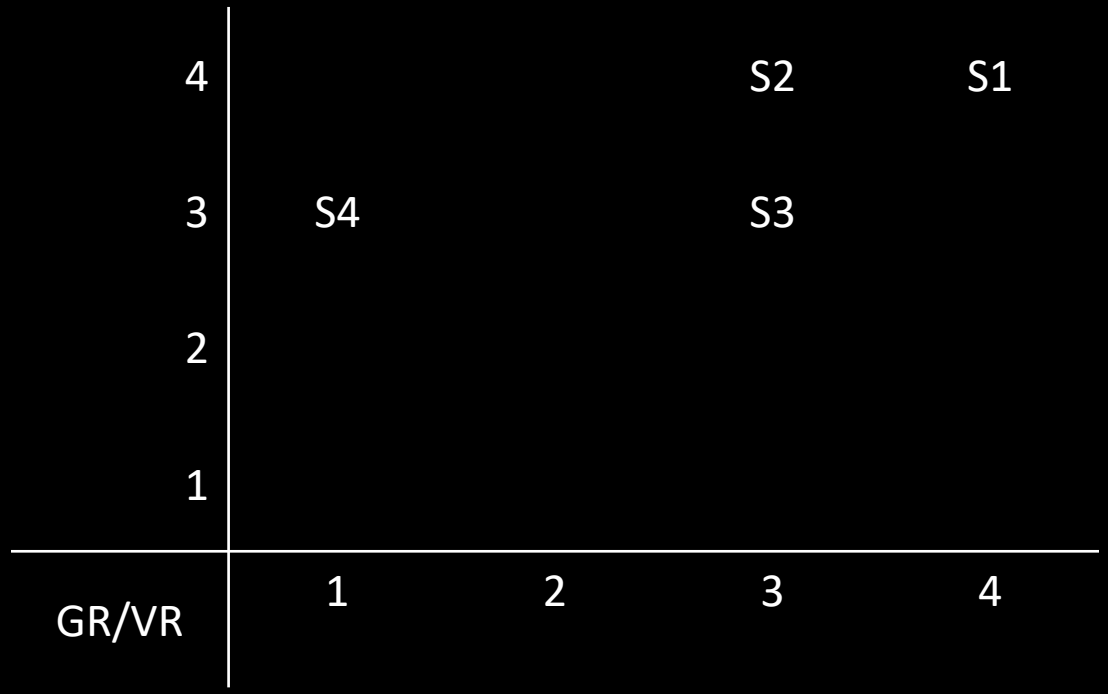
#	Scénario	Probabilité Réussite	Difficulté technique	Vraisemblance	Gravité (rappel)
S1	Ransomware / extorsion	4	1	4	4
S2	Cambriolage	3	2	3	4
S3	Défaçage	3	2	3	3
S4	Sabotage	1	3	1	3

Atelier 5

Traitement du risque

1 – Synthèse des scénarios

- S1 – Ransomware
- S2 – Cambriolage
- S3 – Defaçage
- S4 – Sabotage



2.1 – Stratégie de traitement

Faible

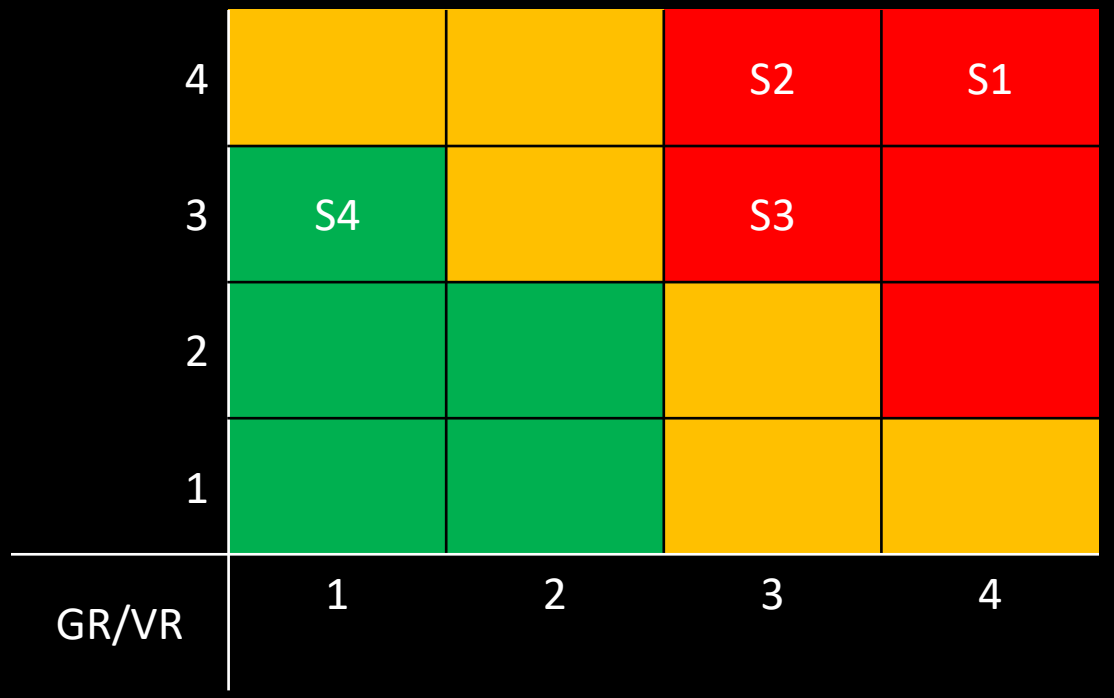
(acceptable en l'état)

Moyen

(Tolérable sous contrôle)

Élevé

(Inacceptable)

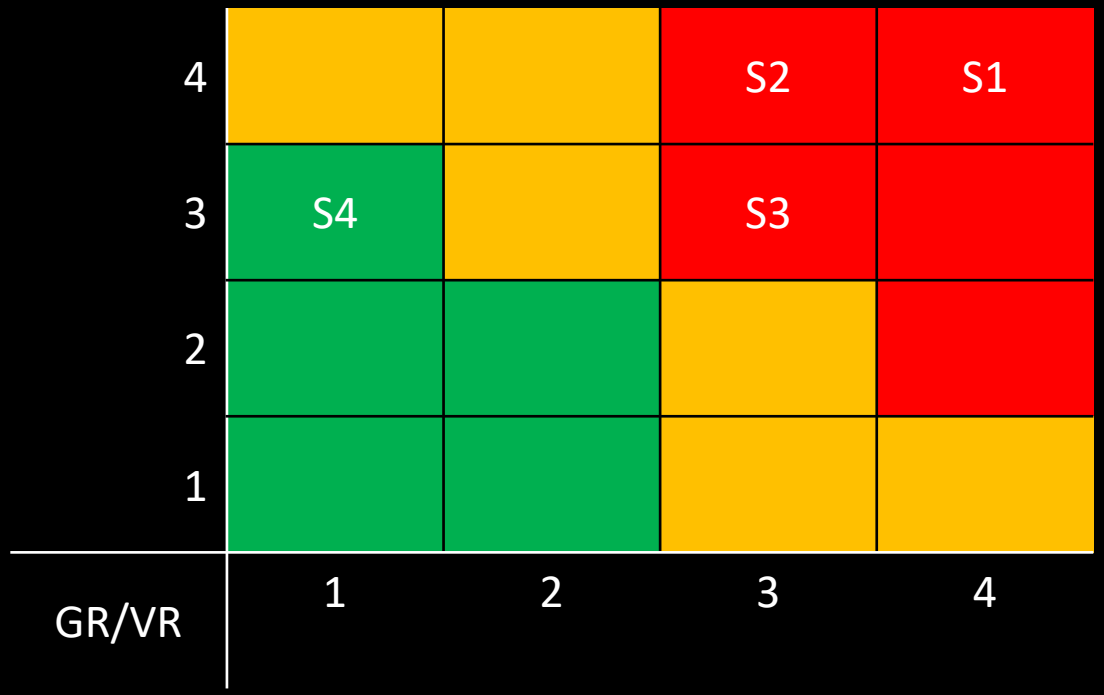


Mesures de sécurité

Mesure	S1	S2	S3	S4	Diff.	Priorité
Mesures organisationnelles						
Formation SSI	✓		✓		+	Long
Organisation d'un audit SSI indépendant	✓		✓		+	Long
Externalisation des sauvegardes	✓	✓	✓	✓	+	Urgent
Mesures techniques						
Mise à jour automatique du système et des anti-virus	✓			✓	+	Urgent
Ajout d'un pare feu réseau et cloisonnement réseaux	✓		✓	✓	+	Moyen
Ajout d'un pare feu applicatif (type waf) en frontal			✓	✓	++	Moyen
Cloisonnement des applications dans des conteneurs (i.e. docker)			✓	✓	++	Moyen
Mesures physiques						
Installation d'une alarme + serrures		✓		✓	+	Urgent

2.1 – Stratégie de traitement

Avant



Après