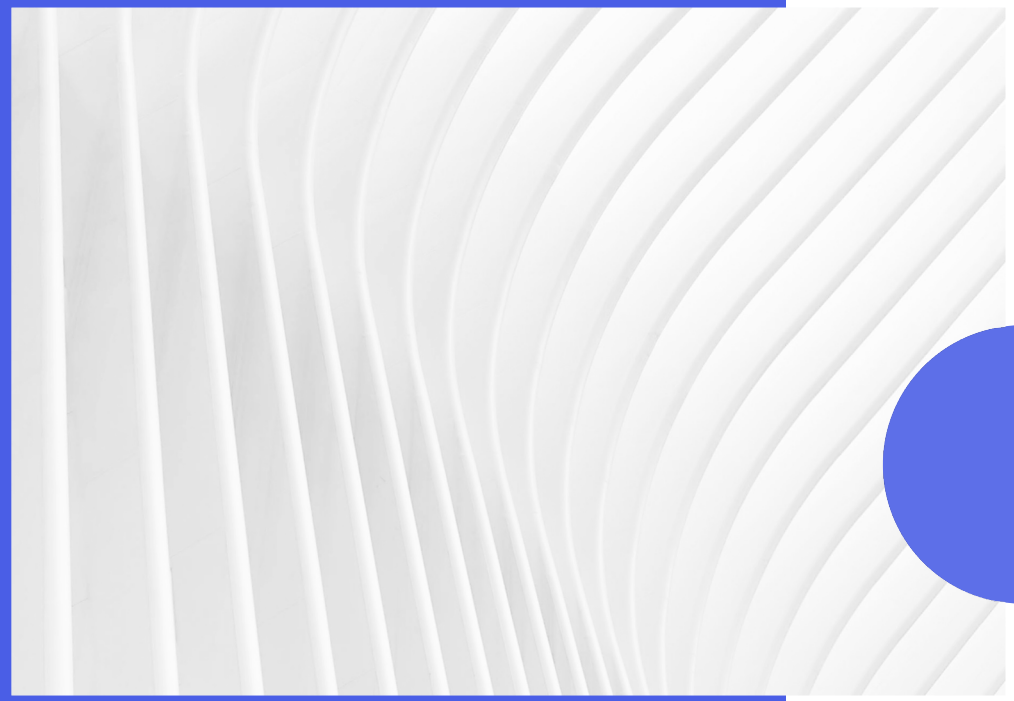
HANDOVER PRESENTATION

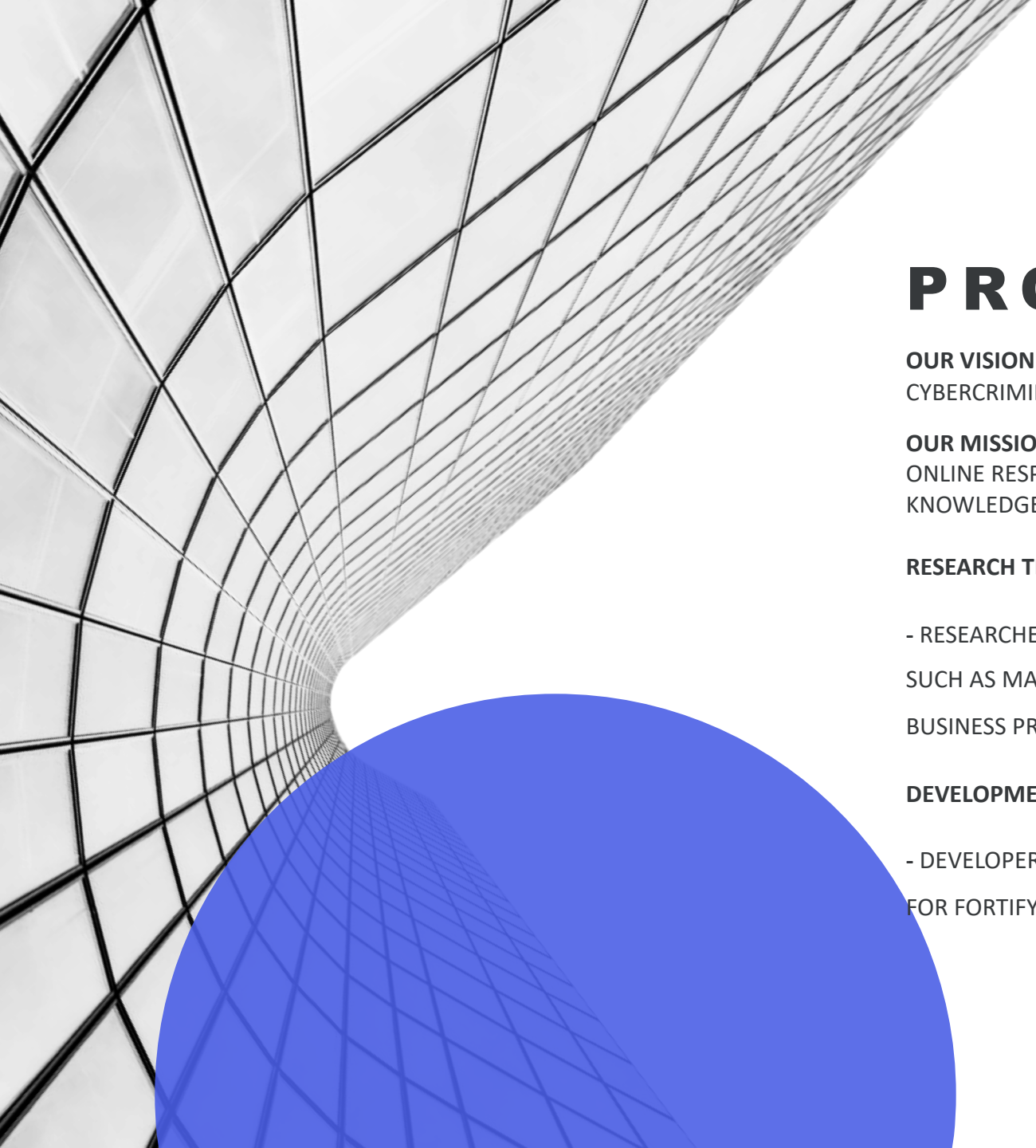
FORTIFY

TRIMESTER 3 2022

WHO ARE WE



Fortify is a non-for-profit online platform which aims to bridge between underrepresented organizations and volunteering experts who will provide industry-standard cybersecurity services. Fortify works together with graduates and other IT professionals looking to build a stronger digital infrastructure for clients. By doing so, we create a range of employability opportunities and a resilient digital community.



PROJECT STRUCTURE

OUR VISION - A WORLD WHERE WE CAN USE WHITEHAT VOLUNTEERS TO COMBAT CYBERCRIMINALS.

OUR MISSION - TO ENSURE SMALL ORGANISATIONS BECOME MORE AWARE ABOUT THEIR ONLINE RESPONSIBILITIES AND ARE GIVEN ACCESS TO RELEVANT SERVICES AND/OR KNOWLEDGE.

RESEARCH TEAM

- RESEARCHERS MAIN TASK IS TO GATHER AND ANALYSE DATA ABOUT STRATEGIC ACTION ITEMS SUCH AS MARKETING, BUSINESS OPERATION AND CLIENTELE REQUIREMENTS TO PLAN THE BUSINESS PROCEEDINGS.

DEVELOPMENT TEAM

- DEVELOPERS MAIN TASK IS TO RESEARCH AND DEVELOP THE TECHNICAL SOLUTIONS NEEDED FOR FORTIFY'S OPERATION SUCH AS DESIGNS, WEBSITE AND DATABASE.

GOALS ACCOMPLISHED THIS TRIMESTER

RESEARCH TEAM

- Built an assessment system for volunteers/companies that will be used to assess the skills of a volunteer and organisational needs of a company.
- Created a business plan that show cases all business proceedings of Fortify and plans for the future.
- Created email templates, feedback post-op system and refined the marketing/advertising strategy.

Development team

- Updated the existing website designs and mock-ups.
- Create a plan on how to build a website and a database in a secure manner.
- Started developing the website the React Stack and adding the functionality.

CONFIDENTIAL

FORTIFY

Connect, Assess and Secure

BUSINESS PLAN

Trimester 3, 2022

TABLE OF CONTENTS

Executive Summary

The Fortify project is an innovative initiative that provides a work-integrated volunteering opportunity for graduates, students and IT professionals and connects them to small businesses and non-profit organisations that do not have the adequate resources to effectively manage their cybersecurity risks. Fortify facilitates and monitors the volunteer-company cooperation by creating the platform for the clients, setting clear guidelines for the volunteers and oversighting the process of collaboration. Fortify aims to fill the gaps in the labour and IT market by giving the volunteers an opportunity to build valuable experience to raise their employability, and by giving small organisations a hand in building their cyber security strategy. This report aims to serve as an outline of intentions, i.e., a plan for the near and distant future of Fortify, with an explanation of means and methods of action to achieve the assumed goals. This paper presents a market analysis that assesses the business idea and serves as the baseline for the creation of informed business decisions, utilising a SWOT analysis and survey data analysis. The technical part of the report aims to clearly describe the required organisational structure of Fortify - consisting of roles, teams and employees - that is essential in the long-term planning of the company. Operational procedures in the report serve as a description of the business operations - from start to finish - with justifications of the chosen methods. The report will describe the market and production milestones to clarify the long-term goals of Fortify.

CONFIDENTIAL - DO NOT DISSEMINATE. This business plan contains confidential, trade-secret information and is shared only with the understanding that you will not share its contents or ideas with third parties without the express written consent of the plan author.

Security Assessment - Technical Controls

*Q1 - Do you/your organisation control who and how software is installed and managed on your devices?

Choose from the dropdown

*Q2 - Do you check of out-of-date unsupported version of your application/software and update on a defined regular basis?

Choose from the dropdown

*Q3 - Has your organisation Disabled Microsoft Office macros in documents, spreadsheets and other Office products?

Choose from the dropdown

*Q4 - Does your organisation have centralised access to identify and/or disable Web Application CVEs (Common Vulnerabilities & Exposures)?

Choose from the dropdown

*Q5 - Does your organisational structure limit system and data access only to authorised members?

Choose from the dropdown

*Q6 - Do you have an update/patching schedule for your Operating Systems (e.g. Windows), Servers and back-end systems?

Choose from the dropdown

*Q7 - Do you have basic secure processes in place to authenticate who is trying to login?

Choose from the dropdown

*Q8 - Do you keep a record of all data using correct naming conventions and dates to be accessed when neccesary?

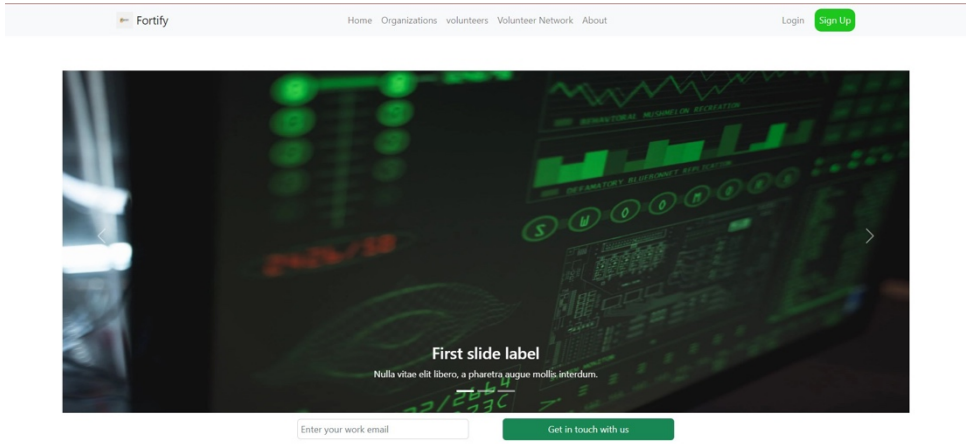
Choose from the dropdown

Continue ›

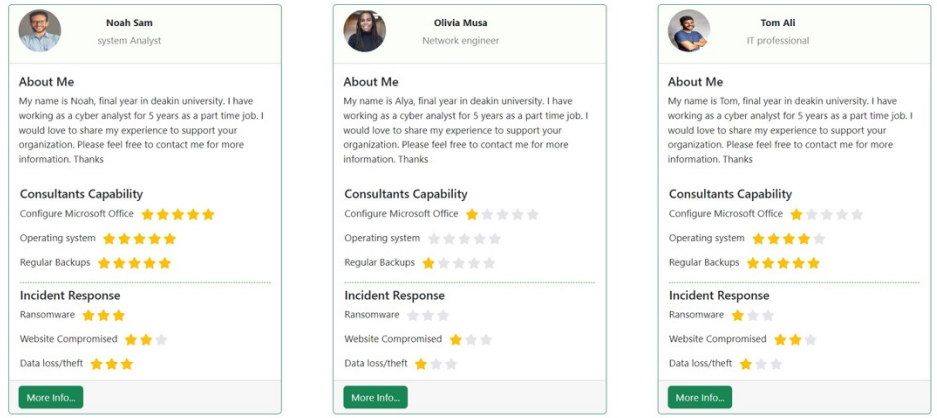
Organisation Self-Assessment

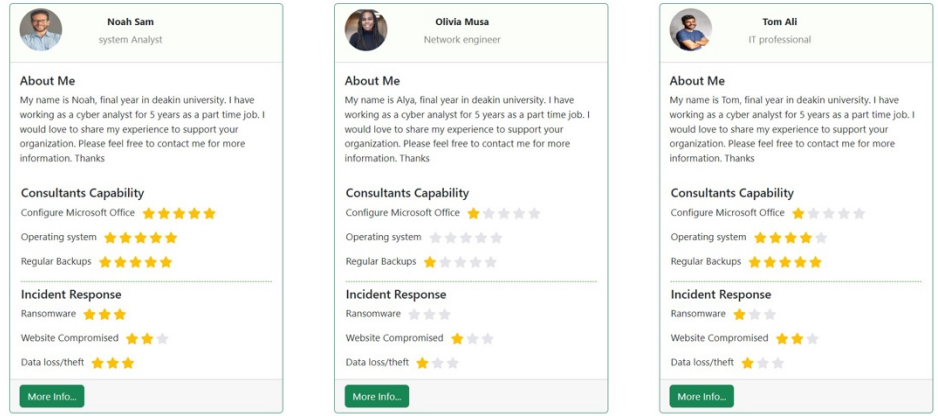
Volunteer/Consultants Assessment

User/Customer based on Essential 8 maturity levels - Environment hardening & Incident Prevention "Technical Controls"			Organisation Self-Assessment Maturity level 0 - 3	Fortify confirmed Maturity level 0 - 3	Volunteers/Consultants Capability/Skill levels - for hardening the environment "Fortify" and prevent incidents		Skills Self Assessment - Skill level 0 - 3	Fortify confirmed Skill level 0 - 3
Technical Control Description	Maturity Level Descriptor	Level			Required Skill	Skill Level description		
Application control - Q1 - Do you/your organisation control who and how software is installed and managed on your devices?	Maturity Level 0: No, we have limited knowledge on this and everyone can install and run applications/software on devices	0	Level 2		Application Control - Ability to configure user access rights centrally managed by group policy	Skill Level 0 I have limited Skills in this area	0	
	Maturity Level 1: We prevent executable software to be downloaded and installed in any of the organization's devices	1				Skill Level 1: Microsoft AD administrator skills with the ability to set group policies	1	
	Maturity Level 2: We can do all described in Level One plus: We can control all applications centrally within a pre-approved set that can be installed by users; We also log 'allowed' and 'blocked' application executions on workstations and internet-facing servers.	2				Skill Level 2: Skill Level 1 plus: Azure AD administrator capabilities as well as on-premises DC/AD administrator. Ability to set policies to ensure applications are installed and run in workstations or systems infrastructure environments. Ability to manage and control devices centrally including applications management utilising administrator tools such as Microsoft Intune to configure Windows Defender Application Control (WDAC), and other 3rd party tools such Ivanti Application Control Management.	2	
	Maturity Level 3: We can do all described in Level One & Level Two plus: Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set.' Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	3				Skill Level 3: We can do all described in Level One & Level Two plus: Ability to monitor and restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an 'organisation-approved set managed for organisation's portal software centre Ability to configure Microsoft's 'recommended block rules 'and Microsoft's 'recommended driver block rules. Ability to validate application control rulesets. Ability to configure the 'allowed and blocked' executions on workstations and servers and enable a centrally managed log which is protected from unauthorised modification and deletion. Ability to monitor for signs of software compromises, and actioned when cyber security events are detected.	3	
Patch applications - Q2 - Do you check of out-of-date unsupported version of your application/software and update on a defined regular basis?	Maturity Level 0: No, we have limited knowledge of this and have not been updating our applications, software or drivers to the latest versions	0			Patch Applications - Ability to work with application vendors and ensure latest software versions are installed and maintained including patching and vulnerability management.	Skill Level 0 I have limited Skills in this area	0	
	Maturity Level 1: Patches, updates or vendor mitigations for security vulnerabilities in Internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in Internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	1				Skill Level 1: Ability to run application patches based on vendors advisory espectally for security vulnerabilities. Ability to implement a mechanism and schedule as to ensure the patching of Internet-facing services/applications are applied within two weeks of release, or within 48 hours if an exploit exists as per advises from vendor vulnerability posts. Have a goof understanding of Microsoft Office productivity suites, web browsers and their extensions, email clients, PDF software, and security products and how vulnerability advisory are distributed by the vendors. Ability to run vulnerability scanners such as Rapid7, Qualys and Tenable.io and use these tools identify missing patches or updates for security vulnerabilities in Internet-facing services. Ability to run vulnerability scanner to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	1	
	Maturity Level 2: All of Level 1 plus: A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.	2				Skill Level 2: All of Level 1 plus: Ability to run a vulnerability scanner and configure a scheduled usage to scan at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications including bespoke software, Service accounts and APIs.	2	
	Maturity Level 3: All of Level 1 and Level 2 plus Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists. Applications that are no longer supported by vendors are removed.	3				Skill Level 3: All of Level 1 & 2 plus. The ability to upgrade or remove systems and applications that are no longer supported by vendors. This includes ability of technical and non-technical change management.	3	
Configure Microsoft Office macro settings - Q3 - Has your organisation Disabled Microsoft Office macros in documents, spreadsheets and other Office products?	Maturity Level 0: No, we have limited knowledge on this and have not been disabled macros in Microsoft Office products	0			Configure Microsoft Office Macro Settings - Microsoft Office macros in documents, spreadsheets and other Office products are disabled	Skill Level 0 I have limited Skills in this area	0	
	Maturity Level 1: Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the Internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macro security settings cannot be changed by users.	1				Skill Level 1 Knowledge and ability to configure Microsoft Office suite and how to disable macros settings Ability to configure email and firewall filtering to block Microsoft Office macros in files originating from the Internet. Ability to configure and enable Microsoft Office macro antivirus scanning. Ability to configure admin privileges and by default disable Microsoft Office macro security settings and ensure that they cannot be changed by users.	1	
	Maturity Level 2: All of Level 1 plus: Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are logged.	2				Skill Level 2 All of level 1 plus: Ability to configure Win32 API calls so Microsoft Office macros are blocked. Ability to establish a loggin systems for 'Allowed and blocked' Microsoft Office macro executions and ensure that they are logged.	2	
	Maturity Level 3: All of Level 1 and Level 2 plus Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute. Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations. Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	3				Skill Level 3 All of Level 1 and Level 2 plus: Ability to configure a sandbox environment to run Microsoft Office macros for testing purposes. Ability to allowed executable micros by establishing a Trusted Location or by provisioning digitally signed certificates by a trusted publisher for the micro. Ability to establish a group policy so that only privileged users are able to validate Microsoft Office macros and can test macros for malicious code. The trusted users will be able to write to and modify content within Trusted Locations. Be able to configure Microsoft Office environment so macros that are digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. Ability to establish loggin service where 'Allowed and blocked' Microsoft Office macro executions are logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.	3	


Fortify
Home
Organizations
volunteers
Volunteer Network
About
Login
Sign Up
First slide label
Nulla vitae elit libero, a pharetra augue mollis interdum.
Enter your work email
Get in touch with us


FEATURES
Get free help from certified cyber security experts
our experts are specialized in ....
Cyber Awareness Training
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Possimus, repudiandae!
Consulting
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Possimus, repudiandae!
The Third Service
Lorem, ipsum dolor sit amet consectetur adipisicing elit. Possimus, repudiandae!


Noah Sam
system Analyst
About Me
My name is Noah, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...
Olivia Musa
Network engineer
About Me
My name is Alya, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...
Tom Ali
IT professional
About Me
My name is Tom, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...


Noah Sam
system Analyst
About Me
My name is Noah, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...
Olivia Musa
Network engineer
About Me
My name is Alya, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...
Tom Ali
IT professional
About Me
My name is Tom, final year in deakin university. I have working as a cyber analyst for 5 years as a part time job. I would love to share my experience to support your organization. Please feel free to contact me for more information. Thanks
Consultants Capability
Configure Microsoft Office
Operating system
Regular Backups
Incident Response
Ransomware
Website Compromised
Data loss/theft
More Info...

DELIVERABLES FOR NEXT TRIMESTERS:

- Develop a mentoring programs.
- Create a list of technical solutions based on Essential 8.
- Create a system to encrypt the communication between the volunteer and the organisation to protect the client and to maintain a duty of care by the volunteer.
- Incorporate the mock-ups into the website.
- Continue the development of the website.