Extended Detection and Response (XDR) CyberRisk Validation Methodology

Version: 1.0

Last Revision 20 September 2023

Language: English

www.secureiqlab.com

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the "Standard"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.4]. SecureIQLab is solely responsible for the content of this Test Plan.

Contents:

1 INTRODUCTION

This validation methodology contains the testing standards for Extended Detection and Response (XDR) solutions. XDR solutions are a form of comprehensive threat detection, investigation, and incident response solution (TDIR).

The difficulty and complexity of effective TDIR is a challenge that modern enterprises grapple with. A lack of integrated security measures across an entire network, system, or infrastructure leads to increased difficulty and complexity in designing and deploying a comprehensive solution for threat detection, investigation, and incident response.

This is a mounting challenge for many modern enterprises. As a result, enterprises find it difficult to enforce uniform and consistent security measures. These security measures include activities such as addressing vulnerabilities and threats by streamlining management processes, improving visibility, and simplifying security operations. All in order to combat a multi-vector attack surface, which is exponentially evolving with the prevalence of advanced and persistent threats.

The mobility and dispersion of the modern workforce have compelled solutions to evolve towards threat detection and investigation-based solutions that are easier to manage and monitor. These solutions include endpoint detection and response (EDR), vulnerability management systems, security information and event management (SIEM), and security orchestration and automated response (SOAR).

Extended Detection and Response (XDR) solutions were primarily born to address some of the key challenges highlighted above while providing relevant alerts, reducing noise and facilitating incident responses when cyberattacks, unauthorized access and misuse are underway.

Omdia[1] defines XDR as an enterprise-grade, unified TDIR solution that offers a guided human-analyst experience across the entire lifecycle—from telemetry gathering and analysis to alerting and investigation—to remediation-response, validation, and process improvement. XDR breaks down the siloed approach with a single, unified system to manage the entire TDIR lifecycle, including key activities across essential IT estate regions encompassing endpoints, networks, and cloud environments.

SecureIQLab expands upon this premise of XDR to also include the unification of telemetry from a multitude of security technologies through automated or semi-automated means to minimize the alert noise and focus on delivering actionable intelligence to end users.

1.1 THE NEED FOR XDR

Enterprises are being targeted by individuals, state sponsored actors, and other criminal organizations. These attackers have different motivations and objectives. They range from financial gain (Black hole Exploit Kit, Zeus Trojan), information sabotage or espionage (Wiper), activism (Defacing web content), and state sponsored cyber-terrorism (Black Energy Trojan, Ukraine electricity grid). To defend against these cyber threats, organizations working with the cyber security community have come up with National and International Frameworks (such as NIST's

[1] https://omdia.tech.informa.com/about/about-us

©SecureIQLab LLC, 2023. All rights reserved.

Identify, Protect, Detect, Respond, Recover) that have helped define these cybersecurity guidelines around such attacks.

Cyber security 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 is a solution that attempts to address all of these issues within the realm of an organization's infrastructure, while providing dynamic insights into emerging and existing threats.

SecureIQLab will be validating XDR solutions based on the solutions ability to manage the TDIR lifecycle from start to finish, while ensuring threat detection data is unified across endpoints, networks, cloud environments, and beyond. It is imperative that each XDR solution's critical insights and context are not lost as investigations move across multiple toolsets; and that the same solution that provides the data and detects the threat, actually conducts the remediation–response action, making sure the resolution effort is successful, and lessons learned are cycled back in to improve the process.

1.2 XDR Feature Highlights

Here are some of the key feature highlights of an XDR solution that will be validated in the context of this methodology, whether the XDR solution:

- Provides holistic threat identification and detection capabilities in a unified and normalized format.
- Provides a comprehensive and contextual defense posture sourced across multiple attack surfaces, leveraging one or more cybersecurity solutions while aggregating, storing, and analyzing real-time structured and unstructured data, threats, and incidents.
- Provides a "Single pane of Glass (SPOG)" across the entire TDIR lifecycle with integrated configuration and management capabilities.
- Provides rapid investigation and remediation response (within 60 secs) in the form of actions if the assessment warrants such behavior.
- Provides return on security investment over time.
- Streamlined incident response workflow.

One can easily surmise from the plethora of XDR features highlighted that XDR is not a single product. In creating categories, SecureIQLab evaluated the current cyber security XDR vendor landscape and conducted consultations with large, medium, and small enterprises.

Consequently, SecureIQLab classifies the XDR solutions in 2 major categories, (1) comprehensive XDR and (2) open XDR (open system XDR stack). Comprehensive XDR is an all-in-one single-vendor technology platform-based architecture with the ability to execute TDIR activities across, at a minimum, endpoints, networks, and cloud environments, within a singular ecosystem. In contrast, open XDR is typically composed of multiple best-of-breed point solutions within a singular eco-system-based XDR architecture with strong integration and interoperability.

The scope of this iteration of the test will be limited to comprehensive XDR, either with a single vendor technology or multi-vendor integrated security stack available through a common marketplace.

©SecureIQLab LLC, 2023. All rights reserved.

1.3 Objective of the XDR CyberRisk Methodology

The XDR test focuses on providing empirically validated data and metrics around security, compliance, and operational capabilities. These criteria were selected with the objective of creating test results that demonstrate the tested XDR solution's ability to identify, detect, and quickly remediate/respond to incidents along with the possibility of mapping XDR solution capabilities to industry guidelines, such as NIST framework, MITRE, and Lockheed, while securing the organizational network, user, application.

It is imperative to note that some of these frameworks are primarily threat-centric in nature and thus do not address all of the use cases, various enterprise workflows in different scenarios, or XDR solutions.

Key differentiating factor

Enterprises struggle to generate actionable strategies from threat-centric tests to reduce their true operational risk. To help enterprises gain actionable information towards lowering risk, this test methodology incorporates another industry standard; the attacker-centric "Cyber Kill Chain Model". The Cyber Kill Chain Model is useful because it provides a defense model perspective. Combining the MITRE ATT&CK framework with the Cyber Kill Chain Model draws from each of the strengths of these industry standards to effectively measure a product's attack detection capabilities to reduce operational risk, a key differentiating aspect of this methodology.

1.4 XDR Security Efficacy Metrics

SecureIQLab's objective for the XDR test methodology is to determine how well XDR solutions perform. In the following areas:

Identification and Detection Features

An XDR should have the ability to identify and provide basic detection of threats. Basic detection must be applicable to individual assets and their associated inter-connected devices. XDR solutions should include an endpoint, a network security solution, and a cloud-based security or analytics component. Basic detection by an XDR solution should provide at least the following information to qualify for a comprehensive XDR evaluation.

Basic Detection

The following illustrates what SecureIQLab defines as "Basic Detection" in the context of an XDR solution or a component within its technology stack:

- Ability to identify threats, contextualize the threats around the attack surface and vector within a specified timeline, and the resulting impact and intent.
- Should a vendor fail basic detection tests, they will be advised to add the missing feature(s) and retest. Otherwise, the vendor will not be qualified for inclusion in the test.

Enhanced detection

Enhanced detection is defined as the combination of basic detection artifacts from one or more individual security components making up the XDR solution, and the ability to provide automated or semi-automated response capabilities.

©SecureIQLab LLC, 2023. All rights reserved.

Extended detection

Extended detection requires the ability to combine enhanced detection with human expertise and external resources (such as IOC, IOA, ML etc..) to provide information beyond what is currently done and provide the required orchestration and response. This is highly important in dealing with threats that are difficult to identify and quantified by the security technology alone.

Apart from detecting and reporting the above-mentioned metrics on how the attacker is trying to attack and compromise the network, additional scenarios will be evaluated in this methodology wherein the attacker(s) has already infiltrated the organization's network. The attacker(s) can further act as:

- Passive Attacker: Perform reconnaissance, gather intelligence about the organization, and pass information to the other attacker(s) [insider threat scenario].
- Active Attacker: fingerprints and models assets, sets up decoys, and gains persistence. The attacker(s) may choose to use malicious code, malicious hardware, or backdoored functions.

Remediation/Response

Remediation/response is the ability to react to an event or act on it. In the context of XDR, response means reaction to an event that XDR is designed to defend against. The speed of response around threats is equally important as it determines how quickly an XDR solution can orchestrate with other systems to act on an attacker or an incident. Response time should be 60 seconds or less. The remediation/response outlined here is a post-investigation remediation response.

Orchestration can come in the form of defined actions that can be automated or semi-automated and can be broadly classified into a few example categories below.

- Remediate/respond to an event or set of events by isolating the perceived threat(s).
- Remediate/respond to an event or set of events by blocking the perceived threat(s).
- Remediate/respond to an event or set of events by allowing the perceived threat(s) to run and take a set of actions.
- Remediate/respond to an event or set of events by allowing a human team to take an appropriate set of actions.
- Remediate/respond to an event or set of events by handing over the set of actions to the orchestration tool and letting orchestration handle the response.
- 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.

1.5 XDR Vendor Participation Selection Criteria

We select vendors based on three following criteria:

1. Market Leaders – In terms of revenue generated, customer numbers globally, or strong channel play.
2. Analyst and Enterprise challengers – Small-mid-large enterprise security professional surveys, direct 1:1 inquiries and engagement with enterprises, organizations, MSP's, MSSP's, Omdia Universe reports, Gartner Magic Quadrant, Gartner's buyers guide, Forrester Wave, and IDC reports.
3. New market entrants and interested participating vendors with breakthrough technology offerings.

There are no known conflicts of interest.

©SecureIQLab LLC, 2023. All rights reserved.

1.6 Scope and targeted XDR vendor List

The scope of this iteration of the test will be limited to comprehensive XDR either with a single vendor technology or multi-vendor integrated security stack available through a common marketplace. These solutions should cover at a minimum: endpoints, networks, and cloud environments within the context of the XDR. These can be XDR security solutions that are available in the cloud marketplace, SaaS offerings, or standalone cloud offerings such as XDR-as-a-service.

Any hardware-based XDR security solutions/product appliances are out of the scope of this methodology.

Below is the alphabetized list of considered vendors at the time of this publication:

- AT&T
- Bitdefender
- BlackBerry Cylance
- Broadcom Symantec
- Check Point
- Cisco
- CrowdStrike
- Cybereason
- Cynet
- Elastic
- ESET
- ExtraHop
- Fidelis Cybersecurity
- Fortinet
- Hillstone Networks
- Microsoft
- Palo Alto Networks
- Qualys
- Red Piranha
- ReliaQuest
- Secureworks
- SentinelOne
- Sophos
- Stellar Cyber
- Trellix
- Trend Micro
- Uptycs
- VMware Carbon Black XDR
- WatchGuard

1.7 Funding Agreement

This is a non-commissioned test that follows AMTSO standards and guidelines which are publicly transparent to everyone. This test effort is funded by SecureIQLab.

©SecureIQLab LLC, 2023. All rights reserved.

1.8 Opt-Out Policy

Opt-Out: Opt-out will only be considered for the following reasons:

1. The product, solution (or) technology is found to be outside the scope in the context of the methodology as determined by SecureIQLab.
2. Any technology, product or a solution that is NOT generally available nor ready for deployment.
3. Publishing the test would not serve the public interests as deemed by SecureIQLab.

Opt-out requests must be provided in writing. Emailed opt-outs must be sent to info@secureiqlab.com. Mailed opt-outs must be sent to:

SecureIQLab LLC
9600 Great Hills Drive
Suite 150W
Austin, TX 78759

Mailed opt-outs are effective by the date received, not the date postmarked. SecureIQLab does not accept opt-outs through phone, voice, social media, etc.

The opt-out must contain the name, title, email, and phone number of the individual authorized to request an opt-out on behalf of the vendor. To be considered a completed opt-out, the request must state under which of the reasons above the request should be considered and provide details to support the request. All vendors have a limited right to opt-out for the designated reasons listed above. The opt out period begins at *Test Commencement* and continues through the end of the *Dispute Phase [Section 5]*. Vendors will be contacted by SecureIQLab within 3 business days of receiving an opt-out request to discuss feasibility. If a vendor successfully opts out before the end of the *Configuration Phase*, the vendor will be listed as 'Participant, not tested '. If a vendor successfully opts out after testing has been performed for their product, their product will be marked in the results 'Participant tested, not published '.

2 General Evaluation Approach

The aim of this section is to verify that the XDR security solution/product referred here as the XDR product under test (PUT) can detect and respond to attack attempts, while remaining resistant to false positives.

The PUT will be configured either by understanding the underlying applications, e-commerce and other sites that utilize XDR framework as relevant (automatically, or manually) or by creating rulesets and a security policy manually. The appropriate deployment model will be chosen per vendor recommendations when available, and the PUT will be deployed to protect against attacks that target the potential protected assets.

2.1 XDR Effectiveness Validation

SecureIQLab will evaluate the security effectiveness of the XDR PUT using the following approaches:

- Blackbox Security Testing - Blackbox testing uses attacks that are performed without any understanding of the test environment.
- Greybox Security Testing – Greybox testing uses attacks that assume some reconnaissance of the environment.

©SecureIQLab LLC, 2023. All rights reserved.

The combination of these two test processes covers both automated or opportunistic attacks and targeted attacks to simulate real-world threat scenarios.

Each of the categories above will consist of the following validation tasks:

2.1.1 Information Gathering and XDR solution Reconnaissance

Information gathering and reconnaissance will be performed against the application to gather as much information as possible. This information will be utilized when penetrating the target during the vulnerability assessment and exploitation phases. SecureIQLab will perform vulnerability analysis using automated tools such as Burpsuite, Nessus and performing manual analysis. The main objective of vulnerability analysis is to discover flaws in systems and applications that can be leveraged by an attacker. These flaws can range anywhere from host and service misconfigurations to insecure application design. Vulnerability analysis will be based on:

- Active Scan: Active scan involves direct interaction with the component being tested for security vulnerabilities.
- Passive Scan: Passive scan involves meta-data analysis and traffic monitoring.

2.1.2 Exploitation

Once information gathering and reconnaissance is completed, exploitation is the next phase in this process. Exploitation involves leveraging the vulnerability information gathered through reconnaissance to gain a foothold within the targeted environment.

2.1.3 Post Exploitation

The term “post-exploitation” refers to the actions taken after the initial compromise of a system or device. It often describes the methodical approach employing privilege escalation or pivoting techniques. This allows the tester to gain additional access to systems or network resources by attacking from a new vantage point within the system. We will demonstrate the risk presented by exploitable systems and what post-exploitation may likely occur with web applications.

2.2 XDR Test Life Cycle

The XDR test plan is within scope if the project remains within six weeks of the timeline below. This methodology is open for feedback and updates until the 15th of September 2023.

SecureIQLab will execute the test in three phases:

1. **Phase 1: Detecting and Investigating Threats.**

   As a part of this step, we will evaluate XDR solution’s ability to detect and investigate threats, while accurately recording them from all the earlier phases of testing.

2. **Phase 2: Threat Response**

   As a part of this step, we will evaluate XDR solution’s ability to respond to threats that stem from Phase 1.

©SecureIQLab LLC, 2023. All rights reserved.

3. Phase 3: Post Assessment Phase

We will review, assess, and document the discovered vulnerabilities and issues, tabulate the scorecard, and prepare the final report.

SecureIQLab will execute the project in six stages, that are listed in table format below:

Schedule Summary for Test Project			
Stage Index	**Test Activity**	**Date Range**	**Dependencies**
1	*Test Commencement*	*October 27th, 2023*	*Vendor Voluntary participation (or) procurement of vendor Software*
2	*Confirm Vendor Configuration Feedback*	*November 10th, 2023*	*All required vendor XDR solutions installed, and testing commences*
3	*Milestone 1 – Preliminary Results*	*November 17th, 2023*	*Vendor confirmation and validation*
4	*Milestone 2 – Test Scorecard First Edition – End of Testing Period*	*December 18th, 2023*	*Based on preliminary result disputes and resolution*
5	*Feedback and Dispute Resolution Time – Retests as Needed*	*December 18th, 2023 – January 5th, 2024*	*Based on report feedback and final dispute resolution*
6	*Milestone 3 – Issue Final Report – End Date for Test*	*December 18th, 2023 – January 22nd, 2024*	*Based on retesting or testing period extended*

No additional risks are known at this time.

2.3 PROPOSED ATTACK TYPES

Testing will demonstrate the effectiveness of the product under test (PUT) at protecting assets from targeted threats and exploitation. This asset/target and threat-based approach form the basis from which PUT security efficacy is measured.

Attack types and test configuration: The SecureIQLab attack types consist of simulation of real-world threat scenarios. Threats introduced in these scenarios are primarily the manifestation of issues caused by bad programming practices, software vulnerabilities, malicious insider, etc. Also, a considerable amount of threat intel

©SecureIQLab LLC, 2023. All rights reserved.

is generated by SecureIQLab's threat research team.

SecureIQLab includes attacks that have a definite outcome i.e., an attacker establishing a reverse connection, file uploads and proof of concept (PoC) attacks are part of the test set. This ensures that the XDR solution's ability is stress tested for outcome-based tests.

2.4 Attack Relevance

SecureIQLab will use and craft attacks that are relevant to applications hosted in the cloud, including cloud native applications. SecureIQLab carefully curates such attacks via research generated by SecureIQLab's own red team, as well as the attacks that are prevalent in the wild. Open-source tool kits are also utilized while performing this assessment.

2.5 Geo-Limitations

While performing web application attacks, SecureIQLab will make every effort to use only attacks that are not geo-location centric when necessary. SecureIQLab will ensure that attacks originate from a wide range of IP addresses.

2.6 Distribution of Test Data

Upon the completion of the six phases of this validation project, the resulting data will be organized into individual test reports and one comparative report. These results will then be publicly available to download at https://secureiqlab.com/publications/.

2.7 XDR Time to Deploy and Detect

XDR solutions are expected to be easier to deploy and manage via a cloud console or a management interface. The ability of the XDR solution to rapidly identify and detect a threat and display relevant information is a very important factor. This can include identifying and detecting primary attack vectors (Web, SMB, applications etc.) and secondary attack vectors that are typically used for lateral movement. The faster the XDR can detect a threat and report the relevant information, the sooner the attack can be stopped, and the sooner any damage can be remediated.

Time-to-deploy (TTD) will be measured from the time it takes to deploy the XDR solution successfully to the point-of-time the XDR is able to detect, record and report on threats or incidents-based events.

Time-to-detect (TTD) will be measured from the time an unknown threat isn't detected to the time it is detected by the XDR solution.

SecureIQLab will report the overall Time-to-deploy the XDR solution and the Time-to-detect threats including the ones that are missed for each tested XDR solution.

©SecureIQLab LLC, 2023. All rights reserved.

2.8 XDR Threat Classification

Not all threats are of equal severity. The ability to classify attacks according to the risk each one poses is an important feature of an XDR solution. While a reduction in TTD measures the time to detect an incident(s), threat classification gives the users the ability to understand the nature and severity of a threat based on additional research and classification.

If there is a specific threat classification methodology or framework used by the vendor's XDR product, it is best that the vendor discusses this and works with SecureIQLab on those details during the initial deployment and configuration phase. This will allow SecureIQLab to map the workflow outcomes to the appropriate threat classification metrics.

3 Control Procedures

Before any test is conducted, SecureIQLab ensures that the XDR solution under test has been validated in the following areas:

- Connection Validation:
  - The XDR solution under test must be accessible by the administrator.
  - The XDR solution must pass normal application traffic.
- Logging:
  - Verify that logs are being generated and recorded. Participating vendors are granted access to test logs through the time of publication.
- Updates:
  - Protocol updates in the form of rules, signatures and reputations will be applied as they become generally available. SecureIQLab will make a best effort to apply these updates to the products prior to the evaluation.

- Closed XDR solution-based testing:

  - Intermittent chaos inside the closed system is generated from within the solution architecture. Such chaos can be caused by operating system updates, apt-get and chocolatey based installations that could be viewed as objects introducing chaos inside the closed XDR solution-based architecture. SecureIQLab will be validating these types of test activities along the following lines,
    - Is the privacy of the user impacted during this activity period?
    - Is this activity occurring based on explicit consent or without consent?
    - Does the activity give consent for all other activities and its dependencies combined?

4 Vendor Participant actions: Setup and configuration

Participating vendors are invited to be actively involved in the setup during the testing process. This process includes:

Setup

©SecureIQLab LLC, 2023. All rights reserved.

- Default configuration. Given the nature of test environments, some tuning may be required. Participating vendors are invited to review XDR deployment to align with default and publicly recommended configurations. Tested XDR vendor's solution will be configured per default configuration and use publicly available recommendations if any additional tuning is required for test harness compatibility.
- Every vendor is invited to configure their own product, or review the configuration of their product, to ensure that the deployment aligns with their default configuration that businesses are able to implement when deploying the firewall in their organizations. The firewall configurations will include multiple security and compliance applications—URL filtering, anti-malware, advanced threat protection, vulnerability protection, firewall policy enforcement, data loss prevention and cloud application security.
- If there are workflows mentioned in this methodology that require specific configuration changes and/or options, vendors are responsible to provide publicly available documentation of these best practices. If there are any concerns with certain workflows, it is best that the respective vendor discusses these with SecureIQLab, and work with us on these options during the initial setup and baselining phase.

5 SCORING AND DISPUTE PROCESS

For all detected attacks, SecureIQLab will give the detection credit to the XDR solution under test. Multiple packet capture tools will validate test results.

If any inconsistencies exist between SecureIQLab's test data capture tools and the vendor's test data tool, SecureIQLab will default to the vendor test tool's captured data as long as it provides sufficient evidence that their captures are accurate. In such cases no credit will be given for missed attacks and there is no negative scoring for attacks/threats missed by the XDR solution. The outcome of the attacks combined with the logging of the attacks and the quality of information highlighted will be used for scoring purposes.

SecureIQLab will follow industry norms and best practices to handle any disputes, especially on the nature and validity of the attacks used during the testing window and will make best efforts to analytically resolve disputes regarding scoring.

Any changes to scoring resulting from disputes will be applied to all vendor results, and not just to the disputing vendor.

All XDR vendors who participate in this test will receive their score. This will include a breakdown of security efficacy and operational efficiency scores. This data set will be shared individually with the XDR vendors and SecureIQLab will work closely with XDR vendors to go over the metrics as well as relevant metadata when warranted. Furthermore, SecureIQLab reserves the right NOT share some types of missed attacks (such as certain types of web-attacks) that are missed during the testing window to third parties unless required by law.

SecureIQLab will provide vendors with up to two weeks for dispute resolution on the nature of attacks. Any security vulnerabilities that are uncovered during the testing windows related to the XDR solution under test will be shared based upon responsible disclosure policy.

XDR Vendors will be provided up to 20 days to fix the vulnerability. Vulnerability details will be disclosed to the broader public when a fix is available, or if SecureIQLab determines that earlier disclosure is in the best interest of

©SecureIQLab LLC, 2023. All rights reserved.

the public. In rare cases 20 days may not be enough time to properly fix a vulnerability, in which case SecureIQLab retains the right to provide additional time on a case-by-case basis.

SecureIQLab reserves the right to change scores as a result of disputes or changes to scoring after the Comparative and Individual Test reports have been published.

6 Threat Triage

Classifying threats according to how they will be resolved helps enterprises respond to attacks in a fast and meaningful approach. Rather than dealing with each threat individually, the admin can potentially resolve several similar threats together, thus saving time and resources.

7 Threat Timeline

Advanced attacks typically take place over an extended period. To understand the nature of a threat, it is necessary to find out which actions took place at what time. Hence, it is important to have a detailed timeline of how each attack has progressed from its initial stages to completion, along with any relevant IOAs or IOCs along the way.

8 Return on Security Investment Metrics

Implementation of XDR solutions can be an expensive process, when factoring in the cost of the product, the amount of time to deploy the solution, and maintenance and personnel expenditures. These factors should be considered when evaluating any security product.

Return on Security Investment (ROSI) is a financial metric used to measure the effectiveness and value of an organization's security investment. The ROSI of a product is derived from its security effectiveness, operational efficiency, ability to avoid false positives, pricing, and the cost of failure to secure assets.

9 SecureIQLab Comprehensive XDR Test Setup

Based on feedback from enterprise clients, SecureIQLab has developed the following enterprise environments with heterogeneous requirements. While this test setup may not encompass the needs of all existing enterprise networks, they represent a common viable standard for all enterprise class XDR solutions, it may be endpoint centric, virtual, or cloud-based and are universally applicable.

SecureIQLab used industry leading test tools, scripts, and databases to provide the most robust, comprehensive, and realistic testing environment possible. The XDR solutions were configured to identify and detect every security related category available within its administrative console and to use all available defenses.

The test setup can be best summarized by the following diagram in Figure 1.

©SecureIQLab LLC, 2023. All rights reserved.

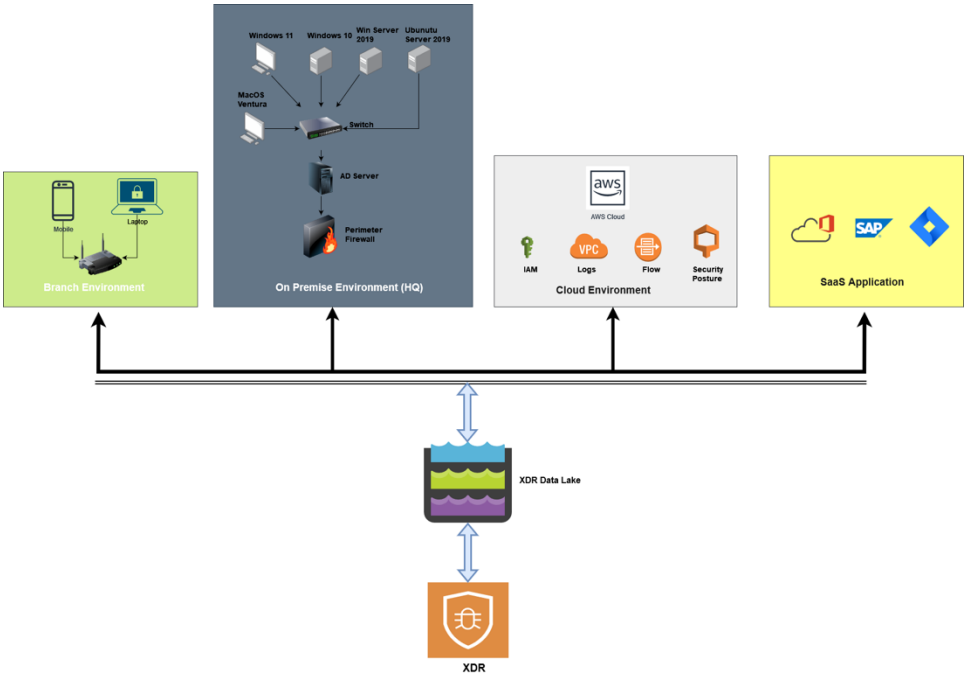

Figure 1. Extended Detection & Response Test Environment

The advanced capabilities of an XDR solution should be able to immediately identify the threat and correlate it with its communications to the attackers in real time.

The analyst workflow will be triggered by an attack based on methods such as the Lockheed Martin Cyber Kill Chain wherever applicable. Given the nature of test environments, some tuning may be required. Participating vendors are invited to review their XDR deployment to align with default and publicly recommended configurations. Test subject vendors will be configured per default configuration and use publicly available recommendations if any additional tuning is required for test harness compatibility.

10 Extended Detection Response Operational Efficiency

XDR Solution operational efficiency refers to the security efficacy and efficiency that an XDR solution can provide security to an organization's cloud infrastructure while minimizing operational costs and complexity.

Operational efficiency in the context of XDR solutions will be measured on the following key areas:

- **Security Policy Configuration:** This helps in the understanding of the environment that organizations are working on, specifically the different persona categories and types deploying, managing, or monitoring the XDR solution with vendor recommended configuration.
- **Security Policy Configuration-Ongoing**: The is the ability to deploy, maintain, change, and monitor the shift in policy over time. This is a very critical aspect of day-to-day XDR operations.
- **Asset Management:** This refers to the ability of the XDR to provide effective visibility and control over the assets that are detected by the XDR.
- **Incident Management:** This refers to the ease with which XDR can be for activity, identify and detect the existence of a security threat followed by a defined mitigation process against it.

©SecureIQLab LLC, 2023. All rights reserved.

- **Compliance Management:** This refers to the ease with which the XDR can be monitored for activity, identify, and detect lack of compliance followed by a process to manage it.
- **Business Continuity Management:** This in the context of XDR solution refers to how services are restored during and post attack or a disaster.
- **Risk Assessment & Mitigation:** The process for understanding risks and the ability to reduce or mitigate them completely from the XDR solution.
- **Security Metrics Reporting:** This is a metric to validate if the XDR solution has sufficient logging and documentation around security events that are reported with the right timeline and context.
- **Configuration and Policy Backup and Restoration:** This refers to the ability of the XDR to consistently backup configuration and policy parameters and be able to restore on-demand.

11 Reporting Capability

Admins should also be able to use the XDR systems to review past incidents and the action taken at the time to decide if the same actions are applicable to the current threat. While providing maximum flexibility to senior analysts, the XDR should support predefined but configurable workflows for less experienced personnel, who may be assigned specific tasks during an investigation.

An XDR platform should have the ability to unify data. That is to say, bring together information from disparate sources, and present it all within its own user interface (UI) as a coherent picture of the situation. Technical integration with the operating system and third-party applications (syslog, Splunk, SIEM or via API) is an important part of this.

12 Operational Accuracy Test

A security product that reports 100% of malicious attacks, but also reports legitimate (non-malicious) actions, can be disruptive and/or noisy. SecureIQLab will use appropriate tools and techniques to ensure that the validated XDR solutions do not raise a significant number of alerts with legitimate applications and processes. This section of the methodology will be performed in conjunction with security efficacy, resiliency and compliance *Workflows* and other independent methodology sections where possible. This will ensure that the XDR products aren't heavily biased towards detection by sacrificing operation accuracy in an enterprise environment.

13 Attestations

I understand and agree that I am submitting this test plan, and the following attestations on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entities to these attestations. All references to "I" or "me" or similar language refer to such an entity. I represent and warrant that the following attestations are true to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

I will provide public notification on the AMTSO website covering my obligation for notification of a public test, regardless of whether a potential Participant is in actual receipt of such notification prior to the commencement date of a test.

All products included in this test will be analyzed fairly and equally.

©SecureIQLab LLC, 2023. All rights reserved.

I will disclose any anticipated or known imbalance or inequity in the test design to all participants in the test.

Although I may charge for participation in a test, I will not charge any additional fees for a vendor to be a test subject under the standards.

I will disclose any material conflicts of interest or other information that could materially impact the reliability of the test.

I will disclose how the test was funded.

I hereby affirm, to the best of my knowledge and belief that this test plan complies with the AMTSO testing standards, as of the date hereof.

Signature: /s/ David Ellis
Name: David Ellis
Test Lab: SecureIQLab
AMTSO Test ID:
AMTSO-LS1-TP089

14 APPENDIX

Proposed Cloud Infrastructure: AWS, Azure, Digital Ocean.

Proposed Communication Provider: ATT.

Proposed Attacker Tool(s): Cobalt Strike, Metasploit, and Raspberry Pie.

Proposed Application: Windows (7-12), Windows Server (2012-2022), Ubuntu LTS 16-20, and Netgear Router.

Proposed physical hardware: Supermicro, Netgear, Dell latitude series laptops, and IoT coffee mug.

14.1 DOCUMENT REVISIONS

Version	Section(s)	Revision overview
V0.95	All	Typos corrected, layout improved, and minor clarifications made throughout document.
V0.95	1.2 and 1.6	Scope of methodology expanded to include multi-vendor integrated security stack available through a common marketplace.
V0.95	1.6	Scope of Vendors list updated to reflect changes in market and methodology scope.
V0.95	2.2	XDR test life cycle reduced from seven phases to three and updated timeline.
V0.95	2.7 and 2.8	Changed to section 2.7 and 2.8 respectfully after the removal of the previous section 2.7.
V0.95	2.8	XDR threat classification simplified with removal of threat classification categories.
V0.95	3, 13 and 14	Compliance, Resiliency, and Operational Accuracy Test sections removed and remaining sections incremented accordingly
V0.95	14.1	Document Revisions section added
V1.0	13	AMTSO Test ID updated

©SecureIQLab LLC, 2023. All rights reserved.

COPYRIGHT AND DISCLAIMER

Copyright © 2023 SecureIQLab, LLC. All rights reserved. The content of this report is protected by United States and international copyright laws and treaties. You may only use this report for your personal, non-commercial, informational purposes. Without SecureIQLab's prior written consent, you may not: (i) reproduce, modify, adapt, create derivative works from, publicly perform, publicly display, or distribute this report; or (ii) use this report, the SecureIQLab name, or any SecureIQLab trademark or logo as part of any marketing, promotion or sales activities. 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.

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (September 2023)