LEGION

INSIDER RISK

DLP Use Case

How a large multi-national financial institution **Automated 60K DLP Alerts per Month**, unlocking significant efficiency while expanding coverage

---

The risk of data exfiltration

Insider risk and data exfiltration are critical threats for any organization handling sensitive data. When employees—or attackers using employee accounts—leak information, the consequences can be severe, affecting both business operations and customer trust.

To prevent this, companies deploy Data Loss Prevention (DLP) tools that monitor, classify, and control data movement across endpoints, networks, and cloud environments. These systems aim to detect abnormal behavior before it results in data exfiltration or compliance violations.

But because DLP tools rely on anomaly detection and rigid regex-based pattern matching, they are often noisy, generating large volumes of alerts that are complex to triage. At major financial institutions, effective triage isn't only important—it's frequently required by regulators.

The challenge

A leading global financial institution receives **60,000 DLP alerts each month**. With limited internal resources, they outsourced only a portion of these alerts, leaving analysts to manually review tens of thousands more. Teams of five or more struggled to keep up, and the repetitive nature of the work led not only to delays but to analyst burnout.

With Legion, the organization was able to investigate **100% of alerts**, with only a small subset escalated to analysts. This resulted in **over 90% time savings**, improved coverage, and full human oversight maintained where it mattered.

How it worked

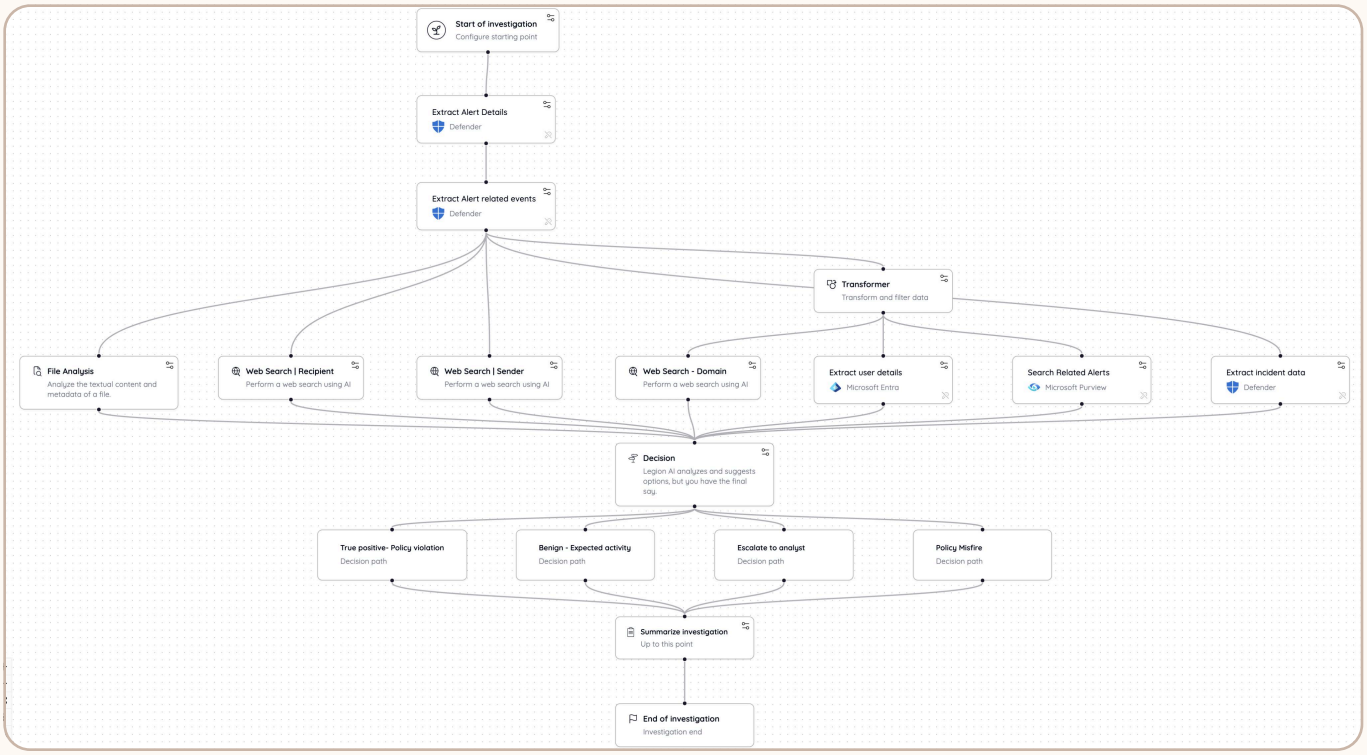
Before Legion, DLP investigations were entirely manual. Analysts had to open emails, download attachments, run SIEM queries, and inspect content to determine whether sensitive data had been exposed.

With sky-high false-positive rates and limited bandwidth, the team faced mounting operational bottlenecks, slower response times, and reduced capacity for strategic work.

Within just a week, Legion recorded several sample investigations and generated a tailored agentic workflow. After some tuning with the team, the workflow was deployed for day-to-day use.

Legion's investigations combine industry best practices with organization-specific context captured from the recordings, enabling high accuracy from day one. Legion operates the same tools you do, including Microsoft Purview, Symantec DLP, Netskope and any other home grown or known tool you operate, leveraging all your available data without any integration. Every investigation is accompanied by a clear, auditable summary—ready for internal review or regulatory audits.

Workflow Visualization



Example Investigation Summary

The incident involved an upload activity by user [redacted] to [redacted] via [redacted], involving a file named '[Redacted]'. The file contained sensitive customer-facing information about [redacted], including details on the end of promotional interest rates. The upload was made to a platform that has been discontinued, raising concerns about the appropriateness of the action.

The investigation revealed that while [redacted] is used by [redacted] for internal project management, the use of [redacted] , especially given its discontinuation, was questionable. The file's sensitive content, if exfiltrated, could pose a risk to the organization. Additionally, the user has a history of Data Loss Prevention (DLP) incidents, further elevating the risk profile.

Given these factors, the incident was classified as a true positive policy violation, as the upload did not align with expected behavior and suggested a potential breach of policy.

Results and Metrics

Before Legion:

Volume of DLP alerts

~60,000

DLP alerts per month,
only a portion investigated

Team

5 analysts

reviewing thousands of
alerts each month each

Manual effort

It takes an analyst roughly

6 minutes

to triage a single DLP alert

False positive rate

Estimated at

95%

of all DLP alerts

Cost

Outsourced investigations cost: **$1 per alert;**

Outsourcing all alerts would exceed

$7M annually

After Legion:

Coverage

100%

of alerts triaged and investigated automatically

Time savings

Over 90%

reduction in analyst time spent on DLP investigations

Smarter escalation

Only relevant and enriched alerts escalated for review, reducing noise and unnecessary analyst effort

---

Key Takeaways

Automation enables full coverage – Legion removes the limits of manual review capacity, ensuring every alert is investigated.

Context-aware triage preserves accuracy – Automation accelerates investigations while keeping critical human judgment in the loop.

Financial efficiency at scale – Significant reduction in manual and outsourced investigation costs while improving operational accuracy and coverage.