# Insufficient Logging & Monitoring (Alerting Delay)

**Insufficient Logging and Monitoring** refers to the failure to properly:

* **Capture security-relevant events** (e.g., logins, access attempts, privilege changes),
* **Store and protect logs securely**, and
* **Alert on suspicious or malicious behavior** in a timely manner.

When combined with **Alerting Delay**, this issue allows attackers to:

* Operate stealthily,
* Maintain persistence, and
* Exfiltrate data without detection.

# Why It’s Dangerous

Most breaches go **undetected for weeks or months** due to:

* No logs,
* Logs not centralized,
* Logs not analyzed,
* Alerts not configured or delayed,
* Teams not monitoring at all.

# Impact

| Area | Risk |
| --- | --- |
| Undetected Intrusions | Attacker can move laterally or persist |
| Regulatory Non-Compliance | Violates PCI-DSS, HIPAA, GDPR, ISO 27001 |
| Delayed Response | Increases cost and impact of breach |
| No Forensics | Hard to investigate or trace root cause |
| Repeat Attacks | No lessons learned = repeated compromise |

# Examples of Insufficient Logging & Alerting Delays

| Scenario | Problem |
| --- | --- |
| Admin login from unknown IP not logged | Can’t detect unauthorized access |
| Failed logins not tracked or counted | Brute force goes unnoticed |
| Role changes not logged | No trace of privilege escalation |
| Data download events not recorded | Exfiltration undetected |
| No alerts on WAF bypass or anomalies | No real-time monitoring |
| Alert delay of 12–24 hours | Too late for prevention or quick response |
| Logs accessible to all users | Tampering or data leakage risk |

# Testing Techniques

| Test | Description |
| --- | --- |
| Log Tampering | Try log poisoning or deleting logs — see if alert is triggered |
| Unauthorized Access | Attempt access from unusual IP/location |
| Replay/Brute Force | Monitor whether repeated failed logins are flagged |
| Role Escalation | Change roles or access levels and review logging behavior |
| Monitor Timing | Trigger a known alertable event and see how long it takes to notify |

# What Should Be Logged

| Event | Why |
| --- | --- |
| Logins (success/failure) | Detect brute force, unauthorized access |
| Privilege changes | Identify role abuse |
| Data exports/downloads | Detect exfiltration |
| Password resets | Monitor account recovery misuse |
| API usage | Monitor abuse or DDoS |
| WAF/IDS logs | Detect known attacks (SQLi, XSS) |
| Backend errors (500s) | Reveal exploitation attempts or DoS |

# Tools for Logging & Monitoring

| Tool | Purpose |
| --- | --- |
| SIEMs (Splunk, ELK, QRadar, Graylog) | Log aggregation, parsing, alerting |
| Wazuh / OSSEC | Host-based intrusion detection |
| Falco / CrowdStrike / EDRs | Runtime behavior monitoring |
| Security Onion | Network and endpoint security monitoring |
| Syslog / AuditD / journald | System-level log capture |
| PagerDuty / OpsGenie / Email | Alerting and escalation |

# Alerting Delay: Key Problem Areas

| Issue | Solution |
| --- | --- |
| Batch-based log processing (1–24 hrs delay) | Use real-time pipelines (e.g., Kafka + ELK) |
| No alert thresholds or logic | Define alerts for anomalies like >5 failed logins |
| No integrations (email/SMS/Slack) | Integrate alert channels with on-call schedules |
| No SOC/SIEM analyst to respond | Automate detection → response playbooks |

# Mitigation

## 1. Implement Centralized Logging

* Use a SIEM (Splunk, ELK, Wazuh)
* Ship logs from:
  + Web servers
  + App servers
  + Databases
  + WAFs / firewalls
  + APIs

## 2. Configure Alerting

* Alert on:
  + 5+ failed logins in 10 minutes
  + Admin login from new country
  + API key abuse or traffic spike
  + Unauthorized file access

## 3. Enable Real-Time Detection

* Use real-time log streams (e.g., Fluentd + Elasticsearch + Kibana)
* Avoid batch-based or once-a-day alerts

## 4. Secure and Protect Logs

* Store logs **write-only** (no deletion by app users)
* Restrict access to logs via RBAC
* Sign or hash logs for integrity

## 5. Regular Review & Audit

* Review logs weekly or during threat hunting
* Set up **log retention policy** (e.g., 90 days min)

# Compliance Requirements

| Standard | Logging Requirements |
| --- | --- |
| PCI-DSS | Log all access to cardholder data, retain logs for 1 year |
| HIPAA | Log access to ePHI, alert on suspicious access |
| GDPR | Ensure ability to detect personal data breaches |
| ISO 27001 | Log security events and review periodically |

# Points

“Insufficient logging is **not just a security flaw**, it’s an **incident response failure** — you can’t stop what you can’t see.”

“Always recommend that logs include **timestamps, IPs, usernames, and request context**, and that alerts trigger within **seconds** for critical actions.”

“Our detection maturity depends on **real-time visibility, correlated alerts, and the ability to respond fast**.”