Custom Reports

PLATFORM FEATURE UPDATE

Adlumin users now have access to our new Custom Reports feature, which enables you to design custom reports for any device that sends log data to Adlumin.

Dashboard operators will benefit from features including:

- The ability to create reports for a device of your choice using a user-specified custom query.
- A preview feature to help you tailor your custom query and ensure that your report is capturing the appropriate and expected log data.
- On-demand generation of your custom reports with the ability to limit the report content to a specific time period.

Additional functionality will be added over the course of the coming weeks based on user feedback. The Custom Reports feature can be accessed in the *Reports* menu on the navigation bar.

| | Custom Reports | General Reports | |
|----------|---|---------------------------|--|
| 2 | About Create a Report My | Executive Reports | mand Reports Completed Reports |
| | | Scheduled Reports | |
| 7 | Structuring Your Custon | Custom Reports New | |
| | Structure the query used to g can contain multiple strings to | Priviledge Analysis | sased on the format of your log data. Examine incoming log data to determine which strings you can use as parameters for your query. Your custom report query sch separated by a double ampersand (&&). |
| 2. U | In the example below, any inco | NCUA ACET | th the strings src.address=10.0.1.1 and dst_address=192.168.0.1 will be included in the report: |
| | src_address=10.0.1.1 && d: | FFIEC CAT | |
| | | Completed Reports | |
| | Exclusions | | ing specified strings from appearing in your custom report. Any string you wish to exclude from the report should be placed within the NOT() operator. You can |
| | | | double pipe ([]). Any log containing one or more of these strings will be excluded from your custom report. |
| <u>a</u> | Note, the NOT() operator is tre- | ated like any other query | string and must be preceded and/or followed by a double ampersand (&&) |
| | srr address=18.8.1.1.56 dst | addresse=102 169 8 1 | |
| | Name your custom report Select a device | _0001033-132.100.0.1 | 66 N0T(severity-informational userservice_account) |
| | Name your custom report | | |
| | Name your custom report Select a device Enter a query to build your custo | | |
| | Name your custom report Select a device Enter a query to build your custo | om report | |
| | Name your custom report Select a device Enter a query to build your custo | om report uste Report | |

