**PROJECT PLAN SCOPE**

| **PROJECT NO.** | **DATE SUBMITTED** |
| --- | --- |
| 23220-RIJJ | 19/04/2024 |
| **PROJECT OBJECTIVES** | |
| The Project aims to implement the development ,execution,evaluation and documentation of a prototype CSOC infrastructure for SMEs both in Virtualized and physical environments. Testing of the operations and documentation of the operations will be carried out. | |

## Step 1. Project Deliverables

| **DELIVERABLE NO.** | **DESCRIPTION** |
| --- | --- |
| 1 | Initial System Configuration: the configuration of the network that will be set up initially. |
| 2 | Prototype System Configuration: the configuration of the network that will be used to test updates or tweaks before being pushed to production. |
| 3 | Production System Configuration: the running configuration of the network that will be used. |
| 4 | Tech documentation: documentation of the networks infrastructure, what software and hardware is being used. |
| 5 | Project Management Documentation: all documented files that describe the plan and progress of the project. |
| 6 | Result Documentation: the documentation of the results of the project. |
| 7 | Presentation: a presentation describing the process, and results of the project, to be presented to the stakeholders. |

## Step 2. List of Project Tasks

## Project Tasks

*Alternatively, you can attach your work breakdown structure (WBS) to the scope statement.*

| **Work breakdown structure (WBS) attached** | | **NO** | **X** | **YES** |  |
| --- | --- | --- | --- | --- | --- |
| *Provide a link, if applicable.* | **N/A** | | | | |

| **TASK NO.** | **DESCRIPTION** | **FOR DELIVERABLE NO. …**  **ENTER TASK #** |
| --- | --- | --- |
| 1 | Planning to set up a CSOC Centre |  |
|  | * Setting up initial Lab environment * Setting up prototype environment * Setting up production environment * Testing the CSOC * Evaluation and Project submission * Standup meetings and Minutes of meeting on regular basis and documentation | 1 |
| 2 | Setting up initial lab environment | 1, 2 |
|  | * Setting up Windows server,clients,KaliPurple,Switch and Palo Alto Firewall * Standup meetings and Minutes of meeting |  |
| 3 | Setting up prototype environment | 1,2 |
|  | * Assign IP addresses for devices * Configure and setup interfaces and zones in PaloAlto firewall * Install VM and set up Virtual networking with firewall * Install Kali purple * Standup meetings and Minutes of meeting |  |
| 4 | Setting up production environment | 1,2,3 |
|  | * Install windows clients and server * Integrate firewall into KaliPurple SIEM * Setting up DMZ web server * Standup meetings and Minutes of meeting |  |
| 5 | Testing the CSOC center networking | 2,3,4 |
|  | * Configure and test domain user accounts and domain group policies * Configure and test management VLAN * Configure and test WAN to DMZ security and NAT Policies * Configure and test domain DNS forwarding * Test firewall to access DMZ server from internet Zone * EStablish network security baselines * Test RBT activities * Implement SSL decryption * Standup meetings and Minutes of meeting |  |
| 6 | Evaluation and Project submission | 3,4,5 |
|  | * Evaluate the performance of the CSOC based on the test results * Update your findings * Submit the project upon successful completion as presentation to the stakeholders |  |

## Step 3. Out of Scope

| This project **will NOT accomplish or include** the following: | * UDP filtering |
| --- | --- |

## Step 4. Project Assumptions

| **NO.** | **ASSUMPTION** |
| --- | --- |
| 1 | List any project factors that you consider to be true, real, or certain. |
| 2 | Assumptions generally involve a certain degree of risk. |
| 3 | Describe the potential impact of assumptions should they prove to be false. |

## Step 5. Project Constraints

| **PROJECT START DATE** | 16/04/2024 |
| --- | --- |
| **LAUNCH / GO-LIVE DATE** | 24/05/2024 |
| **PROJECT END DATE** | 30/06/2024 |
| **LIST ANY HARD DEADLINE(S)** |  |
| **LIST OTHER DATES / DESCRIPTIONS OF KEY MILESTONES** | * Setting up and connecting our internet infrastructure: Palo firewall, Win Domain controller, Kali machines, Switch, and LAMP DMZ * Setting up Virtual environment * Configure Kali purple with SSH, RDP, Console for remote management * Set up Kali purple SIEM with elastic stack * Implementing Fleet Server and Endpoint protection * Configure Firewalls into the SIEM * Setting up the DMZ webserver * Establish a Net Security baseline with ASD essential 8 and app control + Backups |
| **BUDGET CONSTRAINTS** | With a team of 4 working 9 hours a week, over 12 weeks, each getting paid $40 an hour. It should end up costing around $18,000 with no overtime. |
| **QUALITY OR PERFORMANCE CONSTRAINTS** | One major constraint we have is to ensure our project meets at least Maturity Level One in the [ASD’s Essential 8](https://www.cyber.gov.au/sites/default/files/2023-11/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28November%202023%29.pdf): Briefly, this will mean the applications must be scanned with an up to date vulnerability scanner, daily. The vulnerability scanner must also scan the Operating system to identify missing patches regularly. MFA must be used to authenticate users. Restrictive administrator privileges, which follow the principle of least privilege. Application Control methods. Microsoft Office Macros being disabled for those who don't need it, and Macro antivirus scanning implemented. User application hardening including Internet Explorer 11 being disabled and regular backups of the network and data. |
| **EQUIPMENT / PERSONNEL CONSTRAINTS** | We will need to have adequate personal storage for the VDI files, we will need to have sufficient knowledge in the theory and technology behind this project such as networking, network security, and pentesting experience. A personnel restraint would be the fact that the time to do it in class is 3 days a week and we need access to the switch there to get things done. |
| **REGULATORY CONSTRAINTS** | We need to follow the Australian Signals Directive’s Essential 8 and reach maturity level one. As well as ensuring all Personally Identifiable information is properly handled to comply with Australia’s Privacy act of 1988 |

## Step 6. Updated Estimates

| **Estimate the hours required to complete the project.** | 99 Hours (11 weeks with 9 hours working each week, 396 if you want to include that there will be 4 of us working on it) |
| --- | --- |

## Step 7. Approvals

| **STAKEHOLDER NAME & TITLE** | **ROLE OF STAKEHOLDER / APPROVER** | **DATE SUBMITTED FOR APPROVAL** | **DATE APPROVAL RECEIVED** |
| --- | --- | --- | --- |
| Steve Gale | Product owner | 28/04/2024 |  |
| Steve Gale | Product owner | 26/05/2024 |  |
| Steve Gale | Product owner | 16/06/2024 |  |
| Steve Gale | Product owner | 28/06/2024 |  |
|  |  |  |  |