

# Teaching Endpoint Protection through Wazuh: A Project-Based Approach to Cybersecurity Education

Sara Sutton  
College of Computing  
Grand Valley State University  
Allendale, MI, USA  
suttosar@gvsu.edu  
0000-0002-4669-8286

Victor Bungei  
College of Computing  
Grand Valley State University  
Allendale, MI, USA  
bungeiv@mail.gvsu.edu  
0009-0003-7011-0600

Xinli Wang  
College of Computing  
Grand Valley State University  
Allendale, MI, USA  
wangx@gvsu.edu  
0009-0007-0939-237X

Johnfia Frank  
College of Computing  
Grand Valley State University  
Allendale, MI, USA  
johnfiarf@mail.gvsu.edu  
0009-0006-0166-2577

Esther Djan  
College of Computing  
Grand Valley State University  
Allendale, MI, USA  
djane@mail.gvsu.edu  
0009-0003-8109-9152

**Abstract**—In recent years, the demand for practical, real-world cybersecurity education has grown dramatically. Traditional lecture-based methods often fall short in equipping students with the applied skills needed to detect, analyze, and respond to current cyber threats. This paper presents a project-based educational framework focused on the deployment, configuration, and use of real-world software such as Wazuh. Rather than following predetermined steps, students engage with realistic endpoint and network security scenarios, such as installing and configuring Wazuh agents, monitoring and interpreting live system and application logs, detecting simulated security incidents such as brute-force attacks and malware execution, and applying industry-aligned procedures. Evaluation of student performance demonstrates substantial improvements in alert interpretation, rule configuration, and application of cybersecurity knowledge. Our findings indicate that integrating Wazuh into coursework effectively develops both practical technical skills and analytical thinking, aligns with national workforce competency standards, and provides a model that other courses can adopt to integrate enterprise security tools into the classroom.

**Keywords**—Cybersecurity Education, Case Studies, Wazuh, Experiential Learning, Educational Framework

## I. INTRODUCTION

The rapid advancements in cybersecurity have shifted the way education and training are delivered. Rather than relying solely on traditional lecture-based instruction, there is a need to incorporate project-based and experiential learning methods to better prepare students for the realities of defending against cyber threats. The existing cybersecurity competence frameworks, such as the National Initiative for

Cybersecurity Education (NICE) and National Institute of Standards and Technology Workforce Framework (NIST NICE) [1], [2] distinguish professional roles and associated tasks with a strong focus on technical competencies. As attacks on endpoints become more frequent and sophisticated, academic programs must evolve to prepare graduates for operational security roles that require both technical proficiency.

The cybersecurity education domain encompasses a variety of curriculum designs and teaching methods, including traditional lectures, lecture-lab hybrids, peer instruction, and concept mapping. Among these, lectures combined with hands-on exercises have become the instructional standard in the discipline. However, many existing hands-on commercial training platforms, such as those from EC-Council, and preconfigured lab environments are structured in a step-by-step, “hand-holding” format. These labs are typically isolated from one another, or the environments are already set up so that students only need to follow instructions to execute the given commands. While such approaches help students complete technical tasks, they often do so at the expense of problem-solving and critical thinking. As a result, learners may fail to develop a deep understanding of the complex, interconnected concepts that characterize real-world cybersecurity incidents [3].

One promising way to address this gap is to integrate open-source security platforms into curricula using exploratory, problem-based learning approaches. In this context, Wazuh—a widely adopted open-source Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platform offers a flexible and accessible foundation for developing project based activities. With its real-time monitoring, intrusion detection, integrity checking, and log analysis capabilities, Wazuh enables

students to engage with the same tools and workflows used in professional Security Operations Centers (SOCs).

Through our review of cybersecurity education frameworks and project-based learning approaches, we identified a lack of clear answers to the following questions:

1. How can an open-source platform like Wazuh be effectively integrated into a semester-long, project-based cybersecurity course?
2. What technical and analytical competencies frameworks can be developed through such a project?
3. How can scenario-driven security tasks improve students' problem-solving and critical thinking and real-world technical skills?

This paper presents a project-based educational framework centered on cybersecurity objectives related to the deployment, configuration, and use of real-world software such as Wazuh. Rather than guiding students through predetermined steps, the framework immerses them in realistic endpoint and network security scenarios where they must install and configure Wazuh agents, monitor and interpret live system and application logs, detect and investigate simulated security incidents (including brute-force attacks and malware execution), and apply incident response and reporting procedures consistent with industry practice.

When the course is organized around problem-driven tasks, students gain both technical skills like configuring SIEMs and working with log data and analytical skills. Particularly, they learn to interpret alerts from multiple sources, recognize unusual patterns of behavior, and make reasoned judgments even when the evidence is incomplete. This study adapts the Villarroel Authentic Assessment model [4] to design a project-based educational approach for cybersecurity students.

Through this work, we aim to demonstrate how Wazuh can serve as an instructional tool for fostering critical thinking and operational readiness in cybersecurity education. Our contributions include a modular lab design, aligned learning outcomes, example attack simulations, and an assessment framework for measuring student performance.

The rest of the paper is organized as follows. Section II reviews background and related works. Section III presents integration of project based learning in our case study. Section IV details the project design and implementation. Section V presents the case study. Section VI outlines the assessment methodology, and Sections VII, VIII discusses key findings and challenges. Finally, Section IX discusses conclusions.

## II. BACKGROUND AND RELATED WORKS

Cybersecurity education has increasingly turned toward competency-based frameworks and hands-on methods to prepare students for professional roles. This section reviews prior work in four areas relevant to our study: workforce and curriculum frameworks, pedagogical approaches, tools

currently used in cybersecurity education, and the role of open-source SOC platforms.

### A. Educational Framework and Competency Mapping

Cybersecurity education increasingly emphasizes competency-based learning to ensure that students get not only theoretical knowledge but also the practical skills required for professional roles. There are mainly two prominent frameworks that guide curriculum design in cyber defense: the *National Initiative for Cybersecurity Education* (NICE) Workforce Framework for Cybersecurity [1], [5] and the *Centers of Academic Excellence in Cyber Defense* (CAE-CD) Knowledge Units [6]. The NICE framework is selected in this research for its alignment with real-world job roles, fostering collaboration among developers and detailed coverage of cybersecurity topics [7], [8]. It also provides a taxonomy of work roles, knowledge, skills, and abilities (KSAs) required across cybersecurity domains, while the CAE-CD program specifies essential knowledge units that accredited institutions must integrate into their curricula.

In our approach, the Wazuh-based project aligns with these frameworks to ensure that students develop the competencies necessary for roles such as *Cyber Defense Analyst* (NICE Work Role: PR-CDA-001) and *Systems Security Analyst* (NICE Work Role: OM-ANA-001), *Cyber Defense Infrastructure Support Specialist* (NICE work role: PR-INF-001) [9]. This alignment reinforces that the hands-on activities in our case study are not isolated technical exercises but targeted skill-building tasks mapped to recognized national standards.

This project-based lab can be embedded into a range of cybersecurity courses, including but not limited to *Network Security*, *Malware Analysis*, *Digital Forensics*, *system security and operations*, and *Cloud Security*.

### B. Pedagogical Approaches in Cybersecurity Education

Traditional lab exercises in cybersecurity courses often rely on step-by-step instructions for reproducing attacks or defenses such as CompTIA, EC-Council, uCertify [10]–[12], etc. While effective for introducing fundamental concepts, scripted labs provide limited opportunities for critical thinking, decision-making under uncertainty, and operational problem solving. In contrast, project-based learning (PBL) emphasizes open-ended, real-world scenarios that require students to synthesize theory and practice. Prior studies have advocated for pedagogical approaches that balance technical depth with professional competencies [13], [14]. Similarly, competitions such as capture-the-flag (CTF) challenges, virtual hacking labs, and cyber ranges have been used to simulate adversarial contexts. However, these environments often emphasize offensive security. While the advantages of virtual labs are well-documented, their implementation also presents certain challenges. Ensuring the accuracy and fidelity of simulations, maintaining student engagement, and providing adequate support and resources are critical factors that influence the success of virtual labs [13]. If these labs do not accurately

simulate real-world environments, students may fail to develop the necessary skills to handle actual threats effectively.

Endpoint protection plays a critical role as the first line of defense against cyber attacks and remains a key priority in safeguarding an organization's assets from threats. In this book [15], the author demonstrates how Wazuh can be leveraged for enterprise security, providing a valuable resource for those seeking to understand and implement effective security monitoring practices. However, its use in academic settings has not been widely explored, leaving a gap in the literature on how such enterprise-grade tools can be adapted for educational purposes.

Our work extends prior efforts by demonstrating the integration of Wazuh into a graduate-level cybersecurity course through a structured, project-based framework. Unlike prior studies that rely on scripted labs, we emphasize open-ended scenarios mapped directly to NICE KSAs and CAE-CD Knowledge Units. Through this approach, we address both the pedagogical gap (bridging theory and practice via PBL) and the technological gap (leveraging a fully open-source operation platform suitable for academic use).

### III. INTEGRATION OF PROJECT-BASED LEARNING

Project-Based Learning (PBL) serves as the pedagogical foundation of our educational framework [16]. In this model, students engage in open-ended tasks that mirror real-world security operations. Rather than following prescriptive, step-by-step instructions, learners must interpret system alerts, configure security tools, investigate simulated incidents, and propose remediation strategies.

The Wazuh project is designed using the principles of authentic assessment [4], where the learning tasks replicate the demands and constraints faced by practitioners in Security Operations Centers (SOCs). Through iterative engagement with realistic threat scenarios such as brute-force attacks, malware detection, file integrity monitoring, and endpoint hardening students acquire both procedural and analytical skills.

Table I presents the mapping of key Wazuh project tasks to the relevant NICE KSAs and CAE-CD Knowledge Units. This mapping ensures that the educational outcomes of our framework are explicitly connected to nationally recognized cybersecurity competencies.

TABLE I. Detailed Mapping of Wazuh Project Tasks to NICE KSAs [1] and CAE-CD Knowledge Units

Wazuh Project Task	Relevant NICE KSAs (Knowledge, Skills, and Abilities)	CAE-CD Knowledge Units
Deploy and configure Wazuh server and endpoint agents	K0001: Knowledge of networking concepts, protocols, and architectures; K0044: Knowledge of authentication methods and PKI; S0038: Skill in configuring and integrating security tools into enterprise environments	Network Defense; Cybersecurity Principles; Basic Scripting
Implement File Integrity Monitoring (FIM) and detect unauthorized changes	K0070: Knowledge of file system structures and operating system internals; S0011: Skill in using host-based security tools to monitor activity; A0032: Ability to detect indicators of compromise in host environments	Operating Systems Hardening; Vulnerability Assessment and Management
Simulate and respond to brute-force SSH attacks	K0058: Knowledge of common network attacks, exploitation techniques, and tools; S0041: Skill in performing incident triage and containment actions; A0012: Ability to implement protective measures based on threat intelligence	Network Defense; Incident Response
Integrate threat intelligence (VirusTotal) for malware detection	K0108: Knowledge of malware analysis fundamentals; A0043: Ability to use threat intelligence for incident response and decision-making; S0022: Skill in correlating threat data from multiple sources	Malware Analysis; Cyber Threats; Cybersecurity Principles
Perform endpoint configuration assessment against CIS benchmarks	K0069: Knowledge of security configuration standards and compliance requirements; S0005: Skill in assessing system security posture; A0020: Ability to interpret automated vulnerability and compliance reports	Security Program Management; Vulnerability Assessment; Cybersecurity Principles
Analyze Wazuh alerts and produce incident reports	K0160: Knowledge of reporting formats for technical and non-technical audiences; A0066: Ability to analyze and determine incident impact, scope, and cause; S0054: Skill in preparing after-action reports	Cybersecurity Ethics; Security Program Management; Communication in Cybersecurity

By aligning each technical task with specific KSAs and Knowledge Units, we ensure that students are gaining tool-specific experience as well as developing competencies directly tied to industry expectations.

Our proposed project framework supports measurable learning outcomes, such as:

- **Application/Apply:** after completing the course, the student will be able to apply endpoint security tools and techniques to comprehend the major concepts of information security including defense of information assets', detection of and reaction to threats.
- **Comprehension/Describe:** describe industry-standard monitoring systems and their role in threat detection.
- **Analysis/Evaluate:** analyze system logs to distinguish between normal and suspicious activity patterns.
- **Adaptation/Develop:** develop and customize alerting rules for file integrity monitoring based on lab scenarios.
- **Critical Thinking/Problem Solving:** after completing the course, the student will develop critical thinking and problem-solving skills using real equipment and cybersecurity tools.
- **Conceptual and Factual Knowledge:** demonstrate understanding of SIEM concepts, threat intelligence integration, and compliance monitoring, linking classroom theory to real-world practices.

#### IV. METHODOLOGY

This work adopts a project-based learning approach in which students deploy and operate the Wazuh Security Information and Event Management (SIEM) platform in a controlled virtualized environment. The lab environment is hosted on Google Cloud Platform (GCP), where a single-node Wazuh Docker deployment runs on an Ubuntu 22.04 instance. This architecture was selected for its accessibility and scalability in academic settings, while maintaining technical authenticity for simulating small-to-medium enterprise deployments.

To simulate an enterprise environment, Wazuh agents are installed on heterogeneous endpoints running Windows, macOS, and Linux. Students configure these agents to forward system logs, detect vulnerabilities, and, depending on configuration, respond to threats in real time. The environment is further secured with Cloudflare as a reverse proxy, adding an operationally realistic network security layer. Figure 1 shows the deployment architecture and the interaction between monitored endpoints, the Wazuh server, and integrated threat intelligence sources.

The project unfolds through a series of open-ended scenarios designed to replicate SOC workflows. Rather than following rigid, step-by-step instructions, students are presented with a problem statement, a set of realistic operational constraints, and access to relevant Wazuh documentation [15]. They must then install and configure

Wazuh components, generate security events, and investigate alerts. For example, in one scenario, students enable File Integrity Monitoring to track changes in critical directories and the Windows Registry, simulate tampering activity, and validate detection through Wazuh's alerting interface. In another, they simulate an SSH brute-force attack using Hydra against a Linux endpoint and configure active response mechanisms to automatically block the attacker's IP address. Additional scenarios involve deploying known malicious executables to endpoints and analyzing detections via VirusTotal integration [17], as well as conducting endpoint configuration assessments against CIS benchmarks.

The instructional design follows an iterative cycle of preparation, deployment, execution, and analysis. Students begin by reviewing the problem context and relevant documentation, then configure the necessary components, generate and capture events through attack simulations or system modifications, and finally analyze the resulting alerts. The process culminates in the production of an incident report that documents the root cause, impact, and recommended remediation steps. This activity format requires students to engage in both technical implementation and reasoning, including correlating multiple log sources, recognizing attack patterns, and making informed response decisions under uncertainty.

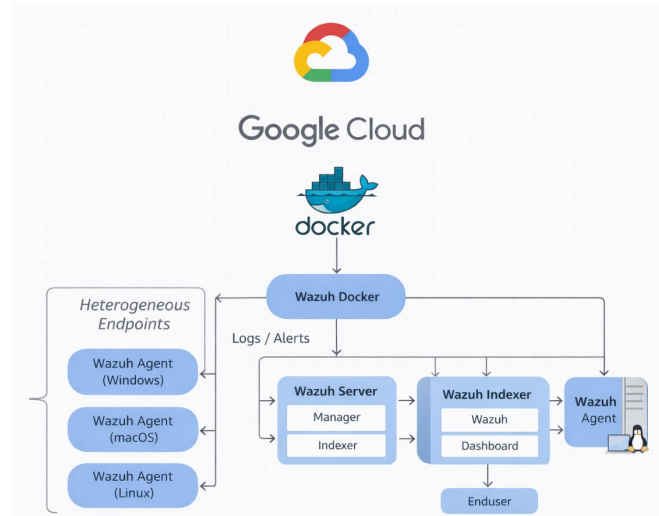


Fig. 1. Wazuh docker deployment architecture

#### V. CASE STUDY: SEMESTER LONG PROJECT

To demonstrate the application of our project-based learning framework, we conducted a case study in a graduate-level cybersecurity course. The class consisted of 18 students, each working in teams of two to three, with access to a shared Google Cloud deployment of the Wazuh server and heterogeneous endpoint instances. Over a 15 week period, students completed a sequence of open-ended scenarios, each designed to replicate an operational task in an operational environment. The project was completed in 4 phases.

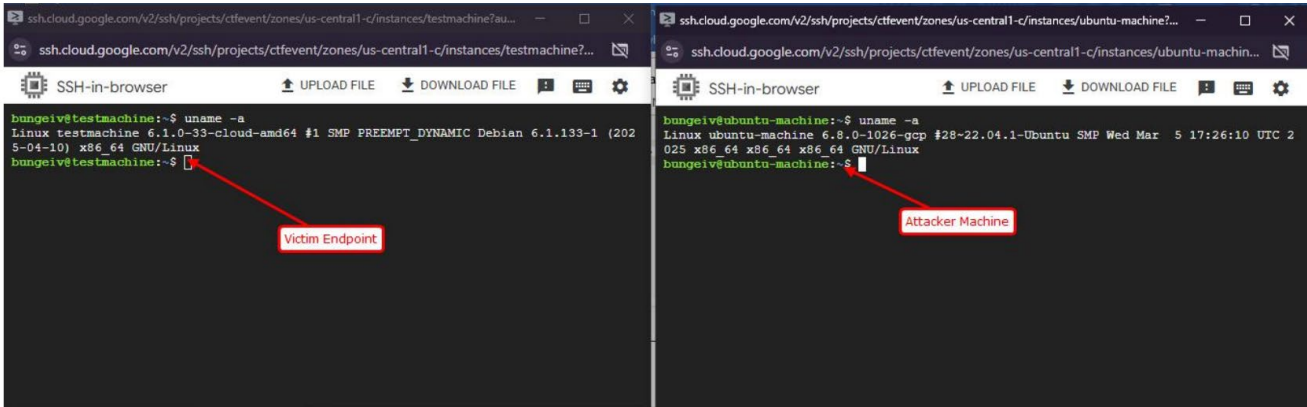


Fig. 2. Attacker and Victim machine

**Phase 1: Environment setup and tool familiarization (weeks 1–3)** In this phase, students deployed Wazuh using the Docker single-node configuration on a Google Cloud Ubuntu 22.04 server instance, with Cloudflare acting as a reverse proxy. Wazuh agents were installed on Linux endpoints. The architecture allowed for centralized log collection, real-time alerting, and agent-based monitoring (Figure 2).

included enabling File Integrity Monitoring (FIM) and introducing controlled changes, such as adding suspicious executables or modifying registry keys. Students identified and analyzed these changes through the Wazuh console, producing initial remediation plans.



Fig. 3. Wazuh Manager configuration

Students then configured the Wazuh Manager and Active Response modules, as shown in Figures 3 and 4, to enable detection rules and automated responses. Early tasks

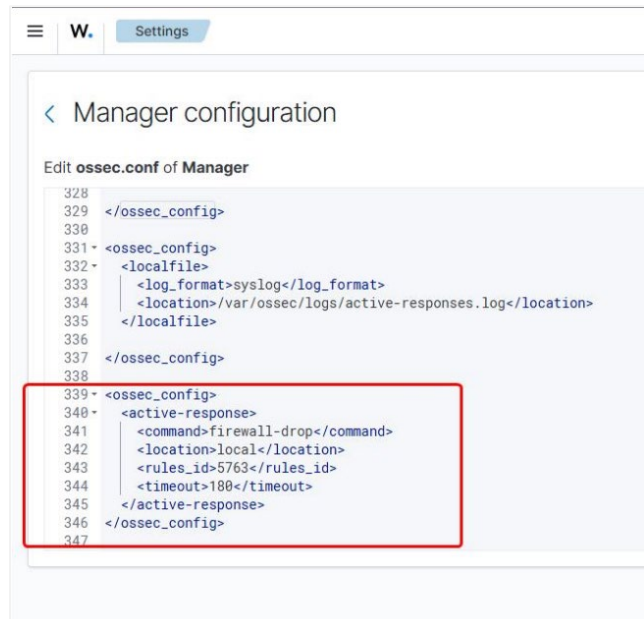


Fig. 4. Active response configuration

**Phase 2: Baseline monitoring and rule customization (weeks 4–6)** Students observed normal endpoint behavior to establish baseline metrics, documented system and application logs, and customized Wazuh detection rules. This phase developed students' ability to differentiate normal operations from anomalies. Figure 5 shows an example alert generated after a suspicious file, `suspicious.exe`, was introduced into a monitored directory.

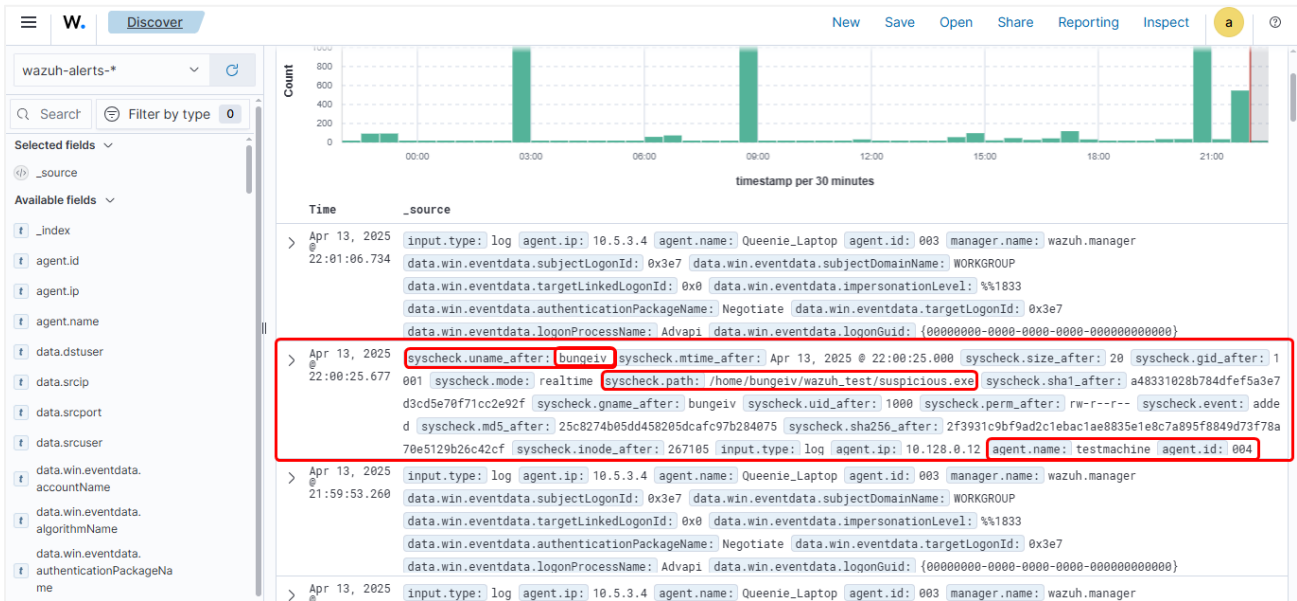


Fig. 5. File integrity monitoring log

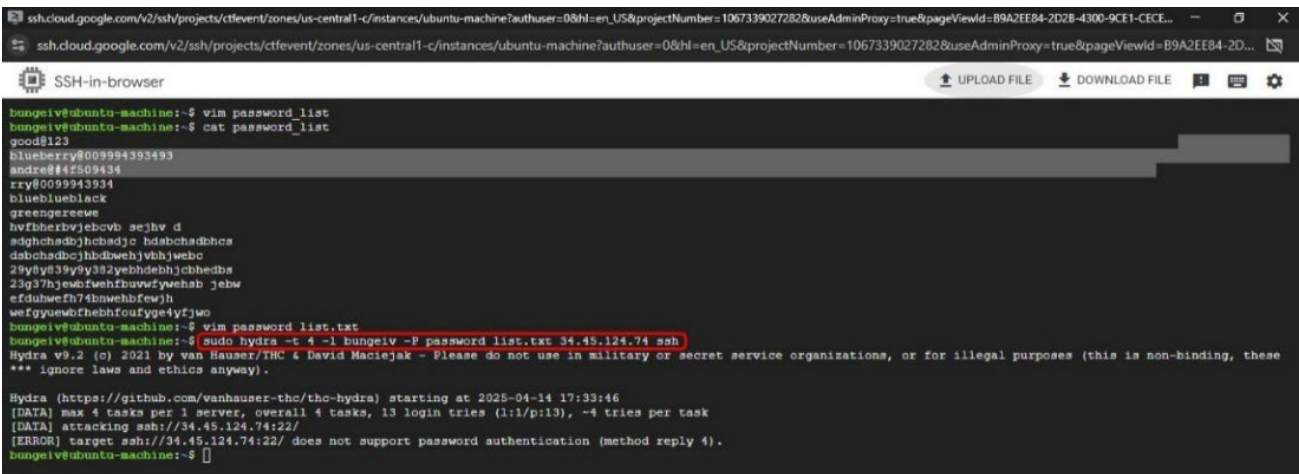


Fig. 6. Brute-force payload using Hydra

**Phase 3: Simulated attack scenarios (weeks 7–11)** In this phase, controlled adversarial activities were introduced, including a simulated SSH brute-force attack using Hydra against a monitored Linux endpoint. Figure 6 shows a brute-force payload executed against the victim endpoint. Teams configured Active Response rules to automatically block the attacking IP after exceeding a defined threshold of failed login attempts.

Figure 7 illustrates the detection log generated by Wazuh. After detection, Wazuh cut the connection between the victim machine and the adversary, evidenced by the 100% packet loss in Figure 8. All student teams achieved correct configuration of the detection rules, though two teams initially set overly

restrictive thresholds, resulting in false positives. This prompted a class discussion on balancing detection sensitivity with operational stability.

Furthermore, students tested Wazuh's threat intelligence integration by introducing a known malicious executable into a monitored endpoint. The file hash was compared against VirusTotal's database via the Wazuh integration module, producing an alert with detailed threat classification. Figures 10 and 11 show the process from the moment a malicious file was downloaded to its detection by Wazuh. From the alert, students could link directly to VirusTotal to review the reporting threat intelligence sources, as shown in Figure 9.

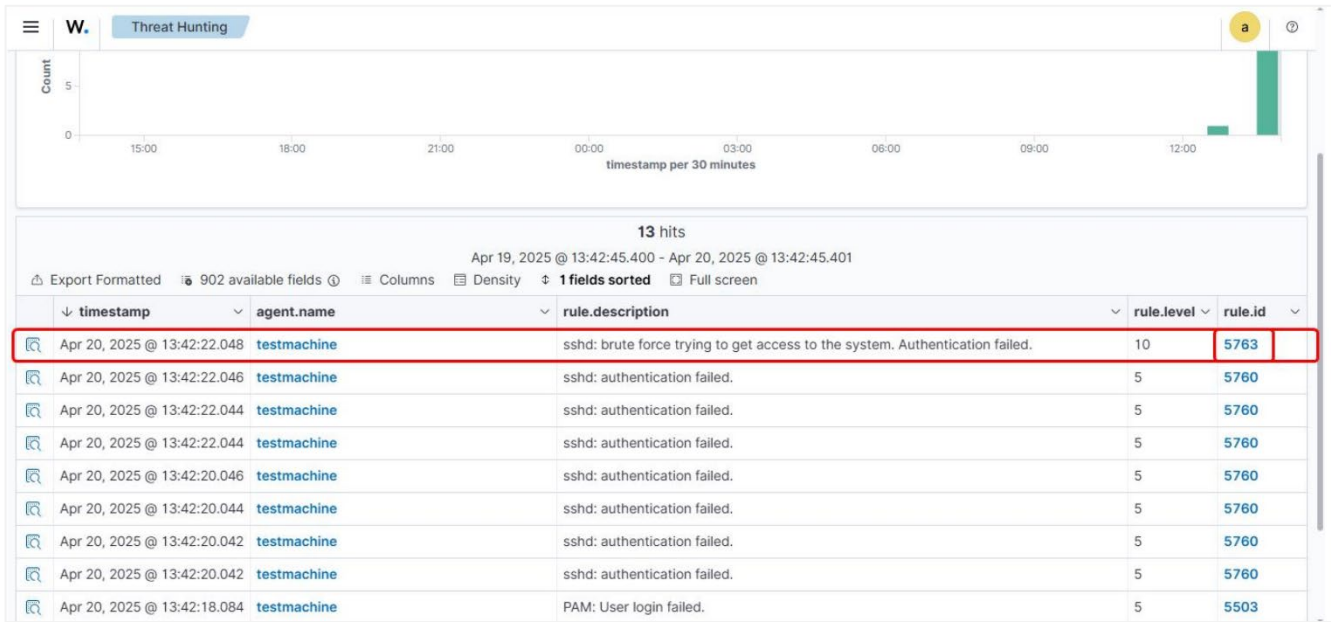


Fig. 7. Brute-force attack detected by Wazuh

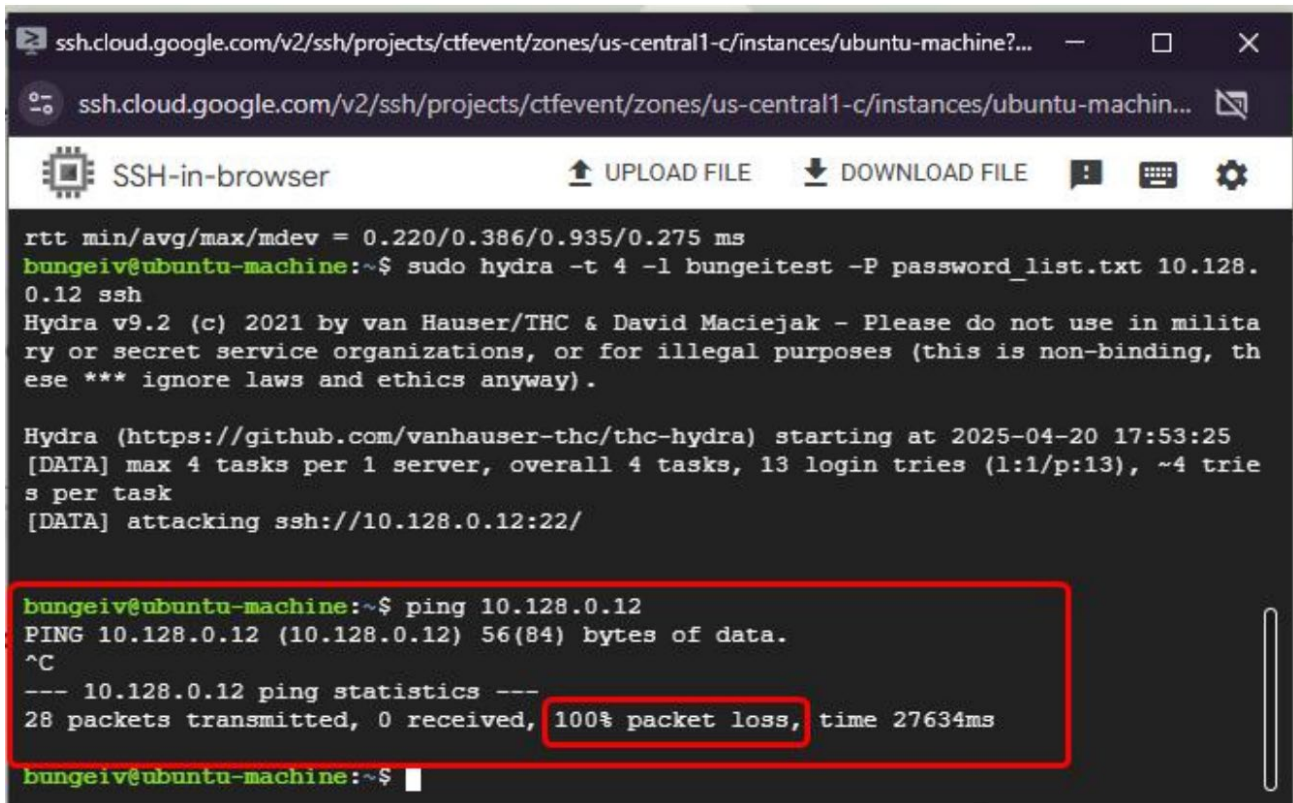


Fig. 8. Wazuh's response by disconnecting the connection between attacker machine and victim machine

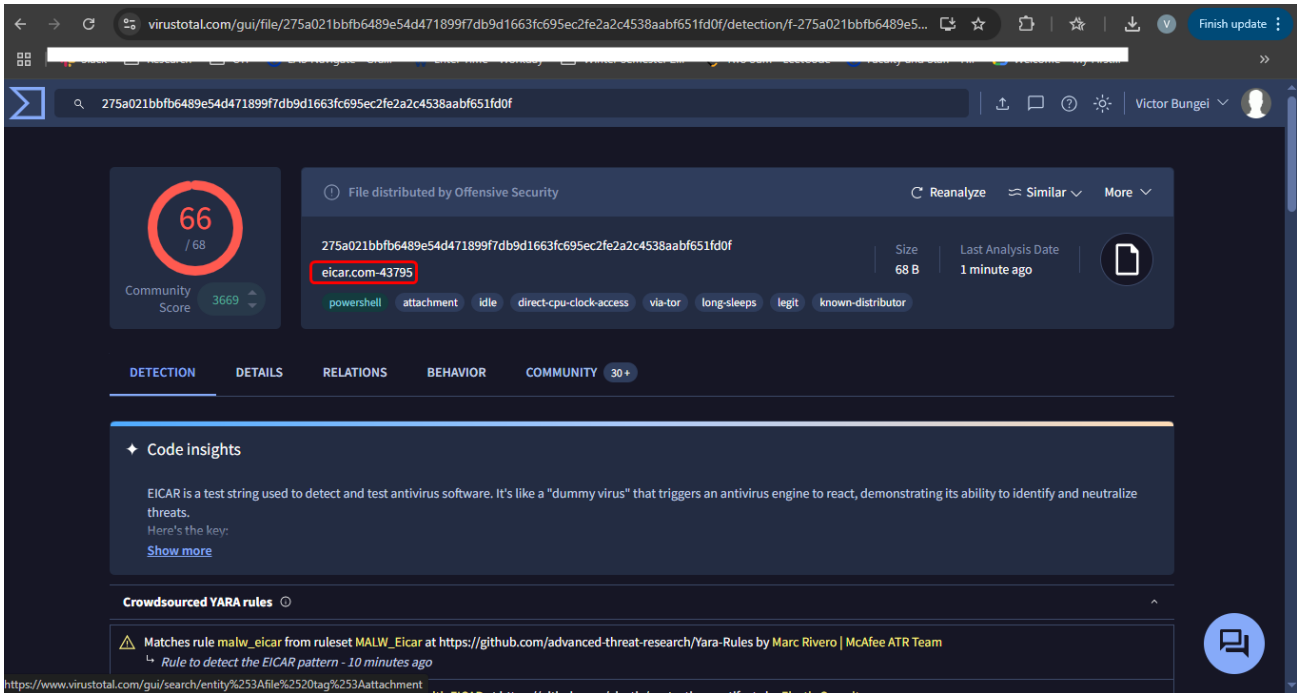


Fig. 9. Malware score based on VirusTotal

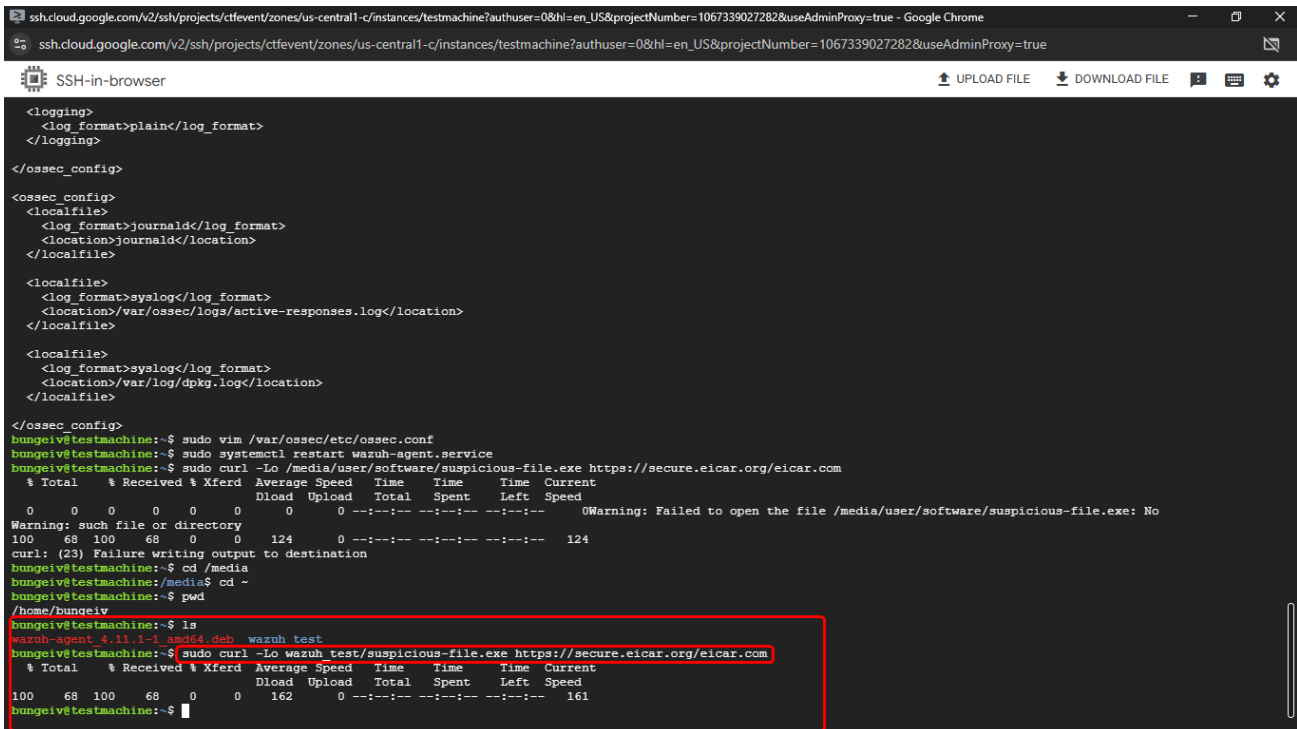


Fig. 10. Malicious file download

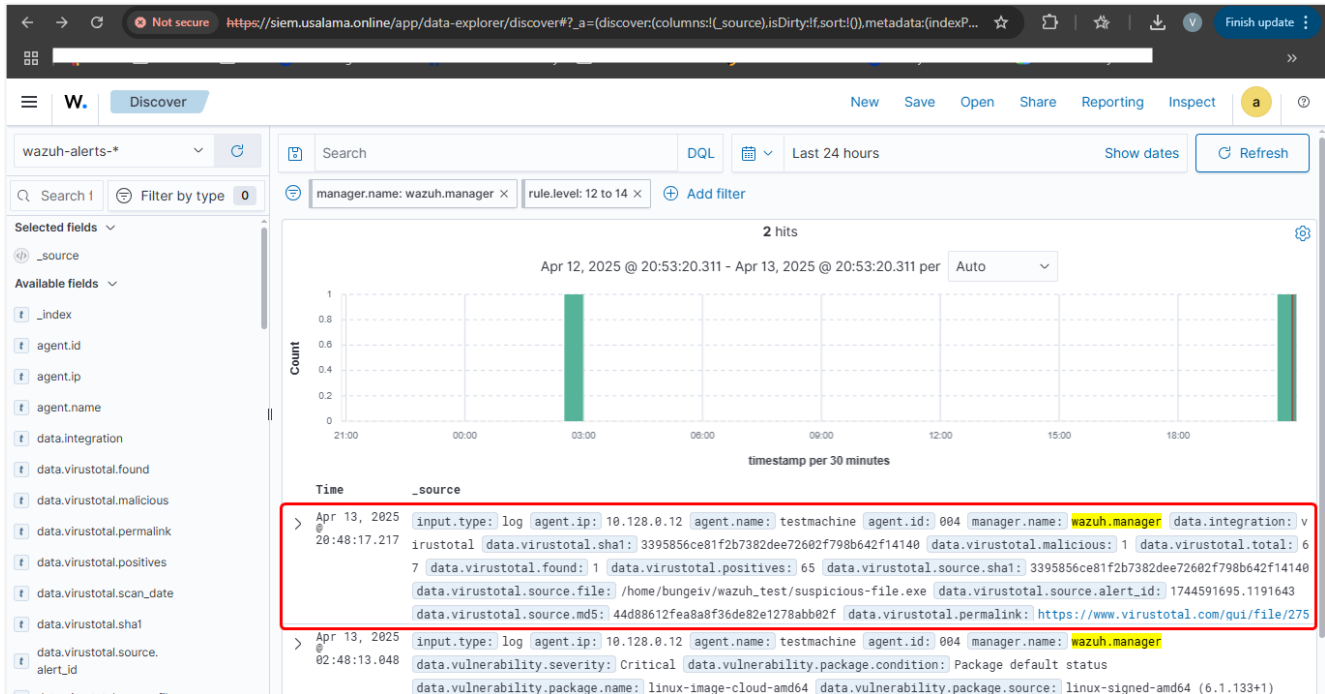


Fig. 11. Malware detected by Wazuh

Then students were required to validate the threat intelligence match, assess potential system impact, and produce an incident report summarizing their findings. Seventeen of eighteen teams met the reporting requirements, though only twelve provided an impact assessment that aligned with standard SOC reporting practices [18]. The case study primarily focused on technical skills, giving students hands-on experience with detection and system configuration. Reporting was included, but the emphasis on proper documentation was limited. For courses with a stronger focus on reporting, providing clearer instructions and templates for incident documentation could help students produce more complete, accurate, and professional reports.

**Phase 4: System Analysis, Reporting, and Presentation (weeks 12–14)** In the final phase, each team compiled an incident report summarizing attack vectors, Wazuh alert analysis, detection and response strategies, and recommendations for hardening. Deliverables include a written report, configuration files, and a final presentation showing their results and findings.

## VI. ASSESSMENT AND EVALUATIONS

Assessment in this project follows the principles of authentic evaluation as described by Villarroel *et al.* [4], with emphasis on technical accuracy, analytical reasoning, and the quality of teamwork. By embedding the Wazuh project into this educational framework, the methodology not only develops practical tool-specific expertise but also fosters the

professional competencies expected in NICE work roles such as Cyber Defense Analyst and Systems Security Analyst.

Our assessment methodology was applied through four key steps:

1. *Contextual Alignment:* As previously shown in Table I, we identified the knowledge, skills, and competencies students must acquire to succeed in the workforce, in alignment with the course learning outcomes. The NICE and ACE frameworks were used to map relevant tasks, knowledge areas, and work roles, ensuring professional relevance.
2. *Realistic Task Design:* Lab tasks were constructed to reflect cybersecurity scenarios that require high cognitive skills, including analysis, synthesis, and evaluation. Students applied these skills within the context of Wazuh-based endpoint protection.
3. *Transparent Evaluation Criteria:* Detailed project rubrics were provided to outline specific requirements and criteria for assessment. This transparency increased engagement and provided a structured basis for evaluating student performance.
4. *Iterative Feedback:* Formative feedback was delivered throughout the semester. This way, students were able to refine their approaches, improve technical accuracy, and improve professional incident reporting skills.

Building on this assessment, the project evaluation focused on three key aspects to measure both technical learning outcomes and collaborative competencies over the semester:

1. **Student Competence Evaluation:** Students' technical skills and understanding were assessed at the beginning and end of the course. Key competencies included the ability to install and configure Wazuh, identify threats and vulnerabilities, assess associated risks, integrating threat intelligence, correlating alerts, monitor and detect suspicious activities. Evidence was gathered through lab submissions, configuration files, and final report and presentation, which were graded against a rubric (Table II) emphasizing accuracy, completeness, and analytical depth. Instructor observations during lab sessions provided further qualitative insight into problem-solving approaches and adaptability under realistic time constraints.

2. **Student Group Evaluation:** Team-based performance was evaluated to measure collaborative skills, manage task dependencies, and overall project outcomes within specified deadlines. Metrics included the number and accuracy of identified threats, and completion of scenario tasks within the expected timeframe.
3. **Peer Evaluation:** Students also provided feedback on the contributions of their teammates, offering insights into individual engagement, communication skills, and professional behavior within the group setting. Peer evaluations were collected using structured scoring (1–10 scale) and qualitative comments, providing additional context to both competence and group performance.

## VII. RESULTS

The results of the Wazuh-based educational project demonstrate both technical effectiveness in achieving learning outcomes and pedagogical impact on student engagement. We summarize the findings along two dimensions: technical task performance and student perception.

TABLE II. Student Competence Evaluation Rubric

Outcome Measure	Evaluation Criteria
Wazuh Installation and Configuration	Quality and depth of system setup; understanding and application of configuration principles; clarity in documenting installation and setup rationale.
Threat Detection and Analysis	Critical analysis of detected threats; effectiveness in identifying vulnerabilities; depth of reasoning in interpreting alerts and correlating events; ability to synthesize information from multiple sources.
Threat Intelligence Integration	Effectiveness in integrating external intelligence sources; depth of insight in interpreting results; application of intelligence to support incident analysis.
Lab Submissions	Detail, accuracy, and timeliness of submitted documents; demonstration of progress and adaptation based on feedback received from prior lab.
Critical Thinking	Quality of reasoning and problem-solving; ability to analyze information and make informed decisions.
Team Work	Contributed meaningfully to the development of shared goals; actively participated in group discussions; completed assigned tasks on time; prepared high-quality work; provided constructive feedback to peers; contributed significantly to the success of the project; demonstrated ethical behavior.
Presentation	Effectiveness in presenting findings to peers and instructors; clarity, organization, and engagement of oral and visual communication.
Time Planning and Management	Timeliness and consistency of submissions; ability to meet project milestones without compromising depth or quality of analysis.

### A. Technical Task Performance

Students successfully completed a sequence of progressively complex tasks for the term project. Figure 12 summarizes the completion rates across major project phases. As observed in the results for Wazuh agent deployment, all students successfully completed the deployment and configuration of agents, as this step serves as the backbone for next phases of the project. Students were provided with well-documented lab instructions and received in-class support to troubleshoot issues. Also, this phase did not require advanced scripting, which made it easier for most students to complete successfully.

The malware detection task using VirusTotal integration had a lower completion rate (86%) compared to other tasks. This task required students to extract file hashes from endpoints, query the VirusTotal API, interpret the results, and integrate the findings into Wazuh alerts. The combination of API interaction, understanding malware analysis results, and configuring Wazuh rules added technical complexity. Students with limited experience in external API usage or malware analysis struggled to complete these steps fully, which contributed to the lower completion rate.

### B. Student Feedback and Perception

Our study revealed significant differences in self-reported competencies before and after participation in the Wazuh-based project across several key areas of cybersecurity education. Figure 13 illustrates the aggregated results.

Students reported the highest confidence gains in skills critical to security operations performance following completion of the project.

Importantly, the greatest gains were observed in understanding of Wazuh features, monitoring endpoints and detecting threats, where median scores increased from approximately 2.5 (low-moderate confidence) to around 4.0 (high confidence).

Similarly, students reported substantial gains in conceptual and factual knowledge of real-world tools and applying cybersecurity knowledge to real-world issues, which highlights the effectiveness of the project in bridging the gap between theory and practice.

In contrast, improvements in critical thinking were more modest, with median scores rising only slightly from 3.2 to 3.6. We expected the score, as critical reasoning skills are less likely to shift dramatically over a single semester and are instead reinforced gradually across multiple courses. Nonetheless, students reported better confidence in analyzing findings from multiple data sources, an essential step toward data analysis.

Overall, our results show that using Wazuh in a project-based learning framework helps students gain practical detection and monitoring skills, while also pointing out areas that need stronger instructional support, particularly in interpreting threat intelligence.

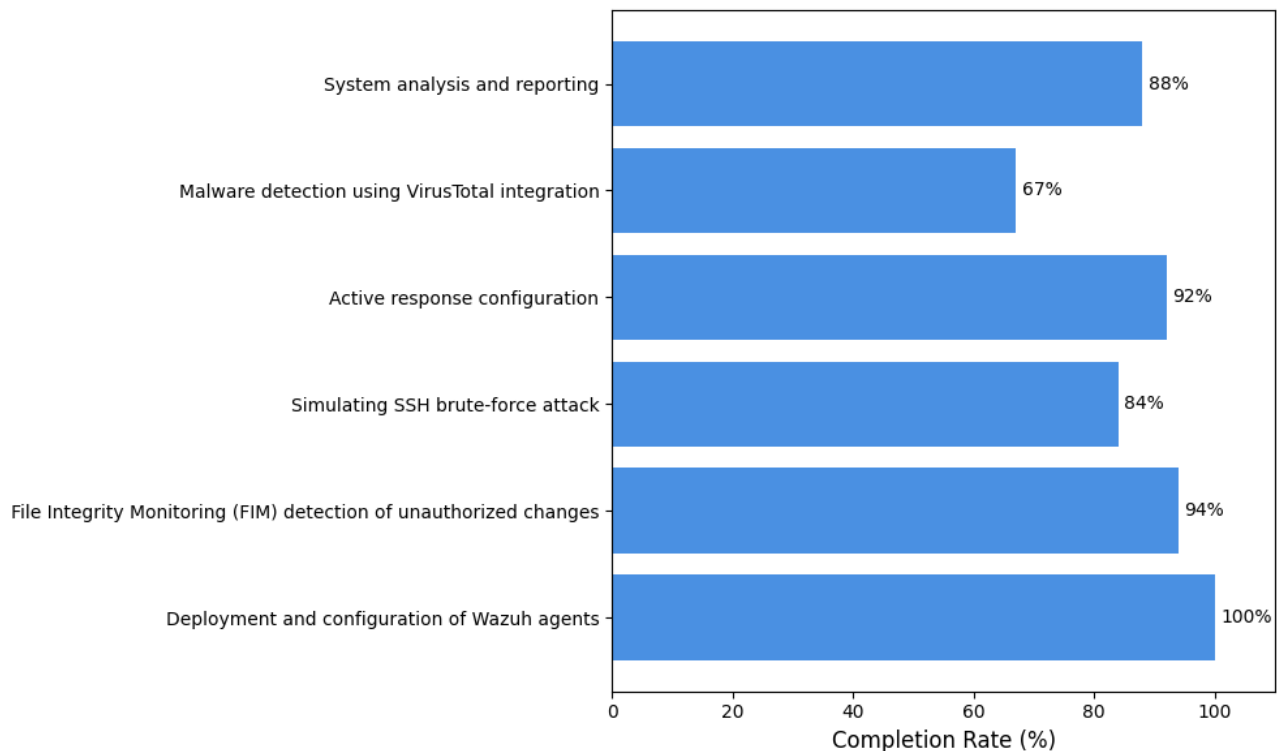


Fig. 12. Student performance across Wazuh project tasks

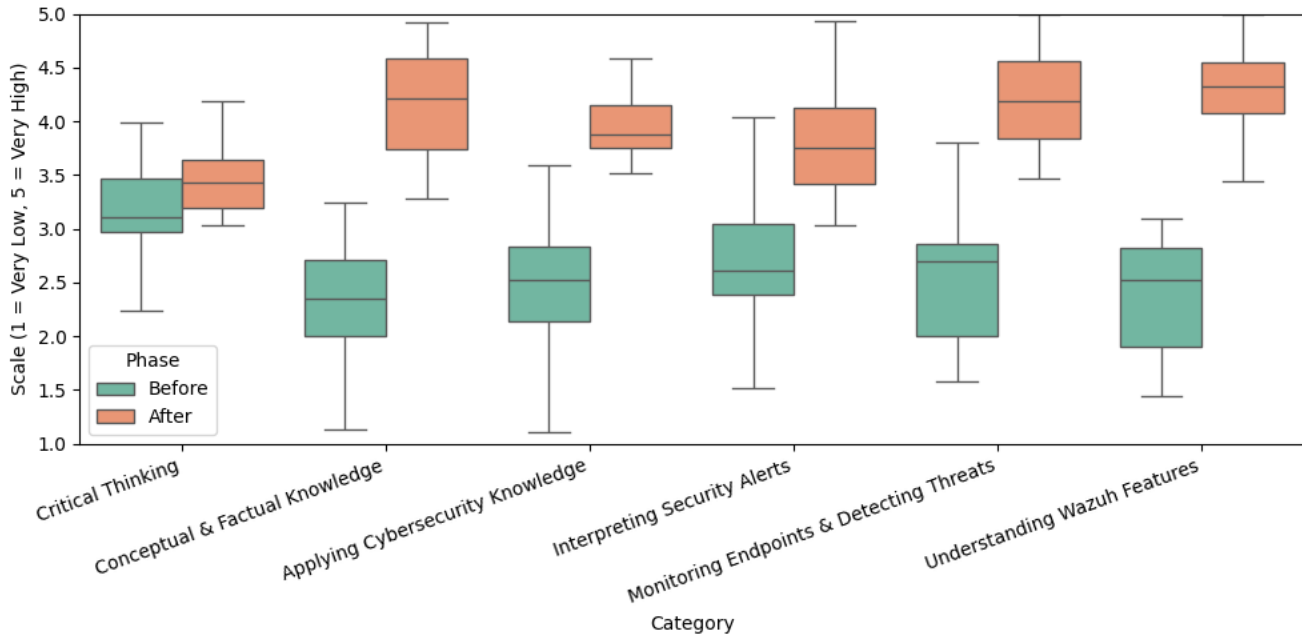


Fig. 13. Student self-assessment of skill gains across major competency areas

## VIII. DISCUSSION

The Wazuh-based project proved effective in demonstrating how realistic endpoint security operations can be embedded into academic settings while advancing competency-based learning.

From the student perspective, the most significant challenges were developing the system on cloud infrastructure, correlating Wazuh alerts, tuning File Integrity Monitoring (FIM) rules and configuring active response scripts. These issues caused misinterpretation of log data, or failed automation, revealing gaps in both technical depth and troubleshooting strategies. Integrating threat intelligence via VirusTotal posed additional hurdles, particularly with API usage and configuration management. In our project, for example, several students misconfigured firewall rules in Google Cloud, which prevented agents from connecting to the Wazuh manager. Others created overly broad monitoring rules that flagged routine system processes as suspicious, overwhelming them with alerts. To address these issues in future iterations, we will provide a minimal working deployment template on Google Cloud with one pre-connected agent to illustrate correct connectivity and distributing pre-defined FIM configuration files for Windows and Linux endpoints that students can later customize. Also, we will provide a short scripting exercise where students debug a pre-broken active response script before applying it in their live environments. These targeted supports would allow students to focus more on analysis and investigative reasoning rather than troubleshooting basic misconfigurations.

From the instructional perspective, the main challenge was the broad range of student technical backgrounds. While

students with stronger background and more hands on experience quickly deployed Wazuh and began experimenting with custom rules, beginner students often struggled with basic Linux commands or troubleshooting agent connectivity, which slowed their overall progress. Our future approach is to design tasks for all teams to complete the required activities, while more experienced students can extend their work by enhancing tasks, such as developing custom detection rules.

**Limitations:** While the findings demonstrate meaningful learning gains, this study is limited by the relatively small sample size ( $N = 18$ ) and the single-institution context. These factors restrict the generalizability of the results to other populations or institutional settings. Future iterations of this work should include larger, more diverse cohorts and longitudinal assessment to examine retention of operational skills over time.

## IX. CONCLUSION

This paper described the design and implementation of a Wazuh-based project for teaching defensive cybersecurity concepts through project-based learning. The exercises allowed students to gain hands-on experience with endpoint monitoring, file integrity checks, threat detection, and active response in a controlled cloud-hosted environment. The project was designed to be integrated into security courses on intrusion detection and prevention.

By embedding open-source SIEM capabilities into a structured, project-based learning model, the study demonstrated how students can engage with realistic endpoint monitoring, threat detection, and incident response tasks in an academic setting. The case study highlighted

measurable gains in students' ability to understand Wazuh features, interpret security alerts, configure monitoring rules, and apply theoretical knowledge to practical scenarios.

The results show the effectiveness of combining real world technical exercises with clear instructional support to ensure that students not only gain tool-specific expertise but also develop analytical and problem-solving skills. The findings also reveal challenges in system configuration and scripting, highlighting the need for curated instructions and structured requirements.

## REFERENCES

- [1] R. Petersen, D. Santos, M. Smith, and G. Witte, "Work-force framework for cybersecurity (nice framework)," National Institute of Standards and Technology, Tech. Rep., 2020.
- [2] National Institute of Standards and Technology (NIST), *Cybersecurity framework*, <https://www.nist.gov/cyberframework/getting-started>, Accessed: 2025-08-12, Washington, DC.
- [3] G. Towhidi and J. Pridmore, "Aligning cybersecurity in higher education with industry needs," *Journal of Information Systems Education*, vol. 34, no. 1, pp. 70–83, 2023.
- [4] V. Villarroel, S. Bloxham, D. Bruna, C. Bruna, and Herrera-Seda, "Authentic assessment: Creating a blueprint for course design," *Assessment & Evaluation in Higher Education*, vol. 43, no. 5, pp. 840–854, 2018. DOI: 10.1080/02602938.2017.1412396.
- [5] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, "Nice: Creating a cybersecurity workforce and aware public," *IEEE Security & Privacy*, vol. 10, no. 3, pp. 76–79, 2012. DOI: 10.1109/MSP.2012.73.
- [6] *National centers of academic excellence in cybersecurity*, <https://www.caecommunity.org/>, Accessed: 2024-01-11, 2024.
- [7] S. Furnell and M. Bishop, "Education for the multifaith community of cybersecurity," in *Computer Security Education*, Cham: Springer, 2020, pp. 32–45. DOI: 10.1007/978-3-030-59291-2\_3.
- [8] M. Hudnall, "Educational and workforce cybersecurity frameworks: Comparing, contrasting, and mapping," *Computer*, vol. 52, no. 3, pp. 18–28, 2019. DOI: 10.1109/MC.2018.2883334.
- [9] National Initiative for Cybersecurity Education, *Work role: Cyber defense analyst (pr-cda-001)*, <https://niccs.cisa.gov/workforce-development/nice-framework>, Accessed: 2025-08-13, National Institute of Standards and Technology, 2020.
- [10] T.-S. Chou, "Labs and three-stage learning process used in a cyber security learning system," in *Proceedings of International Conference on Engineering, Science and Technology*, 2019, p. 54.
- [11] M. A. Pastore, M. Pastore, and E. Dulaney, *CompTIA Security+ Study Guide: Exam SY0-101*. John Wiley & Sons, 2006.
- [12] S. Steiner, A. Jillepalli, and D. C. de Leon, "A survey of cloud-hosted, publicly-available, cyber-ranges for educational institutions," *Journal of computing sciences in colleges*, vol. 38, no. 1, pp. 68–77, 2022.
- [13] B. Sivaneasan, K. Tan, and D. Kumar, "Enhancing cyber security education for engineering adult learners through virtual labs," in *2024 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, IEEE, 2024, pp. 1–8. DOI: 10.1109/TALE62452.2024.10834321.
- [14] D. Bendler and M. Felderer, "Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model," *ACM Transactions on Computing Education*, vol. 23, no. 2, pp. 1–33, 2023. DOI: 10.1145/3573205.
- [15] R. Gupta, *Security Monitoring with Wazuh: A hands-on guide to effective enterprise security using real-life use cases in Wazuh*. Packt Publishing Ltd, 2024.
- [16] H. Pagola, H. Merlino, D. Mazzoni, and P. Peiretti, "Project-based learning in cybersecurity: Methodologies and scope," in *2024 IEEE Biennial Congress of Argentina (ARGENCON)*, IEEE, 2024, pp. 1–8.
- [17] C. Leka, C. Ntantogian, S. Karagiannis, E. Magkos, and V. S. Verykios, "A comparative analysis of virustotal and desktop antivirus detection capabilities," in *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, IEEE, 2022, pp. 1–6. DOI: 10.1109/IISA56318.2022.9904382.
- [18] S. A. Chamkar, Y. Maleh, and N. Gherabi, "Security operations centers: Use case best practices, coverage, and gap analysis based on mitre adversarial tactics, techniques, and common knowledge," *Journal of Cybersecurity and Privacy*, vol. 4, no. 4, pp. 777–793, 2024. DOI: 10.3390/jcp4040036.