Stop chasing alerts. 
Start catching attackers. 

Attackers have the advantage. Using Artificial Intelligence (AI) tools and automation, threat actors have evolved their evasion techniques beyond the defenses of standard ‘find the needle in the haystack’ security technologies. Unfortunately, your Incident Response (IR) teams continue to spend valuable time and resources mired in the turmoil of triaging an avalanche of alerts and false positives—and accepting the sinking likelihood that they are still missing attacks dwelling in the shadows.

**Current approaches aren’t enough**

Alert volume is **50+%** false positives\(^1\)

Analysts spend **24-30 min** investigation time per incident\(^2\)

SOCs report they are missing **39%** of security threats\(^3\)

Flip the dynamic, and **force** attackers to reveal themselves

Goodbye false positives. Hello high-fidelity attack detection

Instead of restrictive controls around your assets, reactive data analytics and the churn of SOC burn-out, Illusive offers organizations concerned about post-breach attack detection a simple alternative to the status quo. Unlike tools that are ‘probabilistic’ in their identification of an incident that might be a threat, Illusive customers gain tactical advantage over cyber adversaries armed with **DETERMINISTIC** notification and precise forensic proof of an attack in motion—saving costly time in defense of your organizations most valuable assets and mission-critical infrastructure. **Game on, and you’re in control!**

---

\(^1\) Enterprise Management Associates, InfoBrief: A Day in the Life of a Cyber Security Pro, 2017
\(^3\) DomainTools, Threat Hunting Report 2018
Illusive puts onus on the attacker, frustrating them once they land on an endpoint by starving them from the real data they expect and need. An environment poisoned with false, but authentic looking data paralyzes the attacker—the second they touch an Illusive deception, they reveal themselves, instantly triggering notification and forensic proof of an attack in motion versus the hope of validating one.

Response shifts from days or weeks of alert analysis to minutes, detailed with source and target. No data parsing or ghost chasing is needed—thus flipping your cyber asymmetry and putting you on the attack.