IBM Security QRadar EDR takes on Turla in 2023

MITRE Engenuity ATT&CK Evaluations

QRadar EDR demonstrates best-in-class capabilities four years in a row

2023

About the report

IBM Security QRadar EDR successfully completed the MITRE Engenuity ATT&CK Evaluations for the fourth time. This report shows how QRadar EDR tested its out-of-the-box, real-time capabilities without modifying detection strategies during the testing process. QRadar EDR autonomously detected all critical events without configuration changes or delays.

What are the MITRE Engenuity ATT&CK Evaluations?

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 cybersecurity professionals.

Security vendors turn to the ATT&CK Evaluations to improve their offerings and to provide defenders with insights into their product's capabilities and performance. Evaluations enable defenders to make better informed decisions on how to leverage the products that secure their networks. The program follows a rigorous, transparent methodology using a collaborative, threat-informed, purple-teaming approach that brings together providers and MITRE experts to evaluate solutions within the context of ATT&CK.

The ATT&CK Evaluations are not competitive analyses; They show what the detections observed and do not provide a "winner." MITRE Engenuity does not score or grade solutions, but the Evaluations are meant to help organizations identify the most suitable solution that meets their specific security challenges.

Turla

For this year's Evaluations, MITRE focused on adversary behavior informed by Turla, a known Russia-based threat group. Turla has been active since at least the early 2000s and has infected victims in 50+ countries. The group is known to target government agencies, diplomatic missions, military groups, as well as research and media organizations.

Turla adopts novel and sophisticated techniques to maintain operational security, including the use of a distinctive command-and-control network in concert with their repertoire of using open source and in-house tools. They are known for their targeted intrusions and innovative stealth.

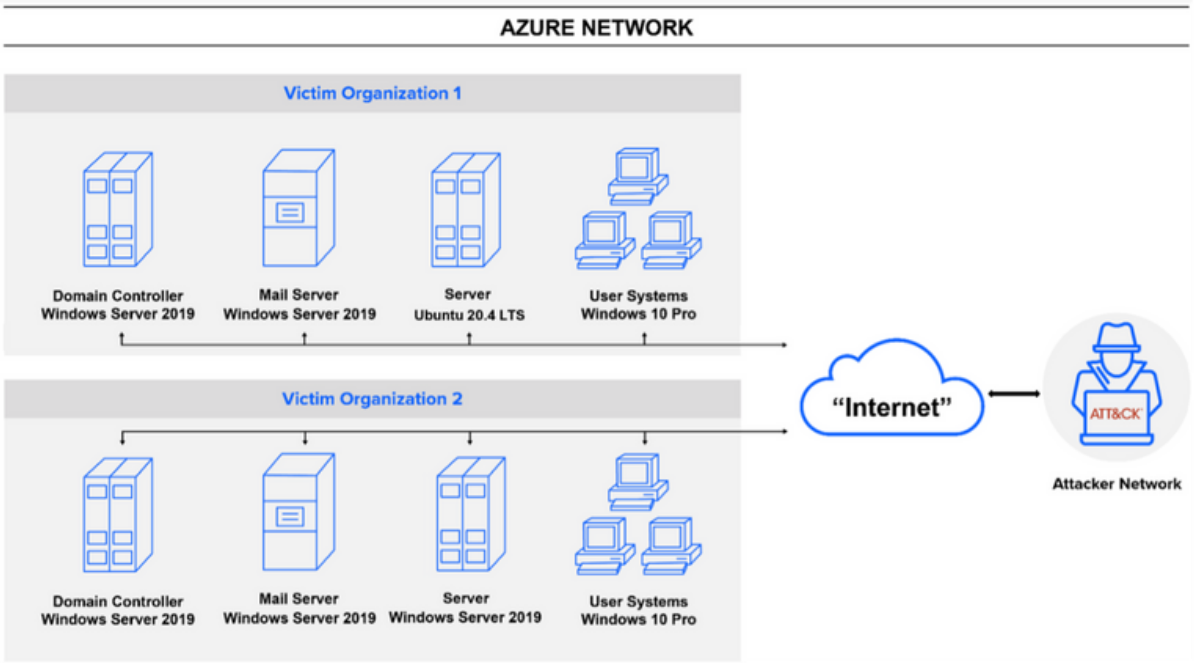
After establishing a foothold and conducting victim enumeration, Turla persists with a minimal footprint through in-memory or kernel implants. Turla executes highly targeted campaigns aimed at exfiltrating sensitive information from Linux and Windows infrastructure.

QRadar EDR Configurations

Vendors are allowed to participate in the Evaluations based on their security stack and strategy. As part of IBM Security's commitment to evaluate behavioral technology out-of-the-box, we intentionally disabled the anti-malware (EPP) module and Hive Cloud (Cloud AV), nor did we incorporate other add-on components.

The strategy is to evaluate behavioral detections and response is a more future-proof way of threat prevention, rather than the reliance on static or signature-based analysis. As with previous years, we were not able to participate in the evaluation with the NanoOS, our endpoint agent that sits outside the operating system, due to testing environment restrictions.

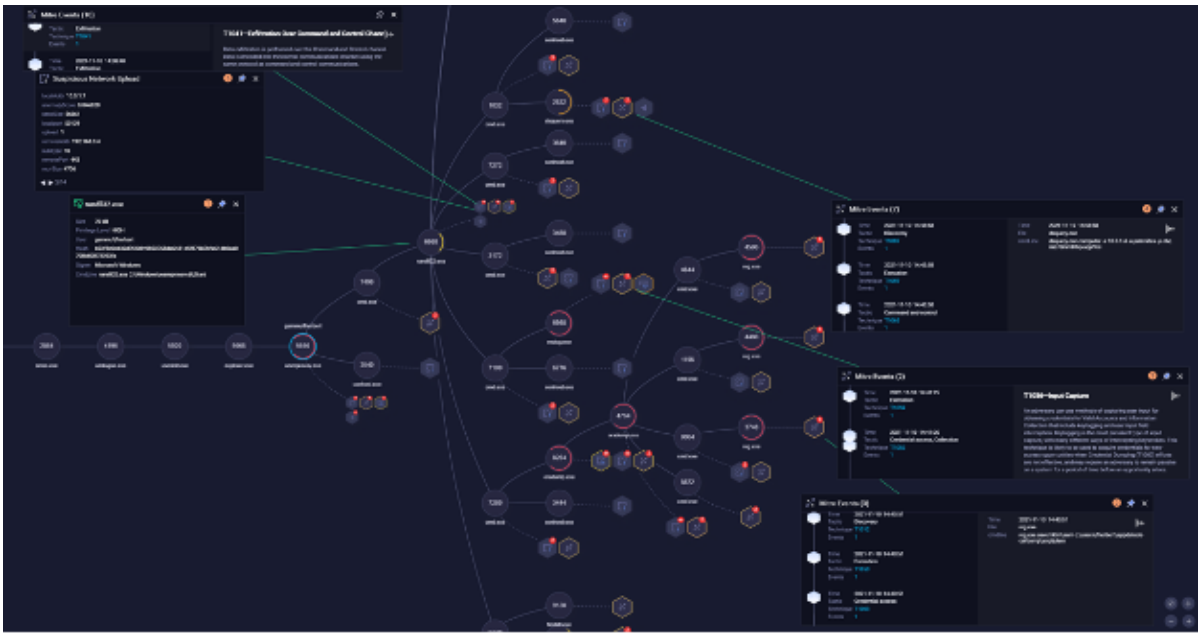
Operating Systems Tested	Evaluation	Product Configuration
• Windows Server 2019 • Windows 10 Professional • Linux Ubuntu 20.04 LTS	• Detection • Protection	• NanoOS – Disabled (due to testing environment) • Anti-malware (EPP) – Disabled • Hive Cloud (Cloud AV) – Disabled



Autonomous detection across all critical events

In this year's evaluation, QRadar EDR achieved 100% visibility across all evaluated stages of the MITRE ATT&CK framework, focusing on what matters most. QRadar EDR autonomously reported and defined critical activity, and provided high-fidelity alerts with meaningful and actionable information. While the testing methodology included an expanded set of detections across the MITRE ATT&CK framework, it’s important to remember that not all ATT&CK techniques carry the same importance.

By design, QRadar EDR does not collect low-fidelity events which are evaluated as part of these missed techniques. While other EDR solutions may rely on API hooking, which is visible and easy to circumvent by attackers, QRadar EDR relies on other data sources at different OS layers for our detections. This allows us to only collect useful information that is essential for the analyst to make a difference in investigation and response outcome.

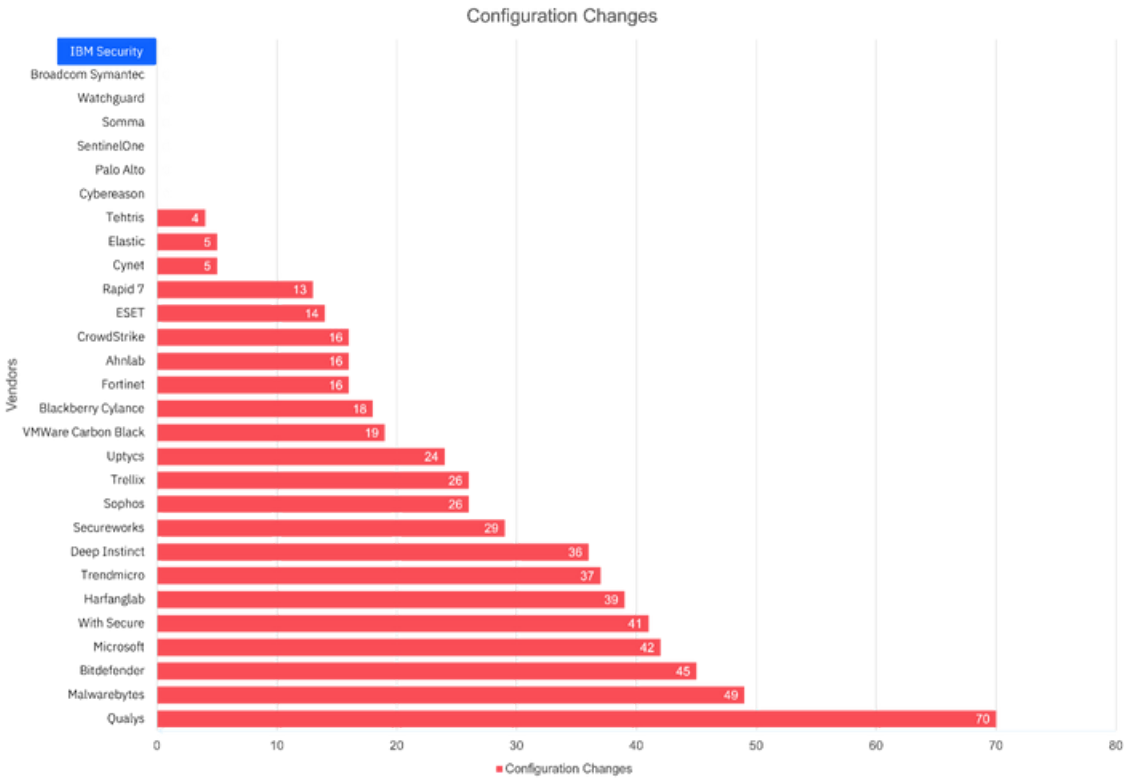


Bottom line – QRadar EDR catches what matters. Collecting more doesn't equate to being better. It simply means analysts have more noise (false positives) to investigate. More data also means increased storage, which translates to higher costs of data retention.

Attackers don't wait for configuration changes

It's important to note that QRadar EDR achieved 100% of its detections with out-of-the-box configurations. Configuration changes help vendors adjust their detections as the attack progresses. Twenty-three of the 30 participating vendors had to tweak their product 'antennas' multiple times before being able to detect alerts, using learnings from Day 1 and Day 2 to accurately detect the threat on Day 3.

In real life, configuration changes are usually unrealistic and reflect hidden resource costs of ownership. The more configurations a solution requires, the more an organization has to invest in its management. Attackers do not give defenders a second chance to tweak their detections.

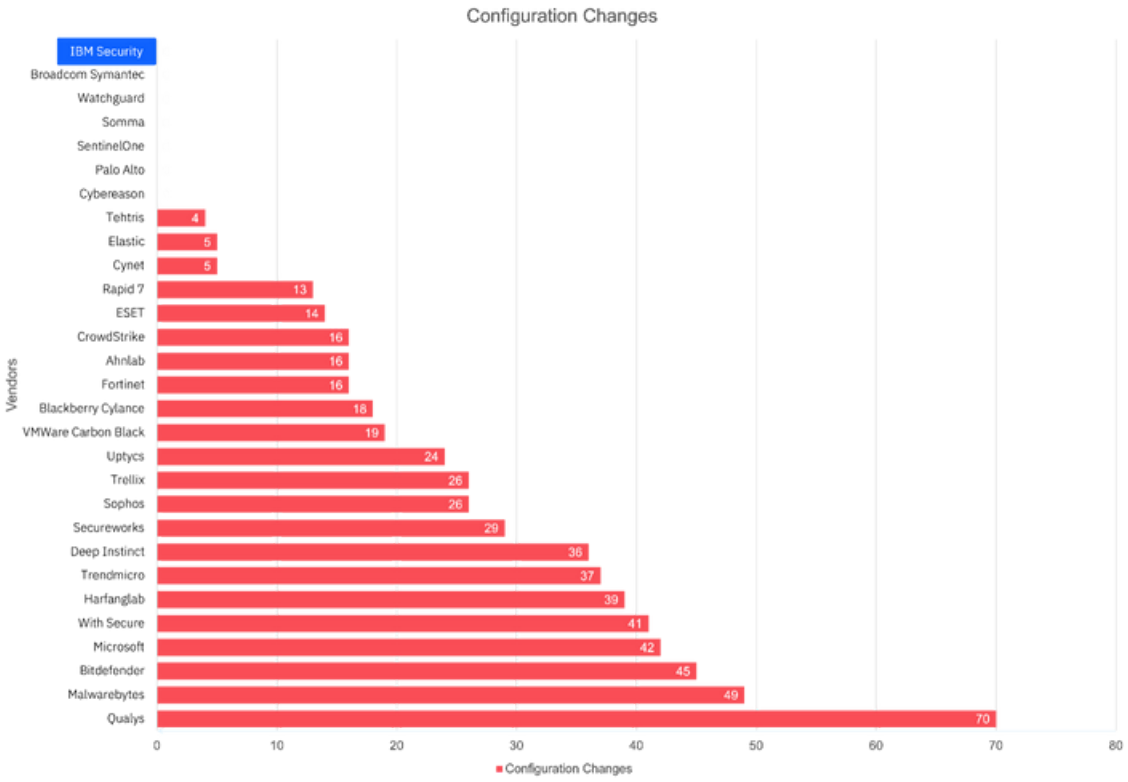


Bottom line – QRadar EDR catches what matters. Collecting more doesn't equate to being better. It simply means analysts have more noise (false positives) to investigate. More data also means increased storage, which translates to higher costs of data retention.

Attackers don't wait for configuration changes

It's important to note that QRadar EDR achieved 100% of its detections with out-of-the-box configurations. Configuration changes help vendors adjust their detections as the attack progresses. Twenty-three of the 30 participating vendors had to tweak their product 'antennas' multiple times before being able to detect alerts, using learnings from Day 1 and Day 2 to accurately detect the threat on Day 3.

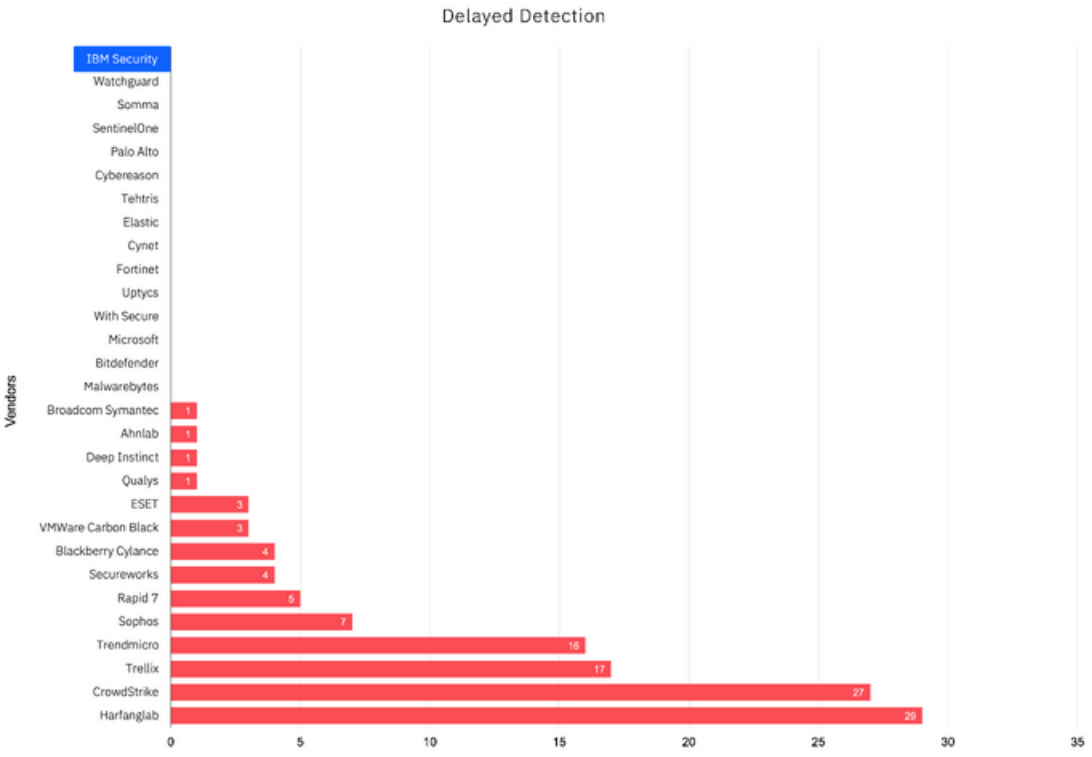
In real life, configuration changes are usually unrealistic and reflect hidden resource costs of ownership. The more configurations a solution requires, the more an organization has to invest in its management. Attackers do not give defenders a second chance to tweak their detections.

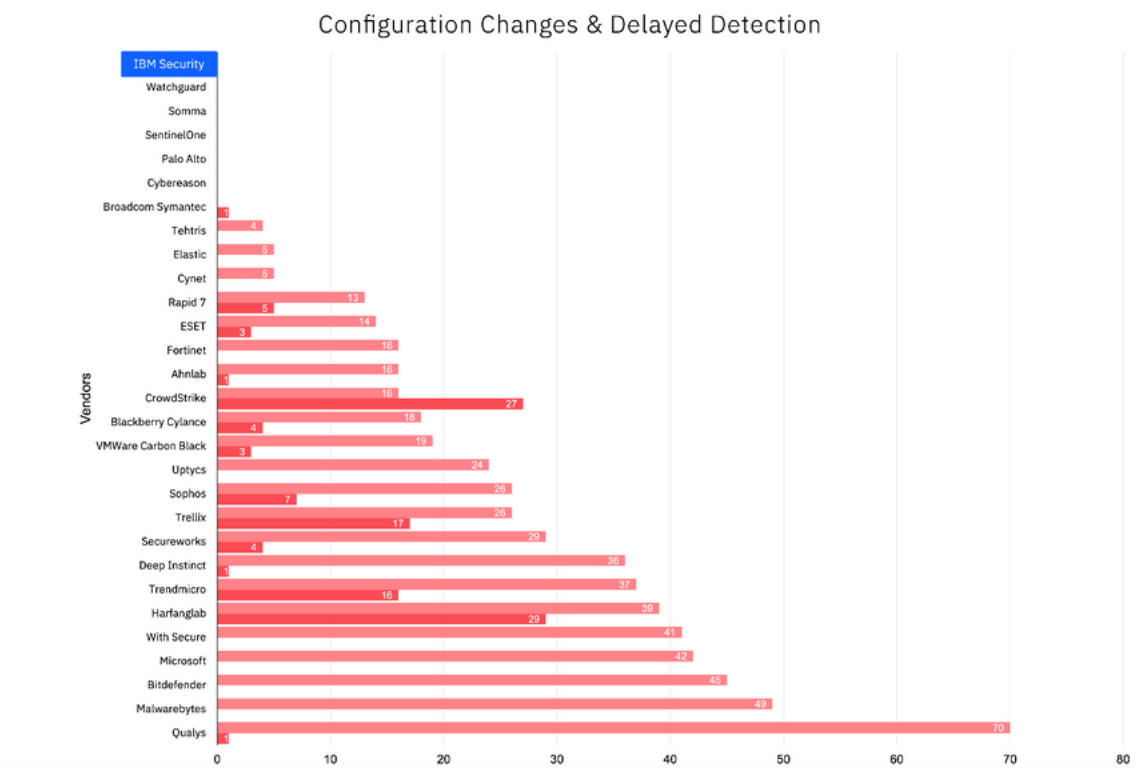


All detections were made in real time

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

Almost half of participating vendors had delayed detections. This is important because as attackers innovate, automation allows them to move extremely quickly within networks. An immediate identification and automated response draw the line between a fully compromised infrastructure and an unsuccessful breach. Being able to detect threats in real-time reduces the overall Mean Time to Detect and Respond, thereby mitigating the actual risk of a cyber breach, saving time, and reducing costs.


Delayed Detection
Vendors
IBM Security
Watchguard
Somma
SentinelOne
Palo Alto
Cybereason
Tehtris
Elastic
Cynet
Fortinet
Uptycs
With Secure
Microsoft
Bitdefender
Malwarebytes
Broadcom Symantec
Ahnlab
Deep Instinct
Qualys
ESET
VMWare Carbon Black
Blackberry Cylance
Secureworks
Rapid 7
Sophos
Trendmicro
Trellix
CrowdStrike
Harfanglab
1
1
1
1
3
3
4
4
5
7
16
17
27
29
0
5
10
15
20
25
30
35


Configuration Changes & Delayed Detection
Vendors
IBM Security
Watchguard
Somma
SentinelOne
Palo Alto
Cybereason
Broadcom Symantec
Tehtris
Elastic
Cynet
Rapid 7
ESET
Fortinet
Ahnlab
CrowdStrike
Blackberry Cylance
VMWare Carbon Black
Uptycs
Sophos
Trellix
Secureworks
Deep Instinct
Trendmicro
Harfanglab
With Secure
Microsoft
Bitdefender
Malwarebytes
Qualys
1
4
5
5
13
5
14
3
16
16
1
16
27
18
4
19
3
24
26
7
26
17
29
4
36
1
37
16
39
29
41
42
45
49
70
1
0
10
20
30
40
50
60
70
80

Testing the protections

With the anti-malware (EPP) module, Hive Cloud (Cloud AV) and other add-on components disabled, malwares were allowed to execute and exhibit malicious behaviors post-execution. This allowed QRadar EDR to track its behavior and kill the application when identified as malicious, allowing protection to follow the same pattern of detection, and making it more resilient to the malware code changes. Once executed, QRadar EDR blocked both scenarios as soon as the malicious files were executed, thereby protecting against any possible threats thereafter. This result was achieved leveraging only the behavioral detection and response components, such as the EDR and the Destra (Detection Strategy) capabilities. QRadar EDR customers can also craft their own logic and customized response activities, so it can be tailored to meet organizational requirements.

Conclusion

For the fourth 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 Evaluations 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.

Takeaway 1: 100% visibility across all evaluated stages of the MITRE ATT&CK framework
Even without NanoOS, QRadar EDR provided 360°-visibility for fast detection of critical threats, delivering only consolidated, high-fidelity alerts that really matter in near real-time. This reduces the amount of 'noise' analysts have to investigate and saves on data retention storage costs.

Takeaway 2: No configuration changes during the entire evaluation
By design, low-fidelity events are not collected and QRadar EDR does not rely on API hooking. Instead, only essential information that makes a difference to investigation and response outcomes is collected. An immediate detection can be the difference between a compromised infrastructure and an unsuccessful breach.

Takeaway 3: 100% of detections done in real-time without delays
IBM Security was 1 of only 7 vendors (out of 29) that participated without any configuration changes in order to detect the attack. In real-life you get one shot; there are no second chances.

Learn more about QRadar EDR to see how it leverages automation and AI to detect and remediate threats in near real-time. For more information, contact your IBM Business Partner.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America December 2023

For more information, contact your IBM Business Partner:

AI SecureNet LLC
208-407-2265 | team@aiSecureNet.com
www.aiSecureNet.com