Partner Brief

Illusive and the LogRhythm NextGen SIEM Platform

Real-Time Post-Breach Threat Detection and Management

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

With Illusive and LogRhythm 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 LogRhythm playbooks
- View high-fidelity alerts within LogRhythm
- Enable additional deception techniques to harden security

How Illusive and LogRhythm Work Together to Identify and Manage Threats

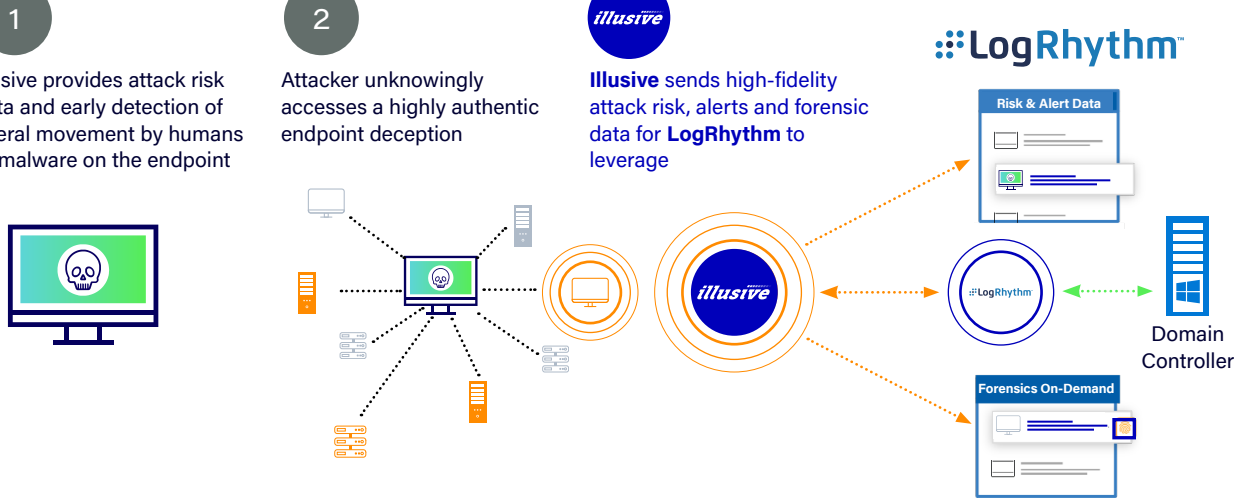
1

Illusive provides attack risk data and early detection of lateral movement by humans or malware on the endpoint

2

Attacker unknowingly accesses a highly authentic endpoint deception

Illusive sends high-fidelity attack risk, alerts and forensic data for **LogRhythm** to leverage



Ensure Attack Surface Hygiene

Illusive identifies and removes unnecessary credentials, connections, and pathways to crown jewel resources.

Early Breach Detection through Deception

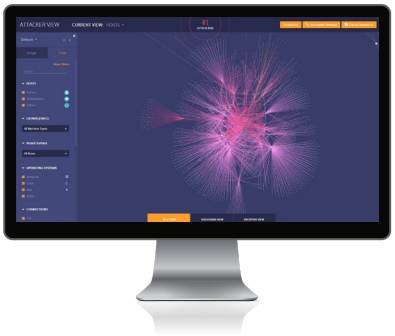
Illusive spreads inescapable deceptions throughout your network that are indistinguishable from the sensitive materials cybercriminals seek to help them move sideways after a breach. Once attackers inevitably interact with one of these deceptions, they provide a high-fidelity incident notification of their malicious presence.

Powerful Source-Based Forensics

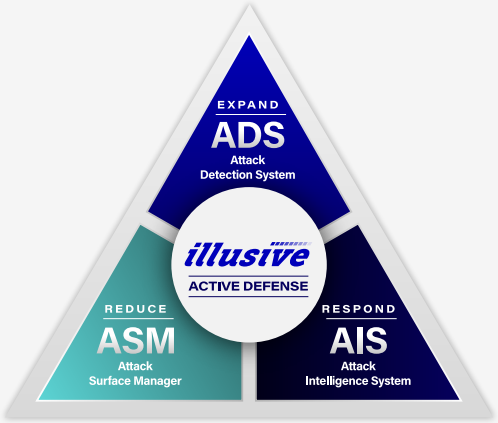
Rich forensics about threats and attackers get captured and can be automated as an integral part of your LogRhythm playbooks. LogRhythm also enables additional deception techniques, leveraging LogRhythm Enterprise Security's communication with your Active Directory to trick attackers into stealing fake credentials, which then act as a beacon that warns of an attacker's presence.

Illusive and LogRhythm 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 LogRhythm
- Harden your security posture with advanced deception techniques



The **Illusive Active Defense Suite** provides centralized management across even the largest and most distributed environments. Three products work together to protect organizations against today's most sophisticated cyberattacks.



ASM: Attack Surface Manager continuously analyzes and removes unnecessary credentials and pathways, reducing the attack surface.

ADS: **Attack Detection System** makes it impossible for attackers to move laterally by transforming every endpoint into a web of deceptions.

AIS: **Attack Intelligence System** delivers human readable on-demand telemetry for current attacker activities to speed investigation and remediation.

Illusive's Active Defense Suite is a vital part of a diversified detection strategy, filling an important attacker lateral movement detection gap in existing perimeter defenses. Each of the products in the Illusive Active Defense Suite play an important role in preventing attackers from achieving their objectives by creating a hostile environment and accelerating the time to detection for an attacker that has established a beachhead.

About Illusive

Illusive reduces cyber risk by shrinking the attack surface and stopping attacker movement. Despite significant investments, it's still difficult to see and stop attackers moving inside your environment. Illusive was founded by nation-state attackers who developed a solution to beat attackers. We help Fortune 100 companies protect their critical assets, including the largest global financials and global pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one! To learn more, visit **www.illusive.com**

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering thousands of enterprises on six continents to successfully reduce cyber and operational risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines advanced security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation and response (SOAR) in a single end-to-end solution. LogRhythm's technology serves as the foundation for the world's most modern enterprise security operations centers (SOCs), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and and OT environments. Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won countless customer and industry accolades. For more information, visit **logrhythm.com**.