

SIEM: Turning a Pile of Logs Into a Story

Sun, Aug 16, 2:00 PM EDT · <https://scottslab.io/posts/siem-and-log-correlation>

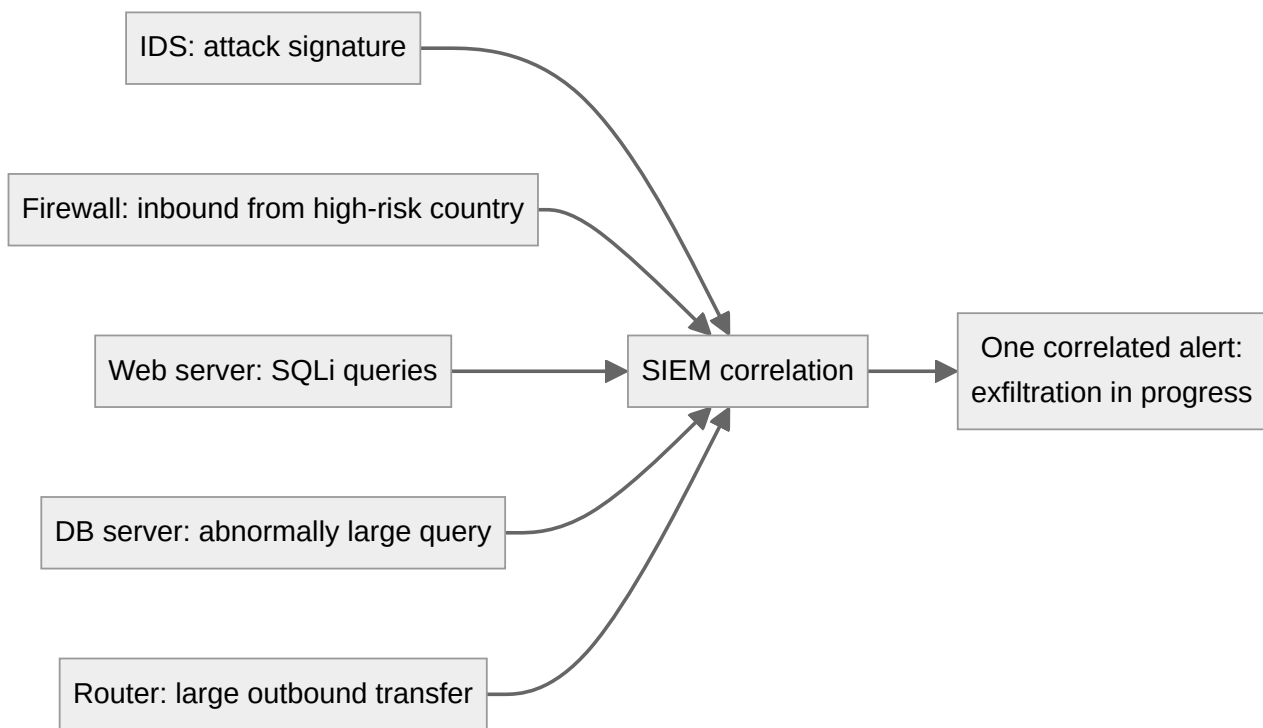


TL;DR

A SIEM does two things: collect logs securely from everything in one place, and correlate across them to spot patterns no single device can see. That correlation is the whole value. It solves the silo problem where each team only sees their own fragment. A real attack lights up in sequence across sensors (IDS signature → firewall connection from a risky country → SQLi at the web server → huge DB query → big outbound transfer), and only the SIEM sees all five as one event.

I've written before about building a SIEM in my home lab, so here's the fundamentals view of why it exists at all. A SIEM (Security Information and Event Management) does two core jobs. First, it's central, secure log collection: every sensor and device ships its logs to one place, off the hosts that generated them, where they can't be quietly tampered with. Second, and this is the part that earns its keep, it correlates (increasingly with AI/ML) across all those sources to surface patterns of malicious activity that no single log would reveal.

The problem it solves is silos. The firewall team sees firewall logs. The web team sees web logs. The DBA sees database logs. Each is looking at one frame of a movie and none of them can see the plot. The SIEM assembles the frames.



SIEM: Turning a Pile of Logs Into a Story

The classic example makes it concrete. On its own, each of these is a shrug; in sequence, it's an intrusion. The IDS flags an inbound attack signature. The firewall logs an inbound connection from a high-risk country. The web server reports suspicious SQL injection queries. The database server reports an abnormally large query coming from the web app. And the router reports a large outbound data flow to the internet. Five different devices, five different teams. And one attacker walks straight through, visible only when something is watching all five at once and connecting them in order.

That's what the SIEM dashboard is for: centralized alerts across every source, trend analysis over time, and sensitivity you can tune so the signal isn't buried in noise (the false-positive fight never ends). Collection gets the data into one place; correlation turns it into the sentence "someone is exfiltrating your database right now." The next question is whether it can act on that by itself. That's where SOAR comes in.