illusive splunk>

Real-Time Post-Breach Threat Detection and Management

The Illusive Platform and Splunk Enterprise Security

Illusive Networks has joined forces with Splunk to provide real-time threat detection at breach beachheads while enhancing and automating incident response. Illusive deception delivers high-fidelity alerts that Splunk customers can leverage to shrink the time and overhead required to identify, analyze and remediate threats. With the power of Illusive Networks and Splunk working together, your organization can increase IR and SOC efficiency, expand threat visibility and ultimately harden your overall security posture.

With Illusive and Splunk working in tandem, your organization reaps the following advantages:

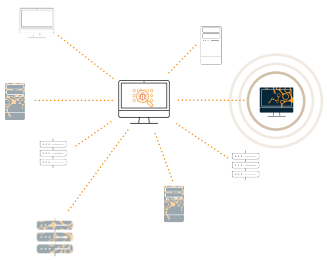
- Detect the most sophisticated human attackers, insiders, and malware
- Automatic or manual isolation of malicious IPs and hosts
- Comprehensive forensic data about attackers and endpoints
- On-demand Illusive forensic collection through Splunk playbooks
- View high-fidelity alerts within Splunk
- Enable additional deception techniques to harden security

How Illusive and Splunk Work Together to Identify and Manage Threats

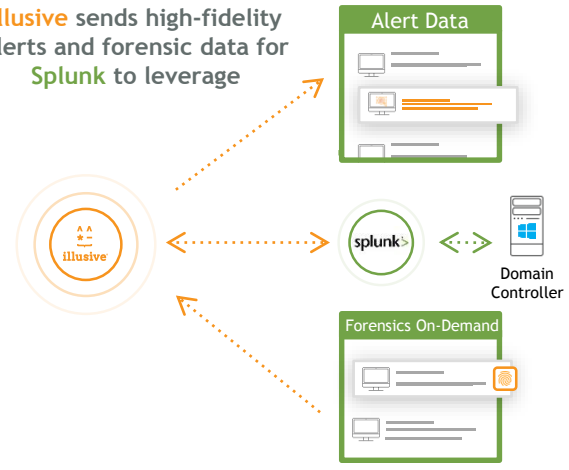
1 — 2 — illusive ⟷ splunk>

Illusive provides the earliest possible detection of lateral movement by humans or malware on the endpoint

Attacker unknowingly accesses a highly authentic endpoint deception



Illusive sends high-fidelity alerts and forensic data for Splunk to leverage



illusive splunk>

Early Breach Detection, Powerful Forensics & Expanded Deception

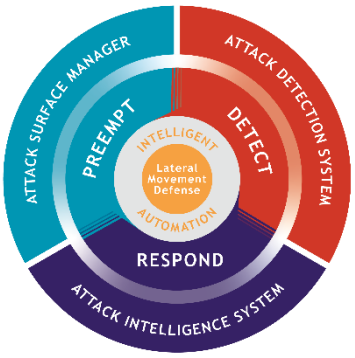
Illusive spreads inescapable deceptions throughout your network that are indistinguishable from the sensitive materials cybercriminals seek to help them move sideways after a breach. Once attackers inevitably interact with one of these deceptions, they provide a high-fidelity incident notification of their malicious presence. Rich forensics about threats and attackers get captured and can be automated as an integral part of your Splunk playbooks.

Splunk also enables additional deception techniques, leveraging Splunk Enterprise Security's communication with your Active Directory to trick attackers into stealing fake credentials, which then act as a beacon that warns of an attacker's presence.

Illusive and Splunk in Collaboration: Key Benefits

- Detect and isolate attackers early in the threat lifecycle
- Halt vertical movement between hybrid and multi-cloud ecosystems
- Amplify the power of limited SOC and IR resources
- Expand viewable attack data & playbook automation scenarios within Splunk
- Harden your security posture with advanced deception techniques

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.



Preempt: Finds and removes errant credentials, connections, and attack pathways to deter unauthorized lateral movement.

Detect: Forces attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making.

Respond: Enables rapid, effective response and remediation when attackers are present by providing contextual source and target forensics.

ABOUT ILLUSIVE

Instead of building walls and restrictive controls around your assets, Illusive disarms the attacker—destroying their decision-making and depriving them of the means to reach their targets.

It's a simple, adaptive approach that empowers your defenders to stop cyberthreats that could otherwise dwell in your environment for months or years.

Built on agentless, intelligent automation that requires very little IT coordination, Illusive immediately shifts the advantage to your defenders—and frees them from the complicated, noisy, data-heavy approaches that burden them today.

ABOUT SPLUNK

Splunk is the world's first Data-to-Everything Platform.

Now organizations no longer need to worry about where their data is coming from, and they are free to focus on the business outcomes that data can deliver.

Innovators in IT, Security, IoT and business operations can now get a complete view of their business in real time, turn data into business outcomes, and embrace technologies that prepare them for a data-driven future.

With more than 5,000 employees in 27 offices worldwide, we're focused on creating lasting data outcomes for our customers.

Visit us at www.illusivenetworks.com

Email us at info@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.