Warum erhalten Sicherheitsteams täglich Tausende von Warnmeldungen, und wie können sie damit umgehen?

Kurze Antwort: Die Alarmüberflutung ist nicht über Nacht entstanden – sie hat sich allmählich aufgebaut, da Angreifer zunehmend automatisierter und ausweichender wurden und einst eindeutige Warnzeichen in schwache, mehrdeutige Hinweise verwandelten, die tiefgreifendes Fachwissen zur Interpretation erfordern. Cyber Crucible wurde entwickelt, um diesen Kreislauf zu durchbrechen, indem Erkennung und Reaktion automatisch erfolgen, anstatt menschliche Teams damit zu beauftragen, endlose Signale mit geringer Zuverlässigkeit zu durchforsten.

Wie Alarmmüdigkeit zur Norm wurde

Die Verschlechterung der Sicherheitsalarmierung geschah nicht, weil Anbieter beschlossen hätten, die Last auf die Kunden abzuwälzen. Sie entstand schleichend, da Angreifer ihre Techniken verfeinerten, um schneller zu mutieren und zu automatisieren, als Verteidigungstools ein Ereignis eindeutig als bösartig einstufen konnten. Was früher ein klarer Kompromittierungsindikator war, wurde zu einem schwachen Hinweis, verborgen unter unzähligen anderen schwachen Hinweisen. Diese ordnungsgemäß zu sichten, kostet erfahrene Analysten erhebliche Zeit, und oft stellt sich heraus, dass das Verdächtige nichts weiter als ein fehlerhafter Druckertreiber ist. Gleichzeitig kann eine einzige übersehene Warnmeldung mit geringer Zuverlässigkeit die einzige sichtbare Spur eines ernsthaften, aktiven Eindringens sein.

Warum mehr Warnmeldungen nicht zu besserer Sicherheit führten

Während Erkennungstools versuchten, mit sich weiterentwickelnden Bedrohungen Schritt zu halten, kompensierten sie dies, indem sie alles auch nur geringfügig Ungewöhnliche

kennzeichneten. Dies führte zu einer Flut von Warnmeldungen, die formal zwar die Anforderung erfüllten, Kunden zu warnen, Sicherheitsteams jedoch nicht realistisch in die Lage versetzten, jede einzelne zu untersuchen. Das natürliche Ergebnis ist eines von zwei Szenarien: Teams beginnen, Warnmeldungen mit geringer Zuverlässigkeit zu ignorieren – genau dort, wo sich raffinierte Angreifer bevorzugt verstecken – oder sie werden überwältigt, und wichtige Arbeit bleibt schlicht liegen, unabhängig von Bemühen oder Absicht.

Ein anderer Ausgangspunkt

In der Erkenntnis, dass punktuelle Verbesserungen ein Problem, das auf Jahren angehäufter Komplexität beruht, nicht lösen würden, näherte sich Cyber Crucible dem Thema aus einem völlig anderen Blickwinkel. Anstatt mehr Warnmeldungen zu erzeugen, die von Menschen priorisiert werden müssen, ist unsere FortressAI-Technologie darauf ausgelegt, Ransomware-, Datendiebstahl- und Identitätsdiebstahlbedrohungen in Echtzeit autonom zu erkennen und darauf zu reagieren. Mit modernen Ansätzen wie generativer KI verfolgt Cyber Crucible das Ziel, die Abhängigkeit von manueller Alarmprüfung zu verringern und das zugrunde liegende Ungleichgewicht zwischen der Automatisierung der Angreifer und den Kapazitäten der Verteidiger zu beheben.

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

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Revision #1
Created 2026-07-24 05:07:04 UTC by Dennis Underwood
Updated 2026-07-24 05:07:04 UTC by Dennis Underwood