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.

SecureIQLab®

Methodology

Cloud Web Application and API Protection CyberRisk Methodology v3.9 - Draft

Version: 3.9 DRAFT

Last Revision: 9 September 2024

Language: English

1 Introduction

1.1 The Need for Web Application Firewalls and Application Programming Interface Protection

In today's digital landscape, enterprises and organizations are increasingly reliant on web applications and APIs to drive their operations, engage with customers, and integrate systems. A Cloud Web Application Firewall (WAF), coupled with API protection, has become an essential solution for enterprises aiming to secure their web applications and APIs from a broad range of growing cyber threats against the critical digital assets as it is paramount to ensuring business continuity, safeguarding sensitive data, and maintaining compliance with industry regulations. By leveraging advanced technologies like machine learning, threat intelligence, and customizable security rules, organizations can defend against zero-day vulnerabilities, bot-driven attacks, and API-specific risks.

Furthermore, as APIs have become the backbone of many modern applications, the need for API security is critical. A WAF with robust API protection capabilities helps prevent unauthorized access, data breaches, and API abuse, ensuring that API interactions are secure and compliant with regulatory requirements such as PCI-DSS, HIPAA, and GDPR. API security also plays a vital role in enhancing the operational efficiency of a Cloud Web Application Firewall (WAF) by providing comprehensive protection for both web applications and APIs. By integrating API security, the WAF can help cover API-specific threats, Improve Performance, enhance visibility, Automated detection and mitigation, optimize scalability and ensure compliance.

The Cloud Web Application Firewall (WAF) continues to be a cornerstone of web application security. Cloud WAFs not only protect against external threats but also offer features like DDoS mitigation, bot management, and the ability to scale with traffic demands, cloud-based WAFs provide a holistic solution that aligns with the dynamic needs of modern enterprises. Cloud WAAP solutions allow enterprises to focus on innovation and application development without being slowed down by security concerns, reducing the time it takes to bring new products and services to market.

The convergence of WAF and API security technologies is driven by the need for comprehensive protection against a broadening range of threats and has given rise to Web Application and API Protection (WAAP) platforms. Enterprises rely on Cloud WAAP to provide comprehensive, scalable, and cost-effective security for web applications and APIs. As digital transformation accelerates, Cloud WAAP solutions enable organizations to stay resilient in the face of evolving cyber threats while ensuring compliance, performance, and business continuity.

1.2 Cloud WAAP Security Benefits:

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

- Less management complexity than on-premises WAAP 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 WAAP Service Delivery Models:

Any proposed solution for Cloud WAAP 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 and application programming interface (API) protection 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 WAAP 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 WAAP 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 web server and web CMS (Content Management System) vulnerability exploits
- Protection against Layer 7 DDoS, application DDoS
- Protection against Geolocation Attacks on Web Applications (IP Geolocation Spoofing, Geofencing Evasion, IP Geolocation Manipulation)
- Protection against vulnerabilities and attacks over encrypted communication channels.
- Protection against account takeover attacks such as Credential Stuffing, brute force attack

- 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 such as web scraping, Inventory Hoarding, content spamming, Fake Account Creation.
- Resistance to WAF bypass techniques
- Protection against emerging threats.
- Protection against web application advanced attacks:
    - The advance web application attacks typically consist 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 web application vulnerability scanner and web exploitation tools.

1. API Security:

- Protection against attacks that can be mapped to OWASP API Security Top 10 2023.
- Resistance to API Security bypass techniques
- 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 specialized attacks for REST, SOAP, WebSocket, GRPC, 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 API Abuse and Malicious Bots
- Protection against Rate Limiting and Throttling.
- API Firewalling.

1.6.2 Administration and integration features

- Validate ease of onboarding and deployment process.
- Validate centralized management or dashboard module.
- Validate rules and security policy management features.
- Validation of Web and API Risk Management.
- Validate integration module with SIEM and SOAR.
- Validate notification and reporting features.
- Validate User Management features.
- Validate Role Management features.

- Validate logging and audit trail capabilities
- Validate API endpoint inventory management.
- Validate of Security Analytics features.
- Validate Identity Management and Access Control
- Validate Support and Documentation

1.7 Cloud WAAP 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 vendors 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	App and API Protector	Test to be evaluated utilizing Security Efficacy and Operational Efficacy
Airlock	Airlock Secure Access Hub - Airlock Gateway	
AWS	AWS WAF & Shield	
Barracuda Networks	Barracuda Application Protection	
Check Point	Cloudguard WAF	
Citrix Systems	NetScaler WAF	
Cloudflare Inc.	Cloudflare WAF and API Gateway	
F5 Networks	F5 Distributed Cloud Web App and API Protection	
Fastly	Fastly Next-Gen WAF	
Fortinet	FortiWeb	
Google	Cloud Armor and Apigee API Management	
Imperva	Imperva WAF and API Security	
Indusface	AppTrana WAAP	
Microsoft	Azure WAF and API Management	
NSFocus Global Inc.	NSFocus Web Application and API Protection	
Oracle	OCI WAF and API Gateway	
Prophaze	Hybrid WAF 3.0 and Advanced API Security	
Radware	AppWall and API Security	
UBIKA	UBIKA WAAP	
Wallarm	Wallarm Advanced API Security	

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 WAAP PUT will be deployed to protect against attacks that target the potential assets beings protected.

2.1 Cloud WAAP Security Effectiveness Validation CRITERIA

SecureIQLab will evaluate the security effectiveness of the cloud WAAP PUT under two major criteria:

1. Security Efficacy Testing
2. Operational Efficiency Testing
3. Performance Testing

2.1.1 Security Efficacy Testing

Security Efficacy Testing is focused on evaluating the effectiveness of security solutions in protecting against various threats and vulnerabilities. This approach assesses how well a security product or system performs its intended

function under real-world conditions, ensuring that it can detect, prevent, and respond to cyberattacks.

Key Objectives of Security Efficacy Testing:

- Threat Detection: Assess the solution's ability to identify and respond to diverse attack vectors.
- Coverage Assessment: Evaluates the comprehensiveness of the solutions in terms of protections against attacks.
- Response Evaluation: Evaluates the timeliness and effectiveness of the solution's response mechanisms.
- Accuracy Measurement: Ensures minimal false positives and negatives in threat identification.
- Validation of Security Claims: Ensures the security solutions meet the vendor's claims and industry standards, offering reliable protection.

The security efficacy testing consists of the following validation tasks to test protections against following 7 threat categories:

1. **OWASP Top 10: 2021 vulnerabilities**

   Testing against the OWASP Top 10 ensures the security solution can effectively detect and prevent critical web application vulnerabilities, such as Injection and request forgeries, that are most commonly exploited by attackers.

2. **Bot Attacks**

   This involves assessing the solution's ability to identify and block malicious bot activities, such as credential stuffing and content scraping, while allowing legitimate traffic to pass through unharmed.

3. **Layer 7 DoS Attacks**

   Testing focuses on the solution's ability to mitigate Layer 7 DoS attacks that overwhelm application services with high volumes of seemingly legitimate traffic, ensuring consistent service availability.

4. **WAF Evasion Attacks**

   This task evaluates how well the security solution can detect and block attempts to bypass the Web Application Firewall (WAF) using obfuscation or other evasion techniques.

5. **Vulnerable Web Environments Exploits**

   Testing the solution's response to specific vulnerable application exploits ensures it can effectively protect against targeted attacks that exploit known security flaws in applications.

6. **API Attacks:**

   API Attacks Validates the security solution's ability to secure APIs from attacks such as Injection, Data Exposure, and Rate Limiting Bypasses, ensuring that APIs remain secure and resilient against unauthorized access and misuse.

7. **WAF Vulnerability Assessments:**

Involves evaluating the Web Application Firewall (WAF) itself for any vulnerabilities, ensuring it is securely built, configured, and capable of protecting itself from various threats.

2.1.2. OPERATIONAL EFFICIENCY TESTING

Operational Efficiency Evaluation is crucial because it ensures that a security solution, like a Web Application and API Protection (WAAP) product, not only provides robust security but also integrates smoothly into the organization's operations without causing unnecessary complexity or inefficiencies. Here's why organizations find Operational Efficiency so vital:

1. Maximizes Productivity

- Streamlined Management: Easier management frees up security teams to focus on strategic tasks, improving overall productivity.
- Faster Response: Quick threat identification and mitigation reduce downtime and potential damage.\

2. Supports Business Growth

- Scalability: Ensures the solution can grow with the organization without becoming a bottleneck.
- Adaptability: Allows the solution to quickly respond to changes, supporting ongoing business evolution.

3. Enhances Security Posture

- Effective Risk Management: Simplifies policy adjustments to continuously protect against emerging threats.
- Comprehensive Monitoring: Improves the ability to detect and address potential security issues proactively.

4. Cost-Effectiveness

- Resource Optimization: Avoids unnecessary costs by optimizing resource use.
- Reduced TCO: Easier deployment and management lower overall costs, making the solution a better long-term investment.

5. Improved User Experience

- Simplified Processes: User-friendly interfaces reduce errors and frustration for security teams.
- Better Support: High-quality support ensures quick resolution of issues, maintaining system integrity.

6. Facilitates Compliance

- Auditing and Logging: Helps meet regulatory requirements, avoiding legal issues and penalties for organizations.

7. Mitigates Risks

- Holistic Evaluation: Ensures the solution does not introduce new risks but helps in discovering and

mitigating risks.

The Operational Efficiency section focuses on helping to assess the WAAP product's practicality and effectiveness in real-world use. So, SecureIQLab will be evaluating the Operational Efficiency against following metrics:

1. Ease of Deployment

Evaluates how straightforward and efficient the process is to deploy the WAAP product in different environments (e.g., cloud, on-premises), including the initial setup, integration with existing infrastructure, and time to go live.

2. Ease of Product Management

Assesses how user-friendly and intuitive the WAAP product is to manage, including daily operations, configuration changes, updates, and maintenance tasks, ensuring that the product can be easily managed by security teams.

3. Ease of Risk Management

Measures how effectively the WAAP product helps manage and mitigate risks, including the simplicity of configuring security policies, responding to alerts, and adjusting settings to address emerging threats.

4. Scalability and Elastic Capabilities

Evaluates the WAAP product's ability to scale efficiently with growing traffic and data volumes, and its capability to adapt to changing demands, such as automatic scaling during traffic spikes.

5. Logging and Auditing Capabilities

Assesses the comprehensiveness and accessibility of the WAAP product's logging and auditing features, ensuring that security teams can easily track activities, investigate incidents, and maintain compliance.

6. Visibility and Analytics

Measures the level of insight the WAAP product provides into web application traffic and security events, including the availability of dashboards, reporting tools, and real-time analytics for informed decision-making.

7. Support and Documentation

Evaluates the quality and availability of vendor support and documentation, ensuring that users have access to necessary resources, troubleshooting guides, and expert assistance when needed.

2.1.3. Performance Testing

This section measures the performance of a Product under Test using various traffic conditions to simulate various real-world traffic scenarios. Testing involves simulating a variety of real-world traffic scenarios to assess how well the WAAP solution handles different loads under various conditions.

The focus will be on assessing the solution's efficiency, stability, and scalability by measuring key performance indicators such as response times, latency and throughput. The results will provide insight into the solution's ability to maintain optimal performance while effectively protecting web applications and APIs under challenging conditions.

2.1.3. Security by Design and Secure by Default Evaluation

Evaluation for Secure by Design and Secure by Default will be based on the recommendations for these areas by CISA[1]. Below are some of the areas this evaluation will include:

- Password management
- Authentication Mechanisms
- Access control
- Data Encryption
- Security Alerts
- Patch Management
- Vulnerability Disclosure policy

2.2 Cloud WAAP Test Life Cycle

The cloud WAAP 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 October 2024.

SecureIQLab will execute the test in eight phases:

1. Deployment

Setup of the Test Environment: This step involves installing and deploying the security solution in the test environment, ensuring that all necessary components are properly integrated and ready for testing.

2. Configuration

Tailoring the Solution: The security solution is configured according to the specific needs and testing scenarios. This includes setting up security policies, rules, and other settings required for accurate evaluation.

3. Smoke Test

Initial Functionality Check: A basic test is conducted to ensure that the solution is functioning as expected after deployment and configuration. It checks for major issues before more in-depth testing begins.

4. Configuration Review

[1] For additional information, please see: https://www.cisa.gov/securebydesign

Verification of Settings: The configuration is reviewed to ensure it aligns with best practices and testing requirements. This step ensures that the solution is optimally set up for accurate and fair testing.

5. Final Test

Comprehensive Testing: A thorough and detailed testing process is carried out, covering all test cases and scenarios to evaluate the solution's effectiveness, performance, and reliability.

6. Disputes

Handling of Discrepancies: Any disagreements or inconsistencies in test results are addressed. This may or may not involve re-testing or discussions with stakeholders to resolve issues before finalizing the results.

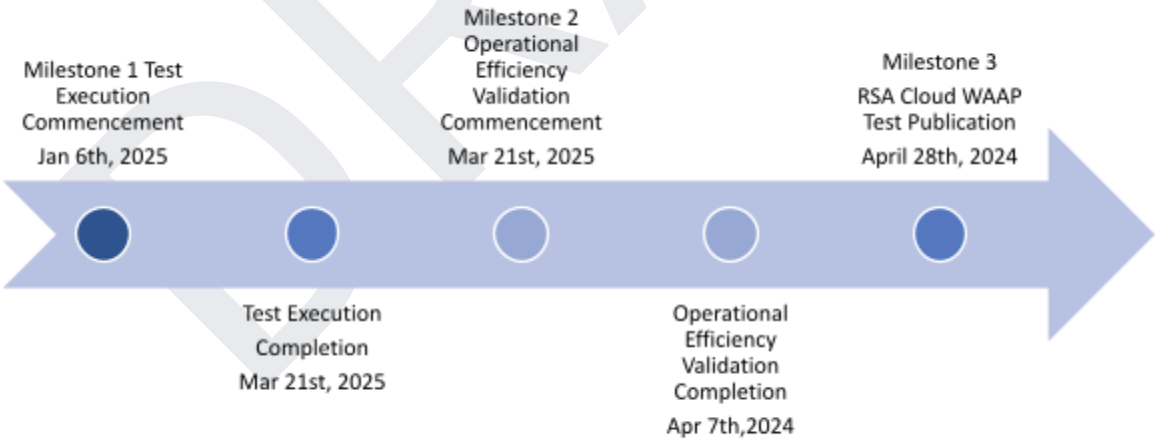
7. Reporting

Documentation of Results: The findings from the testing are documented in a detailed report, including observations, metrics, and any identified issues, providing a comprehensive overview of the solution's performance.

8. Publication

Sharing the Findings: The final report is published and shared with relevant stakeholders, including clients, vendors, and internal teams, to communicate the results of the testing and any recommendations.

SecureIQLab will execute and publish Cloud WAAP v4.0 in the following timeline below:



Cloud-WAAP 4.0 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 WAAP PUT will defend a number of complex web applications that have also been constructed to include known vulnerabilities and coding errors. Benign traffic will be run throughout testing for false positives.

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 WAAP 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:

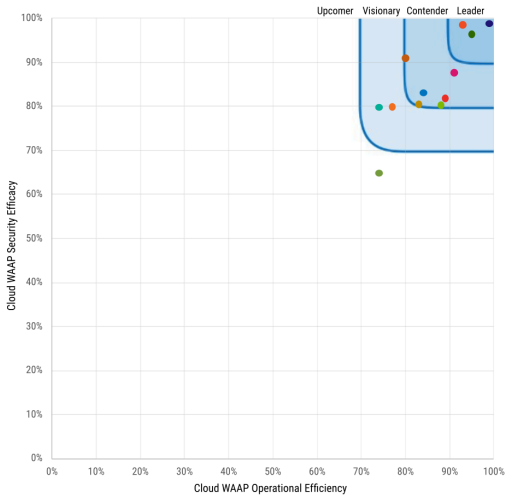


Figure 1. Example of a CyberRisk Ripple

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. Figure 1 provides an example of the CyberRisk Ripple. This figure provides an at a glance comparative for the vendors' resultant security efficacy and operational efficiency and is included in the comparative report. 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 WAAP platform under test have been validated in the following areas:

- Connection Validation:
- The WAAP must be accessible by the administrator.
- The WAAP 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, and where applicable, 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 WAAP 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 WAAP 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 WAAP 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 WAAP 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 WAAP 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-***-****

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.
V3.9	1.1	New Introduction
V3.9		
V3.9	2.7	CyberRisk figure and explanation added
V3.9	1.6.1	Revised the previous points: Protection against Layer 7 DDoS , application DDoS Protection against Geolocation Attacks on Web Applications (IP Geolocation Spoofing, Geofencing Evasion, IP Geolocation Manipulation) Protection against vulnerabilities and attacks over encrypted communication channels.
V3.9	1.6.1	Protection against web server and web CMS (Content Management System) vulnerability exploits added
V3.9	1.6.1	Protection against bot attacks such as web scraping, Inventory Hoarding, content spamming, Fake Account Creation added
V3.9	1.6.1	Protection against bot attacks such as web scraping, Inventory Hoarding, content spamming, Fake Account Creation added
V3.9	1.6.1	Protection against web application vulnerability scanner and web exploitation tools added
V3.9	1.6.1	Resistance to API Security bypass techniques added
V3.9	1.6.1	Protection against specialized attacks for REST, SOAP, WebSocket, GRPC, GraphQL API attacks added
V3.9	1.6.1	Protection against API Abuse and Malicious Bots added
V3.9	1.6.1	Protection against product attack surface removed
V3.9	1.6.1	Protection for microservices removed
V3.9	1.6.2	Validation of Web and API Risk Management added
V3.9	1.6.2	Validate Identity Management and Access Control added
V3.9	1.8	Product Name updated
V3.9	2.1	Added: 1. Security Efficacy Testing 2. Operational Efficiency Testing
V.3.9	2.1.1	SECURITY EFFICACY TESTING Added
V3.9	2.1.2	OPERATIONAL EFFICIENCY TESTING
V3.9	2.2	New CLOUD WAAP TEST LIFE CYCLE added

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)