When it comes to exploitation of cybersecurity, insufficient logging and monitoring have been the major cause of incidents. Attackers are always on a lookout for opportunities like lack of monitoring and timely detection and response to an incident. Security event logging and Monitoring is a procedure that associations perform by performing electronic audit logs for signs to detect unauthorized security-related exercises performed on a framework or application that forms, transmits, or stores secret data. [bctt tweet=”Insufficient logging and monitoring vulnerability occur when the security-critical event is not logged off properly, and the system is not monitored. #logging #monitoring #cybersecurity ” username=”crAPI”]Lack of such functionalities can make malicious activities harder to detect and in turn affects the incident handling process.

**Why are Logging and monitoring considered to be important?**

When a malicious insider with authentic reasons for querying databases, accessing applications, modifying system configurations, and obfuscate records, organizations are left powerless to detect what happened. Hence, details of logging of user access are essential for securing and preventing data breach/theft.

Log monitoring is considered important for several reasons. One of the reasons includes **Log monitoring can prevent downtime on your sites and servers**. Log management tools analyze logs and find problems within them, allowing your site reliability engineers to spend more time-solving problems and less time searching for them or responding in emergencies. **Log monitoring can save your company valuable time and money.**

**Log monitoring can be split up into three parts:**

* **Log collection:**  this includes log enrichment like parsing of logs, converting of logs, filtering of logs, etc.
* **Log management:** keeping data retention policies, keeping shards/indexes for better performance, implementing access control as logs contain sensitive information, etc.
* **Log monitoring/analysis:** visualization, alerting, reporting.

**Remediation**

* Make sure the logs are backed up and synced to another server. The attacker should not be able to clear all the logs after hacking the server and by doing so preventing any forensics. Integrity of the log collection system is the core of any forensic investigation.
* Go over the system and make sure sensitive actions are logged. This would include logins, high-value transactions, password changes, and so on. This is valuable when investigating a hack afterward.
* Make it a routine to look at the most important logs and automate the process for the rest. There should be a system in place that alerts you if a specific warning has been triggered or if a certain warning threshold has reached to accordingly take necessary measures.

**Conclusion**

**Insufficient logging is the most common reason why companies fail to deal with a security** breach effectively. Organizations must be equipped by logging the entire activity or it could be difficult for the organization to find the criminal. Not being able to detect at an early stage may further lead to the occurrence of continuous breaches and significant losses. To stay well informed and compliant, taking appropriate measures and having in place loggings and monitoring is essential.

**4.3** / **5** ( **3** votes )