MITRE ATT&CK Evaluation – Wizard Spider & Sandworm

IBM Security QRadar EDR, formerly known as ReaQta demonstrates best-in-class capabilities for three years in a row

Highlights

100% detection coverage across the cyber kill chain.

No configuration changes during the evaluation.

100% of detections done in real-time and without delays.

About the report

IBM Security QRadar EDR successfully completed the MITRE ATT&CK Evaluation. This report shows that QRadar EDR provides complete coverage of sophisticated cyberattacks with virtually no human intervention while producing top-quality alerts.

What is MITRE ATT&CK Evaluation?

MITRE introduced the ATT&CK framework in 2015 as a knowledge base of adversary tactics and techniques and it has since become the de facto standard framework for cyber security professionals looking to make their organizations more cyber resilient.

In 2019, MITRE started with the ATT&CK Evaluations to help vendors assess their capabilities against adversary behaviors.

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

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.

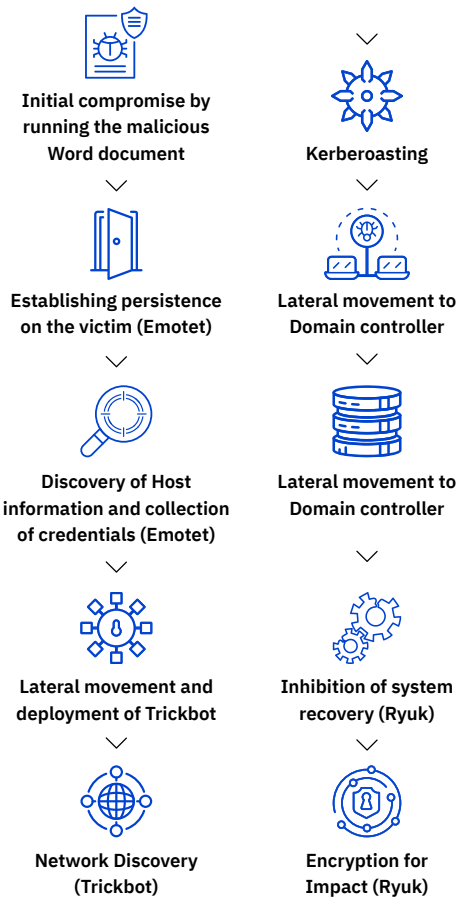
MITRE Evaluation – Wizard Spider and Sandworm

This year's MITRE Evaluation covered two infamous threat groups that have wreaked havoc for many organizations worldwide.

Financially Motivated - focus on extortion through ransomware attacks

The first threat group in the evaluation, Wizard Spider, is a financially motivated Russian speaking criminal group and focuses primarily on extortion through ransomware attacks.

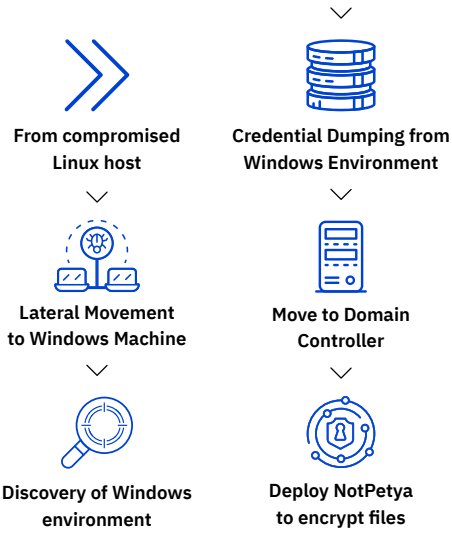
This group has operated the Trickbot botnet (banking Trojan) since 2016, infecting over 1 million computing devices. They are also the group behind Conti (ransomware) and started ransomware campaigns in 2018 targeting larger organizations like hospitals and big corporations. According to the FBI, Wizard Spider extorted USD$61 Million for ransomware attacks within a year alone.



State-Sponsored - focus on data destruction and operational disruption

Sandworm is the second threat group in this year's evaluation. Sandworm Team is state-sponsored and focuses on destruction of data and operational disruption.

The Russian hacking group has been active since 2009 and operated the NotPetya malware in 2017 in a worldwide attack with the purpose of destroying data. This attack caused many casualties such as Maersk shipping, TNT Express and Merck pharmaceutical. The latter claimed USD$1.3 billion in losses due to interrupted operations. Other infamous attacks attributed to Sandworm include the attacks against Ukrainian electrical companies (2016) and the French presidential campaign (2017). In 2018, the Sandworm Team attacked the Winter Olympic Games in South Korea.



QRadar EDR's Configurations and Approach

Similar to previous years, the NanoOS, our live hypervisor used to detect high-level malicious behavior could not be used due to restrictions in the testing environment and QRadar EDR participated with out-of-the-box configurations.

In previous editions, we participated with a Linux agent for detections, but this year we opted out of Linux evaluation as results would not represent our upcoming new generation Linux agent.

- NanoOS: Disabled (due to restrictions in the testing environment)
- Quarantine: Disabled
- Anti-Malware: Disabled
- Protection Policies: Disabled
- Anti-Ransomware: Detection Only
- Telemetry level: Standard
- Detection Strategies (DeStra): Enabled
- Opted out for Linux evaluation as results would not represent our upcoming next-gen Linux agent
- No human intervention

ATT&CK Evaluation Matrix - Tactics and Techniques used

For the tested techniques in the Wizard Spider & Sandworm scenarios, QRadar EDR captured the key important critical events across the tested MITRE ATT&CK cyber kill chain from the Execution stage to Exfiltration and Impact stage.

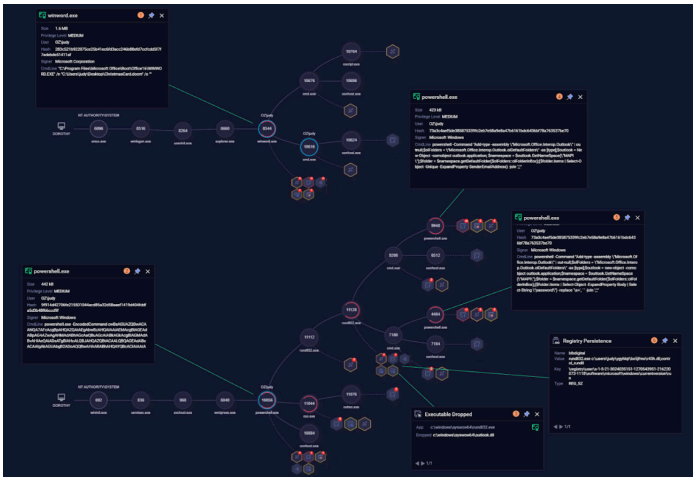
Green highlights techniques that have been detected by QRadar EDR, whereas Grey highlights the areas of information that we do not collect By-Design, which are low-fidelity events tested in the evaluation.

This demonstrates full visibility across the cyber kill chain, and exemplifies QRadar EDR's threat methodology of providing only useful information that is essential for the analyst to make a difference in investigation and response outcomes.

QRadar EDR's Evaluation Results

We take a closer look at the details of QRadar EDR's participation in the evaluation, with additional insights about what it means for clients.

100% detection coverage across the cyber kill chain



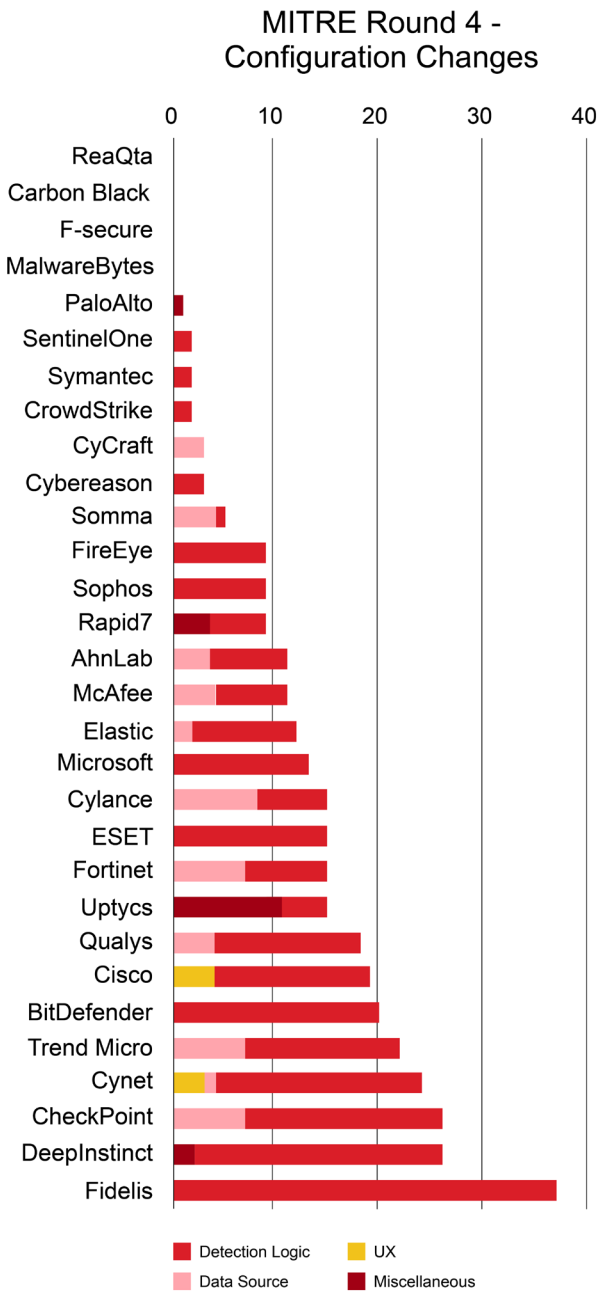
In both Wizard Spider & Sandworm scenarios, QRadar EDR autonomously reconstructed the attack activity across the cyber kill chain into a few condensed high-fidelity alerts with meaningful and actionable steps to the analyst. QRadar EDR detected the most critical events needed for investigation and analysis as well as the key MITRE ATT&CK evaluation objective, Encryption for Data Impact, keeping customers secure.

Why is this important?

Customers prefer less alerts that are highly consolidated as compared to multiple and less informative ones. Our approach reduces manual workload and provides a clear picture of unfolding events, with no need to chase attackers over thousands of different security events.

When malicious or suspicious activity is detected, QRadar EDR switches from smart-logging into deep monitoring mode, capturing all events pertaining to the incident presenting the information in a single consolidated alert. This provides a clear picture of unfolding events, with no need to piece together multiple triggers across thousands of different security events, saving the analyst precious time in triaging and incident response.

No configuration changes during the entire evaluation



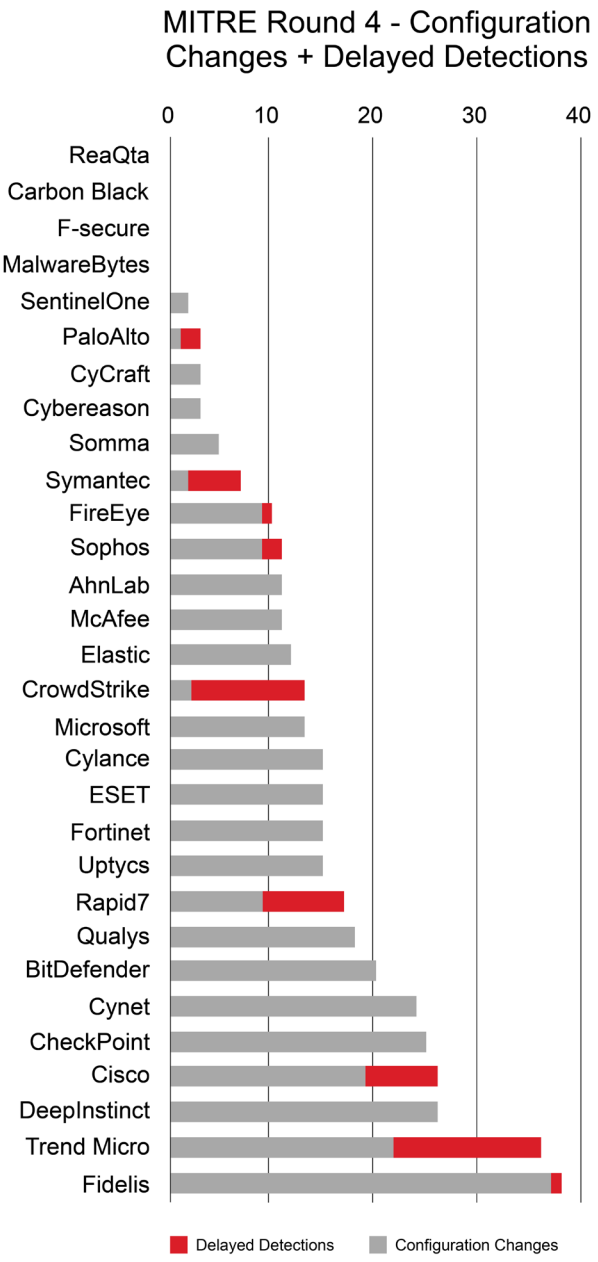
The MITRE results evaluate the number of configuration changes. Configuration changes are essentially modifications to the product after the first evaluation. This means that the product was tweaked in order to improve the detection results. This year, configuration changes were placed in 4 main categories: Detection Logic, Data Source, UX and Miscellaneous.

Throughout the evaluation, QRadar EDR did all the detections without any configuration changes. Configuration changes help vendors adjust their detections as the attack progresses. Most vendors had to tweak their product 'antennas' multiple times before being able to detect meaningful techniques.

Why is this important?

In real-life scenarios, configuration changes are usually unrealistic and implies high operational overheads which was not taken into consideration as part of the evaluation, but has a significant impact to organizations using the solution. The more configurations a solution requires, the more an organization has to invest in its operation and maintenance. Attackers do not give defenders a second chance to tweak their detections before moving to the next step.

100% of detections done in real-time without delays



The MITRE results also evaluate the number of delayed detections (shown in red, see chart: Configuration Changes + Delayed Detections). Delayed detections are detections generated with delay and that are not available to the analyst (e.g., require sandbox evaluation). This may be critical (or not) depending on the threat being detected with delay.

Using QRadar EDR's behavioral analysis engines, all detections were entirely in real-time. Each technique of the attack was tracked as-it-happened, minimizing the risk of losing important events instead of waiting for external components to run their analyses.

Why is this important?

As attackers innovate, automation allows attackers to move extremely quickly within networks. Operations that used to take minutes or hours now take seconds. The ability to have immediate identification & automated response can result in the difference between a threat stopped in its tracks or an organization compromised and having to perform cleanup and recovery operations.

Reflecting on the 2022 Wizard Spider & Sandworm ATT&CK Evaluations

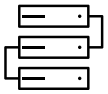
For the third consecutive time, QRadar EDR successfully participated in the MITRE Engenuity ATT&CK Evaluations, showcasing its ability to provide clients with world-class protection against complex and advanced threats.

Scoring the maximum points in the MITRE test requires participants to monitor a high volume of events, but realistically, this might prove to be unnecessary and result in more false positives, causing greater alert fatigue. As a result, analysts miss out on identifying meaningful information efficiently. Such increased data collection also leads to higher storage costs and creates more delays in threat response.

Conversely, QRadar EDR's philosophy is to capture and present only what is necessary so that analysts can do their work in the most efficient way possible. Without inundating analysts with a myriad of alerts, QRadar EDR succeeded in delivering a minimum amount of condensed, high-fidelity alerts that provided full visibility and actionability on all critical attack stages.

Real-Time 360° Visibility for fast Threat Mitigation

QRadar EDR achieved 100% detection coverage across the cyber kill chain cutting through the noise and delivering only the condensed high-fidelity alerts that really matter, in real-time, giving analysts 360° visibility to mitigate threats fast and saving analysts time. This lowers the costs of managing a large blue team and reduces the overall Mean Time to Detect and Respond, thereby mitigating the actual risks of a cyber breach.



QRadar EDR collects What Matters When it Matters

By-design, QRadar EDR does not collect low-fidelity events which are evaluated as part of missed techniques and does not rely on API hooking, but instead only collects useful information that is essential for the analyst to make a difference in the investigation and response outcome. Collecting more doesn't equate to being better, it means analysts now have more noise (false positives) to sieve through before getting to the meat of the investigation.

100% Out-Of-The-Box Experience without Configuration Changes

QRadar EDR was one of the very few vendors that participated with an out-of the box experience, without needing to make any configuration changes in order to detect the attack. In real-life you get one shot, there is no second chance.

Conclusion

Besides the Triton Evaluation in 2021 which focused on ICS vendors, this is the third MITRE Evaluation for IT: APT29 (2020), Carbanak + FIn7 (2021), Wizard Spider & Sandworm (2022). It is also the third time that IBM Security QRadar EDR has successfully participated in the evaluations.

With the completion of MITRE ATT&CK Round 4, IBM Security QRadar EDR remains sure of its mission to simplify the entire cybersecurity process by equipping security teams with advanced detection and rapid response capabilities – while minimizing human intervention – so that analysts can do their most efficient work.

This, in turn, translates to a reduction in operational costs and lowered overall Mean Time to Respond (MTTR), thus mitigating cyber risks for organizations.

IBM Security QRadar EDR is committed to the MITRE Engenuity ATT&CK Evaluations that helps governments and organizations to combat cyber attacks through proven defense practices. We look forward to participating in the next round in 2023 which will focus on the Turla threat group.

To learn more, contact your IBM Business Partner:

Sac-it

mas@sac-it.dk

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
June 2023

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.