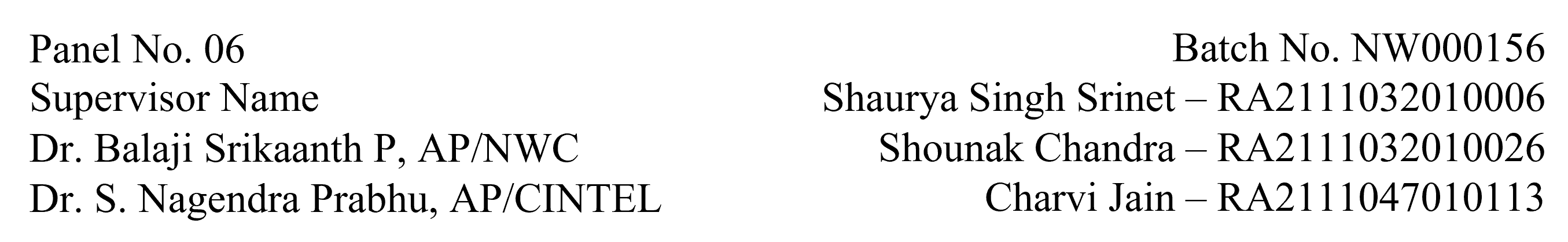
**DDoS Protection System for Cloud: Architecture and Tool**

****

**Functional Document for User Story 4: Performance Testing and System Integration**

**1. Introduction**

This user story focuses on performance testing and integrating the anomaly detection system into the cloud environment. The aim is to evaluate system scalability, monitor performance during high-traffic conditions, and set up CloudWatch alarms for real-time monitoring and alerts.

**2. Product Goal**

To integrate the anomaly detection system into a live environment, ensuring it scales under high traffic loads while maintaining accuracy. Alerts and performance metrics will be used to monitor system health.

**3. Demography (Users Location)**

* **Target Users:** Cloud engineers, security teams, operations managers.
* **User Characteristics:** Users responsible for maintaining cloud infrastructure and monitoring performance.
* **Location:** Organizations globally using cloud-hosted services.

**4. Business Processes**

* **Performance Testing:**
  + Use JMeter to simulate high-traffic conditions, including attack scenarios.
  + Monitor system scalability and response times.
* **System Integration:**
  + Deploy the anomaly detection script in the cloud environment.
  + Configure CloudWatch for traffic monitoring and alerts.

* **Alert Setup**:
  + Define thresholds for triggering alerts.
  + Set up email notifications for anomalies and high-traffic scenarios.

**5. Features**

* **Traffic Simulation:**
  + Simulate high traffic loads with JMeter for performance testing.
* **Cloud Integration:**
  + Deploy detection scripts in the cloud environment (AWS EC2).
* **Monitoring and Alerts:**
  + Configure CloudWatch to monitor traffic and system performance.
  + Send alerts via email when thresholds are breached.

|  |  |
| --- | --- |
| **ROLE** | **Access Level** |
| Operations Manager | Read-only access to performance reports. |
| Cloud Engineer | Full access to cloud environment and monitoring. |
| Security Analyst | Access to monitoring metrics and alert configurations. |

**6. Authorization Matrix**

**7. Assumptions**

* Cloud environment is set up and accessible.
* JMeter tests run successfully without errors.
* CloudWatch is correctly configured for monitoring.

**8. Target Audience**

* **Audience:** Cloud security teams, operations managers, cloud engineers.
* **Effort Estimation:** Approximately 4-5 days for testing and integration.

**9. Acceptance Criteria**

* Performance tests are completed with metrics recorded.
* The anomaly detection system is deployed and functional in the cloud.
* CloudWatch alarms are configured and sending alerts for anomalies.

**10. Checklist**

* JMeter traffic simulations executed.
* Anomaly detection script deployed in the cloud.
* CloudWatch metrics and alerts configured.
* Alerts validated for accuracy and timely delivery.