University of Batna 2
Department of Computer Science

Lab 1 - Cybersecurity
2025/2026

Lab 1 - SIEM/XDR- Wazuh Installation

Send your report only to: <csclass.dz@gmail.com>

Team information (one report by team)

- First Name Last Name ……………………………………………..
- First Name Last Name ……………………………………………..
- First Name Last Name ……………………………………………..

Deadline: Wednesday, Feb 23, 2026.

Part I — SIEM Fundamentals

1. What does **SIEM** stand for?
2. What is the main role of a SIEM?
3. What types of data does a SIEM collect?
4. What is the difference between **logs, events, and alerts**?
5. Why is log correlation important?
6. What is a **false positive**?
7. What is an **incident** in SIEM?
8. What is the difference between **detection** and **prevention**?
9. What are the main components of a SIEM architecture?
10. What is a **use case** in SIEM?
11. Give two examples of attacks detectable by a SIEM.

Part II — XDR vs SIEM

1. What does **XDR** stand for?
2. What is the main difference between SIEM and XDR?
3. What does a SIEM focus on?
4. What does an XDR focus on?
5. Can SIEM and XDR work together? Explain briefly.
6. What types of sources does XDR monitor?
7. What is automated response in XDR?

Part III — Wazuh Architecture

1. What is Wazuh and what are its main components?
2. Explain the role of each component.
3. Describe the data flow from Agent to Dashboard.

Part IV — Wazuh Installation

1. Install Wazuh on your machine.
2. Report the installation steps in detail (how many VMs used, installed elements, …).
3. Verify that all components and agent(s) are running correctly, generate test events, and confirm that alerts are properly detected and displayed in the Dashboard.