SEKOIA et **AMOSSYS** vous présentent le projet

avec le soutien de la **DGA**

DALID Démonstrateur Automatisé de Lutte Informatique Défensive

Problématique

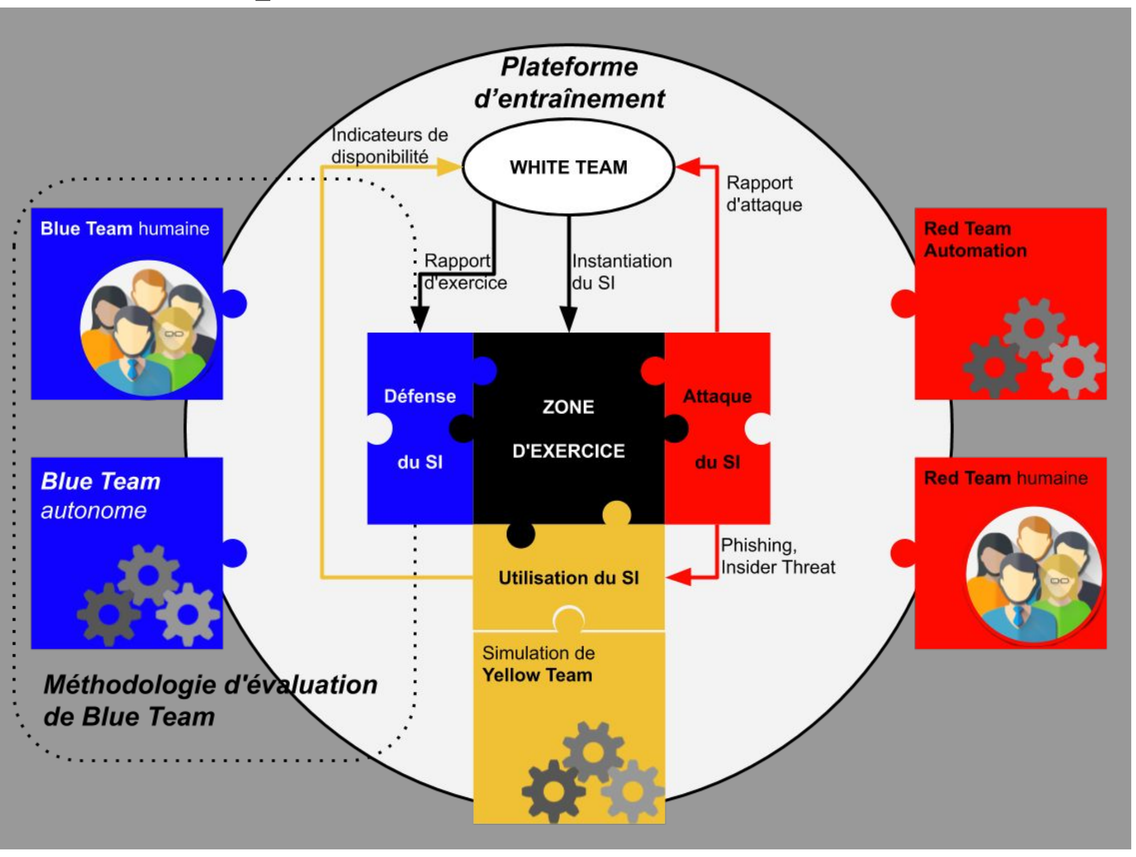
La bonne santé d'une organisation dépend de l'intégrité de son système d'information (SI), Il faut surveiller le SI et adapter sa configuration et celle des équipements de sécurité en cas d'attaque avec un SOC

Mais la mise en place et l'exploitation d'un SOC sont complexes et coûteuses.

- compétences rares
- attaques évoluant rapidement
- asymétrie entre attaque et défense

Objectifs

1. une plateforme d'entraînement et d'évaluation pour la LID
2. un agent autonome capable de réagir rapidement et compléter voire suppléer les opérateurs humains en cas d'attaque



Planning

	Resultats attendus	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Lot 1	L.1.1 : Etat d'avancement intégration	.	.	x																					
	L.1.2 : Spécification format description SI				.	.	x																		
	L.1.3 : Spécification format rapport det indicateurs						.	.	.	x															
	L.1.4 : Documentation et tests API fin d'exercice									.	.	.	x												
	L.1.5.1 : Plateforme DALID en version 1	.	.	.	.	.	x																		
	L.1.5.2 : Plateforme DALID en version 2						.	.	.	.	.	.	x												
	L.1.5.3 : Plateforme DALID en version 3												.	.	.	.	.	.	x						
	L.1.5.4 : Plateforme DALID en version 4																		.	.	.	.	.	.	x
Lot 2	L.2.1 : playbooks de remédiation prédéfinis	.	.	x																					
	L.2.2 : apprentissage/génération règles de détection	.	.	.	.	.	.	.	.	x															
	L.2.3 : apprentissage/génération de playbooks									.	.	.	.	.	.	x									
	L.2.4 : apprentissage par renforcement												.	.	.	.	.	.	.	.	.	x			
Lot 3	L.3.1 : Descriptif traces système et réseau	.	.	x																					
	L.3.2.1 : Yellow Team en version 1	.	.	.	.	.	x																		
	L.3.2.2 : Yellow Team en version 2							.	.	.	.	.	x												
	L.3.2.3 : Yellow Team en version 3																		.	.	.	.	x		
	L.3.3.1 : Red Team Automation en version 1	.	.	.	.	.	x																		
	L.3.3.2 : Red Team Automation en version 2							.	.	.	.	.	x												
	L.3.3.3 : Red Team Automation en version 3																		.	.	.	.	x		
Lot 4	L.4.1 : Méthodo entraînement opérateurs humain													.	.	x									
	L.4.2 : Méthodo évaluation Blue Team autonomes													.	.	.	.	.	x						
	L.4.3 : Rapport entraînement de personnels																					.	.	.	x
	L.4.4 : Rapport évaluation Blue Team autonome																					.	.	.	x

Composants innovants

White Team

La *white team* est responsable de la définition et de l'arbitrage de l'exercice, elle génère et simule le SI cible et produit un rapport.

Yellow Team

La *yellow team* représente les utilisateurs légitimes du système. Elle génère un trafic représentatif du SI.

Red Team

La *red team* attaque le SI selon des objectifs définis avec la white team et informe cette dernière des techniques déployées.

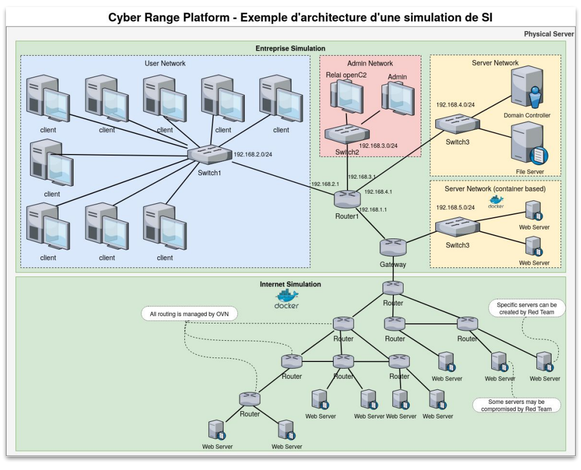
Blue Team

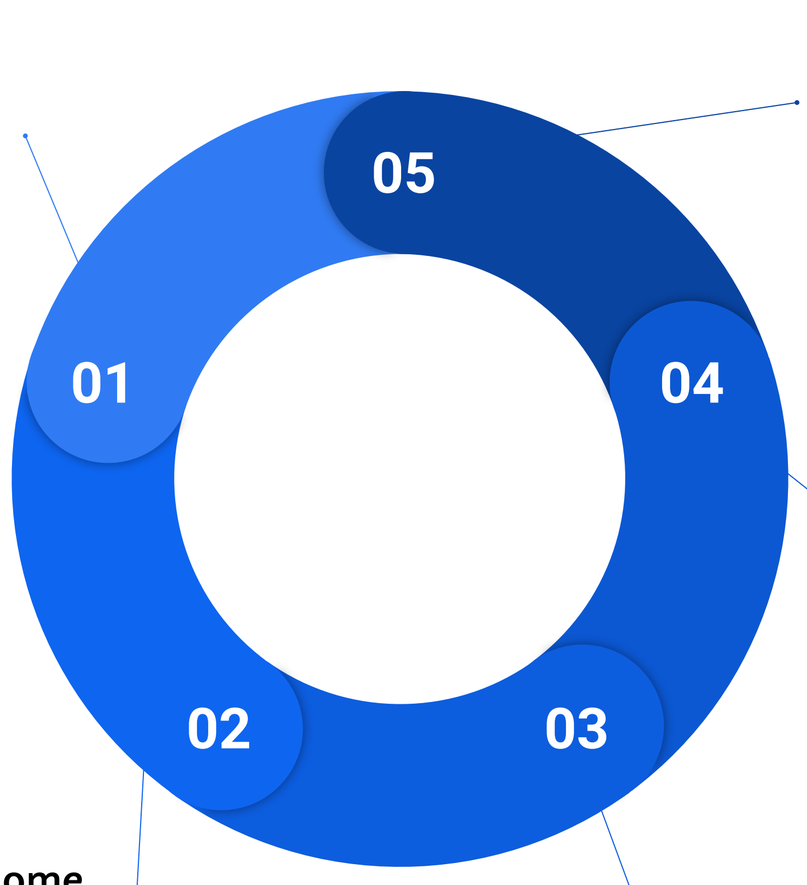
La *blue team* défend le SI sur les angles de l'intégrité et de la confidentialité face à la *red team* tout en assurant la disponibilité.

Une première version de la plateforme déjà déployée

Synthétise un SI

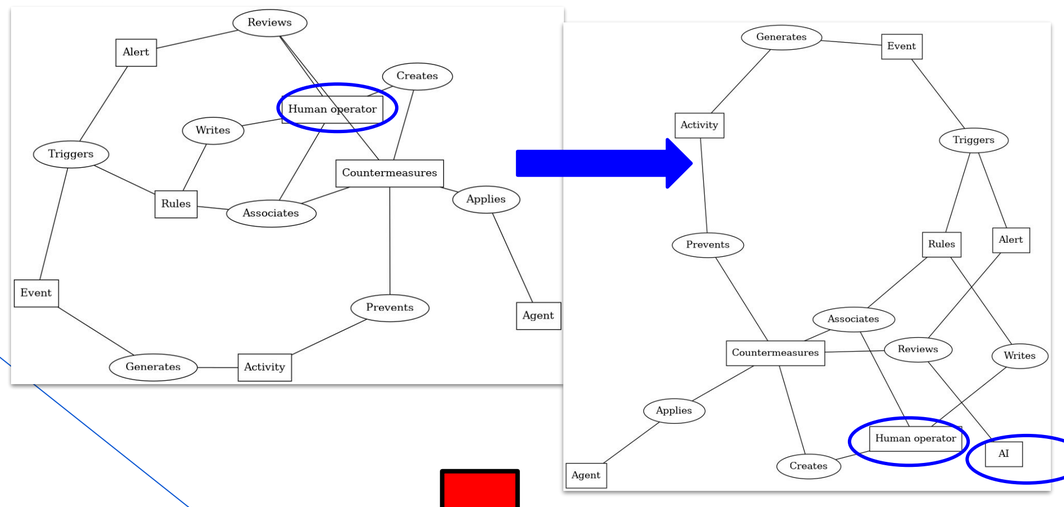
à partir d'une description déclarative, basée sur un profil client réaliste. A venir: mesures de réussite des objectifs de la red et de la blue team.





Détecte et remédie

Les alertes relevées sont qualifiées automatiquement par un classifieur entraîné sur des qualifications effectuées par des opérateurs humains experts. Les contre mesures associées sont automatiquement mises en oeuvre.

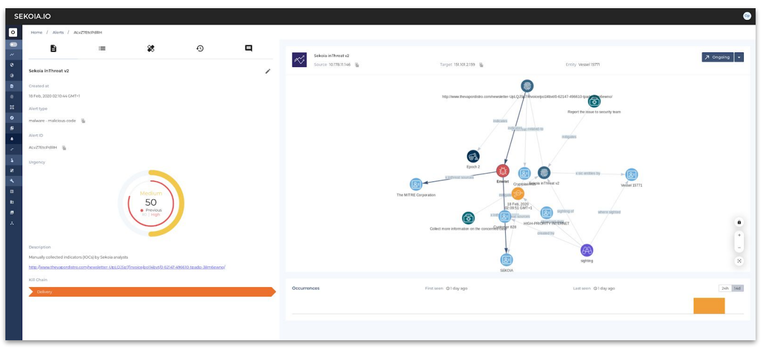


Exécute des attaques

tirées de données sur des attaques réelles et selon le type de profil client simulé. La *white team* peut donner un point d'entrée à la *red team* pour rendre l'exercice intéressant.

Déploie un SOC autonome

avec une remontée automatique des événements et des capacité de remédiations.



Simule de la vie

pour générer une activité utilisateur réaliste, et pour activer certaines étapes d'attaque (phishing).