LOGIN SÉCURITÉ

INTERNSHIP REPORT

SITPI RAJENDRAN - EPITECH 2023

1st of APRIL 2021
31st of JULY 2021

ACKNOWLEDGEMENTS

First, I want to thank my teachers at “L’École pour l’informatique et les nouvelles technologies” also known as, EPITECH. Especially, to my teaching assistants, Mr. Emeric CARAMANNA and Mr. Joffrey RIELA, to their listening and the sharing of their experience.

I would also like to thank, M Antoine Patois, CEO and President of Login Securité, and Guillaume BUFFIER, COO and my internship supervisor, who have given me their trust, supported me throughout my different missions, and were able to give me good pieces of advice in my personal and professional development.

I would like to thank all the Login Securité team, for their welcome, and their cooperation. In particular, Lo*** MA*****, my project teammate and former student of EPITECH

LOGIN SÉCURITÉ

SECTION ONE

INTERNSHIP REPORT
SITPI RAJENDRAN - EPITECH 2023

SUMMARY

IMPORTANT INFORMATION'S

STUDENT

Sitpi RAJENDRAN
sitpi-kevin.rajendran@epitech.eu

SCHOOL

EPITECH Paris – Promotion 2023

DURATION

4 Months

1st of April 2021 – 31st of July 2021

COMPANY

Login Sécurité

INTERNSHIP SUPERVISOR

Guillaume BUFFIER – COO of Login Sécurité

INTRODUCTION

As part of my training at Epitech Paris, I was led to find an internship. This internship must be an experience of the professional world. Moreover, it seemed rather interesting to me to look for an internship related to one of my pre-orientation wishes, namely the web development. Indeed, it is in this field that I wanted to do my internship in order to learn more about the web domain, and to diversify my knowledge in a different field than the one taught at Epitech.

With this objective in mind, I started my internship search at the beginning of February by sending unsolicited applications to more than a dozen companies as well as replies to offers that matched my profile on different platforms such as JobTeaser or Welcome to the Jungle for example. As I was working part-time at the time in the Constellation group, in its subsidiary Fabrick, I also asked my human resource managers to propose my profile to the group's subsidiaries. And that is how I learnt that the cybersecurity branch of the group, Login Sécurité, needed a frontend developer.

So, I contacted the technical director and asked him to interview me so that I could join his team. Being a novice in this field, nevertheless being interested in it, I chose to join Login Sécurité, first to improve myself at the UX/UI level, and at the front-end development level, but also to develop my knowledge about cybersecurity. Following this, the steps for the internship agreement were made fast, as HR already had all the information about me.

This internship has a duration of 4 months (it started on April 1, 2021, and it will end on July 31, 2021). It took place in the city of Saint-Cloud (92210) in the southwest of Paris. My supervisor was Mr Guillaume BUFFIER, Chief Operations Officer of Login Sécurité.

My internship was focused on one main axis: the UX/UI redesign of the "SecOps" platform.

II

THE COMPANY

A. ABOUT THE COMPANY

Login Securité, is a cyber-security company, this means that the company supports Chief Information Office, or IT Manager to define and establish their Digital Trust strategy by relying on two levers: Cybersecurity and the Network.

Created in 2005 by Antoine PATOIS and Pierre Alexandre VANDEWOESTYNE, this company grown alone before joining a group called Constellation in 2017. Nowadays, Login Security have 26 employees distributed in 4 offices in France: Paris (Saint-Cloud), Lyon, Nantes, and Lille. The company has a turnover of 3 million euros for the year 2020.

Our teams deliver consulting, integration, managed services, and training services, adapted to the constraints of our customers, on site or from our Cybersecurity center. The company offers 5 types of services, adapting as much as possible to the needs of its customers :

Advice and Governance

This is the part of the company that accelerates customer's ability to identify, prevent, detect, and respond to cybersecurity risks and to reduce reputational damage and financial loss against a cyberattack.

Audit and Intrusion test

Infrastructure and application vulnerabilities are one of the elements frequently identified in security incidents and constitute a high risk. That is why Login Securité proposes to implement a progress plan to reduce the technical risks of your critical applications.

Training and Awareness

Companies have realized that cyber security is no longer an option. Thus, Login offers companies the opportunity to learn and better understand the risks linked to IT security, the different types of attacks and to adopt the best practices to protect themselves.

Installation of security tools

This offer allows the implementation of security solutions for networks, applications, and accesses in order to reduce the possibilities of attacks and therefore the risks.

Operational safety

Having a Security Operations Centers (SOC) requires investments: technical means, human resources, and more. For this reason, Login Securité proposes to outsource this service in order to guarantee the continuity of your business activities by setting up a detection, reaction and decision support system.

B. COMPETING

The cybersecurity industry is booming, and new companies are joining every day. The seniority of Login allows to have a proof of the seriousness of the company during call for tender.

Most Login's customers come through word of mouth. That is why the design of the platforms to which the customers have access is an important point, since it represents the image of the company.

Moreover, the transversality of the group allows us to have customers from other subsidiaries, and therefore to have a shared customer base. This also requires a very good image so as not to damage the reputation of the whole organization.

C. ABOUT THE GROUP

Constellation is the group with 380 employees, which is behind Login Security. Composed of 8 subsidiaries:

- Novahé : their job is to optimize and make evolve clients'

- Dataxion : which is a huge datacenter with different technology combine in one place .

- Evea Cloud : they assess, design and managed open cloud architectures.

- EasyTeam : it's a company specialized in the Data and the Cloud.

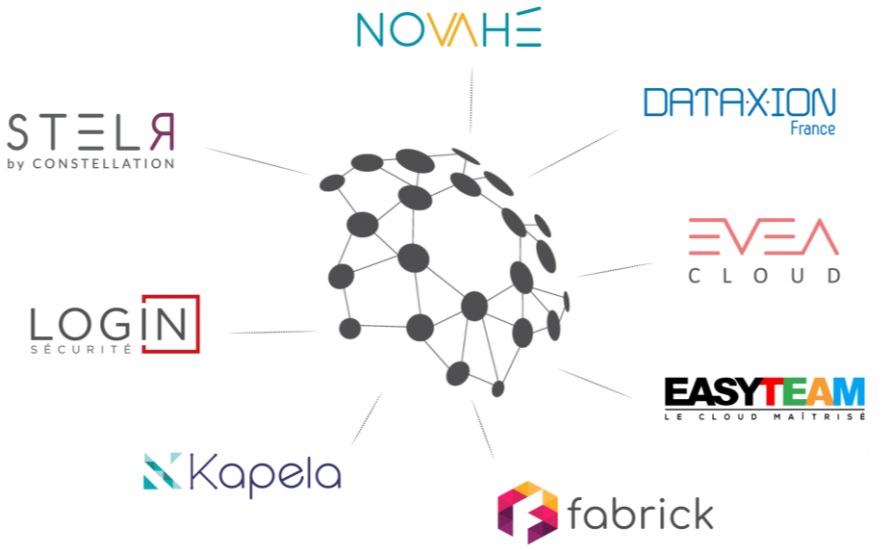
- Fabrick : Designs and creates modern and agile applications according to the DevOps methodology

- Kapela : they bring together our expertise in Business Intelligence, Big Data, Data Management and Artificial Intelligence.

- Login Securité: the cybersecurity company of the group, we provide operational responses in a risk management approach that creates long-term value for its customers.

- StelR : the IT consulting firm, it supports CIOs, and DGs, in the definition and operational implementation of their digital strategy.

The combination of all the subsidaries creates a synergy of skills in order to support their clients in each stage of their IT transformation projects. Constellation's mission is to meet the business challenges of its clients by implementing their digital transformation. Thanks to the different professions in the group, from consulting to development, to integration and outsourcing of agile IT solutions, this allows the group to offer a global IT support service.



Therefore, the group is present in 9 offices: Paris (Saint-Cloud), Trappes, Tours, Nantes, Orléans, Lille, Lyon, and two offices outside of Metropolitan France, one in the French West Indies, and another one in New Caledonia.

The group has set itself the goal of reaching €100 million of turnover by 2022. In fact, the target is close, with 550 customers, the proforma 2020 has reached 90 million euros in turnover.

III

MY MISSION

A. ABOUT THE PROJECT

All my internship was turned around a platform called “SecOps”. This website is the Security Center of Operations portal. It is a platform where there are all security problems gathered in the same place, making it easy for the customers to know where they can find all the information. Thus, the platform allows to:

- Manage all incidents, requests and problems related to information security.

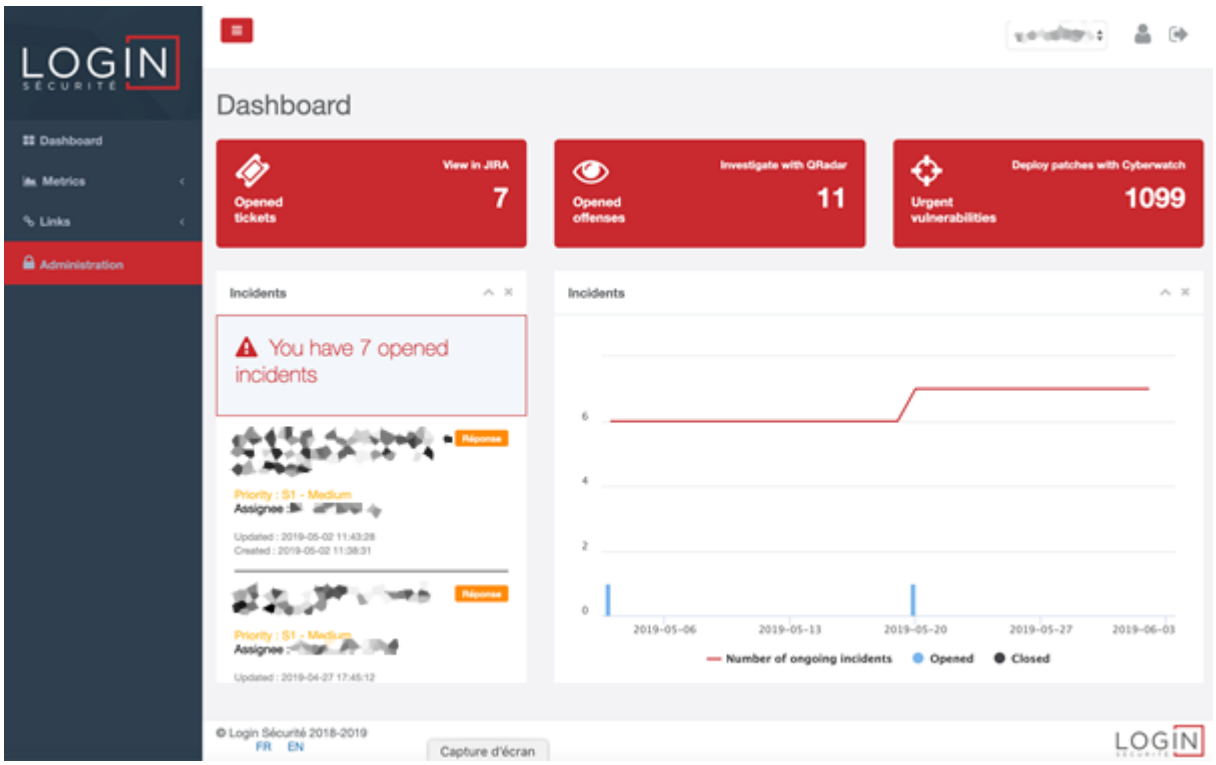
- Centralize all information related to an incident, including confidential data.

- Have a unified communication of action plans between the SOC teams and the client’s production teams.

- Centralize information from the various tools and services.

- Sharing of metric and provisions of trends with plenty of graphics and tools integrated to the platform.

The platform was created bit by bit, block by block, so there is a lack of visual consistency across the platform. Moreover, the latter used an old framework, Angular 6, which makes it very complicated to maintain.



OLD DESIGN OF THE WEBSITE

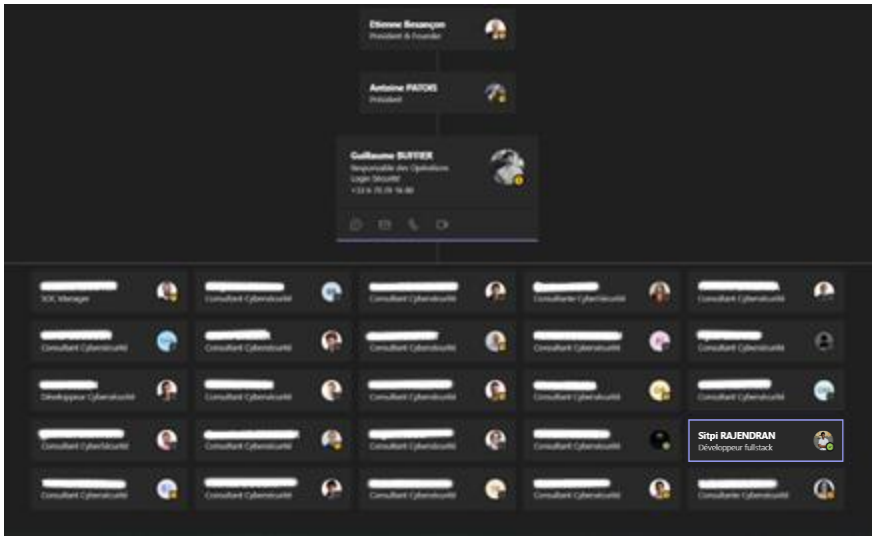
B. ORGANIZATION OF THE TEAM

During the whole internship, I worked in team with Lo*** MA*****, . He is a back-end developer. Then, when he was developing features, I needed to design them to make it as user friendly as possible. For this work I was not alone because, I worked with Ce**** BR******** from the Fabrick Team.

In order to facilitate our collaboration, we work together two days a week in the company's offices, on Tuesdays and Wednesdays. Indeed, every Wednesday, all employees must come on site and work on-site. This allows them to see all the team members, to eat together, and to meet each other. On Mondays, Thursdays, and Fridays, I work from home on those days. However, we talk a lot together to know more about each other's progress as well as each other's opinion. Working from home and autonomously has allowed me to manage my time as I wish. Knowing the hours when I am most productive, I decided to work those hours, i.e. between 11am and 7pm with an hour break for lunch. Indeed, not having the pressure of arriving late or not being able to return, I worked more serenely from home than from an office. I sometimes worked later some days, and finished earlier on others, depending on the goals I set myself for the day.

All tasks are created and implemented on Jira, a project tracking and management system. *(Appendix 1)* Every Monday afternoon, Lo*** and I have a meeting about the progress of our tasks or the addition of new tasks with Antoine Patois, the CEO, and Guillaume BUFFIER. During this meeting, Antoine and Guillaume also approved all the modifications we made to put them into production, so that the customers could benefit from them quickly.

Moreover, every Monday morning, we have a meeting with all the teams, in order to know what is going on, in other words, who is present, who is absent, to know more about the planning of each one, or even the arrivals in the company.



COMPANY ORGANIZATION CHART

C. MY OBJECTIVES AND TASKS

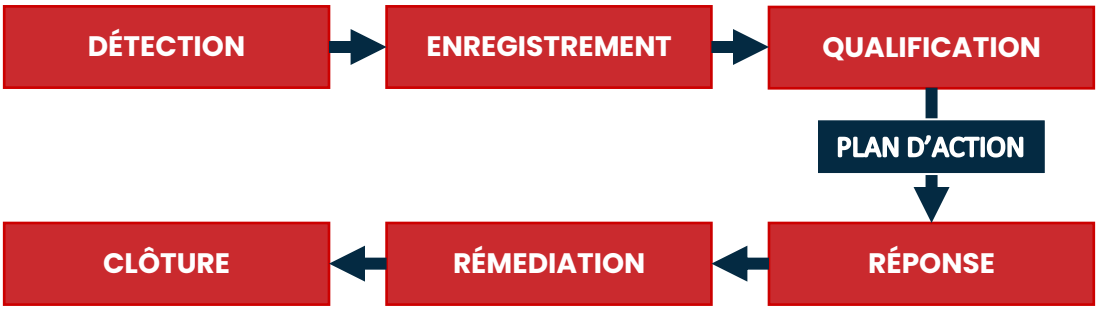
The first task I did when I arrived was to learn about cybersecurity. So, Guillaume, my supervisor, gave me a day to really learn about the vocabulary of computer security. Then, he advised me to complete some challenges on Root Me, so that I could really get to grips with some examples. Indeed, Root Me is a public platform allowing everyone to test and improve their knowledge in the field of computer security and hacking through challenges. *(Appendix 2)*

Secondly, I worked on small changes to the user experience, making some parts of the site more functional, or harmonizing elements, like all the buttons on the website. It is a lot of small tasks that were listed in Jira, which were assigned to me. This allowed me to take control of the technology. Not having done Angular for a long time, it was a good step to get back into the swing of things. Moreover, with the help of Lo***, it allowed me to understand the architecture of the project and its global functioning. *(Appendix 3)*

Following this, Guillaume told me that he wanted to group all the website CSS files into one so that it would be easier to modify, and if the site needed to change colors or fonts, that it could be done in a single file. That is why I proposed the use of the Bulma framework, which allows to simply change the whole website thanks to variables and helps me to code user interface elements easily. Moreover, even if I was working in a team, it was up to me to go and look for user experience mistakes, to find them and to correct them. So, it was partly up to me to create my own tasks.

Then I spent two full days with the SOC (Security Operations Center) Managers, the people who will use the "SecOps" platform in the company. I had to do this in order to better understand their needs, and clients' needs when they go on SecOps in order to propose my improvements. The job of the SOC Managers is to identify incidents, detect false positives, and report problems to customers, proposing an action plan to resolve the incident.

INCIDENT RESPONSE STEPS PLAN



I faced an issue: the site is very badly organized and optimized. So, I checked with Lo*** to see how long it would take him to redo the back end. And he agreed with me, he also found that the back end of the site is easily optimized and improved, if he starts from a healthy base, so we went to Guillaume to propose him to start SecOps from scratch. This would be quicker in every way and would avoid future compatibility problems. Antoine agreed, so we went to rebuild the platform from scratch. For this, I was able to work with Cedric BRAET, a UX/UI designer, to help him create the mock-up for the new SecOps. It is through different working days that we set up the site map, and the wireframe of the website. *(Appendix 4)* Thanks to all this work, Cedric was able to make a first model of the site, so that I could start working on it. *(Appendix 5)* When Cedric delivers me models, I take care of coding them in HTML and in SAAS (a new version of the CSS), using the Bulma framework.

Antoine and Guillaume asked me to change certain things in relation to the models created by Cedric, because in the end, it did not look like what they wanted. So, it was during the Monday meetings that they gave me the changes they wanted to make so that I could make them during the rest of the week.

In parallel, I oversaw other projects like the creation of a logo for the platform, with a favicon, it is the icon which is displayed at the top of the tab name. But I also did, for example, the redesign of the emails that we send to customers when there is an incident. These are side tasks which I liked to do because they allowed me to change projects and not to do the same thing all the time. *(Appendix 6 & 7)*

D. PROBLEMS ENCOUNTERED.

During this internship I learnt a lot about UX/UI design, corporate life and teamwork. However, I do not think I faced any real problems, whether it was the technologies used, the tasks assigned or the general organization of the company. I quickly integrated into the team and got along with my co-workers.

The only thing that was disturbing but normal was the level of security in the company. Indeed, in order to work I had to connect to an internal VPN of the company. I also had to launch dockers containers to run the backend to have a pre-production environment. But the server is not authorized to run, because it was running on my computer. Therefore, I had to copy an authentication token from the real server to my computer every day, to be able to work. (Appendix 8)

IV

CONCLUSION

To conclude, I did my third-year internship of the Bachelor Epitech as a front-end Developer in the company Login Sécurité. During this 4-month internship, I was able to put into practice the knowledge and skills I acquired during my years of training at Epitech Paris. I was lucky enough to be welcomed in the Login Sécurité team and to work on one of the biggest projects of the company since its creation, SecOps, the Security Center of Operations portal of the company.

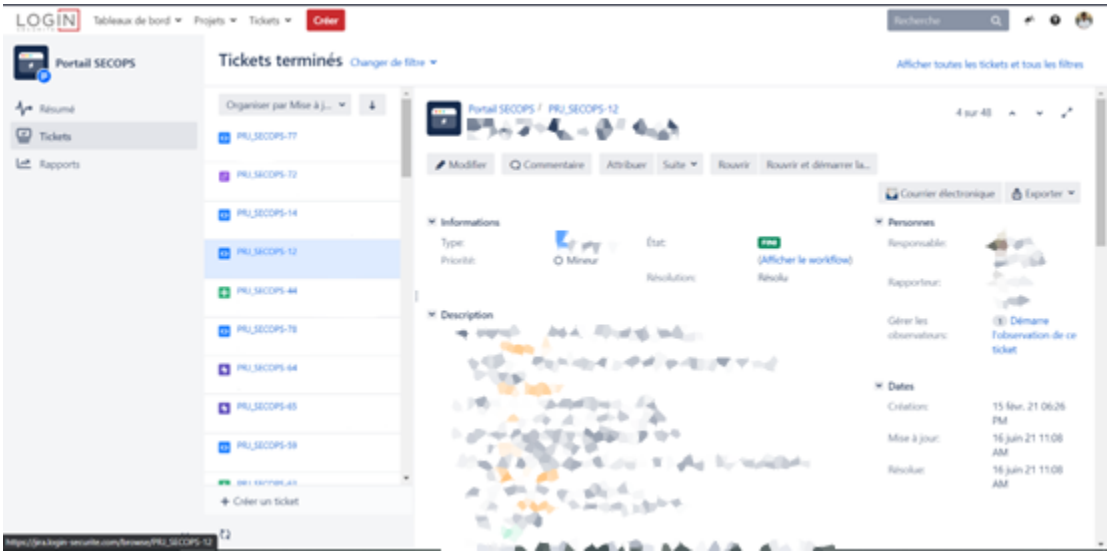
My internship tutor was very educational, as he took the time to accompany me and explain the set of objectives, I had to carry out beforehand. He stayed with me to guide me at the beginning of the projects for which he gave me responsibility with Lo*** MA*****. He allowed me to take initiatives and to propose my ideas. While I was only a trainee, Guillaume gave me the opportunity to be listened to.

I chose Login Sécurité for this 4-month internship because the missions they offered me were exactly what I needed to apply my knowledge in web programming, and in UX/UI design. Through this internship, I have developed my organizational skills and project management in a cybersecurity company. Indeed, being a novice in the field of cybersecurity, this internship also allowed me to learn more about this field. I also learned a lot about business communication as I had to work alongside several colleagues. We had a lot of meetings and brainstorming. I also realized that communication is a key factor in the success of a project and, ultimately, of the company itself. I will keep this information for later in my professional career. This internship was for me a confirmation of my abilities, and a possible career choice to join a company like Login Sécurité in the IT department in the future.

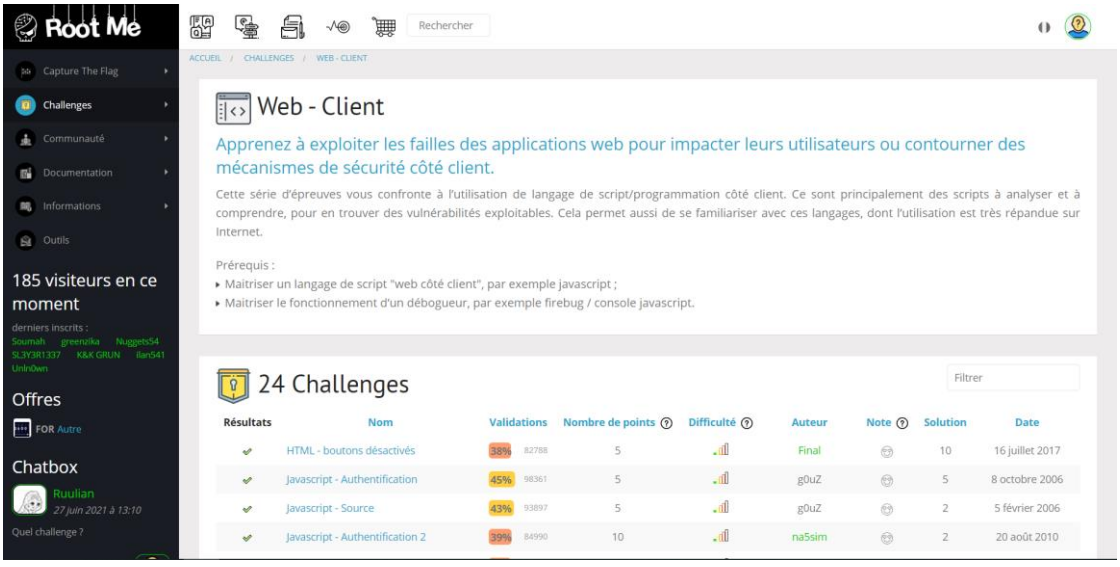
Moreover, I am thinking of continuing my collaboration with Login Sécurité as a freelancer, while continuing my studies in Canada. This will allow me to finance my studies and above all to have more experience. Before moving on to a contract, as my internship tutor and the CEO suggested to me a few days ago.

APPENDICES

APPENDIX 1 : Screenshot of my Jira Dashboard



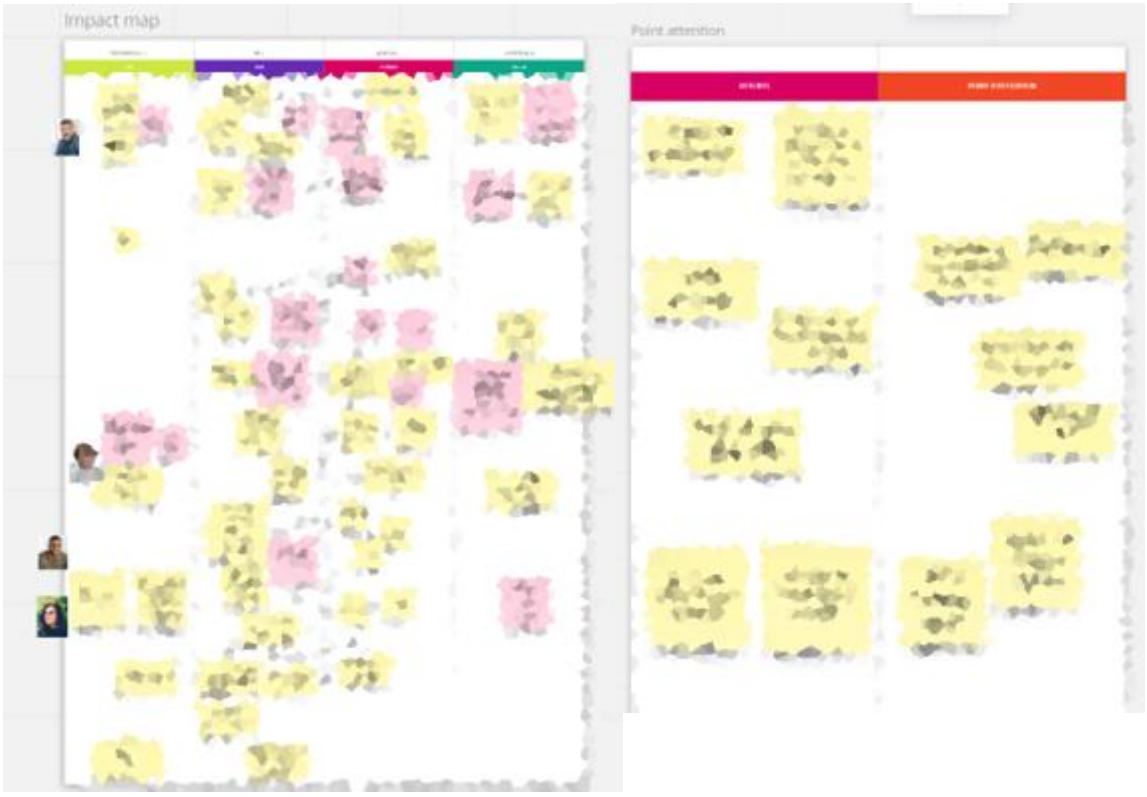
APPENDIX 2 : Screenshot of a RootMe Page

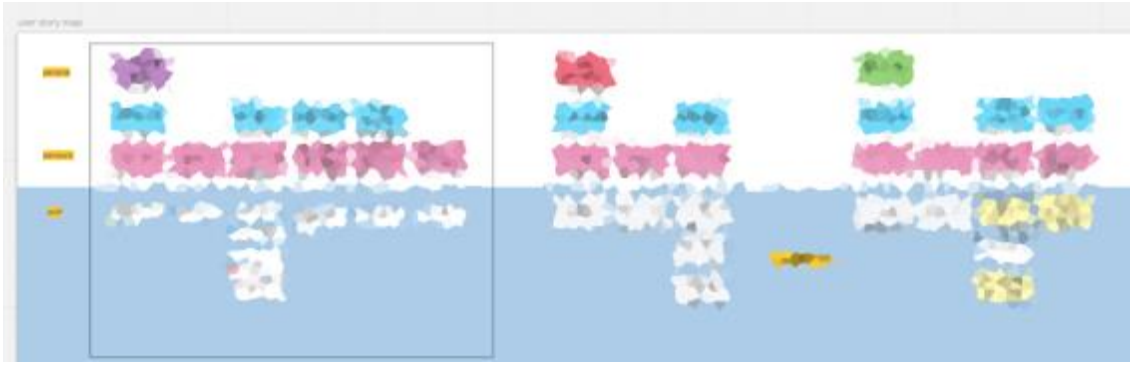


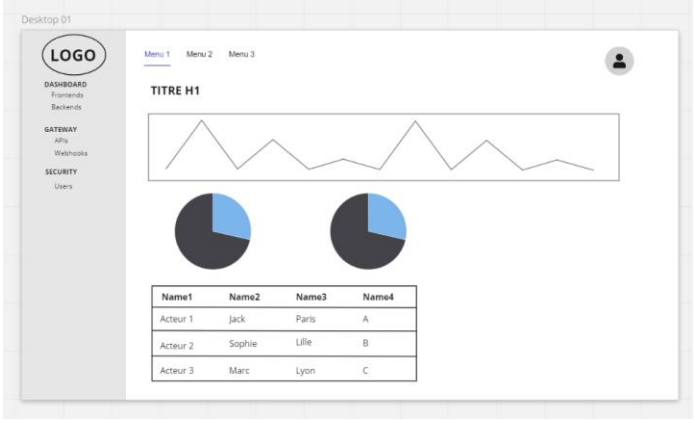
APPENDIX 3 : Website structure

Name	Last commit	Last update
..		
app		3 weeks ago
assets		3 weeks ago
environments		2 months ago
flags		4 months ago
fonts		2 years ago
locale		3 weeks ago
patterns		2 years ago
animate.css		11 months ago
favicon.ico		3 weeks ago
flag-icon.css		4 months ago
font-awesome.css		2 years ago
font-awesome.min.css		2 years ago
index.html		3 weeks ago
karma.conf.js		2 years ago
main.ts		3 months ago
manifest.webmanifest		2 months ago
messages.xlf		11 months ago
polyfills.ts		3 weeks ago
select-beautify.js		2 years ago
styles.css		1 month ago
styles.sass		3 weeks ago
test.ts		2 years ago
theme..scss		11 months ago
toastr.min.css		2 years ago
toolbar.css		3 weeks ago
tsconfig.app.json		4 months ago
tsconfig.spec.json		2 years ago
tslint.json		2 years ago

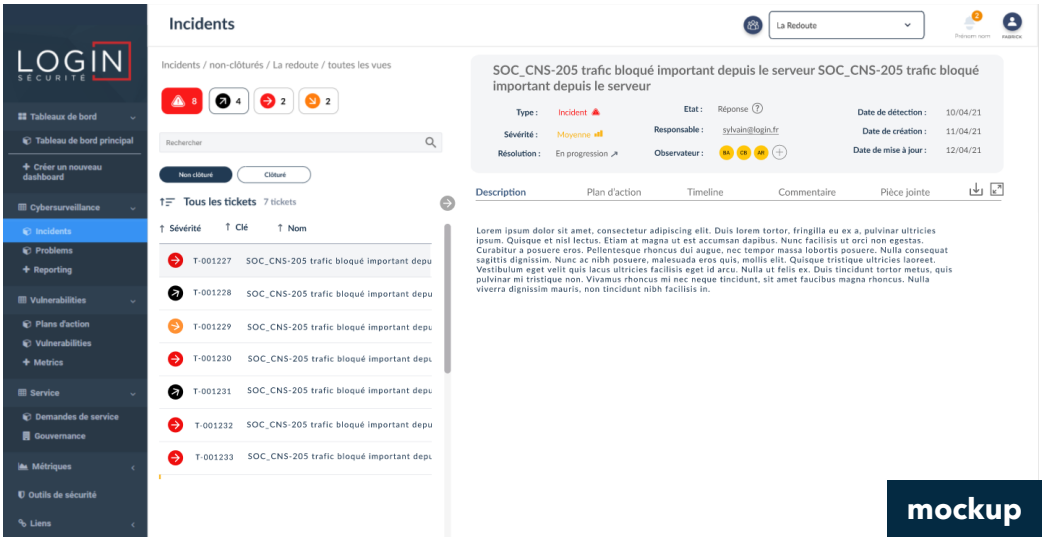
APPENDIX 4 : Some screenshots of the workflow file

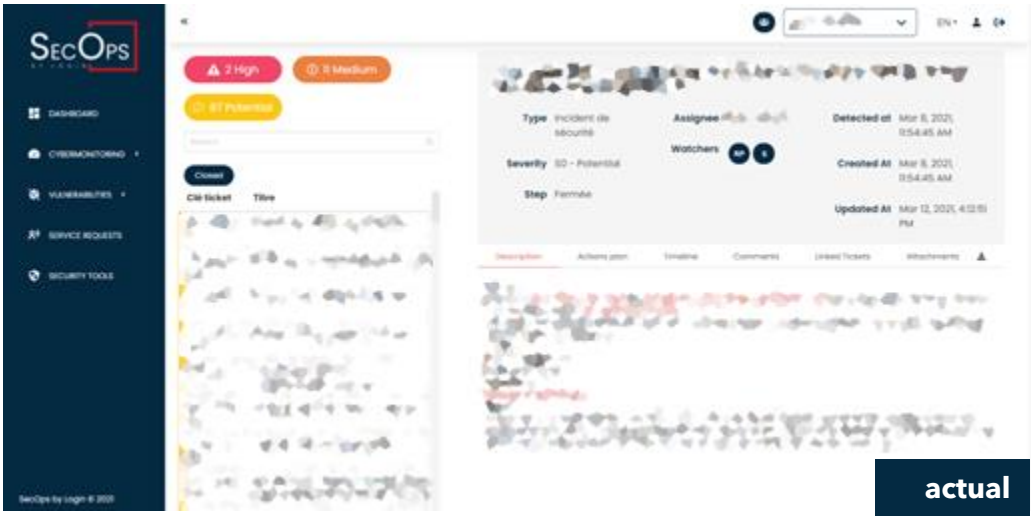






APPENDIX 5 : From the mockup to a real website



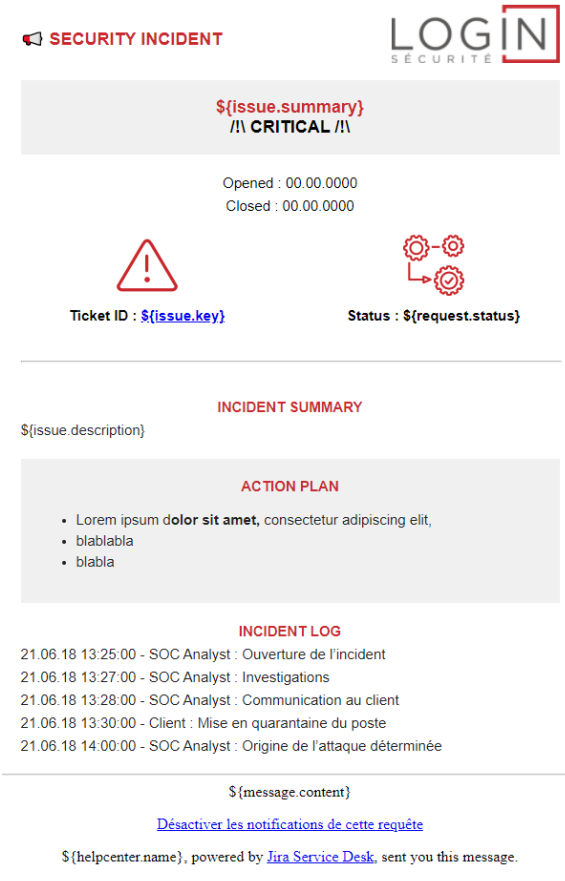


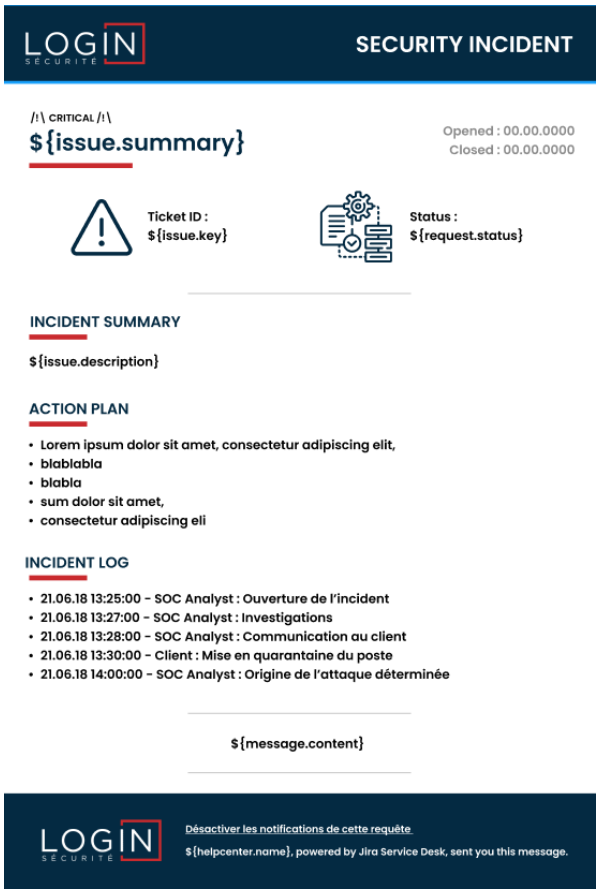
APPENDIX 6 : Logo and Favicon Creation

Logo creation

Favicon creation

APPENDIX 7 : Email Redesign





APPENDIX 8 : Authentification Token

LOGIN SÉCURITÉ

SECTION TWO

From : Sitpi RAJENDRAN – Login Sécurité <srajendran@login-securite.com>

Sended at : Monday 21 June 2021 15:47:04

To : Guillaume BUFFIER <gbuffier@login-securite.com >

Subject : [BlueProject] – Application to join the team

Dear Guillaume,

I would like to discuss with you, about the BlueProject.

As you know, I am currently working as the front developer of the SecOps Project. Over the past months, I have completed all the challenges and tasks that you and the team have given me. The project is about to be completed in a few weeks, that is why I am looking forward, even if the end of this project is the top priority for me.

I would like to explore the possibility of taking over new projects, and new challenges. I heard about the BlueProject and joining the team of this new project would be beneficial for me and the company. Indeed, as I already know the company, how the projects work and the internal organization of the company, I would be more easily integrated than a new employee. Moreover, you know my involvement in the projects in which I participate, my desire to finish my tasks in an optimal way, but with rigor.

Furthermore, the BlueProject interests me because of its innovative aspect. Particularly, by this centralization of information and cybersecurity elements for the customers.

It is for these reasons that I ask you if, at the end of my current project, I can join the BlueProject team.

I remain available if you want to interview me.

Sincerely yours,

Sitpi RAJENDRAN
Front End Developer - Login Securité
srajendran@login-securite.com
+33.6.68.62.99.53