Non-Standard Log Forensics

Investigation of business application logs that no SIEM can onboard: undocumented formats, no parser, no vendor schema.

The question it answers

The systems carrying the most business consequence frequently produce the least usable evidence. They write to their own format, ship no schema, and were never designed to be read by anything except themselves.

When an investigation reaches an application like that, most teams stop. Not because the evidence is absent, but because nothing exists to read it with.

Reverse engineering, not onboarding

Onboarding assumes a parser exists. This work starts from the position that it does not, and that no vendor documentation is coming.

Two problems are solved in sequence. First the format itself, until the records can be read reliably. Then the application's own security model, because a record only means something once you know what the application does when it authenticates, authorizes and audits.

What the work involves

Log format reverse engineering

Proprietary and undocumented formats worked out from the data, until records parse reliably and their fields carry known meaning rather than assumed meaning.

Security model reconstruction

Where no documentation exists, the application's authentication, authorization and audit behaviour is established from observation, so an entry can be read as evidence.

Parsers built for the engagement

Purpose-built parsing and normalization, so the events can be analyzed alongside the rest of the evidence rather than in isolation.

Timeline reconstruction at volume

Reconstruction at volumes approaching a terabyte, processed on the hardware the engagement allows rather than requiring the data to move.

AT A GLANCE

APPLIES TO
Applications no SIEM can onboard

STARTING POINT
No parser, no schema, no documentation

OUTPUT
A working parser and the reconstructed timeline

VOLUME
Reconstruction approaching a terabyte

WHERE DATA IS ANALYZED
On premise, in your tenant, or fully isolated

WHO THIS IS FOR

- Investigations that have stalled at an application nobody can read.
- Organizations whose crown-jewel systems sit outside SIEM coverage entirely.
- Legal and regulatory matters that turn on evidence held in a proprietary format.
- Teams told by a vendor or an integrator that these logs cannot be analyzed.

How an engagement runs

01 **Establish the question**

What the investigation has to prove or disprove is agreed first, because it determines which records matter and how far the reverse engineering needs to go.

02 **Acquire and characterize**

Log data is acquired under agreed handling rules and characterized: structure, encoding, volume, retention, and which parts of the record vary in ways that carry meaning.

03 **Reverse engineer the format**

The format is worked out against the data until parsing is reliable and repeatable, and the parser is validated against records whose meaning can be independently confirmed.

04 **Reconstruct the security model**

The application's authentication, authorization and audit behaviour is established, so entries can be interpreted as evidence rather than guessed at.

05 **Rebuild the timeline**

Events are reconstructed into a sequence and correlated with the other available evidence, with confidence stated and gaps identified explicitly.

WHY ALEXSTA

- Tooling follows the objective, never the reverse. Where nothing can read a log, we build what reads it.
- Depth goes to the systems that carry the most consequence, which are usually the ones with the least coverage.
- Conclusions carry their evidence and a stated confidence level, including what the evidence does not settle.

WHAT WE NEED TO SCOPE IT

- The application and version, and what it does for the business.
- Sample log data, however small.
- Volume held and the retention period.
- What the investigation must establish.
- Constraints on where the data may be processed.

What you receive

Working parser

The parser built during the engagement, handed over with its documentation, so the same logs remain readable after we leave.

Reconstructed timeline

The sequence of events rebuilt from the recovered records, correlated with the other evidence available to the investigation.

Findings with evidence

Each conclusion with the records supporting it, a stated confidence level, and an explicit note of what the evidence does not settle.

Coverage assessment

What the application does and does not record, so the blind spots are known and can be closed before the next investigation needs them.

Request an engagement

Send a sample of the log and what you need to establish. We will tell you whether it can be reconstructed before you commit to anything.

contact@alexsta-cybersecurity.com
+41 76 76 44884
alexsta-cybersecurity.com