

Piattaforma intelligente per la protezione in real time degli asset aziendali dagli attacchi informatici (Sybilla)

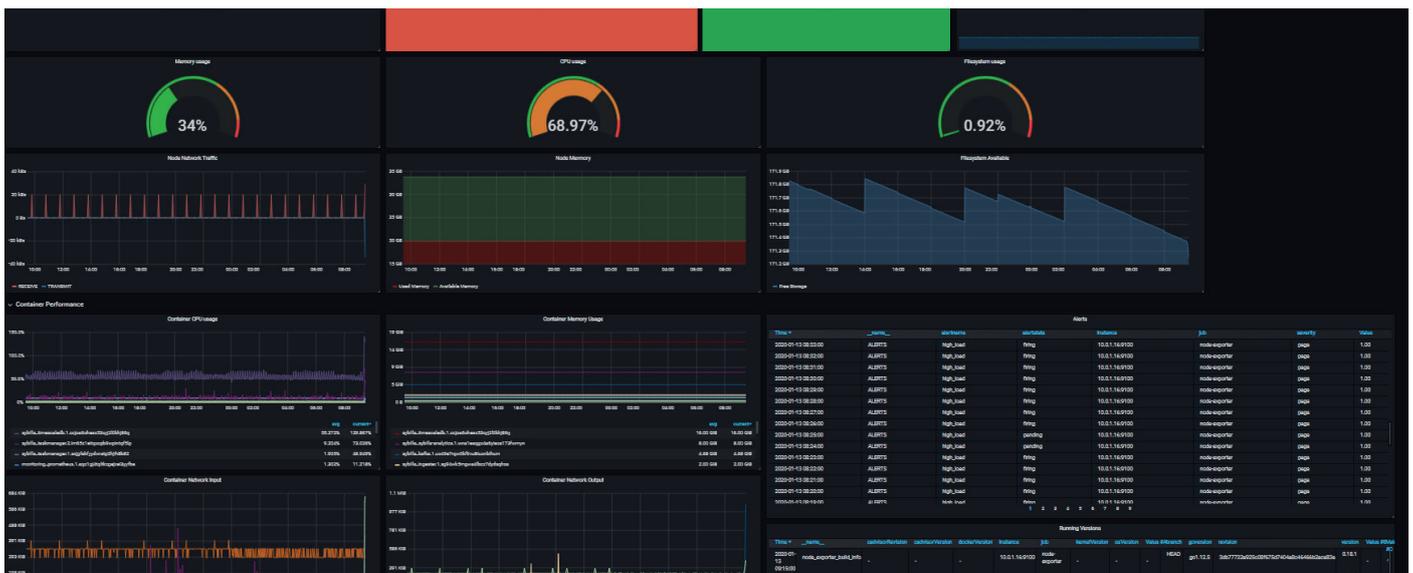
Il progetto Sybilla intende realizzare uno strumento di intelligence aziendale, in grado di integrare tutti i dati provenienti dall'infrastruttura informatica, e in continuo aggiornamento, per **prevenire gli attacchi informatici ed intervenire tempestivamente** al loro verificarsi.

La piattaforma realizzata da Florence consente di prevenire ed individuare eventuali accessi abusivi all'infrastruttura informatica di un'azienda e **monitorare real time lo stato** dell'infrastruttura, integrando le proprie conoscenze con informazioni aggiuntive provenienti da fonti eterogenee, sia interne che esterne al perimetro aziendale. Supportato da un **sistema di machine learning**, l'aggregato di dati ottenuto fornisce un'istantanea della situazione e rileverà l'eventuale presenza di informazioni che possono essere sfuggite al controllo aziendale.



Il moderno scenario di cybersecurity vede un **incremento estremamente significativo degli attacchi informatici**, sia per numerosità che per complessità ed efficacia. La diffusione sempre più pervasiva dei sistemi informatici in ogni ambito aziendale ed industriale, nei processi produttivi e infrastrutturali e nei servizi su vasta scala ha contribuito a rendere le attività illecite di frode, sabotaggio e ricatto, imperniate su tali sistemi, sempre più remunerativa e dunque allettante per potenziali hacker.

Sybilla è una piattaforma informatica di **analisi e correlazione degli eventi all'interno delle infrastrutture IT**, con un focus specifico sul traffico della rete dati, vettore preminente di attacchi e minacce. Sybilla implementa algoritmi di **Machine Learning** e **Behaviour Analysis** per identificare il funzionamento "normale" di un'infrastruttura e conseguentemente rilevare eventuali anomalie che dovessero presentarsi rispetto a tale norma.

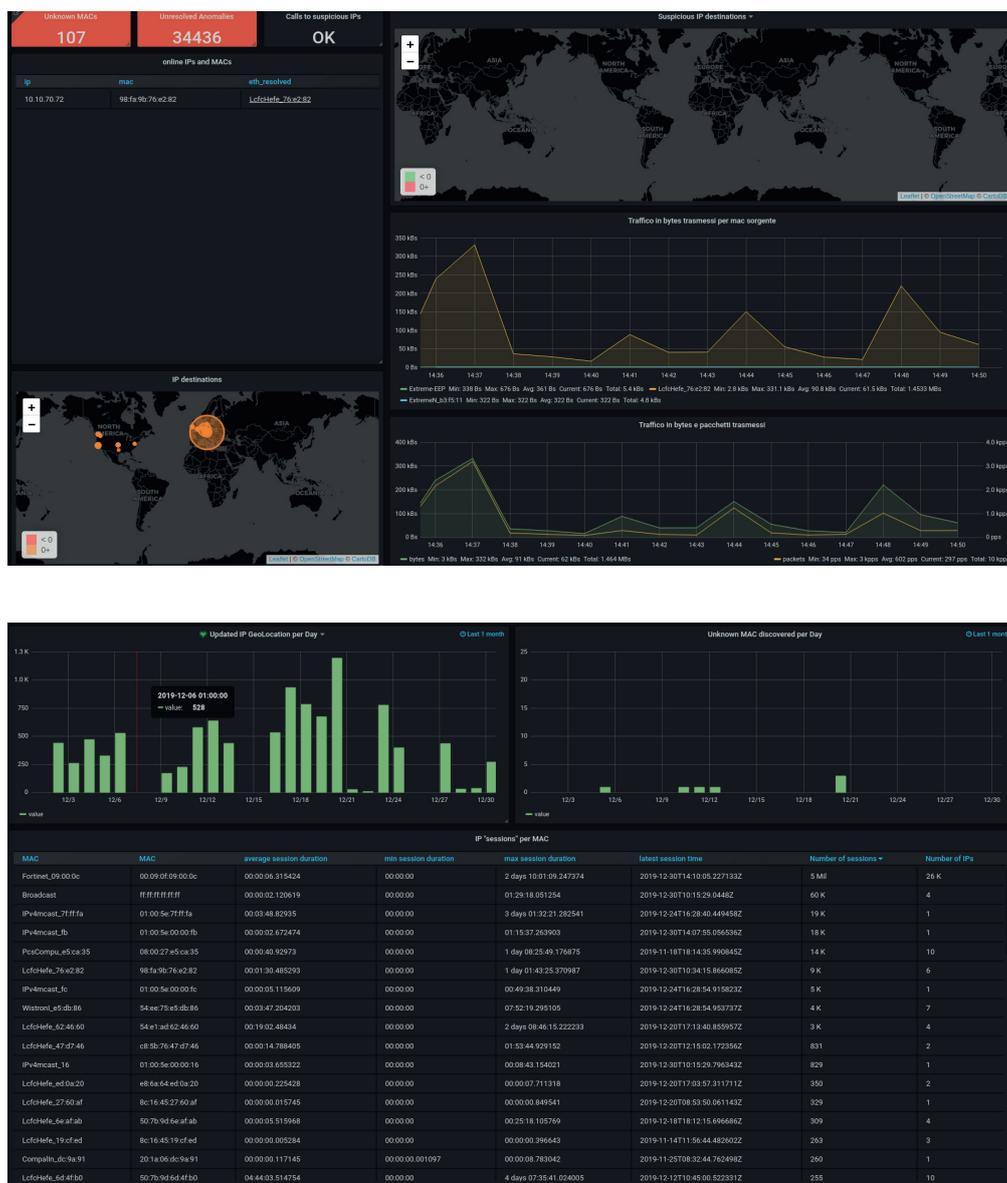


La piattaforma non necessita di agent installati sui client ma si basa sull'**analisi del traffico di rete** all'interno dell'infrastruttura IT. Gli algoritmi implementati all'interno della piattaforma sono quindi capaci di apprendere le condizioni di funzionamento ordinario dell'infrastruttura e di conseguenza di **rilevare variazioni anomale** nel momento in cui queste hanno luogo.

La soluzione può essere implementata con un **impatto minimo sull'infrastruttura esistente**. Agendo come un collettore passivo dei flussi di dati in transito, una virtual appliance raccoglie ed elabora le informazioni e mette a disposizione dell'amministratore di rete un'interfaccia grafica di facile consultazione per visualizzare gli allarmi relativi alle anomalie riscontrate.

Sybilla è in grado di:

- Rilevare la comparsa in rete di **terminali sconosciuti**
- Geolocalizzare e valutare la reputazione di **destinazioni di traffico anomale** per identificare flussi di traffico potenzialmente pericolosi
- Rilevare traffico sospetto, identificando **attacchi di tipo DoS e DDoS**
- Rilevare **attacchi di tipo IP Spoofing**, frequentemente utilizzati in preparazione di offensive informatiche complesse
- Raccogliere i **Fingerprint dei terminali** connessi in rete per monitorare variazioni sospette
- Fornire uno **storico del traffico** analizzato e degli eventi rilevati



Per ricevere subito maggiori informazioni sulla piattaforma Sybilla:

chiamaci al numero **(055) 538-2350**
 invia una mail a info@florence-consulting.it

Florence Consulting Group
 Consulenza IT Enterprise & Digital Transformation

www.florence-consulting.it

