Una possibile soluzione per l'analisi di sicurezza all-in-one

AlienVault-OSSIM in configurazione all-in-one per branch office e sedi medio piccole

Gianluca Peco

INFN CCR Workshop

Sommario

- Contesto 4
- Panoramica dei sistemi esistenti e scelta
- Cos’è e cosa fa OSSIM 3
- Com’è fatto OSSIM 2
- Implementazione del sistema 1
- Demo 5 min.

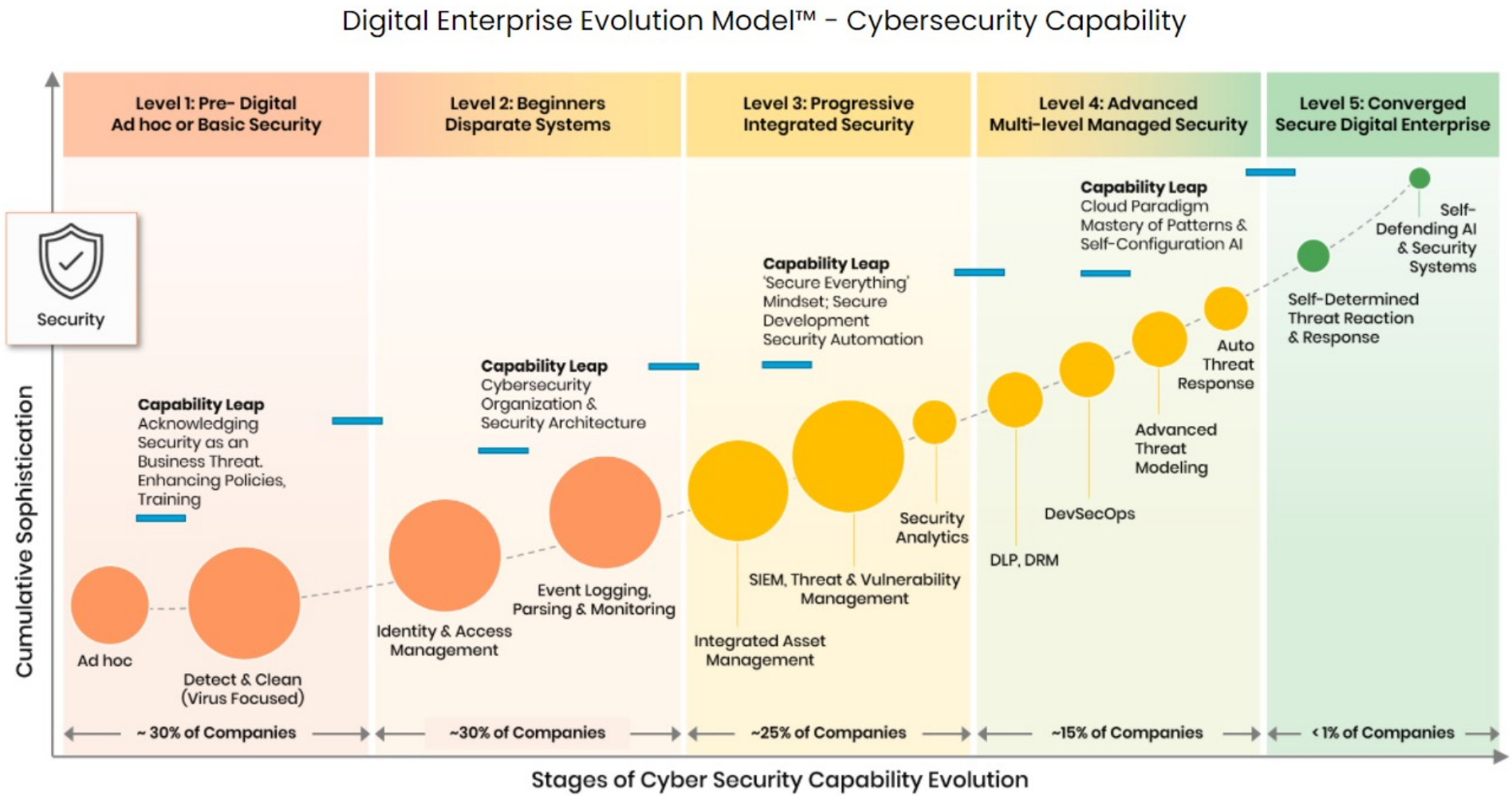
Contesto

Anche a seguito dell'evoluzione delle linee guida di sicurezza delle informazioni risulta estremamente utile dotarsi di uno strumento per il monitoring, l'analisi e la correlazione di eventi di sicurezza (ma non solo), a supporto della difesa attiva, della compliance e dell'analisi forense.

Grandi quantità di dati prodotti dai sistemi di log, dai firewall perimetrali, dalle sonde IDS (Intrusion Detection Systems) e dai sistemi EDR (Endpoint Detection and Response) sono spesso inutilizzati fino all'evento negativo. Esistono strumenti per l'analisi e la correlazione real-time degli eventi di sicurezza sia opensource che commerciali.

I sistemi IT si sono stratificati e differenziati al punto da richiedere la gestione distribuita di attività storicamente centralizzate come l'analisi dei log e degli eventi.

Stadi evolutivi della cybersecurity



Fonte: https://www.trianz.com/cybersecurity

Definizione di SIEM (1/2)

https://it.wikipedia.org/wiki/Security_Information_and_Event_Management

Software e servizi che integrano vari componenti per fornire analisi in tempo reale degli eventi, la possibilità di fornire report inerenti ai dati raccolti, rispondendo alle esigenze di incident response, compliance e analisi forense.

01

Raccolta dati: I log sono la fonte principale di dati analizzati da un SIEM. Ogni apparato di sicurezza, software, database, presente nel sistema invia i dati contenuti all'interno dei file di log al server principale sul quale risiede il SIEM. L'invio dei dati può essere gestito tramite software agent oppure consentendo al SIEM di accedere direttamente al dispositivo. La scelta su quale metodo utilizzare è correlata ai dispositivi che utilizziamo.

02

Parsing e normalizzazione: Ogni dispositivo gestisce e conserva i dati a modo suo, il SIEM provvede ad uniformare i dati raccolti, catalogandoli per tipo di dispositivo e tipo di dato, agevolandone l'interpretazione.

03

Correlazione: La correlazione tra eventi diversi è una delle funzionalità principali, consente di integrare ed analizzare gli eventi provenienti da diverse fonti. Sebbene il SIEM disponga di una serie di regole di correlazione già predefinite, mette a disposizione la possibilità di creare delle regole personalizzate al fine di soddisfare le esigenze degli amministratori. Basandoci sulla correlazione tra gli eventi di sicurezza e i dati sulle vulnerabilità presenti nel sistema è possibile attribuire una priorità ad un evento.

Definizione di SIEM (2/2)

https://it.wikipedia.org/wiki/Security_Information_and_Event_Management

Software e servizi che integrano vari componenti per fornire analisi in tempo reale degli eventi, la possibilità di fornire report inerenti ai dati raccolti, rispondendo alle esigenze di incident response, compliance e analisi forense.

01

***Reporting*:** L'archiviazione dei dati a lungo termine unita alla possibilità di sfruttare query personalizzate per l'estrazione dei dati, consentono la creazione di report. I report possono essere utilizzati a scopo di audit, compliance o di analisi forense.

02

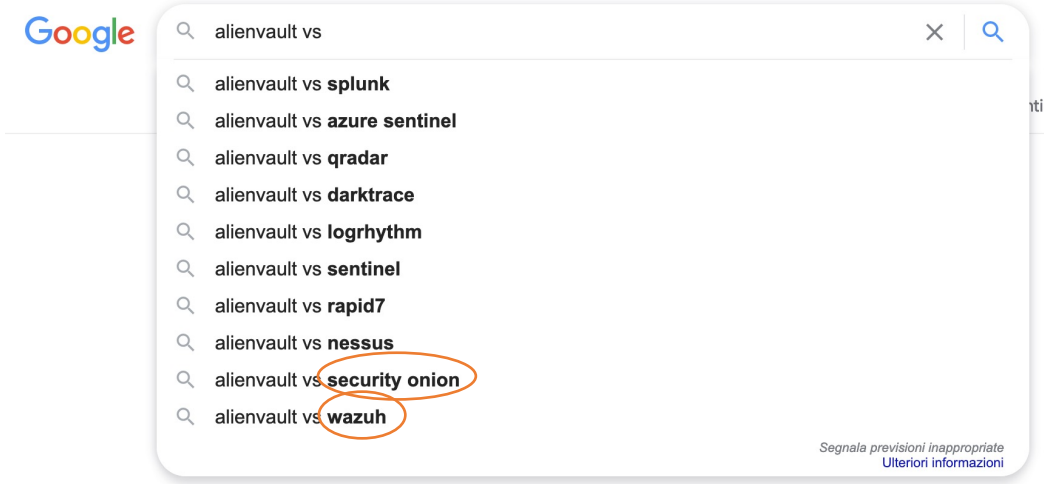
***Dashboard*:** Le dashboard forniscono un quadro generale dell'ambiente di lavoro in tempo reale. Tramite questi strumenti è possibile fornire una rappresentazione dei dati sotto forma di diagrammi o altri modelli, consentendo agli analisti di individuare rapidamente attività anomale.

03

***Notifiche*:** I segnali di notifica e avviso vengono generati al presentarsi di determinati eventi, informando gli utenti di una possibile minaccia. Le segnalazioni posso avvenire tramite dashboard o utilizzando servizi di terze parti come la posta elettronica o gli SMS.

Panoramica dei sistemi esistenti

2020 SIEM Gartner Magic Quadrant



https://l.infn.it/e1

Criteri di scelta:

- Opensource
- Ampia comunità di supporto
- Collaborative Threath Intelligence

Scelta

- La scelta finale è ricaduta su OSSIM che dispone di funzionalità aggiuntive come:
  - Integrazione di molteplici funzionalità in una unico tool “**all-in-one**” (monitoring, asset management, vulnerability scan, analisi dei flussi, NIDS, HIDS, report)
  - Possibilità di integrare, utilizzare e partecipare alla OTX Open Threat *Intelligence* Community
  - Utilizzo di plugin di correlazione e normalizzazione standard, free e modificabili
  - Reportistica per la compliance preconfezionata

Cos'è OSSIM-AlienVault

https://en.wikipedia.org/wiki/OSSIM

https://cybersecurity.att.com/products/ossim/compare

Progetto iniziato nel 2003, nel 2008 viene creata l'azienda AlienVault che inizia a vendere un derivato commerciale di OSSIM: AlienVault Unified Security Management – USM.

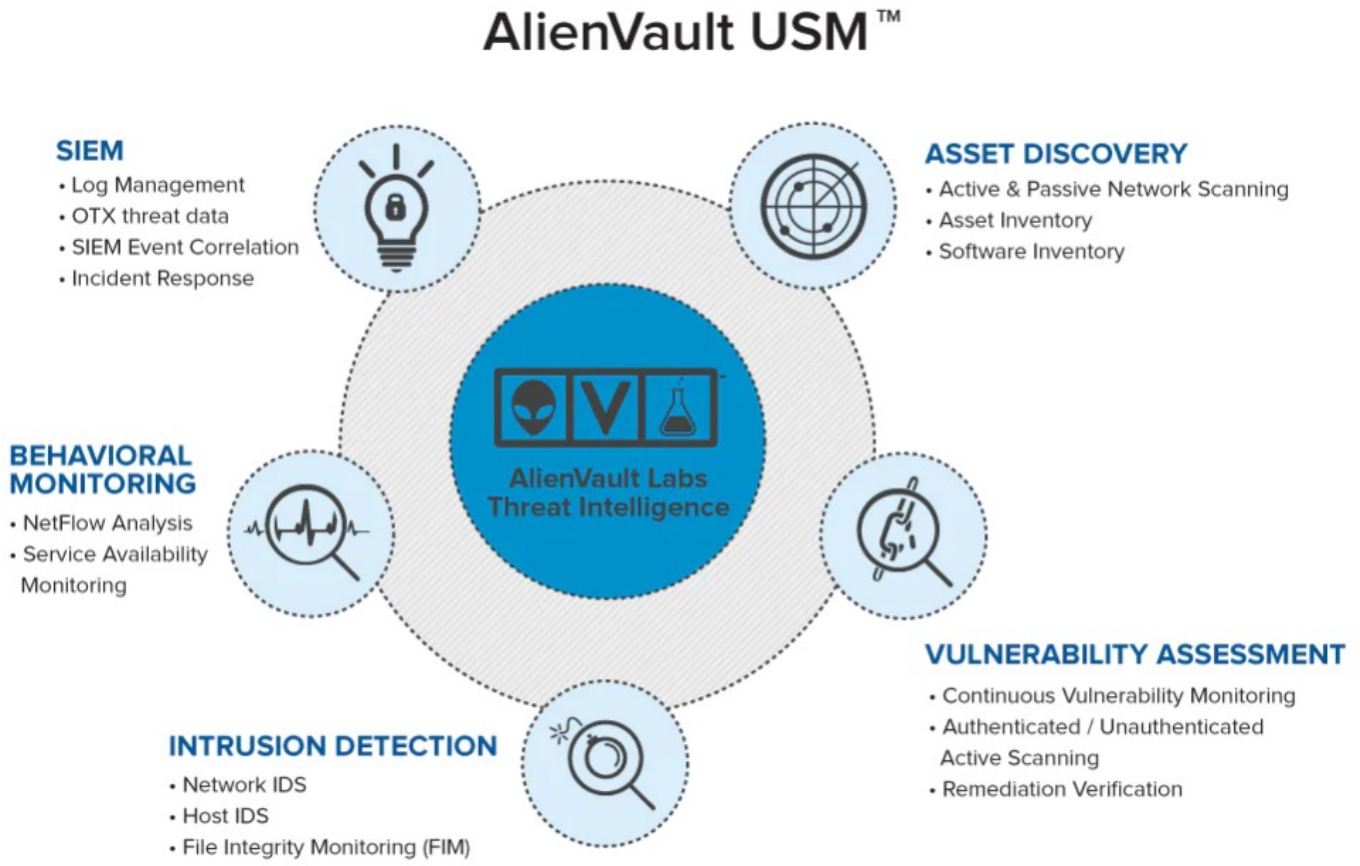
AlienVault viene poi acquisita da AT&T Communications nel 2019 e viene rinominata AT&T Cybersecurity.

OSSIM viene distribuito con licenza GNU GPL e contiene e seguenti componenti:

- **PRADS** usato per identificare host e servizi tramite il monitoraggio passivo del traffico di rete
- **Snort** usato come IDS, e per costruire cross-correlation con OpenVAS.
- **Suricata** usato come IDS (IDS di default a partire dalla versione 4.2)
- **Tcptrack** usato per raccogliere dati sulle sessioni che possono essere correlati agli altri dati per avere più informazioni sugli attacchi
- **Munin** per l'analisi del traffico e come whatchdog dei servizi
- **NFSen/NFDump** usato per collezionare e analizzare le informazioni NetFlow
- **FProbe** usato per generare dati NetFlow dal traffico catturato
- **Nagios** usato per monitorare host e porte specifiche, per verificare la disponibilità degli asset e come sistema di monitoring locale
- **OpenVAS** usato per vulnerability assessment, associato agli asset
- OSSIM include anche una serie di tool sviluppati ad-hoc come un **motore di correlazione** che supporta direttive logche e **l'integrazione dei log** attraverso plugin.

Cosa fa OSSIM-AlienVault

USM Anywhere Architecture Diagram



https://cybersecurity.att.com/documentation/usm-appliance/system-overview/about-usm-solution.htm

Cosa fa

Asset Discovery — Combines core discovery and inventory technologies to give you visibility into the devices that are on your network.

Vulnerability Assessment — Identifies assets and devices with unpatched software, insecure configurations, and other vulnerabilities on your network

Intrusion Detection — Coordinates incident response and threat management across your network with built-in security monitoring technologies, emerging threat intelligence from AT&T Alien Labs™, and seamless closed-loop workflow for rapid remediation.

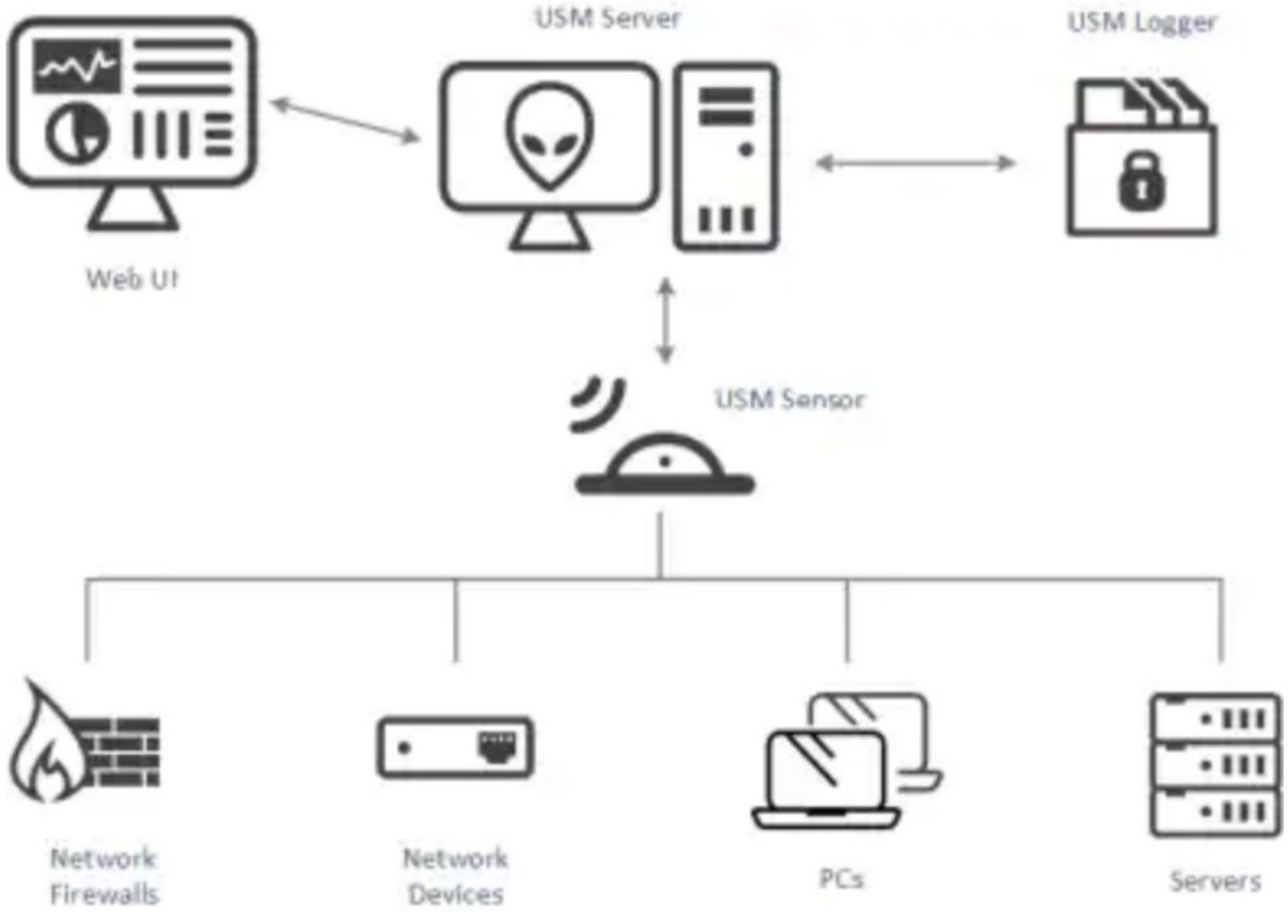
Behavioral Monitoring — Identifies anomalies and other patterns that signal new, unknown threats in your network, as well as suspicious behavior and policy violations by authorized users and devices

Security Information and Event Management (SIEM) — Identify, contain, and remediate threats in your network by prioritizing your risk and response

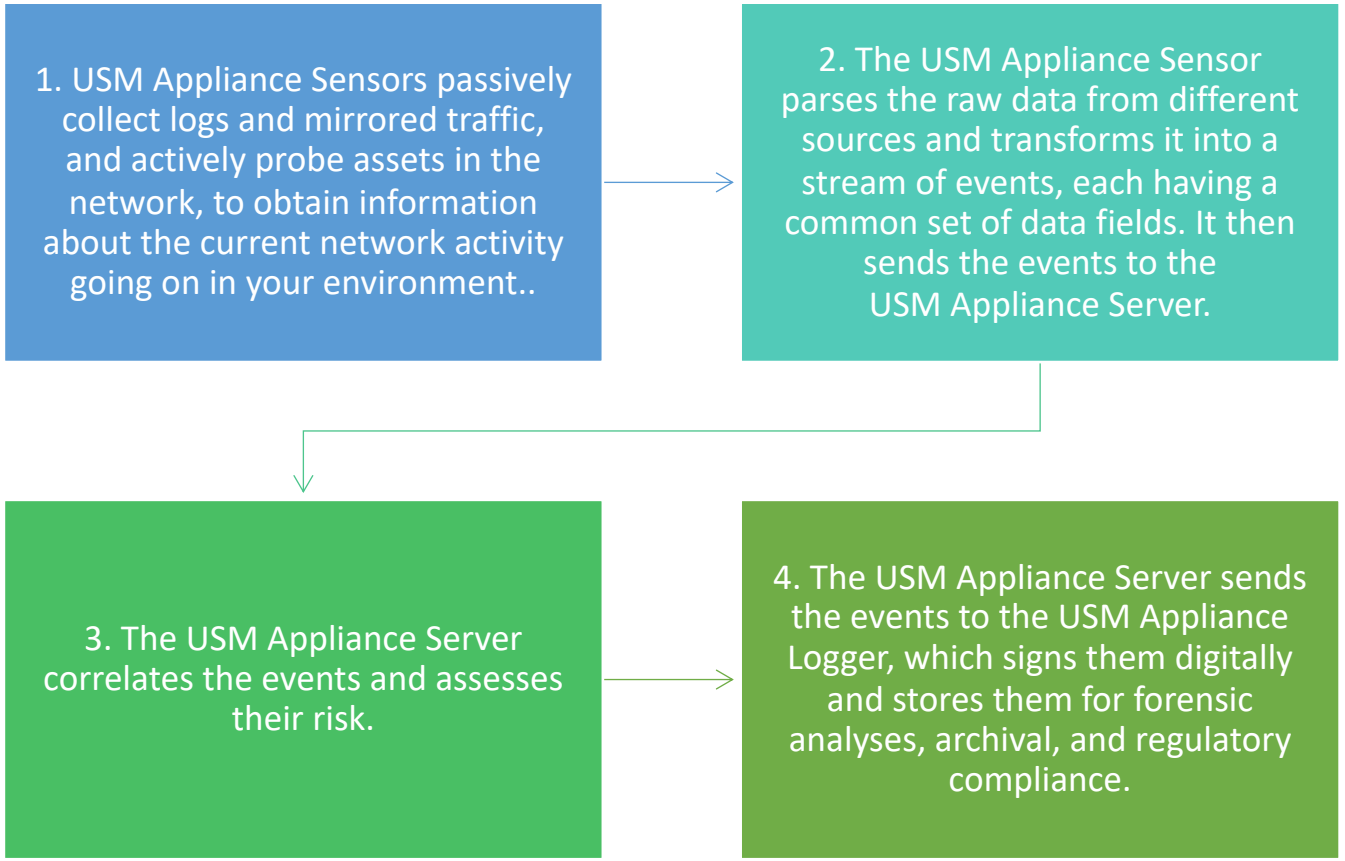
Com’è fatto

The three components of the **USM Appliance architecture** that work together to monitor and provide security are:

- USM Appliance **Sensor(s)** — Deployed throughout the network to collect and normalize information from any devices in your network environment that you want to manage with USM Appliance. A wide range of plugins are available to process raw logs and data from various types of devices such as firewalls, routers, and host servers.
- USM Appliance **Server** — Aggregates and correlates information that the USM Appliance Sensors gather. (This is USM Appliancès SIEM capability). Provides single pane-of-glass management, reporting, and administration through a web-based user interface.
- USM Appliance **Logger** — Securely archives raw event log data for forensic research and compliance mandates. (This archive of raw event data is also referred to as *cold storage*).



USM Appliance Workflow



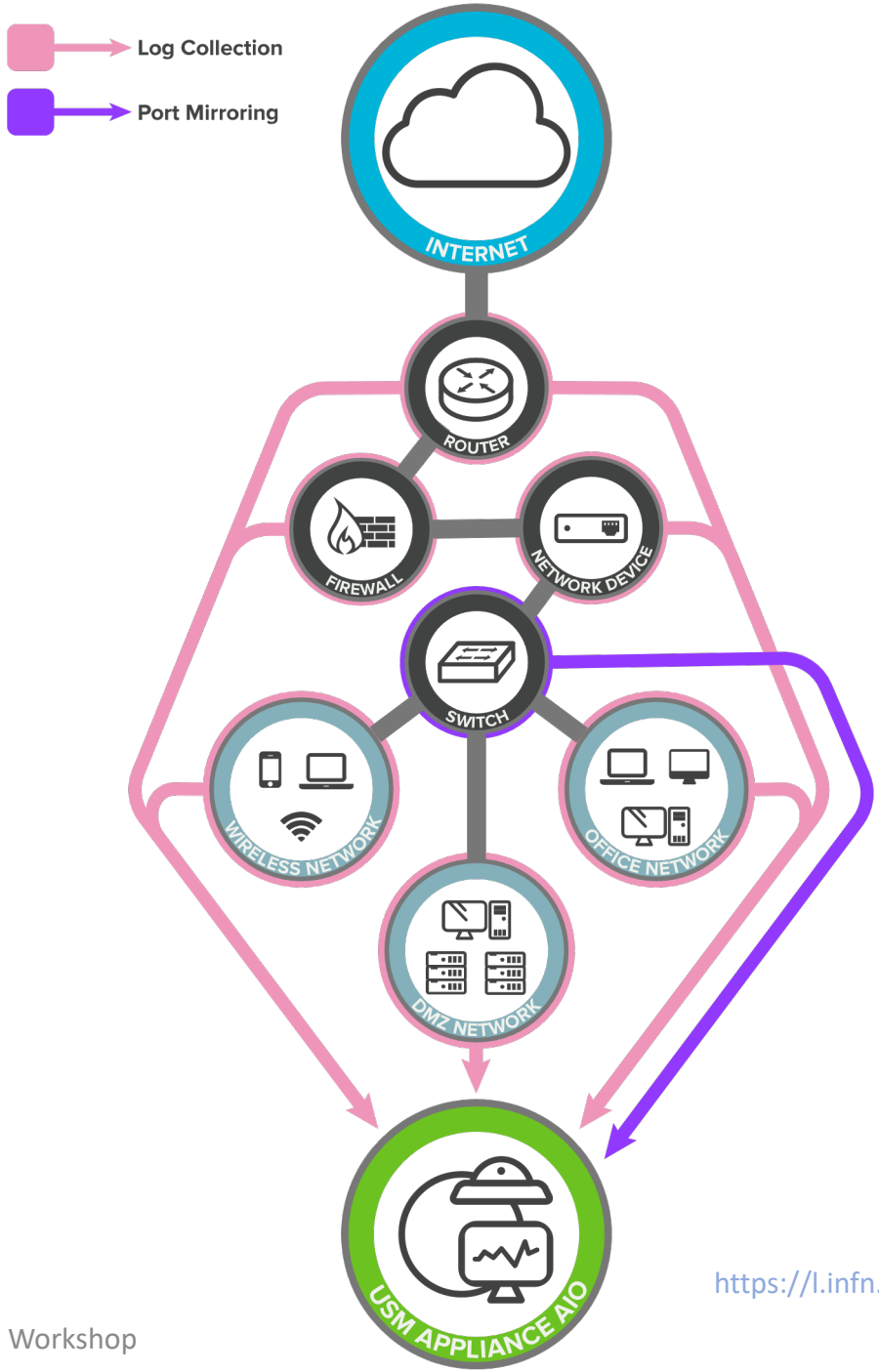
USM Appliance Deployment Options

Simple Deployment Model — All USM Appliance components (Sensor, Server, and Logger) are combined in a USM Appliance All-in-One appliance. This configuration is most often used in smaller environments, as well as for demonstrations and proof-of-concept deployments.

Multi-tier, Distributed Deployment Model — This model deploys each AlienVault USM Appliance component (Sensor, Server, and Logger) as an individual virtual or hardware appliance to create a distributed system topology.

Implementazione del sistema

- Esempio di USM Appliance All-in-One (hardware oppure virtuale) dispiegato dietro ad un corporate firewall.
- Il sensore che fa parte di USM Appliance All-in-One collezione log da diverse reti e apparati:
  - Office network
  - Wireless network
  - DMZ
  - Firewall
- USM Appliance All-in-One monitora il traffico attraverso gli switch.
- Gli switch devono aver abilitato il port mirroring.



https://l.infn.it/eh

Threat Intelligence e OTX

- Abbiamo creato un'account con licenza gratuita alla rete OTX per lo scambio collaborativo degli indicatore di compromissione delle minacce zero day.
- Abbiamo sottoscritto vari feed legati alle tipologie di minacce piu' interessanti per il nostro contesto ed attivato l'integrazione nella Threat intelligence del motore di correlazione degli eventi
- I feed sottoscritti vengono aggiornati realtime attraverso una chiave simmetrica da scambiarsi tra portale e siem
- E' possibile partecipare attivamente alla rete attraverso la pubblicazione di IoC pubblici

Demo

- Dashboard
- Alarms
- Security Events
- Asset Management
- Vulnerability (OpenVAS)
- Availability (Nagios)
- Detection (HIDS-Ossec)
- Reports
- Deployment
- Threat Intelligence
- Open Threat Exchange
- View account details

The end

Domande?