

ARAKNOS

AS-TM  
AkabSensor

# Akab2

## Traffic Monitoring

**AS-TM** è il sensore del sistema **Akab2** dedicato alla raccolta, monitoraggio ed analisi del traffico di rete.

**Akab2** è un'architettura **SIEM+** (Security Information Event Management), modulare e scalabile, composta di apparati (**AkabSensor**) per la raccolta, la normalizzazione, la correlazione e la presentazione di informazioni provenienti da sorgenti eterogenee esterne. Si ottiene così una visione unificata degli eventi e del contesto (**Situational Awareness**) in real-time per la identificazione di attività sospette e di eventuali minacce.

L'inarrestabile crescita delle infrastrutture di rete ha reso sempre più critico il monitoraggio dei flussi di traffico che le attraversano, inoltre la loro distribuzione e granularità li ha resi uno dei sistemi più efficaci per il controllo del corretto funzionamento dei servizi informativi presenti nelle infrastrutture di rete.

L'integrazione dei dati di Traffico nel flusso informativo gestito dall'architettura **Akab2** è fondamentale, sia dal punto di vista del monitoraggio di sicurezza che dal punto di vista della conformità e tracciabilità degli eventi.

## Funzionalità

### Raccolta

I dati di traffico vengono raccolti in modalità **passiva**, in diverse modalità, adattandosi alle necessità e vincoli di deployment.

Il metodo preferenziale prevede l'utilizzo di apparati dedicati quali **TAP Inline/Aggregatori** che permettono di avere completa visibilità sul traffico, anche in condizioni di particolare carico, riducendo la possibilità di errori o corruzione dei dati in ingresso.

In alternativa possono essere utilizzate le porte **SPAN/Monitor** di apparati (switch/router) che le supportino. Questo tipo di modalità permette una maggiore versatilità ed economicità nel deployment, a scapito della qualità del dato raccolto e dell'affidabilità dell'infrastruttura di monitoraggio. Ove disponibile è possibile utilizzare le informazioni di traffico in formato **Netflow/SFlow** provenienti da sistemi di connettività che ne permettano l'esportazione. Questa modalità è quella che fornisce la più ampia visibilità sull'infrastruttura, a scapito però della tipologia di dato che è mancante di attributi a livello applicativo (*Layer7*).

Le prestazioni del sistema **AS-TM** garantiscono la raccolta di traffico con elevato rate di pacchetti senza degradare le funzionalità di analisi.

### Accounting

Il traffico viene analizzato e ne vengono estratte le informazioni di dettaglio (*source/target /ports/packets/flows/bytes/L7protocol*) relative alle conversazioni tra singoli flussi IP utilizzando evolute tecniche di **packet inspection**. I dati sono salvati e storicizzati in formato aggregato secondo diverse risoluzioni in modo da permettere una completa visibilità sui dati storici con modalità di accesso molto rapide e non vincolate dalla finestra temporale di analisi.

Un sofisticato processo di **Deduplicazione** real-time permette di analizzare il traffico proveniente da diversi sensori eliminando le informazioni ridondanti e duplicate e garantendo accuratezza nei dati raccolti.

L'associazione **passiva** delle informazioni di *Utenti* e *Hostname* permette di avere visibilità trasversale, rispetto ai dati IP-based raccolti.

### Domini di Protezione

La definizione dei **contesti** di analisi (Domini di Protezione) garantisce significatività e specificità nei processi di rilevazione, evidenziando gli eventi che maggiormente impattano sui sistemi interni.

### Network Awareness (NA)

Attraverso l'analisi passiva del traffico il sistema costruisce automaticamente una "mappa" (**Network Awareness**) dinamica e real-time degli **asset** presenti e dei relativi attributi (*IP, MAC, OS fingerprint, Servizi, Vulnerabilità*) e attraverso la definizione di fattori di **Criticità** e **Protezione** ne permette l'integrazione nei processi interni di **Risk Management**.

### User Awareness (UA)

L'analisi passiva permette di rilevare anche informazioni **User-related** che permettono di associare ai contesti di traffico i relativi attributi utente (**User Awareness**).

L'identificazione (*Network Login*) dell'associazione **IP-to-ID** garantisce un visibilità completa sulle attività degli Utenti in rete, indipendentemente dal loro indirizzo IP.

La rilevazione degli accessi degli utenti ai servizi (*Application Login*) permette di tracciare l'uso delle risorse applicative in maniera precisa e contestualizzabile con le attività di rete.

L'integrazione (opzionale) con i sistemi di **Identity Management (IAM/LDAP)** permette di effettuare controlli completi su **Ruoli (Role)** ed **Autorizzazioni (Entitlement)** così come definiti dalle policy aziendali.

### Packet Anomaly Detection (PAD)

Il traffico viene analizzato in *real-time* da **PAD** (*post-pond*), un evoluto sistema di analisi **Flow-based** e **Packet-based** basato su algoritmi **statistici non supervisionati** che permette di identificare eventuali **anomalie** presenti nel traffico che si discostano dalla **Baseline** calcolata.

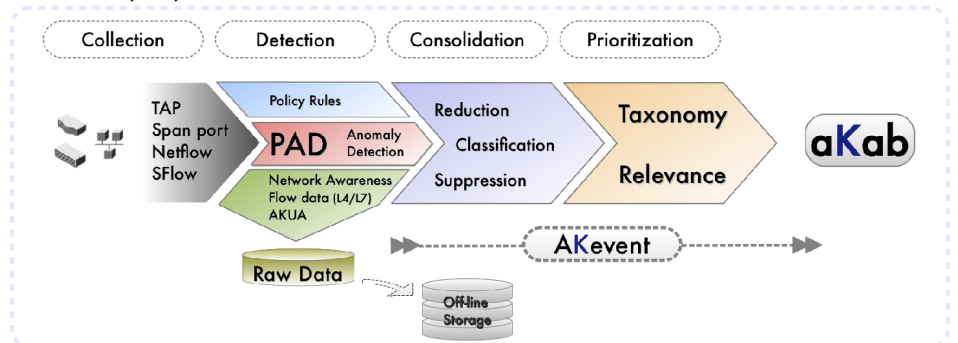
### Policy

Attraverso un articolato processo di filtraggio basato su **regole** configurabili dall'utente è possibile identificare ogni violazione alle **Policy** aziendali relative alle attività di rete permesse.

La sintassi permette di utilizzare tutti gli attributi qualitativi (*IP, porte, ...*) e quantitativi (*duration, byte, ...*) rilevabili dal traffico secondo soglie configurabili. La possibilità di creare nuove regole in maniera semplificata e guidata permette di estendere la libreria integrata che supporta diverse tipologie di eventi (*Portscan, Rogue DHCP e DNS, ...*).

### Prioritizzazione

Ogni evento relativo a cambiamenti nello stato di **NA (Network Awareness)** e **UA (User Awareness)** viene segnalato, permettendo di mantenere sotto controllo lo stato degli **asset** presenti. Nel loro complesso, tutte le informazioni gestite attraverso **NA** ed **UA** contribuiscono al processo di **Prioritizzazione** degli eventi di Sicurezza, permettendo di ridurre in maniera significativa il volume di **falsi-positivi** e garantendo visibilità agli eventi rilevanti nel contesto reale.



## Deployment

### Storage & Backup

Il sistema di *storage* utilizzato implementa un'architettura **proprietaria** ad elevate prestazioni che permette di **superare** i limiti dei tradizionali DBMS. I dati vengono **firmati digitalmente** con algoritmi standard (*SHA256*) e supporto a **TSA** (*Time Stamping Authority*). L'architettura di **backup** permette policy **granulari** per apparato e supporta diverse tipologie di protocolli (*SMB/CIFS, FTP, RSYNC*). Il **partizionamento temporale** e la portabilità del formato ne permettono una semplice gestione.

### Scalabilità

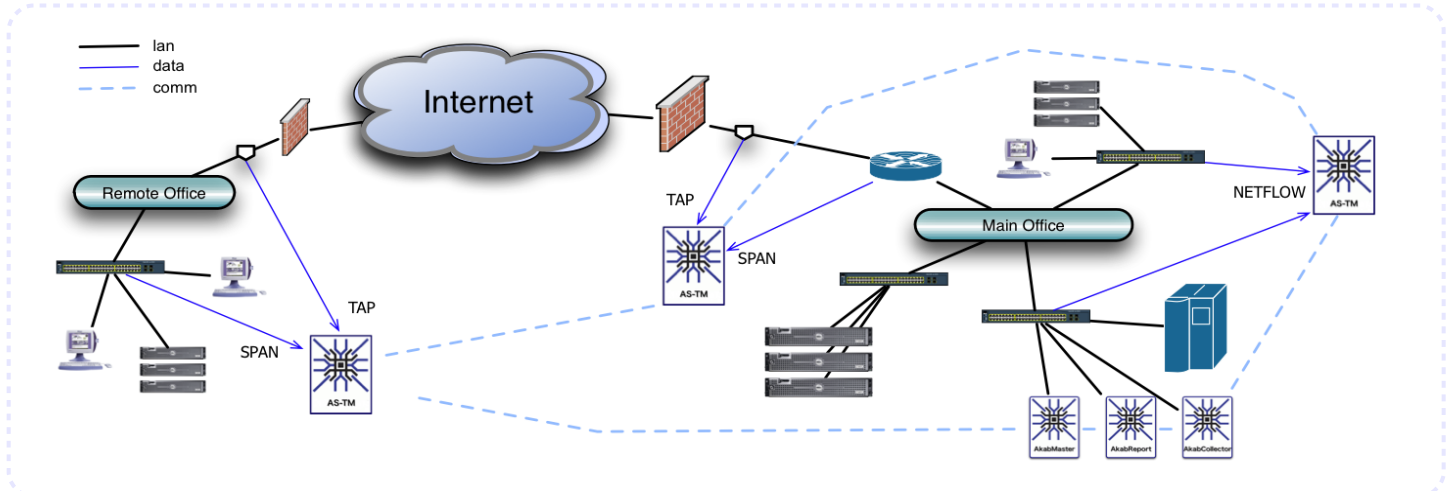
L'architettura **distribuita** di Akab permette l'implementazione di molteplici sensori Akab con questi vantaggi:

- **Flessibilità** in caso di **reti complesse** distribuite sul territorio e Suddivisione del carico di **analisi/raccolta**
- **Economicità** grazie all'ottimale dimensionamento dei singoli sensori necessari ed all'utilizzo di un **unico** punto di gestione ed analisi.

### Sicurezza e Ridondanza

La sicurezza del sistema è garantita a più livelli:

- HW **protetto** e Sistema Operativo (**AraknOS**) hardenizzato e protetto.
- Utilizzo di connessioni di rete **dedicate** inter-apparati e protocolli di comunicazione **sicuri** per la gestione via rete (*HTTPS/SSH*) e **out-of-band** via connessione Seriale (*RS232*)
- **Audit Trail** completo delle attività degli utenti del sistema.
- HW **ridonato** e apparati in **HA** (High Avail.)



## Specifiche Generali

<b>Sorgenti Supportate</b>	<ul style="list-style-type: none"> <li>• Network TAP</li> <li>• SPAN / Monitor port</li> </ul>	<ul style="list-style-type: none"> <li>• Netflow V5/7/9</li> <li>• sFlow v2/4</li> </ul>
<b>Formati</b>	<ul style="list-style-type: none"> <li>• IPv4</li> <li>• UDP/TCP/ICMP</li> </ul>	
<b>Highlights</b>	<ul style="list-style-type: none"> <li>• Real-time Flows Visualization</li> <li>• Historical Accounting</li> <li>• Deduplication</li> <li>• Deep Packet Inspection (DPI)</li> <li>• Passive DNS resolving</li> </ul>	<ul style="list-style-type: none"> <li>• Policing</li> <li>• Anomaly Detection (PAD)</li> <li>• Portscan detection</li> <li>• Rogue DNS/DHCP detection</li> <li>• Fast-Flux detection</li> </ul>
<b>Network Awareness</b>	<ul style="list-style-type: none"> <li>• IP</li> <li>• Service (Port/Protocol)</li> <li>• Vulnerability (CVE/OSVDB)</li> </ul>	<ul style="list-style-type: none"> <li>• MAC</li> <li>• OSFP (OS fingerprint)</li> <li>• Asset Categories (dynamic/static)</li> </ul>
<b>User Awareness</b>	<ul style="list-style-type: none"> <li>• Network Login (IP-to-ID)</li> <li>• Application Login</li> <li>• Auth: AD,LDAP,SMB</li> <li>• IM: XMPP, ICQ, MSN</li> </ul>	<ul style="list-style-type: none"> <li>• Mail: IMAP, POP3, SMTP</li> <li>• DBMS: Oracle, MS-Sql,Postgressql, MySql</li> <li>• Web: HTTP, FTP</li> </ul>
<b>Prioritizzazione</b>	<ul style="list-style-type: none"> <li>• Asset</li> <li>• Criticality</li> </ul>	<ul style="list-style-type: none"> <li>• Vulnerability</li> <li>• Category</li> </ul>
<b>Storage</b>	<ul style="list-style-type: none"> <li>• Vertical database</li> <li>• Compressione dati (sino al 90%)</li> </ul>	<ul style="list-style-type: none"> <li>• Architettura WORM</li> <li>• Elevate performance</li> </ul>
<b>Ridondanza</b>	<ul style="list-style-type: none"> <li>• Apparati in HA (High Availability)</li> <li>• Hardware RAID</li> </ul>	<ul style="list-style-type: none"> <li>• Doppia Alimentazione</li> <li>• Memory mirror</li> </ul>
<b>Integrità</b>	<ul style="list-style-type: none"> <li>• Hashing SHA256</li> <li>• Time Stamping Authority (TSA)</li> </ul>	<ul style="list-style-type: none"> <li>• X.509 certificates</li> </ul>
<b>Archiviazione</b>	<ul style="list-style-type: none"> <li>• SMB/CIFS</li> <li>• FTP</li> </ul>	<ul style="list-style-type: none"> <li>• RSYNC</li> </ul>
<b>Gestione</b>	<ul style="list-style-type: none"> <li>• SSH</li> <li>• SNMP</li> <li>• KVM (local)</li> </ul>	<ul style="list-style-type: none"> <li>• RS232C (console)</li> <li>• Audit Trail</li> <li>• Remote Support</li> </ul>

## Apparati

modelli	AS-TM1	AS-TM2	AS-TM3	AS-TM4
IP gestiti	<b>2000</b>	<b>5000</b>	<b>10000</b>	<b>20000</b>
Flussi/minuto	<b>30K</b>	<b>60K</b>	<b>180K</b>	<b>300K</b>
Banda massima (aggregata)	<b>100 Mbps</b>	<b>400 Mbps</b>	<b>1 Gbps</b>	<b>4 Gbps</b>
Interfacce di Sistema (Mgmt e Comm)	2x Gbit Eth-RJ45			
Interfacce Funzionali	2x Gbit Eth-RJ45	3x Gbit Eth-RJ45	4x Gbit Eth-RJ45	2x 10Gbit XFP
Storage	RAID1 > 500 GB	RAID5 > 1 TB		RAID5 > 2 TB
Chassis	EIA/Rack 1U - 19"		EIA/Rack 2U - 19"	
Peso	25Kg (indicativi)		35Kg (indicativi)	
Alimentazione	350W 100-240V, 50-60 Hz		700W 100-240V, 50-60 Hz	
Condizioni Ambientali	<b>Operative</b> <ul style="list-style-type: none"> <li>• Temperatura: da +10° a +35°</li> <li>• Umidità relativa: 20%-80% senza condensa</li> <li>• Vibrazioni: 3-200 Hz a 0.25G</li> <li>• Urti massimi: 31G a 2.6 m/s</li> <li>• Altitudine: da -16m a 3.048m</li> </ul>		<b>Stoccaggio</b> <ul style="list-style-type: none"> <li>• Temperatura: da -40° a +65°</li> <li>• Umidità relativa: 5%-95% senza condensa</li> <li>• Vibrazioni: 5-500 Hz a 2,2G</li> <li>• Urti massimi: 71G a 2.6 m/s</li> <li>• Altitudine: da -16m a 10.600m</li> </ul>	

