3.3 Technology Stack

3.3.1 Tools explored in this project

1. Endpoint Security Tools:

- **Antivirus/Antimalware Software:** Detects, prevents, and removes malicious software from individual devices.
- **Host-Based Intrusion Detection Systems (HIDS):** Monitors activities on individual devices for signs of unauthorized access or malicious behavior.
- **Endpoint Detection and Response (EDR):** Provides continuous monitoring, detection, and response capabilities on endpoints to combat advanced threats.

2. Network Security Tools:

- **Firewalls:** Hardware or software-based security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.
- **Intrusion Detection Systems (IDS) & Intrusion Prevention Systems (IPS):** Monitor network traffic for suspicious activities and take action to block or prevent potential threats.
- **Network Protocol Analyzers (e.g., Wireshark):** Used for troubleshooting, analysis, and security auditing of network traffic.

3. Vulnerability Assessment Tools:

- **Vulnerability Scanners (e.g., Nessus, OpenVAS):** Identify vulnerabilities, misconfigurations, and malware across various platforms.
- **Cloud-Based Assessment Solutions (e.g., Qualys):** Offer vulnerability management and assessment to identify, prioritize, and remediate vulnerabilities.

4. Encryption Tools:

- **Data Encryption Programs (e.g., PGP):** Provide cryptographic privacy and authentication for data communication.
- **Full-Disk Encryption Features (e.g., BitLocker):** Protect data on disk volumes.
- **SSL/TLS Toolkits (e.g., OpenSSL):** Implement protocols for securing communications over a network.

5. Identity and Access Management (IAM) Tools:

- **Directory Services (e.g., Active Directory):** Manage user identities and permissions in a networked environment.
- **Single Sign-On (SSO) Solutions:** Enable users to securely authenticate once and access multiple applications without re-entering credentials.
- **Multi-Factor Authentication (MFA):** Enhances security by requiring users to provide multiple forms of authentication, such as passwords, biometrics, or tokens.

6. Security Information & Event Management (SIEM) Tools:

- **SIEM Platforms (e.g., Splunk, LogRhythm, IBM QRadar):** Collect, analyze, and correlate security event data from various sources to provide real-time insights into potential security threats and incidents.