SmartBuddy

**WAFv2 Monitoring Report**

Document History

| **Date** | **Version** | **Editor** | **Change** |
| --- | --- | --- | --- |
| Jun 05, 2025 | 1.0 | Nguyen Thanh Nguyen | Initial version |
| Jun 21, 2025 | 1.1 | Nguyen Trung Quoc  Joseph Nguyen | Updated proposal for Cross-Site-Scripting-01/02/03 rules in Caleb, iSchool, SSS WAF rule from Count to Block:  + Section 2.3 The approach (Whitelist special URIs that come from the Caleb Web Portal)  + Section 3 Analysis result  Updated rule action for “AWSManagedIPDDoSList” in Caleb WAF ACL from Count to Block. |

Table of Contents

[**1.0 INTRODUCTION 5**](#_heading=h.t7ysj664oxc9)

[**2.0 ANALYZE PLAN 5**](#_heading=h.aetc1khm0ivw)

[2.1 Environment 5](#_heading=h.jyc4jz9vz7rn)

[2.2 Resources that need to be analyzed 5](#_heading=h.5io5df2hqbdt)

[2.3 The approach 8](#_heading=h.6tne6e3z04od)

[**3.0 ANALYZE RESULT 11**](#_heading=h.pvqlnacvmxzv)

[**4.0 ANALYZE DETAIL 34**](#_heading=h.vafvo8fs51m)

[4.1 Queried Data Results 34](#_heading=h.xjnxd0sm2yp9)

[4.2 SmartBuddy Caleb PROD 34](#_heading=h.9upxbc28b3bs)

[4.3 SmartBuddy iSchool Portal PROD 39](#_heading=h.exha9tdepa7c)

[4.3 SmartBuddy iSchool API PROD 44](#_heading=h.1o1v5o1yg1l5)

[4.4 SmartBuddy SSS PROD 49](#_heading=h.bumxok999pkn)

General Note

The aim of this document is to support the application and engineering efforts of STYL customers that use STYL’s products. This document is intended for testing, evaluation, integration, and information purposes.

STYL makes every effort to ensure that the quality of the information is available. The content of this documentation is provided on an “as is” basis and may contain deficiencies or inadequacies.

STYL disclaims any warranty and all responsibility for the application of the device(s) that is made in relation to the accuracy, reliability or contents of this document. STYL is not liable for any injury, loss or damage of any kind incurred for the use of or reliance upon information.

STYL reserves the right to make any modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to products at any time and without notice.

# INTRODUCTION

This document provides the monitoring plan and monitoring result for the R44 - WAFv2 applied on PROD. For the purpose of reconciliating WAF configuration and WAFv2 rule.

# ANALYZE PLAN

## Environment

The plan will be conducted on the **PROD** environment which has the real user’s traffic and enables WAF V2 from 07 May 2025.

The logs was extracted for the period from:

* From date: 07 May 2025
* To date: 27 May 2025

## Resources that need to be analyzed

In this plan, we will execute queries to analyze WAF’s log and CloudWatch metrics, from that result we will optimize the rules accordingly to better protect the system. There are 4 log groups corresponding to 4 WAF distributions:

| **WAF** | **Cloudfront Distribution** | **Domain** | **Cloudwatch Log Group** |
| --- | --- | --- | --- |
| SmartBuddy\_SSS\_PROD\_WAFv2 | ETDDHTZRF63GZ | www.sss.smartbuddyschools.com  sss.smartbuddyschools.com | aws-waf-logs-SmartBuddy\_SSS\_PROD\_WAFv2 |
| SmartBuddy\_Ischool\_API\_PROD\_WAFv2 | E1Z65OTH0VKQ9X | ischool-api.smartbuddyschools.com  ischool.styl.solutions | aws-waf-logs-SmartBuddy\_Ischool\_API\_PROD\_WAFv2 |
| SmartBuddy\_Ischool\_Portal\_PROD\_WAFv2 | E1C4LT0MALZS1K | www.ischool.smartbuddyschools.com  ischool.smartbuddyschools.com | aws-waf-logs-SmartBuddy\_Ischool\_Portal\_PROD\_WAFv2 |
| SmartBuddy\_Caleb\_PROD\_WAFv2 | EJXEQ7M4ECEFT | caleb.smartbuddyschools.com | aws-waf-logs-SmartBuddy\_Caleb\_PROD\_WAFv2 |

List of rules that need to be analyzed:

* **WAF SmartBuddy\_SSS\_PROD\_WAFv2**

| **Rule** | **To analyze?** | **Purposes** |
| --- | --- | --- |
| AWS-AWSManagedRulesAmazonIpReputationList | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| AWS-AWSManagedRulesBotControlRuleSet | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | No | This rule is confirmed. No further update is required currently. |
| BlanketLimitRequest | Yes | To determine whether we can adjust the rate limit according to the actual workloads and update the rule action from “Count” to a higher security action: Block, CAPTCHA, or Challenge. |
| LogAllUnmatchedTraffic | No | This is the default rule for logging purposes. |

* **WAF SmartBuddy\_Ischool\_API\_PROD\_WAFv2**

| **Rule** | **To analyze?** | **Purposes** |
| --- | --- | --- |
| AWS-AWSManagedRulesAmazonIpReputationList | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| AWS-AWSManagedRulesBotControlRuleSet | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | No | This rule is confirmed. No further update is required currently. |
| BlanketLimitRequest | Yes | To determine whether we can adjust the rate limit according to the actual workloads and update the rule action from “Count” to a higher security action: Block, CAPTCHA, or Challenge. |
| LogAllUnmatchedTraffic | No | This is the default rule for logging purposes. |

* **WAF SmartBuddy\_Ischool\_Portal\_PROD\_WAFv2**

| **Rule** | **To analyze?** | **Purposes** |
| --- | --- | --- |
| AWS-AWSManagedRulesAmazonIpReputationList | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| AWS-AWSManagedRulesBotControlRuleSet | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | No | This rule is confirmed. No further update is required currently. |
| BlanketLimitRequest | Yes | To determine whether we can adjust the rate limit according to the actual workloads and update the rule action from “Count” to a higher security action: Block, CAPTCHA, or Challenge. |
| LogAllUnmatchedTraffic | No | This is the default rule for logging purposes. |

* **WAF SmartBuddy\_Caleb\_PROD\_WAFv2**

| **Rule** | **To analyze?** | **Purposes** |
| --- | --- | --- |
| AWS-AWSManagedRulesAmazonIpReputationList | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge |
| CalebAccess | No | This rule is confirmed. No further update is required currently. |
| AWS-AWSManagedRulesBotControlRuleSet | Yes | To determine if the rule can be updated, the rule action can be changed from “Count” to a higher security action: Block, CAPTCHA, or Challenge. |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | No | This rule is confirmed. No further update is required currently. |
| BlanketLimitRequest | Yes | To determine whether we can adjust the rate limit according to the actual workloads and update the rule action from “Count” to a higher security action: Block, CAPTCHA, or Challenge. |
| LogAllUnmatchedTraffic | No | This is the default rule for logging purposes. |

## The approach

Below is the approach to analyze the WAF’s logs in order to propose solutions to enhance the security of the system:

* **Update the rule action from “Count” to higher security level: “Block”, CAPTCHA, or Challenge.**

Do the below check to determine if the rule action can be updated from “Count” to “Block”:

| **Check #** | **Details** | **Expectation** |
| --- | --- | --- |
| **1** | Execute query in AWS CloudWatch Log insights to check the WAF V2 log, identify if any request that was matched the rule in the past two weeks.  For the request that matches the rule, check the request URI and other information to see if it’s a valid request.  **Query:**    fields @timestamp, @message  | filter @message like '{"ruleGroupId":"<Rule Name>"'  | parse @message '{"ruleGroupId":"<Rule Name>"\*' as info  | parse info ',"nonTerminatingMatchingRules":[\*]}]' as nonTerminatingMatchingRules  | filter nonTerminatingMatchingRules like '<Sub Rule Name>'  | display @timestamp, httpRequest.clientIp, httpRequest.host, httpRequest.uri, @message  | sort timestamp desc  Note: To check the actual rule name in the log, it may different with the one displayed in the AWS portal. | There is no valid request that matches the rule. |

* **Adjust the rate limit according to the actual workloads**

| **Check #** | **Details** | **Expectation** |
| --- | --- | --- |
| **1** | Check CloudWatch metric of the WAF V2, identify number of requests to the system per minute.  Metrics → All metrics → N.Virginia → WAF → Rule, WebACL → All, CountedRequests.  Select tab Graphed metric → Statistic: Sum. Period: 1 minute | Graphed metric show total number of counted requests per minute |
| **2** | Execute query in AWS CloudWatch Log insights to check the WAF V2 log, count the number of requests that passed all the rules, filter out those requests from IP within 1 minute.  Review and filter out the request that URI is invalid.  Find out the average and maximum number of requests from one IP per minute.  From the result, determined the rate limit, usually it will be x5 (to discuss and agree) of the average request from one IP per minute.  **Query:**  fields @timestamp, httpRequest.clientIp, httpRequest.uri  | stats count(\*) as RequestCount by httpRequest.clientIp, httpRequest.uri, bin(1m)  | sort RequestCount desc | Returned a table that contained client IP, requested URI and maximum of total requests of each client IP in time range. |

* **Whitelist special URIs that come from the Caleb Web Portal.**

In the Caleb Web Portal, there are some features that allow portal administrators to input the html content via the content editor, even the end user input the valid content, but sometimes the request is still blocked by WAF. Therefore, in order to ensure the normal operation, we suggest to whitelist special URIs below:

| **#** | **URI pattern** | **Description** | **Justification** |
| --- | --- | --- | --- |
| **1** | /w/notification/preview | API endpoint to preview the push notification content that DBS users are preparing on the Caleb Web Portal. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **2** | /w/notification/task/add | API endpoint to create the notification task. In the request, there is a html content for the detailed push message. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **3** | /w/notification/task/\d+/edit | API endpoint to update the notification task information. Similar to #2, there is a html content for the detailed push message in the request. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **4** | /w/notification/template/add | API endpoint to create the template of the notification. In the request, there is a html content for the detailed push message. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **5** | /w/notification/template/\d+/edit | API endpoint to update information of the template of the notification. Similar to #4, there is a html content for the detailed push message in the request. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **6** | /w/wearable/request/status | API endpoint to approve / reject the watch replacement claim request from the Caleb Web Portal. | The Caleb Web portal has been restricted by whitelist IP addresses. Only STYL and DBS users can access and perform this action.  In the approve / reject message, there is defined html content. |
| **7** | /w/notification/task/add/preverify | API endpoint to pre-validate fields before creating the notification task. This is a new API following the requirement of CR#937 will be released in July 2025. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **8** | /w/notification/task/\d+/edit/preverify | API endpoint to pre-validate fields before editing the notification task. This is a new API following the requirement of CR#937 will be released in July 2025. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **9** | /w/gamification/add | API endpoint to create the gamification. In the request, there is a html content for the description. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |
| **10** | /w/gamification/\d+/edit | API endpoint to edit the gamification. In the request, there is a html content for the description. | The Caleb Web portal has been restricted by whitelist IP addresses. Only DBS users can access and perform this action. |

**Implementation for whitelist URIs:** Set up a statement for the Fortinet rule to exclude the above URIs from inspection since those APIs are only called from restricted allowed IP addresses and authenticated users. For the details of the implementation, please refer to section 3.0 below.

Note: The rule “CalebAccess” will block all requests to the URI “/w” and “/CMS” from un-whitelisted IP addresses. This will ensure that requests via those URIs are only from our authorized IP addresses and authenticated users.

# ANALYZE RESULT

From the analyzed result, below is the proposed new setting for the Smart Buddy WAF V2:

Note: Column “Proposed New Setting” empty means that no update is required. The current setting already meets the requirement.

* **WAF SmartBuddy\_Caleb\_PROD\_WAFv2**

| **#** | **Rules** | **Sub-Rules** | **Current Setting** | **Proposed New Setting (If have)** |
| --- | --- | --- | --- | --- |
| 1 | AWS-AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | Block |
| AWSManagedReconnaissanceList | Count | Block |
| AWSManagedIPDDoSList | Count | Block |
| 2 | CalebAccess | If a request matches all the statement (AND):  Statement 2:  - Negate Statement (NOT): Yes  - Inspect: URI path  - Match type: Matches pattern from regex pattern set  - Regex pattern set: AllowAccessToWebPortal  - Text transformation: None  Not statement 2:  - Negate statement (NOT): Yes  - Inspect: Originates from an IP address in  - IP set: Caleb\_PROD\_IPSET  - IP address to use as the originating address: Source IP address  \* IP set: Caleb\_PROD\_IPSET  - 115.42.252.58/32  - 128.106.20.192/26  - 203.116.37.64/26  - 129.126.200.167/32  - 14.161.37.67/32  - 151.192.70.86/32  - 176.175.16.197/32  - 180.255.91.226/32  - 203.116.36.80/28  - 203.116.93.104/32  - 203.127.89.192/28  - 210.245.32.62/32  - 27.74.253.120/32  \* Regex pattern set: AllowAccessToWebPortal  - /CMS/  - /w/ | Block |  |
| 3 | AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | Block |
| CategoryArchiver | Count | Block |
| CategoryContentFetcher | Count |  |
| CategoryEmailClient | Count | Block |
| CategoryHttpLibrary | Count |  |
| CategoryLinkChecker | Count | Block |
| CategoryMiscellaneous | Count | Block |
| CategoryMonitoring | Count | Block |
| CategoryScrapingFramework | Count | Block |
| CategorySearchEngine | Count | Block |
| CategorySecurity | Count | Block |
| CategorySeo | Count | Block |
| CategorySocialMedia | Count |  |
| CategoryAI | Count | Block |
| SignalAutomatedBrowser | Count | Block |
| SignalKnownBotDataCenter | Count |  |
| SignalNonBrowserUserAgent | Count |  |
| TGT\_VolumetricIpTokenAbsent | Count |  |
| TGT\_TokenAbsent | Count |  |
| TGT\_VolumetricSession | Count | Block |
| TGT\_VolumetricSessionMaximum | Count | Block |
| TGT\_SignalAutomatedBrowser | Count | Block |
| TGT\_SignalBrowserAutomationExtension | Count | Block |
| TGT\_SignalBrowserInconsistency | Count | Block |
| TGT\_ML\_CoordinatedActivityLow | Count |  |
| TGT\_ML\_CoordinatedActivityMedium | Count |  |
| TGT\_ML\_CoordinatedActivityHigh | Count |  |
| TGT\_TokenReuseIpLow | Count | Block |
| TGT\_TokenReuseIpMedium | Count | Block |
| TGT\_TokenReuseIpHigh | Count | Block |
| TGT\_TokenReuseCountryHigh | Count | Block |
| TGT\_TokenReuseCountryLow | Count | Block |
| TGT\_TokenReuseCountryMedium | Count | Block |
| TGT\_TokenReuseAsnLow | Count | Block |
| TGT\_TokenReuseAsnMedium | Count | Block |
| TGT\_TokenReuseAsnHigh | Count | Block |
| 4 | FortinetManagedRulesforAWSWAF-CompleteOWASPTop10  (with special scope of inspection mentioned below, this rule is for the requests that doesn’t matches the special URIs pattern) | Cross-Site-Scripting-01 | Count | Block |
| Cross-Site-Scripting-02 | Count | Block |
| Cross-Site-Scripting-03 | Count | Block |
| SQL-Injection-01 | Block |  |
| SQL-Injection-02 | Block |  |
| SQL-Injection-03 | Block |  |
| Malicious-Robot | Block |  |
| Web-Scanner-01 | Block |  |
| Web-Scanner-02 | Block |  |
| Web-Scanner-03 | Block |  |
| OS-Command-Injection-01 | Block |  |
| OS-Command-Injection-02 | Block |  |
| Web-Application-Injection-01 | Block |  |
| Web-Application-Injection-02 | Block |  |
| Source-Code-Disclosure | Block |  |
| Database-Vulnerability-Exploit-01 | Block |  |
| Database-Vulnerability-Exploit-02 | Block |  |
| Database-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-01 | Block |  |
| Web-Server-Vulnerability-Exploit-02 | Block |  |
| Web-Server-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-01 | Block |  |
| Web-Application-Vulnerability-Exploit-02 | Block |  |
| Web-Application-Vulnerability-Exploit-03 | Block |  |
| Web-Application-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-05 | Block |  |
| Web-Application-Vulnerability-Exploit-06 | Block |  |
| Web-Application-Vulnerability-Exploit-07 | Block |  |
| 5 | BlanketLimitRequest | Request aggregation: Source IP address  Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 600  Evaluation window: 1 min  Action: Block |
| 6 | LogAllUnmatchedTraffic |  | Allow |  |

**The goal of the inspection setting for the rule “**FortinetManagedRulesforAWSWAF-CompleteOWASPTop10**”:**

* Exclude all traffic to whitelisted URIs
* Exclude only POST requests to whitelisted URIs
* Apply Fortinet WAF to everything else

**Setup for Regex pattern set:**

| **#** | **Setting** | **Value** |
| --- | --- | --- |
| 1 | Regex pattern set name | caleb-portal-uri-whitelisted |
| 2 | Description - *optional* | Whitelisted URI pattern for Caleb Portal |
| 3 | Region | Global (CloudFront) |
| 4 | Regular expressions | ^/w/notification/preview$  ^/w/notification/task/add$  ^/w/notification/task/\d+/edit$  ^/w/notification/template/\d+/edit$  ^/w/notification/template/add$  ^/w/wearable/request/status$  ^/w/notification/task/add/preverify  ^/w/notification/task/\d+/edit/preverify  ^/w/gamification/add$  ^/w/gamification/\d+/edit$ |

**FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 - Special scope of inspection**

| **#** | **Setting** | **Value** |
| --- | --- | --- |
| 1 | Choose the scope of inspection | Only inspect requests that match a scope-down statement |
| 2 | If a request | Matches all the statements (AND) |

**NOT statement 1**

| **#** | **Setting** | **Value** |
| --- | --- | --- |
| 1 | Negate statement (NOT) | Negate statement results |
| 2 | Inspect | URI path |
| 3 | Match type | Matches pattern from regex pattern set |
| 4 | Regex pattern set | caleb-portal-uri-whitelisted |
| 5 | Text transformation | Lowercase |

**NOT statement 2**

| **#** | **Setting** | **Value** |
| --- | --- | --- |
| 1 | Negate statement (NOT) | Negate statement results |
| 2 | Inspect | HTTP method |
| 3 | Match type | Exactly matches string |
| 4 | Regex pattern set | POST |
| 5 | Text transformation | Lowercase |

* **WAF SmartBuddy\_Ischool\_Portal\_PROD\_WAFv2**

| **#** | **Rules** | **Sub-Rules** | **Current Setting** | **Proposed New Setting (If have)** |
| --- | --- | --- | --- | --- |
| 1 | AWS-AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | Block |
| AWSManagedReconnaissanceList | Count | Block |
| AWSManagedIPDDoSList | Count | Block |
| 2 | AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | Block |
| CategoryArchiver | Count | Block |
| CategoryContentFetcher | Count |  |
| CategoryEmailClient | Count | Block |
| CategoryHttpLibrary | Count |  |
| CategoryLinkChecker | Count | Block |
| CategoryMiscellaneous | Count | Block |
| CategoryMonitoring | Count | Block |
| CategoryScrapingFramework | Count | Block |
| CategorySearchEngine | Count | Block |
| CategorySecurity | Count | Block |
| CategorySeo | Count | Block |
| CategorySocialMedia | Count | Block |
| CategoryAI | Count | Block |
| SignalAutomatedBrowser | Count | Block |
| SignalKnownBotDataCenter | Count |  |
| SignalNonBrowserUserAgent | Count |  |
| TGT\_VolumetricIpTokenAbsent | Count |  |
| TGT\_TokenAbsent | Count |  |
| TGT\_VolumetricSession | Count | Block |
| TGT\_VolumetricSessionMaximum | Count | Block |
| TGT\_SignalAutomatedBrowser | Count | Block |
| TGT\_SignalBrowserAutomationExtension | Count | Block |
| TGT\_SignalBrowserInconsistency | Count | Block |
| TGT\_ML\_CoordinatedActivityLow | Count |  |
| TGT\_ML\_CoordinatedActivityMedium | Count |  |
| TGT\_ML\_CoordinatedActivityHigh | Count |  |
| TGT\_TokenReuseIpLow | Count | Block |
| TGT\_TokenReuseIpMedium | Count | Block |
| TGT\_TokenReuseIpHigh | Count | Block |
| TGT\_TokenReuseCountryLow | Count | Block |
| TGT\_TokenReuseCountryMedium | Count | Block |
| TGT\_TokenReuseCountryHigh | Count | Block |
| TGT\_TokenReuseAsnLow | Count | Block |
| TGT\_TokenReuseAsnMedium | Count | Block |
| TGT\_TokenReuseAsnHigh | Count | Block |
| 3 | FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-01 | Count | Block |
| Cross-Site-Scripting-02 | Count | Block |
| Cross-Site-Scripting-03 | Count | Block |
| SQL-Injection-01 | Block |  |
| SQL-Injection-02 | Block |  |
| SQL-Injection-03 | Block |  |
| Malicious-Robot | Block |  |
| Web-Scanner-01 | Block |  |
| Web-Scanner-02 | Block |  |
| Web-Scanner-03 | Block |  |
| OS-Command-Injection-01 | Block |  |
| OS-Command-Injection-02 | Block |  |
| Web-Application-Injection-01 | Block |  |
| Web-Application-Injection-02 | Block |  |
| Source-Code-Disclosure | Block |  |
| Database-Vulnerability-Exploit-01 | Block |  |
| Database-Vulnerability-Exploit-02 | Block |  |
| Database-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-01 | Block |  |
| Web-Server-Vulnerability-Exploit-02 | Block |  |
| Web-Server-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-01 | Block |  |
| Web-Application-Vulnerability-Exploit-02 | Block |  |
| Web-Application-Vulnerability-Exploit-03 | Block |  |
| Web-Application-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-05 | Block |  |
| Web-Application-Vulnerability-Exploit-06 | Block |  |
| Web-Application-Vulnerability-Exploit-07 | Block |  |
| 4 | BlanketLimitRequest | Request aggregation: Source IP address  Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 250  Evaluation window: 1 min  Action: Block |
| 5 | LogAllUnmatchedTraffic |  | Allow |  |

* **WAF SmartBuddy\_Ischool\_API\_PROD\_WAFv2**

| **#** | **Rules** | **Sub-Rules** | **Current Setting** | **Proposed New Setting (If have)** |
| --- | --- | --- | --- | --- |
| 1 | AWS-AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | Block |
| AWSManagedReconnaissanceList | Count | Block |
| AWSManagedIPDDoSList | Count | Block |
| 2 | AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | Block |
| CategoryArchiver | Count | Block |
| CategoryContentFetcher | Count |  |
| CategoryEmailClient | Count | Block |
| CategoryHttpLibrary | Count |  |
| CategoryLinkChecker | Count | Block |
| CategoryMiscellaneous | Count | Block |
| CategoryMonitoring | Count | Block |
| CategoryScrapingFramework | Count | Block |
| CategorySearchEngine | Count | Block |
| CategorySecurity | Count | Block |
| CategorySeo | Count | Block |
| CategorySocialMedia | Count | Block |
| CategoryAI | Count | Block |
| SignalAutomatedBrowser | Count | Block |
| SignalKnownBotDataCenter | Count |  |
| SignalNonBrowserUserAgent | Count |  |
| TGT\_VolumetricIpTokenAbsent | Count |  |
| TGT\_TokenAbsent | Count |  |
| TGT\_VolumetricSession | Count | Block |
| TGT\_VolumetricSessionMaximum | Count | Block |
| TGT\_SignalAutomatedBrowser | Count | Block |
| TGT\_SignalBrowserAutomationExtension | Count | Block |
| TGT\_SignalBrowserInconsistency | Count | Block |
| TGT\_ML\_CoordinatedActivityLow | Count |  |
| TGT\_ML\_CoordinatedActivityMedium | Count |  |
| TGT\_ML\_CoordinatedActivityHigh | Count |  |
| TGT\_TokenReuseIpLow | Count | Block |
| TGT\_TokenReuseIpMedium | Count | Block |
| TGT\_TokenReuseIpHigh | Count | Block |
| TGT\_TokenReuseCountryLow | Count | Block |
| TGT\_TokenReuseCountryMedium | Count | Block |
| TGT\_TokenReuseCountryHigh | Count | Block |
| TGT\_TokenReuseAsnLow | Count | Block |
| TGT\_TokenReuseAsnMedium | Count | Block |
| TGT\_TokenReuseAsnHigh | Count | Block |
| 3 | FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-01 | Count | Block |
| Cross-Site-Scripting-02 | Count | Block |
| Cross-Site-Scripting-03 | Count | Block |
| SQL-Injection-01 | Block |  |
| SQL-Injection-02 | Block |  |
| SQL-Injection-03 | Block |  |
| Malicious-Robot | Block |  |
| Web-Scanner-01 | Block |  |
| Web-Scanner-02 | Block |  |
| Web-Scanner-03 | Block |  |
| OS-Command-Injection-01 | Block |  |
| OS-Command-Injection-02 | Block |  |
| Web-Application-Injection-01 | Block |  |
| Web-Application-Injection-02 | Block |  |
| Source-Code-Disclosure | Block |  |
| Database-Vulnerability-Exploit-01 | Block |  |
| Database-Vulnerability-Exploit-02 | Block |  |
| Database-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-01 | Block |  |
| Web-Server-Vulnerability-Exploit-02 | Block |  |
| Web-Server-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-01 | Block |  |
| Web-Application-Vulnerability-Exploit-02 | Block |  |
| Web-Application-Vulnerability-Exploit-03 | Block |  |
| Web-Application-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-05 | Block |  |
| Web-Application-Vulnerability-Exploit-06 | Block |  |
| Web-Application-Vulnerability-Exploit-07 | Block |  |
| 4 | BlanketLimitRequest | Request aggregation: Source IP address  Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 400  Evaluation window: 1 min  Action: Block |
| 5 | LogAllUnmatchedTraffic |  | Allow |  |

* **WAF SmartBuddy\_SSS\_PROD\_WAFv2**

| **#** | **Rules** | **Sub-Rules** | **Current Setting** | **Proposed New Setting (If have)** |
| --- | --- | --- | --- | --- |
| 1 | AWS-AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | Block |
| AWSManagedReconnaissanceList | Count | Block |
| AWSManagedIPDDoSList | Count | Block |
| 2 | AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | Block |
| CategoryArchiver | Count | Block |
| CategoryContentFetcher | Count | Block |
| CategoryEmailClient | Count | Block |
| CategoryHttpLibrary | Count |  |
| CategoryLinkChecker | Count | Block |
| CategoryMiscellaneous | Count | Block |
| CategoryMonitoring | Count | Block |
| CategoryScrapingFramework | Count | Block |
| CategorySearchEngine | Count | Block |
| CategorySecurity | Count | Block |
| CategorySeo | Count | Block |
| CategorySocialMedia | Count | Block |
| CategoryAI | Count | Block |
| SignalAutomatedBrowser | Count | Block |
| SignalKnownBotDataCenter | Count |  |
| SignalNonBrowserUserAgent | Count |  |
| TGT\_VolumetricIpTokenAbsent | Count |  |
| TGT\_TokenAbsent | Count |  |
| TGT\_VolumetricSession | Count | Block |
| TGT\_VolumetricSessionMaximum | Count | Block |
| TGT\_SignalAutomatedBrowser | Count | Block |
| TGT\_SignalBrowserAutomationExtension | Count | Block |
| TGT\_SignalBrowserInconsistency | Count | Block |
| TGT\_ML\_CoordinatedActivityLow | Count |  |
| TGT\_ML\_CoordinatedActivityMedium | Count |  |
| TGT\_ML\_CoordinatedActivityHigh | Count |  |
| TGT\_TokenReuseIpLow | Count | Block |
| TGT\_TokenReuseIpMedium | Count | Block |
| TGT\_TokenReuseIpHigh | Count | Block |
| TGT\_TokenReuseCountryLow | Count | Block |
| TGT\_TokenReuseCountryMedium | Count | Block |
| TGT\_TokenReuseCountryHigh | Count | Block |
| TGT\_TokenReuseAsnLow | Count | Block |
| TGT\_TokenReuseAsnMedium | Count | Block |
| TGT\_TokenReuseAsnHigh | Count | Block |
| 3 | FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-01 | Count | Block |
| Cross-Site-Scripting-02 | Count | Block |
| Cross-Site-Scripting-03 | Count | Block |
| SQL-Injection-01 | Block |  |
| SQL-Injection-02 | Block |  |
| SQL-Injection-03 | Block |  |
| Malicious-Robot | Block |  |
| Web-Scanner-01 | Block |  |
| Web-Scanner-02 | Block |  |
| Web-Scanner-03 | Block |  |
| OS-Command-Injection-01 | Block |  |
| OS-Command-Injection-02 | Block |  |
| Web-Application-Injection-01 | Block |  |
| Web-Application-Injection-02 | Block |  |
| Source-Code-Disclosure | Block |  |
| Database-Vulnerability-Exploit-01 | Block |  |
| Database-Vulnerability-Exploit-02 | Block |  |
| Database-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-01 | Block |  |
| Web-Server-Vulnerability-Exploit-02 | Block |  |
| Web-Server-Vulnerability-Exploit-03 | Block |  |
| Web-Server-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-01 | Block |  |
| Web-Application-Vulnerability-Exploit-02 | Block |  |
| Web-Application-Vulnerability-Exploit-03 | Block |  |
| Web-Application-Vulnerability-Exploit-04 | Block |  |
| Web-Application-Vulnerability-Exploit-05 | Block |  |
| Web-Application-Vulnerability-Exploit-06 | Block |  |
| Web-Application-Vulnerability-Exploit-07 | Block |  |
| 4 | BlanketLimitRequest | Request aggregation: Source IP address  Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 1000  Evaluation window: 1 min  Action: Count | Rate limit: 600  Evaluation window: 1 min  Action: Block |
| 5 | LogAllUnmatchedTraffic |  | Allow |  |

# ANALYZE DETAIL

**Log Query Command:**

1. Query blocked requests

fields timestamp, action, ruleGroupList.0.ruleGroupId, httpRequest.clientIp, httpRequest.host, httpRequest.uri, httpRequest, @message, @logStream, @log

| filter action like "BLOCK"

| sort timestamp desc

1. Query counted requests:

fields @timestamp, @message

| filter @message like '{"ruleGroupId":"<Rule Name>"'

| parse @message '{"ruleGroupId":"<Rule Name>"\*' as info

| parse info ',"nonTerminatingMatchingRules":[\*]}]' as nonTerminatingMatchingRules

| filter nonTerminatingMatchingRules like '<Sub Rule Name>'

| display @timestamp, httpRequest.clientIp, httpRequest.host, httpRequest.uri, @message

| sort timestamp desc

1. Query number of request per minute

fields @timestamp, httpRequest.clientIp, httpRequest.uri

| stats count(\*) as RequestCount by httpRequest.clientIp, httpRequest.uri, bin(1m)

| sort RequestCount desc

## Queried Data Results

Queried Data Results:

1. **Blocked Requests:**   
   Download URL: https://downloader-uat.styl.solutions/?code=7a0a0b09-f519-429e-9a1a-a2b75324b6f3

Download Code: 09190249-2f83-42e5-91a0-5b9e13ab226a

1. **Counted Requests:**   
   Download URL: <https://downloader-uat.styl.solutions/?code=88f9e079-fa5b-4712-a9cc-612fb347fde0>

Download Code: f4ee2ec6-b90b-4c51-aafb-add51634cc00

\*Note: These download links will expire on May 27th 2026.

## SmartBuddy Caleb PROD

* + 1. Counted Request:

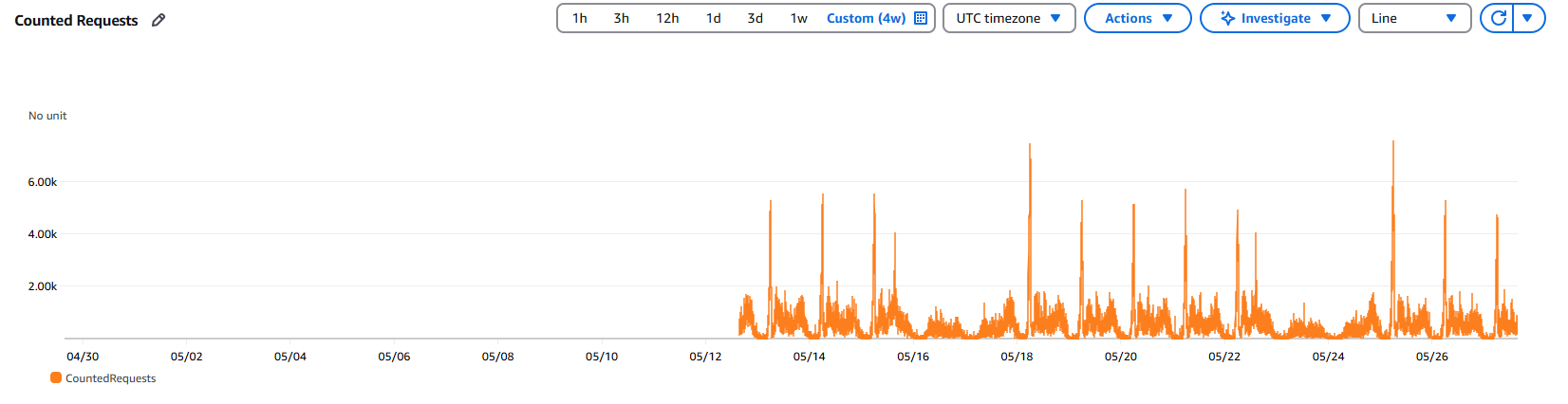


Figure 1: CloudWatch metric number of requests to the system per minute of the WAF Caleb PROD

Number of counted requests based on rules are shown in table below:

| **Rules Name** | **Sub-rules** | **Rule action** | **Counted Requests** |
| --- | --- | --- | --- |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | 311.00 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedReconnaissanceList | Count | 4.00 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPDDoSList | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryArchiver | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryContentFetcher | Count | 408.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryEmailClient | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryHttpLibrary | Count | 1,933,903.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryLinkChecker | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMiscellaneous | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMonitoring | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryScrapingFramework | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySearchEngine | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySecurity | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySeo | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySocialMedia | Count | 25.00 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAI | Count | 20.00 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalKnownBotDataCenter | Count | 427.00 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalNonBrowserUserAgent | Count | 1,939,036.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricIpTokenAbsent | Count | 2,629,387.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenAbsent | Count | 4,645,176.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSession | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSessionMaximum | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalAutomatedBrowser | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserAutomationExtension | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserInconsistency | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityLow | Count | 32,530.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityMedium | Count | 6,909.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityHigh | Count | 50.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpLow | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpMedium | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpHigh | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryLow | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryMedium | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryHigh | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnLow | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnMedium | Count | 0.00 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnHigh | Count | 0.00 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-02 | Count | 138.00 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-03 | Count | 0.00 |

**Table 1**: Number counted requests by rules on WAF SmarBuddy Caleb PROD

Figure 1 presents the graphed metrics of the top 10 managed rules based on the count of requests for SmartBuddy Caleb WAF PROD. This graph representation provides an overview of the frequency of requests attributed to each rule, aiding in understanding the traffic patterns and rule effectiveness.

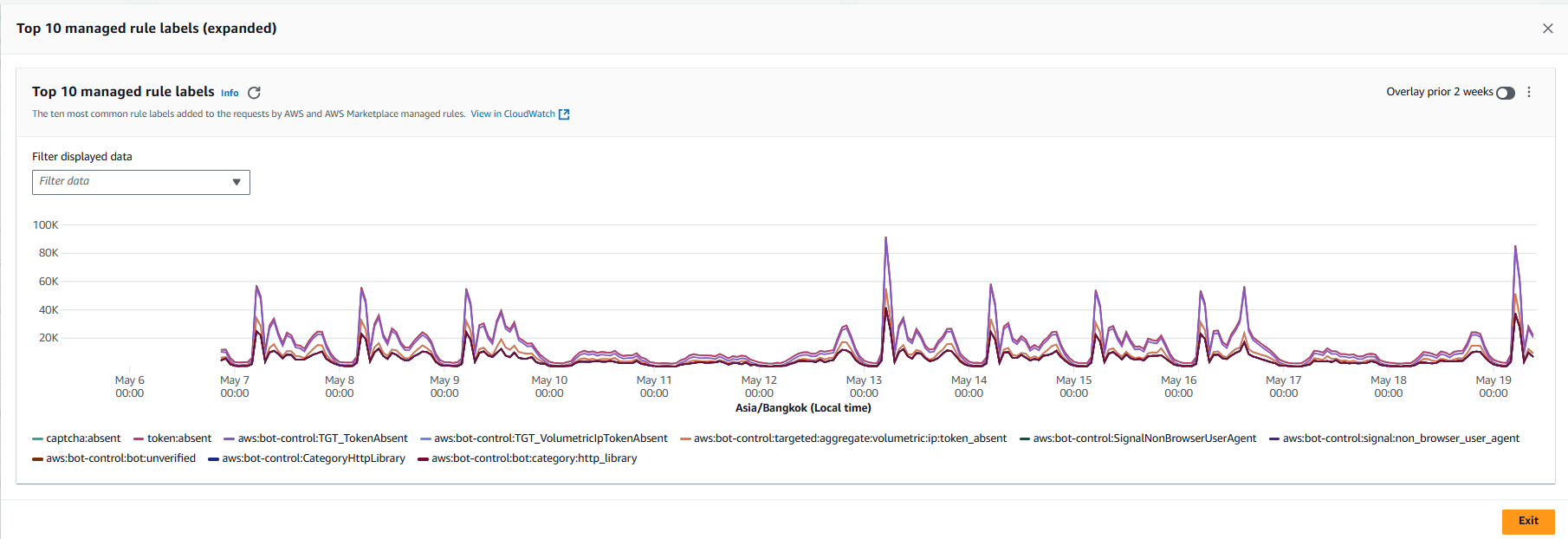
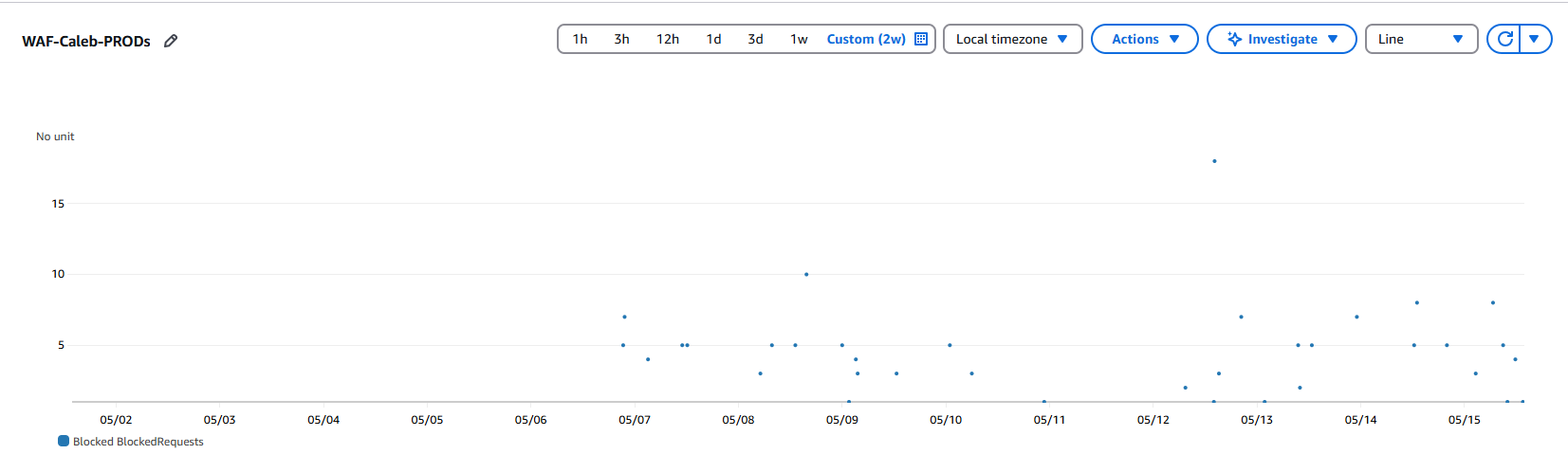


Figure 2: Graphed metrics of Top 10 managed rules counted requests SmartBuddy Caleb WAF PROD

* + 1. Blocked Requests:
* Number of blocker records: 174
* Blocked by rule: AWSManagedRulesAmazonIpReputationList (100%)
* Blocked Reason: IP addresses that have been identified as actively engaging in malicious activities

| **Country of IP Source** | **Number of requests** | **% per total** |
| --- | --- | --- |
| VN | 14 | 8.05% |
| DE | 16 | 9.20% |
| SG | 20 | 11.49% |
| HK | 33 | 18.97% |
| CN | 47 | 27.01% |
| US | 17 | 9.77% |
| PL | 5 | 2.87% |
| NL | 2 | 1.15% |
| UA | 20 | 11.49% |

**Table 2**: Number and percentage of total blocked request on WAF SmarBuddy Caleb



**Figure 3**: Graphed metrics of requests blocked by SmartBuddy Caleb WAF PROD

**4.2.3 Rate Limiting:**

Maximum number of requests per minute: 205

Average number of requests per minute in top 20 most requested client IP: 122.65

| **Client IP** | **URI** | **Time window** | **Rate (per minute)** |
| --- | --- | --- | --- |
| 101.127.8.28 | /child/214434/stats | 2025-05-26 15:33:00.000 | 205 |
| 116.88.10.68 | /child/177838/watch/healthdata/sync | 2025-05-27 15:51:00.000 | 191 |
| 116.89.30.236 | /child/143275/watch/healthdata/sync | 2025-05-18 22:18:00.000 | 189 |
| 111.65.56.176 | /child/213890/stats | 2025-05-21 18:00:00.000 | 180 |
| 116.15.136.170 | /child/213982/stats | 2025-05-22 12:51:00.000 | 180 |
| 58.182.227.53 | /child/135211/watch/healthdata/sync | 2025-05-26 10:51:00.000 | 172 |
| 115.66.60.165 | /child/213590/stats | 2025-05-19 12:04:00.000 | 150 |
| 115.66.212.121 | /child/133058/watch/healthdata/sync | 2025-05-09 11:39:00.000 | 139 |
| 115.66.212.121 | /child/133058/watch/healthdata/sync | 2025-05-09 11:40:00.000 | 118 |
| 218.212.73.103 | /child/201763/watch/healthdata/sync | 2025-05-19 14:26:00.000 | 96 |
| 58.96.200.187 | /child/145645/watch/healthdata/sync | 2025-05-08 14:37:00.000 | 90 |
| 116.15.136.170 | /child/213982/stats | 2025-05-22 12:52:00.000 | 88 |
| 101.127.147.244 | /child/206738/insight/spending/school-expenditure | 2025-05-10 02:59:00.000 | 88 |
| 101.127.147.244 | /child/206738/insight/spending/school-transaction | 2025-05-10 02:59:00.000 | 88 |
| 116.87.172.184 | /child/190430/watch/healthdata/sync | 2025-05-21 23:04:00.000 | 82 |
| 119.234.34.141 | /child/160683/watch/healthdata/sync | 2025-05-22 13:23:00.000 | 80 |
| 202.133.222.69 | /child/180364/watch/healthdata/sync | 2025-05-27 22:57:00.000 | 80 |
| 101.127.171.146 | /child/63328/watch/healthdata/sync | 2025-05-18 15:43:00.000 | 80 |
| 202.133.222.69 | /child/180364/watch/hr/newsync | 2025-05-27 22:58:00.000 | 79 |
| 103.252.200.111 | /child/179830/watch/healthdata/sync | 2025-05-20 12:59:00.000 | 78 |

**Table 3**: Most accessed URI and request rate on WAF SmarBuddy Caleb

## 4.3 SmartBuddy iSchool Portal PROD

4.3.1 Counted Requests Analysis:

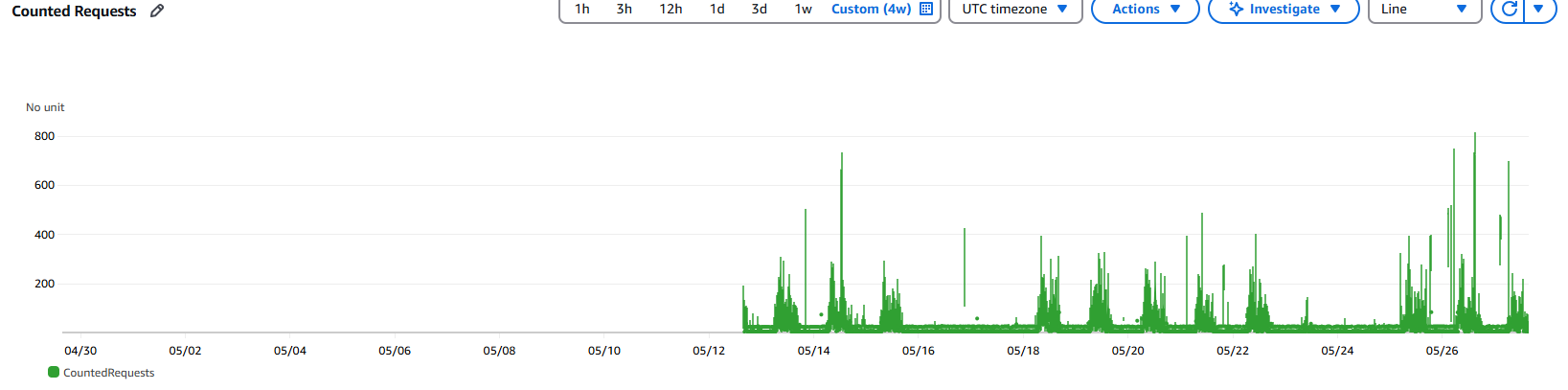
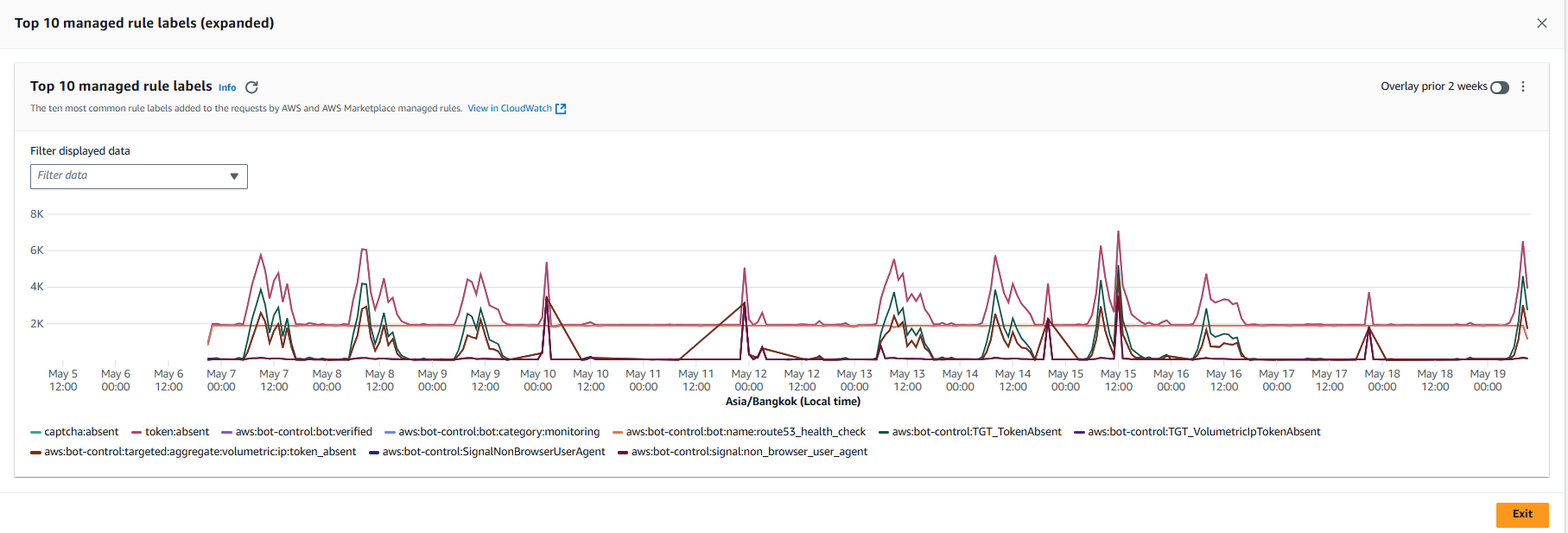


Figure 4: CloudWatch metric number of requests to the system per minute of the WAF Ischool Portal PROD

Count Rule:

| **Rules Name** | **Sub-Rules** | **Rule action** | **Counted Requests** |
| --- | --- | --- | --- |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | 230 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedReconnaissanceList | Count | 2 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPDDoSList | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryArchiver | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryContentFetcher | Count | 2 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryEmailClient | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryHttpLibrary | Count | 4822 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryLinkChecker | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMiscellaneous | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMonitoring | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryScrapingFramework | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySearchEngine | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySecurity | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySeo | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySocialMedia | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAI | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalKnownBotDataCenter | Count | 261 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalNonBrowserUserAgent | Count | 39355 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricIpTokenAbsent | Count | 151657 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenAbsent | Count | 241018 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSession | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSessionMaximum | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserAutomationExtension | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserInconsistency | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityLow | Count | 6585 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityMedium | Count | 358 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnHigh | Count | 0 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-02 | Count | 0 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-03 | Count | 0 |

**Table 4**: Number counted requests by rules on WAF SmarBuddy Ischool Portal PROD



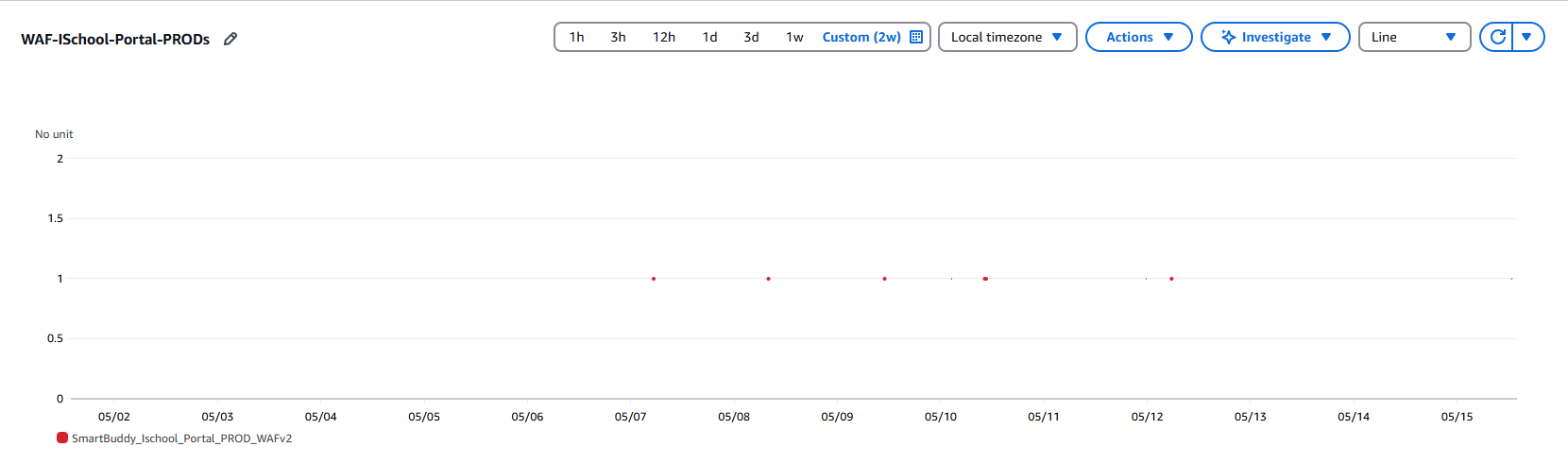
**Figure 5**: Graphed metrics of Top 10 managed rules counted requests SmartBuddy Ischool Portal WAF PROD.

4.3.2 Blocked Requests Analysis:

* Number of blocker records: 27
* Blocked by rule: AWSManagedRulesAmazonIpReputationList (100%)
* Blocked Reason: IP addresses that have been identified as actively engaging in malicious activities

| **Country of IP Source** | **Number of requests** | **% per total** |
| --- | --- | --- |
| IE | 16 | 59.26% |
| US | 11 | 40.74% |

**Table 4**: Number and percentage of total blocked request on WAF SmarBuddy Ischool Portal



**Figure 6**: Graphed metrics of requests blocked by SmartBuddy ISchool Portal WAF PROD

4.3.3 **Rate Limiting**:

Maximum number of requests per minute: 80

Average number of requests per minute in top 20 most requested client IP: 52.84

| **Client IP** | **URI** | **Time window** | **Rate (per minute)** |
| --- | --- | --- | --- |
| 204.48.20.64 | / | 2025-05-21 05:29:00.000 | 80 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-23 03:21:00.000 | 73 |
| 204.48.20.64 | / | 2025-05-21 05:39:00.000 | 60 |
| 180.255.91.226 | /web/assets/img/loading4.gif | 2025-05-27 02:04:00.000 | 60 |
| 180.255.91.226 | /rest/admin/transaction/ | 2025-05-27 02:04:00.000 | 60 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-15 01:21:00.000 | 59 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-15 01:13:00.000 | 55 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-15 01:06:00.000 | 49 |
| 180.255.91.226 | /web/assets/img/loading4.gif | 2025-05-15 01:54:00.000 | 48 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-20 03:32:00.000 | 48 |
| 180.255.91.226 | /rest/admin/transaction/ | 2025-05-15 01:54:00.000 | 48 |
| 180.255.91.226 | /rest/admin/transaction/ | 2025-05-15 01:55:00.000 | 47 |
| 180.255.91.226 | /web/assets/img/loading4.gif | 2025-05-21 01:23:00.000 | 47 |
| 180.255.91.226 | /rest/admin/transaction/ | 2025-05-21 01:23:00.000 | 47 |
| 180.255.91.226 | /rest/school/item/changerequest/checkPendingChangeRequest | 2025-05-19 09:02:00.000 | 47 |
| 180.255.91.226 | /web/assets/img/loading4.gif | 2025-05-15 01:55:00.000 | 47 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-21 02:01:00.000 | 46 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-20 01:30:00.000 | 46 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-07 09:39:00.000 | 45 |
| 180.255.91.226 | /rest/admin/terminal/ | 2025-05-27 02:12:00.000 | 45 |

**Table 6** : Most accessed URI and request rate on WAF SmarBuddy ISchool Portal

## 4.3 SmartBuddy iSchool API PROD

4.3.1 Count Rules:

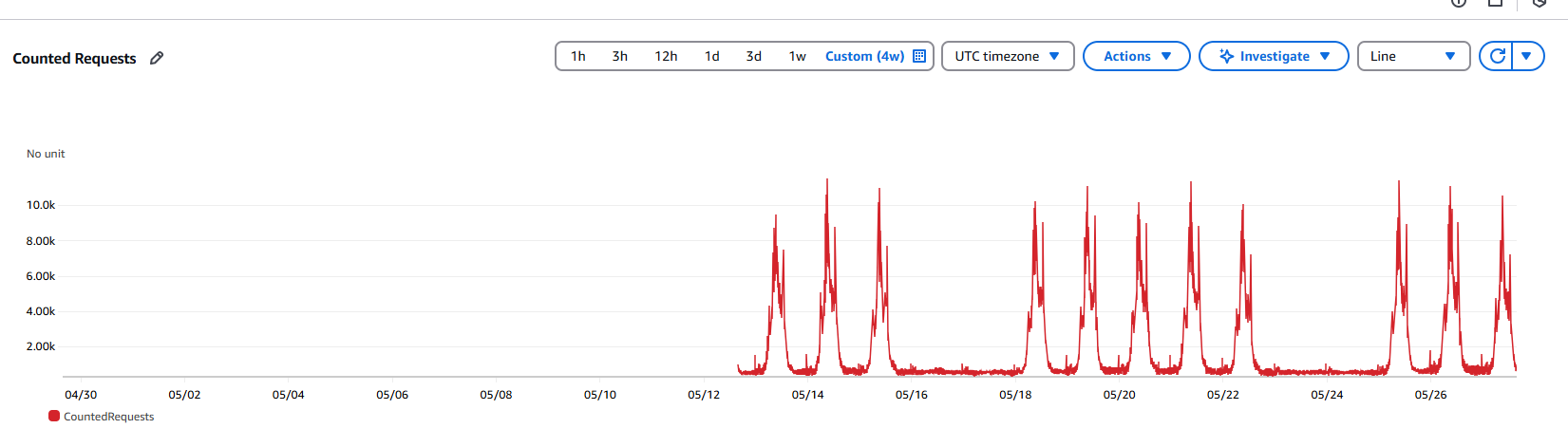
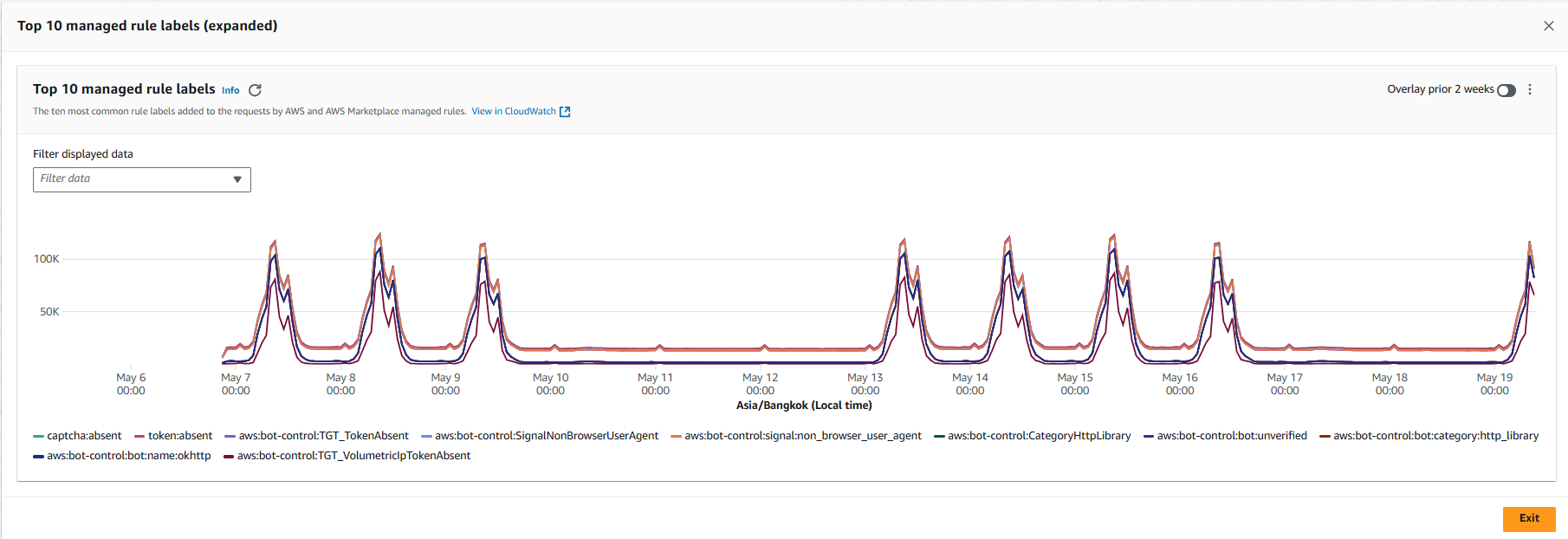


Figure 7: CloudWatch metric number of requests to the system per minute of the WAF Ischool API PROD

| **Rules Name** | **Sub-Rules** | **Rue Action** | **Counted Requests** |
| --- | --- | --- | --- |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | 390 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedReconnaissanceList | Count | 5 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPDDoSList | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryArchiver | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryContentFetcher | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryEmailClient | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryHttpLibrary | Count | 7166650 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryLinkChecker | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMiscellaneous | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMonitoring | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryScrapingFramework | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySearchEngine | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySecurity | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySeo | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySocialMedia | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAI | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalKnownBotDataCenter | Count | 236 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalNonBrowserUserAgent | Count | 11500130 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricIpTokenAbsent | Count | 4198504 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenAbsent | Count | 11505415 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSession | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSessionMaximum | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserAutomationExtension | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserInconsistency | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityLow | Count | 3633672 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityMedium | Count | 1056 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnHigh | Count | 0 |

**Table 7**: Number counted requests by rules on WAF SmarBuddy Ischool API PROD



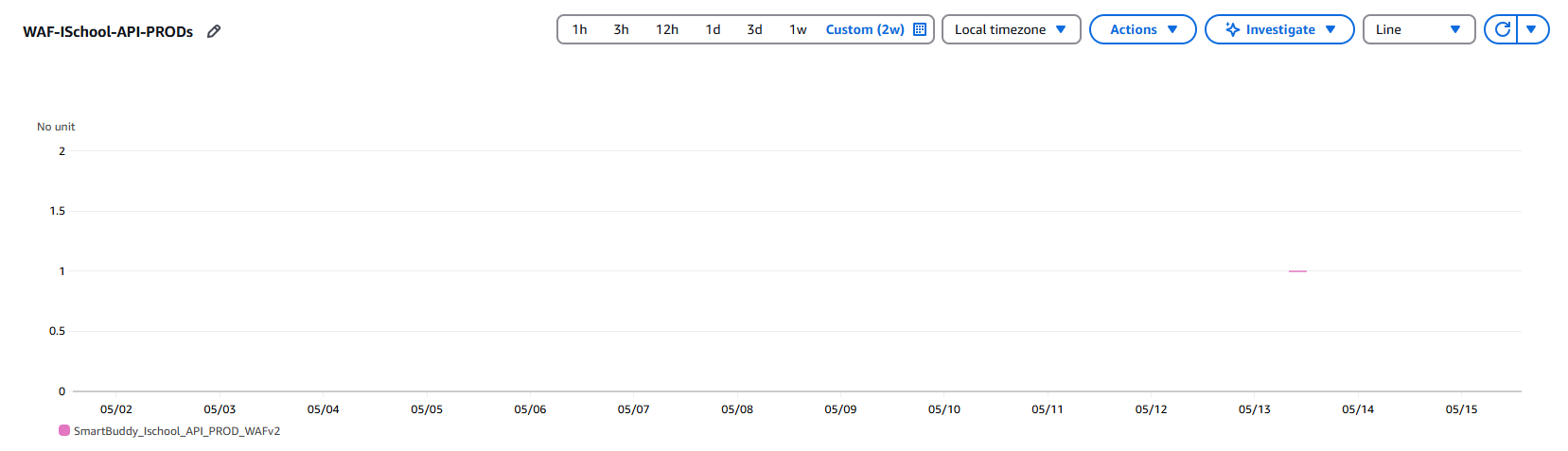
**Figure 8**: Graphed metrics of Top 10 managed rules counted requests SmartBuddy Ischool API WAF PROD.

4.3.2 Blocked Requests:

* Number of blocker records: 3
* Blocked by rule: AWSManagedRulesAmazonIpReputationList (100%)
* Blocked Reason: IP addresses that have been identified as actively engaging in malicious activities

| **Country of IP Source** | **Number of requests** | **% per total** |
| --- | --- | --- |
| US | 3 | 100% |

**Table 8**: Number and percentage of total blocked request on WAF SmarBuddy Ischool Portal



**Figure 9**: Graphed metrics of requests blocked by SmartBuddy ISchool API WAF PROD

**4.3.3 Rate Limiting**

Maximum number of requests per minute: 204

Average number of requests per minute in top 20 most requested client IP: 80.95

| **Client IP** | **URI** | **Time window** | **Rate (per minute)** |
| --- | --- | --- | --- |
| 111.65.46.34 | /terminal/submittxn | 2025-05-21 21:42:00.000 | 204 |
| 111.65.46.229 | /terminal/submittxn | 2025-05-09 06:12:00.000 | 141 |
| 111.65.33.248 | /terminal/submittxn | 2025-05-25 22:14:00.000 | 103 |
| 111.65.46.34 | /terminal/submittxn | 2025-05-21 21:41:00.000 | 92 |
| 111.65.47.225 | /terminal/submittxn | 2025-05-26 03:00:00.000 | 88 |
| 167.172.129.244 | / | 2025-05-21 06:33:00.000 | 68 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-23 17:33:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-26 17:33:00.000 | 66 |
| 111.65.34.219 | /terminal/submittxn | 2025-05-27 23:49:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-24 17:33:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-23 17:39:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-25 17:33:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-27 17:33:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-22 17:39:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-27 17:39:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-25 17:39:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-22 17:33:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-24 17:39:00.000 | 66 |
| 3.1.188.127 | /thirdparty2/store/list | 2025-05-26 17:39:00.000 | 66 |
| 54.255.137.15 | /thirdparty2/store/list | 2025-05-08 17:33:00.000 | 65 |

**Table 9** : Most accessed URI and request rate on WAF SmarBuddy ISchool API

## 4.4 SmartBuddy SSS PROD

4.4.1 Counted Rules:

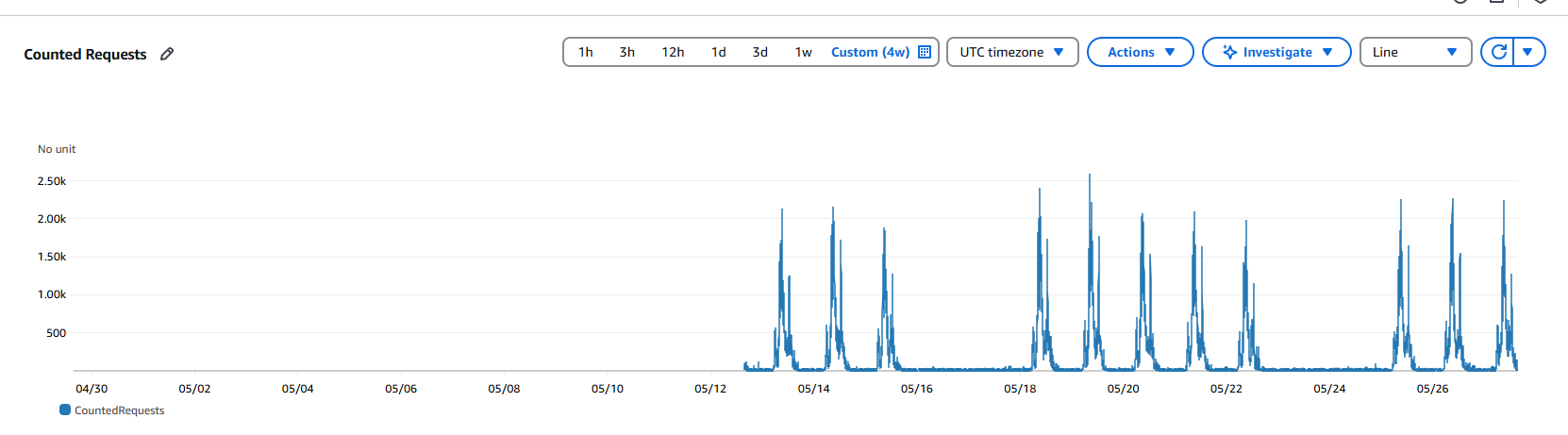
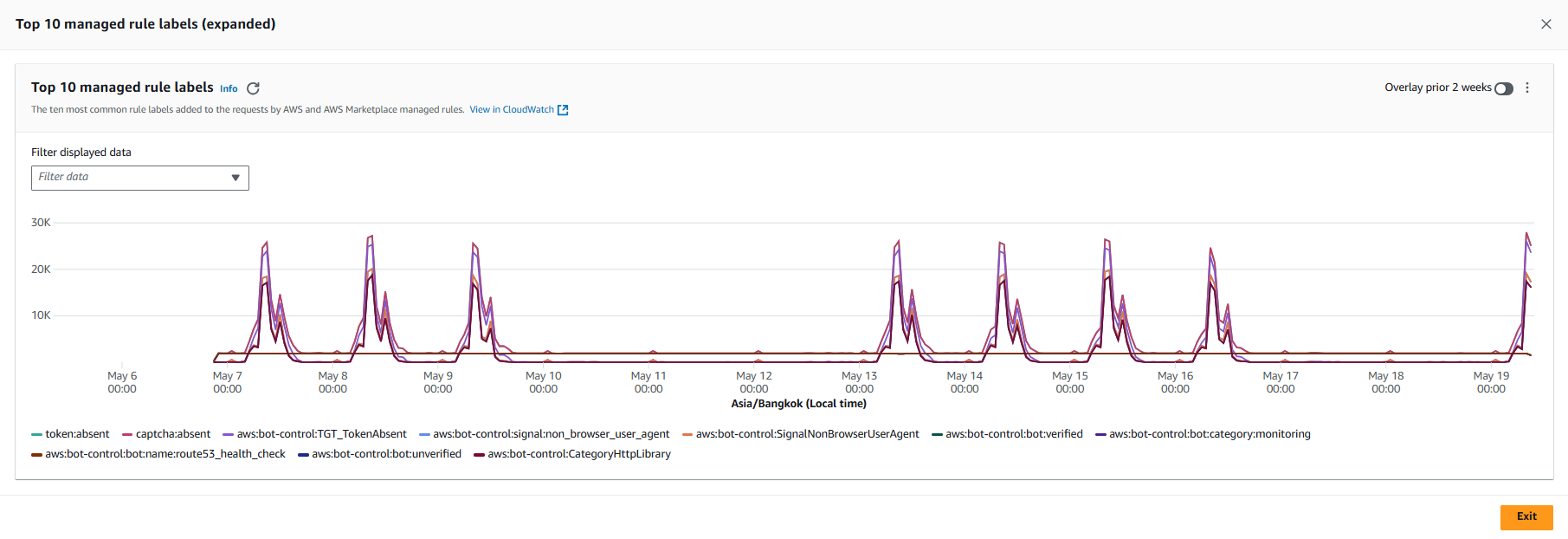


Figure 10: CloudWatch metric number of requests to the system per minute of the WAF SSS PROD

| **Rules Name** | **Sub-rule** | **Rule Action** | **Counted Requests** |
| --- | --- | --- | --- |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPReputationList | Count | 124 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedReconnaissanceList | Count | 5 |
| AWSManagedRulesAmazonIpReputationList | AWSManagedIPDDoSList | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAdvertising | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryArchiver | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryContentFetcher | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryEmailClient | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryHttpLibrary | Count | 738744 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryLinkChecker | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMiscellaneous | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryMonitoring | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryScrapingFramework | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySearchEngine | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySecurity | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySeo | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | CategorySocialMedia | Count | 37 |
| AWS-AWSManagedRulesBotControlRuleSet | CategoryAI | Count | 21 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalKnownBotDataCenter | Count | 30 |
| AWS-AWSManagedRulesBotControlRuleSet | SignalNonBrowserUserAgent | Count | 832013 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricIpTokenAbsent | Count | 474136 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenAbsent | Count | 1116041 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSession | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_VolumetricSessionMaximum | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalAutomatedBrowser | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserAutomationExtension | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_SignalBrowserInconsistency | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityLow | Count | 251231 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityMedium | Count | 4298 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_ML\_CoordinatedActivityHigh | Count | 65 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseIpHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseCountryHigh | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnLow | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnMedium | Count | 0 |
| AWS-AWSManagedRulesBotControlRuleSet | TGT\_TokenReuseAsnHigh | Count | 0 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-02 | Count | 0 |
| FortinetManagedRulesforAWSWAF-CompleteOWASPTop10 | Cross-Site-Scripting-03 | Count | 0 |

**Table 10**: Number counted requests by rules on WAF SmarBuddy SSS PROD



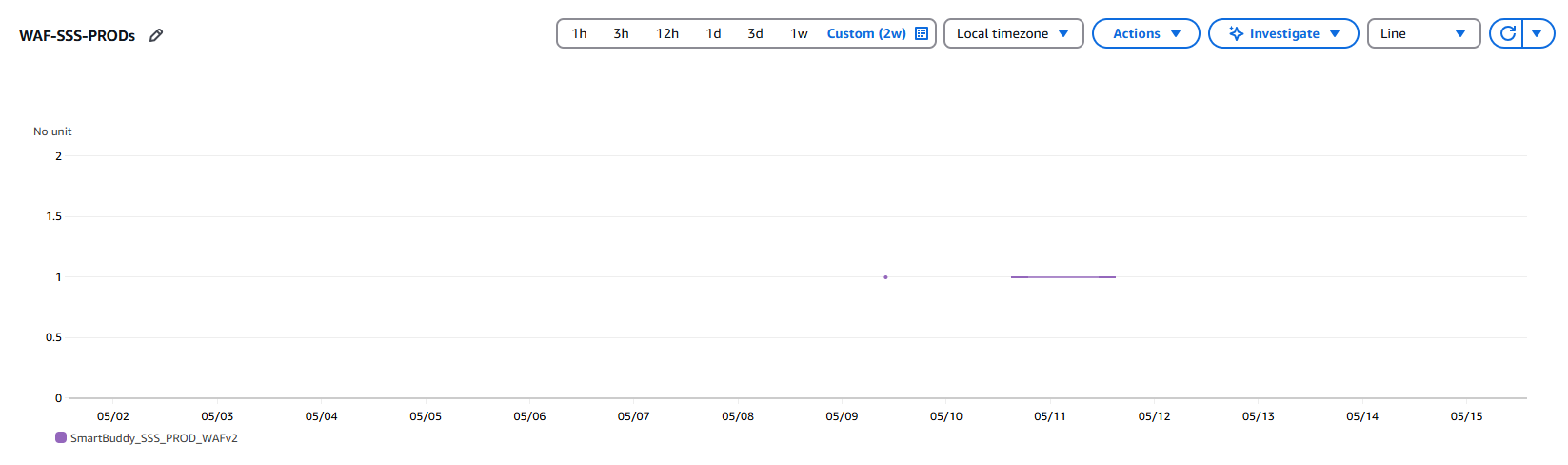
**Figure 11**: Graphed metrics of Top 10 managed rules counted requests SmartBuddy SSS WAF PROD.

4.4.2 Blocked Requests:

* Number of blocker records: 6
* Blocked by rule: AWSManagedRulesAmazonIpReputationList (100%)
* Blocked Reason: IP addresses that have been identified as actively engaging in malicious activities

| **Country of IP Source** | **Number of requests** | **% per total** |
| --- | --- | --- |
| US | 6 | 100% |

**Table 11**: Number and percentage of total blocked request on WAF SmarBuddy SSS



**Figure 12**: Graphed metrics of requests blocked by SmartBuddy SSS WAF PROD

4.4.3 **Rate limit Rule**:

Maximum number of requests per minute: 543

Average number of requests per minute in top 20 most requested client IP: 120.2

| **Client IP** | **URI** | **Time window** | **Rate (per minute)** |
| --- | --- | --- | --- |
| 129.126.34.129 | /rest/school/student/changerequest/page | 2025-05-20 01:30:00.000 | 543 |
| 129.126.34.129 | /rest/school/student/changerequest/page | 2025-05-20 01:31:00.000 | 280 |
| 129.126.34.129 | /rest/school/student/page | 2025-05-20 01:30:00.000 | 275 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:33:00.000 | 88 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:36:00.000 | 88 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:26:00.000 | 86 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:38:00.000 | 85 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:34:00.000 | 84 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:28:00.000 | 82 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:32:00.000 | 80 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:37:00.000 | 77 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:31:00.000 | 76 |
| 129.126.38.113 | /rest/school/student/changerequest/page | 2025-05-13 00:56:00.000 | 75 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:29:00.000 | 74 |
| 129.126.38.113 | /rest/school/student/changerequest/page | 2025-05-13 00:57:00.000 | 73 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:39:00.000 | 70 |
| 129.126.34.133 | /rest/school/student/changerequest/page | 2025-05-08 02:45:00.000 | 68 |
| 129.126.34.99 | /rest/school/student/changerequest/page | 2025-05-09 03:25:00.000 | 67 |
| 129.126.37.87 | /rest/school/student/changerequest/page | 2025-05-14 07:59:00.000 | 67 |
| 129.126.37.151 | /rest/school/student/changerequest/page | 2025-05-23 07:49:00.000 | 66 |

**Table 12** : Most accessed URI and request rate on WAF SmarBuddy SSS

**Contact information**

STYL Solutions Pte Ltd  
81, Ubi Avenue 4  
#05-07, UB.One  
Singapore 408830  
Tel: +65-66948059  
Fax: +65-66948060  
E-mail: [sales@styl.com.sg](mailto:sales@styl.com.sg)