REAQTA

MITRE ATT&CK EVALUATION REPORT

ReaQta-Hive Demostrates Best-in-Class Capabilities

ABOUT REPORT

ReaQta has successfully completed the MITRE evaluation. This report shows ReaQta-Hive's capabilities of providing complete coverage of sophisticated attacks, with no human intervention and while producing top-quality alerts.

HOW DOES THE MITRE EVALUATION HELP ORGANISATIONS

The evaluation does not score or grade solutions and it is meant to help organisations identify the most suitable solution that meets their specific security challenges. Organisations do need to note that the evaluation takes place in isolated environments and have limitations. There are times when certain features of a solution are disabled, as they do not support that particular lab infrastructure, like in case of ReaQta, the NanoOS, the live hypervisor used to detect high-level malicious behaviours, could not be used. Nonetheless the platform performed well, even without its core component.

APT29 Emulation

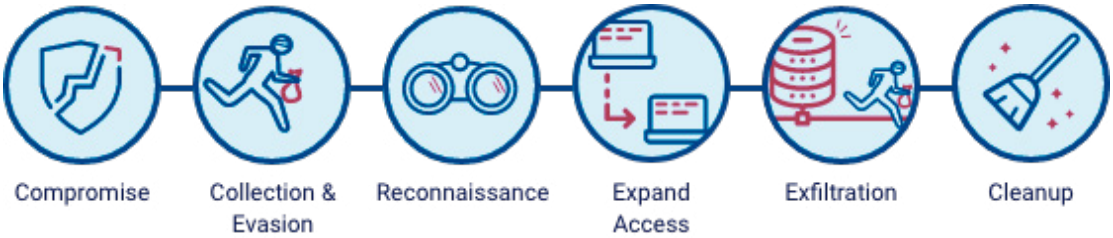
ATT&CK Evaluations 2019

WHAT IS MITRE ATT&CK EVALUATION

MITRE ATT&CK has defined a set of stages during a cyberattack and evaluates solutions on their ability to detect threats in each of these. Each of the listed stages represents a “tactic” along the kill-chain:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

MITRE has a set of identified techniques, each of which belongs to a tactic group, based on the threat actor that they select for the evaluation. MITRE chose APT29 for this round of evaluation.



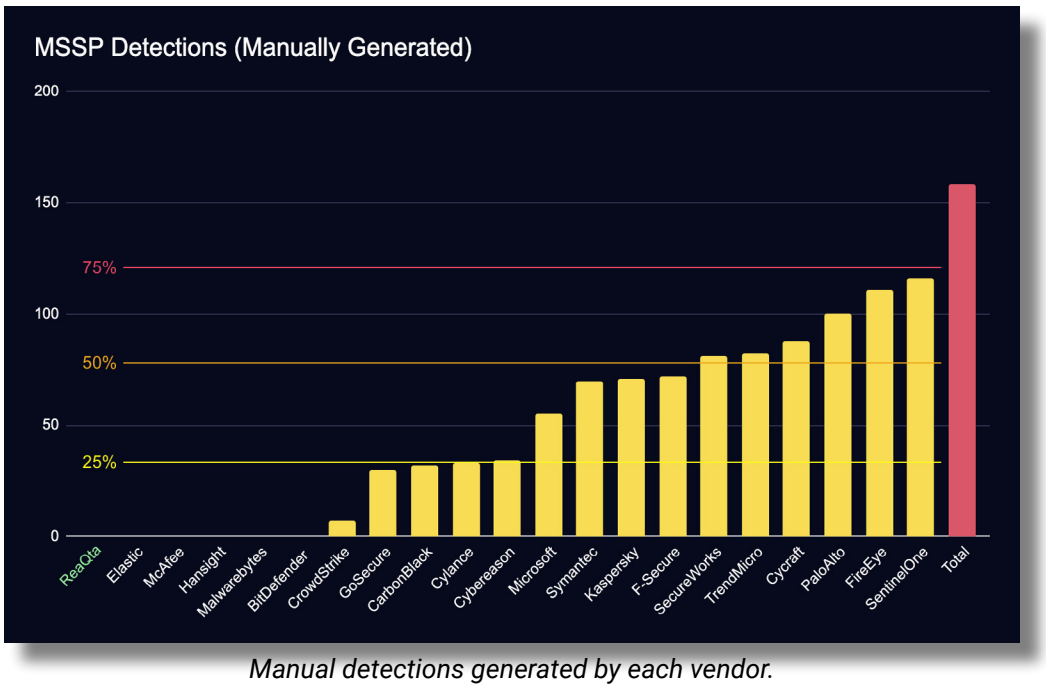
NO MANUAL (MSSP) DETECTIONS

Before starting the evaluation, ReaQta decided to participate without MSSP, that is, without any human interaction during the attack. MITRE is a technology evaluation framework and it may be unfair to introduce humans in the loop. On top of that, the contribution of MSSP detections heavily biases the evaluation. The SOC team knows that an attack is happening and they know exactly where and how.

The MSSP approach wouldn't have provided ReaQta's customers with a fair assessment of the technology. MITRE has been very receptive to feedback and starting from Round 3 all companies will be evaluated without humans in the loop.

MSSPs do add great value and customers should be free to choose between MSSP and stand-alone deployments.

From the graph on the next page, the amount of detections performed by humans had a huge impact on generated detections, in several instances more than 50% of detections – and up to 73% – were created manually. Only 6 companies decided to participate without humans in the loop.

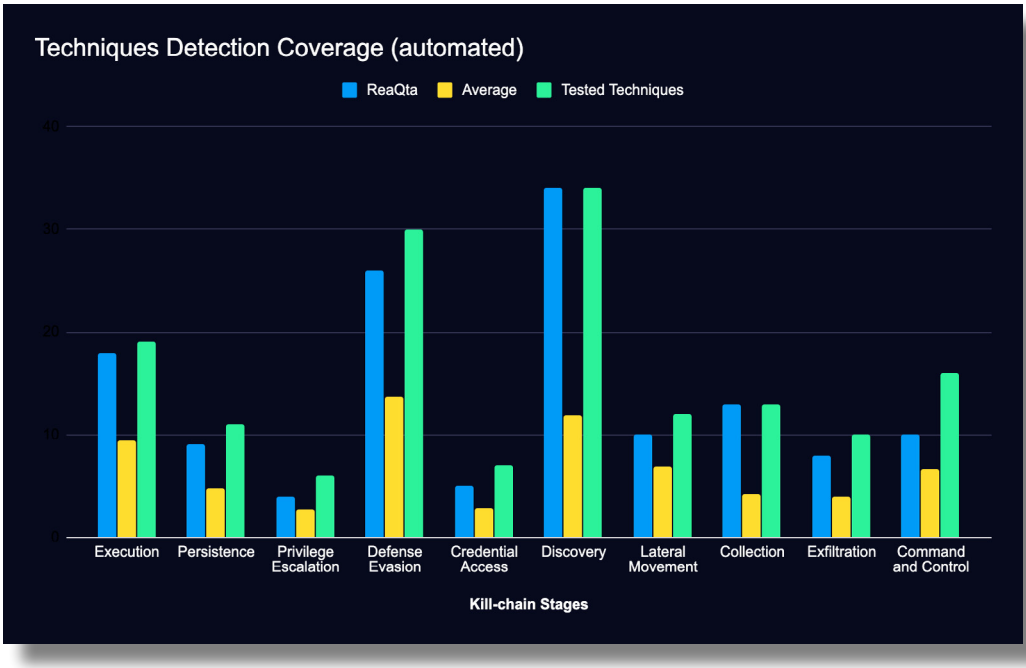


Manual detections generated by each vendor.

MITRE EVALUATION ROUND 2 – APT29

Vendors were tested on their ability to detect the tactics and techniques used by APT29 (also known as The Dukes, Cozy Bear and CozyDuke), a sophisticated nation-state adversary known for their stealthy approach. APT29 is widely-known for being behind notable attacks: the Pentagon in 2015, the Democratic National Committee in 2016, the Norwegian and Dutch governments in 2017.

The change from the previous round was important: APT3 (Round 1) is a noisy threat actor, adopting a variety of tools with much less regard to maintaining a low profile. APT29 on the other hand is extremely stealthy, operating with a very low-profile and leveraging heavily on LOLbins and file-less malware.



ReaQta-Hive automated detection coverage compared to the average

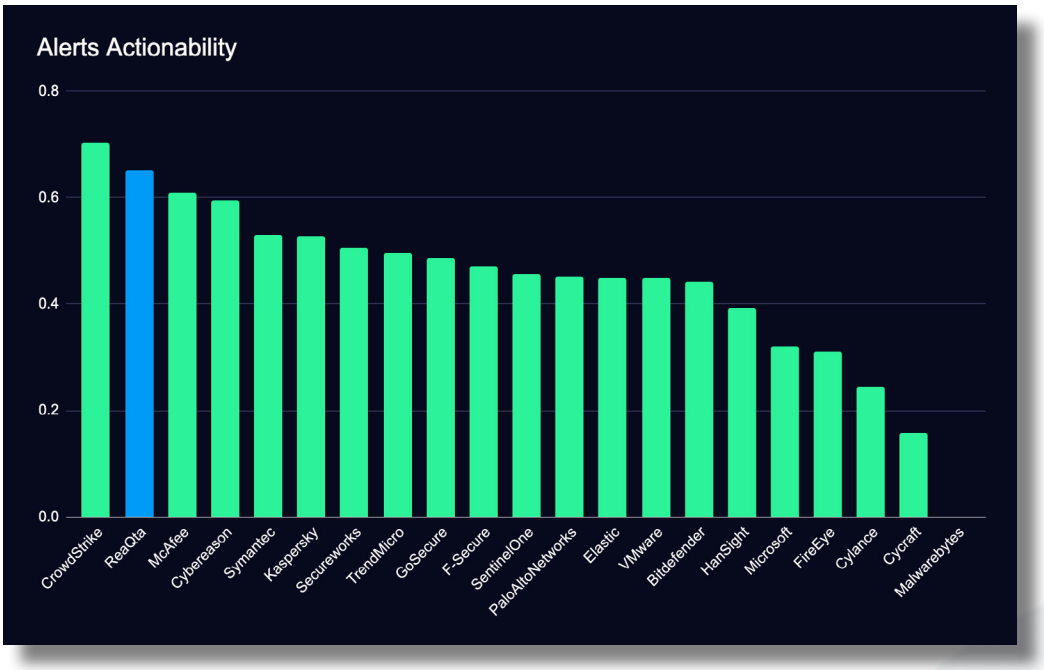
REAQTA EVALUATION RESULTS

The attack unfolded over 2 days in which the attackers gradually moved deeper into the network after obtaining initial access. Vast majority of operations were carried out using powershell, as opposed to custom tools and malware, to maintain a low detection profile. The evaluation goal is to show how tested solutions respond to the attack and what kind of visibility is provided along the entire kill-chain.

VISIBILITY ACROSS THE ATT&CK KILL-CHAIN

As is evident from the summary of the evaluation results above, ReaQta-Hive platform provided complete visibility across the entire kill-chain. ReaQta-Hive detected 90% of the Tactics and Techniques tested, proving its ability to respond and remediate threats at every stage of the attack.

RIGHT ALERTS AT CRITICAL STAGES

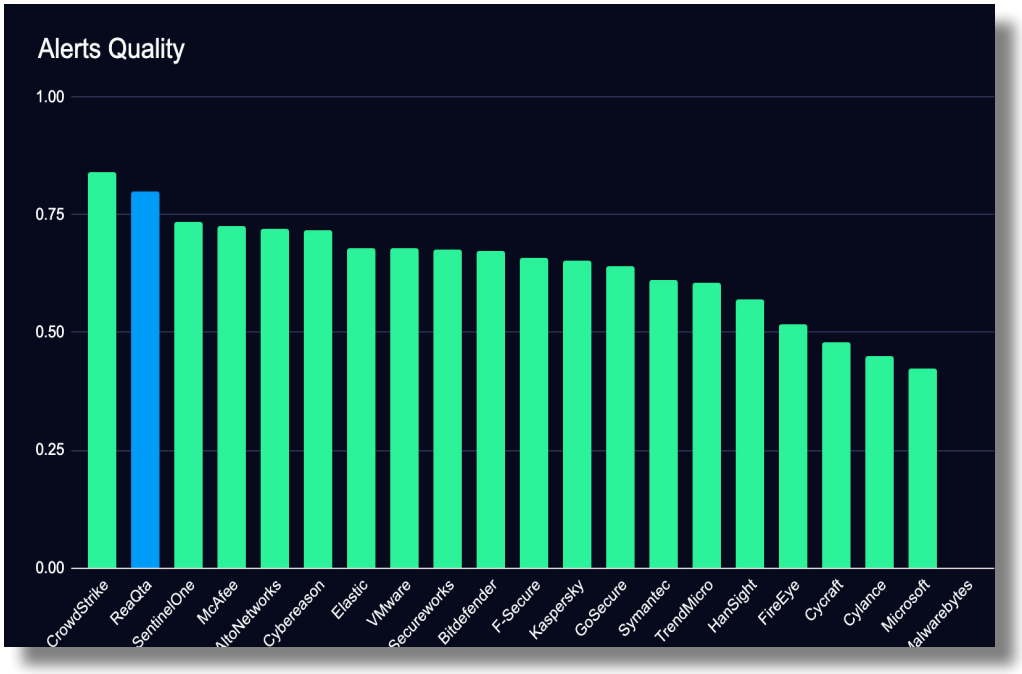


Actionability rates (data includes Manual detections for vendors relying on MSSPs)

The platform detected and generated alerts right from Execution, Persistence, Privilege Escalation and Defense Evasion stages, enabling the security team to track APT29 and their actions. The platform alerts were consistent during the later Kill-chain stages: Lateral Movement, Collection, Exfiltration and Command and Control, showing ReaQta-Hive's ability to respond and limit damages also in the late stages of a cyber attack.

The Actionability rate highlighted the platform's capability to reduce noise by reducing the amount of alerts generated. The platform captured all tactics and techniques in a few correlated alerts, as comapared to one alert per tactic and technique, which would amount to an unmanageable number of alerts for the SOC teams to examine and respond.

REAQTA-HIVE SHOWS ONE OF THE WORLD'S TOP ACTIONABILITY RATES, EVEN WHEN COMPARED AGAINST VENDORS RELYING ON MANUAL (MSSP) DETECTIONS.

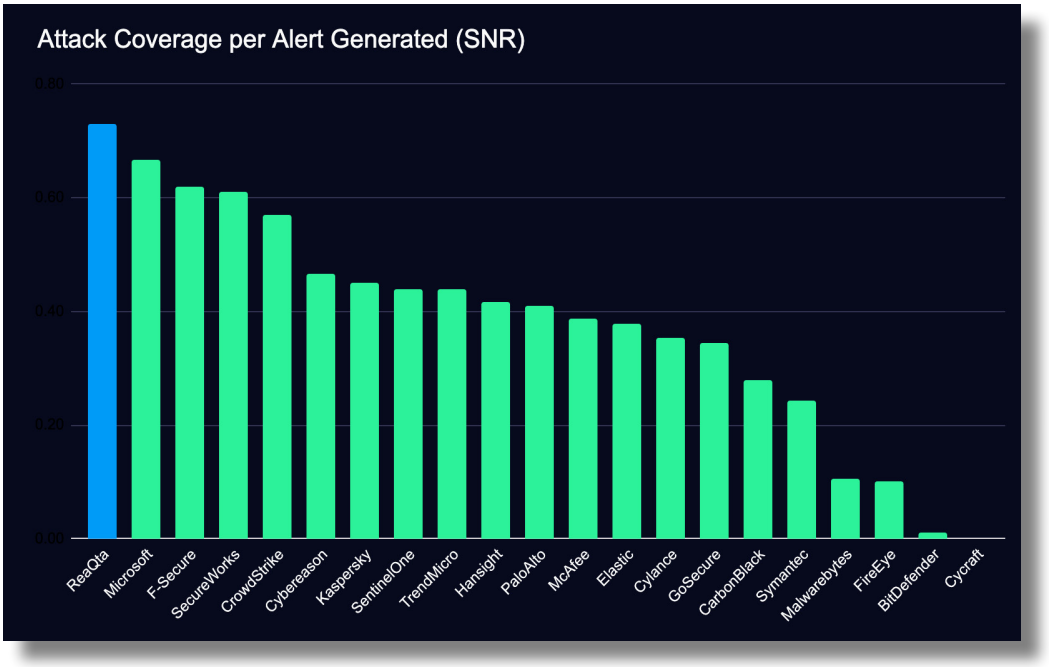


Alerts Quality (data includes Manual detections for vendors relying on MSSPs)

With the amount of visibility provided by ReaQta-Hive it is necessary to filter data, correlate it and generate the smallest amount of alerts possible, each containing the largest amount of related information. This is the purpose of ReaQta's A.I. engines: collect, correlate and summarise the telemetry. Alerts Quality is also confirmed by Forrester's analysis in the chart above.

Once again, ReaQta-Hive provides high-quality alerts without human intervention, while both the first and third vendors relied on manual analysis during the evaluation.

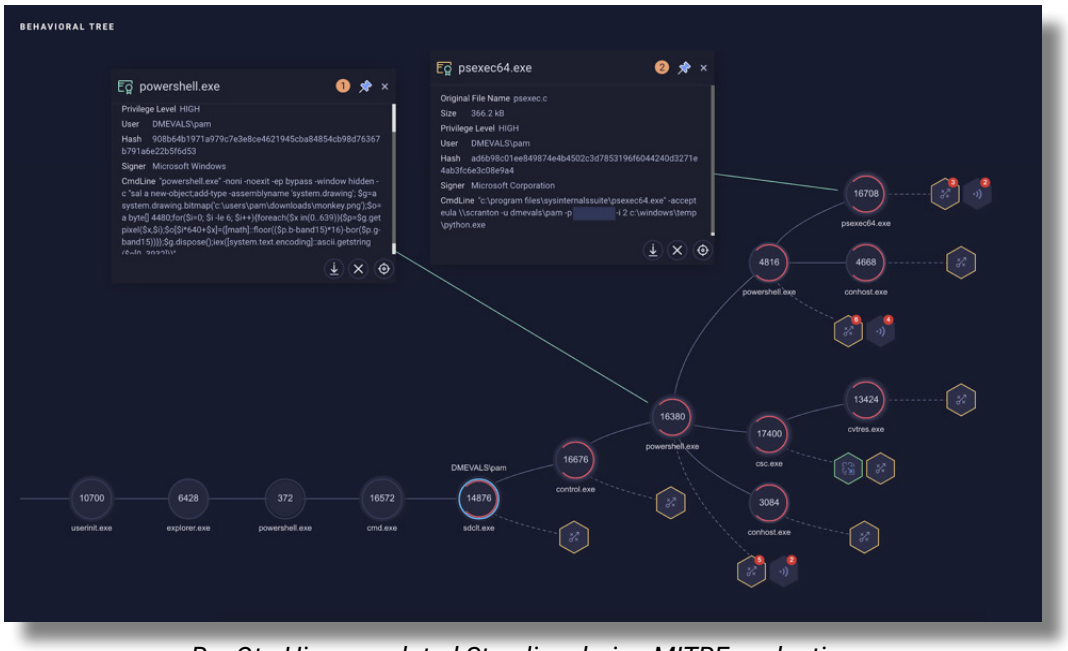
PROVIDING HIGH-FIDELITY AND COMPREHENSIVE ALERTS IS THE CRITERIA THAT SETS A GOOD PLATFORM ASIDE FROM NOISE GENERATORS.



Percentage of attack coverage provided per alert

The graph here shows how ReaQta-Hive behaved compared to other solutions when manual detections are removed. Each bar represents the amount of incident-related information captured under each generated alert. ReaQta's engines have captured the largest amount of information, that translates to a sizeable work-load reduction in real environments.

"ACTIONABILITY IS THE PRODUCT OF ALERT EFFICIENCY AND ALERT QUALITY [...] EFFICIENCY OF ALERTS (NOT TOO MANY) AND THE QUALITY OF THE ALERTS (HOW WELL THEY HELP YOU UNDERSTAND THE STORY) ARE BOTH RELATED AND CRITICAL TO UNDERSTANDING HOW "ACTIONABLE" A PARTICULAR ALERT IS GOING TO BE."
~FORRESTER



ReaQta-Hive correlated Storyline during MITRE evaluation

REAQTA-HIVE CORRELATED STORYLINE DURING MITRE EVALUATION

This allowed analysts to understand and study an active attacker easily, without being distracted by hundreds of alerts being generated with no direct correlation with the original incident. This would have been much harder to handle during a real analysis.

ReaQta-Hive approach reduced the alert fatigue by 85% while preserving complete visibility over the entire attack. ReaQta-Hive is specifically designed to generate the minimal amount of alerts per incident, allowing for a smooth and uninterrupted analysis experience. The ability to maintain everything in a single view helps analysts to respond faster, without requiring jumps to different screen-views, in order to have a complete understanding of the events.

REAQTA-HIVE GENERATED JUST 25 ALERTS AND CORRECTLY GATHERED ALL THE INFORMATION REQUIRED TO TRACK THE ATTACKERS WITHIN EACH ONE OF THEM, INSTEAD OF CREATING 158 ALERTS (ONE PER TECHNIQUE TESTED)

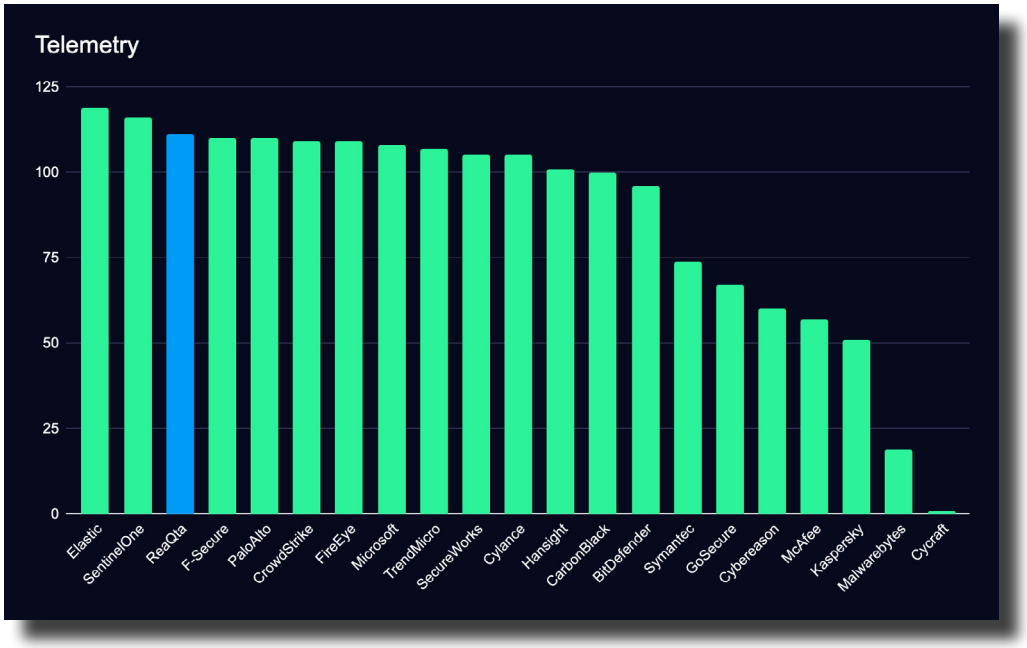
ATT&CK TACTICS AND TECHNIQUES WITH COMPLETE VISIBILITY

The platform was able to maintain correlation between actions at all stages of the ATT&CK kill-chain. Correlating events automatically reduces the time needed to piece together different actions run by the attackers and ultimately it reduces the response time in case of real attacks.

To provide an example related to the evaluation, the graph on the next page shows how an entire stage of the attack has been captured within a single alert. ReaQta-Hive had correlated all the information into an easily comprehensible storyline, thereby providing to a SOC team all the information for timely triage. No human interaction was required and the attack is cleanly explained, and its risk assessed, without requiring any manual activity.

THE ABILITY TO PROVIDE A UNIFIED INCIDENT RESOLUTION WORKFLOW IS CRITICAL TO REDUCE ALERT FATIGUE.

LIST OF DETECTED TACTICS AND TECHNIQUES



Amount of telemetry provided by ReaQta-Hive

Taking a closer look at the detection of APT29 tactics and techniques, ReaQta-Hive provided visibility right from the early stages of the kill-chain to the more sophisticated stages which are often harder to detect. What is noteworthy here is the platform's ability to uniformly detect threats at every stage, thereby providing opportunities for response and remediation at every stage.

REAQTA-HIVE SHOWED ONE OF THE WORLD'S BEST TELEMETRIES.

ReaQta-Hive showed one of the world's best telemetries, combined with an impressive A.I. engine capable of condensing information and assessing risk, it will prove a powerful tool in the hands of any SOC or team that wants to spend time threat hunting instead of managing alerts constantly.

THE WAY AHEAD

ReaQta's AI-powered platform was designed to equip security teams with advanced detection and rapid response capabilities, minimizing human intervention, simplifying the entire cybersecurity process and ensuring business continuity for organisations of all sizes.

This evaluation has validated ReaQta's approach to the detection of sophisticated threat actors. ReaQta will continue to participate in independent third party testing in the future.

ReaQta appreciates and applauds the work of MITRE in helping organisations from making informed decisions with these evaluations.

ABOUT REAQTA

ReaQta was founded by an elite team of offensive and defensive cybersecurity experts and AI/ML researchers. Combining these backgrounds, the team has designed an AI Endpoint Security Platform that leverages on Artificial Intelligence, data mining and a unique NanoOS to protect endpoints from advanced malware attacks and data exfiltration.

This novel approach applies the latest technologies to automate, optimise and simplify the process of detecting and handling new threats. Organisations can now eliminate the most advanced threats in the fastest way possible with an elegant, powerful and easy-to-use platform - entirely without the need for additional skilled personnel.

INFO@REAQTA.COM VISIT REAQTA.COM