XDR Report

Microsoft Defender Extended Detection & Response (XDR) CyberRisk Validation Report

SecureIQLab XDR Validation Methodology v1.0

Test Period: 06 June 2024 – 10 July 2024

Last Revision: 26 September 2024

Contents

1 Executive Summary....2
2 Introduction....2
3 XDR Test Scenario Overview....3
4 XDR Security Filtering Effectiveness....8
5 XDR Operational Accuracy....10
6 Threat Metrics....10
7 Operational Efficiency Metrics....12
8 XDR Solution Benefits and Key Capabilities....13
8.1 XDR Solution Benefits....13
8.2 XDR Solution Key Capabilities....13
9 Conclusion....14
10 Appendix....15
10.1 XDR Statistical Analysis....15
10.2 Microsoft XDR Solution Deployment Overview....15
10.3 Coverage Modules....17
11 Contact Information....17
12 Copyright and Disclaimer....18

1 Executive Summary

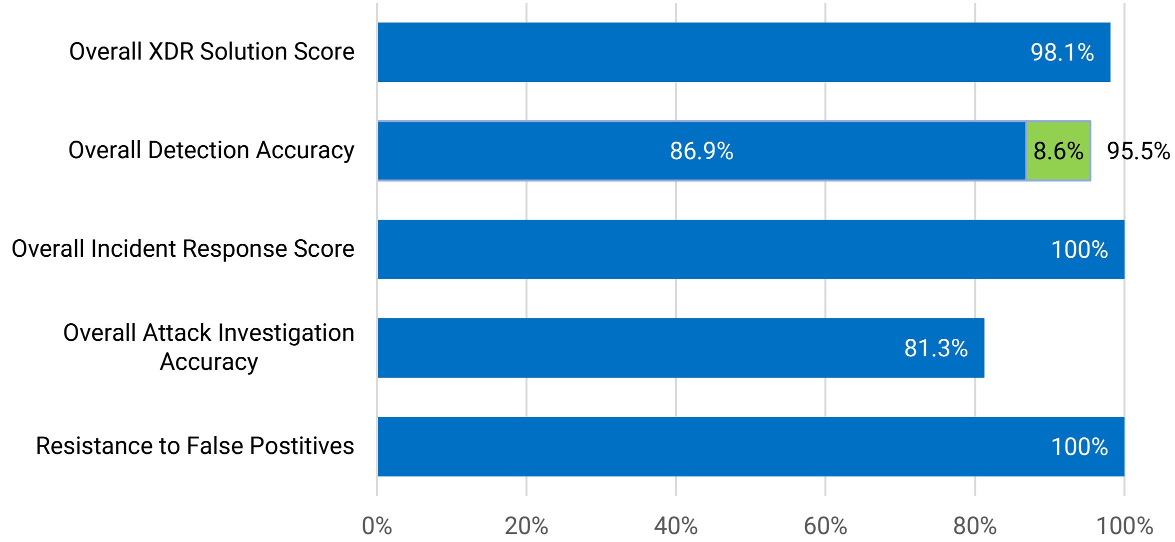

Figure 1. Microsoft XDR Solution Overall Score and Scores by Category

SecureIQLab evaluated the Microsoft Defender XDR (extended detection and response) solution's capability.

The Microsoft Defender XDR received an *Overall XDR Solution Score* of 98.13%. Figure 1 above summarizes its overall scores.

The Microsoft Defender XDR solution performed exceptionally in detection accuracy validation, achieving an *Overall Detection Accuracy* score of 95.45%. In Overall Detection Accuracy, the Microsoft XDR solution's machine learning (AI/ML) component(s) contributed 8.6% (green bar in Figure 1) to this success rate.

The Microsoft Defender XDR solution received an *Overall Attack Investigation Accuracy* score of 81.25%. The Microsoft Defender XDR solution also demonstrated outstanding incident management and response capabilities, acting and/or successfully responding to almost all validated Cyber threat scenarios. It achieved an *Overall Incident Response* score of 100%, the maximum possible.

The Microsoft Defender XDR solution accurately identified and allowed non-malicious traffic and applications and allowed users to perform their tasks without interruption, earning it the maximum score, 100%, for *Resistance to False Positives*.

2 Introduction

Enterprises face cyber threats from individuals, state-sponsored actors, and criminal organizations. Some attackers are motivated by financial gain and use tools such as the Black Hole Exploit Kit and Zeus Trojan; others attack for sabotage or espionage purposes and use tools such as Wiper malware. Still others are driven by activism (e.g., defacing web content) or state-sponsored cyberterrorism.

One example of state-sponsored cyberterrorism is the Black Energy Trojan, which was used to attack Ukraine's electricity grid.

To manage cyber risk, enterprises seek solutions that preserve crucial insights and contextual information during investigations that span multiple toolsets. This helps ensure the prompt and effective mitigation of threats and allows them to protect against similar attacks in the future. Extended detection and response (XDR) solutions intend to do just this. Not only can they detect data and threats, but they can also handle remediation and response. The crucial distinction between traditional remediation and response technologies such as anti-malware and endpoint detection and response on the one hand and

XDR on the other hand is XDR's ability to consume and administer raw information from different components within enterprise perimeters and correlate isolated information generated from those components to create a complete picture of a threat just like a painter would take individual trees, mountains, and lakes to create a landscape.

Microsoft is a leading player in the XDR market. Its XDR solution aims to address visibility challenges such as alert overload or lack of context, as well as issues related to incident prioritization. It collects and analyzes data from the endpoint, cloud, and network to detect and respond to threats. It provides a range of automated and orchestrated response actions, and it integrates curated threat intelligence to provide dynamic insights into both emerging and existing threats.

Microsoft describes its solution as follows: "Our comprehensive solution collects telemetry and other data from across your attack surface and uses security analytics and machine learning to drive better incident response."[1]

SecureIQLab is a next-generation security testing lab established in 2019.

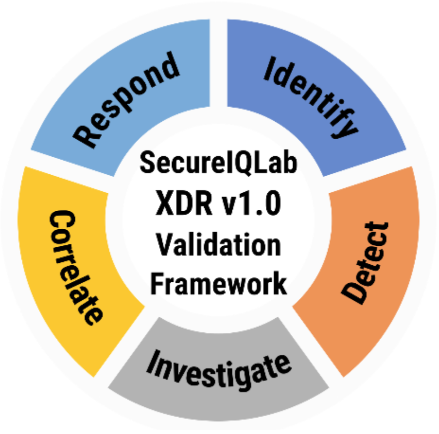

Figure 2. SecureIQLab XDR v1.0 Validation Framework

The SecureIQLab evaluation of the Microsoft XDR solution was conducted according to the SecureIQLab XDR v1.0 Validation Framework, figure 2, found in the SecureIQLab public v1.0 XDR CyberRisk Validation Methodology[2]. It focused on assessing the Microsoft XDR solution's ability to manage the threat detection and incident response (TDIR) life cycle while at the same time ensuring that threat data was unified across endpoints, networks, cloud environments, and other relevant areas.

During the evaluation, SecureIQLab deployed the Microsoft Defender Sensor on infrastructure. The test infrastructure followed good security hygiene, utilizing access control and segmentations that included multiple departments with varied user permissions.

This plausibly defendable deployment helps demonstrate the real-world performance of the XDR solution, and the realistic infrastructure and workloads played an important role during false-positive testing. This hardened test infrastructure represents the difficulty of conducting the attack on the infrastructure and allows measurement of the Microsoft XDR solution's capability to deal with representative elevated and emerging threats.

3 XDR Test Scenario Overview

An XDR solution should have the capability to identify and provide basic, enhanced, and extended detection of threats. XDR detection must be applicable to individual assets and their associated interconnected devices.

This validation primarily focused on the following XDR metrics: resistance to false positives, ability to initiate remediation and response actions accurately, ability to minimize attacker dwell time, and demonstrate enterprise-centric operational efficiency.

This evaluation consisted of an enterprise-representative environment of Windows and Linux, identity services, access management services like Active Directory, and cloud-based infrastructure through containerization. The attack surface was targeted by 44 cyber threat scenarios, where attacks were executed through their complete lifecycle to determine the XDR solution's holistic detection capabilities.

Each XDR scenario involved multiple real-world threats and consisted of multiple attack stages with measurable adversary outcomes. The Microsoft Defender XDR solution detected all scenario steps across 38 of 44 validated XDR scenarios. In 6 of the 44 scenarios, there were detection gaps. In the absence of

[1] Microsoft XDR solution documentation

[2] https://secureiqlab.com/wp-content/uploads/2023/09/XDR-CyberRisk-Validation-Methodology.pdf

detection, it will be difficult for analysts using the XDR solution to provide a comprehensive incident response report evaluating an attack. These gaps represent an exposure in the detection which leads to a lack of protection of the Microsoft XDR solution.

The XDR solution only relies on AI/ML 8.97%[3] of the time, which implies that the Microsoft XDR solution's detection capability is not solely reliant on the AI/ML component(s). This is important for understanding the XDR solution's coverage between other detection models versus AI/ML models.

The *Overall Attack Investigation Accuracy* score was calculated by dividing all the attacks into stages and measuring the stages Microsoft Defender XDR detected compared to the total attack stages. This score measures, for each validated attack detected, the solution's ability to identify attacks and map them to each attack stage in a scenario; the Microsoft Defender XDR's Overall Attack Investigation Accuracy score was impressive.

The *Overall Incident Response* score represents the overall accuracy of a solution's investigation and response capabilities. It is determined by calculating the ratio of a solution's incident management and recommendation scores to the maximum scores possible.

Table 1 below presents the 44 XDR test scenarios in this evaluation as well as the Microsoft XDR solution's detection and response metrics for each scenario. The table represents the Threat Scenario, Threat Actor, Threat Itself, and Vulnerability. The solution accurately detected and responded to 44/44 scenarios.

Scenario ID	Threat Scenario	Threat Actor	Threat	Vulnerability	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
1	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	66.7%	38.9%	100.0%
2	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	66.7%	50.0%	100.0%
3	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	50.0%	100.0%
4	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	88.9%	100.0%
5	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	80.0%	100.0%
6	Unauthorized Access	External Attacker	Account Hijacking	Social Engineering	100.0%	77.8%	100.0%
7	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	80.0%	100.0%
8	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	100.0%	100.0%
9	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	83.3%	100.0%
10	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	72.2%	100.0%
11	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	63.0%	100.0%
12	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	95.8%	100.0%
13	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	77.8%	100.0%
14	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	72.2%	100.0%
15	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	75.0%	100.0%

[3] See Appendix for a Complete Coverage Module percentage overview.

16	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	88.9%	100.0%
17	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	72.2%	100.0%
18	Unauthorized Access	External Attacker	Account Hijacking	Social Engineering	100.0%	61.1%	100.0%
19	Unauthorized Access	External Attacker	Account Hijacking	Exploit	66.7%	50.0%	100.0%
20	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	66.7%	38.1%	100.0%
21	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	76.7%	100.0%
22	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	72.2%	100.0%
23	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	55.6%	100.0%
24	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	71.4%	100.0%
25	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	66.7%	100.0%
26	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	61.1%	100.0%
27	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	66.7%	100.0%
28	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	100.0%	61.9%	100.0%
29	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	61.1%	100.0%
30	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	61.9%	100.0%
31	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	54.2%	100.0%
32	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	66.7%	33.3%	100.0%
33	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	61.1%	100.0%
34	Unauthorized Access	External Attacker	Data Loss	Social Engineering	100.0%	73.3%	100.0%
35	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	57.1%	100.0%
36	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	66.7%	100.0%
37	Unauthorized Access	External Attacker	Data Loss	Social Engineering	100.0%	66.7%	100.0%
38	Unauthorized Access	External Attacker	Data Loss	Exploit	100.0%	52.4%	100.0%
39	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	70.8%	100.0%
40	Unauthorized Access	External Attacker	Data Loss	Social Engineering	100.0%	53.3%	100.0%
41	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	55.6%	100.0%
42	Unauthorized Access	External Attacker	Data Loss	Social Engineering	66.7%	16.7%	100.0%
43	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	83.3%	100.0%
44	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	100.0%	27.8%	100.0%

Table 1. Microsoft XDR Attack Scenarios

A threat model is a system developed to map out the attacker's capabilities that can be used to categorize attacks as a result of some action. The threat model helps to align defense for all attack categorization, and in case of alignment not being achieved with a single defense technology such as XDR, alternative means of defense can be used to plug in those exposures.

The STRIDE threat model is a threat classification system developed by Microsoft as part of threat modeling. STRIDE is an acronym for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. STRIDE helps to align controls associated with confidentiality, Integrity, and availability of computing machinery.

SecureIQLab chose the threat model representation because the threat model allows defenders to plug gaps/exposure appearing in the environment due to lack of coverage. Furthermore, as opposed to frameworks like MITRE ATT&CK, which is heavily centered toward threats appearing in endpoint, STRIDE allows for mapping, initiation, and alignment of other layered threat defenses that are not endpoint protection that can be activated for gaps/exposure. Threat models are useful for organizations that are mature in their cyber security journey.

This report maps threats into relevant metrics within the STRIDE[4] model to demonstrate the degree of coverage of the Microsoft XDR Solution. The table below provides the details.

Scenario ID	Threat Scenario	Threat Actor	Threat	Vulnerability	No. of Steps with Spoofing(S)	No. of Steps with Tampering with Data(T)	No. of Steps with Repudiation(R)	No of Steps with Information (I)	No of Steps with Denial of Service(D)	No of Steps with Elevation of Privilege(E)	STRIDE COVERAGE
1	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	1	1	3	0	0	100%
2	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	2	1	4	0	0	100%
3	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	2	100%
4	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	2	1	1	0	1	100%
5	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	1	100%
6	Unauthorized Access	External Attacker	Account Hijacking	Social Engineering	1	0	0	5	0	0	100%
7	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	1	100%
8	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	2	0	1	0	1	100%
9	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	3	0	1	1	0	100%
10	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	2	0	2	0	1	100%
11	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	4	0	3	100%
12	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	2	0	5	100%
13	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	2	0	3	0	0	100%
14	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	2	0	3	0	0	100%

[4] https://en.wikipedia.org/wiki/STRIDE_model

15	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	2	0	3	0	2	100%
16	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	1	0	3	100%
17	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	1	2	0	1	100%
18	Unauthorized Access	External Attacker	Account Hijacking	Social Engineering	1	2	0	3	0	0	100%
19	Unauthorized Access	External Attacker	Account Hijacking	Exploit	1	3	0	2	0	0	100%
20	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	3	0	2	0	1	100%
21	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	4	1	3	0	1	100%
22	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	2	100%
23	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	3	0	1	100%
24	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	3	100%
25	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	3	0	2	100%
26	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	1	0	4	0	0	100%
27	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	1	0	4	0	0	100%
28	Unauthorized Access	External Attacker	Insufficient Due Diligence	Social Engineering	1	2	0	4	0	0	100%
29	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	3	0	1	100%
30	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	2	0	3	0	1	100%
31	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	4	0	1	1	1	100%
32	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	3	1	2	0	1	100%
33	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	2	1	0	1	0	2	100%
34	Unauthorized Access	External Attacker	Data Loss	Social Engineering	1	1	0	1	0	0	60%
35	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	0	4	0	1	86%
36	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	2	0	1	71%
37	Unauthorized Access	External Attacker	Data Loss	Social Engineering	1	1	0	3	0	0	83%
38	Unauthorized Access	External Attacker	Data Loss	Exploit	1	1	0	2	0	0	57%
39	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	3	0	2	88%
40	Unauthorized Access	External Attacker	Data Loss	Social Engineering	1	2	0	2	0	0	100%
41	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	0	1	3	0	2	78%
42	Unauthorized Access	External Attacker	Data Loss	Social Engineering	1	0	0	1	0	0	50%
43	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	1	1	0	0	0	3	63%
44	Unauthorized Access	External Attacker	System Vulnerabilities	Exploit	2	0	0	1	0	2	83%

Table 2. Microsoft XDR STRIDE Coverage

STRIDE coverage of <100% indicates a lack of coverage in one of the domains of STRIDE.

4 XDR Security Filtering Effectiveness

To protect against modern threats, enterprises collaborate with the cybersecurity community, and this has resulted in the development of national and international frameworks that establish crucial guidelines to help effectively combat such attacks. One well-known example is the NIST Cybersecurity Framework published by the US National Institute of Standards and Technology, which describes standards, guidelines, and best practices for managing cybersecurity risk.[5]

Cybersecurity vendors have developed solutions that align with established frameworks and guidelines while addressing visibility challenges like alert overload, insufficient information, and inadequate incident prioritization. These solutions are designed to detect, contain, and respond to incidents effectively. XDR solutions were primarily created to address some of the key challenges of managing multiple security solutions while providing relevant alerts, reducing noise from activities logged, and facilitating incident response when cyberattacks and misuse are underway.

At a minimum, an XDR solution should log activity at the beginning of each attack scenario, properly identify events with less system overhead, and provide high-fidelity threat classification and correlation scores that result in actionable alerts.

SecureIQLab expands upon this purpose of XDR and asserts that XDR should also include the unification of telemetry from multiple security technologies through automated or semi-automated means to minimize alert noise and focus on delivering actionable intelligence to end users. In other words, the XDR solution should present telemetry in a useful format.

The Microsoft XDR solution logged more than 1 million activities during this validation. The SecureIQLab XDR v1.0 Validation Methodology utilized 44 enterprise-centric XDR cyber threat scenarios that include a total of several attack stages in each of them.

During each of the enterprise-centric scenarios, SecureIQLab carried out between three to 10 attack steps (consisting of one to multiple activities) of the attack kill chain, which resulted in the solution effectively contextualizing several high-fidelity actionable alerts during the evaluation.

The Microsoft XDR solution was able to identify and detect these attack stages generating a total of 12589 events during the evaluation.

Validation of an XDR solution should take into account its alert-to-event ratio during identification, detection, and investigation. Figure 4 below shows the actual number of alerts and the actual number of events generated by the Microsoft solution across the 44 XDR attack scenarios.

[5] https://www.nist.gov/cyberframework

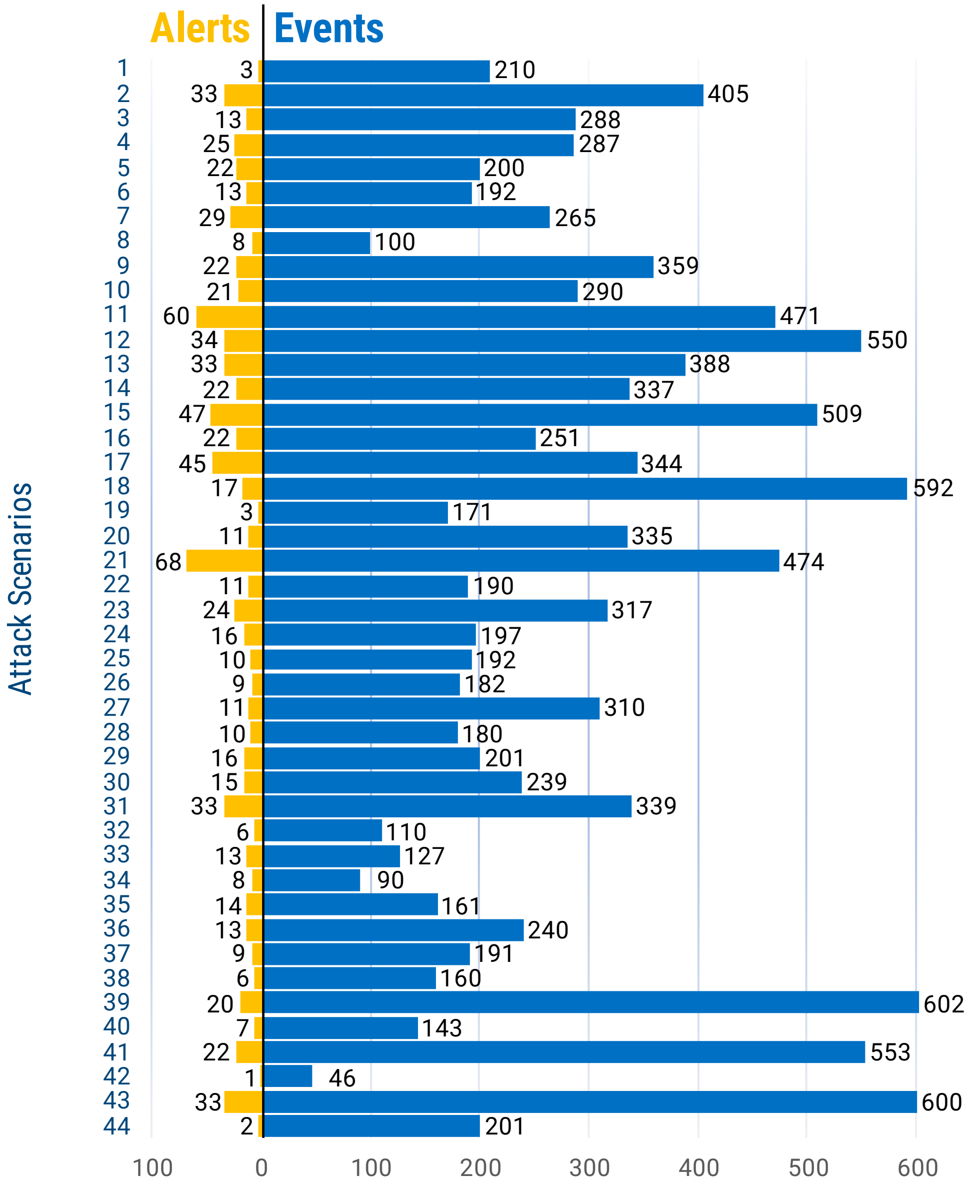

Figure 3. Microsoft XDR Alert and Event Results for Each Scenario

Depending on the type of attack scenario, the number of events generated and alerts correlated may vary. Depending on their baselining and configuration, some XDR solutions may be tuned to have a higher event-to-alert ratio, providing greater visibility but at the cost of a higher noise threshold and a lower response and remediation index. Other XDR solutions may have a lower event-to-alert ratio resulting in a lower noise threshold with higher-fidelity alerting and a higher response and remediation index.

5 XDR Operational Accuracy

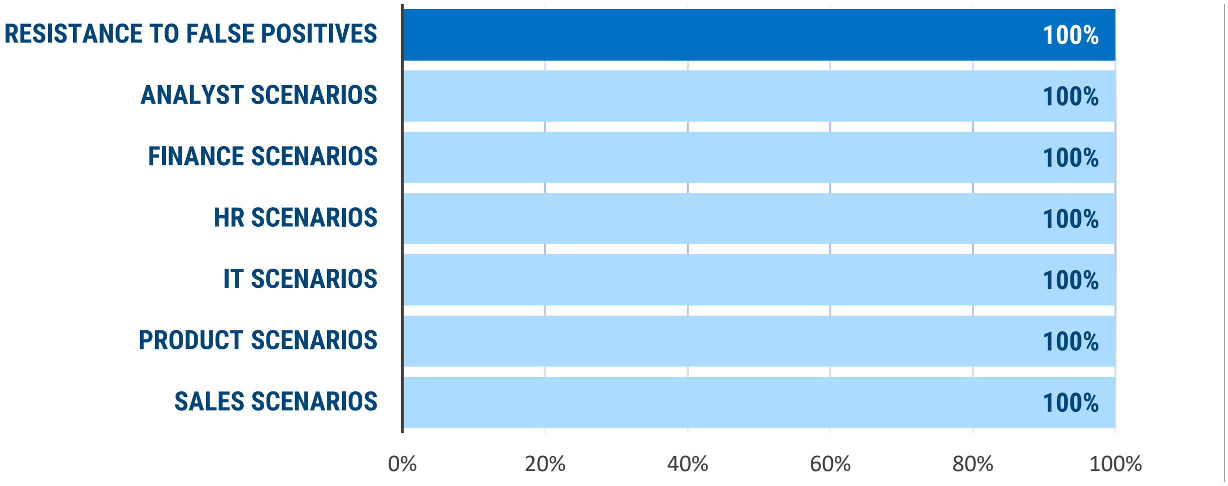

Figure 4. Microsoft XDR Solution Resistance to False Positive Test Results

Unlike traditional approaches that focus on file-based false positives, this test emphasized action-based false positives, reflecting the evolving nature of modern security threats, where attackers often use legitimate activities to mask malicious behavior.

For this test, an XDR solution was considered "extremely noisy" if it not only reported 100% of malicious threats but also flagged legitimate (non-malicious) actions.

SecureIQLab validated the Microsoft XDR solution’s ability to minimize noise across more than 284 real-world scenarios from various enterprise departments, such as human resources, finance, and IT. False-positive testing included different contexts, such as legitimate PowerShell usage for IT or browser activity for sales. This testing was integrated throughout the evaluation to ensure that the XDR solution maintained a balance between prevention and operational accuracy. Additionally, SecureIQLab distinguished between low-importance alarms and false positives, recognizing that the former can provide valuable, non-urgent information while the latter indicates errors in detecting actual threats.

6 Threat Metrics

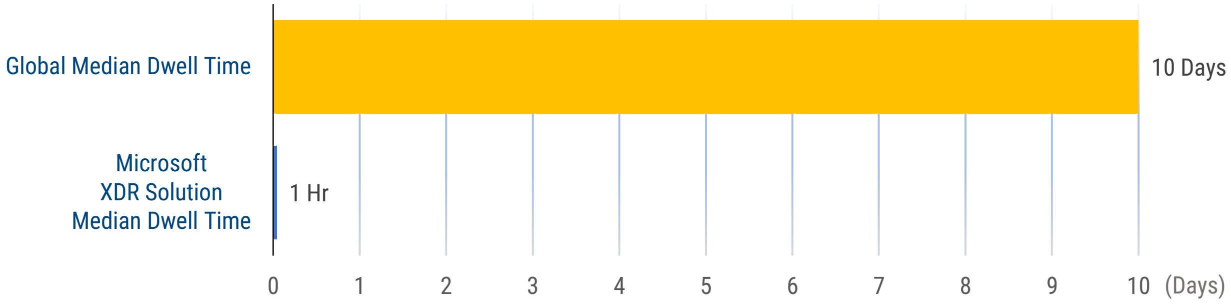

Figure 5. Attacker Dwell Time Comparative

Threat metrics refer to the facts that constitute the state of affairs being measured. Organizational infrastructure is a representation of such a state of affairs and is made of objects like computing machinery.

Threat metrics provide specific data points to demonstrate the ability of an XDR solution to detect and provide high-fidelity threat classification and threat correlation indexing. This should result in appropriate response and mitigation capabilities that help improve the organization's risk posture and security efficacy while continually improving its Return on Security Investment (ROSI).

The Microsoft XDR solution's Threat metrics are shown in Table 3.

Threat Metrics	Microsoft XDR Solution Metrics
Maximum Time-to-Detect (TTD)	≤ 1 Hour
Maximum Attack Dwell Time	≤1 Hour
Threat Classification Fidelity	95.45%
Threat Correlation Index	64.61%

Table 3. Microsoft Threat Metrics Overview

Threat metrics was measured using the following factors:

- **Time-to-Detect (TTD):** The capability of an XDR solution to rapidly identify an attack, classify it as a tangible event leading to a high-fidelity alert detection, and display relevant information is extremely critical. SecureIQLab recorded the attack initiation time frame of every XDR scenario and measured how long it took the Microsoft XDR solution to trigger the initial alert detection. The Microsoft XDR solution had an excellent Maximum Time-to-Detect metric of less than or equal to 1 hour throughout the evaluation.
- **Attack Dwell Time:** It is imperative for an XDR solution to have as little time as possible between the time of attack origination and the initial time of attack detection (Attack Dwell Time). Minimizing Time-to-Detect is critical for reducing dwell time, i.e., the amount of time an attacker is in the environment. This is essential for breach prevention. Because the Microsoft XDR solution's suggested remediation responses were so effective, its Maximum Time-to-Detect and Maximum Attack Dwell Time metrics were essentially the same. In 2023 the global median dwell time for an enterprise was 10 days, or 240 hours. The Microsoft XDR solution demonstrated a Maximum Attack Dwell Time of less than or equal to 1 hour, giving it a median dwell time less than or equal to 1 hour, which is less than 0.4% of the global median. Figure 6 demonstrates the Microsoft XDR solution's median dwell time as compared to the global median dwell time for an enterprise.
- **Threat Classification Fidelity:** Not all threats are of equal severity. The ability to classify attacks according to the risk that each one poses is an important feature of an XDR solution. The measure of an XDR solution's Threat Classification Fidelity is its capability to quickly and accurately identify threats and threat vectors. In addition, the solution must be capable of quickly and accurately contextualizing and classifying the threats based on their severity, i.e., according to the organization's attack surface, threat intent, and risk they pose for the organization. The Microsoft solution achieved a competitive Threat Classification Fidelity score of 95.45%.
- **Threat Correlation Index:** While Time-to-Detect measures the time to detect an incident, the Threat Correlation Index measures how well the solution connects the dots between pieces of information, provides more knowledge about cyber threats, as well as how accurately the threats are mapped to additional research, for example the attack kill chain. The Threat Correlation Index measures how effective the solution is at providing contextualized, actionable, noise-free threat data that can be used to correlate past incidents and threats with current threats to better understand the potential risks organizations may face. This information can be used to assist

enterprise security teams in making critical decisions by giving them a better understanding of the threat life cycle and by helping them understand where to adjust policies and security configurations, not just for the XDR solution but also for any connected threat intelligence platforms. While the Microsoft solution's Threat Correlation Index score of 64.61% demonstrates competence, its threat mapping capabilities can be improved. Threat metrics provide specific data points to demonstrate the ability of an XDR solution to detect and provide high-fidelity threat classification and threat correlation indexing. This should result in appropriate response and mitigation capabilities that help improve the organization's risk posture and security efficacy while continually improving its Return on Security Investment (ROSI).

7 Operational Efficiency Metrics

Operational efficiency refers to the effectiveness and efficiency with which an XDR solution can provide security for an organization's cloud infrastructure while minimizing operational costs and complexity.

Operational Efficiency metrics provide specific data points to demonstrate the ability of an XDR solution to detect and provide high-fidelity threat classification and threat correlation indexing. This should result in appropriate response and mitigation capabilities that help improve the organization's risk posture and security efficacy while continually improving its Return on Security Investment (ROSI).

Time-to-Deploy: A low *Time-to-Deploy* is important for enterprises seeking to shorten their time to value for a solution. The Microsoft solution was quick to deploy and tuning of its security policies and configurations (pre-and-post deployment) was simple. See Section 7 for more details on deployment of the Microsoft solution during this evaluation.

The Microsoft XDR solution's *Operational Efficiency* metrics are shown in Table 4.

Categories	Coverage
Time-to-Deploy	1 Hour
Security Policy Configuration	85.2%
Security Policy Management	81.0%
Asset Management	55.6%
Access Control	100.0%
Incident & Risk Assessment & Mitigation	100.0%
Compliance Management	100.0%
Security Metrics Reporting	100.0%
Backup and restore	33.3%
Analytics	86.7%
Visibility	83.3%
Data Retention	100.0%
Incident Hunt	100.0%
Integration	100.0%
Provisioning	100.0%

Table 4. Microsoft XDR Operational Efficiency Overview

8 XDR Solution Benefits and Key Capabilities

Cyber security solutions provide valuable benefits to disrupting, investigating, and responding to potential Cyber Attacks. These benefits may or may not always work due to the complex interaction of these solutions with internal components and external components such as the cloud. These interactions are common with connectivity, pattern delivery, and difficult-to-understand workflow.

8.1 XDR Solution Benefits

SecureIQLab validated the value proposition of Microsoft's XDR that Microsoft publicly promotes to their customer base. The validation relied solely on interaction with the Microsoft XDR solution as the solution was subjected to simulated cyber attacks. This interaction and simulation under real-world defendable architecture helped us objectively verify capabilities and benefits. The result of this effort is industry-defining insights as it relates to solutions' true capabilities. Tables 5 and 6 highlight these mappings.

Microsoft XDR Solution Benefit Category	SecureIQLab Validation Overview
Increased Visibility	The XDR solution provided some visibility into all 44 attack scenarios and complete visibility into 38 of the attack scenarios. This was within an average time limit of <=1 hr from the original introduction of the attack scenario.
Streamlined SecOps Workflows	The XDR Solution provided workflow for incident response into all 44 attack scenarios resulting in a 100% SecOps Workflow efficiency.
Improved productivity and efficiency	The XDR Solution recorded a 87.18% rating in productivity and efficiency while staging, deploying, and using the product with superior operational efficiency.
Accelerated threat detection and response	The XDR Solution provided a mechanism to detect and respond to action. It achieved the detection and aided response within 1 hr. compared to 10 days of the industry average. It provided 99.6% quicker threat detection and response as compared to the industry average.
Operational complexity and costs	The XDR Solution provided less operational complexity in major categories.
Faster SOC Insights	SOC relies upon tools like XDR to provide operational information that can be leveraged to find threats incoming, and threats persistent in the environment. The XDR Solution provided insights into threats in less than 1 hr.

Table 5. Microsoft XDR Benefits Metrics Overview

8.2 XDR Solution Key Capabilities

Microsoft **XDR (Extended Detection and Response)** solution offers comprehensive threat detection by monitoring across multiple layers leveraging advanced analytics, such as AI and machine learning, to identify known and unknown threats while also having automated response capabilities while delivering centralized visibility through a unified console, enabling security teams to monitor and manage threats across the entire environment from a single interface. SecureIQLab identified and validated these key features that are pertinent to the enterprises as highlighted in the table below.

Microsoft XDR Solution Key Features	SecureIQLab Feature Validation Overview
Incident-based investigation	The XDR Solution provided workflow for incident investigation into all 44 attack scenarios. The XDR solution scored 100% for this capability.
Cyberattack chain visibility	The XDR Solution provided a 64.67% overall visibility. Specifically, it recorded a cyberattack chain visibility of 100% on 38/44 attack scenarios while offering limited visibility across 6/44 attack scenarios.
AI and Machine Learning	The XDR Solution triggered AI and Machine learning components to a maximum of 8.97% for all the detection, correlation, and classification outcomes for attack steps.
Automatic disruption of advanced cyberattacks	The XDR Solution demonstrated the capability to automatically disrupt advanced cyberattacks. These cyberattacks leveraged vulnerability, and exploitation, leveraged identity and access management compromise, and targeted diverse infrastructure not seen in average cyber-attacks. The XDR Solution thus "Passed" this capability.
Auto-healing of affected assets	The XDR Solution demonstrated the capability to auto-heal affected assets by disinfecting assets. During this engagement, SecureIQLab manually verified that assets didn't have a tell-tale sign of infection after auto-healing was done. The XDR Solution thus "Passed" this capability.

Table 6. Microsoft XDR Key Feature(s) Overview

9 Conclusion

The Microsoft XDR solution offers outstanding capabilities in threat detection, investigation, and response (TDIR), as evidenced by its **Overall XDR Solution Score of 98.13%**. Additionally, the solution is quick to deploy, configure, and activate.

A major contributor to this high score is the solution's ability to quickly identify and detect threats while displaying relevant, correlated information. This efficiency significantly reduces the Time-to-Detect, ensuring faster action on emerging threats. The solution's extended detection capabilities excelled in advanced attack scenarios, demonstrating effectiveness in correlating and classifying threats, which minimized noise and consistently resulted in actionable alerts during testing.

Response time is a critical factor for any XDR solution, as delays can lead to breaches. A faster response time reduces the risk of a successful compromise. The time it takes for a solution to observe system activities, trigger an event, and detect threats can vary based on its capabilities, configuration, and the expertise of the security professional or analyst using it. The Microsoft XDR solution consistently showcased highly effective and efficient detection and response capabilities.

Effective asset management is another vital element for reducing response time and containing incidents. The Microsoft XDR solution achieved an **Overall Incident Response Score of 100.0%**, delivering actionable alerts with precision.

Additionally, the Microsoft XDR solution demonstrated strong compliance management, risk assessment, and mitigation capabilities. It also provides seamless integration of detection and response data, accompanied by enhanced security metrics and reporting functionalities.

10 Appendix

10.1 XDR Statistical Analysis

MCC	Precision	Recall
0.83	1.00	0.84

Table 7. Statistical Analysis of the XDR Validation Test Results

At the conclusion of testing, the Microsoft Defender XDR solution test results were analyzed statistically. Table 8 provides the Matthews correlation coefficient (MCC), precision, and recall for the test results. Table 9 provides the definitions for the variables used in the equations to calculate the MCC, Precision, and Recall.

Variable	Meaning	Definition
TP	True Positive	# Benign Allowed
FP	False Positive	# Benign Blocked
FN	False Negative	# Attacks Missed
TN	True Negative	# Attacks Blocked

Table 8. Definitions of Variables

Calculation of the Matthews correlation coefficient is provided in Equation 1 below.

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP + FP) \times (TP + FN) \times (TN + FP) \times (TN + FN)}}$$

Equation 1. Matthews Correlation Coefficient Calculation

Calculations of precision and recall are provided in Equation 2 and Equation 3, respectively.

$$Precision = \frac{TP}{TP + FP}$$

Equation 2. Precision Calculation

$$Recall = \frac{TP}{TP + FN}$$

Equation 3. Recall Calculation

The statistical analysis of the XDR solution test results indicates the relevance of false positive testing. The MCC of 0.83 indicates a reliable and accurate classification of attack steps encountered during the test window. The recall of.84 indicates the need for improvement in attack step detection.

10.2 Microsoft XDR Solution Deployment Overview

Figure 7 provides an overview of the SecureIQLab Deployment Architecture for the Microsoft XDR Solution.

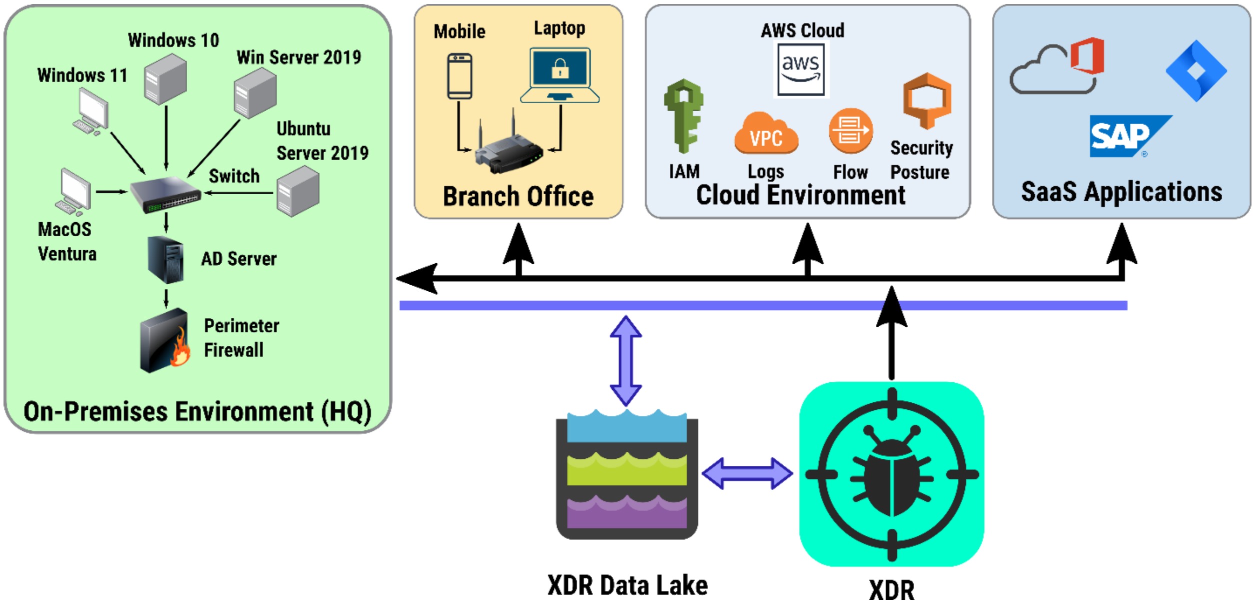

Figure 6. SecureIQLab Deployment Architecture for Microsoft XDR Solution

The Microsoft XDR solution uses the centralized platform for security monitoring of networks and devices in the cloud, on-premises, and in remote locations. The Microsoft XDR solution used components like Endpoint Detection and Response (EDR), Windows Defender Antivirus, and Extended Detection and Response (XDR) for Identity.

Test Infrastructure:

Operating Systems	Number of Virtual Machines
Ubuntu 20.04 LTS	2
Windows 10 x64 Enterprise Edition	10
Kali Linux (Attacker Machine)	1
Linux x86_64	4
Active Directory Domain Controller	1
Container Infrastructure	1

Table 9. Test Infrastructure

Time-to-Deploy measures the total amount of time required to:

- Create a Microsoft Defender XDR account.
- Deploy the XDR sensor in the test environment.
- Verify correct deployment, configurations, and integration of the XDR Sensor.

Configure the following: Client protection, Heuristic protection, Machine Learning based protection, Behavior-based protection, Memory Protection, Network Protection, and AMSI.

10.3 Coverage Modules

Coverage Module	Coverage %
Behavior + Network	53.42%
Behavior + Network + Memory	14.53%
AMSI + Behavior + Network	13.68%
Behavior + Network + Machine Learning	7.69%
Client + Heuristic	2.99%
Behavior	2.56%
Behavior + Machine Learning	1.28%
Client	0.85%
Others	0.85%
Client + Behavior + Memory + Network	0.43%
AMSI + Behavior	0.43%
Behavior + Memory	0.43%
Client + Heuristic	0.43%

Table 10. Detection by Coverage Model

Table 10 shows the percentage of the detection based on the different coverage models. These scores total to 100%. To calculate the Coverage Module’s detection contribution to the Overall Detection Accuracy Score, multiply 95.5% by the Coverage Module’s coverage percentage.

Alerts for the Microsoft XDR are defined as follows:

High-severity alerts indicate a real breach in the system, network, or data center, such as the detection of ransomware activity, the exploitation of a vulnerability, Command and control communication, suspicious use of administrative tools like PowerShell and PsExec, an Active Directory attack, privilege escalation, or lateral movement. These alerts indicate potential threats to critical assets and to the overall security of the domain.

Medium-severity alerts indicate suspicious activity that is more likely to be malicious. Examples include a suspicious file being created, a suspicious account being created, suspicious script execution, and unusual network activity.

Low-severity alerts indicate anomalies or suspicious activity with low certainty or impact. Examples include a suspicious sequence of exploration activities, suspicious system hardware discovery, abnormal file access, and suspicious port scans.

11 Contact Information

SecureIQLab, LLC.
9600 Great Hills Trail Ste 150W
Austin, TX 78759 USA

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

12 Copyright and Disclaimer

THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (a) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (b) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

SecureIQLab (September 2024)