5 Ways to Prevent Supply Chain Attacks Caused by Compromised Vendor Credentials

Don’t let your vendors be the weak link attackers can exploit

1 Continuously monitor for vendor identity exposures

Track both historical and current exposures from the criminal underground – attackers love reusing old credentials available to them

2 Detect infected vendor devices with exposed credentials

Reveal if vendors are unknowingly exposing credentials to internal or shared applications via malware-infected devices

3 Reset credentials where you control access

Integrate exposure data into your Identity Providers (IdPs) to force password resets and block compromised logins

4 Review credential reuse to identify poor security hygiene

Flag vendors with employees reusing passwords across environments to prevent easy pathways for criminals

5 Respond to real-time changes in vendor exposure trends

Use identity intelligence to continuously track and act on identity exposures tied to your third-party ecosystem over time

SpyCloud