Client-Side Protection Dashboard

https://campus.barracuda.com/doc/96012769/

Barracuda Active Threat Intelligence (ATI) provides visibility into changes and the tampering of any external resources, such as JavaScript (JS) and Cascading Style Sheets (CSS) files in the protected application. It also protects against malicious inclusion of such files in the response pages sent to the clients. This feature is configured on the Barracuda WAF using a HTTP Response header called the Content-Security-Policy, a security header defined on the WAF on the **WEBSITES > Client-Side Protection** page. The policy contains directives for various file types and references used by the application. A report-uri directive is also provided and can be used by browsers to report the violations of the policy. For more information on configuring the Client-Side Protection on the WAF, see Client-Side Protection. Analyzing these violations can help the administrator detect any malicious activity within these files. The information can be visualized and analyzed through the Advanced Threat Intelligence dashboard.

The Client-Side Protection dashboard page displays the following information:

Violated Directives Reports

The **Violated Directives Reports** section provides the total number of violations against all CSP directives for the selected period. When a client browser observes any violation against the configured CSP policy, it generates a violation and reports it to the endpoint configured in the **Report URI** or **Report To** fields in the CSP policy. Hover over the graph to view the total count of violations on the directives at a specific time.

By default, all CSP directives are selected in the graph. To see the graph for a particular CSP directive, deselect all other directives apart from the directive for which you want to see the graph. Click on the directive to deselect.

Violations

The **Violations** section displays the total count of violations detected by client browser(s).

Violating Resources

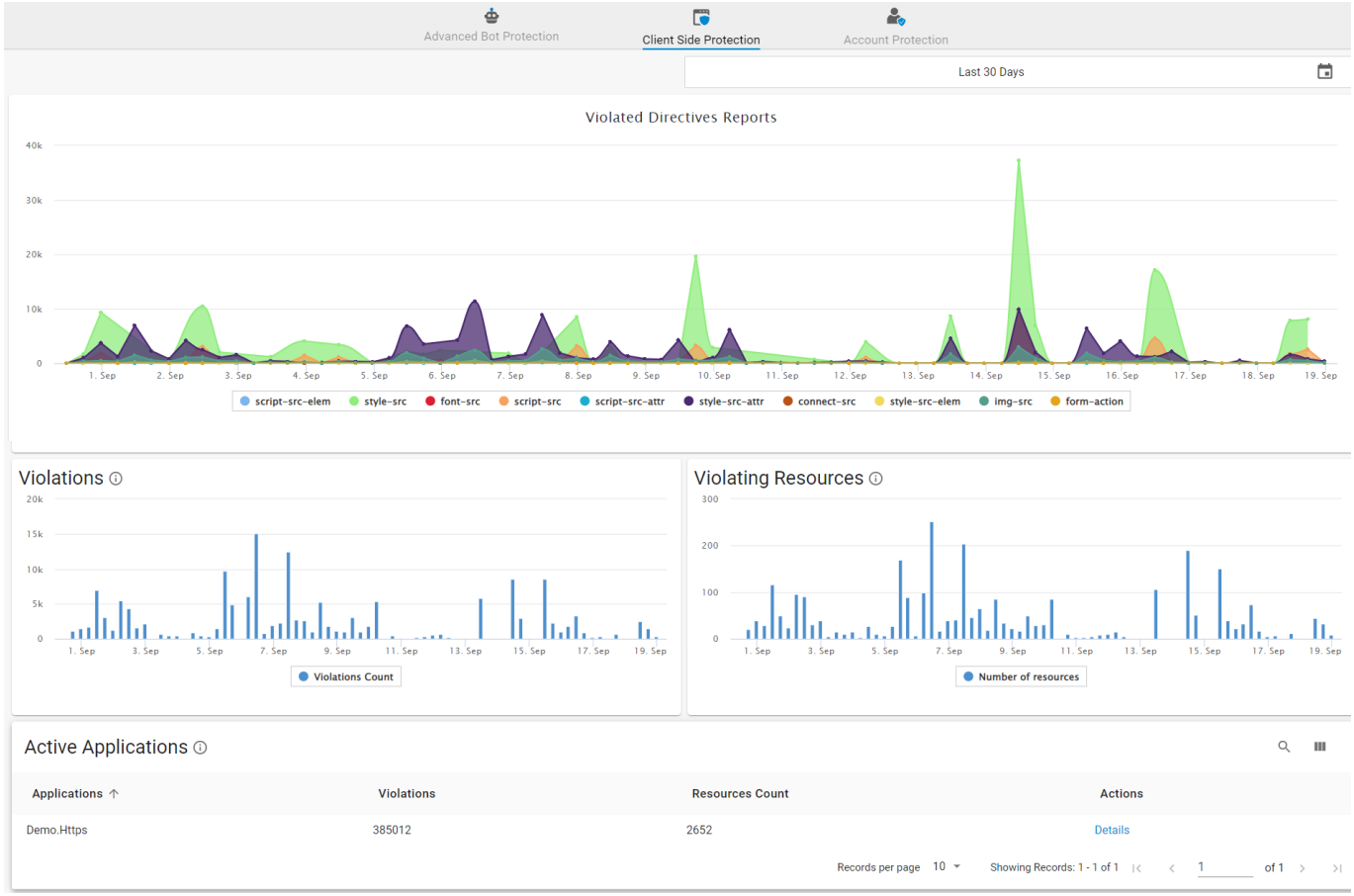
The **Violating Resources** section displays the total number of resources (web pages in the application/service) that violated the configured CSP policy settings.

Active Applications

The **Active Applications** section displays the applications/services that violated the CSP policy settings. The table provides the following details about the applications:

- **Applications**: Name of the application.

- **Violations**: Total number of CSP violations.
- **Resources Count**: Total number of web pages in the application/service for which violation was observed.
- **Actions**: Click **Details** to view the detailed violations data.



The new CSP page provides the following information:

- Dashboard
- Violations
- Policies
- Sources

Figures