Innovative Cyber-Range Solution for W.L.S. Are The Best LLC.

By: Mason Riley, Sujay Kanwar, Muhammad Adeel, Huzaifah Majid

Meet our Team:
Mitnick Mavericks

Adeel

- Cybersecurity expert with background in SIEM and Incident response.

Sujay

- Cybersecurity Graduate from Rutgers University
- Experience With Industry Standard Network Analysis Tools

Mason

- Assistant System Administrator at Rutgers University New Brunswick
- Cloud Architect Enthusiast with a focus on Cybersecurity

Huzaifah

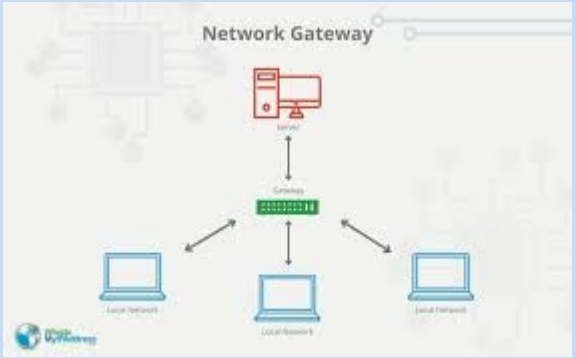
- Security+ Certified
- Double Major CS & ITI
- Linking secure solutions

Executive Summary

- Objectives
- Standards
- Our Solution

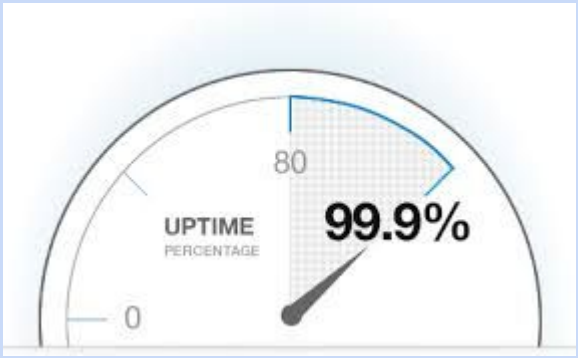
Executive Summary

OBJECTIVE:



- Network gateway

- Company website



- Service uptime

Executive Summary contd.

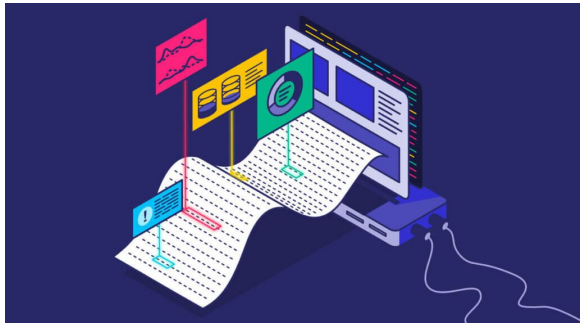
Standards:

Compliant with WEF (Warren’s Exciting Framework)

Our Commitment to You

By the end of this project we guarantee a solution that allows for monitoring of the following W.L.S services:

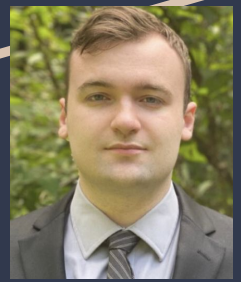
- **Network Gateway**
- **Website**
- **Uptime**



What do we need from you?

- Selection of virtual environments to monitor for log purposes

Project Assumptions



Rules:

- Adherence to predefined timelines
- Maintaining communication
- Ensuring quality

Our Needs:

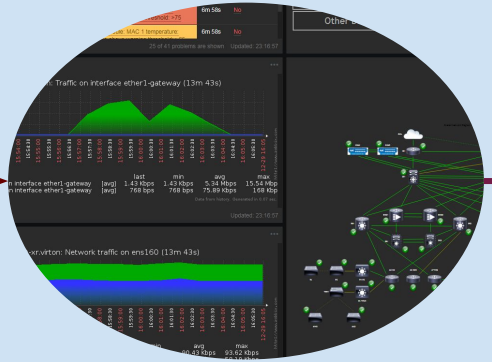
- Collaboration and accessibility to necessary resources and information from W.L.S.

Our Resources:

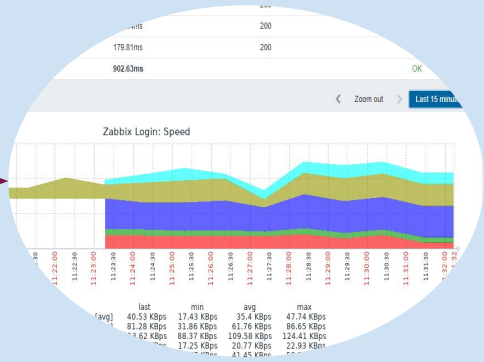
- Expert team, advanced mon dedicated support.

OUR SOLUTION:

Improved Network Security

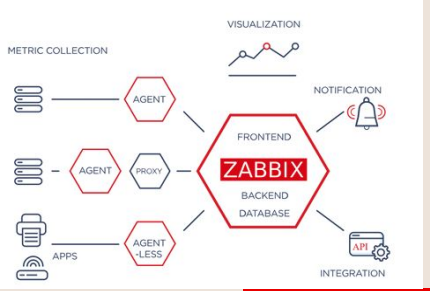


Reliable Website Monitoring



Thorough Gateway Analysis

HOW?



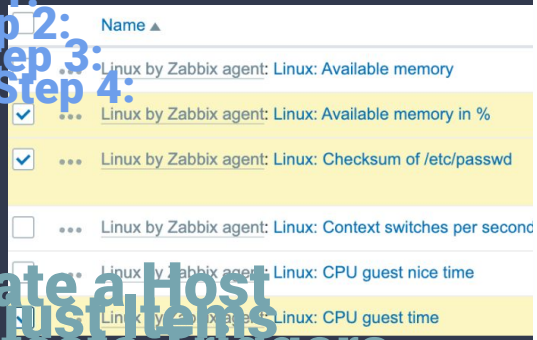
ZABBIX

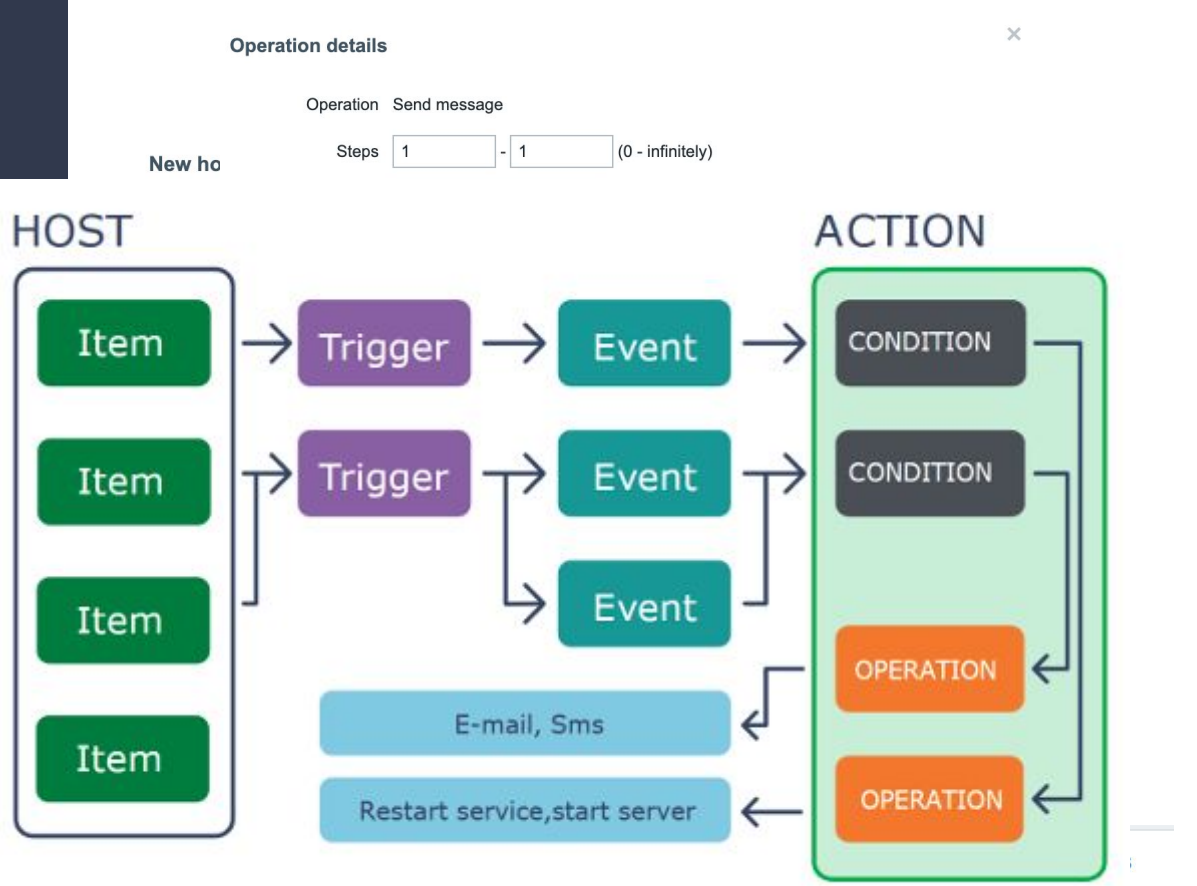
- Real-time insights
  - Network Health
  - Website Performance
- User-friendly interface
- Scalability

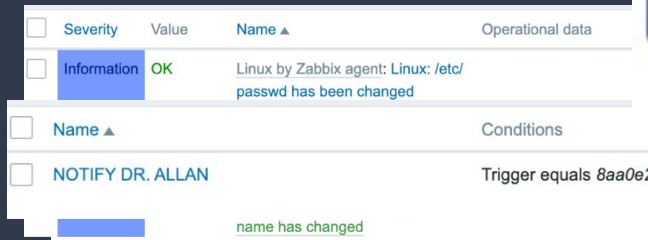
Zabbix Guide

Step 1:
Step 2:
Step 3:
Step 4:

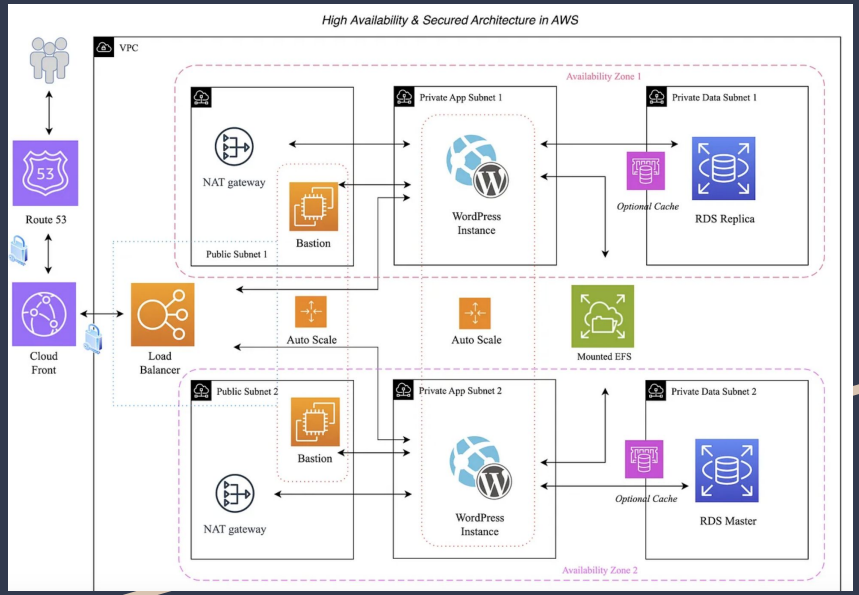
Create a Host
Adjust Items
Create Triggers
Create Alerts







Zabbix + Cloud



- On-site setup will limit
  - Scalability
  - Fault tolerance
  -

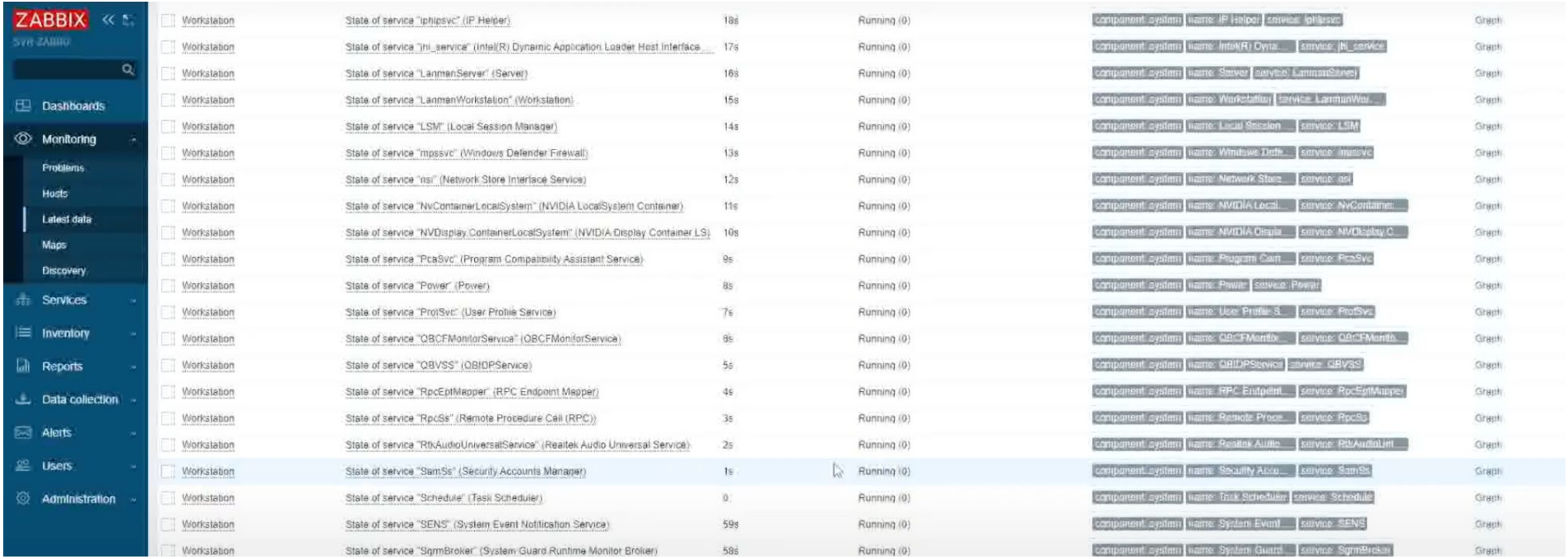
Never forget about security and a safety of your Zabbix. There are some ideas that you can employ on your Zabbix on a Clouds:

- Separating database and cluster infrastructure in a different VPC and control access between those VPC's;
- Secure access to your Zabbix internal VPC reserved for administrative personnel;
- Zabbix database holding lot's of sensitive data. Think about encryption of the database and/or volume.
- Use encryption for the traffic between Server and Proxies. Use the certificates, not PSK.
- Use Vaults for storing sensitive configuration files, such as zabbix_server.conf

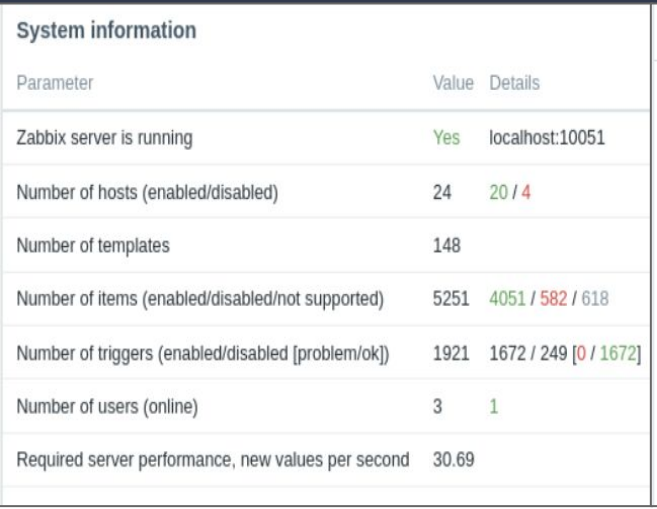
Beyond Monitoring: Enhancing Cybersecurity

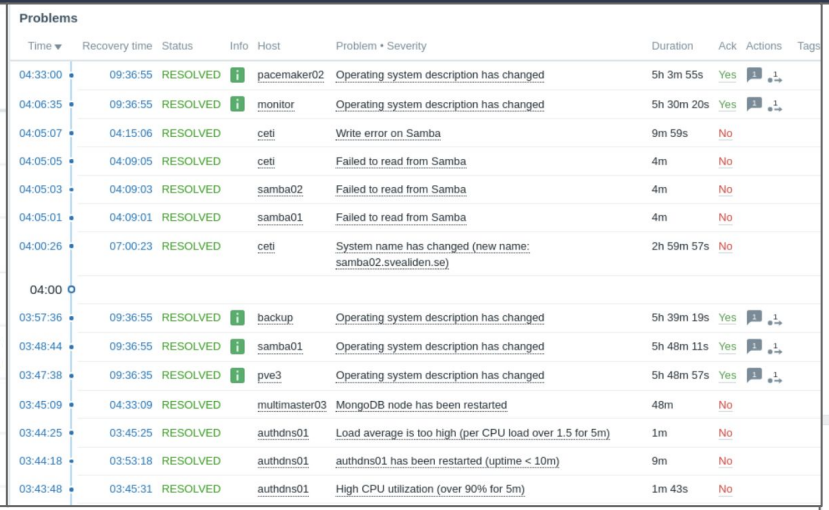
- **Enhanced Security**
  - Implement Intrusion Detection
  - Conduct Threat Analysis
- **Cybersecurity Awareness**
  - Workshops for W.L.S. Staff
  - Regular Training Sessions
- **Advance Monitoring solutions**
  - Insightful Lab Function Analysis
- **Hands On Training**
  - Lab Environments for Security Training
  - Focus on Common Web Exploits
- **Monitoring Skills Development**
  - Understanding Monitoring with Docker

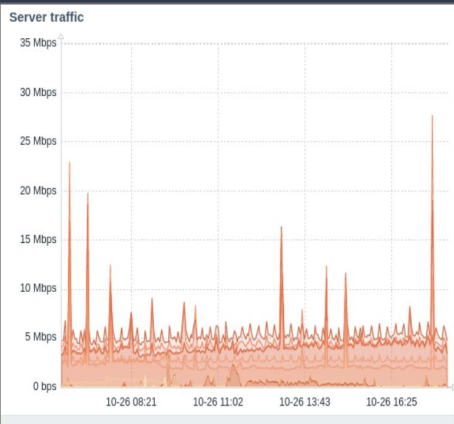
Zabbix Agent Monitoring

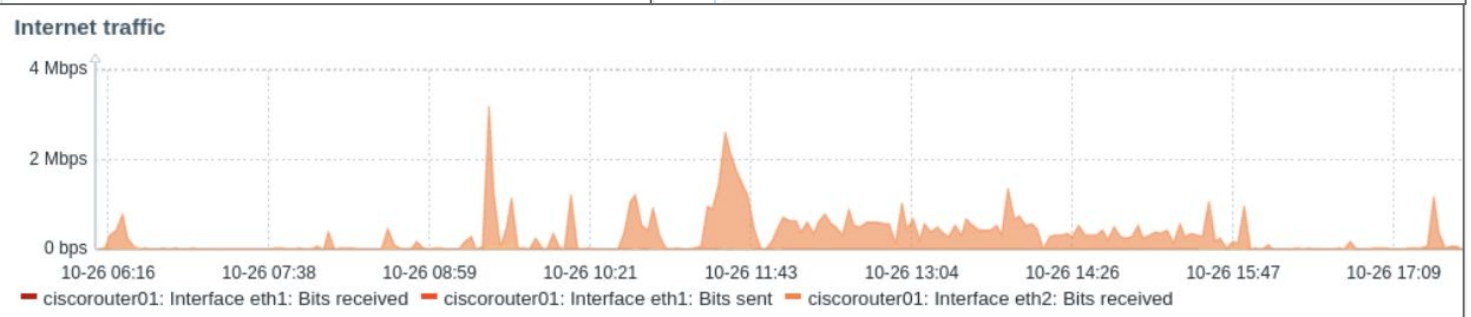


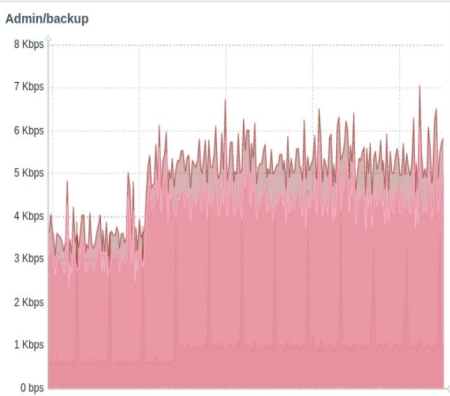
Sample Dashboards











Phases

Phase	Activities
Phase 1: Planning and Initiation	Assess infrastructure; Set up Zabbix in Docker; Develop monitoring strategy
Phase 2: Fieldwork	Implement Zabbix on AWS WordPress site; Configure alerts and metrics; Optimize system
Phase 3: Reporting / Results	Report activities and findings; Evaluate system performance; Adjust and discuss scalability

Detailed Timeline

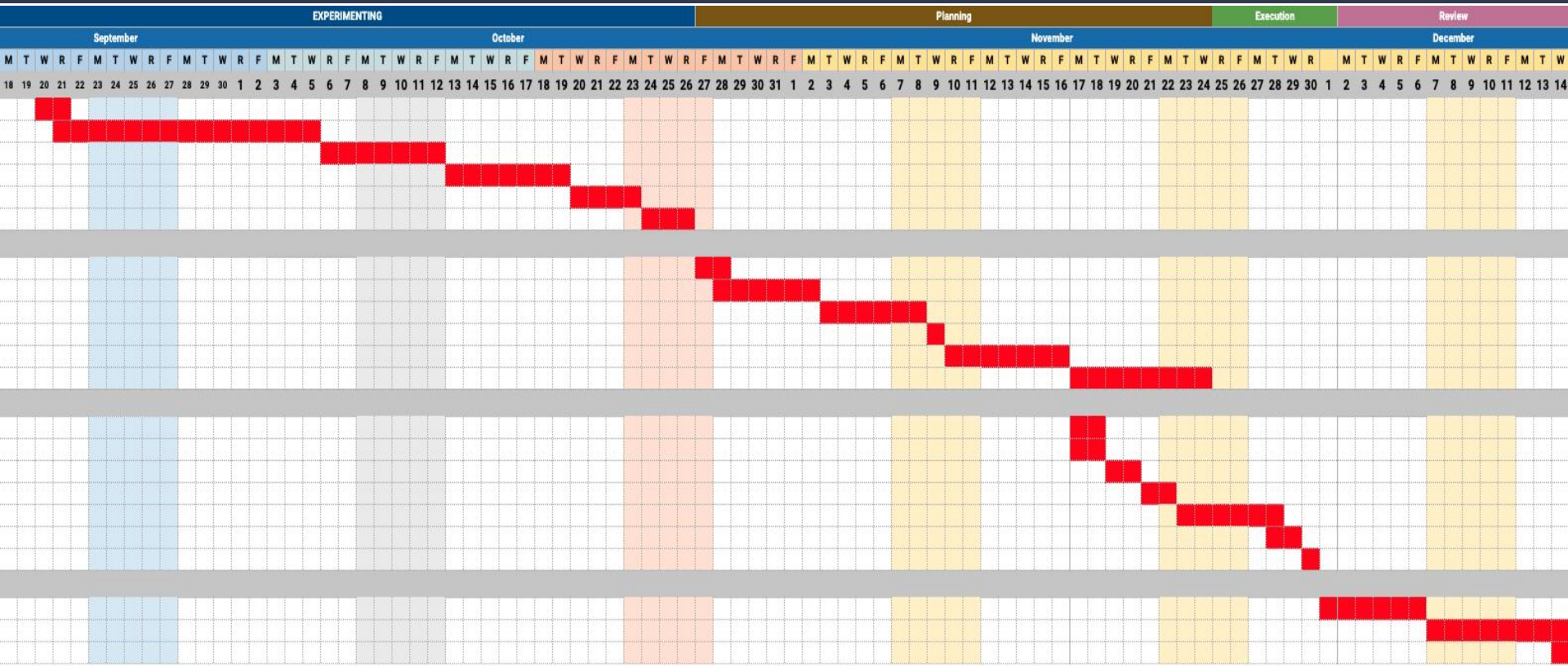
1	Project Conception and Initiation	Start	End
1.1	Virtualization	9/20/23	9/21/23
1.2	Learn Kali Linux	9/21/23	10/5/23
1.3	Networking Fundamentals	10/6/23	10/12/23
1.4	Nmap	10/13/23	10/19/23
1.5	NetDevOps	10/20/23	10/23/23
1.6	Docker	10/24/23	10/26/23

2	Project Definition and Planning		
2.1	Cyber Range Scope Requirements	10/27/23	10/28/23
2.2	Research Docker Tools	10/28/23	11/2/23
2.3	Draft initial Architecture	11/3/23	11/8/23
2.4	Request for Proposal Release	11/9/23	11/9/23
2.5	Draft Request for Proposal	11/10/23	11/16/23
2.6	Final Request for Proposal	11/17/23	11/24/23

3	Project Conception and Initiation		
3.1	Set Up Docker Containers	11/17/23	11/18/23
3.2	Set up Bridged Virtual Machines	11/17/23	11/18/23
3.3	Configure Zabbix	11/19/23	11/20/23
3.4	AWS Cloud Deployment	11/21/23	11/22/23
3.5	Solution Updates	11/23/23	11/28/23
3.6	Testing	11/28/23	11/29/23
3.7	Presentation	11/30/23	11/30/23

4	Project Performance / Monitoring		
4.1	Document Lessons Learned	11/30/23	12/6/23
4.2	Solution Enhancement	12/7/23	12/14/23
4.3	Project Performance	12/14/23	12/14/23

Gantt Chart


EXPERIMENTING
Planning
Execution
Review
September
October
November
December

THANK YOU


Busy Processes of Zabbix server
Pinger Processes
0.00%
Housekeeper Processes
0%
Poller Processes
0.00%
Alerter Processes
0%
History Syncer Processes
0.89%
Trapper Processes
0.02%
CPU/Memory/Disk/Network of Z
ZABBIX
CPU steal time 0
CPU system time 3
Load average (15m avg) 0.710 0.820 0.765 0.710
Zabbix preprocessing queue 0 1.500 K 240 0
Zabbix queue 1 1 1 1
Network Adapters
Interface enp3s0: Bits received 934 kB/s 942 kB/s 942 kB/s
Interface enp3s0: Bits sent 99 kB/s 143 kB/s 139 kB/s
Available memory
Available memory 4.61 GiB 4.64 GiB 4.61 GiB
Free disk space
/: Total space 54.0 GiB 54.0 GiB 54.0 GiB
/: Used space 23.7 GiB 23.7 GiB 23.7 GiB