- Cyber Security Audit: I was asked to travel to a client's site along with two other work colleagues and conduct a complete cyber security audit of their organization. This was done by me and one other person conducting interviews of head of departments, including their Head of IT, to find out about their daily routines in order to find the gaps in their organizational cyber security while another person performed penetration testing on their systems. After we were done conducting the interviews, we asked for evidence for every claim they made. We then inspected the physical security of their servers and backup sites. After we were done, we created a cyber security audit report mentioning all the gaps they had in their security with respect to ISO 27001 and ISO 27002.

Reflective Journal Entries

(I started my Internship with Vertex Cyber Security from the beginning of Week-3 of this session. Thus, my Week-1 would actually represent my Journal entry from Week-3 of the session and so on. However, I worked through the two weeks of midterm break and included them as activities for)

Week 1

Goals, Activities and Outcomes

The goal set forth for me this week was to communicate with a client and provide basic IT support for him, and learn laptop hardening for Windows operating system from the documentations provided to me by Martin.

I communicated with the client and found out his requirements. As per the requirements, I synced his Microsoft calendar with his Google calendar, synced one of his Google calendars with another Google calendar of a different account, set up Outlook application for his multiple accounts, set up Office 365 family subscription for his organization, transferred his Dropbox files to his Google drive, and synced his google workspace with Microsoft Outlook. I also read the documentations provided to me on Laptop hardening and familiarized myself with the concepts.

The outcome I achieved was client satisfaction from solving the IT issues he was facing and gained familiarity with Windows operating system and Laptop hardening concepts.

New Knowledge, Skills and Experience

I gained extensive knowledge on Windows operating system and learned how to perform basic IT operations.

I gained skills related to communicating with the client and handling their needs and requirements.

I gained practical experience on basic IT operations by solving the issues face by the client.

Rewarding Experience

For me, the rewarding experience for this week was getting hands-on experience in dealing with clients and solving basic IT issues for them. Learning how the Windows operating system works in the background was also very rewarding.

Difficult Experience

The most difficult experience for me during this week was familiarizing myself with the intricate workings of Windows operating system in order to perform various tasks related to hardening in terms of security. Being a particularly introverted person, I also faced difficulty familiarizing myself with my new workplace and colleagues.

Tasks for the upcoming week

In the upcoming week, my goals were to learn further tasks related to laptop hardening for Windows PCs and perform those tasks on a client's PC.

Week 2

Goals, Activities and Outcomes

The goal for this week was to apply laptop hardening on clients' laptops as a method of securing them from malicious attacks. I also had to read the documentation on the "Netfiler" vulnerability of Linux and try to exploit it as a part of trying to secure it. I also needed to familiarize myself with securing Google Workspace which is categorized as Application Security.

As for my activities during the week, I learned laptop hardening steps in depth by reading the documentations provided to me and from the web. Then I tested them on VMware so as to be sure of my capability of applying them on a real working environment. Once I was sure that I could perform laptop hardening without breaking anything, I then applied them on two clients' laptops in order to secure them from malicious threats. I also read the documentations on the Linux "Netfilter" vulnerability and the Google Workspace Hardening documentations provided to me by Vertex.

I achieved client satisfaction by securing their PCs from malicious attacks. I also created detailed step-by-step documentation for laptop hardening.

New Knowledge, Skills and Experience

I gained insight on how Windows processes and services work in the background, gained knowledge about how DNS over HTTPS works, and gained further insight on Linux OS.

I gained Windows PC Hardening skills. I also gained skills on creating documentations and researching vulnerabilities in OSes.

I gained practical experience on PC hardening for clients.

Rewarding Experience

Being able to effectively enhance security for clients' computers in the real world was particularly rewarding for me during this week.

Difficult Experience

The most difficult experience for me this week was gaining an understanding of how Windows services and processes work in the background using 'procmon'.

Tasks for the upcoming week

In the upcoming week, my goals were to learn Google Workspace Hardening processes, test them in a test account, and then apply them for clients.

Week 3

Goals, Activities and Outcomes

The goals for me this week were to learn, test, document and apply Google Workspace hardening for a client as a method of securing their organization from malicious attacks. I was also scheduled to attend Vertex's in-house secure code training session.

I learned Google Workspace hardening steps in depth. Tested them on a test account, documented them in detail and then applied them for a client's organizational Google Workspace account. I also read ISO 27001 and 27002 standards and familiarized myself with them. I also attended the interactive secure code training session.

I achieved client satisfaction by securing their organization's Google accounts from malicious attacks such as phishing and Man-in-the-Middle attacks. I also created detailed, step-by-step documentation on Google Workspace Hardening. Additionally, I learned the basics of coding with security in mind.

New Knowledge, Skills and Experience

I gained insight on different email protocols, SPF, DKIM and DMARC for email authentication, familiarization with ISO 27001 and 27002 standards. I also learned the basics of secure coding.

I gained skills related to securing Google Workspace from malicious attacks. I also learned how to test and update official documentations.

I gained practical experience on providing Google Workspace security for clients.

Rewarding Experience

The rewarding experience for this week was learning how to enhance security for clients' Google Workspace accounts by applying real-world defenses.

Difficult Experience

The most difficult experience for me during this week was trying to map the old documentation provided by Vertex to the updated Google Workspace settings and trying to come up with workarounds for insecure mail protocols such as IMAP and POP. I also faced difficulties with DKIM and DMARC setup due to lack of access to DNS.

Tasks for the upcoming week

In the upcoming week, my goals were to continue updating the Google Workspace hardening documentation and familiarize myself with the Essential Eight documentations.

Week 4

Goals, Activities and Outcomes

My goals for this week were to continue working on Google Workspace hardening and updating the documentation, applying changes to the client's Google Workspace account and troubleshooting the issues faced by them. I also had to read the Essential Eight documentations and figure out implementations for Windows and Macs.

I figured out a solution for implementing Google Workspace into Outlook with GWSMO. I then updated the documentations and applied the changes to client's Google Workspace account. I solved the issues arising from Google Workspace hardening regarding setting up work profile for the client. I then read up on the Essential Eight mitigation strategies, implemented some mitigation strategies for Windows PCs on a test environment and documented them.

The outcome was achieving client satisfaction by securing their Google Workspace from malicious attacks and allowing seamless integration of Microsoft Outlook and Google Workspace. I also updated the organizational documentation for Google Workspace hardening.

New Knowledge, Skills and Experience

I gained extensive knowledge Essential Eight mitigation strategies for different Maturity Models recommended by ACSC.

I gained skills related to securing Google Workspace from malicious attacks. I solidified my skills of testing and updating documentations, and client handling.

I gained practical experience on troubleshooting Google workspace hardening for clients.

Rewarding Experience

For me, the rewarding experience for this week was improving security for clients' workstation from malicious attacks in the real world.

Difficult Experience

The most difficult experience for me during this week was finding the optimum balance between security and functionality for the client.

Tasks for the upcoming week

In the upcoming week, my goals were to keep working on implementing Essential Eight mitigation strategies for Windows and Macs and creating detailed documentation on their application for different Maturity Models. I also needed to attend another session of the interactive secure code training.

Week 5

Goals, Activities and Outcomes

The goal set forth for me this week was to keep working on implementing Essential Eight mitigation strategies for Windows and Macs and creating detailed documentation on their application for different Maturity Models. I was also asked to learn how to perform Website Load Testing using JMeter and K6 and was scheduled to attend another session of the interactive secure code training.

I figured out and implemented Essential Eight mitigation strategies for Windows and MacOS on test environments and documented them. I learned how to use JMeter and K6 from watching video tutorials on the web and tested it on fabricated scenarios on random test websites. I used an android emulator and BurpSuite proxy to load test mobile APIs as well. I attended another session of secure code training.

The outcome was creation of a documentation for Essential Eight mitigation strategies and familiarization with load testing using JMeter and K6. I figured out if a client's website and mobile application were using the same API endpoints using the BurpSuite Proxy.

New Knowledge, Skills and Experience

I gained knowledge of different tools to use in implementing Essential Eight mitigation strategies; I also gained knowledge of load testing API endpoints. I also furthered my knowledge on secure coding.

I gained skills related to using JMeter and K6 to perform load testing for web sites and mobile APIs; I also gained further skills related to secure coding.

I gained practical experience on performing load testing on fabricated test scenarios and mobile APIs using BurpSuite Proxy.

Rewarding Experience

For me, the rewarding experience for this week was getting familiarization with load testing using two useful tools which I found very interesting.

Difficult Experience

The most difficult experience during this week was figuring out if website and mobile application were using the same API endpoints using the BurpSuite Proxy.

Tasks for the upcoming week

In the upcoming week, my goals were to conduct a meeting with a client regarding Essential Eight mitigation strategies using Windows and MacOS. I also had to create load testing scripts for different scenarios and run load tests with multiple virtual users on a client organization's website and document my findings.

Week 6

Goals, Activities and Outcomes

The goal set forth for me this week was to conduct a meeting with a client regarding Essential Eight mitigation strategies using Windows and MacOS. I also had to create load testing scripts for different scenarios and run load tests from a remote server with varying amounts of virtual users and document the website's performance in a table form. Then I had to match the failure point of the websites with Amazon AWS performance data. I was also scheduled to attend another secure code training session.

I successfully conducted the Essential Eight mitigation strategies meeting alongside Martin and informed the clients on processes to implement Essential Eight maturity level one for their organization using Windows and MacOS. I performed load testing for the client's website and tabulated the data found from different scenarios using K6. I familiarized myself with Amazon AWS and mapped my findings to the client organization's website's performance with graphs on their Amazon ECS, Database, and Cloudfront and documented my findings and provided

verdict on the reason for failure of their website. I also attended another secure code training session.

The outcome I achieved was client satisfaction from successfully imparting knowledge on Essential Eight mitigation implementations and combining all of my findings in a single documentation with explanations and an overall verdict regarding the reason of failure.

New Knowledge, Skills and Experience

I learned how to navigate through different AWS performance metrics and make sense of it; I also furthered my knowledge on secure coding practices. Additionally, I learned how to prepare documentation on load testing for clients.

I gained skills to build and run load testing scripts; Additionally, I gained public speaking skills by conducting meetings with multiple people from an organization and efficiently collaborating with them.

I gained practical experience on performing load testing for clients using real world scenarios and communicating the findings from those load tests to the clients.

Rewarding Experience

For me, the rewarding experience for this week was getting hands-on experience in performing load testing in real-world scenarios for client organizations.

Difficult Experience

The most difficult experience for me during this week was familiarizing myself with AWS and its different performance metrics.

Tasks for the upcoming week

In the upcoming week, my goals were to familiarize myself with penetration testing for clients' systems.

Week 7

Goals, Activities and Outcomes

For this week, my goals were to learn, implement and document Essential Eight controls for MacOS.

I learnt different mitigation strategies for MacOS according to different maturity models using Essential Eight and applied them on a test environment.

The outcome from this week's activities is a detailed documentation on Essential Eight implementation for different maturity models on MacOS.

New Knowledge, Skills and Experience

I gained extensive knowledge on how to implement Essential Eight mitigation strategies for MacOS.

I gained skills on Application Control for MacOS; Application patching on MacOS; MacOS patching; Administrative privileges restriction on MacOS; Creating and accessing backups on MacOS; Setting up MFA for users on MacOS.

I gained practical experience on applying Essential Eight mitigation strategies for different maturity models on MacOS.

Rewarding Experience

For me, the rewarding experience of this week was gaining familiarity with MacOS and learning to apply real-world controls in order to help protect users from malicious attacks.

Difficult Experience

The most difficult experience for me during this week was learning how to set-up MacOS in a virtual setting.

Tasks for the upcoming week

In the upcoming week, my goals were to continue with interactive secure code training. Create a workplan on providing a lecture on Essential Eight mitigation strategies for a client (a School) using both Windows and MacOS.

Week 8

Goals, Activities and Outcomes

This was a very short week because of a public holiday. Also, I took a personal leave because of a religious festival.

The goal set forth for me this week was to conduct a meeting with a client regarding Conduct meeting with client about Essential Eight and to try and implement Google's Context Aware Access to block Outlook.

I attended another session of interactive secure coding this week. I also applied Google's Context Aware Access through browsers, but wasn't able to block Outlook from accessing through GWSMO. I also conducted the meeting with clients informing them about Essential Eight controls for MacOS and Windows.

The outcome I achieved was client satisfaction from successfully imparting knowledge on Essential Eight mitigation implementations. I furthered my knowledge about secure coding and also learnt that Outlook cannot be blocked by Google's Context Aware Access.

New Knowledge, Skills and Experience

I gained knowledge about Google's Context Aware Access and furthered my knowledge on how to code securely.

I furthered my skills on Google Workspace security controls.

I gained practical experience on Essential Eight security consulting for clients.

Rewarding Experience

For me, the rewarding experience of this week was getting to perform security consulting for a client organization.

Difficult Experience

I faced no particular difficulty this week.

Tasks for the upcoming week

In the upcoming week, my goals were to conduct a meeting with a new client to consult them about their organizational security.

Week 9

Goals, Activities and Outcomes

During this week, my goals were to learn, test and implement Context-Aware Access and API Controls for Google Workspace and learn and try some pentesting steps on a client website. Additionally, I was assigned to consult a new client about their organizational security.

I attended and conducted a meeting with the new client, found out his organization's current security posture and then made notes of what needs to be done for them, including- laptop hardening, Microsoft Office 365 hardening, MDM, etc. I learned, tested and applied Context Aware Access and API Access controls on a test account and then updated our organizational documentations on Google Workspace hardening accordingly. I read up on some pentesting documentations to get an idea of ethical hacking. I also read up on Microsoft Office 365 hardening controls.

After the activities of this week, I had some idea about practical ethical hacking, including- XSS, SQL Injection, etc. I noted down the client's organizational security requirements. I also gained

a better understanding of Google Workspace hardening controls and Vertex's organizational documents were also updated accordingly.

New Knowledge, Skills and Experience

New knowledge gained this week included application knowledge about Google's Context-Aware Access and API Access Controls; Additional knowledge gained was regarding Microsoft 365 Hardening controls.

New skills added under my belt was Google Workspace Hardening in terms of Context-Aware Access and API Access Controls.

My new experience for this week was performing penetration tests on a client's website.

Rewarding Experience

Gaining experience on real-world penetration testing (Ethical Hacking) was rewarding for me.

Difficult Experience

The most difficult experience for me during this week was mapping Vertex's existing Microsoft Office 365 hardening documentations to the actual controls.

Tasks for the upcoming week

My goals for the upcoming week consisted of learning and testing the implementations of Microsoft Office 365 hardening in more details.

Week 10

Goals, Activities and Outcomes

The goal set forth for me this week was to learn Microsoft Office 365 hardening steps in detail, test them and document them. Additional task assigned to me was to conduct an incident response meeting for a client organization.

Most of the week, I tested Microsoft Office 365 hardening steps and documented them in detail as preparation for a client meeting where I would need to harden their organizational Office 365 account. I conducted the incident response meeting along with a co-worker where an employee with admin access to organizational accounts containing sensitive data was fired. We went through a list of all the accounts he had access to and revoked all of his accesses.

After this week's activities, I had completed and updated the documentation to harden Microsoft Office 365 accounts for organizations. I also learned how to perform time-sensitive incident response.

New Knowledge, Skills and Experience

This week, I gained in-depth knowledge of Microsoft 365 security controls.

I gained incident response skills.

I gained practical experience on performing time-sensitive incident response for a client organization.

Rewarding Experience

Getting hands-on knowledge of how to perform time-sensitive incident response for an organization was a rewarding experience for me during this week.

Difficult Experience

Mapping Vertex's existing Microsoft Office 365 hardening documentations to the updated controls was particularly difficult for me during this week.

Tasks for the upcoming week

For the following week, my goals were to conduct a security consultation meeting with a client and apply security controls for their organization.

Week 11

Goals, Activities and Outcomes

The goal set forth for me this week was to conduct a security consultation meeting with a client to find out their security gaps. Additionally, I was asked to go along to clients' sites in order to perform disaster recovery tests on a client organization's website and database servers, and also to perform a security audit on a school's IT systems.

For my activities this week, I went to the client's site and directed them on how to perform disaster recovery for their web servers and database servers running on AWS. This was done by turning off their primary servers to see if the backup servers picked up the traffic load from the primary and vice versa. This was then documented and a report was presented to the client. For the audit, I went to the school along with work colleagues and asked questions to their Head of IT, Head of Recruitment and Head of Finance to find out their security gaps and asked for evidence for every control they claimed to have in place. We then had a tour of their primary server, backup server and DR sites to check gaps in their physical security. Finally, we created a report on our findings where we suggested improvements to their security.

The outcome achieved was that a security audit of a school was performed and a draft for the report to improve their security stance was created. Disaster Recovery tests were also performed for a client organization.

New Knowledge, Skills and Experience

During this week, I gained insights on how to perform security audits and how to perform disaster recovery tests.

I gained investigative skills in addition to auditing and disaster recovery skills.

My new experience for this week was performing a security audit and a disaster recovery test for client organizations.

Rewarding Experience

For me, the rewarding experience for this week was gaining real-world experience on how to perform security audits and finding out gaps in their security by the means of investigation.

Difficult Experience

The most difficult experience for me during this week was trying to find out gaps in cyber security from conversations with people who has little to no idea or awareness about it.

Tasks for the upcoming week

In the upcoming week, my goals were to perform a security audit of Office 365 and Firewall controls for a client organization. I was also asked to tie off all of the open projects assigned to me within the upcoming week before ending my internship.

Week 12

Goals, Activities and Outcomes

During this week, I needed to follow up with the client for evidence of their security controls in order to continue writing the report for the audit that was performed last week. I also had to perform Office 365 security controls audit for a client organization. As an additional task, I was asked to help with performing an incident response for an organization that had fallen victim to phishing email.

I reached out to the client for whom we performed the security audit and got back evidence regarding their security controls and edited the audit report accordingly. The phishing email victim client reached out to us for help regarding the incident and we went through their Office 365 security controls and hardened them by adding log retentions, eDiscovery, blocking all auto-forwarding and enforcing 2FA for all their accounts. Then we went over all the suspicious emails that may have caused the phishing to occur and all of the logs that Office 365 had retained automatically (which were insufficient). We found out the phishing email chain but we were still looking into how exactly they gained access to the credentials of the employee. I also performed a security audit for Office 365 controls for another client organization and found out their security gaps and noted them down to present to the client.

The outcomes from this week were performing an incident response to harden security controls for Office 365; performing security controls audit, and finding out the gaps in security for another client. I also furthered the report for the security audit performed last week. The overall outcome was tying off all tasks and projects assigned to me due to this being the last week of my internship at Vertex Cyber Security.

New Knowledge, Skills and Experience

During this week, I gained insights on how to perform time-sensitive incident response.

I gained skills to investigate phishing attacks and to perform time-sensitive security hardening.

The new experience of this week was performing incident response for a phishing victim.

Rewarding Experience

I found the real-world experience of performing time-sensitive incident response in order to secure an organization from further attacks to be very rewarding.

Difficult Experience

The most difficult experience for me during this week was trying to find the point of phishing attack from logs and suspicious emails.

Tasks for the upcoming week

This being the final week for my internship, I did not have any tasks lined up for the upcoming week.

Work Samples

Due to the sensitive nature of the work and the confidentiality agreement signed with Vertex prior to starting the Internship, I am unable to attach any work samples to this report. However, brief steps of some of the works are provided below:

Laptop Hardening for Windows

The steps required to perform laptop hardening for windows are as follows:

- Change DNS settings to Quad9
- Disabling SMB service and SMB client
- Removing admin privileges from normal user accounts
- Enforcing security updates
- Enabling Firewall and removing or disabling all inbound rules
- Configuring Group Policies and Registries
- Configuring Structured Exception Handling Overwrite Protection (SEHOP)