mitiga

CASE STUDY

ZERO-IMPACT BREACH PREVENTION

Stopping Payroll Diversion Without Disrupting the Business

Identity compromise turned into potential payroll diversion within minutes. Mitiga reconstructed the Okta-to-Workday attack path, moved targeted detections into production within hours, and enabled safe restoration of payment-change functionality.

Attackers got in. They got nothing.

Time to Actionable Detection

Okta IoA backfilled and deployed within hours.

Payroll Risk Contained

Identity anomalies tied to payroll modification attempts.

Timeline Dispute Reduced

Validated sequencing anchored the post-incident review.

Operational Confidence

Workday payment changes re-enabled with telemetry proof.

THE INCIDENT

Valid credentials became a payroll attack path

The pattern was clear and repeatable: failed Okta login attempts, a successful new-device sign-in, a rapid pivot into Workday, and attempted changes to direct deposit or payment election details.

01 **Failed Okta logins** → 02 **New-device sign-in** → 03 **Workday access** → 04 **Payment election attempt**

Okta was the entry point. Workday was the objective.

The attacker did not exploit a misconfiguration. They logged in with valid credentials and moved directly toward monetization.

Speed increased. Documentation fragmented.

Identity teams, application teams, containment owners, and a real-time scribe moved in parallel during escalation.

Leadership needed proof

Which accounts were compromised? Were payroll changes executed?
When were containment actions taken?
Could payroll change functionality be safely restored?

MITIGA IN ACTION

Detection, visibility, and timeline clarity

01 Detecting the Pattern

Mitiga built an Indicator of Attack for one source IP targeting multiple Okta accounts. Thirty days of activity were backfilled, and the detection moved into production within hours.

02 Validating the Pivot

Mitiga restored Workday log visibility, resolved processing blockers, and brought sign-on and user activity into one investigative view with Okta anomalies.

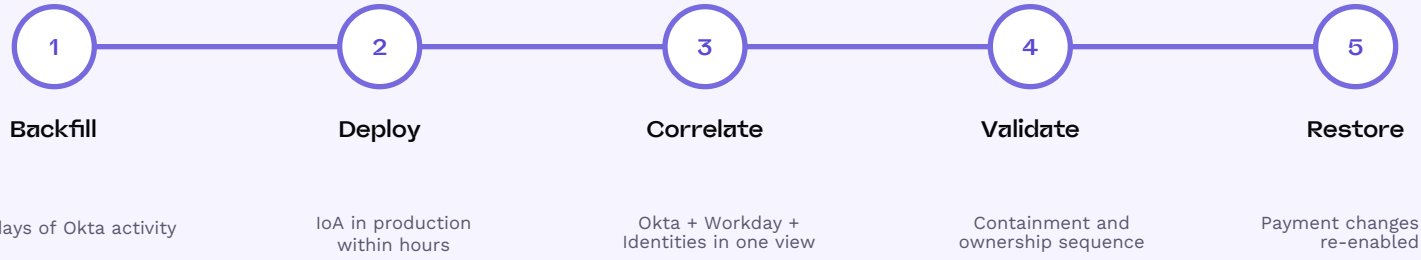
03 Reconstructing Timeline

A detailed write-up correlated identity and payroll telemetry, confirmed containment timing, and clarified who did what and when.

> "Your write up was instrumental in helping us validate the timelines."

POST-INCIDENT REVIEW FEEDBACK

Unified response timeline



OUTCOME

The breach attempt didn't become a business crisis

Mitiga provided panoramic visibility across identity and payroll systems, decoded the attack path into a validated timeline, and enabled decisive containment without disrupting payroll operations.

01

Payroll diversion risk contained

Identity anomalies were correlated to attempted payroll modification activity.

02

Manual stitching eliminated

Okta and Workday telemetry appeared in one investigative view.

03

Sequencing uncertainty reduced

The incident write-up became a forensic anchor for review.

04

Operational confidence restored

Payment-election changes were re-enabled with validated telemetry.

Meet with Mitiga

Meet with us to learn how Mitiga helps security teams detect, investigate, and contain cloud and SaaS attacks before business impact.

www.mitiga.io/demo