

**TOLUWANI ADEFISOYE**

**CYBLACK INTERNSHIP 2022  
FINAL REFLECTIVE REPORT**

**INFORMATION SECURITY AUDITING**

This report is based on what I learnt during this task about information security auditing. During this task, MasterCard Inc. contracted Safe Tech cybersecurity consultants to perform a risk performance and compliance assessment.

During this task, an excel sheet was used in analysing different control requirement and their findings. Each member of my team (Safe Tech consultancy) members was allocated two of the control requirements and their findings to analyse their risks, corrective action, timeline and status.

I was allocated to analyse

1. Protecting against external and environmental threats
2. Securing offices, rooms and facilities

During this task, I contributed to the conclusion based on the report compiled and attended meetings with the rest of the group while chipping in ideas when needed.

Finally, I learnt the essence and how important physical security is important in data security. I also learnt different ways of implementing different physical security techniques and mitigating different threats as regards physical security.

**INCIDENT RESPONSE TASK**

An incident report is an approach or scheme used as a tool by an organization to take account of the attack launched at the organization. This usually takes account of injuries, damages issues and the vulnerability exploited.

In this report, Safe-Tech Consultancy was implored to perform an incidence response assessment by Mastercard based on previous attacks launched at the company. Safe-Tech consultancy consists of about 9 cybersecurity analysts including me.

This report was compiled after the tasks were subdivided into different parts and everyone was attached to complete a part of the task. This task increased my collaborative skills and I had the opportunity to understand the concept behind the incidence report. During this task, different tools were used including the blue-team lab was used to solve different tasks online.

**CONTRIBUTIONS**

*Also, during this task, I couldn't attend meetings due to personal issues and sickness (Covid) but I watched recordings and collaborated with my partner to work on our part.*

**ETHICAL HACKING TASK**

Safe Tech consultancy is a cybersecurity analyst company consisting of 9 cybersecurity analysts. At the beginning of this task, every member of the safe tech company took time to gather research on the topic, and then came together to share ideas about how the task will be solved.

For the purpose of this task, a virtual machine with Kali Linux was used. We carried out every reconnaissance and exploitation in the virtual environment. A Nmap scan also showed the number of open ports while a further scan exposes some web application loopholes.

This report was subdivided into different parts and every member of the group contributed to it. The scope of study of the report was done by me from the perspective of the whole report.

## **LESSON LEARNT**

I learnt how to install Kali Linux on a virtual machine and also run a Nmap scan to see open ports and other vulnerabilities.

## **CLOUD SECURITY TASK**

Master card Inc. has recently started a digital transformation, and part of the transformation is implementing cloud computing. SafeTech cybersecurity consultancy that includes my team and I have been left with the responsibility of migrating the company's infrastructure to the cloud in a secure manner. For the purpose of this task, Microsoft Azure was used

In the process of making this task as optimal as possible, roles were assigned to every member of the group. I was assigned the role of a customer service officer.

The duties of a customer service officer include

1. Helpdesk admin,
2. Customer Lockbox access approver
3. External ID user flow administrator
4. Service support administrator,
5. External ID user flow attribute admin

I attended task meetings and listened to recordings of missed meetings.

During this task, we created a free azure account that manages 9 members of the team whilst MFA was being enforced.

I learnt how to create users and assign roles to members of the group on azure while implementing MFA security measures while gaining access to the account. During this task, I understood the concept behind creating a virtual machine to monitor the resources available both on the cloud and on-site.

I learnt how to use Sentinel as a threat indicator.

## **THREAT INTELLIGENCE TASK**

This report was conducted by **Toluwani Adefisoye**, a cybersecurity analyst in **Safe-Tech consultancy**. For the purpose of this report, it is stated that the task given to Safe-Tech consultancy by Mastercard (A financial company) was to perform threat intelligence checks on the company's overall system.

Threat intelligence is a proactive measure usually done to mitigate vulnerabilities and calculate threat impacts. While the advantages are endless, the below are regarded as important benefits:

1. Cost-effective
2. The security team's efficiency is increased
3. Anticipated risks are mitigated
4. A data breach is prevented
5. Cyber threat analysis becomes a collaborative knowledge

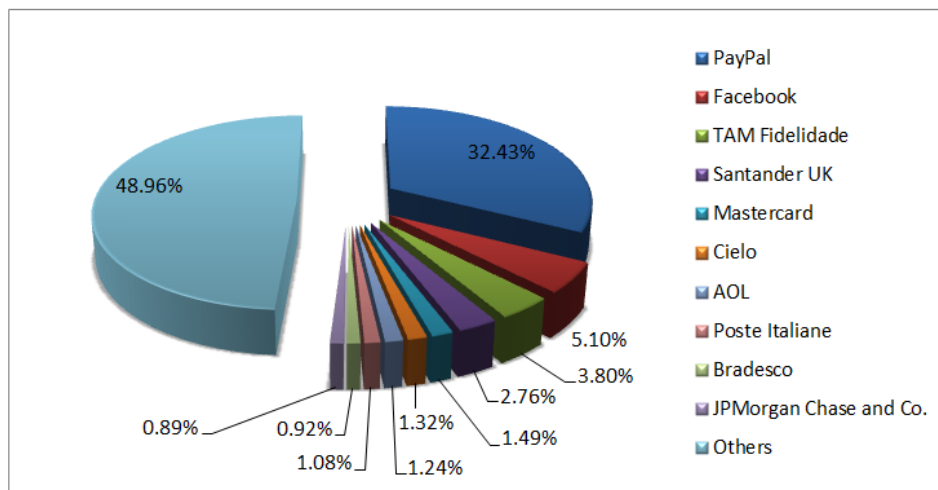
Safe-Tech consultancy implored my colleagues and I to work collaboratively and remotely during this process. In order to achieve an optimum result, we broke the task into smaller chunks that included Information gathering, threat modelling, threat landscape, analysis and reporting.

My colleagues and I were assigned to the previous sub-tasks, and we worked collaboratively and achieved an optimum result while we all learnt and increased our knowledge about new and existing tools.

I was assigned to the threat landscape sub-task with another colleague which was a great experience. I handled the global landscape scope, where I was exposed to the top 5 threats affecting financial industries globally. These threats include phishing/email compromise, data theft, malware attacks, ransomware

attacks and DDoS (Distributed Denial of Service) attacks. I analysed these threats based on how they are used as a tool to exploit financial industries in respect to the time at which they skyrocketed. Also, ENISA a European Union agency for cybersecurity produced top trends during a reporting period and time in which these threats were used to penetrate for financial gain in 2021-2022. These ENISA reports shed light more on the impact and trends of these top threats affecting the financial industry and MasterCard as a case study.

The image below was generated to give an insight into the percentage of some companies like Mastercard that are also exposed to the global threat landscape.



During this project, I learnt about the relationship between some popular industries and how they all have similar threat problems and how the top threat vectors have been affecting these companies over the years. I also increased my collaborative strength as I had a new experience working with other cybersecurity analysts and using new collaborative tools like Trello, Teams and Slack.

### **CONTRIBUTION TO THE PROJECT**

Over the few weeks, I have helped set up an azure account for the group and the virtual machine where we did the testing took place. I also increased my collaborative skills immensely as working with a hardworking team is just what this project needed.

I made research on cloud computing and took a course on it to learn more.

As a team player who will be useful in the real world, I also offered suggestions and assisted a group member in completing the assignment.

Positive comments from group members and positive feedback from my supervisor after I submitted my progress evaluation demonstrate that my contribution to this project has been recognised and that I am motivated to complete it successfully.

In addition, I have recorded all of the work I did throughout the internship for future use.

### **PERSONAL ADVANTAGES**

1. An internship gives students the chance to get practical experience while networking and building vital professional connections before they graduate. The more people you meet in the working world who share your interests, the more chances you'll have to succeed professionally.
  2. I've gotten better at communicating
  3. The primary objective of the advanced internship programme is to provide students with the opportunity to apply everything they have learned in the classroom. I applied a range of programming and computing skills I obtained in college while participating in the advanced programme with my group.
  4. This internship also enhanced my resume, making it clear that I have experience with the real-world operations of the industry.
  5. This internship also allowed me the ability to socialise with individuals from various cultures. Observing and learning about the daily activities and professions of people from many cultures was intriguing.
- Success in the corporate world depends on one's ability to see things from several angles and viewpoints.