# Pourquoi les équipes de sécurité reçoivent-elles des milliers d'alertes par jour, et comment peuvent-elles y faire face ?

**Réponse courte :** La surcharge d'alertes n'est pas apparue du jour au lendemain — elle s'est accumulée progressivement à mesure que les attaquants devenaient plus automatisés et plus évasifs, transformant des signaux d'alerte autrefois clairs en indices faibles et ambigus nécessitant une expertise approfondie pour être interprétés. Cyber Crucible a été conçu pour briser ce cycle en gérant automatiquement la détection et la réponse, plutôt qu'en demandant aux équipes humaines de trier d'innombrables signaux à faible fiabilité.

## Comment la fatigue liée aux alertes est devenue la norme

Les systèmes d'alerte en sécurité ne se sont pas dégradés parce que les éditeurs ont décidé de reporter la charge sur leurs clients. Cela s'est produit lentement, à mesure que les attaquants perfectionnaient leurs techniques pour muter et s'automatiser plus vite que les outils défensifs ne pouvaient qualifier un événement de malveillant avec certitude. Ce qui constituait autrefois un indicateur clair de compromission est devenu un indice ténu, noyé parmi d'innombrables autres indices tout aussi ténus. Les trier correctement demande un temps considérable à des analystes chevronnés, et souvent, ce qui semble suspect n'est rien de plus qu'un pilote d'imprimante défaillant. Pendant ce temps, une seule alerte à faible fiabilité négligée peut être la seule trace visible d'une intrusion active et grave.

## Pourquoi davantage d'alertes n'a pas amélioré la sécurité

À mesure que les outils de détection tentaient de suivre le rythme des menaces en constante évolution, ils ont compensé en signalant tout ce qui semblait tant soit peu inhabituel. Cela a créé un flot d'alertes qui, techniquement, remplissait l'exigence d'avertir les clients, mais laissait les

équipes de sécurité dans l'incapacité réaliste d'enquêter sur chacune d'elles. Le résultat naturel est l'un des deux scénarios suivants : les équipes commencent à ignorer les alertes à faible fiabilité — précisément là où les attaquants sophistiqués ont tendance à se dissimuler — ou elles se retrouvent submergées, et le travail critique n'est tout simplement pas accompli, quels que soient les efforts ou les intentions.

# Un point de départ différent

Conscient que des correctifs incrémentaux ne résoudraient pas un problème enraciné dans des années de complexité accumulée, Cyber Crucible a abordé la question sous un angle entièrement différent. Plutôt que de générer davantage d'alertes à trier par des humains, notre technologie FortressAI est conçue pour détecter et neutraliser de manière autonome, en temps réel, les menaces liées aux rançongiciels, au vol de données et à l'usurpation d'identité. En s'appuyant sur des approches modernes telles que l'IA générative, Cyber Crucible vise à réduire la dépendance à l'examen manuel des alertes et à corriger le déséquilibre sous-jacent entre l'automatisation des attaquants et la capacité des défenseurs.

https://player.vimeo.com/video/1186492629?texttrack=fr

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

---

Revision #2
Created 2026-07-24 07:27:27 UTC by Dennis Underwood
Updated 2026-08-06 18:39:15 UTC by Dennis Underwood