Answers

1. Initial Infection Vector

- **Email Logs:**
  The email sent from `noreply@secure-billing.com` to `pmiller@steelflow.local` with the subject "Payment Failed - Action Required" contained an attachment: `PaymentDetails_2024.exe`.
    - **Key IOC:** The `.exe` file is an unusual attachment and likely malicious.
    - **Supporting Evidence:**
        - **Endpoint Logs:** `PaymentDetails_2024.exe` was downloaded and executed by `pmiller@steelflow.local`.
        - **System Event Logs:** A scheduled task named `UpdateScheduler` was created shortly after the execution, a common persistence tactic in ransomware attacks.

---

2. Scope of the Attack

- **Affected User:** `pmiller@steelflow.local` initiated the attack by executing the malicious file.
- **Propagation:**
    - **Firewall Logs:** Outbound connection from `192.168.10.12` (user `pmiller`) to a suspicious IP `185.212.123.45` on port `9001` indicates communication with a ransomware command-and-control (C2) server.
    - **File Modifications:** Unauthorized modifications to files in the shared drive:
        - `C:\\Shared\\ProductionData.xlsx`
        - `C:\\Shared\\Financial_Report.docx`
    - **Lateral Movement:**
        - **Firewall Logs:** Inbound SMB traffic on port `445` from `192.168.10.12` to `192.168.10.20` suggests the ransomware attempted to spread to other systems via the shared drive.

---

3. Indicators of Compromise (IOCs)

- **Email Logs:** Malicious email with `.exe` attachment.
- **Endpoint Logs:** Execution of `PaymentDetails_2024.exe` by `pmiller`.

- **System Event Logs:**
  - Creation of a suspicious scheduled task: `UpdateScheduler`.
  - Failed login attempts and remote desktop session activity from unusual IPs.
- **Firewall Logs:**
  - Outbound connection to `185.212.123.45` on port `9001` (C2 server).
  - Lateral movement via SMB traffic on port `445`.

---

4. Recommendations for Containment and Recovery

1. **Containment:**
   - Isolate the infected endpoint (`192.168.10.12`) from the network.
   - Block outbound traffic to the suspicious IP (`185.212.123.45`) at the firewall.
   - Disable the scheduled task `UpdateScheduler` on `pmiller@steelflow.local`.
   - Lock down SMB access temporarily to prevent further lateral movement.

2. **Forensic Analysis:**
   - Preserve logs and a copy of the malicious file (`PaymentDetails_2024.exe`) for analysis.
   - Investigate other systems for signs of infection (e.g., unusual processes, encrypted files).

3. **Recovery:**
   - Restore affected files from backups after ensuring the infection is fully removed.
   - Reimage the infected system to eliminate persistence mechanisms.

4. **Post-Incident Actions:**
   - Train employees on recognizing phishing emails and suspicious attachments.
   - Implement stricter email filtering to block malicious file types like `.exe`.

- Deploy advanced endpoint protection to detect and quarantine ransomware activity.
- Monitor for additional unauthorized activity using a SIEM platform.

Summary

The attack began with a phishing email targeting `pmiller`. The user downloaded and executed a malicious `.exe` file, which led to file encryption and attempted lateral movement. Immediate containment and recovery actions should focus on isolating the infected endpoint, blocking C2 communication, and restoring from backups.