Stop chasing alerts.

Start catching attackers.

#stopsidewaysattacks

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.

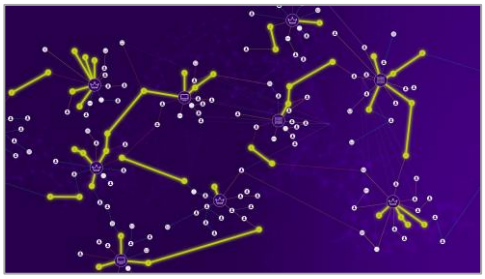
Improve Security Outcomes

- Cloud Security
- Insider Threat Defense
- Lateral Movement Defense
- M&A Security
- Wire Fraud Prevention
- SOC Efficiency
- Red Team Exercises
- IoT/OT Device Protection

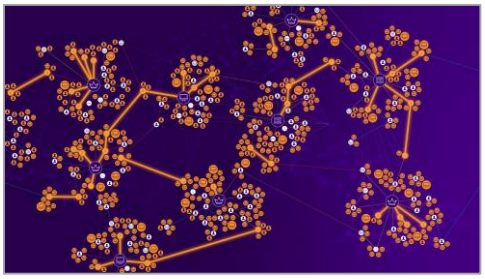
Game on, and you're in control!

[1] Enterprise Management Associates, InfoBrief: A Day in the Life of a Cyber Security Pro, 2017
[2] Enterprise Management Associates, InfoBrief: A Day in the Life of a Cyber Security Pro, 2017
[3] DomainTools, Threat Hunting Report 2018

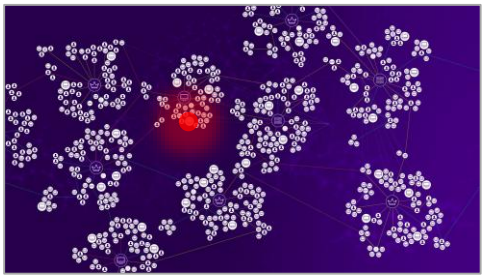
Flip cyber asymmetry from 'probabilistic' to '**deterministic**'



Clean. Identify and remove attack pathways



Distort reality. Create an inescapable trap



Detect and stop. One false step triggers detection

What you see

- Continuous hygiene of errant credentials and attack pathways
- Auto-discovery of 'Crown Jewels'
- Maze of authentic deceptions
- Real-time forensic notifications

What attackers see

- Environment that *looks* authentic, but is actually a maze of deceptions:
  - ✓ Errant credentials
  - ✓ Misconfigurations
  - ✓ Connections and pathways
  - ✓ 'Crown Jewels'

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.

CUSTOMER TALES FROM THE SHADOWS

Perpetually remove attack pathways

- Discovered and remediated Domain Admin account on 3,000 machines
- Centrally disabled local Admin account on 2,000 laptops
- Identified and removed 100s of high-privileged user connections to data center

Your environment becomes a trap

- Discovered insider money laundering campaign previously operating for 22 months
- Detected nation-state attack on ISP that had been present for 11 months before Illusive deceptions deployed
- **Undefeated** in 100+ Red Team vs Blue Team exercises

Remediate with real-time forensics

- Reduced investigation time by two-thirds, gaining weeks of effort previously done manually
- Provided incontrovertible forensic evidence for prosecution of malicious insider
- Delivered detailed information on attacker techniques to inform security improvements to critical systems

Engineered by people steeped in nation-state cyber intelligence and defense, we are here to help!
See a demo or discuss steps for a free Attack Risk Assessment at info@illusivenetworks.com

Visit us at www.illusivenetworks.com

Call us at +1 844.455.8748 (North America) or +972 73.272.4006 (EMEA and AsiaPac)

Illusive Networks stops cyberattacks by destroying attackers' ability to make safe decisions as they attempt to move toward their targets. Using Illusive, organizations eliminate high-risk pathways to critical systems, detect attackers early in the attack process, and capture real-time forensics that focus and accelerate incident response and improve resilience. Through simple, agentless technology, Illusive provides nimble, easy-to-use solutions that enable organizations to continuously improve their cyber risk posture and function with greater confidence and agility.