REAQTA

Securing your Success with ReaQta's Hive As A Service (HaaS)

One Single Dashboard for all your Triaging with a Multi-Tenanted Cloud Platform

Hive As A Service (HaaS)

One Single Dashboard for all your Triaging

1 Instant Detection

- **Endpoints Visibility**
  24/7 endpoints visibility with immediate alerts to suspicious and malicious behaviours
- **Response Support**
  Regular review calls with recommendation for next-steps
- **Behavioural Policies**
  Use of advanced AI for customized whitelisting and blacklisting of suspicious behaviours
- **Dashboard Access**
  End users have separate access to Hive dashboard

2 Proactive Threat Hunting

- **Posture Check**
  Provides immediate assessment with potential RAT behaviours and top scripting engines
- **Proactive Hunt**
  On an ongoing basis, hunting queries from threat intelligence data and research will be generated in the environment to search for emerging threats
- **Extended Hunt**
  Extensive threat hunting perimeters at your disposal to hunt for suspicious applications for possible dormant or infected assets
- **Custom Detection**
  Users may build their own customized detection strategies

3 In-depth Analysis

- **Infrastructure Analysis**
  Gathering and analysis of additional artifacts from infrastructure for in-depth analysis
- **Malware Analysis**
  In-depth dive into malicious executables to understand attack modes, origins and their relationship to similar tools used elsewhere
- **Threat Analysis**
  Further analysis to understand how discovered malicious activities might affect your organization

4 Remediation Control

- **Incident Remediation**
  With a single click, orchestrated actions and options to quarantine assets or kill off processes, APT, dropped files
- **Remote Remediation**
  Upon detection of breach, a secure connection can be made to infected hosts to pull or push files, kill processes, perform memory dumps and quick remediation from anywhere in the world
- **Security Remediation**
  In special cases, automated isolation of endpoint is enabled for further investigation of attack chains to gain insight into the attacker's behaviour and close security gaps

Key Services with HaaS

MSP ELEMENTS	TRIGGERED BY	SERVICE LEVEL AGREEMENT
Incident Monitoring	MSP Analysts	✓
Access to Console	MSP Analysts and End Users	✓
Proactive Threat Hunting	MSP Analysts	✓
On-Demand Threat Hunting Request	End Users	✓
Quarantine Endpoint Request	MSP Analysts	✓
Creating Blacklist / Whitelist	End Users	✓
Threat Reporting*	MSP Analysts	✓
Method of Reporting	MSP Analysts	✓
Incident Review Call	MSP Analysts	✓

**Threat Reporting consists of Information about the threat; MSP analysts assessment; Actions performed to contain or terminate the threat; Any post incident actions required of the End User*
Other types of service response are also available, depending on requirements.

ReaQta's Leading Differentiators

1. **Ease of Use**
   - Ease of deployment, updates can be easily grouped
   - User-friendly dashboard with quick overview and in-depth analysis where required
2. **Automated Reports**
   - Regular reports can be generated and scheduled for management reporting
   - Reports provide clear visibility on infrastructure and activities flow captured
3. **Cloud Scanning**
   - Metadata relating to any discovered incident can also be cross checked for file presence in the cloud
   - Alerts enrichment for highly precise detection
4. **Customizable detection strategies**
   - Enables freedom to create (unlimited) new detections – whenever, whatever!

About ReaQta Hive

1. **State-of-the-art technology: WORLD'S FIRST AND ONLY NanoOS**
   The world's first cyber security solution capable of working outside the Operating System (Ring-1) which makes it INVISIBLE to malware. As such, it cannot be shut down and it provides full visibility of behaviours, beyond what is currently available in the market.

2. **First class Integration: Endpoint A.I. + Infrastructural A.I. solution**
   A frontend A.I. engine detects threats aimed at the endpoint like ransomware, remote access trojans (RAT) and malicious software usage. A centralized backend A.I. engine learns the behaviour at the infrastructural level, creating a constantly evolving profile for the detection of lateral movements, supply-chain attacks and dormant threats.

About ReaQta

ReaQta is founded in 2014 by a team with rich experience in government-led cyber intelligence operations and Threat Intelligence. With a deep understanding of the modern cybersecurity landscape, ReaQta is one of the fastest growing solution providers to craft a highly advanced, Artificial Intelligence (AI) powered endpoint threat response platform and solution service that analyses, detects, threat-hunts and remediates cyberattacks. Headquartered in Amsterdam and Singapore, the company is currently represented in 18 countries.

REAQTA

CONTACT INFO

SALES
sales@reaqta.com

TWITTER
@reaqta

WEBSITE
www.reaqta.com

GLOBAL REPRESENTATIVES

AUSTRALIA
DUBAI
FRANCE
HONG KONG
INDIA
ITALY
INDONESIA
JAPAN
MALAYSIA
NETHERLANDS
PHILIPPINES
SINGAPORE
SOUTH KOREA
SPAIN
SWITZERLAND
THAILAND
UNITED KINGDOM
UNITED STATES OF AMERICA
VIETNAM