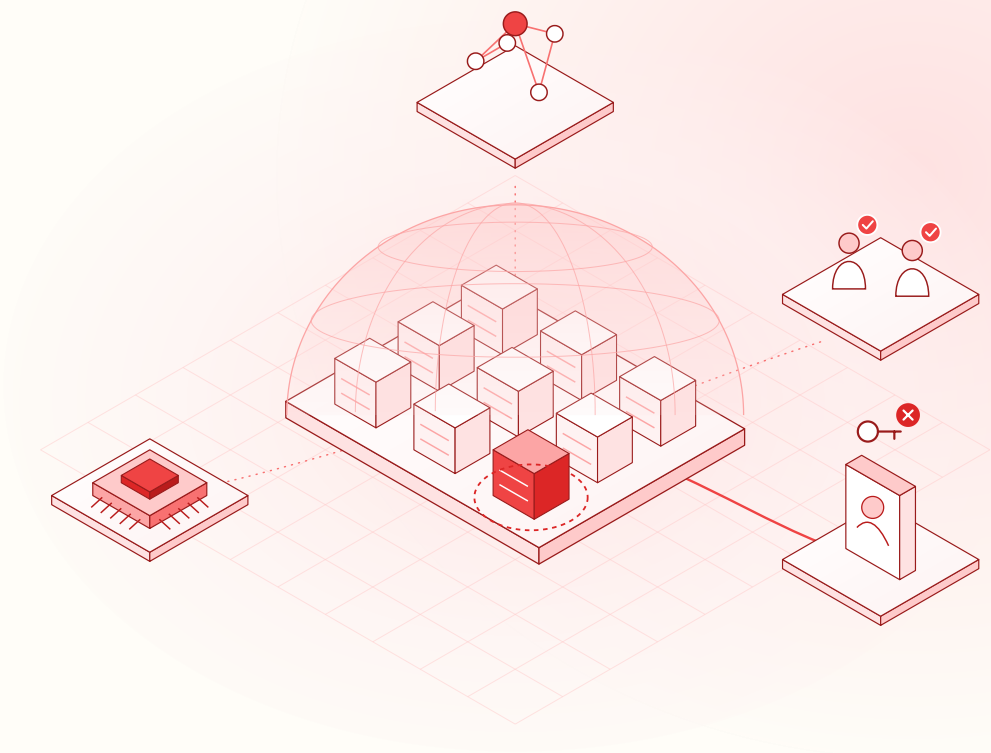
ZERO-TRUST ▪ EBPF EDGE ▪ SOAR CON HUMAN-IN-THE-LOOP

AegisMesh: Contenimento Zero-Trust alla Velocità della Macchina, con Governance Umana

Più veloce dell'attacco, più saggia del panico. La sonda eBPF blocca in locale anche quando il cloud non risponde; un grafo temporale lega processi, host e identità; sugli asset critici due persone approvano il contenimento duale: congelamento del container e revoca delle sessioni cloud, senza distruggere le evidenze.



AEGISMESH

Contenimento duale host + identità cloud · regola delle due persone · validata in staging

02

Cos'è AegisMesh & Value Proposition

Panoramica

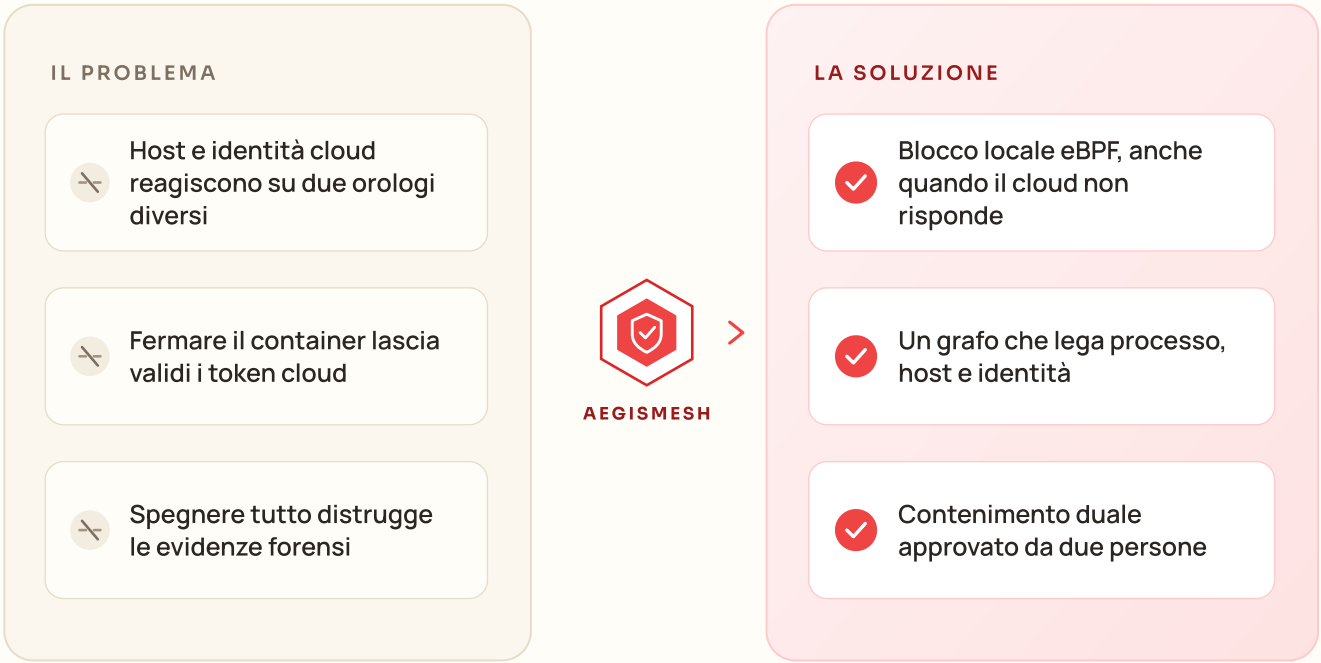
AegisMesh è una piattaforma di cybersecurity Zero-Trust che unisce la telemetria del kernel all'identità cloud federata. È organizzata in quattro livelli: aegis-fabric (identità e posture cloud), aegis-probe (sensori eBPF sul nodo), aegismesh-pipeline (ingestione e archivio nello standard aperto OCSF) e aegis-brain (grafo di attacco e agenti SOAR), più la CLI aegisctl che firma i comandi di contenimento. La piattaforma è stata validata end-to-end su un nodo di staging dedicato.

Il Problema che Risolve

Oggi il perimetro da difendere è l'identità, non più la rete. Quando un server o un container viene compromesso, la compromissione può impiegare minuti o ore a riflettersi sui controlli IAM del cloud. Bloccare solo il processo lascia validi i token federati, con cui l'attaccante può muoversi lateralmente; terminare i workload, invece, distrugge le evidenze forensi.

La Soluzione

Un'elaborazione asimmetrica Edge/Cloud: al bordo la sonda decide da sola, in pochi millisecondi e senza dipendere dal cloud; al centro il grafo correla l'evento con l'identità e propone il contenimento. Le regole di governance sono scritte nel codice: sugli asset standard il contenimento parte in automatico con comandi firmati, sugli asset tier-0 servono due approvatori distinti, anche via ChatOps.



Dal problema alla soluzione.

03

Architettura & Moduli Chiave

01

aegis-probe · Sensori eBPF al Bordo

Programmi eBPF agganciati alle chiamate di sistema execve e connect inviano gli eventi alla sonda (Go) tramite ring buffer; loopback e traffico di infrastruttura vengono scartati già nel kernel. La sonda applica in locale policy firmate che terminano il processo o congelano il container (cgroup v2), anche senza cloud, ed esegue i comandi di isolamento firmati.

02

aegismesh-pipeline · OCSF e Archivio a Due Livelli

Ogni evento viene normalizzato nello standard aperto OCSF 1.3+ (classi 1007 Process Activity e 4001 Network Activity) prima di entrare nel bus Kafka. Un archivio «caldo» ClickHouse serve la caccia interattiva e il SOAR; un archivio «freddo» in Parquet/Apache Iceberg su object storage conserva lo storico a costi inferiori.

03

aegis-brain · Grafo Temporale e SOAR

Il grafo Neo4j collega in tempo quasi reale host, processi, storyline, identità e permessi, e query Cypher riconoscono tecniche MITRE ATT&CK (pacchetto iniziale: T1059, T1078, reverse shell in uscita). Gli agenti SOAR di triage, indagine e rimedio propongono il contenimento; le bozze generate con assistenza GenAI finiscono in coda di revisione, mai in produzione in automatico.

04

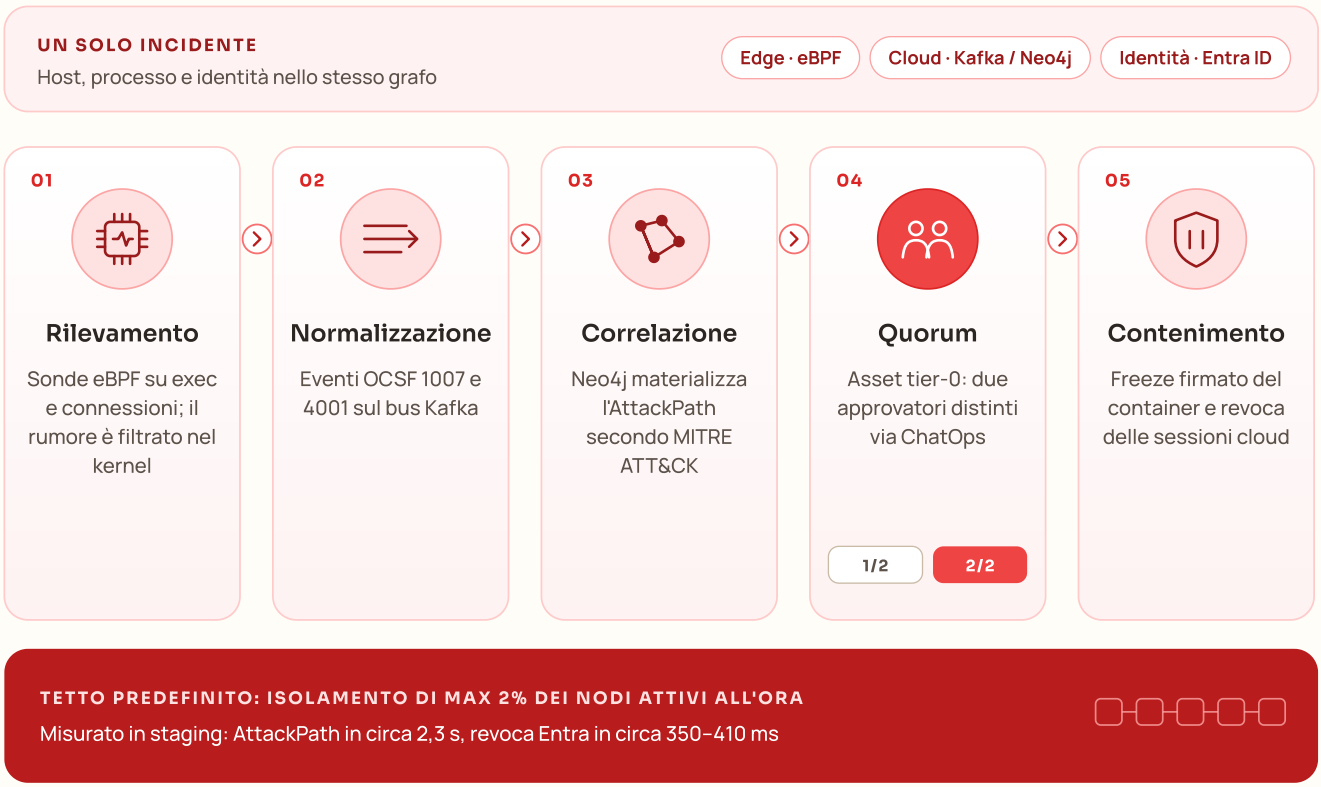
aegis-fabric & aegisctl · Isolamento Firmato

aegisctl firma ogni comando (ISOLATE_HOST, FREEZE_CONTAINER, revoca di sessione) con HMAC-SHA256 e lo pubblica sul bus di controllo: nessuna porta di gestione esposta. Gli isolatori cloud revocano le sessioni Microsoft Entra ID e sono predisposti per la quarantena delle istanze AWS via security group. Il dead-man switch isola il nodo se la sonda smette di dare segni di vita.



03 · ARCHITETTURA

Dal kernel all'identità: il ciclo di contenimento



Sintesi visiva dei moduli descritti nella sezione 03 (catena validata in staging nella fase P7).

04

Vantaggi Strategici

Per SOC, team di piattaforma e responsabili della sicurezza

Velocità al Bordo, anche Offline

La sonda non attende il cloud: blocca e congela in locale. Se Kafka, il cervello centrale o l'identity provider non rispondono, policy locali e dead-man switch continuano a operare.

Governance Scritta nel Codice

Due approvatori distinti per gli asset tier-0 (la stessa persona non vale due volte), un tetto predefinito di isolamento del 2% dei nodi attivi all'ora e una traccia verificabile del quorum: proposta, approvatori, card ChatOps.

Contenimento Duale, Evidenze Intatte

Revoca delle sessioni sull'identity provider e congelamento non distruttivo del container nello stesso intervento: l'attaccante perde host e token, mentre memoria e processi restano disponibili per l'analisi forense.

05

Pronto a chiudere la porta sull'host e sull'account nello stesso momento?

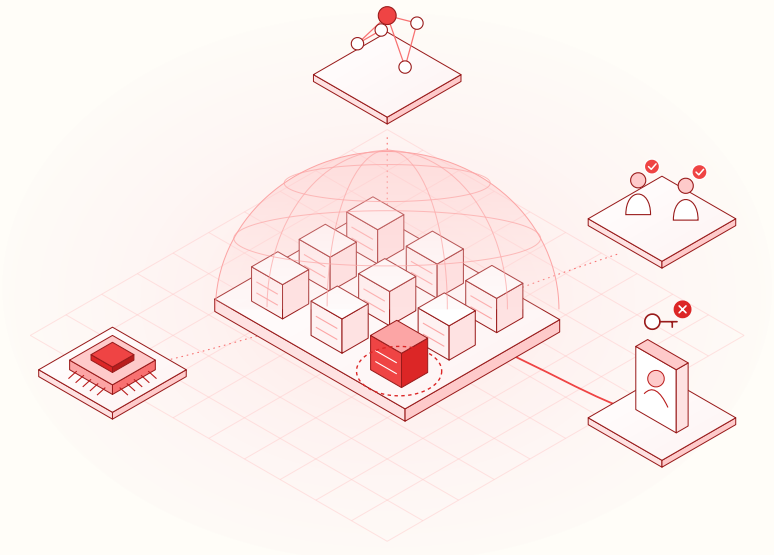
Parla con il nostro Team di Security Engineering

GLOBAL CONSULTANT di Roberto Bonadies

E-MAIL info@globalconsultant.eu

WEB globalconsultant.eu

TELEFONO +39 393 5756044



AegisMesh è validata in ambiente di staging (fasi P4–P7); il passaggio in produzione si concorda per ogni progetto. I tempi indicati sono stati misurati in staging e non costituiscono livelli di servizio garantiti. Il documento non attesta certificazioni né conformità normative. Microsoft Entra ID, Slack e AWS sono marchi dei rispettivi titolari. AegisMesh è una tecnologia di GLOBAL CONSULTANT di Roberto Bonadies.