National College of Ireland

MSc Configuration Manual
MSc Cyber Security

Gearóid Kelly
Student ID: X20197365

School of Computing
National College of Ireland

Supervisor: Mark Monaghan
Industry Supervisor: Declan Byrne

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Gearóid Kelly
Student ID:	X20197365
Programme:	MSc CyberSecurity **Year:** 2022
Module:	MSc Interinship
Supervisor:	Mark Monaghan
Submission Due Date:	15th August 2022
Project Title:	Migrating an Email Filtering Solution from on Premise to Cloud
Word Count:	4047 **Page Count 20**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: *Gearoid Kelly*

Date: 12/08/2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Table of Contents

Introduction

This document contains content that was created for the Masters' Internship Project. The approach taken for the Masters' Internship is different to what a typical research-based project would feature. The nature of this report was practical, whereby the skillset and knowledge learnt within the PGD CYB could be utilised within a Cyber Operations team. All aspects of this are covered in the Tri-Party Agreement and must not be shared outside these communities.

This document also covers the rationale for choosing the master's project, the detailed project plans and additional documentation created for the project's completion.

Background Overview –

Background of my work was initially working in Release Management and IT Operations system administration & configuration management. Working within this role provides an insight into operating and adhering to Cyber Security best practices. In August 2021, a decision was made by ESB to purchase a UK Supply Business, creating a merger between the 2 companies. Alongside the consolidation occurring within the ESB, there was no longer a role within the ESB Energy Team. An opportunity became available to move to the cyber operations team. This coincided with completing the PGD and electing to continue to achieve the masters' accreditation. Both of which occurred in February 2022. This was also one of the critical aspects of choosing to complete an industry-based project over a research-based project. The project's start coincided with a transition to a cyber-based role. Selecting this is beneficial in showing how theory and practical elements can be combined. In addition, working within a critical infrastructure highlights the need for best practices within organisations. Some of the other options I had thought of are outlined below -

Project Ideas –

Return to Office protocol and implementation of best practices within an organisation. - Post-COVID, as organisations prepared to return to the office, one major factor was that devices were not connected to a corporate network for 2 years. As a result, devices could have several exposed vulnerabilities, and connecting to the corporations' network could have a widespread impact.

Behaviour Analysis on the vulnerabilities in an organisation – It's fair to say I'm cynical and cautious. We have seen a drastic increase in cyber-attacks from both a personal and organisational level. Moreso, we are seeing individuals being targeted via phishing campaigns whereby perpetrators contact individuals requesting all types of information. Despite media campaigns from financial institutions, Retail and all organisations, people are still being breached – This can be costly for individuals and the hackers are constantly gaining financially. I would like to investigate further why individuals click and hand over information and if there is a behavioural trait across the individual.

Monthly Internship Activity Report

Student Name: Gearóid Kelly Company: ESB

Student number:x20197365

Month Commencing: February 2022

Diary of Internship

Month One End Feb -March –

Transition from an IT Operations team/ Release management role to a Cyber Operations Role.

Following a merger in the UK contingent of a supply business, a transition of all systems and users had to be completed. The business unit within ESB was no longer operating as a running business, and operations would be moved to the purchased organisation. As part of mergers, there is a significant workload for IT Departments. The workload consists of the customers' transition to the new entity alongside the decommissioning of all the assets within the ESB Network. In my role within the IT operations team within ESB Energy, it was my duty to decommission the Billing system. The billing platform is an intricate system with multiple interconnected systems alongside various teams, both in-house and outsourced accessing the domain. As with the role of IT Ops System Administrators, it was always a duty to work with cyber security aspects in mind. A holistic view of the systems had to be completed. It is not as simple to just remove users. We also had to ensure that all third-party interconnectivity was disabled -Network Connectivity between third parties and that all residual data was removed.

Cyber Operations Team –

Introduction to the Cyber Operations team – The cyber operations team within ESB is tasked with managing day-to-day operations. They work alongside cyber teams such as Cyber Engineering, Threat & Vulnerability Management, Cyber Monitoring & Incident response.

The period of Month One was a hybrid of the closure of the ESB Energy Organisation & being introduced to the toolkits used by the Cyber Operations Team and processes used.

These Tasks include

Health Checks –

- Ensuring all Toolkits are working as expected and no incidents are outstanding
- Service Management – Completion of service tasks requested by business units
- Spam Mailbox Management
- SEPM Devices

SEPM Implementation – Endpoint Protection system implementation

I'm currently tasked with assisting in deploying a new endpoint protection system in a new domain as part of a project. This involves creating, building and testing a DMZ, which will be used by one of the organisational departments. This environment will have best-in-class features and components. I was involved in an initial workshop where an install package was created and deployed to a client. I was then trained further on how to deploy the package to clients alongside familiarisation with the software.

Month One was spent familiarising myself with tools and processes within the cyber operations team and choosing a topic suitable for completing the Master's research topic.

Employer comments

Gearóid has joined the Cyber Operations from an IT Operations role within ESB Energy. His primary focus for the month was working within the ESB Energy ensuring that all tasks were completed to allow a transition to his new role. He has also joined and integrated into the cyber operations team immersing himself into the daily tasks across the cyber landscape. He has a reviewed processes and suggested and implemented process improvements alongside leading the Endpoint Protection implementation on another project.

Month 2- March – April

Having become familiar with the toolsets and the processes within the team, I was completing the daily health checks alongside familiarising myself with some additional toolsets such as Windows Defender. Implementing a tool like this at a corporate level with circa 4000+ employees means security alerts get generated and require investigating. I was tasked with researching these alerts and completing a Standard Operating Policy for sharing amongst the team. Microsoft Defender checks are now part of the Security Operations team's daily tasks. Given the volatile nature of the globe at the moment, we see increasing alerts from a Ukraine Perspective alongside additional cyber-attacks such as Conti and phishing attempts.

Arriving from the outside into the team, there are already embedded processes. Some legacy processes in organisations can be improved at all levels to make our day-to-day operations more efficient and serve our customers by advising them of specific outcomes. Since 91% of all cyber-attacks begin with a phishing email, email filtering is one of the most crucial aspects of an organisation's gateway. We have toolsets in place to filter mails; however, there can always be legitimate-looking emails that will creep through – One Such email is a recent one from An Post. And while initial views of the email looked legitimate, the primary warning was that it came from support@anpost.com rather than a . i.e. domain. While emails like this can escape the filtering, it ensures those who receive the email don't click on the links within it. While the links within it can be blocked from access, it also removes the issue from a mailbox level. I developed and implemented a process to improve our spam monitoring process regarding email. – If we see that users have received spam emails, we will block the sender and any links contained within it. We will also take the additional step of removing the email from people's mailboxes. This will then protect the company and individuals from phishing attacks. We can also complete this task where users receive spam emails which may not be malicious. Specific organisations may also issue marketing content to users, which may be of nuisance and cause noise. These can also be blocked and removed as part of the improved spam monitoring process.

Microsoft Defender Alerts – Process improvement. When we receive informational alerts in Microsoft Defender, particular remediation and preventative tasks are carried out. Scans and security updates will be completed on devices. As part of this, I am seeking a way of automating this process where if an alert is received, the device will be automatically scheduled for a software scan, and the alert will be closed off if all is in order.

SEPM Management- I'm currently managing the installation of the SEPM Clients on the project domain alongside troubleshooting issues being encountered.

SPE Installation – A protection engine requires installation on a client. We had a vendor in to complete the installation of this software. Unfortunately, there were complications in the installation, meaning a new server build was required, so the task had to be rescheduled.

Items learnt in this Month –

- Further familiarisation with health checks
- Microsoft Defender overview and process implementation
- Spam Monitor Improvements
- SEPM Implementation & Management
- SPE Installation

Employer comments

Gearóid continues to focus and gain knowledge within the Cyber Operations Space. He is competent in completing all tasks within the cyber operations space. Additionally he continues to go the additional step where he will review processes and suggest areas for improvement. He takes initiative with this and will roll out the process changes and implement them within

Industry Supervisor Signature: Declan Byrne

Student Signature: Gearóid Kelly

Month 3 April – May

As you can see here is that the work is varied. There are routine day-to-day tasks which require completion. However, there are also the tasks, such as the SEPM or SPE installation, which may not go to plan and can take up significant time and resources. Additionally, it is also finding an item which is a suitable candidate for the Industry Internship. As an employee in an organisation, it is working to what the organisation requires and is most important to fulfil the needs. This is where one needs to be adaptable and reactive to completing the tasks required. In addition, the purpose of conducting an internship is that one can demonstrate the academic skills learnt throughout the PDG and utilise these in the workplace. It is challenging to find a suitable topic for a research-based industry internship as the nature of an internship is much more practical than electing to complete a 100% based research project.

I provided an overview of some topics I would have chosen in the project ideas. The opportunity also presented to complete the industry internship on migrating our Email Security Appliance from on Prem to a cloud-based solution.

Tasks Completed within April – May

Within the team, there is a roster to complete health checks – Typical schedule of these is once a month. However, with Leave and other commitments, we are assisting when required.

Some low-level tasks which required additional investigation were some new alerts received in Defender, whereby we had to isolate devices to ensure security scans were completed, and no issues were diagnosed.

SEPM Environment Installation- Significant time has been spent in the past few months on the SEPM Client installation. This was done with our vendor; however, as the number of clients deployed to the environment increased, we encountered issues on specific clients whereby alerts were generated. Unfortunately, these alerts created false positives and noise for one of the stakeholders. As a result, I had to liaise with our vendors to work towards a resolution and host a workshop with a vendor to attempt to diagnose the issue, which remains outstanding.

It is essential to take a holistic overview when diagnosing issues and ensuring adequate change management controls are in place. To assist in the troubleshooting process and not impact all devices within the system, it was essential to isolate the changes to only the impacted clients. Having completed configuration management in a previous role, selecting an incorrect setting can negatively impact an organisation. Additionally, I'm keeping track of all the environmental changes should a role back be needed. Documentation on troubleshooting is also being created to ensure that if the issue reoccurs, there will be less time spent investigating the matter. The decision was made to go to basics on this install and increase functionality as we proceed, given that the root cause is not determined. While also working on the above issue around alerting, an additional change was made at a project level which impacted my ability to access the environment. Investigations were that no policy changes had been made, so the root cause was that something had changed from a software endpoint level. Time was spent between my team and the vendor in trying to diagnose the issue. Ultimately, it turned out to be an internal change made at a policy level rather than a vendor level.

Items learned this month –

- Decision on the topic of choice for masters
- Importance of Change Management Processes
- Defender Alerts investigation
- SEPM Troubleshooting
- Project kick-off on ESA Cloud Migration

Employer comments

Gearóid has suggested that he could lead the work piece around our ESA migration from the on premise solution to cloud. He has shown initiative and has previous experience involving system releases. I am happy for him to lead this work piece and will provide any support where required.

Student Signature: Gearóid Kelly
Industry Supervisor Signature: Declan Byrne

Month 4 May – June

Internship Month

Having fully discussed and chosen the topic, I have started to document and complete the literature review. The chosen topic is around migration from an on-premise email filtering application to a cloud-based application in addition to this. It is recording and documenting this from a master's perspective – A challenge in itself as it is more practical than a typical research project. However, I created a plan on which the overall document will take format –

Overview – 91% of cyber-attacks begin with an email Cybercriminals are targeting multiple organisations across the globe every x seconds. These statistics provide an insight into how organisations can remain vulnerable to attack. Working within the critical network infrastructure, the upkeep of mail filtering tools provides one defence barrier to an organisation. While it is not the only defence mechanism used by organisations, it is one of the entry barriers that potential cyber criminals can use to infiltrate an organisation's security controls.

Literature Review -

- Get Metrics on mail traffic in and out of the organisation.
- Managing the project on Migration of an On-Prem Appliance to Cloud-Based Client
- Advantages and disadvantages of on-prem vs moving to cloud-based infrastructure.
- Further metrics on IT Projects and Cyber input with privacy by design and adhering to regulations.

The implementation and upgrade of a platform are much more than a plug-and-play scenario. There are processes to be adhered to alongside policies and governance controls to be input.

Artefact/Product development –

- Overview of Project Lifecycle
- Identification of Stakeholders
- Review with Stakeholders

- Planning of the implementation
- Review of the Go live project plan
- Market place product offerings and how they protect an organisation.

Evaluation

Review of ESA Implementation
Review of Environment health check completed – Prior Health Check – Migration Health Check – Post Migration Health Check.

Configuration Manual –

Diary of additional work completed
Project plans and documentation of the project
References and Reports on Email Security appliances

In addition to the above, from a project perspective, I have carried out the following –

Health check on the environment – A health check was due on the environment – Completing this check allows for a view of the current state of the environment and then looking at the future state of the environment depending on the results.

Employer comments

Gearóid has worked alongside our Vendor and Stakeholders to identify all aspects of the Migration to cloud. He has presented the outputs of the Environmental health check to our Management team. Alongside this he has also implemented some of the recommendations. Gearoid continues to upskill and gain knowledge across the team.

Student Signature: Gearóid Kelly
Industry Supervisor Signature: Declan Byrne

Month 5 June – July

The focus over the past month has been working on the overall deployment and completing the research-style paper. This task was difficult given the general difference between a research-based paper and one practical and hands-on one. Research papers are more tailored to a research-based question versus completing project work. In addition, the documentation available from an NCI was geared primarily at research-based over industry placements. I found this a significant challenge in structuring and creating the paper topic. I elected to tailor the project plan to be a research-based paper to the best of my ability. However, it still was made with the project plan and lifecycle.

Configuration Manual

The configuration manual contains project-level items created and worked on as part of migrating from on-prem to cloud. It also features aspects of the environmental health check.

Deployment/ Migration Plan -

This section contains the documentation and plans created by Gearóíd Kelly. The plans have been created and developed by me. Some minor aspects of information have been input by other teams across the cyber landscape. I have also removed individual names to protect identities and ensure confidentiality. The deployment document contains various subsections, and the sub is the document which was created for the tracking and status updates of the project.

Deployment Plan

Date for Completion	Action	Responsible Company	Responsible Person	Status	Comments
	Preparation				
	Risk Assessment Form Completion	XXX	XXX	Complete	In Progress - Awaiting greenlight from Risk Assessment
	Account Set up within Vendor Cloud	XXX	XXX	Complete	Accounts set up for local users - SSO to follow
	Export Current User List for Migration	XXX	XXX	Complete	
17/06/2022	Confirm Production Upgrade with Software Vendor	XXX	XXX	Complete	**Go Live Plan Shared with Vendor**
20/06/2022	Call to Discuss Business Department Mail Domain	XXX	XXX	Complete	

28/06/2022	**Health Check on Environment - MSM 566468**	XXX	XXX	Complete	To be implemented on 27/06/2022
29/06/2022	**SOC SIEM Integration**	XXX	XXX	WIP	Not on the critical path
29/06/022	**SSO Implementation**	XXX	XXX	WIP	
22/06/2022	**Security Architecture Sign Off**	XXX	XXX	WIP	
22/06/2022	**Firewall/ Networks Review**	XXX	XXX	Planned	
22/06/2022	**Implement IP Restriction on Cloud Environment**	XXX	XXX	WIP	Email sent to IPNS To request IPs
21/06/2022	Raise the Change ticket with Change Management	XXX	XXX	Complete	MSM - CHG-568332
	SOFTWARE VENDOR Configs - Daily Call for Config and Implementation	XXX	XXX	Complete	
01/07/2022	Schedule Knowledge Transfer - Sec Ops	XXX	XXX	Planned	
01/07/2022	Schedule Knowledge Transfer - CATS	XXX	XXX	Planned	

30/06/2022	Schedule Exit Report Meeting - Before Go Live	XXX	XXX	Planned	
20/06/2022	Clean Period of No Config Changes in Environment - Issue notifications to the team	XXX	XXX	Complete	

Test Plan –

The test plan has been created and is currently a live working document. The criteria around this test plan are it is kept at a high level of the process. These are critical path tests. There is a blocker on proceeding if any of these fail in testing.

Testing of Mails	**Team Dependencies**	**Criteria**	**Acceptance Criteria**	**Result**
Pre Requisites				
Environment Configured	Cyber Ops/	The environment must be configured with the configuration of the on Prem Solution	Configuration replicates on Prem	
SSO Implemented	Cloud Desk	SSO must be implemented, and users successfully logging in via Microsoft AD	SSO is visible on the landing page of the Vendor	Pass
Successful Log into Environment	Cyber Ops	Users can log into the environment	Users can log into the environment via ESB SSO	Pass
Configuration Review Completed	Cyber Ops/	A review of the Cloud Configuration must be completed with both parties	Both Parties review and sign off on Configuration	
Test Domain Configured between Environments	Cyber Ops/ Exchange Team	The linkage between our cloud domain and Mail servers must be completed	ESB Mail Exchange and Software Vendor Cloud have been integrated	Pass
Mail Traffic Test	Cyber Ops/ Exchange Team	Test Traffic must be transported between Cloud and ESB Mail Domain	An external mail sent to a test ESB Domain travels through Vendor and is successfully delivered	Pass

Content Filter Tests	Cyber Ops	Testing of Content Filters and Spam Creation - Choose various content filter terms and include these in the subject or body of the mail.	Fraudulent emails are either dropped or blocked by Vendor	Pass
Mail Policy Tests	Cyber Ops	Testing of Mail Policies Choose various Policy terms and include these in the subject or body of the mail.	Fraudulent emails are either dropped or blocked by Vendor	Pass
Dictionary Test	Cyber Ops	Testing Of Dictionaries - Choose various dictionary terms and include these in the subject or body of the mail.	Fraudulent emails are either dropped or blocked by Vendor	Pass
Test Domain failover Test	Cyber Ops/ Exchange Team	Creation of a failover scenario	If the delivery of the mail fails on Cloud, it should failover to the on-prem solution with the configuration of MRX Records	
Mass Email being Sent				
Internal Mails being Sent				
Run through of General Environment Procedures	Cyber Ops	All general health check tasks and environment maintenance are carried out on the environment - EG Content Filters - Dictionaries- the sender- Subject - IP Blocks	Users can successfully maintain and support the environment	
IP Restriction Implementation	IPNS/ Cloud Desk/ Software Vendor	A user can only log into the environment over the ESB Network	A user cannot reach the landing page outside of the ESB Network	

RAG Status

Overall High Level for reporting to Management. This is completed at a higher level than the above deployment plan

25/06/2022	Complete Health Check Tasks in MSM 566468	Complete	25/06/2022
25/06/2022	Configure Vendor Cloud	On Schedule	25/06/2022
01/07/2022	SSO Implementation	Complete	01/07/2022
01/07/2022	SOC/ SIEM Integration	Delayed	01/07/2022
01/07/2022	Review Cloud Configuration	On Schedule	01/07/2022
01/07/2022	Testing of SSO	Delayed	01/07/2022
01/07/2022	IP Restriction Review	Delayed	01/07/2022
08/07/2022	Training in Cloud Environment	Complete	01/07/2022
08/07/2022	Document of Process Changes	Complete	01/07/2022
15/07/2022	**Testing of Features**	Complete	15/07/2022
22/07/2022	Training / KT With Staff	On Schedule	19/07/2022
22/07/2022	Testing Documentation Review	On Schedule	19/07/2022
22/07/2022	Email Migration Plan	On Schedule	19/07/2022
22/07/2022	Go - No Go and Review of Schedule	On Schedule	18/07/2022
29/07/2022	Production Migration	On Schedule	29/07/2022
	Outgoing Mails Configs		

Deployment Plan*

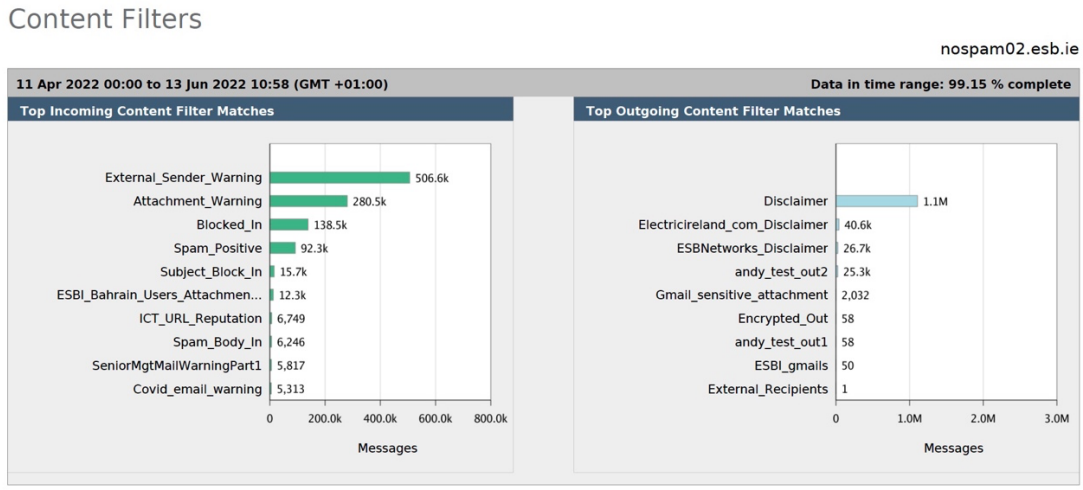
The deployment plan is only for live email domains. All other aspects have already been completed within the configuration and testing phase.

25/07/2022	**Migrate @ESBENERGY.CO.UK Domain -**	**ESB/Vendor**
	Update Configurations for Migration	Vendor
	Hyper care Monitoring	ESB
	All tasks above complete	ESB
	Validation	
26/07/2022	**Migrate @esbnetworks.ie Domain**	
	Update Configurations for Migration	ESB
	Hyper care Monitoring	ESB
	All tasks above complete	ESB
27/07/2022	**Migrate @esbI.ie Domain - 189 Users**	
	Update Configurations for Migration	
	Hyper care Monitoring	
	All tasks above complete	
28/07/2022	**Migrate @esb.ie Domain**	
	Update Configurations for Migration	
	Hyper care Monitoring	
	All tasks above complete	

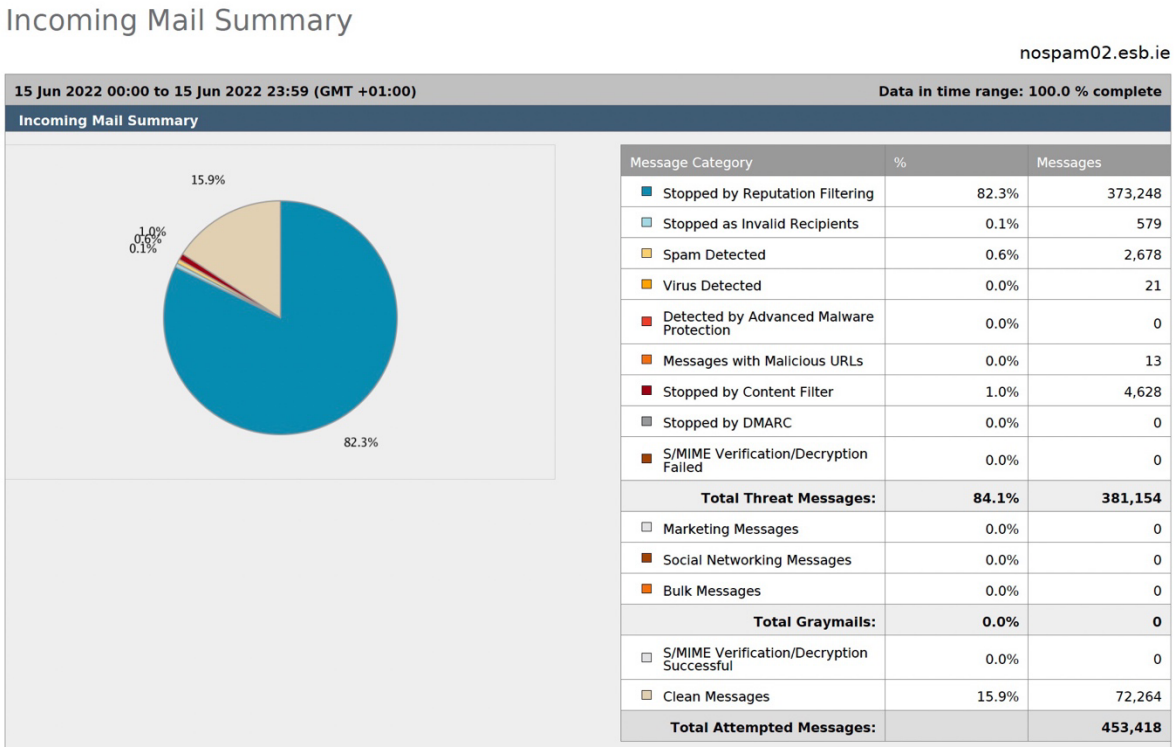
Health Check Documents –

The software appliance could generate system reports. These reports formulated the basis of the testing plan and environmental health checks and maintenance. Some of the screenshots are withdrawn from the reports with a brief explanation –

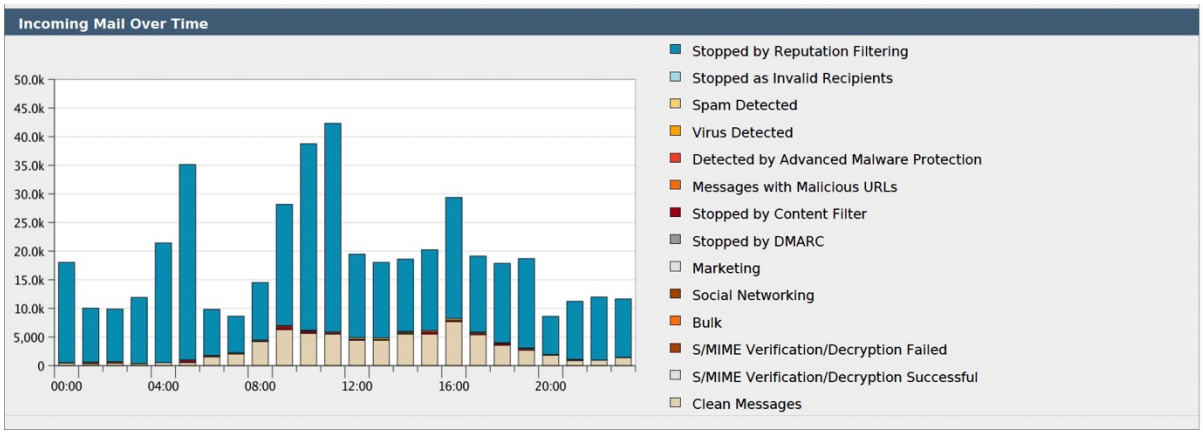
Content Filters –
The term Content Filters is broad ranging in terms of our application and can be attributed to both inbound and outbound emails -



Incoming Mail Summary –
As part of the migration, we must ensure that all aspects of migrating from on-premise to Cloud will remain the same. The report of incoming emails provided some metrics on what we needed to ensure would be configured as part of the migration.



Message Category	%	Messages
Stopped by Reputation Filtering	82.3%	373,248
Stopped as Invalid Recipients	0.1%	579
Spam Detected	0.6%	2,678
Virus Detected	0.0%	21
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	0.0%	13
Stopped by Content Filter	1.0%	4,628
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**84.1%**	**381,154**
Marketing Messages	0.0%	0
Social Networking Messages	0.0%	0
Bulk Messages	0.0%	0
Total Graymails:	**0.0%**	**0**
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	15.9%	72,264
Total Attempted Messages:		**453,418**



Test Evidence

The purpose of this document is to summarise the testing conducted during the migration of the Email Filtering Tool On-Premise to the Cloud Application.

Application Overview

This project aims to move from Email Filtering Tool On-Premise to Email Filtering Tool Cloud. Email Filtering Tool is the Mail Filtering Application for ESB. It filters both Inbound and Certain outbound Mail Filtering

Scope of Testing

In Scope

This section details the items which are in scope for testing.

- SSO Implemented
- Successful Log into Environment
- Configuration Review Completed
- Test Domain Configured between Environments
- Mail Traffic Test
- Content Filter Tests
- Mail Policy Tests
- Dictionary Test
- Test Domain failover Test
- Mass Email being Sent
- Internal Mails being Sent
- SOC SIEM Integration

Out of Scope

The following have been deemed out of scope for this project.

- Implementation of new feature sets as a result of Cloud Migration
- X Mail Domain

Items not tested

The below test cases were not tests as they were not possible to execute in the Cloud Environment:

- Mass Emails incoming to Cloud Environment

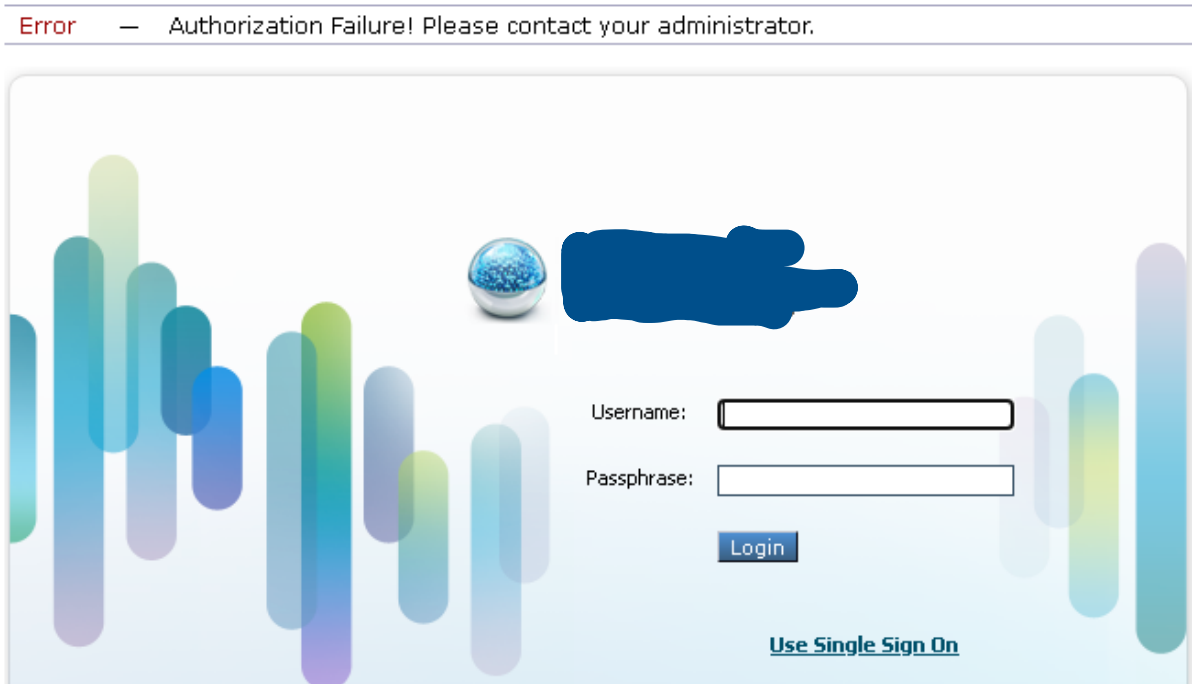
Test Execution Evidence

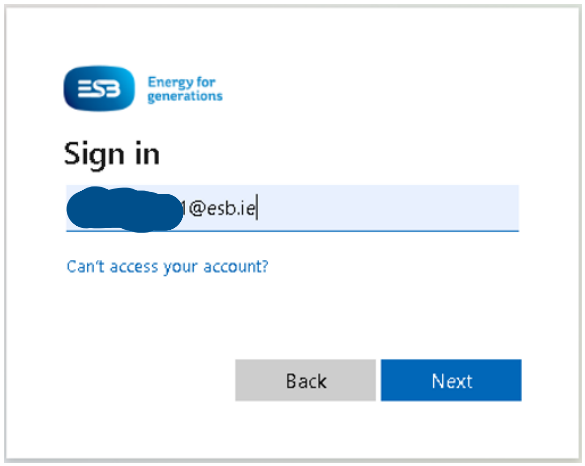
Please find a summary of Test Evidence below

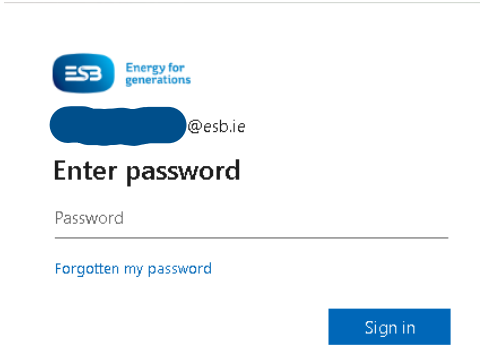
Testing Screenshots

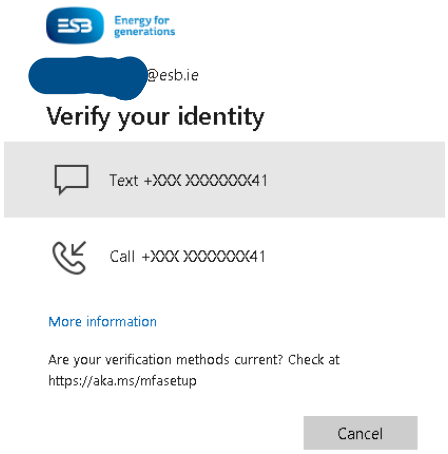
SSO Testing –

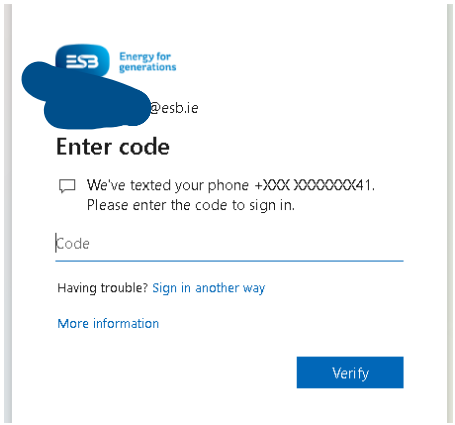
Log in outside of AD Group –



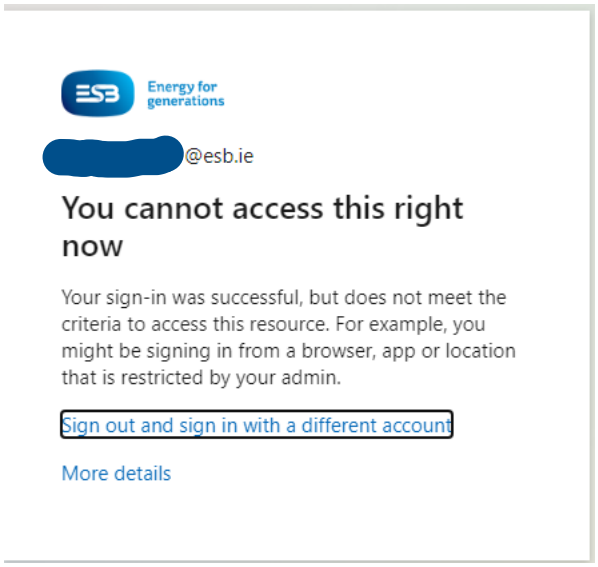




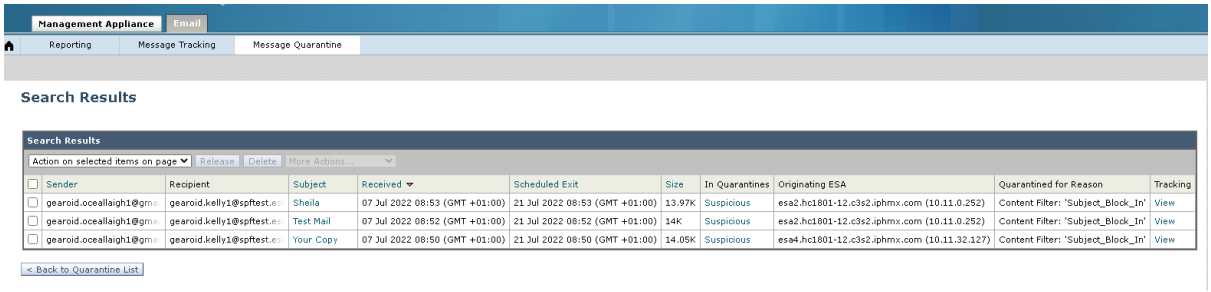




Log in outside of ESB LAN –



Testing of blocked Subjects -



Test Execution Results

This section details the test execution results –

All Test Scenarios have been tested and are in a status of passed. However, during the testing process, several issues were encountered.

Defects and Issues Encountered

Defect

One* Defect on SSO – Single Sign-on was misdirecting. The vendor resolved this With fix CSCwc22821

Issues

- Issues encountered with Dictionaries. Certain aspects of Dictionaries failed to load during the migration process. This was due to Special Characters.

- Text Resources did not upload – Fix to upload Text Resources manually
- Content Filters Testing – Expected behaviour was that when the Profanity Subject Criteria were tested, the emails being sent would be blocked and not forwarded to the end user. Instead, emails with profanity in the subject and body are being delivered to the end user. Upon investigation, it was determined that this is expected behaviour with the current configuration. Therefore, this has been added to the future improvement plan.

Conclusion

This document contained a broad range from the day-to-day work experience diary to the base level configuration manuals and test information. All the information contained within the document was created with permission from ESB. The names of systems have been removed; however, a general explanation has been provided.