PGBC Log File Intelligence

Actionable AI Intelligence for your files and data from Fully Encrypted Log Files: Security, Compliance, Privacy

OmniIndex

White Paper

OmniIndex

The Log File Challenge

A key way to gain intelligence is through analyzing log files. This is because they provide a detailed record of system activity, enabling you to identify and predict security incidents and audit user activity.

However, log files also offer a dangerous repository of information for potential attackers, meaning they need to be constantly protected from manipulation & unwanted access.

The Log File Solution

Only OmniIndex enables logs to remain encrypted at all times even while being analyzed with AI/ML. This ensures they're protected while still enabling real-time actionable AI intelligence.

OmniIndex

Secure Log File Management

OmniIndex PGBC handles log files through a unique, security-first architecture that transforms them from a simple record into a source of inoculated real-time intelligence.

This is achieved through three core principles:

Immutable and Decentralized Storage:
All log files are stored on PGBC, a Web3 fork of Postgres. This means every log entry is recorded on a blockchain, making it cryptographically immutable. Once written, a log cannot be altered or deleted by anyone, including administrators, which guarantees the integrity of the data against tampering or ransomware. This ledger is also decentralized across a network of nodes, eliminating any single point of failure and ensuring continuous availability.

The 'Never Decrypt' Workflow:
From ingestion to analysis, log files remain fully encrypted at all times: at rest, in transit, and most importantly, in use. This "never decrypt" workflow eliminates the primary vulnerability of traditional systems, where data must be decrypted to be analyzed. By keeping logs perpetually encrypted, it ensures that even if the system is compromised, the sensitive information within the logs remains secure and unreadable.

Real-Time Encrypted Analysis (FHE):
The platform leverages patented Fully Homomorphic Encryption (FHE) to analyze the encrypted log files in real-time. This allows a native AI to continuously monitor all system activity, detecting and alerting on compliance breaches or security threats as they happen, without ever exposing the raw data. This turns log files from a reactive, forensic tool into a proactive source of threat and compliance intelligence, providing a definitive, unalterable record of all actions.

OmniIndex

Log File Intelligence Case Study

Cross River State in Nigeria is using OmniIndex's log file intelligence to ensure the highly confidential and regulated educational data of the state's students and staff is kept secure. This is done in partnership with Future-X Education who are using OmniIndex as the data platform for their Educational Management System.

OmniIndex

The Problem

Educational data is highly sensitive and regulated. As such, it is crucial to have a transparent record of data access and to identify any potential threats/vulnerabilities in the database while keeping that information confidential and secure.

The Solution

The EMIS (Educational Management Information System) was migrated to OmniIndex PGBC and our log file intelligence was therefore able to run automatically on the fully encrypted data to provide real-time threat & compliance intelligence on imutable and inoculated logs.

OmniIndex

Potential Threat Intelligence

Given the sensitive nature of educational data, it's crucial to monitor log files for any activities that could indicate potential threats. Here are a few examples of potential actionable security insights possible with LoggerBC from the data and file systems.

1. Unauthorized Access Attempts:

- Brute Force Attacks: Frequent failed login attempts from unusual IP addresses or locations could suggest a brute force attack is underway.
- Unauthorized User Access: Detection of logins by users who should not have access to the system or attempts to access restricted resources.

2. Data Exfiltration:

- Large Data Transfers: Unusual spikes in data transfers, especially outside of normal business hours, could indicate data exfiltration attempts.
- Suspicious File Downloads: Monitoring for downloads of sensitive data files by unauthorized users or to unusual destinations.

3. SQL Injection Attacks:

- Error Messages or Unexpected Behavior: Unusual error messages or unexpected behavior in the application could be indicative of SQL injection attempts.
- Suspicious Query Strings: Analyzing query strings for potentially malicious input.

4. Malware Activity:

- Unknown Processes or Files: Detection of unknown processes or files running on the system, which could be signs of malware infection.
- Network Traffic Anomalies: Unusual network traffic patterns, such as excessive outbound connections or suspicious DNS requests.

5. Insider Threats:

- Privilege Abuse: Monitoring for instances where users with elevated privileges are accessing data or performing actions they shouldn't have permission to do.
- Unusual Access Patterns: Such as accessing sensitive data outside of normal working hours or places.

6. Data Breaches:

- Data Loss or Corruption: Identifying instances of data loss or corruption, which could be indicative of a data breach.
- Unauthorized External Access: Detecting unauthorized access to the system from external IP addresses.

OmniIndex

Potential Compliance Intelligence

Given the strict regulations governing educational data, it's essential to continuously monitor log files to ensure and prove compliance with data protection policies. Here are a few examples of potential actionable compliance insights possible:

1. Data Access and Usage Audits:
Continuously audit data access against defined user roles to enforce the principle of least privilege. All access to Personally Identifiable Information (PII) is automatically flagged, creating a definitive, unalterable audit trail for regulators.

2. Data Modification and Integrity:
Alert on any attempts to modify critical data, providing irrefutable proof of tampering. The immutable log acts as a "golden record" to programmatically verify data integrity across all connected systems.

3. Data Retention and Deletion:
Enforce data retention policies automatically. The immutable log provides permanent, auditable proof of erasure for "right to be forgotten" requests, ensuring compliance with data disposal rules.

4. Automated Compliance Reporting:
Instantly generate unalterable audit trails for regulatory inquiries. Monitor all third-party vendor access to create a clear record, ensuring adherence to data-sharing agreements.

For more information, including a demo, please get in touch.

www.omniindex.io
info@omniindex.io
+1 (650) 297-4682