WHITE PAPER: SYSTEMS DIAGNOSTICS DATA

Status	Published
Categories	Guidelines
Tag	

TELEMETRY ARTERIES, HEALTH MONITORING, AND DETACHED AUDIT LOGGING

Executive Summary

Systems Diagnostics Data is the engine that keeps our high-velocity platforms stable, optimized, and secure. This white paper details how we collect performance telemetry, health metrics, and infrastructure logs without compromising user privacy or application integrity.

1. Telemetry Taxonomy

Diagnostic tracking is strictly limited to infrastructure performance metrics and operational health data:

```
+---------------------------+-----------------------------------+-----------------------
----------------+
| Data Vector Class         | Metrics Tracked                   | Storage Architecture
|
+---------------------------+-----------------------------------+-----------------------
----------------+
| Performance Telemetry     | CPU utilization, API latency,     | Ephemeral Time-Series D
atabase         |
|                           | memory usage, database speeds     | (Retention: 30 Days)
|
+---------------------------+-----------------------------------+-----------------------
----------------+
| Structural Audit Logs     | Gate actions, auth states,        | Read-Only Write-Once-Re
ad-Many (WORM)  |
|                           | system errors, access tracking    | Dedicated Log Bucket
|
```

```
+---------------------------+-----------------------------------+-----------------------
----------------+
| Behavior Mapping          | Scroll depths, UI interaction     | Anonymized Analytics En
gine             |
|                           | flows, page-view durations        | No PII Attached
|
+---------------------------+-----------------------------------+-----------------------
----------------+
```

2. Hard Security Boundaries & Log Isolation

To prevent diagnostics data from becoming an attack vector, we isolate our logging infrastructure:

- **WORM Storage Policies:** Security logs are written to specialized write-once, read-many storage buckets. Once written, these records cannot be altered or deleted by any user or application script, ensuring an unyielding audit trail for forensics.
- **Zero-Context Error Capture:** When an application error occurs, our error-tracking systems capture stack traces and structural code faults. They are strictly prohibited from recording database parameters or input field values, preventing sensitive client data from spilling into system logs.

3. Real-Time Security Incident Monitoring

System logs are continually analyzed by automated Security Information and Event Management (SIEM) systems.

- **Anomaly Traps:** Automated monitoring rules track baseline system behavior. If a sudden spike in traffic or an irregular access pattern occurs, the system flags the anomaly and fires automated alerts to operational staff within 2.4 seconds.
- **Continuous Compliance Logging:** All diagnostic logs are structured to easily generate compliance validation reports, satisfying the deep audit requirements of frameworks like **NIST AI RMF**, **ISO/IEC 42001**, and **CISA critical infrastructure guidelines**.