mitiga

Workday Logs

A Now You See Me cheat sheet

workday

"Now You See Me" demystifies SaaS security log by log with the why, what, and how of SaaS threat hunting.

Why Workday Belongs in Your Security Scope

Workday is a SaaS ERP platform used to manage finance, HR, payroll, and procurement. It holds sensitive business and employee data that attackers want.

Misuse doesn't require a Workday vulnerability. It happens when visibility, logging, and monitoring fall short. Workday needs to be part of your security program.

What's Actually in Workday Logs

Workday delivers several logs that can be used for audits and should be surfaced to detection and incident response teams, including:

User Activity Logs and Audit Trails are all about tracking what users do in the system so that there is a complete and comprehensive record for compliance, troubleshooting, and security reviews.

SignOn Logs primarily capture activities related to authentication, providing detailed records of login attempts, session management, and security checks. These logs are very important for monitoring access security and detecting potential unauthorized attempts.

What You May Not Know About These Logs

Short retention and limited history. Out of the box, Workday limits user-activity reports to around 30 days. Without exporting, historical analysis beyond that window is impossible.

Misleading assumptions. "Everything is logged by default" is a dangerous assumption. If user-activity logging was not enabled or if the APIs are not configured, you might not see data for key events.

Workday Threat Hunting Tips & Investigation Tricks

Skilled threat hunters and detection engineers should make use of these kinds of tactics with Workday logs.

Impossible travel or unusual geo signatures in signon events:

Look for events like an HR admin logging in from one country and then 10 minutes later a report export starts from another. If you have it, combine this with IP and device data.

New integration system user or reused API key:

Monitor for creation of integration system users (ISUs) or changes to the schedule of integration jobs. Also, look for high-volume exports or executions that happen outside of business hours. Attackers often leverage integration keys because they bypass typical MFA and alerting.

Privileged role changes/domain security policy edits:

Raise a flag if someone added themselves or a service account to a super-privileged security group or modified the business process definition for employee termination or distribution.

Correlate logs across systems:

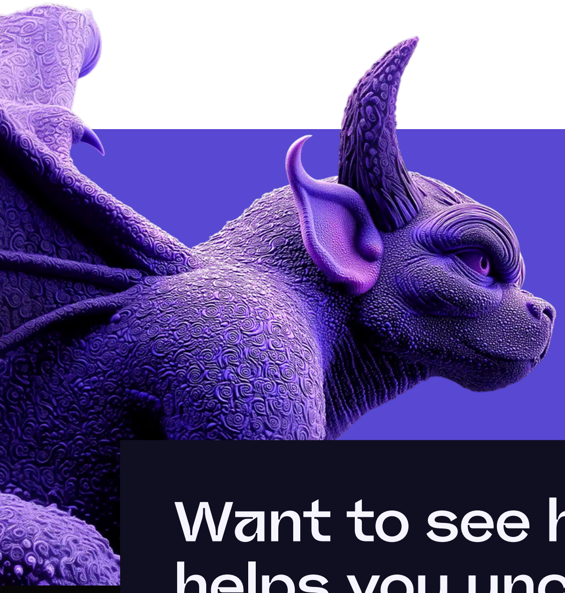
For example, Okta logs show a suspicious login for user.finance.Minutes later, Workday records the same user adding themselves to the Payroll_Approver group and performing an unscheduled employee compensation report export. This sequence of unusual IdP logins followed by role changes and high-value data access in Workday highlights a potential credential compromise and risky internal activity.

Large data exports or report generations:

In audit logs, check for reports that dump large amounts of sensitive data, like compensation and bank details. Keep an eye out especially for unusual frequency, time of day, or destination accounts.

Dormant account reuse:

You can detect when previously inactive integration or service accounts suddenly become active. Combine this with login history and config change trails.



Don’t leave Workday as a “nice-to-monitor” SaaS application. A simple mistake, like failing to extend retention beyond 30 days or ignoring API-driven admin changes, can become the exact blind spot an attacker exploits.

Want to see how Mitiga helps you uncover what others miss?

Learn more about our **Zero-Impact Breach Prevention** platform or request a live demo.

www.mitiga.io/demo