Free and Open-Source Security Orchestration, Automation, and Response Platform (FOSS-SOAR)

Aedan Podest, Cooper Landen | podesta@xavier.edu, landenc1@xavier.edu | Xavier University | CAE Symposium 2026

Introduction

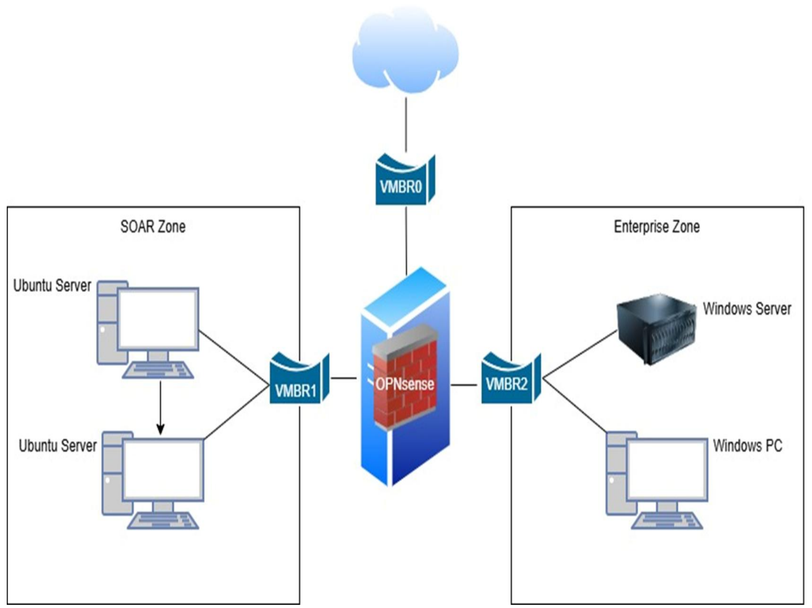
Security Operations Centers (SOCs) rely on SOAR platforms to streamline alert triage and incident response. Commercial solutions are often proprietary and costly, limiting access for students and researchers.

FOSS-SOAR integrates open-source tools to simulate SOC workflows in an educational setting, providing hands-on experience with real-world security automation pipelines at no cost to institutions.

Research Goals

- Integrate open-source tools into a cohesive SOC pipeline
- Simulate real SOC workflows for educational use
- Demonstrate cost-effective alternatives to proprietary SOAR

System Architecture



SOC Tool Stack

SU Suricata | SY Sysmon | WZ Wazuh | TH TheHive | CX Cortex

Suricata Sysmon Wazuh TheHive Cortex

Monitoring

- Suricata – Network intrusion detection
- Sysmon – Windows endpoint telemetry

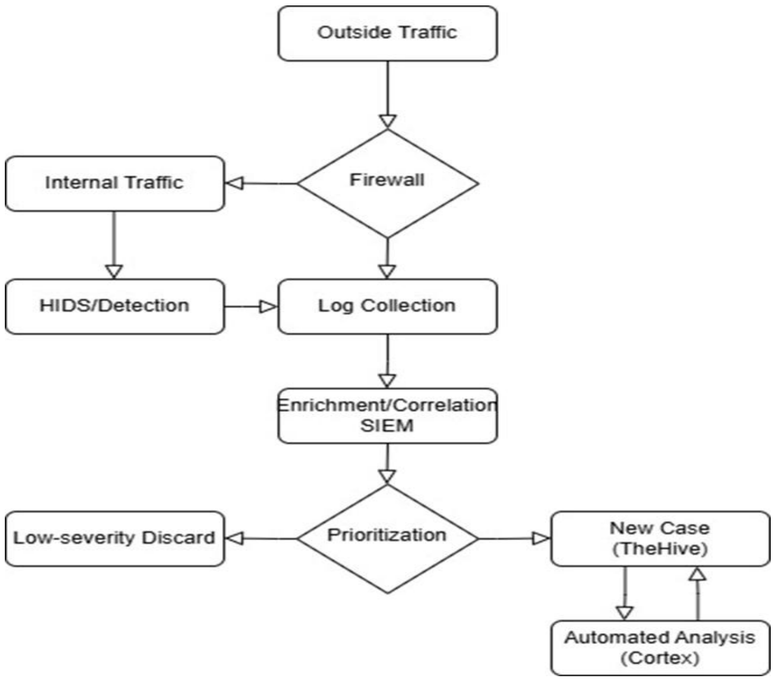
Logging / SIEM

- Wazuh – Log aggregation & SIEM

Analysis & Automation

- TheHive – Incident case management
- Cortex – Automated threat enrichment

Automation Workflow



Infrastructure

Network Design

- OPNsense firewall for traffic control and segmentation
- Isolated SOAR analysis zone and enterprise zone
- Ubuntu SOAR servers and Windows enterprise endpoints

Platform

- VMware-based virtualization environment
- Internal DNS and DHCP for realistic network simulation
- All components deployed as open-source, zero-cost stack

Conclusion

FOSS-SOAR demonstrates that open-source security tools can be integrated into a fully functional SOC automation pipeline at no cost to institutions.

The platform lets students experiment with automated incident response while maintaining full analyst visibility into triage and decision-making processes.

Key Takeaways

- Open-source tools rival commercial SOAR capability
- Practical hands-on learning for cybersecurity students
- Extensible framework for continued CAE research

Acknowledgments

This work was conducted at Xavier University under the NSA/DHS National Centers of Academic Excellence in Cyber Defense program. We thank the Xavier CS faculty for their guidance and support.