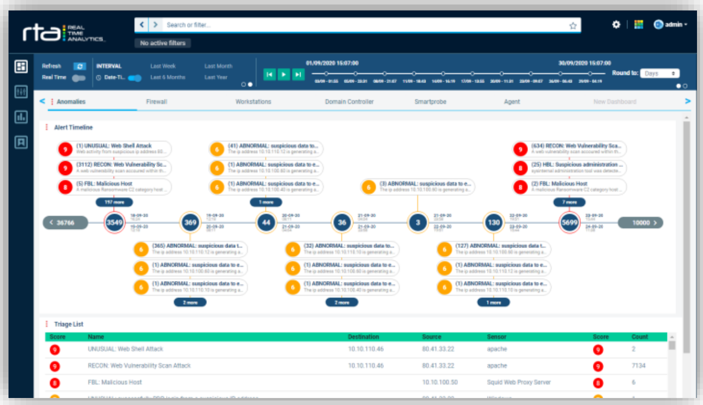
Supercharge Your Threat Detection

Real Time Analytics (RTA) is a cyber security solution that enables analysts to detect cyber security anomalies and creates the conditions to rapidly strike back.

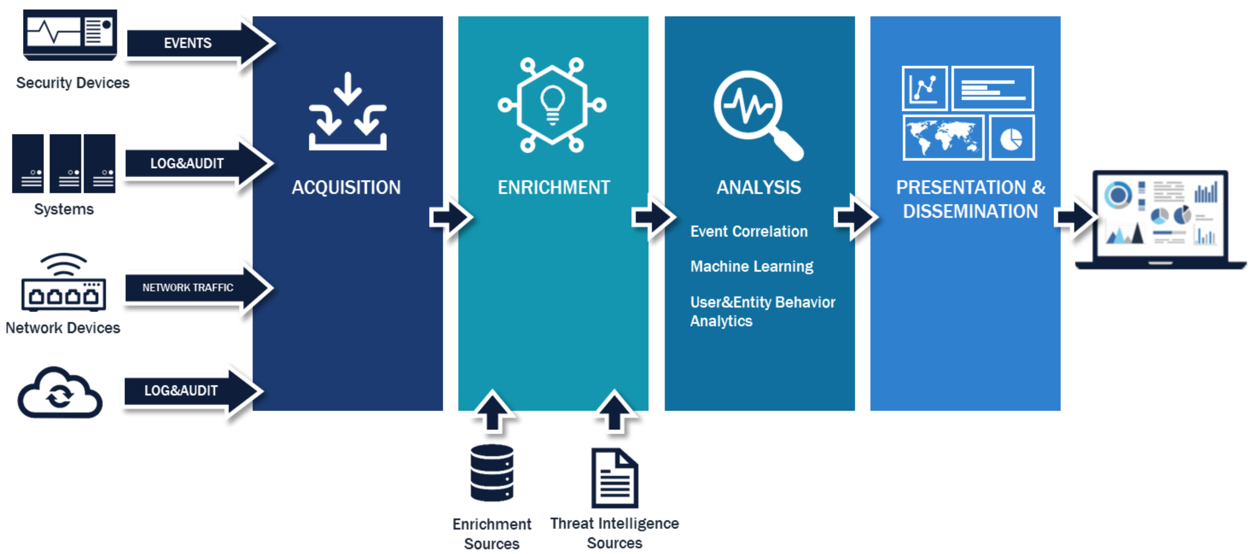
Threats evolve even more rapidly, new attack patterns appear each year inside an heterogeneous infrastructure based on multiple intelligent components which exchange data, commands and deductions using a chain of trust that can be attacked or abused.

This means that a secure environment must take in care the combinations and limits described before, using an adaptive approach oriented to empower the overall cyber security level.

Able to collect millions of data per minutes, RTA can be considered as a modular platform able to coordinate and manage normalizations, transformations, analysis and indexing of millions of data, exploiting typical paradigms of As-A-Service architectures, used in cloud environments.



Collect, Enrich, Analyze, Disseminate

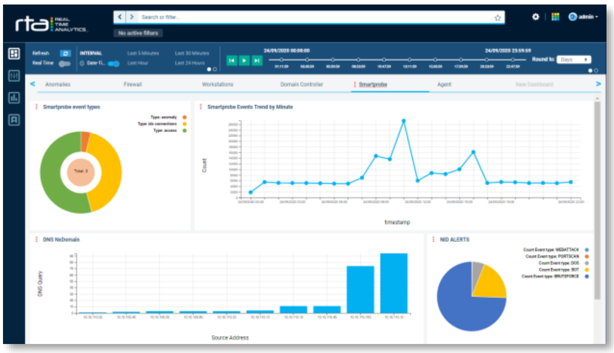


Value Drivers

- RTA can collect and normalize huge amount of events from a large number of IT sensors, including proprietary sources, OT devices and cloud services, or directly from the network equipment or from the raw traffic
- RTA enriches data in real-time: More enrichment means more contextualized events, more contextualized events means better insight
- RTA adopts a mixing of rules, statistical baselining and machine learning approaches which scales up using a full distributed infrastructure
- RTA can be defined as a “Time Machine” which allows the analyst to gather back the information in order to “freeze the crime scene” within evolving situations and review it using a “time machine” approach
- RTA shows data for humans, giving a real-time exploration experience inside a single point-of-view

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

RTA Platform Features



Big Data Visualization

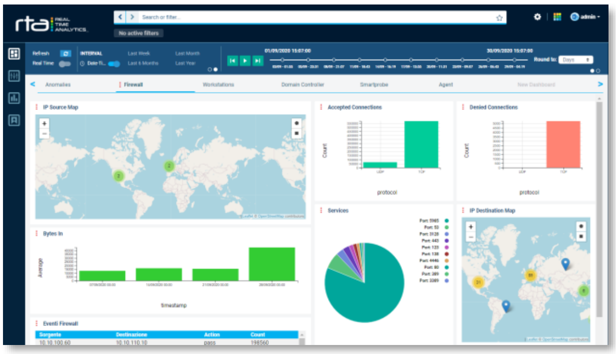
Dashboards and widgets can be customized according to customers' needs, and are all time-based: updates itself according to time range defined.

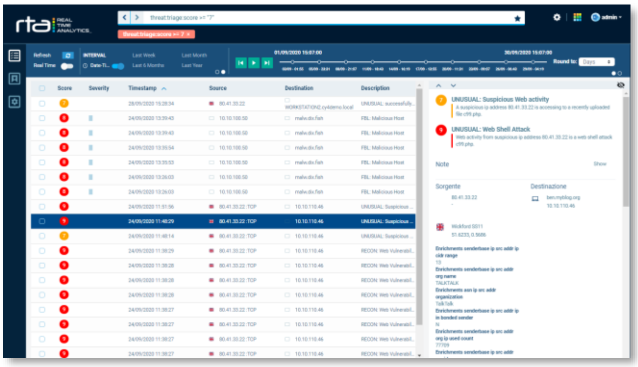
Dashboards include a) Tag cloud, b) Heat Map or Summary map, c) Tables, d) Summary Indicators, e) Pies, f) Diagrams Lines or Areas, g) Vertical/Horizontal Histograms.

Time Machine Analysis Approach

RTA allows to navigate through data backward and forward within the time.

The platform shows an animated time line (where starting and ending points can be easily set by the Analyst) with "*play*" and "*stop*" buttons that can be used to understand what was happening at a specific moment.





Event Drill Down

RTA allows to search among data selecting a specific time range and using a smart query language.

The Drill Down process allows to analyze details of a specific event and perform a quick evaluation regarding triage, enrichment, threat analysis and threat intelligence feeds thanks to indicators and filters.

Relationship Graph

RTA allows to navigate through data and understand relations between different entities.

The graph (built on fields such as IP addresses, domain names related to a specific time range) and shows the co-occurrences of selected entities (the nodes) within all the events, in a selected time range.

Extended Industrial Control Networks (SCADA)

RTA allows advanced ICS and SCADA networks cyber security monitoring and protection.

As the sophistication of cyber-attacks increases, understanding how to defend critical infrastructure systems - energy production, water, gas, and other vital systems - becomes more important, and heavily mandated.

RTA Supported Devices

Below the list of the technologies already integrated with the RTA platform. Other sources can be easily integrated using the open architecture of the JConnector component, which supports sysol, file, SQL, REST API, and other transport models to collect events and parse and normalize them for further analysis.

Cloud Services

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

Network Security

- Bro Network Monitor / IDS
- Checkpoint with 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

Endpoint Security:

- 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

Network Devices

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

Database Systems

- Microsoft SQL Server
- Oracle Audit

SIEM

- IBM QRadar
- Microfocus ArcSight

Virtualization

- VMWare ESXi

Installation Options

RTA cluster nodes for processing and indexing data can be installed on **physical** or **virtual** 64bit instances based upon CentOS Linux Release 7.6.810 (Core), or 64bit RHEL Release 7.6.810 (Core), or Oracle Linux Release 7.6.810 (Core).

RTA officially supports the following virtualization platforms:

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

RTA has been certified to run best on:

- CentOS Linux Release 7.6.810 (Core),
RHEL Release 7.6.810 (Core),
Oracle Linux Release 7.6.810 (Core) using KVM
- VMWare ESIXi 6.5.0
- Azure IaaS