SecureIQLab®

REPORT

AT&T Cybersecurity Extended Detection & Response (XDR) Validation Report

SecureIQLab XDR Validation Methodology v1.0

Test Period: September 5, 2023 – November 15, 2023

Last Revision: January 22, 2024 | *Commissioned by: AT&T Cybersecurity*

Contents

1 Executive Summary

AT&T Cybersecurity commissioned an independent evaluation of its extended detection and response (XDR) solution by SecureIQLab to validate the solution's capability to respond to true threats without producing false positives, accurately and efficiently initiate remediation and response actions, minimize attacker dwell time, and demonstrate enterprise-centric operational efficiency.

This Validation Report summarizes the results of the SecureIQLab evaluation.

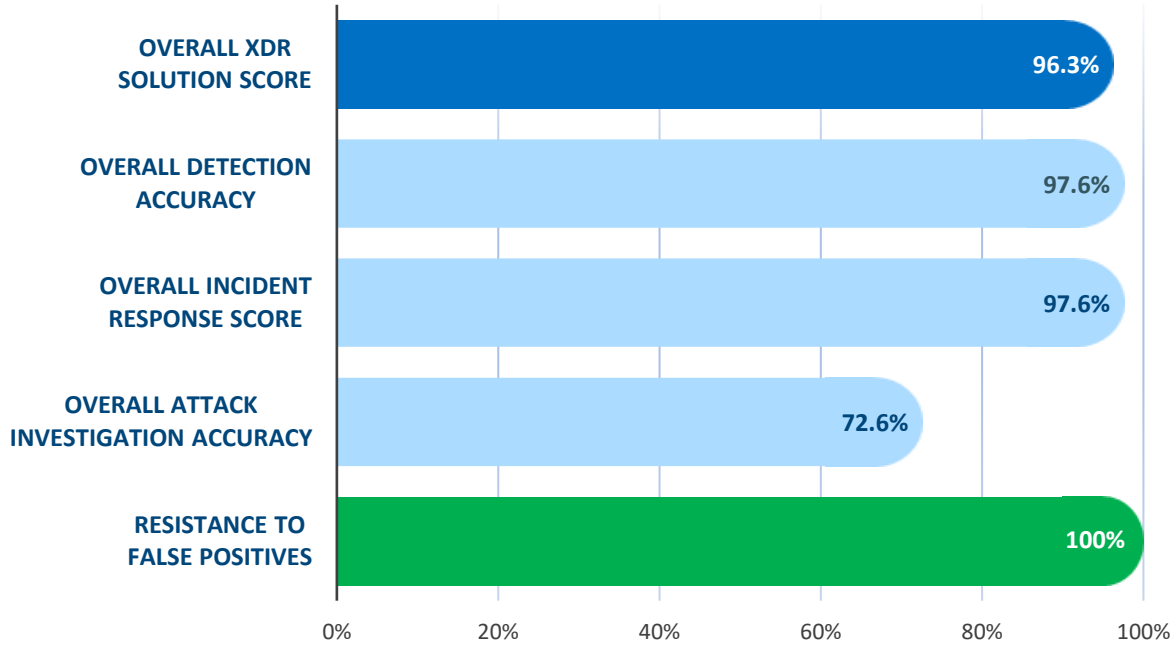


Figure 1. AT&T Cybersecurity XDR Solution Overall Score and Scores by Category

The AT&T Cybersecurity solution received an *Overall XDR Solution Score* of 96.3%. A summary of the solution's overall scores is provided in Figure 1.

The AT&T Cybersecurity XDR solution performed exceptionally well in detection accuracy validation. Its *Overall Detection Accuracy* score of 97.6% demonstrates high-fidelity threat detection, correlation, and classification across 40 of 41 validated XDR scenarios. Each XDR scenario involved multiple real-world threats and consisted of multiple attack stages with measurable adversary outcomes.

The AT&T Cybersecurity XDR solution received an *Overall Attack Investigation Accuracy* score of 72.6%. This score was calculated by dividing the total number of attack stages per scenario detected by the AT&T Cybersecurity XDR solution by the overall number of attack stages per scenario. This score measures the fidelity of the context provided by the solution for each validated attack detected. The AT&T Cybersecurity XDR solution's ability to identify attacks and map them to each attack stage in a scenario was very good overall.

The AT&T Cybersecurity XDR solution demonstrated outstanding incident response capabilities, acting and/or successfully responding to almost all validated attack scenarios and achieving an *Overall Incident Response* score of 97.6%. This 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 score possible.

The AT&T Cybersecurity XDR solution accurately identified and allowed non-malicious traffic and allowed users to perform their tasks without interruption, which earned it a maximum score of 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 such example 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 implement lessons learned 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.

AT&T Cybersecurity 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 efficiently 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.

AT&T Cybersecurity 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, an innovative security testing lab established in 2019, collaborates with enterprises, government entities, and security vendors to address the knowledge gap between market analysis and technology research. SecureIQLab offers services to assist in operationalizing security measures and establishing metrics that enable organizations to enhance their Return on Security Investment (ROSI) while reducing risks.

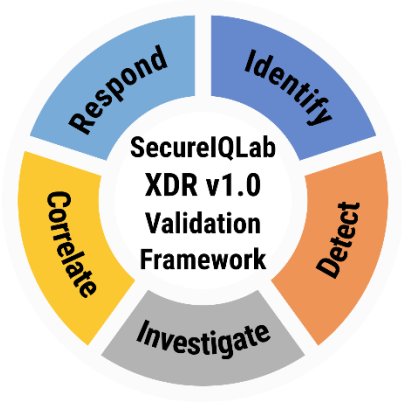


Figure 2. SecureIQLab XDR v1.0 Validation Framework

The SecureIQLab evaluation of the AT&T Cybersecurity 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 and focused on assessing the AT&T Cybersecurity solution's ability to comprehensively 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. The evaluation was based exclusively on the SecureIQLab XDR validation methodology selection criteria.[2]

During the evaluation, SecureIQLab deployed the AT&T Cybersecurity USM Anywhere Sensor on endpoint, network, and cloud 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 helped demonstrate the real-world performance of the XDR solution and the realistic infrastructure and workloads played an important role during false-positive testing.

[1] https://cybersecurity.att.com/solutions/extended-detection-and-response

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

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 inter-connected devices.

Basic detection in the context of an XDR solution or component within its technology stack should be the ability to identify threats and provide context for these threats with regard to attack surface, attack vector, intent, and potential impact—and all within a specified time frame.

Enhanced detection requires the ability to combine basic detection artifacts from one or more of the security components making up the XDR solution and provide automated or semi-automated response capabilities.

Extended detection requires the ability to combine enhanced detection with human expertise and external resources (such as indicators of compromise [IOCs], indicators of attack [IOAs], machine learning [ML], etc.) to provide information beyond what is currently siloed and provide the required orchestration and response.

Table 1 below presents the 41 XDR test scenarios in this evaluation as well as the AT&T Cybersecurity XDR solution's detection and response metrics for each scenario. The solution accurately detected and responded to 40/41 scenarios.

XDR Test Scenario	XDR Attack Scenario Overview	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
1	Attack scenario using the Metasploit's HTA web7 server exploit.	Yes	Yes	Yes
2	Attack scenario using 'Hoaxshell' tool to create PowerShell script that when run on victim gives reverse PowerShell session.	Yes	Yes	Yes
3	Attacker gains access to local admin machine via encoded payload.	Yes	Yes	Yes
4	Attacker gains access to IT admin machine via encoded payload.	Yes	Yes	Yes
5	Attacker requests ticket-granting service tickets of specific SPN, e.g., webserver and extracts these tickets from memory by invoking Rubeus command- Kerberoasting.	Yes	Yes	Yes
6	Attacker requests ticket-granting service tickets of all SPNs and extracts these tickets from memory by invoking Mimikatz command- Kerberoasting.	Yes	Yes	Yes
7	Attacker requests ticket-granting service tickets of all SPNs and	Yes	Yes	Yes

XDR Test Scenario	XDR Attack Scenario Overview	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
	extracts these tickets from memory by invoking PowerView commands.			
8	Attacker elevates the privilege and explores the directories. Finds ntds.dit file.	Yes	Yes	Yes
9	Attacker uses BOF Psc script to enumerate processes with established TCP and RDP connections.	Yes	Yes	Yes
10	Attacker has krbtgt NTLM hash. Attacker then obtains Forged TGT and uses the Pass-the-Ticket technique to gain access to Domain Controller- Golden Ticket	Yes	Yes	Yes
11	Attacker compromises Domain admin, Explores domain controller's C:\. Uploads the powershell beacon payload in DC.	Yes	Yes	Yes
12	Attacker stole DC's NTLM hash. Attacker then obtains Forged TGT service ticket and uses the Pass-the-Ticket technique to gain access to Domain Controller- Silver Ticket.	Yes	Yes	Yes
13	Attacker uses PS-Tools.cna to enumerate processes with established TCP and RDP connections.	Yes	Yes	Yes
14	Attacker uses Enumkit to enumerate IP information, OS architecture and list of installed applications on victim, and AntiForensicsKit to disable Prefetch.	Yes	Yes	Yes
15	Attacker collects the Windows version information and makes registry modification by enabling WDigest Credential Caching.	Yes	Yes	Yes
16	Attacker uses BOF scripts to enable a specific subset of privileges and enumerates system information for Domain Controller.	Yes	Yes	Yes
17	Attacker compromises Domain admin, migrates to another process using sec_inject BOF.	Yes	Yes	Yes

XDR Test Scenario	XDR Attack Scenario Overview	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
18	Attacker uses Detect-Hooks BOF to check the API hooks in place by AV/EDR.	Yes	Yes	Yes
19	Attacker uses 'Hoaxshell' to create PowerShell script that when run on victim gives reverse PowerShell session.	Yes	Yes	Yes
20	Attacker uses 'Villian' tool to create PowerShell script that when run on victim gives reverse PowerShell session.	Yes	Yes	Yes
21	Attacker gets access to domain admin and upload beacon payload to DC, executes the payload and gets the session.	Yes	Yes	Yes
22	Attacker gains foothold on normal user and check a domain for known abusable Kerberos delegation settings using DelegationBOF.	Yes	Yes	Yes
23	Attacker explores the local admin's system and find the network shared drive and copies all files in the local machine.	Yes	Yes	Yes
24	Attacker uses Outflank's BOFs to queries AD for username "derek"; Password sprays by guessing the password for Derek which he find out to be the right one.	Yes	Yes	Yes
25	Attacker uses Outflank's BOFs to enumerate domain information using Active Directory Domain Services from normal user.	Yes	Yes	Yes
26	Attacker explores the process list and then uses Psm BOF script to query detailed information on a specific process id like SentinelAgent.exe.	Yes	Yes	Yes
27	Attacker explores Windows details using Winver BOF and Psw BOF from outflank.	Yes	Yes	Yes
28	Attacker enumerates the user information, processes and domain information using Domaininfo.cna BOF script.	Yes	Yes	Yes

XDR Test Scenario	XDR Attack Scenario Overview	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
29	Attacker uses the tool called WinPeas.ps1 to search for system information, Users information, possible paths for privilege escalation, network information, etc.	Yes	Yes	Yes
30	Attacker checks the user information, drives in the system using wmic, and disables Smartscreen then uses UACBypass BOF script to escalate privilege using uac_fodhelper.	Yes	Yes	Yes
31	Attacker takes advantage of LibreOffice Version 6.1.2.1(x64) Remote Code Execution vulnerability and creates a libre.odt malicious meterpreter reverse tcp payload and send over to victim via email.	Yes	Yes	Yes
32	Attacker takes advantage of LibreOffice Version 6.2.52(x64) Remote Code Execution vulnerability and creates a evilib.odt malicious command shell reverse tcp payload and send over to victim via email.	Yes	Yes	Yes
33	Attacker takes advantage of RAR 5.61 Remote Code Execution vulnerability and creates a mscrar.ace malicious command windows/meterpreter/reverse_tcp and send over to victim via email.	Yes	Yes	Yes
34	Attacker takes advantage of ScareCrow's ELZMA Encryption to encrypt meterpreter Shellcode to bypass AV detection.	Yes	Yes	Yes
35	Attacker takes advantage of ScareCrow's ELZMA Encryption to encrypt meterpreter Shellcode to bypass AV detection.	Yes	Yes	Yes
36	Attacker uses ScareCrow’s ELZMA Encryption to encrypt beacon Shellcode to bypass AV detection.	Yes	Yes	Yes
37	Attacker uses ScareCrow's ELZMA Encryption to encrypt beacon Shellcode to bypass AV detection.	No	No	No

XDR Test Scenario	XDR Attack Scenario Overview	XDR Solution Detection Accuracy	XDR Solution Investigation & Correlation	XDR Solution Response Efficacy
38	Attacker uses shikata_ga_nai encoding 10 times to encode the payload.	Yes	Yes	Yes
39	Attacker uses persistence.cna and persist_assist.cna to add Registry Key persistence as well as Scheduled Task Persistence.	Yes	Yes	Yes
40	Attacker uses ScareCrow's ELZMA Encryption to encrypt beacon Shellcode to bypass AV detection.	Yes	Yes	Yes
41	Developer Philip is using the machine with the name XDR Docker Environment to test out docker containers.	Yes	Yes	Yes

Table 1. AT&T Cybersecurity XDR Attack Scenarios

4 XDR Security Filtering Effectiveness

To protect against these varied 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.[3]

Cybersecurity vendors have responded with solutions that try to map to these frameworks and guidelines, while also attempting to address visibility concerns such as too much data or too little information, a lack of incident prioritization, etc., that are able to effectively detect and contain incidents and provide a response or an action plan for these incidents. XDR solutions primarily were 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, unauthorized access and misuse are underway.

At a minimum, an XDR solution should start logging activity at the beginning of each attack scenario while having the ability to identify Events, which in turn should 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.

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

AT&T Cybersecurity Security Filtering Effectiveness	XDR Solution Event Filtering Scores
Total number of activities logged	4,025,318
Total number of events generated	555
Total number of actionable alerts generated	301
Event Filtering Effectiveness (EFE)	99.98%

Table 2. AT&T Cybersecurity XDR Security Filtering Effectiveness Overview

As shown in Table 2 above, the AT&T Cybersecurity XDR solution recorded more than 4 million activities during the evaluation. The SecureIQLab XDR v1.0 Validation Methodology utilizes 41 enterprise-centric XDR attack scenarios that include a total of 241 attack stages. The AT&T Cybersecurity XDR solution was able to identify and detect 175 of those attack stages, which resulted in it generating a total of 555 events during the evaluation. This gives the AT&T Cybersecurity XDR solution an *Event Filtering Effectiveness* (*EFE*) score of 99.98%, which is exceptional.

Figure 3 provides the method used to calculate the EFE score:

$$EFE = \left(\frac{Total\ Logged\ Activites - Total\ Event - Total\ False\ Positives}{Total\ Logged\ Activities}\right) \times\ 100\%$$

Figure 3. Calculation of Event Filtration Effectiveness (EFE)

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 a total of 301 high-fidelity actionable alerts during the evaluation. These alerts could be used to develop actionable incident management and response metrics. Based on the contextualization provided around the attacks, the suggested attack responses could be initiated by a security administrator or analyst.

The EFE metric is integral to measuring the XDR solution's response effectiveness. 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 AT&T Cybersecurity solution across the 41 XDR attack scenarios.

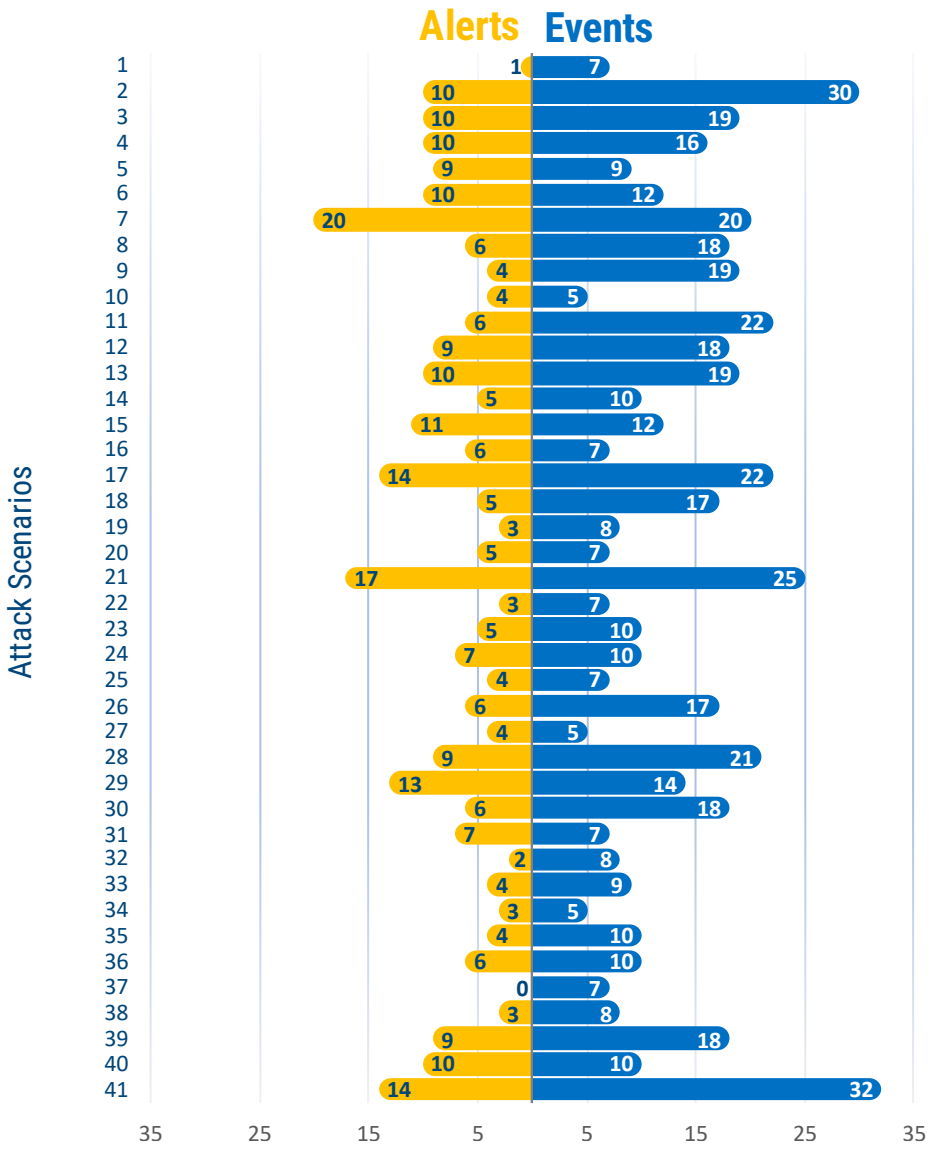


Figure 4. AT&T Cybersecurity XDR Alert and Event Results for Each Scenario

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.

Enterprises therefore should tune this metric based on their own infrastructure and deployment, and according to the risk metrics that they are tracking.

The remediation/response categories broadly outlined below are post-investigation and can be in the form of defined actions that can be automated or semi-automated.

- **Isolate:** Remediate/respond to an event or set of events by isolating the perceived threat(s).
- **Block:** Remediate/respond to an event or set of events by blocking the perceived threat(s).

- **Observe for response:** Remediate/respond to an event or set of events by allowing the perceived threat(s) to run and take a set of actions.
- **Alert:** Remediate/respond to an event or set of events by allowing a human team to take an appropriate set of actions.
- **Orchestration:** Remediate/respond to an event or set of events by handing over the set of actions to the orchestration tool.
- **Firewall:** Remediate/respond to an event or set of events by handing over the set of actions to a firewall, in the event of recurring threats, until a permanent solution is put in place to handle such threats.

5 XDR Operational Accuracy

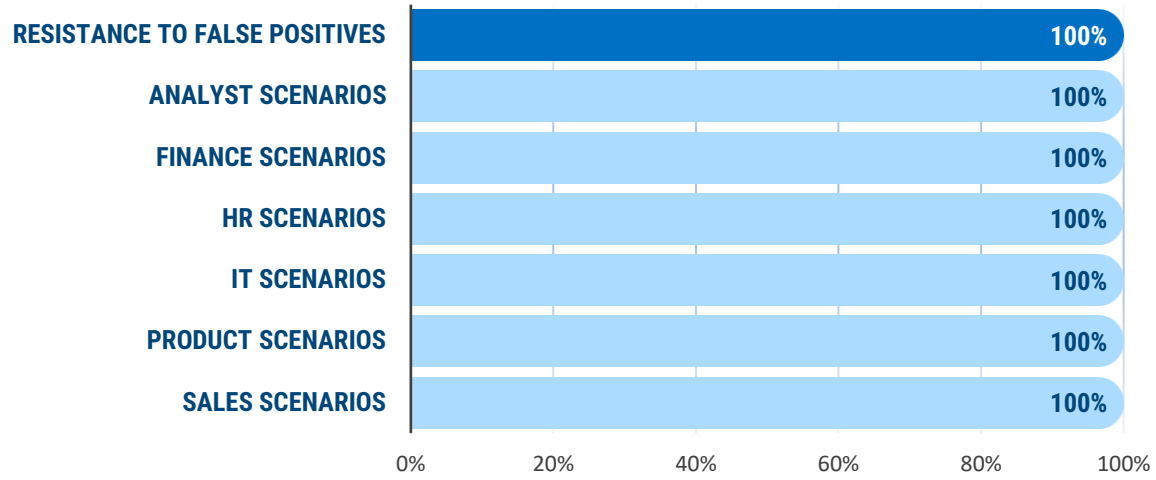


Figure 5. AT&T Cybersecurity XDR Solution Resistance to False Positive Test Results

For the purposes of this test, an XDR solution is considered extremely noisy if it not only reports 100% of malicious threats but also reports legitimate (non-malicious) actions. SecureIQLab employed appropriate tools and techniques to ensure that the AT&T Cybersecurity XDR solution did not raise significant numbers of alerts from end users engaging in legitimate applications and processes. False-positive testing validated the solution's resistance to generating noise for more than 30 real-world scenarios for different enterprise departments, such as human resources and finance, with the results summarized above in Figure 5.

For example, the false-positive testing for the IT scenarios involves the usage of legitimate PowerShell and Command Prompts, while false-positive testing for the sales scenarios focuses on browser usage and downloads. It is important to note that false-positive testing was performed in conjunction with workflow and during all stages of the evaluation to ensure that the XDR solution wasn't heavily biased towards prevention by sacrificing operational accuracy in an enterprise environment.

Additionally, SecureIQLab differentiates between low-importance alarms and false positives. False-positive detections are inaccuracies in the overall XDR attack detection process and occur when a solution wrongly flags benign activities as malicious. Low-importance, low-priority, or informational alerts help accurately detect events that may not pose an immediate risk. Low-importance alarms provide valuable information that may not require immediate action.

6 XDR 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 datapoints 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 AT&T Cybersecurity XDR solution's *Operational Efficiency* metrics are shown in Table 3.

Operational Efficiency Categories	AT&T Cybersecurity XDR Solution Metrics
Time-to-Deploy	2 Hours
Maximum Time-to-Detect (TTD)	≤1 Hour
Maximum Attack Dwell Time	≤1 Hour
Threat Classification Fidelity	87.0%
Threat Correlation Index	50.9%

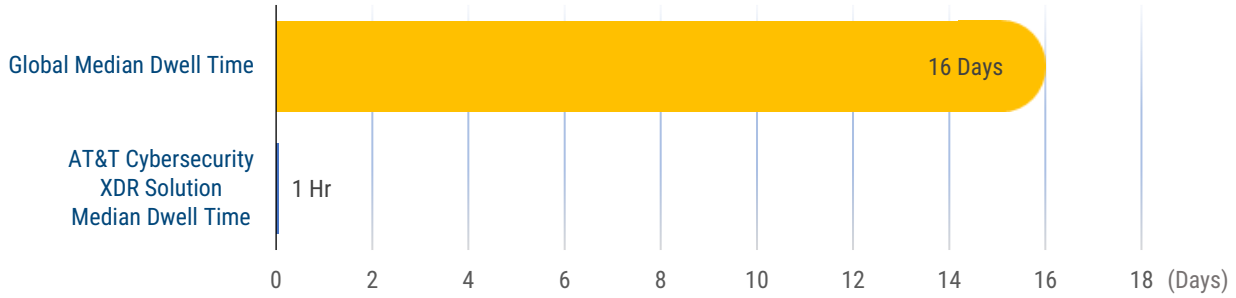
Table 3. AT&T Cybersecurity XDR Operational Efficiency Overview

Operational efficiency was measured using the following factors:

- **Time-to-Deploy**: A low *Time-to-Deploy* is important for enterprises seeking to shorten their time to value for a solution. The AT&T Cybersecurity 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 AT&T Cybersecurity solution during this evaluation.
- **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 AT&T Cybersecurity XDR solution to trigger the initial alert detection. The AT&T Cybersecurity XDR solution had an excellent *Maximum Time-to-Detect* metric of ≤ 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 AT&T Cybersecurity 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 2022, the global median dwell time for an enterprise was 16 days,[4] or more than 380 hours. The AT&T Cybersecurity XDR solution demonstrated a *Maximum Attack Dwell Time* of ≤ 1 hour, giving it a median dwell time ≤1 hour,

[4] M-Trends 2023, Mandiant

which is less than 0.3% of the global median. Figure 6 demonstrates the AT&T Cybersecurity XDR solution's median dwell time as compared to the global median dwell time for an enterprise.



- *Figure 6. Attacker Dwell Time Comparative*

- **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 AT&T Cybersecurity solution achieved a competitive *Threat Classification Fidelity* score of 87%.
- **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 AT&T Cybersecurity solution's *Threat Correlation Index* score of 50.9% demonstrates competence, its threat mapping capabilities can be enhanced to provide further value.

7 AT&T Cybersecurity XDR Solution Deployment Overview

Figure 7 provides an overview of the SecureIQLab Deployment Architecture for the AT&T Cybersecurity USM Anywhere.

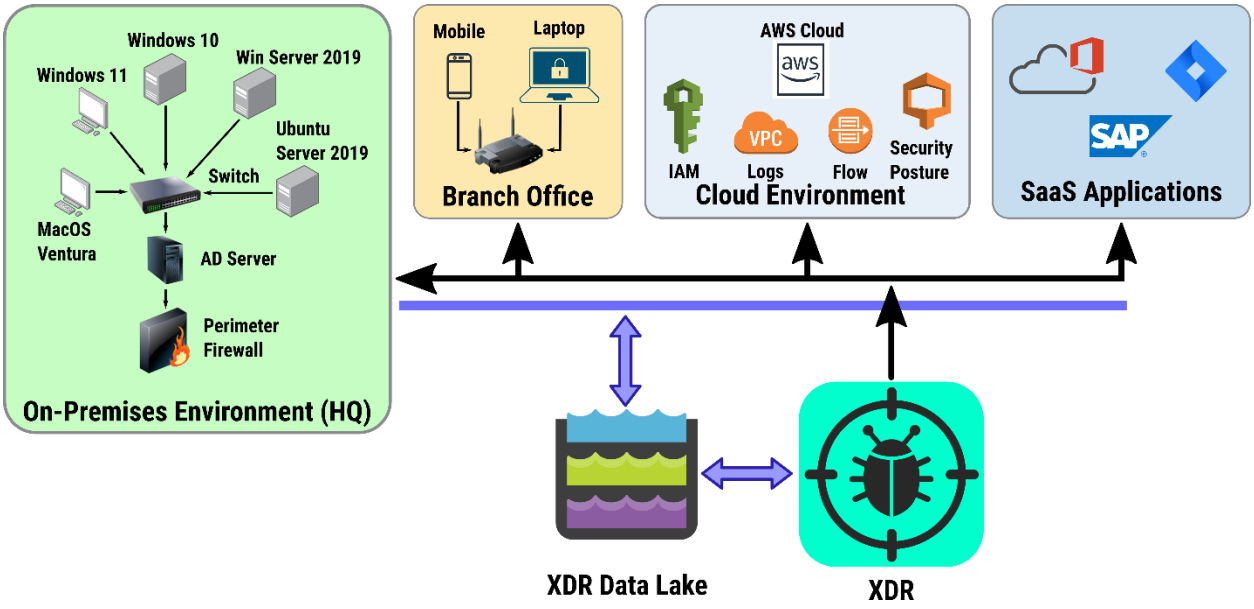


Figure 7. SecureIQLab Deployment Architecture for AT&T Cybersecurity XDR Solution

The AT&T Cybersecurity XDR solution uses the USM Anywhere centralized platform for security monitoring of networks and devices in the cloud, on premises, and in remote locations. Time-to-Deploy measures the total amount of time required to:

- Create a USM Anywhere account
- Deploy the AWS sensor using the AWS CloudFormation template provided by AT&T Cybersecurity to automatically deploy the USM Anywhere platform in the test environment
- Deploy and configure endpoint security and USM Anywhere agents throughout test infrastructure
- Integrate endpoint security, USM Anywhere agents, and existing firewalls with USM Anywhere
- Verify correct deployment, configurations, and integration of security tools with USM Anywhere

8 Conclusion

The core components of the AT&T Cybersecurity XDR solution provide excellent threat detection, investigation, and response (TDIR) capabilities and the solution's *Overall XDR Solution Score* of 96.3% reflects this. Additionally, the complete solution was quick to deploy, configure, and enable.

A key factor in the AT&T Cybersecurity solution's high *Overall XDR Solution Score* is its ability to rapidly identify and detect a threat and display relevant, correlated threat information. A high *Overall XDR Solution Score* results in a solution that is more effective at reducing the active Time-to-Detect. The solution's extended detection capabilities were excellent across the advanced attack scenarios it was validated against. It was highly effective at correlating (and classifying) threats that resulted in actionable alerts (minimizing noise) throughout the test.

Response time is critical for an XDR solution especially when any incident could turn into a breach. A faster time to response lowers the risk of successful compromise. A solution's observation of activities on the system, triggering of an event, and amount of time taken to detect may vary widely depending on its different security capabilities, features and functionality, as well as on how it is configured and the skill level of the security professional or analyst (human user). The AT&T Cybersecurity XDR solution demonstrated highly effective and efficient detection and response capabilities.

Effective asset management is another factor essential for reducing response time and containing an incident. The AT&T Cybersecurity XDR solution achieved an exceptional *Overall Incident Response Score* of 97.6% with actionable alerts.

The AT&T Cybersecurity XDR solution demonstrated broad compliance management, risk assessment and mitigation capabilities. It also provided comprehensive integration of detection and response data, and enhanced security metrics reporting capabilities.

9 Contact Information

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

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

10 Copyright and Disclaimer

SecureIQLab (January 2024)