



Case Study: Financial Services

How a Fortune 100 Financial Services Company Achieved Zero Data Exposure

at 40,000 Transactions/Second — With Zero Human Intervention.

40K/s

TRANSACTIONS MONITORED

<50ms

AUTONOMOUS BLOCK TIME

<3%

FALSE POSITIVE RATE

75

REPOSITORIES PROTECTED

An Invisible Architectural Trap

THE OPERATIONAL REALITY

Processing voice-activated payments, hotel reservations, and financial transactions for Fortune 100 clients — the company was operating DLP through human review cycles against a threat moving at machine speed.

"Our legacy DLP alerted us hours after the window had closed. By the time an analyst touched the queue, the exposure decision had already been made — by inaction."

— VP Information Security

KEY FAILURE POINTS

- Human review cycles operating at human speed vs. machine-speed threats
- Alerts arriving hours after the data exposure window had already closed
- DLP protecting sampled transactions — not 100% coverage
- False positives eroded analyst trust and slowed response
- Daily manual overhead: tagging, config updates, alert review

Hands-Off. Zero-Ticket. Real-Time.

GC Cybersecurity's ISE replaced the human review loop entirely. The platform identifies, classifies, decides, and blocks — without a ticket being opened, without an analyst being paged.

45 min

FULLY OPERATIONAL

Time from start to live deployment

2 hrs

ONTOLOGY CONFIGURATION

One-time setup — never repeated

MINIMAL

ONGOING HUMAN EFFORT

System is entirely self-managing

WHAT ISE DOES THAT LEGACY DLP CANNOT

Identifies: PCI/PII patterns across ALL data — structured and unstructured

Classifies: Topical & Security classification with zero manual tagging

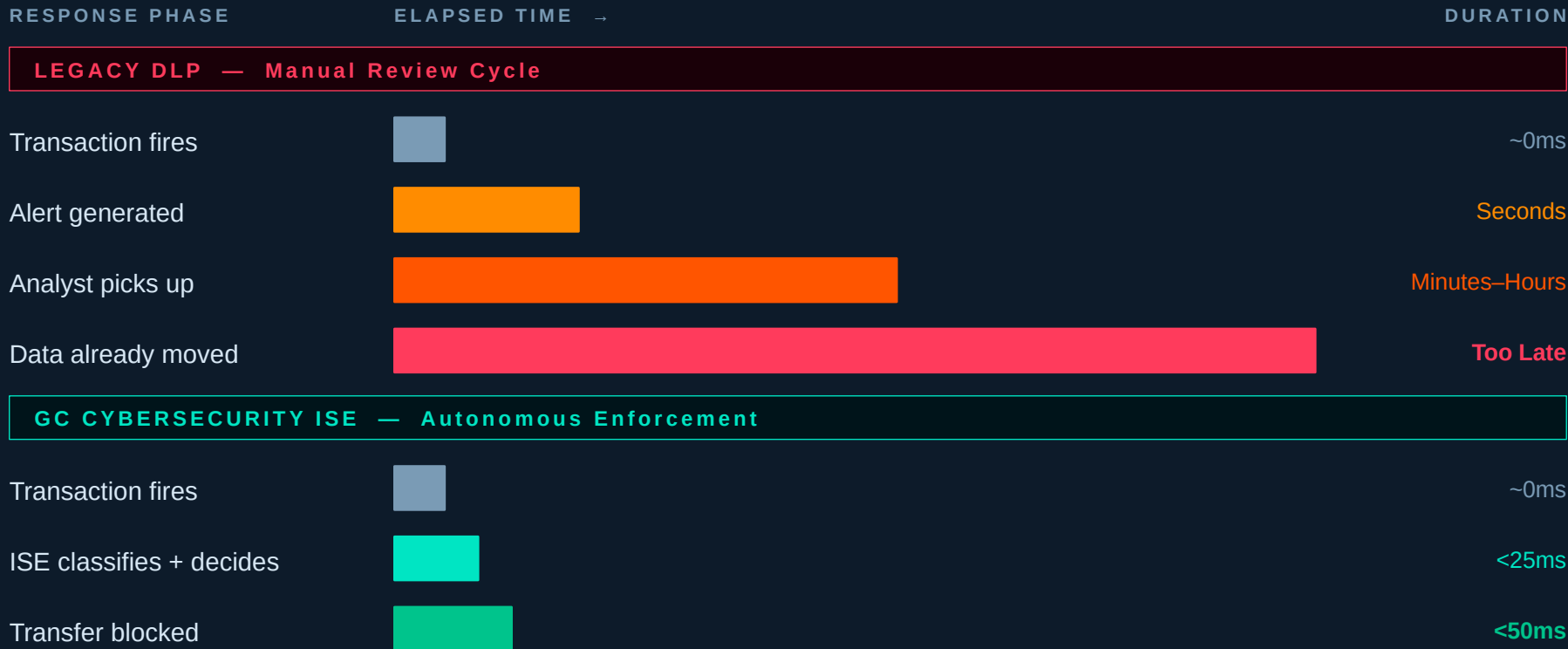
Decides: Auto Policy Synthesis: transfer context vs. authorization scope

Blocks: Transfer halted inside the transaction window — no human loop

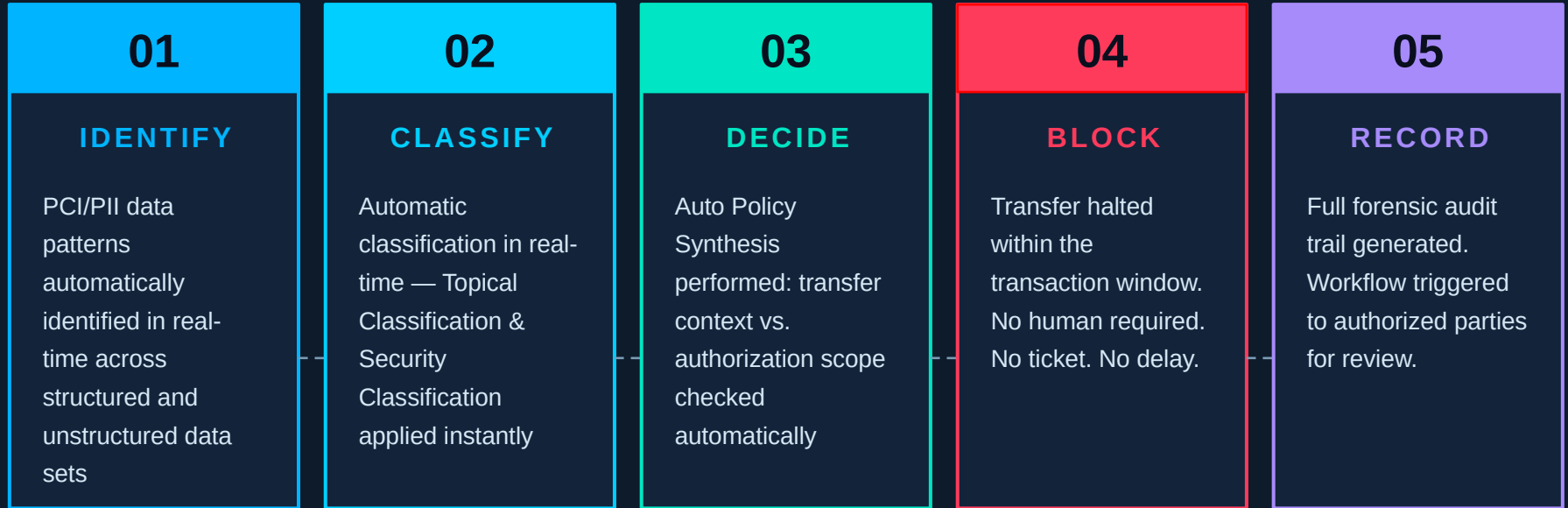
Records: Full forensic audit trail + workflow to authorized parties

Legacy Response Time vs. Autonomous Action

This gap is where data is lost.



No Ticket Opened. No Analyst Paged.



Hard Metrics. No Fluff.

Numbers a CISO takes to the board.

< 5 min

MEAN TIME TO RECOVERY

vs. hours-to-days with legacy DLP

100%

AUDIT-READY COMPLIANCE
STATUS

PCI, PII — real-time GRC enforcement

MINIMAL

ONGOING LABOR COST

Manual tagging eliminated post-deployment

METRIC	BEFORE (LEGACY)	AFTER — GC ISE
Deployment time	Weeks to months	45 minutes — fully operational
Data classification	Manual tagging, perpetual overhead	Automated — one-time Ontology setup
Protocol coverage	Partial — 3rd-party decoders needed	Universal: FTP, FTPS, SMTP, HTTP/S, MAPI...
Transaction throughput	Sampling-based, volume ceiling	40,000 tx/sec — 100% coverage
False positive rate	High — analyst trust eroded	Less than 2%
Human intervention (ongoing)	Daily – tagging, config, alert review	None – system is self-managing post-setup
Audit readiness	Manual documentation process	Real-time GRC enforcement + forensic trail

The gap between those two timeline bars is not a metric.

It is the operational window your adversary owns.

GC Cybersecurity's ISE closes it.

"When your DLP alerts, does it block — or notify?

*The difference between those two verbs is the difference between
your policy and your protection."*

READY TO CLOSE THE GAP?

gccybersecurity.ai

