Attack Intelligence System™

Get actionable, real-time or on-demand attack telemetry and insight to accelerate blocking and remediation.

Attack Intelligence System (AIS) delivers human readable on-demand intelligence for current attacker activities to speed investigation and remediation. It delivers in-progress screenshots of attacker activity, the tool set in use, command-and-control information, files deployed, and a chronological timeline of the attack as it is occurring. Unlike current approaches to endpoint analytics which require collection and synthesis of data from multiple sources, AIS provides live and detailed insights into attacker tactics and intent. This on-demand telemetry typically reduces SOC analyst investigation time by 60-90%.

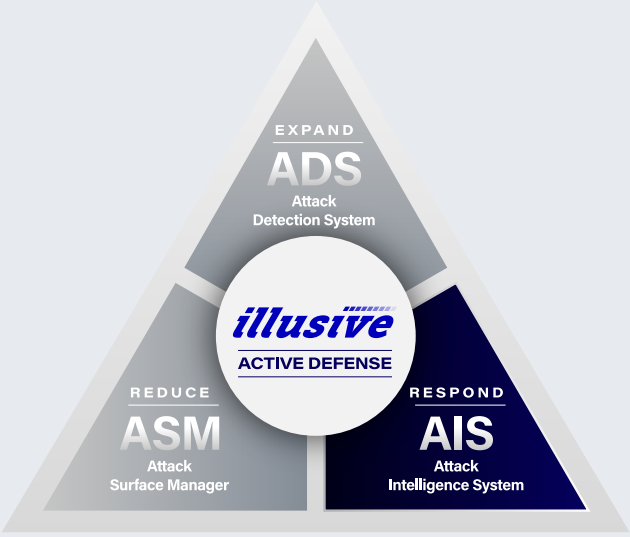
Don't Just Collect More Data – Collect the Right Data and Act

When a ransomware, nation-state or other dangerous attack is in progress and an alert has sounded, time is critical. Often, understaffed incident response teams must execute many separate collection processes and mine volumes of event data across a variety of different and incompatible tools. Attack Intelligence System provides access to detailed, source-based event data delivered in real-time to security teams so they can rapidly analyze and respond effectively to the most urgent incidents. Illusive captures telemetric data from the systems where attackers are operating so defenders can:

- **Quickly make smart decisions under fire**, leveraging real-time, precision intelligence. Immediately upon detection, IR teams can see the attacker's position in relation to critical business assets and are equipped with context-aware data to understand the incident, focus the investigation process, and quickly determine the best course of action.
- **Magnify the power of limited IR resources** by having a single, easily viewable source of unified forensic data that empowers both expert and non-expert defenders.
- **Improve long-term cyber resilience** by gaining in-depth insight into the tools, tactics and techniques of the attacker to integrate lessons and improve future defenses.

Faster, Smarter Incident Response

- Gain efficiency as attacks happen. At the moment of detection, responders have comprehensive insight to quickly determine the best course of action.
- Deploy authentic decoys in minutes, anywhere in the network with minimal IT support.
- Alleviate resource shortages by magnifying the power of expert and non-expert responders.
- Streamline remediation with a clear telemetry snapshot that focuses investigation activity.
- Improve cyber resilience with in-depth insight into attacker motives and methods.



Attack Intelligence System is part of Illusive's comprehensive Active Defense Suite to stop attackers by preempting, detecting and responding to malicious lateral movement.

Attack Intelligence System Features & Benefits

Forensics On Demand

Give probabilistic alerts from other systems the necessary context to speed up investigations and empower junior analysts. Harnessing the power of Illusive's agentless technology, IR teams can initiate forensics collection on any targeted machine, returning in mere seconds precise threat intelligence even if another security solution triggered an alert.

Forensics Timeline for Alert Prioritization

Don't sift through multiple tools and systems looking for the data needed to validate escalation. Illusive's precision, real-time forensics display all collected forensic artifacts in chronological order, allowing analysts to quickly drill down and reduce response time by up to 90%.

Attacker View Dashboard

The management console provides risk context by showing the attacker's proximity to critical systems and privileged credentials.

Trap Server

Interacts with attackers at the endpoint and gathers real-time host forensics when endpoint-based deceptions are activated.

Decoy Module

Enables rapid creation and efficient central management of high-interaction, full-OS decoys. Decoys are created from golden images — a scalable method that produces authentic-looking decoys that reflect the standards and practices native to each customer environment.

Specialized Device Emulations

Use Illusive's pre-built images to speed up and simplify creation of medium-interaction decoys for IoT, OT and network devices so that malicious activity can be detected in environments hostile to agents.

Illusive API

When other tools trigger alerts, Illusive can collect endpoint forensics, provide Forensics Timeline records, and show machines in the Attacker View dashboard.

FirstMove Alert Services

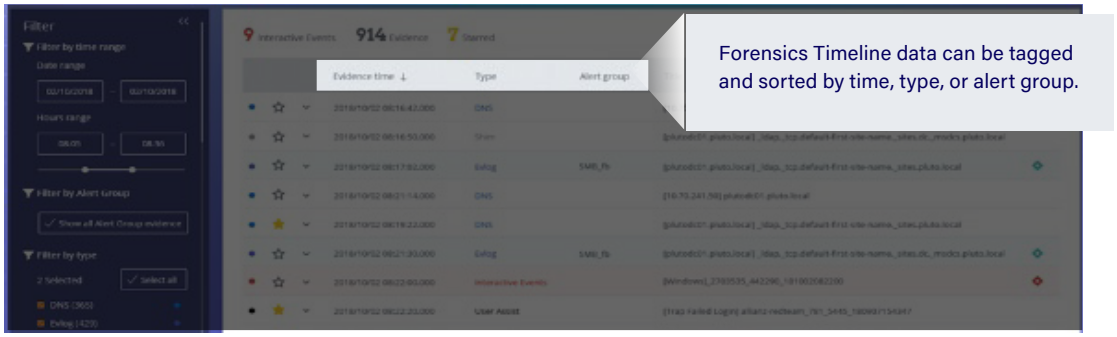
Complement Illusive telemetry and forensics on demand with an alert service contract, giving your team access to our forensic analysts and threat researchers.

From Telemetry to Attack Intelligence

Combined with Illusive's deception-based Attack Detection System, Illusive is the most effective and efficient platform for quickly detecting and stopping malicious lateral movement before attackers reach business-critical assets. Illusive's Decoy Module enables organizations to deploy real-OS, centrally managed decoy systems anywhere in the network—in minutes, and with almost no IT support. Illusive's endpoint forensic collection can also be extended to support any other alerting mechanism in the security operations center. Illusive captures:

1. **Source forensics** from the endpoints where attackers are operating. Source forensics include volatile and non-volatile data from the endpoint, as well as real-time screenshots of in-progress attacks.
2. **Target forensics** from highly-interactive decoys—deceptive surrogate systems ("decoys") that attackers would be interested in compromising. Target forensics provide continuous visibility into the tools, methods, and intent of the attacker.

Compiled into a single **Forensics Timeline**, this intelligence provides unified access to an unprecedented wealth of incident data to accelerate both immediate triage and the larger incident investigation and remediation phases of incident handling.



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 pharmaceuticals. Illusive has participated in over 130+ red team exercises and has never lost one! To learn more, visit **www.illusive.com**