Silverfort | PagerDuty

Silverfort and PagerDuty: Real-time alerting for identity incidents

Available for: *On-prem ITDR*

As organizations build their Identity Threat Detection and Response (ITDR) programs, detection alone is not enough. Every incident needs to reach the right responder, in the tool they already work in, with the context required to act fast. Incident management platforms like PagerDuty are where security and operations teams already triage, escalate, and respond to what's urgent.

Silverfort extends these workflows by sending its incidents directly into PagerDuty, ensuring that identity threats—like kerberoasting, lateral movement, and brute-force attacks—are not just detected, but surfaced to the right responder, escalated, and resolved through the on-call rotations your teams already run.

Turning identity incidents into into on-call action

The Silverfort and PagerDuty integration brings identity incidents into the on-call and escalation workflows your teams already run. **Every incident is:**

- Raised in PagerDuty the moment it's detected, alerting the on-call responder
- Enriched with the context needed to triage and act —incident type, severity, and the affected identity
- Synced end-to-end, with the PagerDuty incident reflecting Silverfort's status as it moves from **triggered** to **acknowledged** and **resolved**

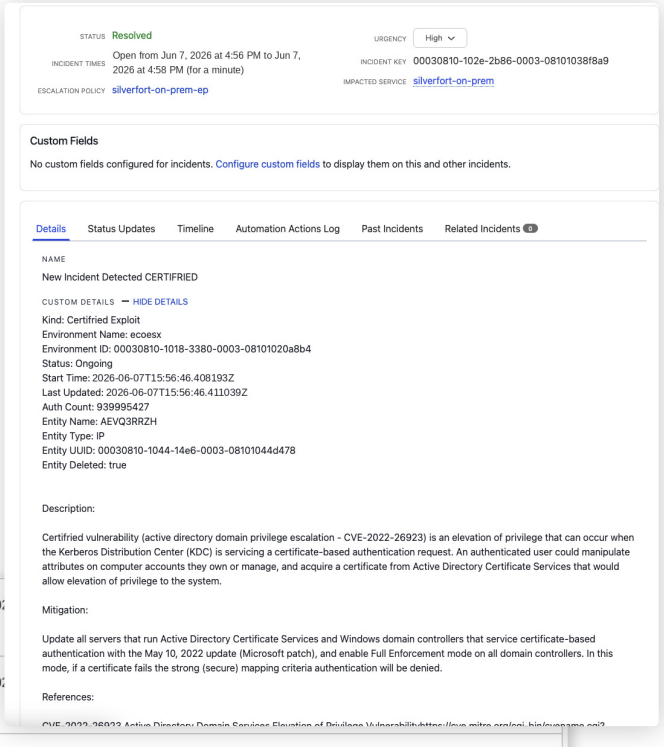
By connecting identity incidents to PagerDuty, you close the gap between detection and response, cutting the time between when an incident is raised and when the right person acts on it.

How it works

When Silverfort detects an identity incident, it's raised in PagerDuty automatically—triggered the moment it's created, with no manual steps. Each incident is assigned to the PagerDuty service, escalation policy, and priority you've configured, so it reaches the right on-call responder through the rotations and escalation rules your team already runs.

Silverfort sets each PagerDuty incident's urgency from a mapping you define, matching incident types to high, medium, or low so responders can prioritize what needs attention first.

As the incident progresses, the integration keeps PagerDuty in sync: when Silverfort marks an incident acknowledged or resolved, PagerDuty reflects the same status—so you keep a single source of truth.



Key benefits

Get identity threats to responders in real time

Surface identity incidents in PagerDuty the moment Silverfort detects them, so threats reach the on-call responder as fast as any other critical alert.

Prioritize identity threats by what matters most

Map each incident type to a PagerDuty urgency so the most critical identity threats rise to the top of the queue.

Put identity threats on the same escalation path as your other alerts

Run identity incidents through the escalation policies and on-call rotations your team already trusts, so identity gets the same fast, accountable response as the rest of your operations.

Keep identity incident status aligned across tools

Reflect Silverfort's acknowledged and resolved states in PagerDuty automatically, so responders track one consistent view.

About Silverfort

Silverfort secures every dimension of identity—human, machine, and AI—across on-prem, cloud, and hybrid environments. We are the first to deliver an end-to-end Identity Security platform that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline and at runtime to stop lateral movement, ransomware, and other identity threats.