**Identifying Stakeholders and their Roles.**

1. **Project Manager**

* Manages the project, establishes timelines, and makes certain that resources are used efficiently.
* Guarantees that deadlines and objectives are achieved promptly.

1. **Network Administrators**

* Create and deploy network setups for the NIDS.
* Oversee the system's efficiency and capacity, and establish network monitoring guidelines.

1. **Security Analysts**

* Collaborate with the system to analyze alerts and pinpoint potential threats.
* Create and evaluate detection rules for targeted attacks and anomalies.

1. **System Developers**

* Develop and maintain the software components, including the dashboard, rule engine, and reporting functionalities.
* Ensure seamless integration of the system with other security tools and the overall network infrastructure.

1. **IT Support Team**

* Offer technical support during the installation and deployment of the Network Intrusion Detection System (NIDS).
* Diagnose system issues, monitor performance metrics, and assist with system configuration.

1. **End Users**

* Utilize the Network Intrusion Detection System (NIDS) to actively monitor the network and respond to threats in real-time.
* Analyze alerts and reports to take appropriate actions, such as blocking IP addresses or updating detection rules.

1. **Compliance Officers**

* Ensure the NIDS adheres to industry regulations and standards, such as GDPR and HIPAA.
* Assist in implementing and maintaining data privacy and security measures throughout the project's lifecycle.

1. **Executive Management**

* Define and communicate the project's vision and strategic direction to align stakeholders and guide the team.
* Allocate the necessary budget and resources effectively, and evaluate the project's success against predefined metrics and goals.

1. **Forensic Investigators (If needed)**

* Leverage historical data collected by the NIDS to conduct thorough post-incident analyses and investigations.
* Assist in identifying previously undetected threats by performing deep analyses of past network traffic patterns and behaviors.

10. **Vendors**

* Provide any necessary third-party tools, hardware, or software needed for the project, including packet capture tools, analytics platforms, or specialized equipment.