Project: METAL SNAKE

Resource Plan

Project Sponsor: Brendan Gasparin

Project Manager: Brendan Gasparin

Date of Project Approval: 14/08/2024

Commencement Date: 29/07/2024

Estimated Completion Date: 24/10/2024

Estimated Project Duration: 17 Weeks

Version: 1.0 (2024-08-23)

1. Executive Summary

1.1 Purpose

The purpose of this Resource Plan is to define and allocate the resources required to complete Project: METAL SNAKE. The plan ensures that human resources, hardware, software, and facilities are available and properly managed to meet the project's objectives of building a secure on-premises cybersecurity lab with web hosting and integrated cloud infrastructure.

1.2. Overview

The project requires a combination of technical expertise, networking hardware, software tools, and facilities to create and maintain the on-premises lab. Key resources include IT and security personnel, Raspberry Pi devices, cloud-based services, and secure facilities for the setup and ongoing operation of the infrastructure.

Table of Contents

Resource Plan 0
1. Executive Summary 1
1.1 Purpose 1
1.2. Overview 1
Table of Contents 2
2. Introduction 3
2.1. Project Overview 3
2.2. Scope of the Resource Plan 3
2.3. Assumptions 3
3. Functional Requirements 4
3.1. Human Resources 4
3.2. Hardware Resources 5
3.3. Software Resources 5
3.4. Facilities and Physical Space 6
4. Resource Allocation 7
4.1. Resource Allocation Schedule 7
4.2. Resource Dependencies 7
5. Resource Budget 8
5.1. Personnel Costs 8
5.2. Hardware Costs 8
5.3. Software Costs 8
5.4. Facility Costs 8
5.5. Contingency Budget 8
6. Resource Risks and Mitigation 9
6.1. Resource Risks 9
6.2. Mitigation Strategies 11
7. Resource Monitoring and Control 12
7.1 Resource Tracking 12
7.2. Change Management 12
8. Approval and Sign-Off 13
9. How To Use This Template ..... **Error! Bookmark not defined.**

2. Introduction

2.1. Project Overview

Project: METAL SNAKE involves setting up an on-premises cybersecurity lab, including a LAMP stack web server, Mautic email automation, and a cloud-based SIEM system for security monitoring.

The project's goal is to reduce reliance on cloud hosting and improve the organization's security posture while providing a replicable solution for others via public documentation.

2.2. Scope of the Resource Plan

This Resource Plan covers all necessary resources for the project, including personnel, hardware, software, and facilities. It outlines resource allocation, scheduling, and budget considerations.

2.3. Assumptions

- It is assumed that all necessary personnel (IT, security, project management) will be available as required.
- Raspberry Pi devices and other hardware will be procured on time.
- Cloud services will remain stable and accessible throughout the project lifecycle.
- Residential users sharing the network will not interfere with business-critical resources.

3. Functional Requirements

3.1. Human Resources

3.1.1. Role Descriptions

As a single person business, the same person will be responsible for all of the following roles:

- **Project Manager:** Responsible for overall project coordination, managing timelines, communication, and resource allocation.
- **IT Team:** Handles hardware installation, network setup, server configuration, and cloud integration.
- **Security Team:** Focuses on security planning, firewall configuration, security testing, and SIEM system integration.
- **Operations Team:** Responsible for maintaining and supporting the system after deployment and handover.

3.1.2. Resource Allocation

- **Project Manager:** 20 hours per week, throughout the project lifecycle.
- **IT Team:** 30 hours per week during the Execution and Testing phases.
- **Security Team:** 20 hours per week during the Planning and Design, Execution, and Testing phases.
- **Operations Team:** 10 hours per week during the Closure and Maintenance phase, ongoing after deployment.

3.1.3. Skills and Expertise

- **Project Manager:** Project management, communication, and resource coordination.
- **IT Team:** Expertise in networking server configuration, Raspberry Pi setups, and cloud services.
- **Security Team:** Proficiency in cybersecurity, firewall configurations, SIEM systems, and penetration testing.
- **Operations Team:** Experience in system monitoring, maintenance, and ongoing technical support.

3.1.4. Resource Availability

[Confirm the availability of resources, noting any constraints (e.g. part-time availability, concurrent project involvement.]

- **Project Manager:** Available full-time.
- **IT Team:** Available part-time (3 days a week).
- **Security Team:** Available part-time (2 days a week).
- **Operations Team:** Available on-demand post-deployment.

3.2. Hardware Resources

3.2.1. List of Equipment

Resources	Procurement
Raspberry Pi 5 B 8GB x 4	Purchase
Raspberry Pi 5 Power Supply x 4	Purchase
Raspberry Pi 5 Official Case x 2	Purchase
Argon NEO 5 Raspberry Pi Case x 2	Purchase
Raspberry Pi Active Cooler x 4	Purchase
Raspberry Pi Keyboard	Purchase
Raspberry Pi Mouse	Purchase
512GB SanDisk MiniSD Card x 4	Purchase
Micro HDMI Cable x 2	Purchase
Wireless Network Adapter x 2	Purchase
USB to Ethernet Adapter x 2	Purchase
External Storage 5TB	Purchase
LAN cables x 5	Purchase
ISP Router	Premises Owners
Intern	Family

3.2.3. Source of Equipment

Raspberry Pis: Purchased from Core Electronics and Pi Australia.

Network Switch and Cables: Network switch already in inventory. Cables purchased from Amazon.

Peripherals: Purchased from Amazon.

3.3.4. Availability

Hardware is expected to be available within 7 days of order placement. Procurement will be done during the Planning and Design phase to ensure timely availability for execution.

3.3. Software Resources

3.3.1. List of Software

- **Operating Systems:** Xubuntu, pfSense, OpenWRT.
- **Server Software:** Apache, MySQL, PHP, Mautic.
- **Security Software:** UFW firewall(?), Fail2Ban(?), OpenVPN(?), cloud-based SIEM system.
- **Cloud Services:** Cloud web server (e.g. Google Cloud or AWS), SIEM system (e.g. Splunk or LogRhythm).

3.3.2. Licenses and Subscriptions

- **Cloud Web Server:** Google Cloud, scalable for client hosting.
- **SIEM System:** Basic subscription for log aggregation and threat detection, upgrading as necessary based on project needs.
- **Open-Source Software:** All other software (e.g. Xubuntu, Apache, MySQL, PHP) is open-source and free to use.

3.3.3. Configuration and Setup

- **Operating Systems:** Pre-installed on microSD cards for all Raspberry Pi devices.

- **LAMP Stack:** Installed and configured on the Raspberry Pi web server, including secure SSL configuration.
- **SIEM System:** Set up for remote monitoring and alerting, connecting to on-premises log sources.

3.4. Facilities and Physical Space

3.4.1. Workspace Requirements

- A secure, climate-controlled room for hosting the on-premises network infrastructure (e.g. Raspberry Pi devices, network switch.)
- Desk space for IT and Security teams to configure and monitor the infrastructure.

3.4.2. Facility Resources

[List any specific facility needs, such as power, cooling, or networking infrastructure.]

Power Supply: Sufficient power outlets and backup power (e.g. UPS) for critical components.

Networking Infrastructure: Broadband Internet connection with static IP for external access, provided by ISP in bridged mode.

4. Resource Allocation

4.1. Resource Allocation Schedule

4.1.1. Resource Gantt Chart or Timeline

4.1.1.1. Initiation Phase

Project Manager: 40 hours

4.1.1.2. Planning and Design Phase

Project Manager: 60 hours

4.1.1.3. Execution Phase

Project Manager: 160 hours

4.1.1.4. Testing Phase

Project Manager: 20 hours

4.1.1.5. Deployment Phase

Project Manager: 20 hours

4.1.1.6. Closure and Maintenance Phase

Project Manager: 40 hours

4.2. Resource Dependencies

4.2.1. Internal Dependencies

- The hardware installation and network setup must occur before the firewall and SIEM system can be configured.
- The Operations Team requires completed documentation and training from the IT and Security Teams before taking over maintenance.

4.2.2. External Dependencies

- Delivery of hardware from online supplies.
- Stability and availability of cloud services (web hosting and SIEM).
- ISP provision of broadband Internet and static IP configuration.

5. Resource Budget

5.1. Personnel Costs

Personnel will work for free.

5.2. Hardware Costs

Expense	Type	Est. Cost	Running Total
Raspberry Pi 5 B 8GB x 4	Hardware	538.00	538.00
Raspberry Pi 5 Power Supply x 4	Hardware	82.60	620.60
Raspberry Pi 5 Official Case x 2	Hardware	34.42	655.02
Argon NEO 5 Raspberry Pi Case x 2	Hardware	69.90	724.92
Raspberry Pi Active Cooler x 4	Hardware	34.44	759.36
Raspberry Pi Keyboard	Hardware	32.00	791.36
Raspberry Pi Mouse	Hardware	18.00	809.36
512GB SanDisk MiniSD Card x 4	Hardware	323.96	1,133.32
Micro HDMI Cable x 2	Hardware	15.10	1,148.42
Wireless Network Adapter x 2	Hardware	93.60	1,242.02
USB to Ethernet Adapter x 2	Hardware	39.98	1,282.00
External Storage 5TB	Hardware	189.00	1,471.00
LAN cables x 5	Hardware	14.99	1,485.99
		Grand Total	1,485.99

5.3. Software Costs

Expense	Type	Est. Cost	Running Total
Cloud Web Server	Software	$15.00/mo	$15.00
SIEM System	Software	$15.00/mo	$30.00
		Grand Total	$30.00
		Total/Year	$360.00

5.4. Facility Costs

Expense	Type	Est. Cost	Running Total
Static IP Hire	Utility	$10.00/mo	$10.00
		Grand Total	$10.00
		Total/Year	$120.00

5.5. Contingency Budget

Expense	Type	Est. Cost	Running Total
Contingency Budget	Contingency	$500.00	$500.00
		Grand Total	$500.00

6. Resource Risks and Mitigation

6.1. Resource Risks

6.1.1. Personnel Risks

ID #	Description	Score	Management Strategies
0007	Human error during installation and configuration	High	**Avoidance:** Staff training. Thorough documentation on installation and configuration. **Exploitation:** Document any repairs or reconfigurations. **Mitigation:** Thorough testing of hardware and software.
0016	Stakeholder Conflicts	High	**Mitigation:** High level of communication with stakeholders and adherence to their expectations from the project.
0021	Negative Reputation of Partners	Medium	**Avoidance:** Avoid unethical partners or partners with negative reputations. **Mitigation:** Maintain relationships with various partners and vendors to provide choice in those the organization deals with.
0022	Project Sponsor/Manager in poor health	Medium	**Acceptance:** The project and business fail, as there is no-one left to complete the project and execute business operations.
0029	Miscommunication of information leads to impact on project resources, scope, schedule, budget, or risks	Medium	**Mitigation:** A clear communications plan with policies and procedure for communicating with all stakeholders involved with the project.

6.1.2. Hardware Risks

ID #	Description	Score	Management Strategies
0001	Data loss	Medium	**Mitigation:** Backup three times to two different media types with one backup stored off-premises.
0004	Supply chain disruptions	Medium	**Avoidance:** Maintain relationships with various vendors. **Mitigation:** Buy necessary equipment in advance of implementation.
0005	System failures in hardware and software	Medium	**Avoidance:** Good software implementation practices. Thorough documentation. **Mitigation:** Contingency budget for replacing hardware and software.
0010	Technological obsolescence	Medium	**Acceptance:** Buy improved technology with the contingency budget. **Avoidance:** Maintain access to state-of-the-art technology. **Exploitation:** Identify obsolescence and use it to improve systems with new technology.

			Mitigation: Monitor performance of network and websites. Research into new, better technology.
0012	Resource scarcity of essential equipment	Low	**Acceptance:** Extend project deadlines to account for delays in equipment delivery. **Avoidance:** Buy necessary equipment early, before implementation. **Exploitation:** Buy necessary equipment early and gain advantage over less-equipped competition. **Mitigation:** Use different vendors to minimize the risks of losing resource availability.
0020	Global economic conditions affecting financial viability or supply chains	High	**Acceptance:** Global economic changes are not within the organization's control. **Exploitation:** Procure equipment early to gain a competitive advantage over less well-equipped competitors. **Mitigation:** Procure equipment early to avoid disruption in supply chains.
0026	Project requires unanticipated hardware/software	Medium	**Acceptance:** Tap contingency budget to buy the required technology. **Mitigation:** Thorough project planning, research, and procurement of necessary inventory.

6.1.3. Software Risks

ID #	Description	Score	Management Strategies
0001	Data loss	Medium	**Mitigation:** Backup three times to two different media types with one backup stored off-premises.
0002	Data protection issues resulting in legal penalties and reputational damage	Medium	**Avoidance:** Implementation of firewalls and other preventative measures. **Mitigation:** Strong security practices. Implementation of SIEM for security monitoring.
0005	System failures in hardware and software	Medium	**Avoidance:** Good software implementation practices. Thorough documentation. **Mitigation:** Contingency budget for replacing hardware and software.
0006	Cost fluctuations (e.g. cloud hosting)	Medium	**Mitigation:** Maintain relationships with different vendors. Train in various cloud platforms.
0007	Human error during installation or configuration	High	**Avoidance:** Staff training. Thorough documentation on installation and configuration. **Exploitation:** Document any repairs or reconfigurations. **Mitigation:** Thorough testing of hardware and software.
0010	Technological obsolescence	Medium	**Acceptance:** Buy improved technology with the contingency budget.

			Avoidance: Maintain access to state-of-the-art technology. **Exploitation:** Identify obsolescence and use it to improve systems with new technology. **Mitigation:** Monitor performance of network and websites. Research into new, better technology.
0011	Exchange rate fluctuations impacting costs	Medium	**Acceptance:** The organization cannot change or affect exchange rate fluctuations. **Mitigation:** Contingency budget.
0013	Insufficient testing	Medium	**Acceptance:** Iteratively fix bugs as they become apparent. **Avoidance:** Strong and thorough testing practices. **Exploitation:** Improve systems while fixing any bugs. **Mitigation:** Staff training in testing.
0026	Project requires unanticipated hardware/software	Medium	**Acceptance:** Tap contingency budget to buy the required technology. **Mitigation:** Thorough project planning, research, and procurement of necessary inventory.
0030	Licensing issues with software	Medium	**Mitigation:** Research multiple software solutions for each software component of the project.
0031	Compatibility problems between software	Medium	**Mitigation:** Research multiple software solutions for each software component of the project.

6.1.4. Facility Risks

ID #	Description	Score	Management Strategies
0024	Loss of physical premises	Medium	**Avoidance:** Maintain good relationship with landlords. **Exploitation:** Move to better premises, delaying projects but improving facilities and operations.
0027	Difficulty filming in laboratory	Medium	**Avoidance:** Rearrange laboratory space prior to the execution phase for better shooting opportunities. **Mitigation:** Film on other locations when possible.
0033	Power outages affect project progress	Medium	**Mitigation:** Invest in a UPS power supply.
0034	Network disruptions (e.g. residential Internet) affect project progress	Medium	**Mitigation:** Obtain authorization to deal with Telstra, to facilitate troubleshooting of external network problems.

7. Resource Monitoring and Control

7.1 Resource Tracking

The Project Manager will track resource usage through weekly status reports, project management tools (e.g. ClickUp), and other documentation. Regular reviews of hardware usage and budget will be conducted to ensure the project stays on track.

7.2. Change Management

Any changes to resource allocations will follow the Change Management Plan. The Project Manager will assess the impact of changes on resources before reallocating or adding resources.

8. Approval and Sign-Off

Agreement between all stakeholders to implement the Resource Plan.

Project Manager:

Brendan Gasparin

X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted]

X _____

(Signature)

X _____

(Date)

Premises Owner:

[redacted]

X _____

(Signature)

X _____

(Date)