BU/23C/IT/9684

HALA SAMBO

CLOUD COMPUTING

Below is the summary of the notes I took

Wazuh EDR (Endpoint Detection and Response) is an open-source solution created in 2015 that provides tools and applications to monitor devices for suspicious activity and potential security breaches. It uses agents, which are devices being monitored, and a manager that handles these agents. New agents can be deployed by navigating to Wazuh → Agents → Deploy new agents. Wazuh offers a powerful vulnerability assessment module to periodically scan operating systems for installed applications and version numbers, and it can audit and monitor agent configurations while recording event logs. Its security event monitor logs both successful and unsuccessful authentication attempts, typically found at /var/ossec/logs/alerts/alerts.log. Wazuh can also aggregate events from Sysmon for processing and uses the auditd package on Debian, Ubuntu, and CentOS systems. Additionally, the Wazuh management server features a rich API for command-line interaction and a reporting module to view summarized breakdowns of events on agents. The installation comes bundled with sample data that can be loaded at your convenience, making Wazuh an extensive and flexible EDR solution.