



**SISTEMA DI RILEVAMENTO DI MINACCE
AD ALTA INTERAZIONE**

COSA FA JAMMER

Jammer è la soluzione di Deception Technology ad Alta Interazione, specializzata nell'analisi approfondita delle minacce e nella generazione di Cyber Threat Intelligence, che si integra in modo non invasivo con l'infrastruttura di sicurezza esistente, evitando il vendor lock-in delle grandi suite.



Servizi reali (digital twin)
o simulati (alta interazione)



Attaccante bloccato
all'interno della trappola



Estrazione di ThreatInt tramite
probe invisibili che registrano la
sessione d'attacco in dettaglio

INTEGRAZIONE E POTENZIAMENTO

Il sistema potenzia le capacità di sicurezza e risposta dell'infrastruttura senza sostituire gli strumenti esistenti, ma affiancandoli ed integrandosi a valle delle soluzioni già in uso per garantire un'interoperabilità efficace.

PROTEZIONE

Una barriera di protezione avanzata, in grado di rilevare e contrastare qualsiasi tipo di violazione della sicurezza, neutralizzando i vantaggi delle nuove minacce e delle vulnerabilità ancora sconosciute.

REAZIONE

Fornisce un'analisi forense dettagliata, consentendo una risposta più efficace e tempestiva. Grazie a informazioni approfondite sull'origine, la dinamica e l'impatto dell'incidente, permette di individuare con precisione le vulnerabilità sfruttate, arginare rapidamente i danni e rafforzare le difese per prevenire future minacce.

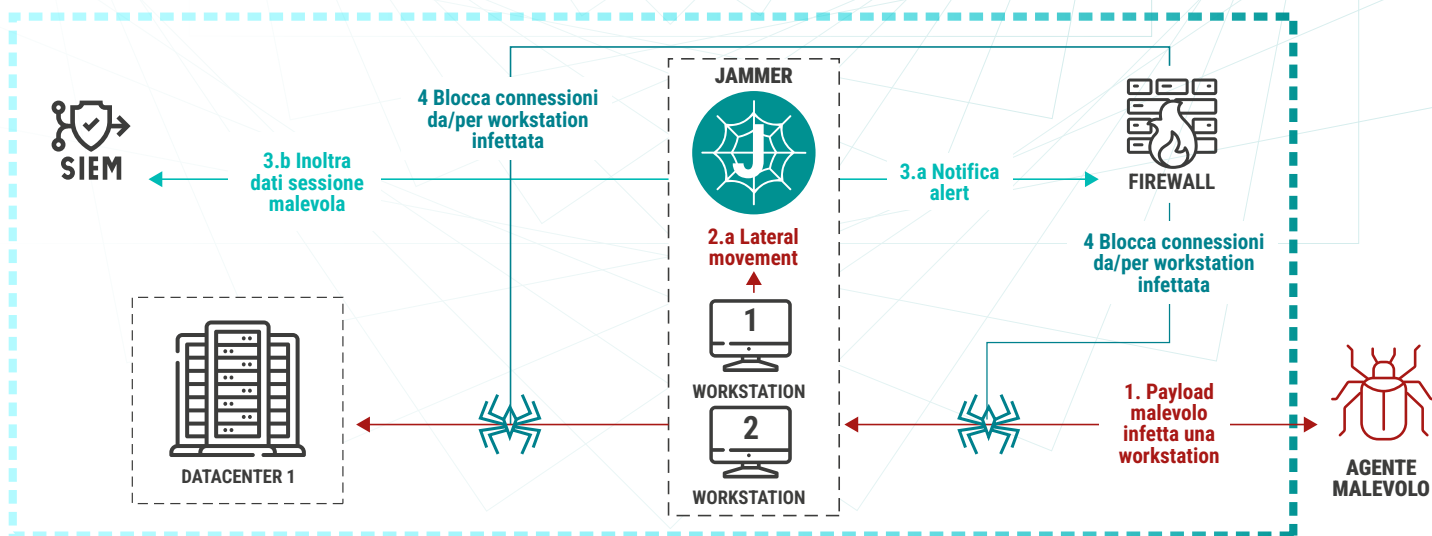
1

Qualora un agente malevolo contatti una delle trappole di Jammer, **siamo sicuri al 100%** che l'attività è malevola o quantomeno sospetta. Ciò significa **rischio nullo di falso positivo!**

2

60/65% è il risparmio temporale garantito in termini operativi nella fase di disaster recovery. Tale percentuale è valida anche per il tempo necessario al rilevamento di accesso non autorizzato e per il *lateral movement*.

INTRANET ORGANIZZAZIONE



PARCO SERVIZI COPERTI



1 DATABASE E STORAGE (DATA ASSETS)

- Database Relazionali: MARIADB, POSTGRESQL
- Database NoSQL: MONGO, REDIS
- Search & Analytics: ELASTIC

2 ACCESSO REMOTO E GESTIONE (MANAGEMENT)

- Shell/Console: SSHD, TELNETD.
- Desktop Remoto: RDP.
- Legacy/Specifici: FINGERD (storico protocollo di informazione utenti)

3 PROTOCOLLI INDUSTRIALI E IOT (OT/ICS)

- /PLC: MODBUS, OMRON, SNAP7 (Siemens)
- IoT Messaging: MQTT

4 WEB STACK E CONTENT DELIVERY

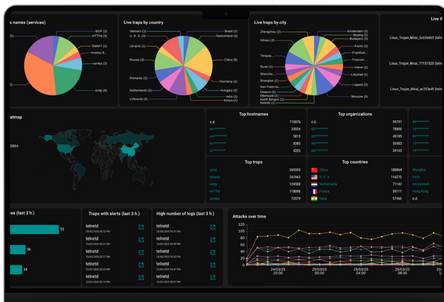
- Web Server/Proxy: HTTPD (Apache), NGINX
- Visualizzazione Dati: KIBANA
- AI/LLM Hosting: OLLAMA (molto rilevante per i nuovi vettori di attacco su AI)

5 INFRASTRUTTURA DI RETE E SERVIZI CORE

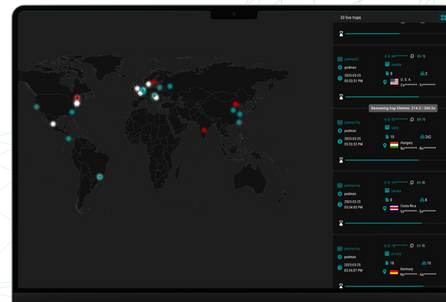
- Routing: BGP.
- Risoluzione Nomi: DNS.
- Monitoraggio: SNMP.
- Secrets Management: VAULT.
- Orchestrazione: NOMAD.

6 TRASFERIMENTO FILE E COMUNICAZIONE

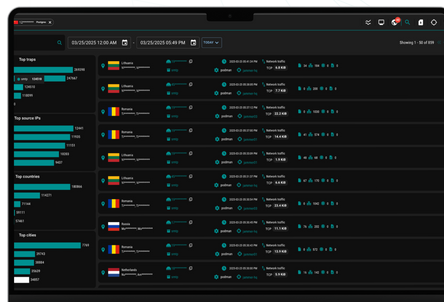
- File Sharing: FTP, SAMBA (SMB/CIFS).
- Posta Elettronica: SMTP.
- Streaming Video: RTSP (spesso telecamere IP).



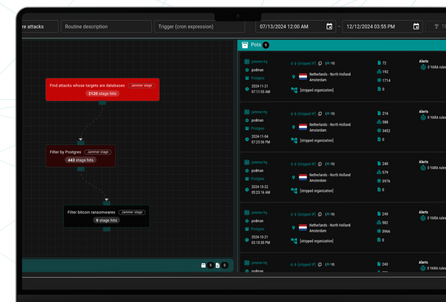
TUTTI I TUOI DATI,
CENTRALIZZATI



MONITORA LA TUA
INFRASTRUTTURA
IN TEMPO REALE



RICERCA AVANZATA
DI SESSIONI DI ATTACCO



ESEGUI AZIONI POSTUME
ALL'ATTACCO GRAZIE
ALL'ENGINE
DELLE ROUTINES

PERCHÉ JAMMER



	RILEVAMENTO TRADIZIONALE	JAMMER
Dipendenza da firme/regole	ALTA richiede aggiornamenti costanti	Nessuna : ogni interazione è sospetta
Alta: richiede aggiornamenti costanti	ALTA richiede aggiornamenti costanti	Media in ingresso , ma aumenta durante movimenti interni
Probabilità di rilevamento in rete laterale	MEDIA (richiede correlazione complessa tra eventi)	Alta se honeypot posizionato in segmenti chiave
Visibilità nel comportamento attaccante	Limitata a eventi loggati o segnalati	Completa : ogni azione è monitorata (script, comando, esfiltrazione)
Attrattività verso l'attaccante	NULLA : è invisibile finché non reagisce	Alta : finto asset credibile stimola interazione
Copertura delle fasi MITRE ATT&CK	4-5 su 14 (es. initial access, execution)	Fino a 10-12 su 14 (includere exfiltration, impact)
Intercettazione comportamenti avanzati (APT)	Complessa, spesso post-compromissione	Alta : honeypot è un'esca credibile per APT
Falsi positivi	Frequenti (eventi benigni possono sembrare malevoli)	Quasi nulli (ogni accesso al twin è anomalia)
Valore delle informazioni raccolte	Limitato (IP, firma exploit, timestamp)	Alto : payload, shell, C2, tecniche usate, fingerprint attaccante
Probabilità complessiva di intercettazione	Dipende dal tuning, media nel tempo	Alta se integrato e posizionato correttamente

LA NOSTRA AZIENDA

Infinitaware SRL sviluppa soluzioni avanzate di cybersecurity per la protezione di infrastrutture critiche e dati sensibili.

Parte del Gruppo Sistematica, l'azienda unisce l'agilità dell'innovazione tecnologica alla solidità di una guida strategica consolidata.

I NOSTRI PILASTRI

SOLUZIONI TAILOR-MADE

Sviluppo di tecnologie resilienti e su misura, frutto di una costante attività di R&D.

EXPERTISE

Un team con oltre 10 anni di esperienza dedicato alla sicurezza di Governi, Istituzioni e Imprese.

VISION

Creare un ecosistema digitale sicuro affrontando le minacce con tecnologie all'avanguardia.

info-jammer@infinitaware.com