Why do security teams get thousands of alerts a day and how can they cope?

Short answer: Alert overload didn't appear overnight — it built up gradually as attackers grew more automated and evasive, turning once-clear warning signs into faint, ambiguous hints that require deep expertise to interpret. Cyber Crucible was built to break this cycle by handling detection and response automatically, rather than asking human teams to sift through endless low-confidence signals.

How Alert Fatigue Became the Norm

Security alerting didn't degrade because vendors decided to push the burden onto customers. It happened slowly, as attackers refined their techniques to mutate and automate faster than defensive tools could definitively label an event as malicious. What used to be a clear indicator of compromise became a faint clue buried among countless other faint clues. Sorting through them properly takes senior-level analysts significant time, and often what looks suspicious turns out to be nothing more than a misbehaving printer driver. Meanwhile, a single overlooked low-confidence alert can be the only visible trace of a serious, active intrusion.

Why More Alerts Didn't Mean Better Security

As detection tools tried to keep pace with evolving threats, they compensated by flagging anything even slightly unusual. This created a flood of alerts that technically satisfied the requirement to warn customers, but left security teams unable to realistically investigate each one. The natural result is one of two outcomes: teams start ignoring low-confidence alerts—exactly where sophisticated attackers tend to hide—or they become overwhelmed, and critical work simply doesn't get done, regardless of effort or intent.

A Different Starting Point

Recognizing that incremental fixes wouldn't solve a problem rooted in years of accumulated complexity, Cyber Crucible approached the issue from a different angle entirely. Instead of generating more alerts for humans to triage, our FortressAI technology is designed to autonomously detect and respond to ransomware, data theft, and identity theft threats in real time. Using modern approaches like generative AI, Cyber Crucible aims to reduce dependence on manual alert review and address the underlying imbalance between attacker automation and defender bandwidth.

https://player.vimeo.com/video/1186492629

Watch on Vimeo · Captions: English, Français, Español, العربية

Revision #4
Created 2026-07-23 23:17:57 UTC by Dennis Underwood
Updated 2026-07-24 00:31:20 UTC by Dennis Underwood