RAPPORT PROJET

Déploiement automatique d'infrastructure
Analyse Forensique AFC

GUILET Arthur | DEMARCO Hugo | CAPE Swann
ENGASSER Antoine | CLOUX Erwan | HALIMI Yohan

contact@goatline.tech

goatline.tech

Diffusion				
Société / Entité	**Destinataires**	**Fonction**	**Diffusion**	**Pour info**
GoatLine	Service IT	Rapport	Réseau, mail, papier	

Visas			
Société/Entité	**Nom**	**Fonction**	**Lieux**
Esiee-IT	M. KAIDI K.	Management Projet	Pontoise (95)

SUIVI DES VERSIONS

Version	Date	Auteur	Raison	Nombre de pages
V1.1	03/06/2024	ENGASSER Antoine DE MARCO Hugo HALIMI Yohan GUILET Arthur CLOUX Erwan CAPE Swann	Rapport de Projet	26

COORDONNEES

Contacts		
Nom	**E-mail**	**Téléphone**
GoatLine	contact@goatesque.tech	

Table des matières

contact@arthur-guilet.fr

contact@arthur-guilet.fr

1. Abstract

L'entreprise fictive GOATLINE a entrepris un projet de déploiement automatique d'infrastructure avec une analyse forensique visant à tester et améliorer la résilience de son système. Ce projet s'inscrit dans un contexte pédagogique où la croissance des cyberattaques nécessite une réactivité pour identifier, catégoriser, et corriger les vulnérabilités. L'objectif est d'appliquer, les connaissances théoriques acquises au cours de l'année, afin d'assurer la sécurité des données de l'entreprise.

C'est pourquoi, le projet est décomposé en nombreuses étapes, l'établissement d'une infrastructure automatisée puis sa protection par la détection d'intrusion. Suivi d'une attaque informatique exploitant les vulnérabilités de l'infrastructure ; et enfin l'analyse d'incidents de sécurité, la collecte des preuves numériques et leur exploitation pour l'établissement d'un rapport forensique.

Pour gérer ce projet de manière structuré et organique, nous avons utilisé différentes méthodes managériales, avec l'outil collaboratif SharePoint, permettant une collaboration efficace entre les membres du projet, une gestion centralisée des documents, et un suivi précis des tâches et des échéances.

Depuis, ce rapport vous pourrez comprendre, les différentes étapes, méthodes, et outils utilisés durant nos travaux. Nous remercions nos professeurs pour leurs conseils, et l'aide qu'ils nous ont apportés durant ce projet.

Bonne lecture.

contact@arthur-guilet.fr

2. Description du projet

2.1 Contexte

L'objectif principal de ce projet est de renouveler une infrastructure d'entreprise puis de la soumettre à une cyberattaque afin de développer des compétences en cybersécurité en pour les employés de l'entreprise, et de faire ressortir les points d'amélioration de l'infrastructure. Les employés auront pour tâche de mener une enquête approfondie pour comprendre la portée de l'attaque, identifier les acteurs impliqués, et proposer des mesures correctives.

Différentes étapes sont demandées :

- Préparation de l'environnement
- Détection de l'incident
- Isolation et Préservation des Preuves
- Analyse Forensique
- Rapport d'Analyse Forensique
- Production d'attendus et livrables

2.2 Enjeu

Le projet comporte de nombreux enjeux, la première étant la capacité à mettre en place un environnement automatiquement ne possédant pas des failles de sécurité évidente, similaire à des infrastructures d'entreprises traditionnelles. Puis, la mise en place d'une attaque documentée et intégrant les méthodologies inhérentes, ainsi que la détection, l'isolation des preuves. Enfin, une analyse forensique de l'attaque enregistrée, doit nous permettre de comprendre les lacunes de notre système informatique, et les leçons apprises.

2.3 Objectif

Ce projet offre une expérience pratique et immersive dans deux domaines, le DevOps et la cybersécurité, permettant aux employés de développer des compétences en automatisation, attaque et en défense tout en renforçant leur compréhension des vulnérabilités et des mécanismes de sécurité. Voici les différentes étapes du projet :

contact@arthur-guilet.fr

1. **Conception de l'Environnement :**
    - Créer un environnement virtuel avec plusieurs machines virtuelles, de façon automatisée avec des outils modernes.
    - Sécuriser l'environnement selon les bonnes pratiques d'organismes reconnus.

2. **Formation des Équipes Cybersécurité:**
    - Les employés sont divisés en deux équipes : une équipe attaquante et une équipe de défense.
    - L'équipe attaquante doit comprendre les différentes méthodes d'attaque, tandis que l'équipe de défense doit mettre en place des mécanismes de détection et d'analyse d'attaque.

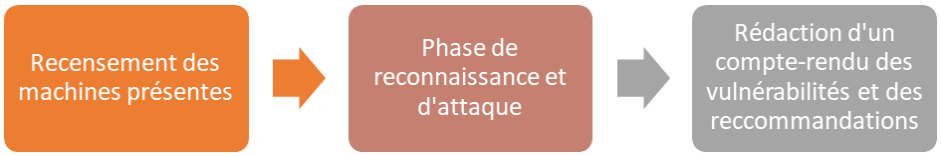
3. **Attaque de l'infrastructure :**
    - Recherche de vulnérabilités et de tentatives d'exploitations dans l'infrastructure déployée au préalable

4. **Analyse forensique:**
    - Exploitation et analyse des preuves récoltées, en vue de proposer des solutions pour l'entreprise GoatLine.

Voici un schéma des différentes actions qui se dérouleront :

Pour la partie infrastructure :

Pour la partie cybersécurité :

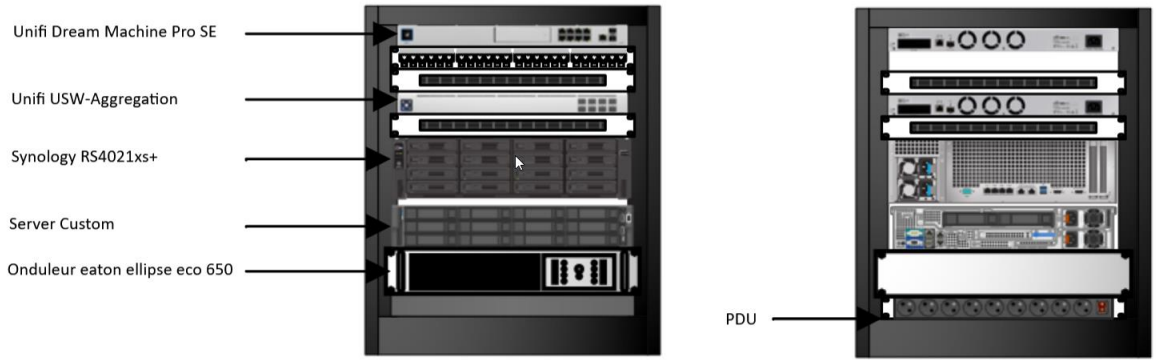


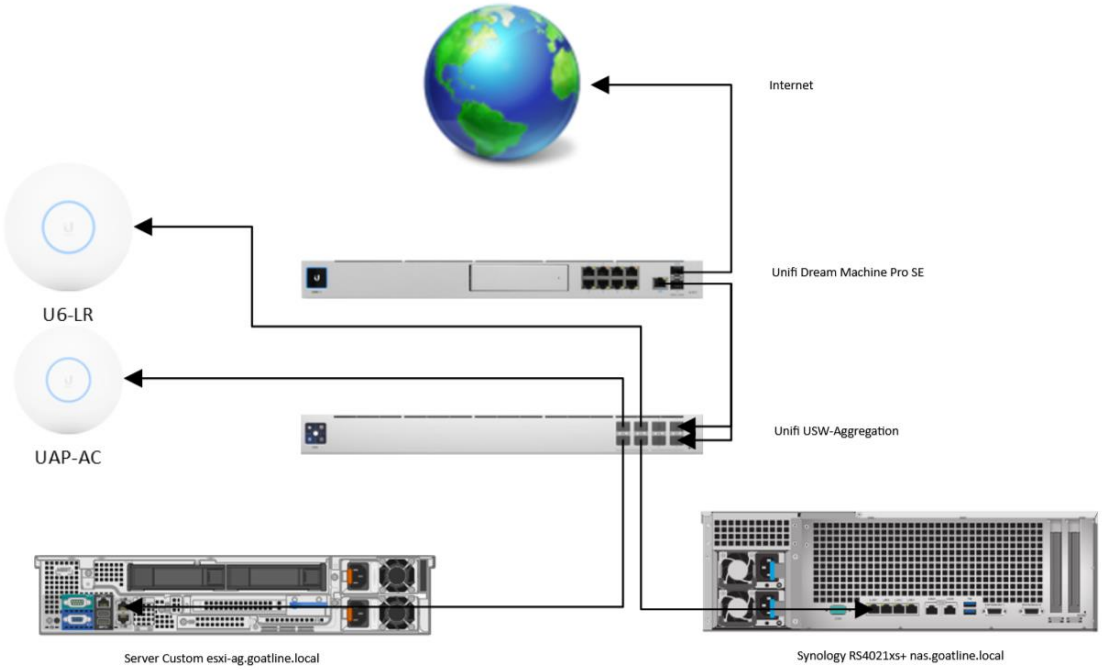
contact@arthur-guilet.fr

2.4 Périmètre (fonctionnel et technique)

2.4.1 Étude de faisabilité

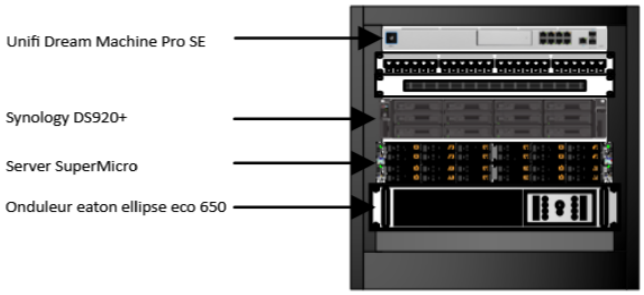
Nous disposons de deux infrastructures auto-hébergées. La première est située sur le site d'Arthur. Elle est composée d'une baie qui comporte en entrée WAN (internet) un pare-feu, à savoir l'Unifi Dream Machine Pro. Ensuite, derrière le pare-feu, il y a un commutateur d'agrégation qui distribue internet au serveur et au NAS, avec une interconnexion en 10 Gbits. De plus, des bornes Wi-Fi Unifi sont connectées pour mettre en place un réseau Wi-Fi à usage professionnel et pour les invités.

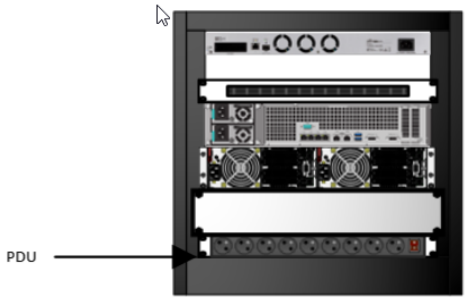


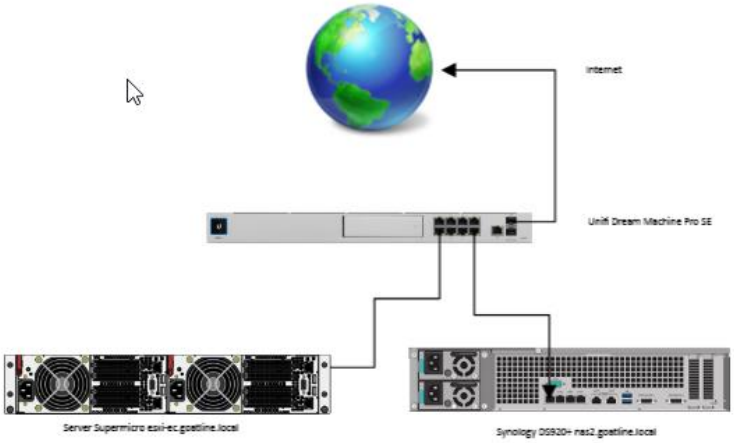


contact@arthur-guilet.fr

La deuxième est située sur le site d'Erwan. Elle est composée d'une baie qui comporte en entrée WAN (internet) un pare-feu, à savoir l'Unifi Dream Machine Pro. Ensuite, derrière le pare-feu. Le firewall distribue internet au serveur et un NAS, avec une interconnexion en 10 Gbits. De plus, des bornes Wi-Fi Unifi sont connectées pour mettre en place un réseau Wi-Fi à usage professionnel et pour les invités.







2.4.2 Besoins fonctionnels

Dans le cadre d'un projet de mise en place d'une infrastructure d'un système informatique d'entreprise, il est important de répondre aux besoins fonctionnels qu'elle doit fournir. Cela passe par la mise en place de services essentiels, tel qu'un serveur web avec la capacité de recevoir et traiter des requêtes HTTP, à servir de page web statique ou dynamique, un serveur SMTP/IMAP capable de gérer efficacement la réception et l'envoie des courriels des salariés de GOATLINE, d'un serveur de stockage

contact@arthur-guilet.fr

pour gérer les données de manière centralisée et efficace, un Active Directory permettant une gestion de l'authentification, et la gestion des ressources.

De plus, il est nécessaire de répondre à des critères de sécurité à un SI d'entreprise, cela passe par la mise en place de pare-feu qui est primordiale pour assurer un filtrage et contrôle du flux du système d'information de GOATLINE, la mise en œuvre de mécanisme de sauvegarde régulier pour garantir la disponibilité et l'intégrité des données, une segmentation du réseau est fondamentale entre des services exposés et non-exposés (LAN et DMZ).

Enfin, le système doit être constamment supervisé par une plateforme prévue à cet effet.

2.4.3 Besoins non-fonctionnels

Dans le cadre de la mise en place d'une infrastructure d'entreprise, les besoins non fonctionnels sont aussi cruciaux que les besoins fonctionnels. Ces besoins portent sur les aspects de performance, de sécurité, et de disponibilité de l'ensemble du système. En ce qui concerne la performance, GOATLINE a défini un temps de réponse attendu et une gestion efficace des pics de charge. Du côté sécurité, la protection des données par une démarche RGPD est effectuée par nos services, ainsi que l'application des normes de sécurité de l'ANSSI. Enfin, en ce qui concerne la disponibilité, la planification de sauvegardes régulière, une redondance de service, ainsi que la mise en place d'un plan de continuité d'activité.

2.5. Parties prenantes et rôles

Le projet est composé de différentes phases et de sous-phases, c'est pourquoi différentes équipes y ont été assignées, afin d'assurer le bon fonctionnement du système d'information. L'équipe infrastructure est chargée de la création du système informatique, de la maintenance et de la supervision de celle-ci. Elle s'assure que les composants matériels et logiciels fonctionnent et répondent aux besoins de l'entreprise et des équipes. Parallèlement, l'équipe cybersécurité est divisée en deux sous-équipes complémentaires : "Blue Team" et "Red Team". La Blue Team se concentre sur la défense et le contrôle de la sécurité du système d'information. Elle identifie les vulnérabilités, surveille les activités suspectes, et réagit aux incidents de sécurité pour protéger les données et ressources de l'entreprise. A contrario, la Red Team adopte une approche offensive en simulant une attaque sur le système d'information de GOATLINE, pour identifier les différentes failles de sécurité que les cyberattaquants pourraient exploiter. En menant des tests d'intrusion et des scénarios d'attaque, la Red Team aide à renforcer la résilience du SI de GOATLINE, la Blue Team s'occupe de la correction et de l'analyse des preuves.

2.6. Contraintes

Nous pouvons dire que les contraintes de l'équipe attaquante correspondent au prérequis de l'équipe de déploiement. En effet, notre équipe de déploiement a créé une infrastructure d'entreprise complète de manière que celle-ci soit le plus réaliste possible. Ce qui est une contrainte non

contact@arthur-guilet.fr

négligeable pour l'équipe de pentester qui devront redoubler d'efforts afin de pénétrer dans l'infrastructure, ce qui ne sera pas une tâche aisée.

2.7. Analyse et gestion des Risques

GoatLine doit être informé des éventuels risques liés aux tests d'intrusions. En effet, des débordements peuvent s'appliquer indépendamment de la volonté des équipes d'attaques (Blue Team et Red Team).

Ainsi, les risques possibles identifiés sont :

- Déni de service sur des machines non inclues dans les règles de conventions de Pentest
- Pertes de données
- Violation des DIC (Disponibilité, Intégrité et Confidentialité) avec, mais sans s'y limiter :
    - Chiffrage de données
    - Suppression de données
    - Reverse engineering
    - Piratage de mot de passe

Afin de répondre à ces risques, plusieurs éléments ont été mis en place :

- Rédaction d'un ROE : Document guidant les attaquants vers les cibles autorisées ou non, et les règles pour attaquer en toute sécurité.
- Mise en place d'un plan de sauvegarde : L'infrastructure est sauvegardée sur plusieurs supports avec une restauration disponible quasi immédiate permettant de rétablir l'infrastructure en cas de soucis majeur
- Monitoring : Afin de détecter des défaillances sur des matériels non ciblés initialement, un monitoring avec un PRA est mis en place

En cas de doutes et de problèmes, les responsables sont :

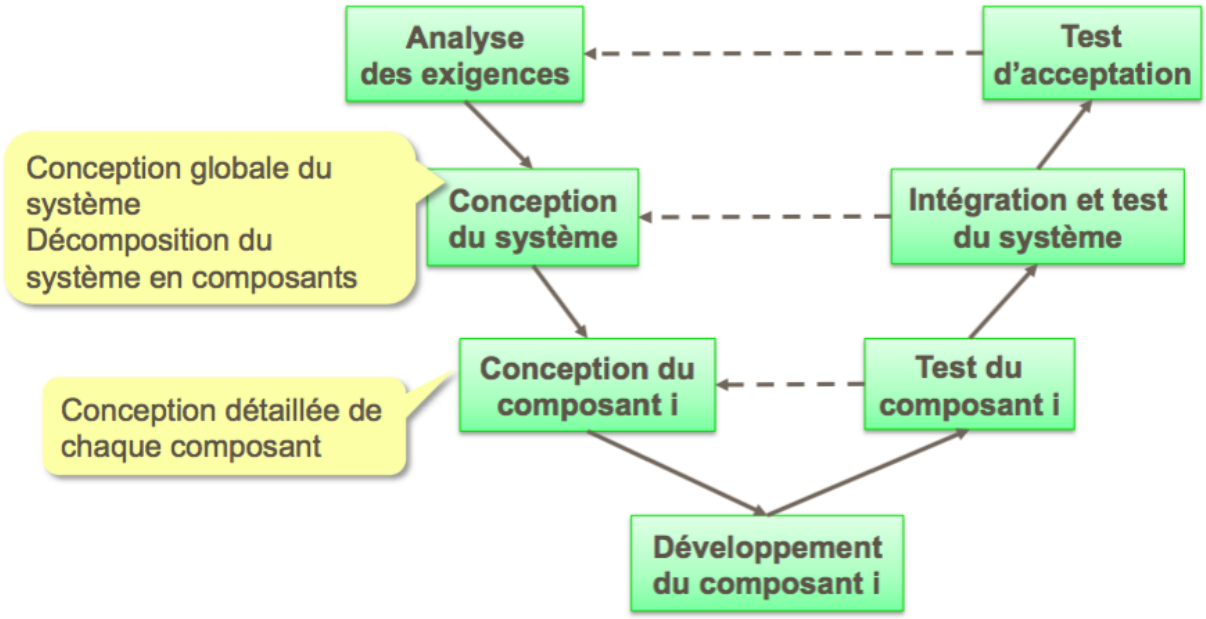
- Responsable Cyber : Hugo DE MARCO
- Responsable hébergement : Arthur GUILET
- Responsable DevOps : Erwan CLOUX

contact@arthur-guilet.fr

3. Méthodologie de gestion de projet

3.1 Choix et Description de la méthodologie de gestion de projet

Dans le cadre de notre projet, nous avons adopté la méthode en V comme stratégie de conception agile. Cette méthode structure le processus de développement en plusieurs phases linéaires et synchronisées, avec des tests qui se déroulent en parallèle à chaque étape de développement. Il est essentiel de compléter chaque phase de développement et de test correspondante avant de passer à la suivante.



La méthode en V se caractérise par une progression linéaire, où chaque étape succède logiquement à la précédente jusqu'à l'achèvement du projet. La branche gauche du V détaille les phases de conception et de vérification, tandis que la branche droite concerne les phases de validation, qui se déroulent parallèlement au développement. Les phases de conception et de validation convergent au sommet du V.

L'un des principaux avantages de cette méthode est sa structure linéaire, qui clarifie les étapes du projet et facilite la gestion des tâches. Cette organisation permet une gestion claire et prédictive du projet, où il est facile de déterminer les phases actuelles, passées et futures.

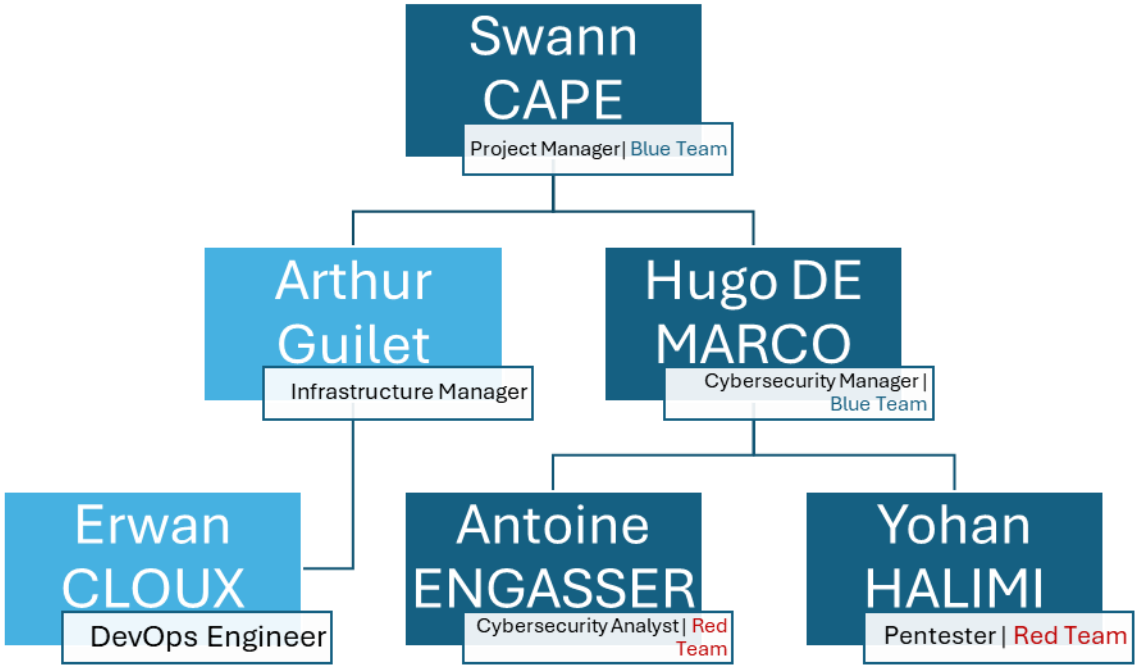
Bien que le caractère linéaire, rigide et restrictif du cycle en V puisse sembler être un désavantage, cette rigueur est en fait bénéfique pour les projets ayant des exigences strictes et des délais non flexibles. En effet, cette méthode permet une excellente gestion du temps et s'adapte bien aux projets nécessitant le respect de délais précis et l'accomplissement de phases clairement définies.

contact@arthur-guilet.fr

3.2 Organisation de travail et pilotage

Notre équipe est composée de 6 personnes :

- Swann CAPE notre directeur général
- Antoine ENGASSER notre analyste de cybersécurité
- Hugo DE MARCO notre ingénieur de cybersécurité
- Arthur GUILLET notre architecte cloud
- Erwan CLOUX notre ingénieur DevOps cloud
- Yohan HALIMI notre Pentester



Le pilotage et le partage de connaissance sont centralisés depuis l'outil SharePoint, une plateforme de collaboration et de gestion de contenu comprise dans la suite Microsoft 365. L'utilisation de cette plateforme nous a permis de créer un espace de partage de contenu, et de planification/gestion de projet.

Le pilotage du projet s'est effectué selon des rôles bien distincts. Afin de mener à bien le projet et d'en faciliter les échanges, Hugo de Marco, Manager de la partie Cybersécurité du projet, a eu la charge de faire le lien entre l'équipe CyberAttaque, CyberDéfense et Infrastructure.

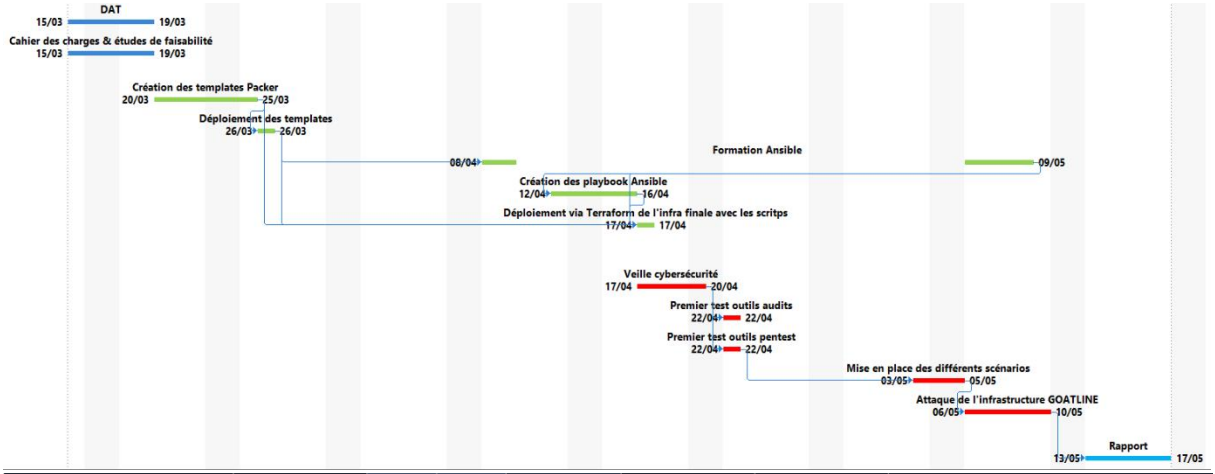
En effet, pour être mené à bien, le projet nécessitait un profil correspondant, capable de récolter les informations et de comprendre les enjeux du projet auprès de chaque équipe, afin d'ensuite pouvoir proposer un plan d'action de réalisation du projet au chef de projet.

contact@arthur-guilet.fr

Ainsi, dès lors qu'une équipe avait une interrogation sur un aspect du projet concernant une autre équipe, Hugo se chargeait de faire circuler les informations, tout en prenant soin de ne pas divulguer d'informations confidentielles (Surtout entre les équipes attaque et défense), qui pourraient nuire au projet.

3.3 Planning et Diagramme de Gantt

Le projet est supervisé de manière efficace par l'emploi de différents outils et de technique. Pour une vision globale, un diagramme de Gantt a été établi pour visualiser le calendrier des tâches et suivre l'avancement du projet, en identifiants les éventuels retards, les tâches critiques, afin d'élaborer les ajustements nécessaires. Parallèlement, un planning a été établi, définissant les étapes clés et les échéances, assurant une vision claire du déroulement du projet.



Tâche	Assigné à	Début	Fin	Durée	Statut	Priorité	Commentaire
DAT	Arthur	15/03	18/03	3	Fini	Faible	
Cahier des charges & études de faisabilité	Yohan, Antoine, Hugoat, Swann , Arthur	15/03	18/03	3	Fini	Faible	
Création des templates Packer	Erwan	20/03	25/03	5	Fini	Moyen	
Déploiement des templates	Erwan	26/03	26/03	0	Fini	Moyen	
Formation Ansible	Erwan	20/03	25/03	5	Fini	Faible	
Création des playbook Ansible	Erwan, Arthur	26/03	26/03	0	Fini	Moyen	
Déploiement via Terraform de l'infra finale avec les scripts	Erwan	08/04	11/04	3	Fini	Moyen	
Veille cybersécurité	Antoine	11/04	20/04	9	Fini	Faible	
Premier test outils audits	Antoine, Hugoat, Swann	22/04	22/04	0	Retard	Faible	UDM SITE AG Remplacé, reprise
Premier test outils pentest	Antoine, Yohan	22/04	22/04	0	Retard	Faible	UDM SITE AG Remplacé, reprise
Mise en place des différents scénarios	Antoine, Yohan	03/05	05/05	2	Retard	Moyen	UDM SITE AG Remplacé, reprise
Attaque de l'infrastructure GOATLINE	Yohan	06/05	10/05	4	Retard	Élevé	UDM SITE AG Remplacé, reprise
Rapport	Arthur, Swann , Yohan, Hugoat, Antoine, Erwan	13/05	17/05	4	Non démarré	Élevé	UDM SITE AG Remplacé, reprise

De plus, des réunions régulières ont été organisées pour favoriser la communication et la coordination entre les différents employés, résoudre les problèmes rapidement et ajuster les plans en fonction des imprévus. Par ailleurs, le coût des structures a été évalué, permettant une gestion rigoureuse du budget et des ressources.

contact@arthur-guilet.fr

4. Livrables

4.1 Tests de validation

Les différentes étapes clés de notre projet étants la construction, la défense, l'attaque et l'exploitation de preuves de l'infrastructure, les différentes étapes ont été validées lors de la construction de la documentation propre à ces étapes ; soit :

- La validation du plan d'infrastructure déployée, dans le livrable *Technical Architecture Document*
- La validation du plan d'attaque, dans le livrable *Rules of Engagement*
- La validation du système de détection d'intrusion, dans le livrable *Documentation on Snort*
- La validation de la phase d'attaque, dans le livrable *Pentest Report*
- La validation de la phase d'investigation, dans le livrable *Forensic Report*

L'intégralité de ces livrables sont présents dans les annexes de ce dossier.

4.2 Documentation technique

Notre projet visant à faire monter en compétences les équipes informatiques de l'entreprise GoatLine, il était impératif de mettre en place des documentations pour tous les aspects techniques du projet, afin d'effectuer un transfert des compétences propres aux différents profils composants le service informatique de l'entreprise.

4.2.1 Documentation de la topologie de l'entreprise

Voir Annexe "DAT Goatline; IT topology"

La première documentation technique réalisée par l'équipe infrastructure de Goatline fut la documentation traitant de la topologie de l'entreprise. Cette documentation, contenant un schéma détaillé du réseau, ainsi qu'un document d'architecture technique (DAT) contenant l'ensemble des informations sur l'infrastructure physique et virtuelle déployée chez Goatline, a permis à l'équipe de CyberDéfense, qui n'avait pas participé à son développement, de connaître les moindres spécificités de l'infrastructure et par conséquent de pouvoir identifier et sécuriser les différentes surfaces d'attaques.

4.2.2 Documentation du déploiement de l'infrastructure

Voir Annexe « Documentation on Packer and Terraform »

Une autre documentation clé réalisée par l'équipe infrastructure a été la documentation procédurière de déploiement automatisé de l'infrastructure.

En effet, avec la réalisation de ces procédures, l'équipe infrastructure a pu rendre compréhensible par les autres équipes du projet l'intégralité du processus de déploiement automatisé de toutes les machines qui composent l'infrastructure de Goatline. Un transfert de compétences indispensable,

contact@arthur-guilet.fr

puisqu'il a permis à l'équipe Cyberdéfense de mieux comprendre comment avait été mise en place l'infrastructure, et d'effectuer des recherches sur différentes vulnérabilités connues qui pouvaient découler de ce type de déploiement automatisé.

Cette documentation a également permis d'assurer le maintien en condition opérationnel de l'infrastructure d'un point de vue prévisionnel : En assurant ce transfert de compétences, les membres en charge du déploiement automatisé s'assuraient que des effets de bords pourraient être compris et résolus beaucoup plus rapidement en éliminant les zones d'ombres au maximum.

4.2.3 Documentation de la sécurisation de l'infrastructure

Voir Annexe « Documentation on Snort »

Une fois que l'équipe de CyberDéfense avaient une parfaite connaissance de l'infrastructure, cette dernière a pu réaliser une documentation technique traitant de la mise en place de la sonde Snort, chargée d'effectuer un scan complet du réseau et d'effectuer une remontée d'alerte lors de la détection d'évènements suspects.

En effectuant cette documentation technique, l'équipe de CyberDéfense s'est assurée que tous les membres en charge de la sécurité de l'infrastructure possédaient les compétences requises afin de comprendre le fonctionnement de la sonde de détection, et pourraient donc continuer de la maintenir en conditions opérationnelles. Un aspect non négligeable, puisque la sonde repose sur des règles de détections de vulnérabilités connues, règles devant être mises à jour manuellement par les personnes en charge de la sonde.

La réalisation de cette documentation a également permis de sensibiliser l'équipe infrastructure à ce sujet, et par conséquent d'effectuer un travail de collaboration entre l'équipe infrastructure et cyberdéfense, visant à configurer la sonde de façon optimale pour surveiller l'infrastructure mise en place.

4.2.4 Documentation de la phase d'attaque

Voir Annexe « Pentest Report »

Une autre documentation fondamentale de notre projet a été réalisée par l'équipe de CyberAttaque. En réalisant le rapport de pentest, l'équipe de CyberAttaque y a décrit toute la démarche d'attaque, de la méthode de reconnaissance de l'infrastructure, jusqu'à la phase post-exploitation.

Cette documentation a permis dans un premier temps aux membres de l'équipe CyberAttaque d'historiser leurs actions, et d'effectuer un partage de connaissance en interne afin d'effectuer une montée en compétences.

Également, lorsqu'elle a été mise à la disposition des équipes CyberDéfense et système à la fin du projet, cette documentation a permis de sensibiliser les équipes de Goatline sur les différents modes,

contact@arthur-guilet.fr

enjeux et impacts d'une cyberattaque, et donc de faire monter en compétences l'intégralité des équipes sur les manières de se préparer et de réagir à une attaque de ce type.

4.2.5 Documentation de la phase forensique

Voir Annexe « Forensic Report »

La dernière documentation technique ayant joué un rôle clé dans notre projet a été la documentation de rapport forensique. Réalisé par l'équipe CyberDéfense, ce document décrit la manière dont cette dernière a réagi à la cyberattaque, et de quelle manière les alertes générées par la sonde de détection ont été interprétées pour procéder à des analyses forensiques.

L'outil « Autospy », servant à effectuer des analyses forensique y est présenté, ainsi que la procédure de listage des preuves sur les machines virtuelles attaquées.

La mise à disposition de ce rapport permet à l'équipe de CyberDéfense en interne de partager les compétences de chaque membre, ainsi que de mieux se préparer et réagir lors d'une prochaine CyberAttaque.

Ce document a également permis, lorsqu'il a été mis à la disposition de l'équipe CyberAttaque, d'effectuer une montée en compétences en les sensibilisant sur la notion de preuves d'attaque informatiques, et les manières de détecter et parer une attaque informatique sur une infrastructure réelle.

5. Synthèse

5.1 Résultats

Le projet finalisé a marqué plusieurs résultats significatifs dans la réalisation du projet

5.1.1 Résultats apportés par l'équipe Système

Au terme de la phase d'élaboration de l'infrastructure, l'équipe système a pu fournir les résultats attendus par le cahier des charges initial, en déployant l'infrastructure de l'entreprise Goatline de manière automatisée, et en suivant les bonnes pratiques de sécurisation d'un système d'information selon des organismes officiels tels que la CNIL et L'ANSSI.

L'équipe système a donc pu apporter une infrastructure représentative d'une entreprise réelle au 26 avril 2024, contre le 17 avril 2024 initialement prévu.

5.1.2 Résultats apportés par l'équipe Red Team

Au terme de la phase d'attaque, l'équipe de CyberAttaque ont réussi à pénétrer dans l'infrastructure de l'entreprise par divers moyens, décrits dans l'annexe « *Pentest Report* ». Suite à cette phase d'attaque, l'équipe de CyberAttaque possédaient un accès au compte « contact@goatline.tech » et par conséquent un accès à des informations confidentielles.

contact@arthur-guilet.fr

L'équipe de CyberAttaque a pu également se connecter à une machine du réseau de l'entreprise GoatLine, obtenant des accès permettant d'impacter l'intégrité de l'infrastructure.

De ce fait, l'équipe CyberAttaque (Red Team) ont pu démontrer la présence de vulnérabilités dans l'infrastructure de l'entreprise Goatline du mardi 21 au vendredi 24 mai.

5.1.3 Résultats apportés par l'équipe Blue Team

Au terme de la phase de forensique, l'équipe de CyberDéfense est parvenue à exploiter les preuves récoltées, afin de prouver l'attaque menée par l'équipe de CyberAttaque et la capacité des systèmes mis en place à détecter ces types d'événements.

En effet, diverses traces de l'attaque ont pu être détectées et conservées par la sonde Snort mise en place, et par la suite utilisés par l'équipe de CyberDéfense pour constituer le rapport « *Forensic Report* » présent en annexe.

De ce fait, l'équipe CyberDéfense (Blue Team) a pu démontrer le bon fonctionnement de l'équipement de détection mis en place, et leur capacité à exploiter les preuves recueillies du 25 au 26 mai.

5.2 Problèmes rencontrés

5.2.1 Problème matériel

L'infrastructure Goatline dépend de quatre matériels identifiés comme critiques :

- 2x Serveur de virtualisation
- 2x Routeur Unifi Dream Machine Pro

En cas d'indisponibilité d'un de ces matériels, un site voir les deux sites de l'entreprise deviennent injoignables. Ainsi, ce souci a été rencontré durant le projet à date du 16 avril 2024 avec l'Unifi Dream Machine Pro du site d'Arthur Guilet.

Conséquence

La conséquence de l'indisponibilité fut immédiate, nos services ne répondaient plus et l'infrastructure côté Arthur Guilet n'avait plus internet.

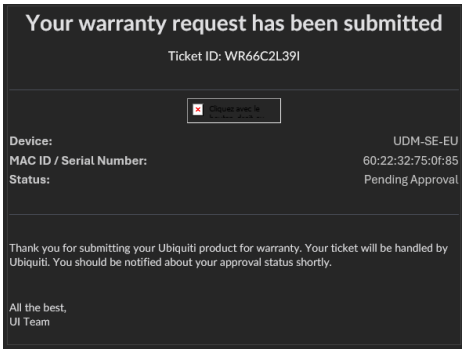
Cause

Après de multiples investigations sur la panne, notre équipe infrastructure a déduit que la panne provenait de l'Unifi Dream Machine. De plus, après plusieurs essais de réinitialisation en vain, la console ne redémarrait simplement plus, laissant supposer une panne matérielle.

Solution / Décision

Après une demi-journée d'enquête, une demande au RMA de chez Unifi a été déposée afin d'obtenir un matériel de remplacement.

contact@arthur-guilet.fr



Malheureusement, le déploiement de l'infrastructure était en cours et a donc été impacté. Fort heureusement, Unifi a été réactif et une console de remplacement nous a été envoyée le 25 avril. En parallèle, les équipes ont pu continuer de travailler en mode dégradé.

La partie infrastructure a finalisé le déploiement sur un site puis a préparé au maximum le déploiement du second afin que dès la réception du nouveau matériel, l'infrastructure soit finalisée. La partie cyber quant à elle a pu avancer sur les étapes préliminaires.

5.2.2 Manque de matière pour l'analyse forensique

À l'origine, nous avions prévu que la phase d'attaque laisse un grand nombre de preuves, y compris sur les disques des machines avec des téléchargements, exécutions de programmes malveillants ou autres manipulations qui auraient été effectuées par l'équipe d'Attaque ; néanmoins, lors de la phase de forensique, nous avions beaucoup moins de matière que prévu à analyser.

Conséquence

La phase de forensique devait initialement se décomposer en deux parties :

- L'analyse des alertes générées par la sonde, qui permettrait de localiser les machines impactées par l'attaque.
- Utiliser l'outil Autopsy afin d'investiguer sur les preuves présentes dans les disques de ces machines.

Néanmoins, le manque de matière a contraint l'analyse forensique à se centrer uniquement sur l'exploitation des alertes générées par la sonde réseau, car aucune preuve supplémentaire n'était présente sur les disques des machines répertoriées dans les alertes.

Cause

La cause de ce problème découle de la phase d'attaque. En effet, nous étions conscients que la phase d'attaque serait une tâche difficile, étant donné le respect des bonnes pratiques durant le déploiement de l'infrastructure. Néanmoins, les seuls moyens de pénétration ayant fonctionné pour l'équipe d'attaque sont des méthodes permettant d'obtenir des mots de passes pour ensuite obtenir des accès

contact@arthur-guilet.fr

sur les machines. Ce qui ne crée aucune interaction avec le disque des machines attaquées, et donc ne laisse aucune preuve à exploiter par un logiciel de forensique.

Solution / Décision

Lorsque nous avons rencontré ce problème, afin de conserver le plus possible l'aspect réaliste du projet, nous avons pris la décision de ne pas apporter d'aide supplémentaire à l'équipe CyberAttaque, et d'effectuer l'analyse forensique avec les alertes et le trafic réseau enregistré seulement, en démontrant tout de même la capacité de l'équipe Blue Team à utiliser un logiciel d'analyse forensique en expliquant son utilisation théorique dans le « *Forensic Report* »

5.3 Leçons apprises – Retour d'expérience

5.3.1 Partie technique

D'un point de vue exclusivement technique, ce projet a permis à l'ensemble de notre équipe de juger nos compétences dans la construction, l'attaque, la défense et l'enquête d'une infrastructure informatique complète.

Ce projet a permis notre entreprise de nous rendre compte que les équipes internes du pôle CyberAttaque auraient eu besoin de plus de formations et de bagages dans le domaine de la CyberAttaque afin de remplir les attentes initiales de la phase de pentest du projet.

Au terme du projet, Hugo de Marco a pu soulever un réel intérêt dans le domaine de la cyberdéfense, et dans les missions de regroupement et d'exploitation de preuves de cyberAttaque.

Swann Capé a pu être sensibilisé à l'importance d'être méfiant lorsque des informations sensibles sont mises à notre disposition et nous sont demandées par des personnes tierces.

Antoine ENGASSER a compris, que l'autonomie et l'initiative son maître-mot dans un projet de groupe. Il a découvert une passion pour le monde du pentesting, et souhaite se développer davantage dans ce domaine.

Erwan CLOUX a approfondie ses connaissances en DevOps, et a permit la création d'une base réutilisable de déploiement de machines afin de faire évoluer les infrastructures futures plus facilement.

Arthur GUILET a pu mettre en pratique ses compétences pour la conception complexe d'une infrastructure d'entreprise, tant sur le plan système que sur le plan réseau. Il a pris conscience des difficultés organisationnelles d'un projet d'envergure avec une petite équipe.

5.3.2 Partie management

D'un point de vue managérial, ce projet nous a appris l'importance de définir des rôles précis au sein d'une équipe projet, mais également de faire des réunions de point régulièrement. Ce qui nous a

contact@arthur-guilet.fr

permis de nous rendre compte que les enjeux, la direction et la vision globale du projet n'étaient pas les mêmes selon les différents acteurs du projet.

Nous avons donc pris conscience de l'importance de s'attarder sur la phase de planification du projet, afin d'organiser notre projet selon la meilleure méthode de management correspondante ; permettant à toutes les parties du projet de partager le même niveau d'information et d'avancer dans une même direction conforme aux attentes du projet.

6. Annexes

- Technical architecture document (DAT)
- IT Topology
- Documentation on Packer and Terraform
- Rules of Engagement (ROE)
- Calendar
- Salarial costs
- Documentation on Snort
- Pentest Report
- Forensic Report
- Cahier des charges Goatline

contact@arthur-guilet.fr