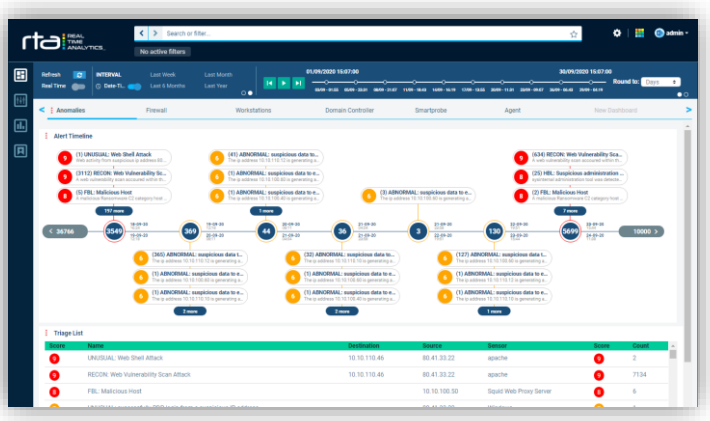
Potenzia Il Tuo Rilevamento Delle Minacce

Real Time Analytics (RTA) è una soluzione di sicurezza informatica che consente agli analisti di rilevare le anomalie in materia di sicurezza informatica e di creare le condizioni per reagire rapidamente.

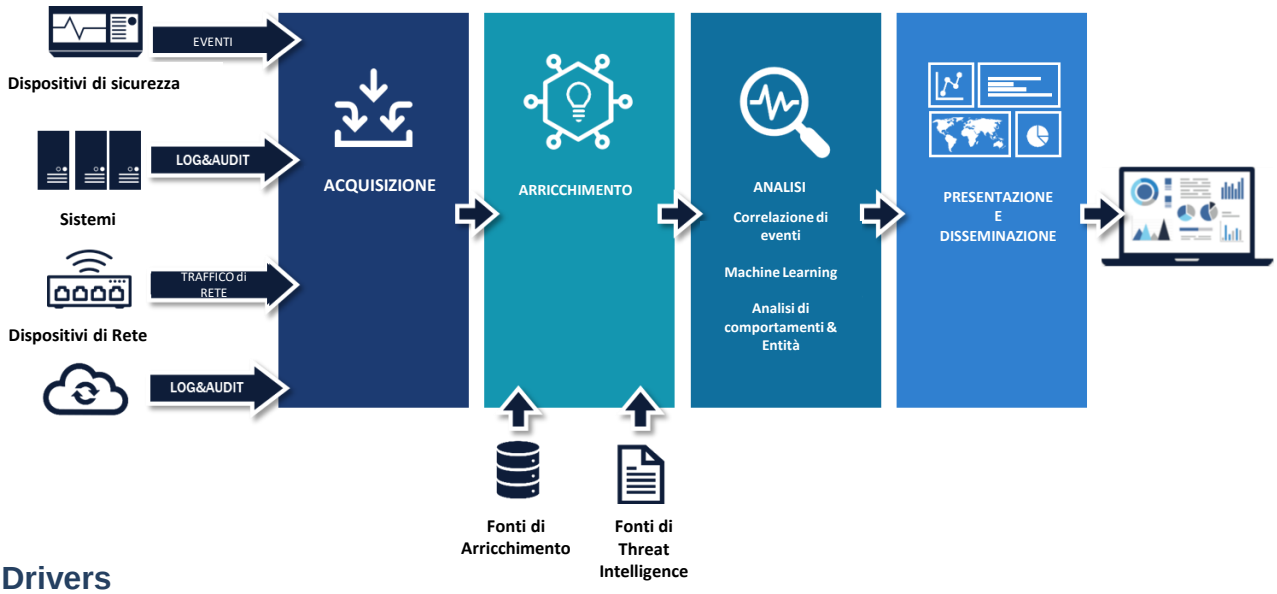
Oggigiorno le minacce cyber evolvono sempre più rapidamente, infatti ogni anno nuovi modelli di attacco vengono sperimentati all'interno di infrastrutture eterogenee, basate su componenti intelligenti e in grado di scambiarsi dati, comandi e informazioni, utilizzando una catena di relazioni di fiducia che può essere infranta o attaccata.

Un ambiente sicuro deve tenere in considerazione le combinazioni e i limiti descritti in precedenza, utilizzando un approccio adattivo orientato a potenziare il livello di sicurezza informatica globale.

Essendo in grado di raccogliere milioni di dati al minuto, RTA può essere considerata come una piattaforma modulare atta a coordinare e gestire normalizzazioni, trasformazioni, analisi e indicizzazione di milioni di dati, sfruttando paradigmi tipici delle architetture As-A-Service utilizzate in ambienti Cloud.



Raccogli, Arricchisci, Analizza, Dissemina

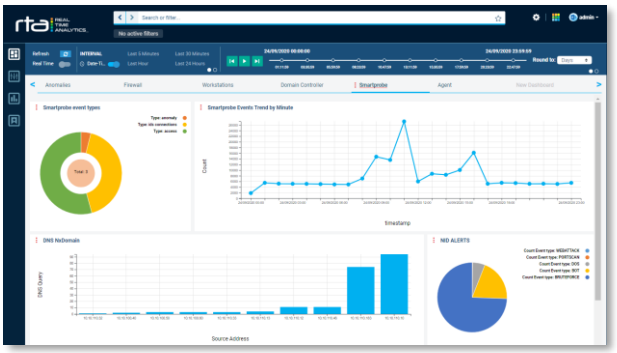


Value Drivers

- RTA raccoglie e normalizza ingenti quantità di eventi da un gran numero di sensori IT, comprese fonti proprietarie, dispositivi OT e servizi Cloud, o direttamente dalle apparecchiature di rete o dal traffico grezzo
- RTA arricchisce i dati in tempo reale: un maggiore arricchimento significa ottenere eventi più contestualizzati; ed «eventi più contestualizzati» è sinonimo di un'analisi migliore
- RTA adotta un mix di regole, basi statistiche e approcci di apprendimento automatico (*Machine Learning)* che si sviluppano utilizzando un'infrastruttura ben distribuita e completa nelle sue funzionalità
- RTA può essere definita come una "macchina del tempo" che consente all'analista di raccogliere tutte le informazioni necessarie al fine di "congelare la scena del crimine" in situazioni in continua evoluzione, e di rivedere un determinato evento in uno specifico arco di tempo utilizzando funzionalità ad hoc.
- RTA mostra i dati per esseri umani, offrendo un'esperienza di esplorazione in tempo reale all'interno di un unico punto di vista.

CY4GATE S.p.A.
Via Morolo, 92 - 00131 Rome - ITALY
www.cy4gate.com

Funzionalità della piattaforma RTA



Visualizzazione dei Big Data

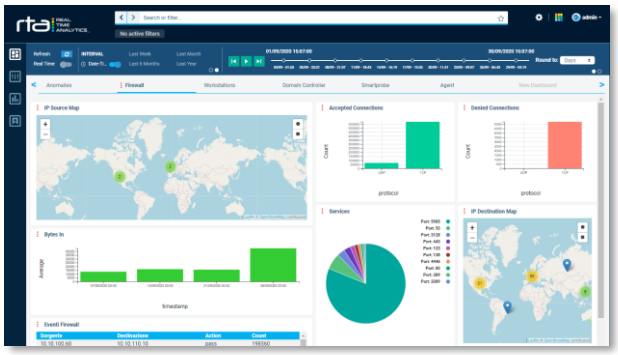
Dashboard e widget possono essere personalizzati in base alle esigenze dei clienti e sono *time-based*: ovvero, si aggiornano automaticamente in base all'intervallo di tempo stabilito.

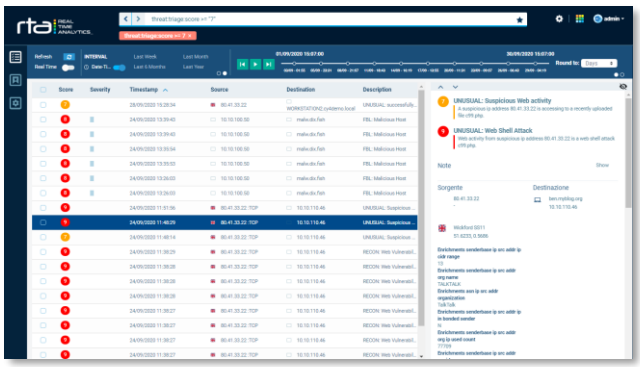
Le dashboard includono: a) Tag cloud; b) mappature termiche o mappe di sintesi; c) Tabelle; d) Indicatori di riepilogo; e) Grafici; f) Diagrammi, linee o aree; g) Istogrammi verticali e/o orizzontali.

Approccio all'Analisi in stile «Macchina del tempo»

RTA consente di navigare tra i dati avanti e indietro nel tempo.

La piattaforma presenta una linea temporale interattiva (l'arco temporale viene definito dall'Analista) che può essere azionata tramite i pulsanti "play" e "stop": ciò permetterà di analizzare un determinato evento accaduto in un determinato arco di tempo.





Drill Down degli Eventi

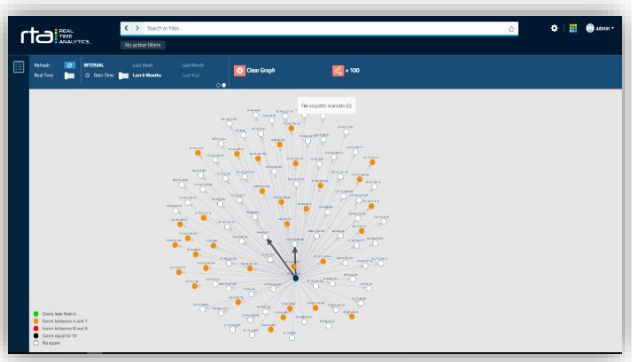
RTA consente di effettuare una ricerca tra i dati selezionando un intervallo di tempo specifico e utilizzando un linguaggio di *query* intelligente.

Il processo di *Drill Down* consente di analizzare i dettagli di un evento specifico e di eseguire una rapida valutazione su triage, arricchimento, analisi delle minacce e feed di Threat intelligence grazie a degli indicatori e a dei filtri specifici.

Grafo delle Relazioni

RTA consente di navigare tra i dati e di comprendere quali siano le relazioni tra entità diverse.

Il Grafo (costruito su campi come indirizzi IP e su nomi di dominio relativi a uno specifico intervallo di tempo) mostra le co-occorrenze delle entità selezionate (i «nodi») all'interno di tutti gli eventi in un intervallo di tempo prestabilito.



Reti di Controllo Industriale Estese (SCADA)

RTA consente il monitoraggio e la protezione della sicurezza informatica delle reti ICS e SCADA.

Con l'aumentare della sofisticazione degli attacchi informatici, comprendere quale sia il modo migliore per difendere i sistemi d'infrastruttura critici – produzione di energia, acqua, gas e altri sistemi vitali – diventa un impegno sempre più importante e atto doveroso.

CY4GATE S.p.A.
Via Morolo, 92 - 00131 Rome - ITALY
www.cy4gate.com

Dispositivi Supportati da RTA

Di seguito, si elencano le tecnologie già integrate nella piattaforma RTA. Esse si possono eventualmente integrare con ulteriori fonti tramite l'utilizzo dell'architettura aperta del componente «Jconnector», il quale supporta i modelli sysol, file, SQL, REST API, nonché altri modelli di trasporto, per raccogliere eventi, analizzarli e normalizzarli ai fini dell'analisi.

Servizi Cloud

- Akamai
- Azure Windows OMS e Log Analytics
- CloudFlare
- Imperva Incapsula

Sicurezza delle Reti

- Bro Network Monitor / IDS
- Checkpoint con Log Exporter
- Cisco ASA
- Cisco Email Security Appliance (ESA)
- Cisco ISE
- Cisco PIX
- Cisco SourceFire / Snort
- Cisco Stealthwatch
- Cisco ThreatGrid
- Citrix Netscaler Web App Firewall
- FireEye EX, NX
- Forcepoint Web Security Suite
- Fortinet Fortigate/FortiAnalyzer
- IBM Guardium
- Imperva Securesphere
- McAfee ATD
- McAfee Network Security Manager
- McAfee Email and Web Security Appliance
- ModSecurity
- pfSense
- Palo Alto Networks
- Squid
- Suricata

Sicurezza Endpoint

- FireEye HX
- McAfee VirusScan Enterprise
- McAfee EPO
- Trendmicro
- Wazuh

OS

- Linux
- Microsoft Windows Server (2012/2016/2019)
- Microsoft Windows (7 / 8 / 10)
- Red Hat Linux
- Snare for Microsoft Windows
- Unix

Web/Application Server

- Apache Tomcat
- Apache WebServer
- IBM WebSphere Application Server
- Microsoft IIS
- Microsoft Active Directory
- Microsoft Exchange/Tracking log
- Microsoft Network Policy Server
- Oracle Weblogic

Dispositivi di Rete

- Cisco Catalyst OS
- Cisco IOS
- Cisco NX-OS
- Cisco WLC
- CiscoWorks
- HP Switch

Sistemi di Database

- Microsoft SQL Server
- Oracle Audit

SIEM:

- IBM QRadar
- Microfocus ArcSight

Virtualizzazione:

- VMWare ESXi

Opzioni di installazione

I nodi del cluster RTA per l'elaborazione e l'indicizzazione dei dati possono essere installati su istanze **fisiche** o **virtuali** a 64 bit basate su CentOS Linux vers. 7.6.810 (Core), o RHEL vers. 7.6.810 (Core) a 64 bit o Oracle Linux Release 7.6.810 (Core).

RTA supporta le seguenti piattaforme di virtualizzazione:

- VMware ESX/ESXi 6.x and 5.x
- CentOS Linux 7, RHEL 7, Oracle Linux 7 con KVM Virtualization

RTA è stato certificato per funzionare al meglio su:

- CentOS Linux vers. 7.6.810 (Core),
  RHEL vers. 7.6.810 (Core),
  Oracle Linux vers. 7.6.810 (Core) con KVM
- VMWare ESIXi 6.5.0
- Azure IaaS

CY4GATE S.p.A.
Via Morolo, 92 - 00131 Rome - ITALY
www.cy4gate.com