Email Authentication in SOC 🛡️

“When analyzing suspicious emails, understanding SPF, DKIM, and DMARC is key. Here’s what I’ve learned as someone building SOC skills:”

Investigation Workflow:

🔍 1. SPF (Sender Policy Framework)

- Checks if the email came from an **authorized sending server**.
- Steps I follow:
  - 📌 Look up the domain’s SPF record in DNS.
  - 📌 Verify the sending IP against authorized IPs.
- Outcome:
  - ✅ Pass → sender is authorized
  - ❌ Fail → email may be spoofed or spam

🧠 2. DKIM (DomainKeys Identified Mail)

- Ensures the email **hasn’t been tampered with** and is really from the sender domain.
- Steps I follow:
  - 📌 Check for a DKIM signature in the email header.
  - 📌 Verify signature using the domain’s public key from DNS.
- Outcome:
  - ✅ Pass → email integrity verified
  - ❌ Fail → content may have been altered or forged

📬 3. DMARC (Domain-based Message Authentication, Reporting & Conformance)

- Uses SPF & DKIM results to enforce policies and report suspicious emails.
- Steps I follow:
  - 📌 Check the domain’s DMARC policy in DNS.
  - 📌 Understand policy actions:
    - **None:** Monitor only
    - **Quarantine:** Send to spam
    - **Reject:** Block email completely
- Extra: Review DMARC reports to track who is sending emails on behalf of the domain

---

As a learner in SOC, understanding SPF, DKIM, and DMARC helps me **analyze suspicious emails systematically**, detect phishing attempts, and strengthen email security.

#LearningSOC #CyberSecurity #EmailSecurity #SPF #DKIM #DMARC #SOCJourney #IncidentResponse #CyberSecLearning