Unicis Open Positions

All open hiring positions at Unicis can be found here.

job, hiring, job, position

SOC Engineer SOC Engineer (Open Source Tech Stack)

SOC Engineer (Open Source Tech Stack)

Company: Unicis

Location: Remote

Job Type: Part-Time

About Us

Unicis is building a cutting-edge Security Operations Center (SOC) using an open-source technology stack. We are looking for an experienced SOC Engineer who has hands-on experience in setting up and managing a SOC using open-source tools such as Zabbix, Wazuh, and MISP, containerized with Docker.

Job Description

As a SOC Engineer, you will be responsible for designing, deploying, and maintaining an open-source SOC for Unicis. You will work with the latest versions of Zabbix, Wazuh, and MISP, and ensure these tools are seamlessly integrated to provide comprehensive security monitoring and alert management capabilities. Your role will involve customization of integrations, setting up automation workflows, and ensuring that all security alerts are reported and managed through the Zabbix interface.

Key Responsibilities

- Design and deploy a SOC using Zabbix 7, Wazuh 4.x, and MISP 2.4.x in Docker containers.
- Integrate MISP with Wazuh for threat intelligence sharing and Wazuh with Zabbix for alert management.
- Customize SOC components to ensure MISP reports to Wazuh and Wazuh alerts (level 7+) are reported to Zabbix.
- Configure Zabbix to handle, display, and act upon all security alerts.
- Develop and maintain Docker Compose scripts for deploying and managing SOC components.
- Secure the SOC environment, including securing Docker containers and setting up encrypted communications.
- Implement automated testing and continuous monitoring to ensure SOC performance and reliability.
- Collaborate with IT and security teams to ensure smooth SOC operations and incident response.

Required Qualifications

- Proven experience in setting up SOCs using open-source technologies.
- Proficiency with Zabbix, Wazuh, and MISP, including the latest versions.
- Strong knowledge of Docker and container orchestration.
- Experience with integrating security tools and setting up automated alert workflows.
- Solid understanding of network security, threat intelligence, and incident response.
- Strong scripting skills (Python, Bash, etc.) for automation and integration tasks.
- Excellent problem-solving skills and attention to detail.

Preferred Qualifications

- Experience with CI/CD tools such as GitLab CI/CD.
- Familiarity with infrastructure as code (IaC) tools like Ansible.
- Knowledge of cloud environments and deploying SOCs in cloud infrastructure.

Benefits

- Competitive salary and benefits package.
- Opportunities for professional development and certification.
- Collaborative and innovative work environment.
- Flexible work hours and potential for remote work.

Technical Specification Document for SOC Intranet Center at Unicis

1. Introduction

This document outlines the technical specifications for setting up an open-source SOC at Unicis using Zabbix, Wazuh, and MISP with Docker containers. The goal is to deploy a scalable and customizable SOC that centralizes security alerts and facilitates effective incident response.

2. Objective

Deploy a SOC leveraging Zabbix, Wazuh, and MISP to:

- Integrate MISP with Wazuh for threat intelligence sharing.
- Report Wazuh alerts (level 7 and above) to Zabbix.
- Centralize security alert management in Zabbix.

3. System Architecture

Components

- **Zabbix 7.0**: Monitoring and alert management.
- **Wazuh 4.x**: SIEM and log analysis.
- **MISP 2.4.x**: Threat intelligence platform.
- **Docker**: Containerization for scalability and portability.

4. System Requirements

4.1 Hardware Requirements

- **CPU**: Minimum 4 cores, recommended 8 cores.
- **Memory**: Minimum 16 GB RAM, recommended 32 GB.
- **Storage**: Minimum 500 GB SSD, recommended 1 TB SSD.
- **Network**: 1 Gbps Ethernet or higher.

4.2 Software Requirements

- **OS**: Linux (Ubuntu 20.04 LTS recommended).
- **Docker**: Latest version of Docker and Docker Compose.
- **Zabbix**: Version 7.0.
- **Wazuh**: Version 4.x.

- **MISP**: Version 2.4.x.
- **Database**: PostgreSQL or MySQL/MariaDB.
- **Web Server**: Nginx.

5. Deployment Architecture

5.1 Docker Container Setup

- **Zabbix Server**: Monitoring and alert management.
- **Zabbix Agent**: For monitored systems.
- **Wazuh Server**: SIEM and integration with MISP.
- **Wazuh Agent**: For data collection.
- **MISP**: Threat intelligence sharing.
- **Database Containers**: For Zabbix, Wazuh, and MISP.
- **Reverse Proxy**: Nginx for web traffic management.

5.2 Networking

- Secure communication with Docker networks.
- Use an overlay network for distributed deployments.
- Implement Docker secrets for secure configuration.

6. Integration and Customization

6.1 MISP to Wazuh

- Use MISP API to push intelligence to Wazuh.
- Automate threat feed import into Wazuh for real-time detection.

6.2 Wazuh to Zabbix

- Configure Wazuh to send high-severity alerts to Zabbix.
- Use custom scripts or Zabbix integrations to process Wazuh alerts.

6.3 Alert Management in Zabbix

- Customize Zabbix templates for Wazuh alerts.
- Create dashboards for monitoring SOC metrics.
- Set up alerting and response actions in Zabbix.

7. Security Considerations

- Use best practices for securing Docker containers.
- Implement TLS for secure communications.
- Set up RBAC in Zabbix, Wazuh, and MISP.

8. Testing and Validation

- Perform integration testing for all components.
- Conduct stress testing to validate system performance.
- Implement automated testing for updates and security patches.

9. Deployment Process

9.1 Steps

1. **Environment Setup**: Install Docker and dependencies.
2. **Docker Network**: Create secure Docker networks.
3. **Deploy Containers**: Use Docker Compose for deployment.
4. **Integration**: Set up MISP, Wazuh, and Zabbix connections.
5. **Testing**: Verify all integrations and performance.
6. **Production**: Deploy and monitor continuously.

9.2 Automation and CI/CD

- Use CI/CD pipelines for deployment and updates.
- Automate configuration with Ansible or similar tools.

10. Documentation and Training

- Provide detailed guides for managing the SOC.
- Train SOC analysts on Zabbix, Wazuh, and MISP.

11. Maintenance and Support

- Schedule updates and patches.
- Monitor performance and adjust as needed.
- Set up alerts for system issues.

Conclusion

The SOC at Unicis will leverage Zabbix, Wazuh, and MISP with Docker for a robust security monitoring solution. By integrating these tools, the SOC will centralize alert management, enabling Unicis to maintain a strong security posture.

How to Apply

Please send your resume, a cover letter detailing your relevant experience, and any examples of your work (e.g., GitHub repositories) to [recruitment@unicis.tech] or on the form below.

Name * Your Name GitHub * Repository Your E-Mail Address * When can you start (optional) Tell us why your interest and motivated to work at Unicis * Upload CV * Apply