Illusive Networks for Improved SOC Efficiency

A deception-based approach for early attack detection, with real-time forensic insight for accelerated incident response

It's no surprise that SOC operators are under incredible strain—from talent shortages and data overload, to the sheer volume of disparate technologies they maintain. Under constant attack and barraged by piles of alerts, SOC teams must examine and prioritize meaningful alerts that warrant further investigation. Piecing together a picture of what actually happened can take months. In the event of a true attack, the attacker may already have been well entrenched in the network—or may already have exfiltrated data.

With Illusive's deception-based technology, organizations can turn the incident model upside down. Illusive tells you in real time when an attacker is actually DOING something—i.e. is in the midst of the human decision-making process to probe the environment and attempt lateral movement.

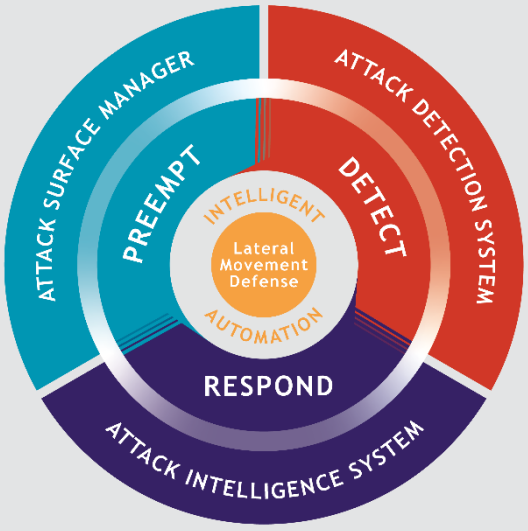
The Illusive platform helps companies to:

- **Detect suspicious threat activity early on with accuracy and speed**
- **Immediately know how close a potential attacker is to critical systems and domain admin credentials**
- **Quickly gather the forensic evidence—both source and target—needed to expedite investigations and take appropriate action**
- **Reduces noise in the security operations center and focus incident response where it matters most**

Now teams have clear options. They can isolate the attacker or take other rapid action to stop the attack, or—especially if they have honeypots or decoys—they can continue to observe and collect information on the attacker's goals and techniques.

With deception-generated notification reports, SOC teams can kick-start the triage process and give precise focus to broader correlation, analysis and eradication efforts.

The Illusive Platform provides centralized management across even the largest and most distributed environments. Three modular components can work together or be operated separately to preempt, detect, and respond to cyberattacks.



Changing the math for early attack detection

Reducing the number of real artifacts while saturating endpoints with deceptive ones increases the odds that attackers will choose deceptions—and be instantly caught.

How the Illusive Platform Detects Attackers and Improves SOC Efficiency

- **Attack Surface Manager:** Finds and removes errant high-privilege credentials, connections, and attack pathways to deter unauthorized lateral movement from one endpoint to another.
- **Pathways:** A feature that automatically reveals attack paths from any machine to high-value targets, provides drill-down details on the systems in each path, and enables point-and-click elimination of excess connectivity, leveraging risk and connectivity ratings.
- **Attack Detection System:** Distributes deceptive data on every endpoint across the network, forcing attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making. As soon as an attacker interacts with a deception, an immediate notification is sent to the security team, along with detailed forensics (see below).
- **Attacker View:** Shows real-time proximity of attackers to Crown Jewel systems and high-privilege credentials.
- **Attack Intelligence System:** Empowers Incident Response teams with easy-to-use, precision forensics—both source-based and from high-interaction decoys—so they can rapidly determine the best course of action to minimize business damage and improve future cyber resilience.
- **Forensics Timeline:** A unified, sortable per-incident chronology of forensic data.
- **Specialized Device Emulations:** Pre-built images speed up and simplify creation of medium-interaction decoys for OT, IoT and networked devices.
- **Illusive API:** When other tools trigger alerts, Illusive can collect endpoint forensics, provide Forensics Timeline records, and show machines in Attacker View.
- **FirstMove Services:** Assistance in planning deployments, use case development and interpretation of security notifications.

Value Gained for SOC and IR Teams

- Ensure early attacker detection—no matter where compromise begins
- Efficiency under fire. At the moment of detection, responders have comprehensive insight to quickly determine the best course of action
- Reduce noise in the SOC by focusing attention on high-fidelity notifications
- Authentic full-OS decoys deployed in minutes, anywhere in the network with minimal IT support
- Agentless technology deploys in days with little IT involvement
- Alleviate resource shortages by magnifying the power of expert and non-expert responders
- Streamline remediation with a clear snapshot that focuses investigation activity

"Illusive is a huge time-saver, reducing our triage from hours or days to just minutes. Illusive generates high-fidelity alerts based on quantifiable, real-time data from the source of the attack. If we get an alert, we know we need to investigate immediately."

Security Manager, Retail and Distribution Company

Illusive Networks empowers security teams to reduce the business risk created by today's advanced, targeted threats by destroying an attacker's ability to move sideways toward critical assets. Illusive reduces the attack surface to preempt attacks, detects unauthorized lateral movement early in the attack cycle, and provides rich, real-time forensics that enhance response and inform cyber resilience efforts. Agentless and intelligence-driven, Illusive technology enables organizations to avoid operational disruption and business losses by proactively intervening in the attack process so they can function with greater confidence in today's complex, hyper-connected world

Visit us: www.illusivenetworks.com

Email us: info@illusivenetworks.com

Call us:: US: +1 844.455.8748

EMEA / AsiaPac: +972 73.272.4006

Find us: