EPITECH 2022
Leo Smith
2nd Year Internship

INTERNSHIP REPORT

AF 2018

Computer security support intern.

Content

PART 1 :

THE CONTEXT

The context:

1. The Company

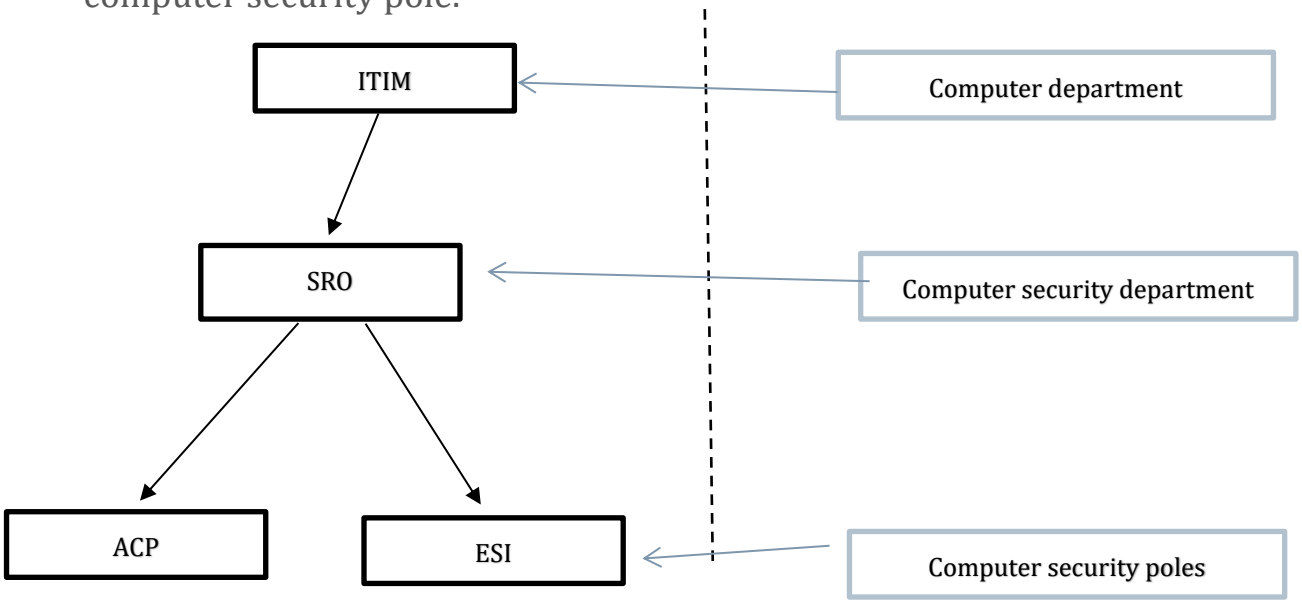
The company I was employed at is the Societe Generale. Owned by frederic oudea. It is one of the oldest banks in france, it owns a lot of banks all around the world and in France. The focus of the company is working with people and working towords a better world. This mentality is reflected with the companys catch sentence: the future is you. During my internship I was located at the dunnes. The dunnes is the head campus for the IT depertament of the Societe Generale. It is constituted of 5 buildings a canteen and break rooms. Each building of the dunnes is a departement of IT pole of the Societe Generale. The building I was at is the computer security departement building, it has 7 stores with 3 stair cases. Every store has a canteen fitted with a vending machine. The venting machines are verry cheap, you can buy coke and other food in them. Next to the vending machines there is a table football table where you can play with your colleagues. To get into the dunnes you have a card to prevent strangers getting in the building. There also are coffee shops inside of the campus where you can go on a break. They also include a rest room where you can sleep and take a break when you need to. There also is a canteen that is discounted for the people that work with the Societe Generale it has 5 different menus that change everyday to keep the employees fit. There also is a fitness room for the employees so that the morning they can do their fitness. The campus is located next to a train station wich helps the employees come early and it's enviromental friendly to avoid traffic jams.

2. The company's activities

The Societe Generale principal activity is banking, the societe generale owns a lot of different bank (Credit du Nord, Boursorama Bank, …) and owns a lot of the banking market internationally. It is also known for it's inovation inside of the computer thechnology and information field, it is a company that is ranked number one for digital maturaty and keeps up to date on the new technologies (computer security, cloud, blockchain, …). The Societe General also offer courses to learn about the different jobs they offer so that they stay cuting edge technology wise.

3. The company's organization

The Societe Generale is organised in different poles each with there specialities, (blockchain, cloud, security assessment, pentesting, ….). The computer security departement where I worked at was organised in a special way, it had two magor poles: the security assessement pole and the pentest expert pole. These two poles are united une the computer security pole of the Societe Generale and is linked with administration of the computer security pole.



- Computer departement:

The computer departement so called ITIM inside of the company, ITIM is an acronym for: Innovation, Technologies et Information pour les Metiers (aka: Innovation, Technology for Information for the Jobs). ITIM is the main departement inside of the company for all the computer science jobs.

- Computer security departement:

The computer security departement also called SRO for Sécurité Risk Opérationnel (aka: Security and Risk Assessment). Is the only departement that help projects get a full risk assessment.

- Computer security poles:

The computer security poles is the division of the computer security departement and is divided in two poles. The first pole is called ACP that is an accronym for: Accompanement Projet (aka: Project Assessment). This pole is the one that orchestrates risk assessment on project and it works hand in hand with ESI that is an accronym for: Expertise Sécurité Intrusion (aka: Expert and Pentesting). This second pole ESI is the one that helps out ACP to do risk assessment, ESI gives more technical assessments on projects.

4. My place in the company

At the Société Générale, I was placed in the security assessment pole but because I have pentesting skills my internship suporvisor allowed me to also work with the pentesting pole so that they could use me at my full potential. I spent my internship going through both of the poles completing different mission and helping out my colleagues with my technical knowledge for the

security assessment pole and with my newly aquired security assessment skills for the pentesting pole. By travelling throught the different areas of the company I was able to have a really good understanding of a typical computer security team and how they are organized inside of a company. I was also able to branch out of the computer security departement and discover other poles like the cyber defence or programming pole. By beeing able to branch out I also discovered other jobs and skills I could learn. I spent thow most of my internship inside of the computer security assessment pole because most of my missions was located there I was on the fourth flour of the computer security building.

PART 2 :

MY MISSION

My mission:

1. My integration

My integration to the company was orchestrated for one month that my internship supervisor named the incubation phase. During my incubation phase I started discovering the organization of the company and how each group worked in correlation with each other. To organize my integration, I realized a roadmap so that I could keep track of what I did and what I had to do (see *image 1*). During the first two weeks of my incubation phase, I presented myself to the entire department and had a meeting with every employee I had to work with so that they could present me their job and what they were currently working on. I therefor discovered that inside of the computer security business there where two types of employee, the internal and external ones. Internal employees are hired directly by the firm and have different job possibilities, Analyst or Correspondent, for security assistance and pen-tester or expert for the pentesting pole. Analysts evaluate the risk of an application and how certain technologies are dangerous with the security of the application. Correspondents do the communication between the owner of the application and the analysts that are more tech-savvy. The pen-tester are the employees that will do the technical research on pointy vulnerabilities in an application and the experts are the ones that know well a field, they help analyst do their work easier by explaining how certain technologies create security loop holes inside of an application because it is not using the appropriate software.

Axe	Action à traiter	Objet	Statut	Doc	Aspect
...	[S-07] - Découverte de l'équipe CERT	Discussion		N/A	
...	[S-07] - Découverte de l'équipe SOC	Discussion		N/A	
SRO / ACP	[S-01] - Apprentissage de la norme DSP2	Etude de documents		docs/Directive_des_services_des_paiements.docx	
SRO / ACP	[S-01] - Apprentissage de la norme ISO 27005	Etude de documents		https://fr.wikipedia.org/wiki/ISO/CEI_27005	
SRO / ESI	[S-01] - Découverte des différents pentest	Discussion		docs/mettier_pentest.docx	
SRO / OPS	[S-01] - Découverte du pole EFRAUDE	Discussion		docs/sécurité_des_opérations.docx	
SRO / ACP	[S-01] - Rdv avec un analyste	Réunion		docs/Securite_dans_les_projets_et_expertise.docx	
SRO / ACP	[S-01] - Rdv avec un correspondants	Réunion		docs/Securite_dans_les_projets_et_expertise.docx	
SRO / ESI	[S-01] - Rdv avec un pentester	Réunion		docs/Securite_dans_les_projets_et_expertise.docx	
SPX	[S-01] - Rdv PMO Guichet	Réunion		docs/delevery_management_guichet.docx	
SRO / ESI	[S-02] - Cours audit de code	Découverte		docs/audit_de_code.docx	
SRO / ESI	[S-02] - cours d'audit de code	Formation		tutoriels/2017 - Présentation de l'offre Audit de Code.ppt	
SPX	[S-02] - Création doc PMO Guichet	Etude de documents		docs/delevery_management_guichet.docx	
SRO / ESI	[S-02] - Etude des vulnérabilité web	Formation	63%	https://www.root-me.org/fr/Challenges/Web-Client/	Incubation
SRO / ACP	[S-02] - étude GDPR	Etude de documents		tutoriels/GDPR Présentation _V1.0.ppt	
SRO / ACP	[S-02] - étude Open banking	Etude de documents		docs/open_banking.docx ; https://fr.wikipedia.org/wiki/Open_banking	
SRO / ESI	[S-02] - Rédaction du doc sur les failles XSS	Rédaction		docs/xss.docx	
SRO / ACP	[S-03] - Actualisation de la plaquette RTI	Rédaction		N/A	
Stage	[S-03] - Préparation road map générale	Excel		roadmap_stage_leo_smith.xlsx	
SRO / ACP	[S-03] - Présentation de l'organisation de ACP	Réunion		In OneNote	
SRO / ACP	[S-03] - Prise du point pour plaquette RTI	Prise de Réunion		26/09/2018 - 16h à 16h30	
Stage	[S-03] - Rédaction roadmap générale ACP	Excel		roadmap_stage_leo_smith.xlsx	
Stage	[S-03] - Rédaction roadmap générale ESI	Excel		roadmap_stage_leo_smith.xlsx	
SRO / ICI	[S-03] - Rencontre avec pole incident contrôle interne	Réunion		docs/Securite_dans_les_projets_et_expertise.docx	
SRO / ESI	[S-03] - Rencontre expert ESI	Réunion		docs/Securite_dans_les_projets_et_expertise.docx	
SRO / ESI / ACP	[S-04] - Finalisation de la plaquette RTI	plaquette		plaquette RTI.pdf	
SRO / ESI / ACP	[S-04] - mise à jour de la plaquette RTI	plaquette		plaquette_rti.docx	
SRO / ACP	[S-04] - Réalisation de la plaquette petit dej ACP	plaquette		carte_petit_dej.pdf	
Stage	[S-04] - Rédaction roadmap détaillé ACP	Excel		roadmap_stage_leo_smith.xlsx	
Stage	[S-04] - Rédaction roadmap détaillé bis	Excel		roadmap_stage_leo_smith.xlsx	
Stage	[S-04] - Rédaction roadmap détaillé ESI	Excel		roadmap_stage_leo_smith.xlsx	
Stage	[S-04] - Rédaction roadmap générale bis	Excel		roadmap_stage_leo_smith.xlsx	
SRO	[S-04] -MOOC Ansii	MOOC	88%	https://secnumacademie.gouv.fr	
SRO / ACP	[S-05] - Découverte du ds light	Réunion		N/A	
SRO / ACP	[S-05] - Rédaction doc analyse flash et RRO	Rédaction		docs/Analyse flash.docx	
SRO / ACP	[S-05] - Réunion découverte analyse flash	Réunion		N/A	
SRO / ACP	[S-05] - Réunion découverte Ques-RO	Réunion		N/A	
SRO / ACP	[S-05] - Réunion font de panier	Réunion		N/A	
SRO / ACP	[S-06] - Découverte du ASA	Réunion		N/A	
SRO / ACP	[S-06] - Foire Agile	Présentation		N/A	
SRO / ACP	[S-06] - Participation grille d'éligibilité	Réunion		N/A	
SRO / ESI	[S-06] - Point analye IAM	Réunion		mois2 / Analyse IAM	
SRO / ACP	[S-06] - Réunion font de panier	Réunion		N/A	
SRO / ACP	[S-07] - Réunion font de panier	Réunion		N/A	
SRO /ESI	[S-07] - Completion slide shema	Réunion		mois2 / Analyse IAM	
SRO / ACP	[S-07] - Cours ISO 27005	Etude de video		docs/iso27005.md	ACP - ESI
SRO / ACP	[S-07] - Point ASA, apprentisage du ASA	Réunion		N/A	
SRO / ACP	[S-08] - terminé Cours ISO 27005	Etude de video		docs/iso27005.md	
SRO / ESI	[S-08] - XSS réfléshi	Etude de faille informatique		root-me.org	
SRO / ESI	[S-09] - DVWA	Etude de faille informatique		http://dvwa.co.uk	
SRO/ACP	[S-09] - Plaquette RTI remise en forme	plaquette		plaquette_rti/plaquette_rti_11-18	
SRO/ACP	[S-09] - Plaquette RTI changement de la mise en page	plaquette		plaquette_rti/plaquette_rti_11-18_landscape	
SRO/ESI	[S-09] - Cours ROP	Cours		N/A	
SRO/ACP	[S-09] - Annimation fond de panier	Animation Réu		N/A	
SRO/ESI	[S-09] - point WHATS	WHATS		Analyse IAM/Grille_de_validation_WHATS_ITIM_2018_2	
SRO/ESI	[S-09] - point WHATS	WHATS		Analyse IAM/Grille_de_validation_WHATS_ITIM_2018_2	
SRO/ESI	[S-09] - point WHATS	WHATS		Analyse IAM/Grille_de_validation_WHATS_ITIM_2018_2	
SRO/ESI	[S-09] - Creation doc Processus de validation	WHATS		Analyse IAM/Processus_de_validation_SSI_de_la_creation_des_rôles_WHATS_08_11	
SRO/ESI	[S-10] - Refaite de la plaquette rti	plaquette		plaquette_rti/plaquette_rti_11-18_landscape	
SRO/ACP	[S-10] - Travail ASA	Découverte		N/A	
SRO/ESI	[S-10] - checkmarx	Découverte		plaquette_rti/plaquette_rti_11-18_landscape	
SRO/ACP	[S-10] - Réunion plaquette RTI	Découverte		plaquette_rti/plaquette_rti_11-18_landscape	
SRO/ESI	[S-10] - Attelier WHATS	WHATS		WHATS/	

image 1

After the two weeks of discovering the two major poles I would be working with my internship supervisor, he made me discover the other area of expertise the company had so I met different type of people: software developers, cyber defense experts. This gave me a clear image of how a

corporate business worked and what kind of job exists in cyber security. I was instructed to organize meetings with cyber defense experts and learned the different kind of attack a bank is under on a day to day basis. During my incubation phase I also had the chance of having a few computer security exercises so that I could update my technical skills. I had the help of the pentesting team so that every time I got stuck on an exercise, they help me complete them. They also gave me advices on what I should research and learn next so that when I start working full-time, I would be able to be as efficient as I wish to be. To finish my integration phase my internship supervisor gave me an online course to follow so that I was able to understand more the security assessment side and the different laws that they have to take in count to secure the information of their clients. My integration phase was very enriching and helped me be very motivated to work inside of the company. I was able to learn a lot about the company in a really short period of time and the knowledge I learned during that phase helped me a lot throughout my entire internship.

2. My mission with the security assessment pole

In the security assessment pole, I had two major mission, the first one was writing a document on how to use the code audit software (see *image 2*). To be able to write this paper I had to have a course on how worked the software, so I began by organizing meetings with me and the code audit expert of the company. He sat me through how the software worked and how a regular code audit is realized. After explaining me how it worked, he then realized a code audit in front of me so that I could grasp the idea of how a code audit was requested and how it was processed. After those lessons, I started working on a new version of the code audit tutorial document. That document is created so that the application owner could have a more

detailed explanation on where the security flaws are in their application. For that task, I was assigned to a college of the security assessment group and we worked hand in hand on updating the document so that it fit the company's needs. We had to go to meetings together and revise the paper a lot of times because the owner of the paper did not know how he wanted the paper to look like, so we had to work on different versions of it with different styles. We produced two paper I helped out on the design of the paper and the content of it and my colleague searched the information I had to put in the document and organized all of the meetings.

QU'EST CE QUE C'EST ?

Checkmarx est un outil d'audit de code permettant de réaliser une analyse syntaxique et contextuelle à la recherche de vulnérabilités. Il est accessible via l'authentification SESAME. Checkmarx est incorporé dans la plate-forme DEVOPS.

QUE M'APPORTE CETTE SOLUTION ?

Destinée aux développeurs au sein d'ITIM, il permet de :

5. Détecter des vulnérabilités potentielles dans le code source des projets.
6. Remédier aux vulnérabilités au plus tôt dans le cycle de fabrication de l'application.
7. Indiquer le meilleur endroit où appliquer la mesure correctrice afin de remédier à un maximum de vulnérabilités en une fois.

PRÉ-REQUIS

1. Le code source est la propriété de la Société Générale.
2. Le code source doit être mis à disposition sur la plate-forme Checkmarx
3. Une demande d'habilitation doit être faites par votre RDA dans OSMA.

CHECKMARX

Comment l'utiliser ?

| AUDIT DE CODE AVEC CHECKMARX | AJOUTER DES PROJETS A CHECKMARX | COMPREHENSION DES FAILLES A CORRIGER |

UN COMPILED SOURCE CODE SCANNING
REMEDIATION ADVICE
ATTACK VECTOR EXPLANATION
BEST FIX LOCATION
1
2
3
4

L'INTERFACE

1. Les catégories de vulnérabilités
2. La liste des vulnérabilités
3. Le vecteur d'attaque
4. Le code source

MODE D'INTEGRATION

L'ajout de projet à Checkmarx est d'un coût de 2J/H qui est utilisé pour un onboarding de l'application. A noter qu'il y a aussi un mode où l'audit est totalement réalisé par ESI : c'est le mode one shot (7J/H).

LIENS UTILES

https://sbc.safe.socgen/groups/itim-securite-maitrise-d-oeuvre
https://spice.socgen/CxWebClient/

CONTACT

Itim-audit-rti.fr@socgen.com

COMMENT ÇA MARCHE ?

- Pour accéder à l'outil Checkmarx, aller sur ; https://spice.socgen/CxWebClient
- Après habilitation, renseigner son Login et son Mot de passe. Puis dans « Options », choisir SESAME.
- Après connexion, la liste des projets associés au compte s'affiche. Cliquer sur le nom du projet pour afficher son état.

FAIRE UNE DEMANDE D'AUDIT DE CODE

Pour auditer votre application, adressez une demande d'habilitation via OSMA puis une demande d'audit via la boîte mail : itim-audit-rti.fr@socgen.com. NB : Ajouter à l'objet du mail : [Checkmarx] demande d'audit d'application.

Corps du mail : Bonjour,
Nous voudrons intégrer notre appli à l'audit avec une intégration [nom du mode d'intégration].

FONCTIONNEMENT DE L'AUDIT

Scans — Intégration du projet dans CheckMarx et lancement des scans périodiques.
Analyses — Les développeurs analysent les résultats avec une assistance ESI.
Corrections — Les développeurs appliquent les corrections avec une assistance ESI.
Restitution — ESI réalise une restitution technique avant la mise en homologation.

C'EST VOUS L'AVENIR SOCIETE GENERALE
ITIM SRO
Crédit du Nord

Image 2

The second mission I had to work on was to create a document to realize security assessment on an application. The document groups different security assessment documents so that when the owner of the application receives it, he would have a resume of the entire security assessment in one document. This document has also built-in functionalities so that an analyst who is doing the security assessment, knows how deep in the assessment he must do for the application. The other major built-in functionality of this document it's his categorization of every risk the analyst finds so that it can be saved in a database to automate future risk assessment. For this second mission I was placed alone but was helped by my colleagues that work with the risk assessments administration. They organized me meetings to explain me how risks are stored inside of there database and how I should categorize them. I also had my internship supervisor checking on me with several meetings to give me directives on how to write the paper. He explained me the needs that I had to understand to write the paper. Those two missions allowed me to learn new security assessment skills and to work on my technical security skills. The code audit paper mission was one of the easiest missions I did and the risk assessment mission was the hardest but the most interesting because it was very enriching for my experience in security assessment.

3. My mission with pen-testing pole

With the pentesting pole I had only one mission but was perpetrated during the entire internship. My mission was to write paper algorithms (see *image 3*) so that the administration of the computer security department can give role to the developers and application owner on there testing servers. These different algorithms are supposed to determine if a role should be given to a user in the environment of the application. It helps secure the company and

the information of their clients so that if an attacker decides to attack them, they can react accordingly and protect as much the entry points of an application. Certain roles already had their algorithms explained in paragraphs, so I just had to represent them but others where not complete, so I had to organize a few meetings to understand the different roles and how they work. After writing the paper algorithms for the administration I had to go to different workshops to teach the administration on how to use the algorithms and tell them how to give the different roles. The administration is not based in France, so we had to do a lot of skype calls and we had to write a document explaining how the roles work and how the interface of the role giving application works. For this mission I worked hand in hand with the head of the administration and an employee that used to be the one giving roles to their clients. This mission was really interesting and made me learn how roles where given inside a corporate company and what where the different roles one could have as a developer or an application owner to maintain an application inside of its different phase of creation.

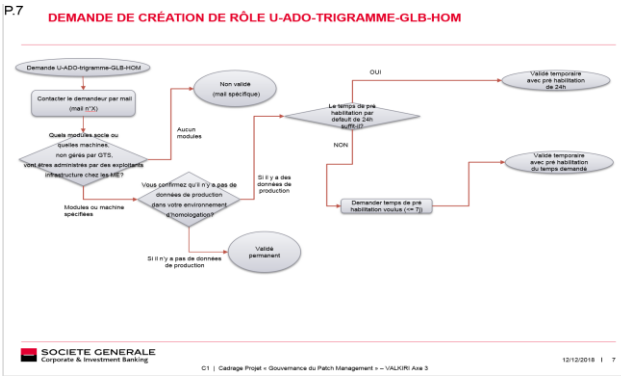


Image 3

PART 3:

THE ACCOMPLISHEMENT OF MY MISSION

The accomplishment of my mission:

1. My integration

Like said forehand my integration was done in the span of one month and was named the incubation phase. I discovered the company and how it was organized. I was able to go around all of the company visiting most of the departments and discovering how everything worked.

a. It's facilities

Integrating the company was easy thanks to all of the support everyone gave me, I was able to discover by myself every area of the industry and that was very enriching for me. I also had help from other interns who showed me their departments and field of expertise. It also was an easy process to meet every employee thanks to my newly developed social skills. In the span of one month I had a perfect picture of the company. After visiting the entire department, I was at I gave myself the task of writing documents about every department I visited, writing those papers where very easy and was simplified by the meetings I attended to that explained me every part of the company. I was able to create on the intranet a smaller scaled roadmap that represented my integration so that every other intern after me could discover the company a lot more easily.

b. It's difficulties

The main difficulty of my integration was setting up meetings with every employee and finding the courage to meet everyone inside of the company. I found it very difficult to understand every acronym inside of the company and I had to write different reports and definitions for every acronym and area inside of my internship. I was able to tackle these difficulties with the help of meetings and resources to meet and understand

the company. I also had a lot of meetings with my internship supervisor that gave me tips to organize myself during the internship. It was also very difficult to organize myself at the beginning because I did not know where to start inside of the company and where to go, so my internship supervisor gave me different documents explaining the department I was located in and how they worked hand in hand together. With help of that document I was able to create a small roadmap for my integration phase and branch out to every other department so that I could have a better picture of the company. I also struggled with understanding the different fields inside of the company and how their jobs where realized and to understand this better I was helped by my colleagues that have a lot more experience than I have inside of their jobs.

2. My mission with the security assessment pole

Inside of the security assessment pole I had two principal missions, like said forehand the first one was creating a tutorial paper for the audit code platform named checkmarx. The second mission was creating a security assessment paper that resume every security assessment paper that the security assessment pole uses.

a. It's facilities

Writing the paper for code audit was facilitated by the support I had from older code audit papers and the help from the employees inside of the pentesting pole that realize the code audits. Having a lot of experience in code helped me a lot for this task because I was able to understand how the software worked really easily because it replicates how a human audit a piece of code. It was also facilitated by the patterns the application showed us inside of the code so that we could understand better it's logic. For the security assessment paper, I

had a few analysts explaining me how most security assessment paper work and how I could use that to model the paper I had to write. It was very straight forward to understand the different modes of security assessment depending on how critical the vulnerabilities where. Writing down the different information's for the application owner was very easy because most of the information needed where already written in other documents so I had to go through all of them and rewrite them to fit the needs of the new paper. It was also pretty easy to write the data for the administration because after all of the meetings with them an employee helped me out by giving me all of the information needed and I framed them inside of an excel sheet.

b. It's difficulties

Understanding the code audit software was difficult so I had to organize a few meetings to understand the software properly and how a code audit is orchestrated. I also struggled with finding the resource on the intranet and search through a lot of paper work about their code audit software. For the security assessment document, I had to understand the parts that created a security assessment document and how they worked hand in hand together to create a full summary about them. I also had to understand how they categorized risk and stored it. To combat that difficulty, I organized meetings with the administration of the security assessment pole and worked hand in hand with them to complete the security assessment document. Working with the security assessment pole administration pole was also complicated because there are based outside of France so I had to be aware of the time difference.

3. My mission with the pentesting pole

With the pentesting pole I had a very important mission, writing algorithms to automate the process of role giving inside of the company. So that it was firmer on who had which role inside of the company. It was a simple mission to execute but hard to understand. This mission was perpetrated during the third month of my internship.

a. It's facilities

Writing the algorithms was a straight forward process. I already had experience in writing algorithms for humans to understand, and most processes for each role where explained to me forehand. To write the algorithms I used very simple drawings that where easy to picture inside of my head and the head of others. I was able to draw them easily with the help of a few tools that where given to me by the chief of the role giving, most of the algorithms logic where written forehand and I just had to figure out how to draw them but some had some missing information so I had to understand thoroughly the process of role giving to write them. It was also very easy to explain to the administration on how to execute the process of giving a role to a user and it was very interesting to animate meetings with the administration to give them directives on how to give roles to users. I also had to show them the different interfaces where they could find the different roles to process them and how they accept to give a role or not.

b. It's difficulties

Understanding the roles inside of the company was a tedious task for me and I had to organize a lot of meetings so that my mission manager could correct me on the algorithms I wrote. It took me a lot of time to understand how every role worked hand in hand with each other

inside of the company and how they where given to the users. The other difficulty during this mission that we encountered was to explain how the role system worked to the people we were giving the algorithms to. Explaining the interface of the role giving application was also complicated because the application is not very maintained and has a lot of bugs so explaining its functions is complicated. The other difficulty was that my manager for this mission had a lot of new directives coming while we were working on it, so she had to leave me a lot on my own, so I had to figure out how the roles worked on my own with the research I did.

CONCLUSION

Conclusion:

1. What did I learn about the industry?

During my internship I discovered the computer security industry and how it worked. The computer security industry has a very special way of working, inside of every major company there are two types of employee, internal and external employees. Internal employees have been hired directly by the company and usually have the most important jobs inside of the company and the external employee work for a special firm that is a partner of the company. The external employee usually occupies the entry jobs inside of the computer security field. I also had the luck of meeting other jobs inside of the industry and how computer security is divided. Computer security is divided in three major domains, Internal security, External security and Application security. Internal security also called CERT (aka: Computer Emergency Response Team), is the department that looks after the internal security of the firm. They handle all of the monitoring of the network and most data security inside of the company. The Internal security has a special team named the blue team that work on creating the best defense for the company. External security is the department that looks after all of the external security threats. Their job is to research how the attackers got inside of their information system and help the Internal security team to protect the company better. The external security also has a team of experts named the red team. The job of the red team is to create attacks to the company to test their defense mechanisms. For the application security field, that is where I did my internship, they take care of testing every application the company need so that an attacker can not use an application of the firm to turn it against them. Usually all those fields in the industry are interchangeable and computer security experts have experience in all three of them.

2. What skills did I learn?

During my internship I was able to exercise many skills, I first started by working on my social skills by engaging with the teams I had to work with by presenting myself and discovering what they did inside of the company. With the meeting I organized I was also able to gather information about each field that was exercised inside of the company so that I could write different documents to learn my redaction skills. After gathering as much information as possible and being social I used those new skills to learn about the different field inside of the company. I started by organizing one on one meetings with every analyst so that they could explain to me every skill I had to know about their job and what I had to work with. During each meeting I picked a risk analysis document so that we could go through it together so that they could teach me on how they would proceed in completing one and how I could also by replicating their actions write one myself. I then organized one on one meetings with every correspondent, in the same style as the meetings with the analyst, they explained to me the different skills of their jobs and how they would go through a risk assessment. With all of that new knowledge acquired I started writing papers on the intranet of the company on how each field worked and started learning by myself every bit I had to know. After learning the different field inside of the risk assessment department, I then moved to the pentesting pole, there I organized a meeting with the chief of the code audit department so that he could teach me on how to do a code audit, after that meeting I also wrote a document on how a code audit is orchestrated. I also went around the pentesting pole asking advices to the team on how to do a correct pentest inside of a company, this was part of a personal goal I gave myself before arriving at the internship because I am extremely interested on how pentesting are realized.

3. What did I bring to the company?

During my Internship I was a polite and happy intern. I believe that I brought happiness and positive energy to the company. I also helped my colleagues in completing some crucial task inside of the company. Like said forehand I helped them create a document explaining the orchestration of a code audit and how to demand a code audit on your software, I also helped the company write a complex risk assessment document that resumes most risk assessment documents and automate the process of categorizing the different risks and how to solve them inside of their database. I also brought a new method of automation for role definition inside of application servers for the developers. Being inside of a corporate company made me learn a lot about the industry and having a new employee with very few experiences about the corporate world gave my colleagues a challenge on how they could work with me knowing that I didn't know much. Because of my past experiences in freelance it was very interesting for them to understand my point of view with clients. Even though it was inside of the same company I saw that the people asking for risk assessments acted exactly how a client would act like outside of a company and I was able to give advice to some of my colleague on how to deal with more complicated clients inside of the company. I also was able to give my technical expertise inside of computer security and computer architecture to a few employees to help them complete their risk assessments and to give them an external view of there risk assessments.

Acknowledgement:

I would like to thank my internship supervisor who was very patient with me and helped me during my internship by giving me missions and guiding me through the inner-working of the company and allowed me to freely navigate through every department of the computer security pole of the company. I would also like to thank the Societe Generale who allowed me to discover the company and trusted me in being a good intern. I also would like to thank the security assessment and pentesting teams who welcomed me inside of their team and helped me with the missions I had to complete inside of the department. I also wish to thank the school who allowed me to do this internship. I learned a lot during this internship between my social and security assessment skills and discovered a lot about this industry that I always wished to work in.