server baselines have not been updated to incorporate security patches released in the last quarter.

- **Gap - Network Devices:** Formalized baseline configurations for network switches and firewalls have not yet been developed or enforced. A project to address this is scheduled for Q3 2025.

3. Conclusion:
Control PR.IP-1 is partially implemented. While foundational baselines exist for key systems, they require updates, and coverage needs to be extended to network infrastructure.

Content for `Justification_DE.CM-1.pdf`

Document Title: Justification for Control DE.CM-1: Network Monitoring

Date: June 14, 2025

1. Control Implementation:
Continuous network monitoring is achieved through our SIEM solution, which aggregates and analyzes log data from across the enterprise network.

2. Evidence:

- **Technology:** The organization utilizes a market-leading SIEM platform. Log sources include firewalls, domain controllers, critical application servers, and endpoint detection and response (EDR) agents.
- **24/7 Monitoring:** The Security Operations Center (SOC) is staffed around the clock to investigate and respond to SIEM alerts.
- **Alerting Rules:** Custom alerting rules have been developed to detect common attack techniques, such as brute-force login attempts, malware signatures, and