NIST SP 800-52 recommendations for handling a security incident:

**1. Monitor Alerts in SIEM (Security Information and Event Management) System**

* You identified suspicious activities through alerts triggered in your SIEM system, such as failed login attempts, SSH authentication, and logins from an unknown or suspicious IP address. This is consistent with NIST 800-52’s guidelines to monitor systems for suspicious activity using secure communication channels and logging mechanisms.

**2. Verify IP Address Reputation**

* By checking the reputation of the flagged IP address using an external database (IP scanner tool), you verified the malicious intent behind the activity. This matches the NIST guideline to ensure that malicious traffic is detected and validated as part of a secure incident response procedure.

**3. Escalate the Incident**

* After identifying the threat, you escalated the event to the appropriate SOC team member. NIST emphasizes that once suspicious activities are identified, proper communication and escalation procedures are essential for mitigation. You correctly routed the information to the SOC Team Lead.

**4. Block the Malicious IP Address**

* Following verification, you took immediate action to block the malicious IP address via the firewall. NIST 800-52 recommends blocking any identified threats to ensure they no longer pose a risk to the system. This step directly aligns with preventing further intrusions or data compromise from known malicious entities.

**5. Document Incident Resolution**

* The final step, confirming that the malicious IP was blocked and the incident resolved, reflects NIST's focus on documenting incidents and maintaining proper logs for future reference. The SIEM system and firewall logging these actions are crucial for maintaining a secure system.