Azure Web Application Firewall Modification required for the WSM PWA

Attempting to access the WSM progressive web app (PWA) was unsuccessful when accessed via the Azure application gateway with the standard, out of the box, OWASP_CRS 3.0 Web Application Firewall (WAF) enabled in Prevention mode (the default). When the WAF was switched to Detection mode, the below log (see *Snippet of Azure WAF Log* and *Azure WAF Log* below) was generated. But the connection was still unsuccessful.

Reviewing the logs indicated the following:

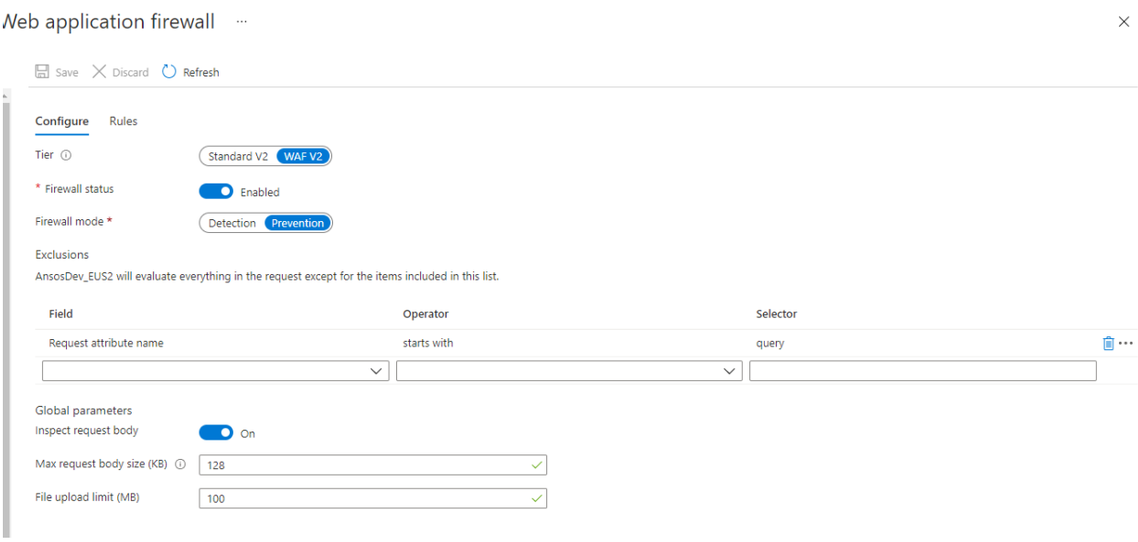
- The rules in question are mandatory, and exclusion rules are needed to successfully connect with the Web PWA.
- If you do a Google search on OWASP_3.0 with the different ruleID (such as 932100), you'll get more information. Basically, the PWA, when querying the database, is causing the WAF to determine there is malicious activity (such as "# of special characters exceeded (12)") occurring and is shutting down the connection from the log below.

After discussion with one of Microsoft's Azure Support Engineers, the presence of "ARGS:" indicates that there is an Attribute causing the errors in question, with the text following the "ARGS" indicating the contents of the attribute (for example, special characters).

With this information from the Azure Engineer, the rule in the below screenshot was implemented. Once implemented, the WAF was switched back to Prevention mode. With the below rule (see WAF Rule below), the PWA was able to successfully access WSM in Prevention mode.

Note about the rule below. When the Field "Request attribute name" is found and it starts with the selector "Query", then the WAF does not prevent the connection. When Hank and Chris discussed this further, we believe there might be a better rule to put in place that is more restrictive, but since we hope that this type of rule won't be needed in the future, we are not investigating this further.

WAF Rule:



Snippet of Azure WAF Log:


```
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932100","message":"Remote Command Execution: Unix Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"942430","message":"Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)","action":"Matched","site":"Global"
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"949110","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Score: 8)","action":"Detected","site":"Global","de
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"980130","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=3,XSS=0,RFI=0,LFI=0,RCE=5,
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932100","message":"Remote Command Execution: Unix Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932110","message":"Remote Command Execution: Windows Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Patte
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932115","message":"Remote Command Execution: Windows Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Patte
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"942430","message":"Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)","action":"Matched","site":"Global"
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"949110","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Score: 18)","action":"Detected","site":"Global","c
,"requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"980130","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Inbound Score: 18 - SQLI=3,XSS=0,RFI=0,LFI=0,RCE=1
```

Azure WAF Log:

{ "timeStamp": "2021-05-24T11:45:58+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932100","message":"Remote Command Execution: Unix Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"(?:;|\\\\{|\\\\|\\\\|\\\\|\\\\||&|&&|\\\\n|\\\\r|\\\\$\\\\(|\\\\$\\\\(\\\\(|`|\\\\${|<\\\\(|>\\\\(|\\\\(\\\\s*\\\\))\\\\s*(?:{|\\\\s*\\\\(\\\\s*|\\\\w+=(?:[^\\\\s]*|\\\\$.*|\\\\$.*|<.*|>.*|\\\\'.*\\\\'|\\\".*\\\")\\\\s+|!\\\\s*|\\\\$)*\\\\s*(?:'|\\\")*(?:[\\\\?*\\\\[\\\\]\\\\(\\\\)\\\\-\\\\|+\\\\w'\\\"\\\\.\/\\\\]+\/)?[\\\\'\\\"]*(?:l[\\\\'\\\"]*(?:w[\\\\'\\\"]*p[\\\\'\\\"]*-[\\\\'\\\"]*(?:d[\\\\'\\\"]*(?:o[\\\\'\\\"]*w[\\\\\" at ARGS:query .... ","data":"Matched Data: {\\\\x0a id\\\\x0a ansosId\\\\x0a wsmAcctId\\\\x0a userName\\\\x0a defaultDisplayName\\\\x0a customDisplayName\\\\x0a dcpos\\\\x0a skill\\\\x0a email\\\\x0a phone\\\\x0a altPhone\\\\x0a defaultRole\\\\x0a areasSA {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a areasEmp {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a saDefaultAreaId\\\\x0a saDefaultPage\\\\x0a empDefaultAreaId\\\\x0a roles\\\\x0a functionAccess {\\\\x0a id\\\\x0a empCalendarViews\\\\x0a ...","file":"rules\/REQUEST-932-APPLICATION-ATTACK-RCE.conf","line":"79"},"hostname":"portal3.myansos.com","transactionId":"3b2e64a4ceed5a05024e4502b93395e4","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:58+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"942430","message":"Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"((?:[\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\\"\\\\'\\\\´\\\\‘\\\\’\\\\`\\\\<\\\\>][^\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&\\\\*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\\"\\\\'\\\\´\\\\‘\\\\’\\\\`\\\\<\\\\>]*?){12})\\\" at ARGS:query .... ","data":"Matched Data: {\\\\x0a userProfile {\\\\x0a id\\\\x0a ansosId\\\\x0a wsmAcctId\\\\x0a userName\\\\x0a defaultDisplayName\\\\x0a customDisplayName\\\\x0a dcpos\\\\x0a skill\\\\x0a email\\\\x0a phone\\\\x0a altPhone\\\\x0a defaultRole\\\\x0a areasSA {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a areasEmp {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a saDefaultAreaId\\\\x0a saDefaultPage\\\\x0a empDefaultAreaId\\\\x0a roles\\\\x0a functionAccess {\\\\x0a id\\\\x0a empCale...","file":"rules\/REQUEST-942-APPLICATION-ATTACK-SQLI.conf","line":"1002"},"hostname":"portal3.myansos.com","transactionId":"3b2e64a4ceed5a05024e4502b93395e4","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:58+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"949110","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Score: 8)","action":"Detected","site":"Global","details":{"message":"Warning. Operator GE matched 5 at TX:anomaly_score. ","data":"","file":"rules\/REQUEST-949-BLOCKING-EVALUATION.conf","line":"57"},"hostname":"portal3.myansos.com","transactionId":"3b2e64a4ceed5a05024e4502b93395e4","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"980130","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Inbound Score: 8 - SQLI=3,XSS=0,RFI=0,LFI=0,RCE=5,PHPI=0,HTTP=0,SESS=0): Restricted SQL Character Anomaly Detection (args): # of special characters exceeded

(12)","action":"Detected","site":"Global","details":{"message":"Warning. Operator GE matched 5 at TX:inbound_anomaly_score. ","data":"","file":"rules\/RESPONSE-980-CORRELATION.conf","line":"73"},"hostname":"portal3.myansos.com","transactionId":"3b2e64a4ceed5a05024e4502b93395e4","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932100","message":"Remote Command Execution: Unix Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"(?:;|\\\\{|\\\\|\\\\|\\\\|&|&&|\\\\n|\\\\r|\\\\$\\\\(|\\\\$\\\\(\\\\(|`|\\\\${|<\\\\(|>\\\\(|\\\\(\\\\s*\\\\))\\\\s*(?:{|\\\\s*\\\\(\\\\s*|\\\\w+=(?:[^\\\\s]*|\\\\$.*|\\\\$.*|<.*|>.*|\\\\'.*\\\\'|\\\".*\\\")\\\\s+|!\\\\s*|\\\\$)*\\\\s*(?:'|\\\")*(?:[\\\\?*\\\\[\\\\]\\\\(\\\\)\\\\-\\\\|+\\\\w'\\\"\\\\.\/\\\\]+\/)?[\\\\'\\\"]*(?:l[\\\\'\\\"]*(?:w[\\\\'\\\"]*p[\\\\'\\\"]*-[\\\\'\\\"]*(?:d[\\\\'\\\"]*(?:o[\\\\'\\\"]*w[\\\" at ARGS:query .... ","data":"Matched Data: {\\\\x0a id\\\\x0a areaId\\\\x0a from\\\\x0a to\\\\x0a notice\\\\x0a periods {\\\\x0a id\\\\x0a from\\\\x0a to\\\\x0a reset\\\\x0a __typename\\\\x0a }\\\\x0a areas {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a skills {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a schEmpTotals {\\\\x0a id\\\\x0a skill\\\\x0a schEmps {\\\\x0a id\\\\x0a employee {\\\\x0a id\\\\x0a name\\\\x0a dcpos\\\\x0a jobClass\\\\x0a s...","file":"rules\/REQUEST-932-APPLICATION-ATTACK-RCE.conf","line":"79"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932110","message":"Remote Command Execution: Windows Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"(?i)(?:;|\\\\{|\\\\|\\\\|\\\\|&|&&|\\\\n|\\\\r|`)\\\\s*[\\\\(,@\\\\'\\\\\"\\\\s]*(?:[\\\\w'\\\\\"\\\\.\/]+\/|[\\\\'\\\\\"\\\\^]*\\\\w[\\\\'\\\\\"\\\\^]*:.*\\\\|[\\\\^\\\\.\\\\w'\\\\\"\/\\\\]*\\\\|)?[\\\\\"\\\\^]*(?:m[\\\\\"\\\\^]*(?:y[\\\\\"\\\\^]*s[\\\\\"\\\\^]*q[\\\\\"\\\\^]*l(?:[\\\\\"\\\\^]*(?:d[\\\\\"\\\\^]*u[\\\\\"\\\\^]*m[\\\\\"\\\\^]*p(?:[\\\\\"\\\\^]*s[\\\\\"\\\\^]*l[\\\\\"\\\\^]*o[\\\\\"\\\\^]*w)?|h[\\\\\"\\\\^]*o[\\\\\"\\\\^]*t[\\\\\"\\\\^]*c[\\\\\"\\\\^]*o[\\\\\"\\\\^]*\\\\\" at ARGS:query .... ","data":"Matched Data: \\\\x0a label\\\\x0a date\\\\x0a team\\\\x0a task\\\\x0a home\\\\x0a duty\\\\x0a order\\\\x0a format\\\\x0a pending\\\\x0a __typename\\\\x0a }\\\\x0a __typename\\\\x0a }\\\\x0a schCounts {\\\\x0a id\\\\x0a date\\\\x0a emps\\\\x0a minutes\\\\x0a __typename\\\\x0a }\\\\x0a __typename\\\\x0a }\\\\x0a __typename found within ARGS:query: query areaSchedule($areaId: AreaId!, $periodStartDate: Date!, $r...","file":"rules\/REQUEST-932-APPLICATION-ATTACK-RCE.conf","line":"183"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"932115","message":"Remote Command Execution: Windows Command Injection","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"(?i)(?:;|\\\\{|\\\\|\\\\|\\\\|&|&&|\\\\n|\\\\r|`)\\\\s*[\\\\(,@\\\\'\\\\\"\\\\s]*(?:[\\\\w'\\\\\"\\\\.\/]+\/|[\\\\'\\\\\"\\\\^]*\\\\w[\\\\'\\\\\"\\\\^]*:.*\\\\|[\\\\^\\\\.\\\\w'\\\\\"\/\\\\]*\\\\|)?[\\\\\"\\\\^]*(?:s[\\\\\"\\\\^]*(?:y[\\\\\"\\\\^]*s[\\\\\"\\\\^]*(?:t[\\\\\"\\\\^]*e[\\\\\"\\\\^]*m[\\\\\"\\\\^]*(?:p[\\\\\"\\\\^]*r[\\\\\"\\\\^]*o[\\\\\"\\\\^]*p[\\\\\"\\\\^]*e[\\\\\"\\\\^]*r[\\\\\"\\\\^]*t[\\\\\"\\\\^]*i[\\\\\"\\\\^]*e[\\\\\"\\\\^]*s[\\\\\"\\\\^]*(?:d[\\\\\"\\\\^]*a[\\\\\"\\\\\\\\\" at ARGS:query .... ","data":"Matched Data: \\\\x0a reset\\\\x0a __typename\\\\x0a }\\\\x0a areas {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a skills {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a schEmpTotals {\\\\x0a id\\\\x0a skill\\\\x0a schEmps {\\\\x0a id\\\\x0a employee {\\\\x0a id\\\\x0a name\\\\x0a dcpos\\\\x0a

jobClass\\\\x0a skillCode\\\\x0a email\\\\x0a phone\\\\x0a __typename\\\\x0a }\\\\x0a assignments {\\\\x0a ...","file":"rules\/REQUEST-932-APPLICATION-ATTACK-RCE.conf","line":"224"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"942430","message":"Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)","action":"Matched","site":"Global","details":{"message":"Warning. Pattern match \\\"((?:[\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\\"\\\\'\\\\´\\\\’\\\\‘\\\\`\\\\<\\\\>][^\\\\~\\\\!\\\\@\\\\#\\\\$\\\\%\\\\^\\\\&\\\\*\\\\(\\\\)\\\\-\\\\+\\\\=\\\\{\\\\}\\\\[\\\\]\\\\|\\\\:\\\\;\\\"\\\\'\\\\´\\\\’\\\\‘\\\\`\\\\<\\\\>]*?){12})\\\" at ARGS:query .... ","data":"Matched Data: ($areaId: AreaId!, $periodStartDate: Date!, $role: UserRole!) { found within ARGS:query: query areaSchedule($areaId: AreaId!, $periodStartDate: Date!, $role: UserRole!) {\\\\x0a areaSchedule(areaId: $areaId, periodStartDate: $periodStartDate, role: $role) {\\\\x0a id\\\\x0a areaId\\\\x0a from\\\\x0a to\\\\x0a notice\\\\x0a periods {\\\\x0a id\\\\x0a from\\\\x0a to\\\\x0a reset\\\\x0a __typename\\\\x0a }\\\\x0a areas {\\\\x0a id\\\\x0a name\\\\x0a __typename\\\\x0a }\\\\x0a ski...","file":"rules\/REQUEST-942-APPLICATION-ATTACK-SQLI.conf","line":"1002"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"949110","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Score: 18)","action":"Detected","site":"Global","details":{"message":"Warning. Operator GE matched 5 at TX:anomaly_score. ","data":"","file":"rules\/REQUEST-949-BLOCKING-EVALUATION.conf","line":"57"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}

{ "timeStamp": "2021-05-24T11:45:59+00:00", "resourceId": "/SUBSCRIPTIONS/CCEBB513-A134-4AE8-ACC1-225BD8CA5658/RESOURCEGROUPS/ANSOS_DEV/PROVIDERS/MICROSOFT.NETWORK/APPLICATIONGATEWAYS/ANSOSDEV_EUS2", "operationName": "ApplicationGatewayFirewall", "category": "ApplicationGatewayFirewallLog", "properties":
{"instanceId":"appgw_0","clientIp":"136.56.26.212","clientPort":"","requestUri":"\/api\/gql","ruleSetType":"OWASP_CRS","ruleSetVersion":"3.0.0","ruleId":"980130","message":"Mandatory rule. Cannot be disabled. Inbound Anomaly Score Exceeded (Total Inbound Score: 18 - SQLI=3,XSS=0,RFI=0,LFI=0,RCE=15,PHPI=0,HTTP=0,SESS=0): Restricted SQL Character Anomaly Detection (args): # of special characters exceeded (12)","action":"Detected","site":"Global","details":{"message":"Warning. Operator GE matched 5 at TX:inbound_anomaly_score. ","data":"","file":"rules\/RESPONSE-980-CORRELATION.conf","line":"73"},"hostname":"portal3.myansos.com","transactionId":"91035b37553f008c69a7032316adc238","policyId":"default","policyScope":"Global","policyScopeName":"Global"}}