# Why a Jupyter Notebook Is Insufficient as an Audit Trail for Akamai Automation

## Summary of Findings

- Jupyter notebooks lack proper version control and change history, making it difficult to track who changed what and when.

- The interactive and mutable nature of notebooks leads to inconsistent and non-reproducible execution sequences.

- Notebooks do not provide centralized logging or archiving, which is essential for a reliable audit trail.

- Access control and traceability are limited or nonexistent in local notebooks.

- They do not integrate well with CI/CD pipelines or infrastructure as code, making them unsuitable for production automation.

- Forensic investigation and postmortem analysis are unreliable with notebooks due to their ease of modification and deletion.

## Detailed Analysis

### Lack of Formal Change History or Version Control

Jupyter notebooks do not inherently support commit history, diff tracking, or authorship logging. Without integration into a version control system like Git, it is impossible to know who made changes or to revert to a previous state, making them unsuitable as an auditable source of truth.

### Mutable and Interactive Execution

Notebooks allow code to be executed in a non-linear order, which can result in inconsistent outputs and internal states. This compromises reproducibility and predictability, both of which are critical for auditing purposes.

### No Centralized Logging or Archiving

Since notebooks run locally and do not push logs to centralized systems, any logs or execution results can be lost if the machine fails. There is no durable record of actions performed, which weakens compliance.

### No Access Control or Role-Based Auditing

Desktop notebooks can be edited or deleted by anyone with local access, with no built-in role-based access control. This makes it difficult to enforce accountability or ensure audit integrity.

### Poor CI/CD and Infrastructure Integration

Notebooks are not natively designed to integrate into CI/CD pipelines or infrastructure-as-code workflows. Actions taken within notebooks are out-of-band and are often not captured in main deployment logs or systems.

### Lack of Immutable Logging for Forensics

Notebooks can be modified or deleted easily, which means any logs or results can be tampered with without detection. This makes them unreliable for any sort of forensic investigation or compliance audit.