1. Executive Summary

A security incident involving unauthorized access attempts was detected on a monitored system. The incident was identified through SIEM alerts, analyzed by the SOC team, and contained without business impact. Immediate response actions were taken to prevent further risk, and recommendations were provided to strengthen security controls.

(Keep this **non-technical**, ~80–100 words.)

---

2. Incident Overview

- **Incident Type:** Brute Force / Unauthorized Access
- **Detection Source:** SIEM Alert
- **Affected System:** Server-X
- **Severity:** Medium
- **Status:** Contained

---

3. Timeline of Events

Time	Action
11:00	Alert triggered in SIEM
11:05	Analyst reviewed logs
11:10	Incident classified
11:15	Host monitored / access restricted
11:25	Incident documented

---

4. Detection and Triage

The alert was generated after multiple failed authentication attempts were detected from a single source. Initial triage confirmed the activity as a true positive based on log correlation and threat intelligence validation.

- **Event ID:** 4625
- **Source IP:** 192.168.1.100
- **Failed Attempts:** Multiple
- **MITRE Technique:** T1110 – Brute Force

---

5. Incident Response Actions

Actions taken during response:

- Reviewed authentication logs
- Assessed scope of activity
- Monitored affected system
- Recommended account lockout and IP blocking

No evidence of successful compromise was found.

---

6. Impact Analysis

- No data loss observed
- No service disruption
- No lateral movement detected

The incident was contained at an early stage.

---

7. Recommendations

- Enforce account lockout policies
- Strengthen password complexity
- Improve alert thresholds
- Conduct user awareness training

---

8. Conclusion

The incident was detected and handled effectively following SOC best practices. The structured response minimized risk and demonstrated the importance of proactive monitoring and alert triage.