MITRE ATT&CK Evaluation

IBM Security ReaQta shows best-in-class capabilities

Highlights

Promote business continuity while freeing your security team from manual analysis of cyberthreats

Reduce alert fatigue and simplify your cybersecurity by generating the minimum number of necessary threat alerts

Gain complete visibility over your endpoints to enable rapid response at every stage

About the report

ReaQta, an IBM Company, has successfully completed the MITRE ATT&CK Evaluation. This report[1] shows that ReaQta provides complete coverage of sophisticated attacks with virtually no human intervention while producing top-quality alerts.

What is a MITRE ATT&CK Evaluation?

MITRE ATT&CK defines a set of stages during a cyberattack and evaluates solutions on their ability to detect threats. 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

REAQTA
an IBM Company

IBM

How the MITRE evaluation helps organizations

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

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

Compromise

Collection and evasion

Reconnaissance

Expand access

Exfiltration

Cleanup

Promote business continuity while freeing your security team from manual analysis of cyberthreats

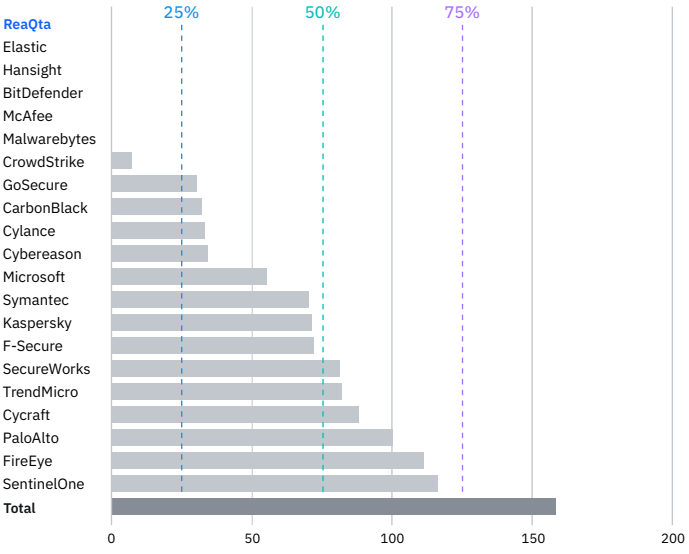
Before starting the evaluation, ReaQta decided to participate without a managed security service provider (MSSP), that is, without any human interaction during the attack. MITRE is a technology evaluation framework, and it seemed disingenuous to introduce humans into the loop. On top of that, the contribution of MSSP detections heavily biases the evaluation. The security operations center (SOC) team knows that an attack is happening and exactly where and how.

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

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

As shown in the graph below, the number 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.

MSSP detections (manually generated)



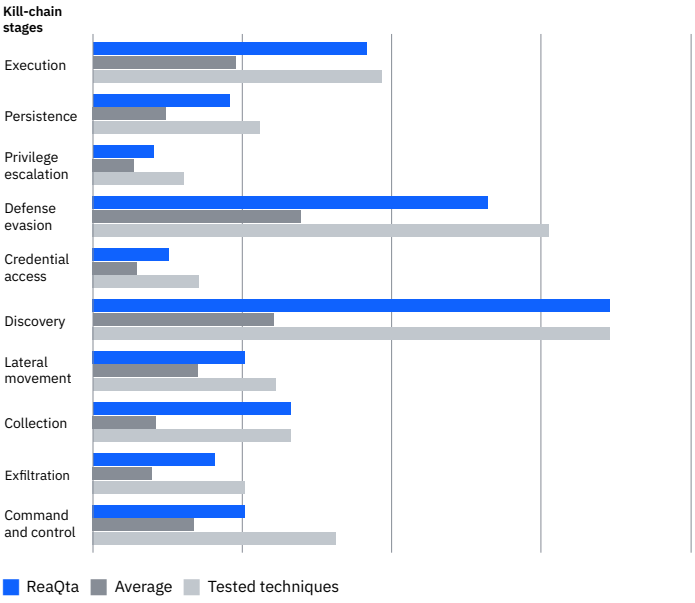
Manual detections generated by each vendor

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 its stealthy approach. APT29 is widely known for being behind notable attacks: the Pentagon in 2015, the Democratic National Committee in 2016, and the Norwegian and Dutch governments in 2017.

The change from the previous round was important: APT3 (Round 1) is a noisy threat actor, adopting various 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 relying heavily on LOLBins and fileless malware.

Techniques detection coverage (automated)



ReaQta automated detection coverage compared to the average

ReaQta evaluation results

The attack unfolded over two days in which the attackers gradually moved deeper into the network after obtaining initial access. The vast majority of operations were carried out using Microsoft 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.

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

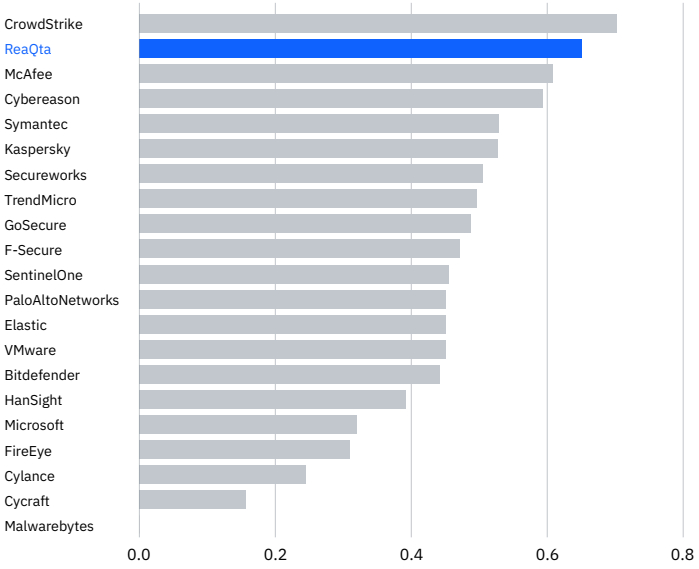
ReaQta shows one of the world's top actionability rates, even when compared against vendors relying on manual detections by MSSPs.

Reduce alert fatigue and simplify your cybersecurity by generating the minimum number of necessary threat alerts

The platform detected and generated alerts right from the execution, persistence, privilege escalation, and defense evasion stages, enabling the security team to track APT29 and its actions. The platform alerts were consistent during the later kill-chain stages: lateral movement, collection, exfiltration, and command and control, showing ReaQta's ability to respond to and limit damages also in the late stages of a cyberattack.

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

Alerts actionability

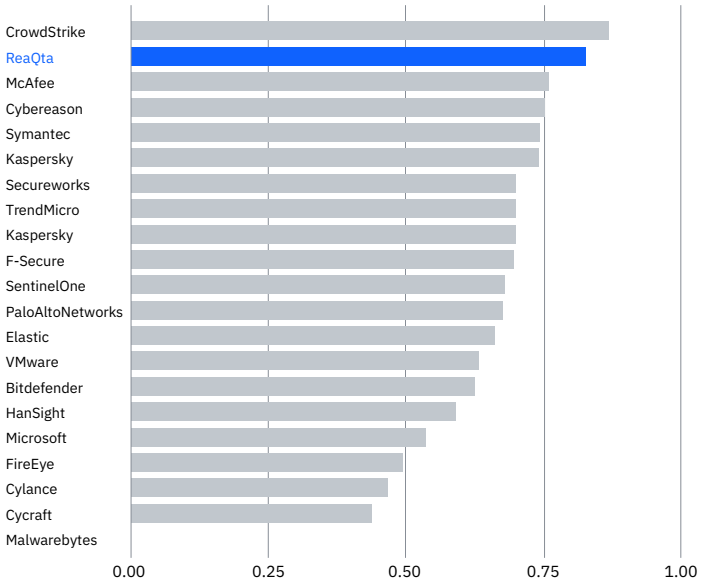


Actionability rates (data includes manual detections for vendors relying on MSSPs)

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

The amount of visibility provided by ReaQta makes it necessary to filter data, correlate it and generate the smallest number of alerts possible, each containing the largest amount of related information. This is the purpose of ReaQta's AI engines: collect, correlate and summarize the telemetry. Alerts quality is also confirmed by Forrester's analysis in the chart below.

Alerts quality



Alerts quality (data includes manual detections for vendors relying on MSSPs)

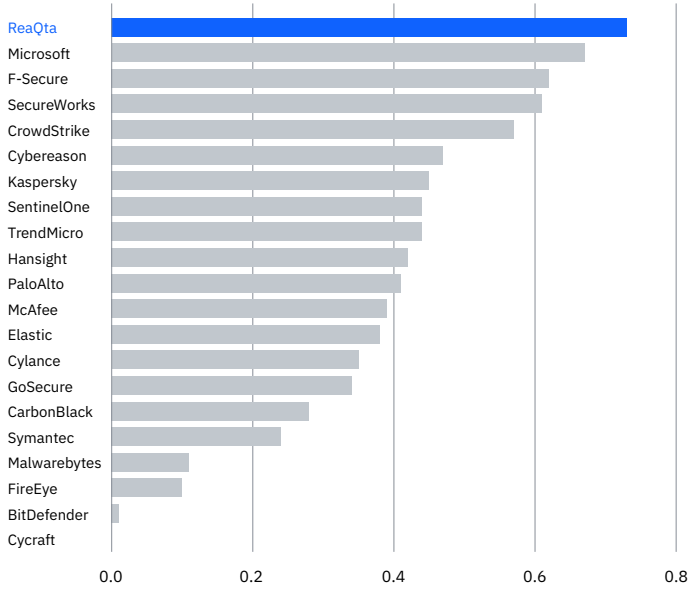
“Actionability is the product of alert efficiency and alert quality [...] efficiency of alerts (not too many) and the quality of the alerts (how well they help you understand the story) are both related and critical to understanding how ‘actionable’ a particular alert is going to be.”

Forrester [2]

Providing high-fidelity, comprehensive alerts is the criterion that distinguishes a good platform from mere noise generators.

The graph below shows how ReaQta behaved compared to other solutions when manual detections were removed. Each bar represents the amount of incident-related information captured under each generated alert. ReaQta’s engines captured the largest amount of information, which translates to a sizable workload reduction in real environments.

Attack coverage per alert generated (signal-to-noise ratio)



Percentage of attack coverage provided per alert

ReaQta 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.

The ability to provide a unified incident resolution workflow is critical to reduce alert fatigue.

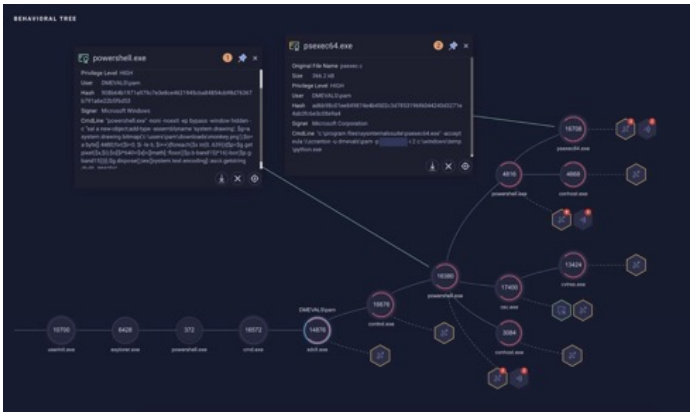
ReaQta correlated the storyline during the MITRE evaluation. This allowed analysts to understand and study an active attacker easily, without the distraction of hundreds of alerts being generated with no direct correlation with the original incident. This would have been much harder to handle during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

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

Gain complete visibility over your endpoints to enable rapid response at every stage

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

Behavioral tree



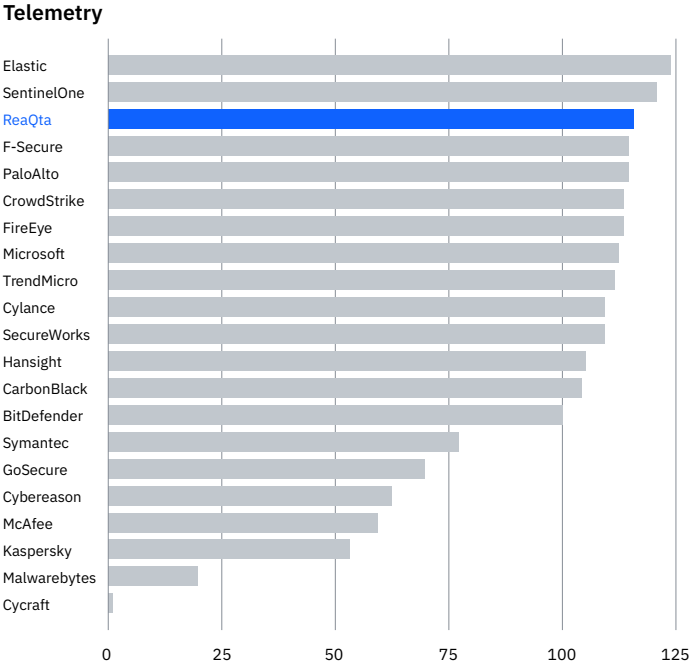
ReaQta correlated storyline during MITRE evaluation

To provide an example related to the evaluation, the graph above shows how an entire stage of the attack was captured within a single alert. ReaQta 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 was clearly explained, and its risk assessed, without requiring any manual activity.

Taking a closer look at the detection of APT29 tactics and techniques, ReaQta 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 showed one of the best telemetries, combined with an impressive AI 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 constantly managing alerts.

ReaQta showed one of the best telemetries.



Amount of telemetry provided by ReaQta

Conclusion

ReaQta's AI-powered platform equips security teams with advanced detection and rapid response capabilities, minimizing human intervention, simplifying the entire cybersecurity process and promoting business continuity for organizations of all sizes.

This evaluation 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 organizations make informed decisions with these evaluations.

For more information, visit:
ibm.com/products/reaqta

IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
March 2022

1 MITRE ATT&CK evaluation, The MITRE Corporation and MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, Forrester blog, 4 May 2020.