ReaQta-Hive

Artificial Intelligence Threat Response

Targeted and campaign-based cyberattacks are using advanced or purpose built malwares, specific for the organization being targeted and therefore capable of bypassing traditional protection solutions. This approach is increasingly being adopted by organized crime and high-profile attacks, therefore a new strategy is necessary to identify, hunt and block these malicious applications that are created on a daily basis.

ReaQta-Hive is the first Artificial Intelligence Threat Response solution that protects organizations from known and future threats by adopting an entirely new approach, based on Artificial Intelligence and big data analytics, to secure the endpoints from a constantly evolving cyberthreat landscape.

Book your live demo at **reaqta.com/demo**

Solution

ReaQta-Hive adopts a powerful and proven technology, ReaQta's NanoOS, to collect behavioral data from the endpoints with an unprecedented level of detail, without impact on the device's performances and taking full advantage of the hardware isolation protection offered by modern CPUs.

The Artificial Intelligence engine is deployed both on the endpoints and analysis server. This means that your devices are capable of future-proof protection even when disconnected from the infrastructure.

Behavioral data collected from the endpoints is analyzed in real-time, looking for signs of intrusions, new attack patterns and malicious activities. State-of-the-art Artificial Intelligence is used to detect new and potentially dangerous behaviors that can be immediately blocked or reported according to the organization's choice.

When malicious or suspicious activity is detected, an incident is automatically generated and the triage phase can be carried out with ease in a matter of seconds: the A.I. is capable of filtering out the noise while organizing and synthesizing a vast amount of information to make it increadibly easy to understand, without requiring a highly skilled team.

ReaQta-Hive can be configured to automatically respond to incidents by protecting the endpoints or isolating them to contain the threat and to prevent lateral-movement. Alternatively, the malicious activity can be monitored and tracked to better understand the impact of the threat. Endpoints can be queried in real-time to retrieve security related data, offering in-depth visibility within the organization and centralized hunting capabilities.

Features

- Full visibility on workstations and servers
- On-demand and real-time queries to the endpoints
- Triage security incidents in seconds
- Strong protection against advanced malware and ransomware
- Clear and easy to use dashboard
- Centralized control of every device, local or remote

Benefits

Discover low-and-slow threats: tracking an attack back in time as far as needed is easy, allowing an in-depth analysis of activities that might have been initially overlooked.

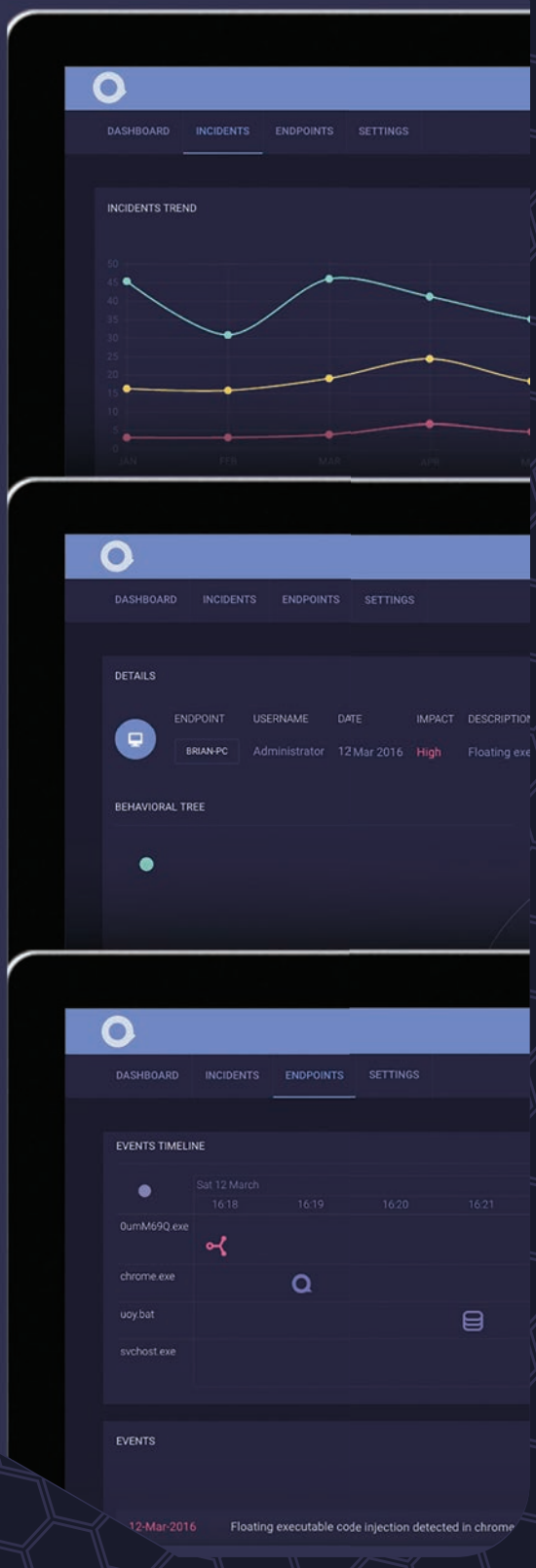
Protect and monitor: threatened endpoints can be automatically isolated for deeper analysis, or the protection modules can be activated to prevent lateral movements without any human intervention.

Real-time visibility: endpoints can be queried in real-time in order to look for the presence of specific indicators of interest, allowing a proactive approach to mitigate threats.

Time Travel: makes it easy to take an endpoint back in time to automatically restore those resources that have been affected after an incident, like a ransomware attack.

Streamlined Workflow

Triage your incidents in just 15 seconds!



REAQTA

ReaQta-Hive

ReaQta LTD
+356 77489802 / info@reaqta.com

WWW.REAQTA.COM