illusive

Attack Intelligence System™

Actionable, real-time forensic insight for accelerated incident response

When a cyberattack is in progress and an alert has sounded, time is critical. Amassing the relevant information is a challenge. Often, understaffed incident response teams must execute many separate collection processes and mine volumes of log files. In the delay, volatile system data is lost. If responders have an incomplete picture of what is happening, hasty decisions can be made that result in failure to address the true nature of the incident.

Incident responders need more than data

Having readily available and easy-to-use information about the attack while it’s in progress is one of the most critical elements of cyber defense. Under pressure, security teams must be able to:

- Quickly discern the attacker’s tactics and objectives
- Pinpoint the attacker’s location in relation to critical assets
- Prioritize actions and make rapid decisions based on potential business impact

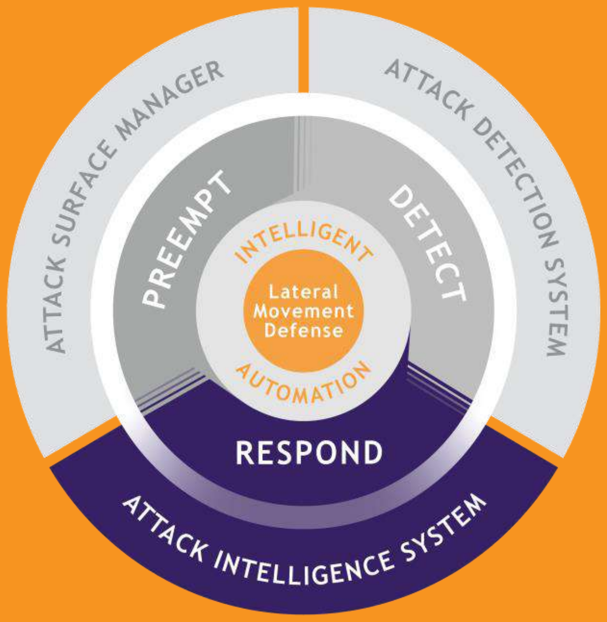
To gauge your confidence level, several questions need to be asked: Are you able to prioritize and escalate incidents quickly? Do you have access to both source and target-based forensics? Can you capture both volatile and non-volatile data? Is the data presented clearly and time-stamped for correlation? Is that data valuable for later investigation to improve future cyber resilience?

From forensic data to attack intelligence

Responders don’t need *more* data, they need the *right* data. Illusive Networks Attack Intelligence System provides rich, precise incident data delivered in real-time, in human-readable format, and supported by insight on potential business impact.

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 Networks Attack Intelligence System empowers IR teams with easy-to-use, precision forensics — both source-based and from decoys — so they can rapidly determine the best course of action to minimize business damage and improve future cyber resilience.



Attack Intelligence System is part of Illusive’s comprehensive portfolio to stop attackers by preempting, detecting and responding to lateral movement.

illusive

Attack Intelligence System components

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.

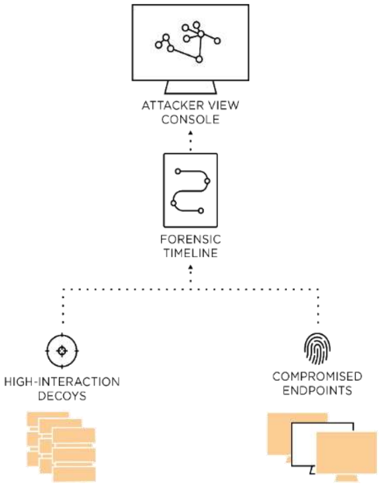
Forensics Timeline: Provides a sortable, per-incident chronology of data collected from endpoint-based deceptions, and high- and medium-interaction decoys.

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

Specialized Device Emulations: Pre-built images speed up and simplify creation of medium-interaction decoys for IoT and networked devices.

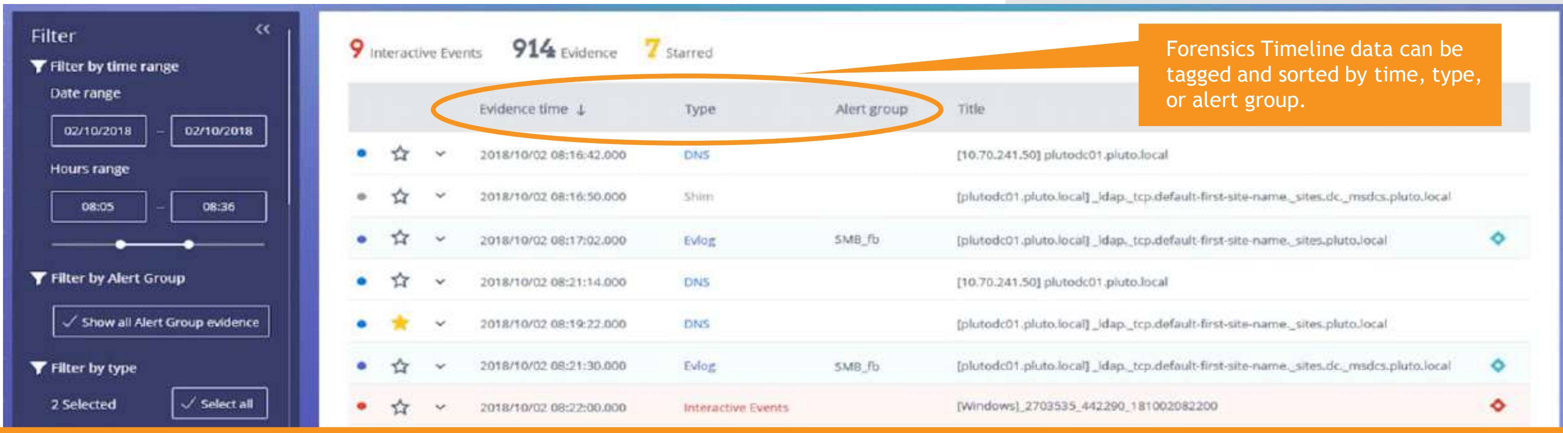
Illusive API: When other tools trigger alerts, Illusive can collect endpoint forensics, provide Forensics Timeline records, and show machines in Attacker View.

FirstMove Alert Services: Illusive forensic analysis and threat researchers can help interpret the severity and nature of events and suggest mitigation options.



Faster, smarter incident response

- **Gain efficiency under fire.** 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 snapshot that focuses investigation activity.
- **Improve cyber resilience** with in-depth insight into attacker motives and methods.



Filter

Filter by time range

Date range: 02/10/2018 – 02/10/2018

Hours range: 08:05 – 08:36

Filter by Alert Group

✓ Show all Alert Group evidence

Filter by type

2 Selected ✓ Select all

9 Interactive Events 914 Evidence 7 Starred

		Evidence time ↓	Type	Alert group	Title	
●	☆	2018/10/02 08:16:42.000	DNS		[10.70.241.50] plutodc01.pluto.local	
●	☆	2018/10/02 08:16:50.000	Shim		[plutodc01.pluto.local]_ldap._tcp.default-first-site-name._sites.dc._msdcs.pluto.local	
●	☆	2018/10/02 08:17:02.000	Evlog	SMB_fb	[plutodc01.pluto.local]_ldap._tcp.default-first-site-name._sites.pluto.local	◇
●	☆	2018/10/02 08:21:14.000	DNS		[10.70.241.50] plutodc01.pluto.local	
●	★	2018/10/02 08:19:22.000	DNS		[plutodc01.pluto.local]_ldap._tcp.default-first-site-name._sites.pluto.local	
●	☆	2018/10/02 08:21:30.000	Evlog	SMB_fb	[plutodc01.pluto.local]_ldap._tcp.default-first-site-name._sites.dc._msdcs.pluto.local	◇
●	☆	2018/10/02 08:22:00.000	Interactive Events		[Windows]_2703535_442290_181002082200	◇

Forensics Timeline data can be tagged and sorted by time, type, or alert group.

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 laterally 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:	in 🐦 f