SecureIQLab®

Cloud Web Application Firewall (WAF) and Application Programming Interface CyberRisk Validation Methodology

Version:	**3.0**
Last Revision:	**14 December 2023**
Language:	**English**

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

1.1 THE NEED FOR WEB APPLICATION FIREWALLS AND APPLICATION PROGRAMMING INTERFACE PROTECTION

Attackers have adapted to exploiting the changing landscape of remote workforce environments, where businesses must open up more surfaces to meet growing business demands. No longer solely targeting web servers and their underlying operating systems, attackers now focus on exploiting web applications running on these servers that interface with critical corporate data. Even minor code mistakes can make these apps vulnerable to remote exploits. Web application hacking was the top action vector for incidents and breaches in 2022 (DBIR Verizon, 2022).

The Web Application Firewall (WAF) remains the most frequently used security control to protect web applications (84%). The global web application firewall market size was valued at $3.9 billion in 2020, and is projected to reach $25.6 billion by 2030, growing at a Compound Annual Growth Rate (CAGR) of 20.88% from 2021 to 2030. (Allied Market Research 2022).

There are elements that the WAF does not protect. The application programming interface is the mechanism that provides a level of abstraction. This abstraction is usually required by programmers to make applications function properly. This trend of abstraction has given birth to the application programming interface (API) security space. The API security space helps overcome the internal traffic visibility that is outside the scope of pure WAF protection. As a result, WAF-based and API-based protection technologies work hand in hand to secure both the internal and external traffic, thus giving rise to WAAP.

Omdia is a research group that assesses technology trends. Writing for Omdia, senior principal analyst Rik Turner states: “The trend for multiple defensive functions to be delivered as services and, crucially, to be offered by a single provider, whether to secure the development pipeline or the application runtime, is a positive one. There is the commercial simplification of being able to go to a 'one-stop shop' for all your application security needs. For runtime security, threat intelligence can be gathered at a common backend, benefiting all the disparate application security services the provider offers.”[1]

To counter such attacks, enterprises must in turn evolve their network defenses to provide a different kind of protection. Web application firewalls (WAF) exist to prevent web servers and their applications from being exploited.

On-premises deployment helps WAAP discover internal APIs.

Why cloud based WAF’s are on the rise:

- Certain government and industry regulations, such as PCI DSS, require WAF deployment for compliance.
- 95.1% of the enterprise based WAF controls are deployed in the cloud today.
- Enterprises report 49% of their workloads are in public cloud with plans to expand workloads in cloud by 6% in the next twelve months. (Flexera 2022)

[1] Turner, R. (2022, October 18) Executive Summary: Fundamentals of Next-Generation Application Security, Omdia

- 69.2% of the enterprises manage their own cloud based WAF controls and 25% are managed by their Cloud providers. Only 6.2% of the WAF based cloud deployments are managed by a 3rd party/Managed Security Service Provider (MSSP).
- The main challenges to WAFs are cost and performance. (Mordor Intelligence 2021)
- With the DC traffic primarily constituting HTTPS (75.9%) and HTTP (64.5%) based traffic, WAFs are expected to play a critical role in protecting applications.

1.2 Cloud WAF and API Security Benefits:

Cloud WAF technology allows for the creation of customized security and benefits organizations in the following ways:

- Less management complexity than on-premises WAF solutions.
- Ease of integration with existing security solutions.
- Scalable and elastic.
- Fast deployment and easy to set up.
- Protect web applications against external and internal attacks.
- Live monitor and control over web applications.
- Allows all transactions except those that contain threat/attack (Negative Security Model).
- Able to collect access logs for compliance/auditing and analytics.

API security technology benefits organizations in the following ways:

- Dynamic detection of API usage.
- Meter API usage.
- Broker authentication and authorization for APIs.

1.3 Proposed Cloud WAF Deployment Models:

Any proposed solution for Cloud WAF and API security platform should be available as cloud and on-prem component, cloud service and deployment models are:

- IaaS deployment as a software appliance or virtual machine.
- Software as a Service (SaaS).
- Reverse Proxy.
- Offered as pay-as-you-go service.

1.4 Statement of Intent:

The purpose of this cloud web application firewall (WAF) and application programming interface (API) security test is to provide empirically validated data based upon industry guidelines, such as OWASP, to assist in securing cloud applications. SecureIQLab believes that the test will lead to better, more secure cloud WAF and API security products.

1.5 Testing Goals Include:

Testing goals include the following:

- Publicly publish results that improve transparency and accountability within the security community.
- Highlight key technology differentiators.
- Inspire innovation.
- Refine forward looking technology.

1.6 Cloud WAF and API Security Features to be Evaluated

1.6.1 Security Features

The following are the list of cloud web application firewall security features that to be validated:

WAF:

- Protection against attacks that can be mapped to OWASP Top 10 2021.
- Protection against multi-layered application-based attacks.
- Geolocation attack protection from Layer 7 DDoS, SQL injection, and Cross-site scripting.
- Protection against encrypted attacks.
- Protection against account takeover attacks.
- Protection against automated attacks targeting gRPC, REST-API, SOAP, GraphQL, and WebSocket
- Validate payload processing capabilities for protection against web attacks delivered via techniques such as Base64, JSON, XML, and Gzip.
- Protection against bot attacks.
- Resistance to WAF bypass techniques
- Protection against emerging threats.
- Advanced attacks:
  - The advance web application attacks typically consists of the following: Local/Remote File Inclusion (RFI), server-side template injection attack, Server-Side Request Smuggling, Web Cache Poisoning, Advanced Cross-Site Scripting (XSS): Utilizing sophisticated techniques like polyglot vectors, Advanced SQL Injection: Leveraging advanced techniques, such as blind SQL injection, time-based attacks, or out-of-band (OOB) exploitation, Prototype pollution attack, Deserialization Attacks.
- Protection against tool-based attacks.
- Protection against product attack surface.

API Security:

- Protection against attacks that can be mapped to OWASP API Security Top 20 2023.
- Protection against encoded payload attacks
- API Monitoring and logging - enable the detection of security incidents, debugging, and forensic analysis. Logging security-relevant events, such as authentication failures, access violations, and abnormal behavior, can help in identifying and responding to security incidents promptly.

- Protection against GraphQL API attacks.
- Authentication and authorization mechanisms.
- Validate access control mechanisms and restrict unauthorized access to APIs and resources.
- Validating API discovery module for the capability to uncover Shadow, Zombie and Orphan API endpoints.
- Protection against GraphQL and REST API vulnerabilities.
- Protection against Account takeover attack.
- Protection against JSON & XML-Based Attacks.
- Protection against Malicious bot.
- Protection against Rate Limiting and Throttling.
- Protection for microservices.
- API Firewalling.

1.6.2 Administration and Integration Features

- Validate ease of onboarding process.
- Validate centralized management or dashboard module.
- Validate rules and security policy management features.
- Validate integration module with SIEM and SOAR.
- Validate notification and reporting features.
- Validate User Management features.
- Validate Role Management features.
- Validate Audit Trail features.
- Validate API endpoint inventory management.
- Validate of Security Analytics features.
- Validate integration with single sign-on (SSO).

1.7 Cloud WAF Vendor Participation Selection Criteria

We select vendors based on three following criteria:

1. Market Leaders – Either 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 and Gartner MQ, 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 that exist.

1.8 Scope:

The scope of this iteration of the test will be limited to cloud WAF products that claim to provide API security that are available in the cloud marketplace, SaaS offerings, or standalone cloud offerings. Any physical WAF is out of the scope of this methodology.

Considered vendors at the time of this publication:

Vendor	Product Name	Process Used
Akamai	Kona SiteDefender	Test to be evaluated utilizing Blackbox Security and Greybox Security Tasks
Alert Logic	Alert Logic	
Airlock	Airlock gateway	
AWS	AWS WAF	
Barracuda Networks	Barracuda	
Check Point	Cloudguard Appsec	
Citrix Systems	NetScaler AppFirewall	
Cloudflare Inc.	Cloudflare	
F5 Networks	BIG-IP Local Traffic Manager	
Fastly	Fastly	
Fortinet	FortiWeb	
Google	Cloud Armor	
Imperva	Incapsula	
Indusface	AppTrana WAF	
Microsoft	Azure WAF	
NSFocus Global Inc.	NSFocus	
Oracle	Oracle Cloud	
Palo Alto Networks	Palo Alto Next Gen Firewall	
Prophaze	Cloud WAF	
Radware	AppWall	
ThreatX	ThreatX	
UBIKA	UBIKA WAAP	
Wallarm	Wallarm Cloud WAF	

1.9 FUNDING AGREEMENT:

This is a non-commissioned test funded by SecureIQLab.

1.10 OPT-OUT POLICY

1.10.1 ACCEPTABLE REASONS FOR OPTING OUT:

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

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

All vendors have a limited right to opt-out for the designated reasons listed above.

1.10.2 How to opt out:

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

SecureIQLab
9600 Great Hills Trail, Suite 150W
Austin, TX 78759

Mailed opt-outs are effective by the date received, not the date posted. We do not accept opt-outs through phone, voice, social media or similar. Only mailed or emailed opt-outs will be accepted.

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. For your convenience, an opt-out form is included in the appendix.

The opt out period begins at the *Test Commencement* and continues through the end of the *Dispute Phase [Section 2.2]*. Vendors will be contacted by SecureIQLab within 3 business days of receiving the 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 cloud web application firewall and application programming interface security, referred here as the product under test (PUT), is capable of detecting, preventing, and logging attack attempts accurately, while remaining resistant to false positives.

The PUT will be configured either by walking through the applications, e-commerce, and other sites as relevant (automatically, or manually) or by creating rulesets and a security policy manually. The appropriate deployment model will be chosen per vendor recommendations where available, publicly available documentation, or industry best practices. The WAF and API security will be deployed to protect against attacks that target the potential assets beings protected.

2.1 Cloud WAF Security Effectiveness Validation

SecureIQLab will evaluate the security effectiveness of the cloud WAF and API security PUT using the following approaches:

- Blackbox Security Testing
- Greybox Security Testing

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

2.1.1 Information Gathering and PUT Reconnaissance

Information gathering and reconnaissance will be performed against the application to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. SecureIQLab will perform vulnerability analysis using automated tools such as Burpsuite and Nessus and perform 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:

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

2.1.2 Exploitation

Once information gathering and reconnaissance is over, we will begin exploitation as the next phase in this process. Exploitation involves leveraging the vulnerability information gathering 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 of using 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.

2.1.4 Defense Evasion Testing

Defense evasion is an important tool in an attacker’s arsenal. This allows old methods and techniques to be repurposed to evade protection against attacks that might otherwise get blocked by the cloud WAF. SecureIQLab will focus defense evasion testing in the following areas.

- Pre-processor Attacks: These attacks involve the decision on whether a request will be processed further. We will perform the pre-processor attack by identifying possible application inputs and end points.
- Normalization: We will perform the normalization task by tweaking the different end points, for example, a compress whitespace attack where we convert the whitespace characters to spaces.
- Validate Input with Payload: Check user input against policies. We will perform fuzzing and prepare payloads in an attempt to bypass the security rules set by the cloud WAF.

2.2 Cloud WAF Test Life Cycle

The cloud WAF and API security test plan is within scope if the project remains within four weeks of the below timeline. This methodology is open for feedback and updates until 1 December 2023.

SecureIQLab will execute the test in six phases:

1. **Phase1: Reconnaissance**

   We will start the initial validation with basic and advance level reconnaissance.

2. **Phase 2: Attacking the pre-processor**

   As a part of the input validation, we will perform pre-processor attack by trying to skip input validation.

3. **Phase 3: Attempting an impedance mismatch.**

   We will attempt to make the WAF interpret a request differently than the backend to not be detected.

4. **Phase 4: Bypassing the rule set.**

   We will prepare a payload that will not be blocked and can bypass the WAF's rule set.

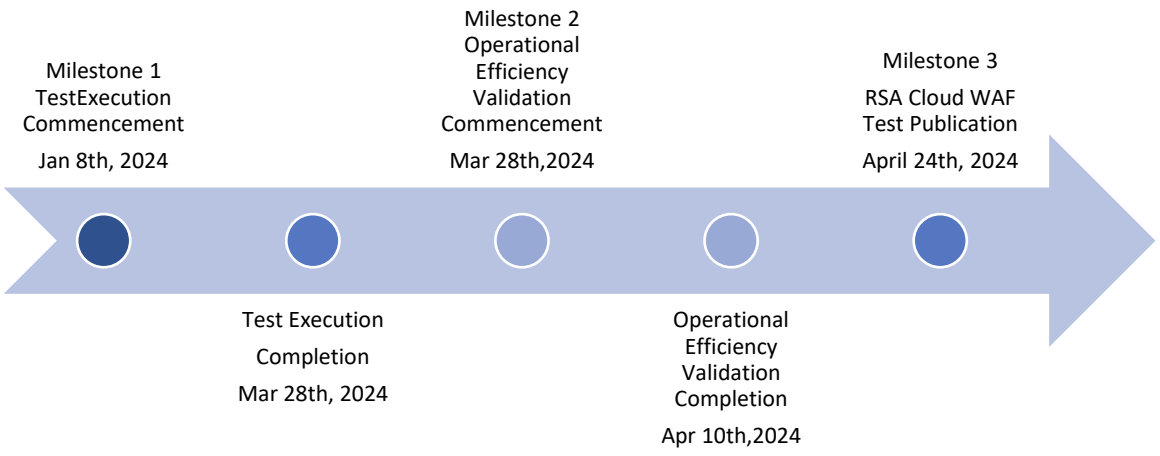
5. **Phase 5: Identifying the vulnerabilities.**

   We will perform the security testing based on the guidelines around the OWASP Security Testing guidelines along with customized testing.

6. **Phase 6: Post Assessment Phase.**

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

SecureIQLab will execute and publish Cloud WAF v3.0 in the following timeline below:



Cloud-WAF v3.0 Overall Test Timeline

2.3 Risk and Risk Management:

No additional risks are known at this time.

2.4 Proposed Attack Types

Testing will demonstrate the effectiveness of the PUT to protect vulnerable assets from targeted threats and exploitation. This asset/target and threat-based approach forms the basis from which PUT security effectiveness is measured.

Attack types and test configuration: The SecureIQLab threat and attack suite contains attacks (including mutations of the same underlying attacks) and proprietary exploits either harvested through our test harness or crafted by our threat research team. Crafted exploits are intended to simulate attacks in the wild. Groups of exploits are carefully selected from the attack library to test based on the intended attack. Each exploit has been validated to impact the target vulnerable host(s) by compromising either the asset which can vary from a web server, web application or sites.

Cloud WAFs and API security PUTs will defend a number of complex web applications that have also been constructed to include known vulnerabilities and coding errors.

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

The level of compromise can vary between instigating a Denial of Service (DoS) condition, providing administrator/root access to the host server, allowing malicious users to amend system parameters or application data before submission, browse and/or retrieve files stored on the host server, escalating user privileges and so on.

2.5 Attack Relevance:

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

2.6 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 also originate from as wide a range of IP addresses as possible.

2.7 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, one for each PUT, and one comparative report containing summary information for all PUTs. These results will then be publicly available to download at https://secureiqlab.com/publications/.

Vendors are offered an optional partnership after we are done testing. This optional partnership is for marketing rights of test results and is based on the potential utility of publicizing testing results to highlight specific security offerings. This optional partnership is intended to be useful for vendor marketing. If there is a fee agreement in exchange for services rendered, vendors are given the option to progress forward with published results following AMTSO standards.

3 CONTROL PROCEDURES

Before any test is conducted, the attacks will be validated against an unprotected target to ensure impact, meaning that we will confirm the attacks alter the behavior of the system. Additionally, SecureIQLab will ensure that the cloud WAF and API security platform under test have been validated in the following areas:

- Connection Validation:
- The WAF and API must be accessible by the administrator.
- The WAF must pass normal application traffic.
- Logging:
- Verify that logs are being generated and recorded. Test subjects will not have access to test logs. 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 it becomes generally available. SecureIQLab will make a best effort to apply these updates to the products prior to the evaluation.

To further substantiate results, testing may include repeated execution of attacks in various sequences. To ensure a consistent comparison, these diverse sequences will be applied uniformly across all products being tested.

4 DEPENDENCIES

Participant and test subject vendors suggested actions:

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

- Setup
- PUT version recommendation.
- Default configuration
- Where tuning is required, publicly available best vendor practices will be followed. Vendors are invited to review configurations prior to testing.
- Testing
- Vendors are invited to provide scorecard feedback for their tested cloud WAF and API security products.
- Reports
- Participating vendors are invited to provide report feedback prior to publication.

5 Scoring and Dispute Process

For all attacks blocked by the cloud WAF and API security PUT, SecureIQLab will give the block credit to the products under test under test. Repeated attacks will only be scored once. Additionally, multiple packet capture tools will ensure test result accuracy.

If any inconsistencies exist between our packet capture tools and the vendor's packet capture tool, SecureIQLab will default to the vendor packet capture as long as it provides sufficient evidence beyond reproach. No credit will be given for missed attacks and there is no negative scoring for attacks missed by the cloud WAF or API security PUT. The outcome of the attacks combined with the logging of the attacks will be used for scoring purposes.

Industry norms and best practices will be followed if there are any disputes on the nature of the attacks used during the testing window.

SecureIQLab will make best efforts to resolve disputes regarding scoring. Any changes to scoring resulting from successful disputes will be applied to all vendor results as required, and not just to the results of the disputing vendor.

All cloud WAF and API security vendors who participate in this test, and are not only test subjects, 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 cloud WAF and API security vendors, and SecureIQLab will work closely with these vendors to go over the metrics as well as relevant metadata where warranted. Furthermore, SecureIQLab will not share attacks that are missed during the testing window to third parties unless required by law. SecureIQLab will provide vendors up to two weeks for the dispute resolution on the nature of attacks. Any security vulnerabilities that are uncovered during the testing windows related to the products under test will be shared based upon responsible disclosure policy which provides vendors up to 20 days to fix the vulnerability. Vulnerability details will be disclosed to the broader public when a fix is available or when discussion is in the interest of the general public.

SecureIQLab will not entertain disputes or changes to scoring after the Comparative and Individual Test reports have been published.

6 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 entity to these Attestations. All references to "I" or "me" or similar language refer to such 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.

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-TP097

7 APPENDIX:

7.1 DOCUMENT REVISIONS:

Version	Section	Revision overview
V2.0	1.6.2	Added protection against product attack surface.
V2.0	1.8	Removed AWS compatibility requirement.
V3.0	1.6.2	Added Administration and Integration Features Section
V3.0	1 - 7	Scope of test to include API protection
V3.0	2.4	Specific callout that exploits have been validated to impact the target vulnerable host(s)
V3.0	3	Added SecureIQLab will share logs with participating vendors.
V3.0	3	Attacks will be run multiple times in different ordered sequences.

7.2 EXAMPLE ATTACK TYPES:

- Cookie/Session Poisoning
- Manipulation of cookie or session variables to access protected information/areas of a website.
- Cross-Site Scripting (XSS)
- The process of manipulating user input in such a way that, when rendered in the context of a webpage, it will be interpreted by the browser as code.
- Directory traversal
- The URL to access areas of the web server that should not otherwise be accessible.
- SQL Injection
- Manipulating user input in such a way that, when processed by the database server, it will be interpreted as code, potentially providing direct access to private data.
- Protection against Account takeover protection
- Protection against JSON & XML-Based Attacks

7.3 OPT-OUT FORM

Vendor name: _____

Vendor representative name: _____

Title: _____

Email: _____

Phone number: _____-_____-_____

Reason for opt-out:

[ ] Outside of scope

[ ] NOT generally available nor ready for deployment.

[ ] Against the public interest

[ ] Other

Details: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

This form should be emailed to:

info@secureiqlab.com.

Mailed opt-outs must be sent to:

SecureIQLab
9600 Great Hills Trail, Suite 150W
Austin, TX 78759

8 COPYRIGHT AND DISCLAIMER

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

SecureIQLab (December 2023)