

● Jammer - high-interaction deception

Trap the adversary. Own the intelligence.

Jammer deploys convincing digital twins of your IT, OT and AI services. Anyone who touches one is hostile by definition. They are held inside the trap, every command is recorded, and you get evidence-grade threat intelligence without the alert noise.



FALSE POSITIVES

≈0

Any contact with a trap is malicious or suspicious by design

OPERATIONAL TIME SAVED

60–65%

In disaster recovery, unauthorised-access and lateral-movement detection

MITRE ATT&CK TACTICS

10–12/14

Up to 10–12 of 14 covered, vs 4–5 for traditional detection

TRAP COVERAGE

IT/OT/AI

A vast, growing portfolio of emulated services, from databases to PLCs and LLM hosting

Figures: Infinitaware, January 2026. Results depend on trap placement and integration.

◆ THE PRINCIPLE

Detection that can't be tuned out, because nothing legitimate ever triggers it.

Signatures and anomaly models guess. A trap doesn't have to: no user, service or process has a reason to touch it.

Jammer turns that certainty into an operational advantage. It exposes intruders and lateral movement early, wastes the adversary's time on decoys, and captures their payloads, shells, C2 and techniques in full. It does all this alongside the tools you already run, without replacing them.

◆ HOW IT WORKS

Lure. Contain. Observe. Respond.

A three-stage mechanism, built to integrate non-invasively downstream of your existing security stack and to avoid big-suite vendor lock-in.



01

Real or simulated services

High-interaction traps run as digital twins of real services or as faithful simulations. They are credible enough to engage human operators and APT tooling, not just scanners.



02

Attacker held inside the trap

Each trap is an isolated, configurable environment. Hostile activity is redirected into it and contained, so it never reaches production assets.



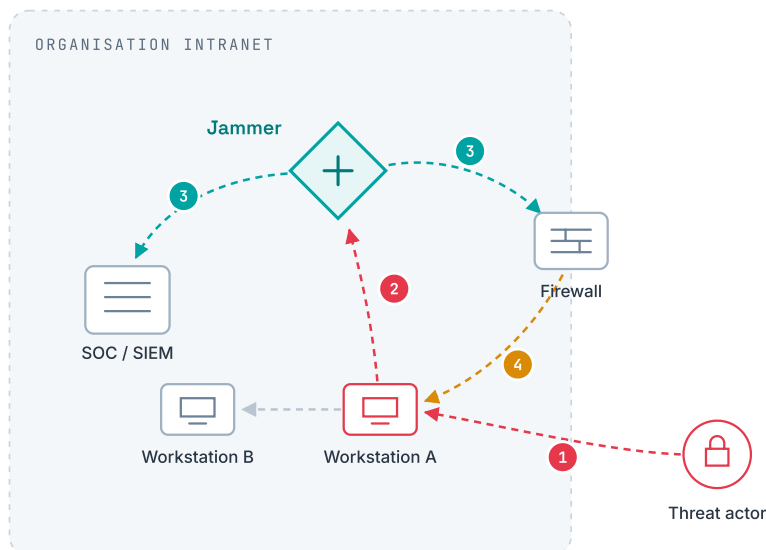
03

Invisible probes record everything

Probes the attacker cannot see log the full session: every command, script, file and network call. This is the raw material for forensic analysis and threat intelligence.

◆ ATTACK SCENARIO

From a single infected workstation to a blocked adversary.

**1 Initial compromise**

A malicious payload infects a workstation. Perimeter tools often miss it, especially if the technique is new.

2 Lateral movement hits a trap

The intruder explores the network and reaches a Jammer trap posing as a valuable service. That contact alone is an unambiguous indicator of compromise.

3 Alert and session forwarding

Jammer notifies the firewall and forwards the full malicious session (commands, payloads, IOCs) to your SOC or SIEM for analysis.

4 Containment

Connections to and from the infected workstation are blocked. The adversary is cut off, and you hold a complete record of what they did and how.

Integrate and reinforce

Jammer strengthens your detection and response capabilities without replacing anything. It sits alongside your current tools and integrates downstream of them for real interoperability.

Protect against the unknown

An advanced barrier that detects and counters any kind of breach. Because it keys on behaviour rather than signatures, it blunts the advantage of new threats and still-unknown vulnerabilities.

React with precision

Detailed forensics on the origin, dynamics and impact of each incident. Pinpoint the exploited weakness, contain the damage fast and harden your defences against the next attempt.

◆ DEFENCE • GOVERNMENT • CRITICAL INFRASTRUCTURE

DEFENCE & GOVERNMENT	Unambiguous early warning inside segmented networks	Seed sensitive segments with traps that mirror real systems. Any touch is a high-fidelity indicator of compromise. Lateral movement surfaces early, and APT tradecraft is recorded end to end instead of being reconstructed after the fact.
CRITICAL INFRASTRUCTURE	OT/ICS deception	Modbus, Siemens S7, Omron and MQTT traps expose reconnaissance against industrial control systems before it reaches real PLCs.
CERT • CSIRT • CTI	Intelligence you can share	Full TTPs, payloads and C2 indicators exported as STIX 2.1. ORB Spotter maps the relay infrastructure behind campaigns.
AI INFRASTRUCTURE	Decoys for LLM attack surfaces	Ollama-based decoys capture attempts against model hosting, including efforts to extract credentials from LLM systems.
REGULATED OPERATORS	NIS2-ready evidence	Forensic-grade session records support incident detection, analysis and reporting obligations.

TRAP COVERAGE

An extensive portfolio of emulated services across IT, OT and AI.

Traps span the assets attackers target first, from data stores and remote access to industrial controllers and AI model hosting.

01 Databases & storage

The data assets attackers come for: relational, NoSQL, search and analytics engines.

MariaDB PostgreSQL MongoDB Redis Elasticsearch

02 Remote access & management

Shells, consoles and remote desktop: the first pivot point in most intrusions.

SSH Telnet RDP Finger

03 Industrial & IoT (OT/ICS)

PLC and industrial protocols for critical infrastructure, plus IoT messaging.

Modbus Omron Siemens S7 MQTT

04 Web stack & AI hosting

Web servers, proxies and dashboards, plus LLM hosting decoys for the newest attack vectors against AI.

Apache httpd NGINX Kibana Ollama

05 Network core services

Routing, name resolution, monitoring, secrets management and orchestration.

BGP DNS SNMP Vault Nomad

06 File transfer & communication

File sharing, mail and video streaming, including the RTSP endpoints typical of IP cameras.

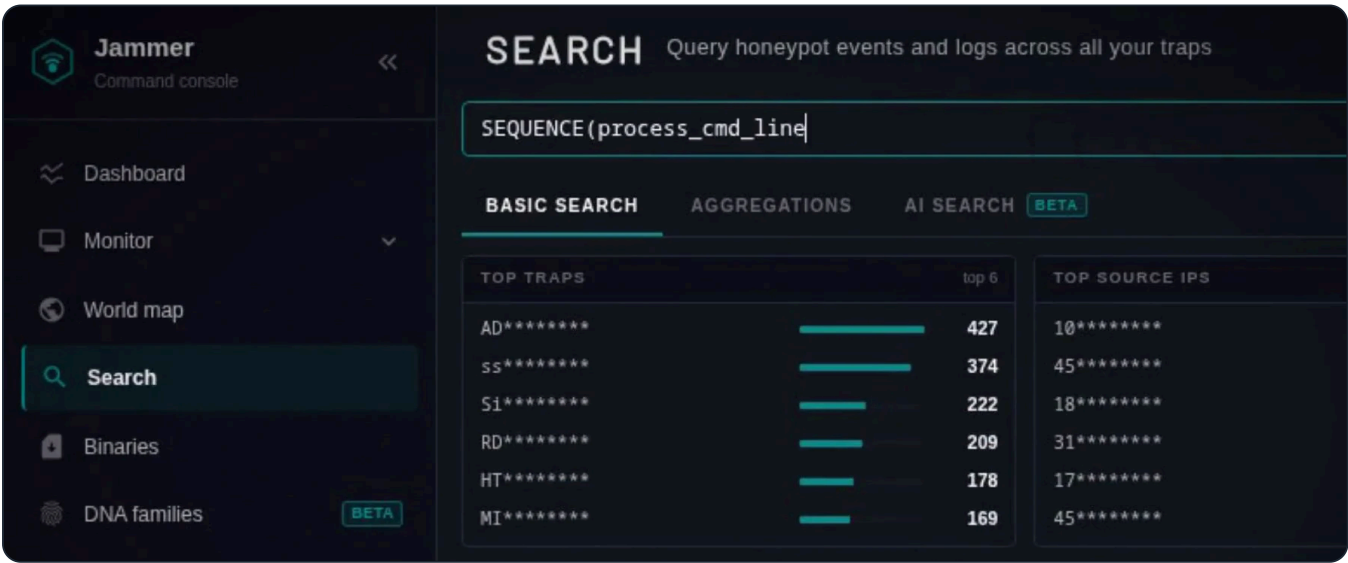
FTP SMB/CIFS SMTP RTSP

Custom traps on demand. The portfolio keeps growing and can be extended with traps that replicate the specific services and applications your organisation runs.

THE PLATFORM

From raw sessions to actionable intelligence.

A modern web console for live inspection and post-analysis, plus APIs and automation for everything else.



Jammer web console, search view. Identifying data is masked.

All your data, centralised

One dashboard aggregates traps, sources, organisations and threats across every sensor.

Live monitoring

A world map of active traps and sessions, updated in real time as attacks unfold.

Advanced session search

A query language over every recorded session, in the console and through the REST API.

Post-attack routines

A visual engine chains filters and actions and runs them on a schedule for tagging, reporting and enrichment.

WHY DECEPTION

Traditional detection vs Jammer.

CRITERION	TRADITIONAL DETECTION	JAMMER
False positives	Frequent: benign events can look malicious	Near zero: every access to a twin is an anomaly
Maintenance burden	High: requires constant signature updates	Low: no signatures, every interaction is suspicious
Lateral-movement detection	Medium: needs complex event correlation	High, with traps placed in key segments
Visibility into attacker behaviour	Limited to logged or reported events	Complete: every script, command and action is monitored
Attractiveness to the attacker	None	High: traps invite interaction
MITRE ATT&CK tactic coverage	4-5 of 14 (e.g. initial access, execution)	Up to 10-12 of 14
Advanced persistent threats (APT)	Complex, often post-compromise	High: a credible lure for APT operators
Value of collected intelligence	Limited	High: payloads, shells, C2, techniques

Figures: Infinitaware, January 2026. Results depend on trap placement and integration.

INTEGRATIONS

No rip-and-replace and no vendor lock-in: Jammer feeds detections and intelligence to your existing stack through open standards.

STIX 2.1 Share threat intel in the standard format	REST API Query and export everything programmatically	IDS / IPS Feed detections to existing sensors	Firewall Trigger blocking of hostile sources	SIEM / SOC Forward full attack sessions for analysis
--	---	---	--	--

WHY SERIOUS ORGANISATIONS WORK WITH US

European, Italian engineering

Designed and developed in Italy by Infinitaware, part of Gruppo Sistematica.

Runs inside your perimeter

Traps deploy within your own network, and the intelligence they collect stays yours.

Non-invasive by design

Installs without disrupting your infrastructure and complements the security tools you already own, so past investments keep their value.

10+ years of expertise

A team with over a decade securing governments, institutions and enterprises.

Tailor-made by R&D

Traps, protocols and integrations adapted to mission-specific environments.

Offensive DNA

Red teaming and reverse engineering experience shape traps that real adversaries believe.

Request a confidential briefing.

Tell us about your environment and we'll show you where Jammer fits. Start with a scoped pilot in a key network segment and decide on evidence.

JAMMER & PARTNERSHIPS
jammer@infinitaware.com

GENERAL
info@infinitaware.com

WEB
infinitaware.com