Silverfort | Sekoia

Silverfort and Sekoia Integration

Identity is the fastest-moving layer in any attack, and the hardest one to see once a threat is underway. Security teams see incidents and risk signals as they happen—but responding to them means leaving the tools they already work in.

To detect identity threats as they unfold, security teams need identity authentication and risk data flowing into the platform they already monitor. Silverfort forwards live identity events—authentication, MFA, and risk—continuously into Sekoia.io, enabling security teams to monitor, detect, and hunt on identity threats without leaving their existing workflow.

Faster detection of identity threats

The Silverfort integration with Sekoia forwards identity authentication and MFA events into the Sekoia platform, where events are normalized and made available for detection and threat hunting. Instead of monitoring identity activity separately from the rest of their telemetry, SOC teams receive a continuous, risk-scored feed of authentication events in the platform they use to investigate everything else.

This enables security teams to:

- Monitor Silverfort authentication and MFA activity alongside the rest of their telemetry in Sekoia
- Detect identity-based attacks—such as account takeover and lateral movement—using Sekoia's built-in and custom detection rules
- Prioritize triage with Silverfort risk levels and risk indicators carried on every event
- Hunt and pivot across identity activity using normalized fields in the Sekoia events page

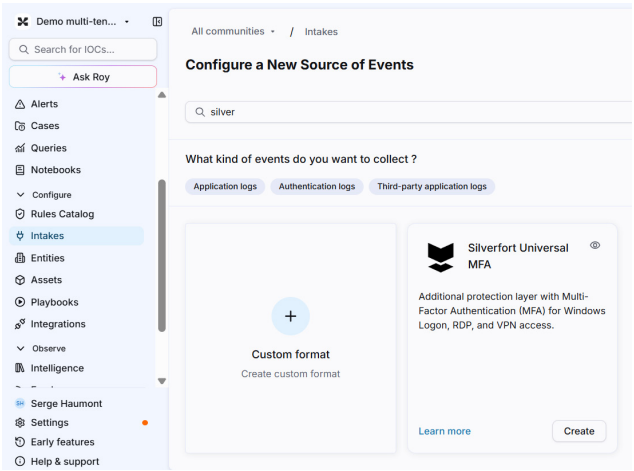
By bringing Silverfort's identity telemetry into Sekoia, SOC teams gain earlier detection, richer identity context, and a single place to investigate identity threats.

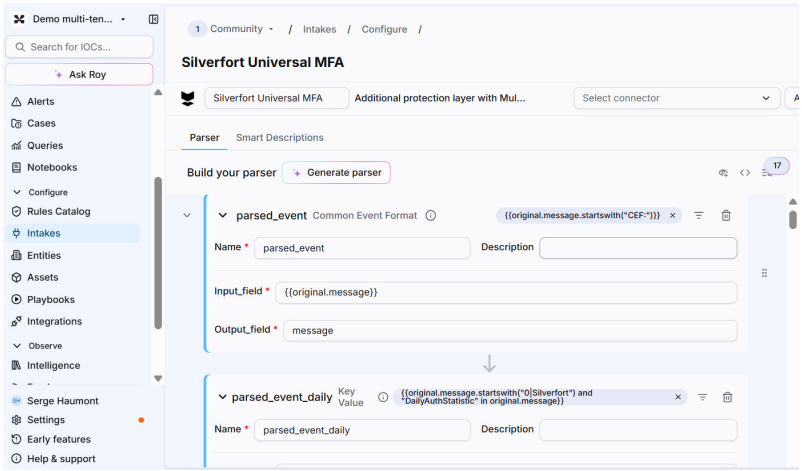
How it works

Silverfort forwards identity events to Sekoia via syslog in CEF (Common Event Format). On arrival, Sekoia's built-in Silverfort intake parses each event and normalizes it to a common schema, so it lands detection-ready. The feed covers three Silverfort data sources: authentication logs (Windows Logon, RDP, and VPN), MFA request and response events, and daily authentication statistics for volume monitoring.

Send events over standard syslog in CEF	Parse and normalize automatically with the built-in intake	Cover authentication, MFA, and daily auth statistics	Feed Sekoia's built-in rules, custom rules, and hunting

By parsing and normalizing Silverfort's events on arrival, Sekoia gives SOC teams detection-ready identity data right away—with no custom parser to build or pipeline to maintain.





Key benefits

Detect identity attacks earlier

Silverfort's authentication and MFA events feed Sekoia's built-in and custom detection rules, so identity-based attacks like account takeover and lateral movement surface in the SOC as they unfold.

Hunt across identity activity

Normalized events let analysts pivot and search across users, sources, and protocols in the Sekoia events page, turning authentication data into proactive investigation.

Risk scoring on every event

Each event arrives with Silverfort's risk level and risk indicators, giving analysts the signal to prioritize the authentications that matter instead of sifting raw logs.

Correlate identity with the rest of your data

With Silverfort events flowing into Sekoia, analysts investigate identity activity alongside telemetry from across the environment, in the same place they work everything else.

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.