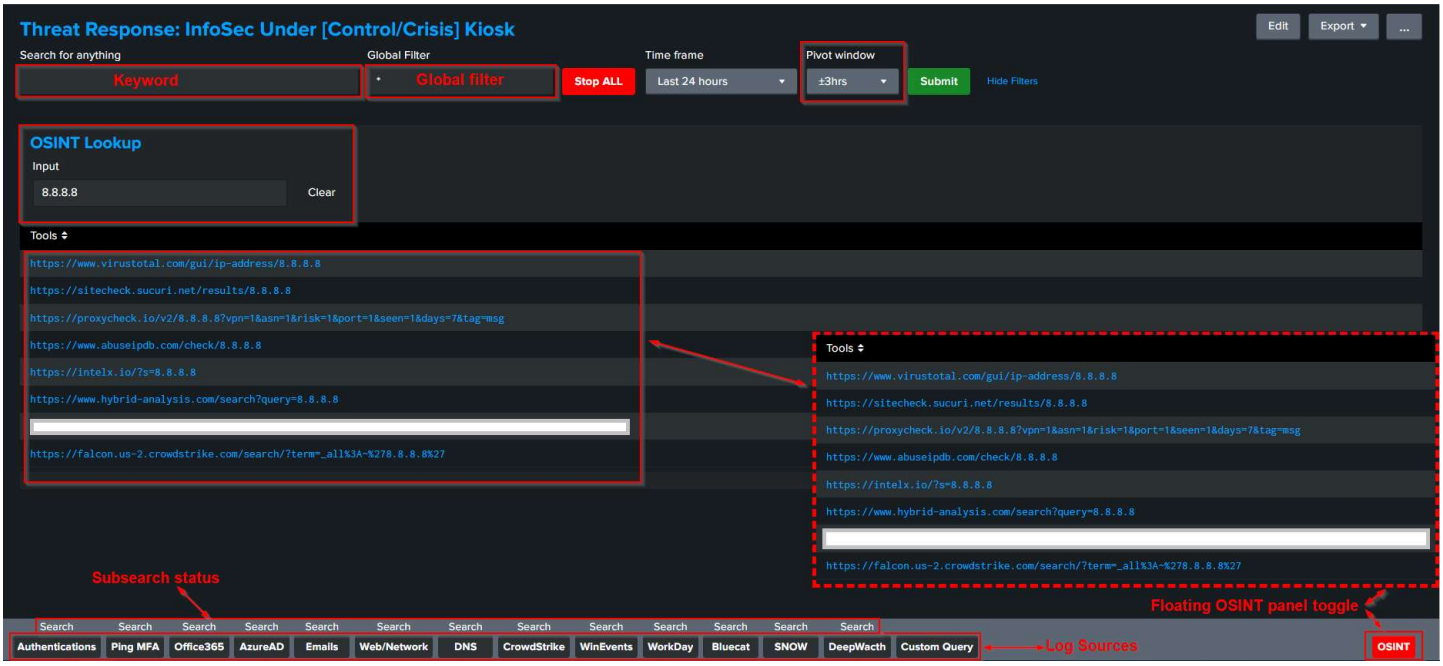
Threat Response: InfoSec Under [Control/Crisis] Kiosk Dashboard

What is it?

- This was made from the idea of “one-stop-shop” for common Splunk searches that you might need to perform when investigate something (included but not limited to: users, host, IP, URL, domain name, a random string, etc.).
- You can do Splunk searches without writing complex Splunk queries, it will search across multiple log sources; Raw data will be normalized to display the essential information for the investigation.

The Interface

Main Page



Keyword: Thing that you want to search for, could be anything. You can use AND/OR operators here.
Global filter: this filter will apply to all sub searches
Stop ALL: stop all searches in case you made an error. Once stopped, one of the inputs (keyword, filter, timeframe) must be changed to re-submit the search.
Pivot window: explain later.

OSINT Lookup: you can use this panel to generate links to common OSINT tools for quick reference. Depends on the input (IP, URL, domain, or string), it will generate links to the relevant tools. It also includes links to our Recorded Future and CrowdStrike.
OSINT button: this will toggle a floating panel with the result of the OSINT Lookup, could be useful when you are in the middle of the dashboard and don't want to scroll all the way up.

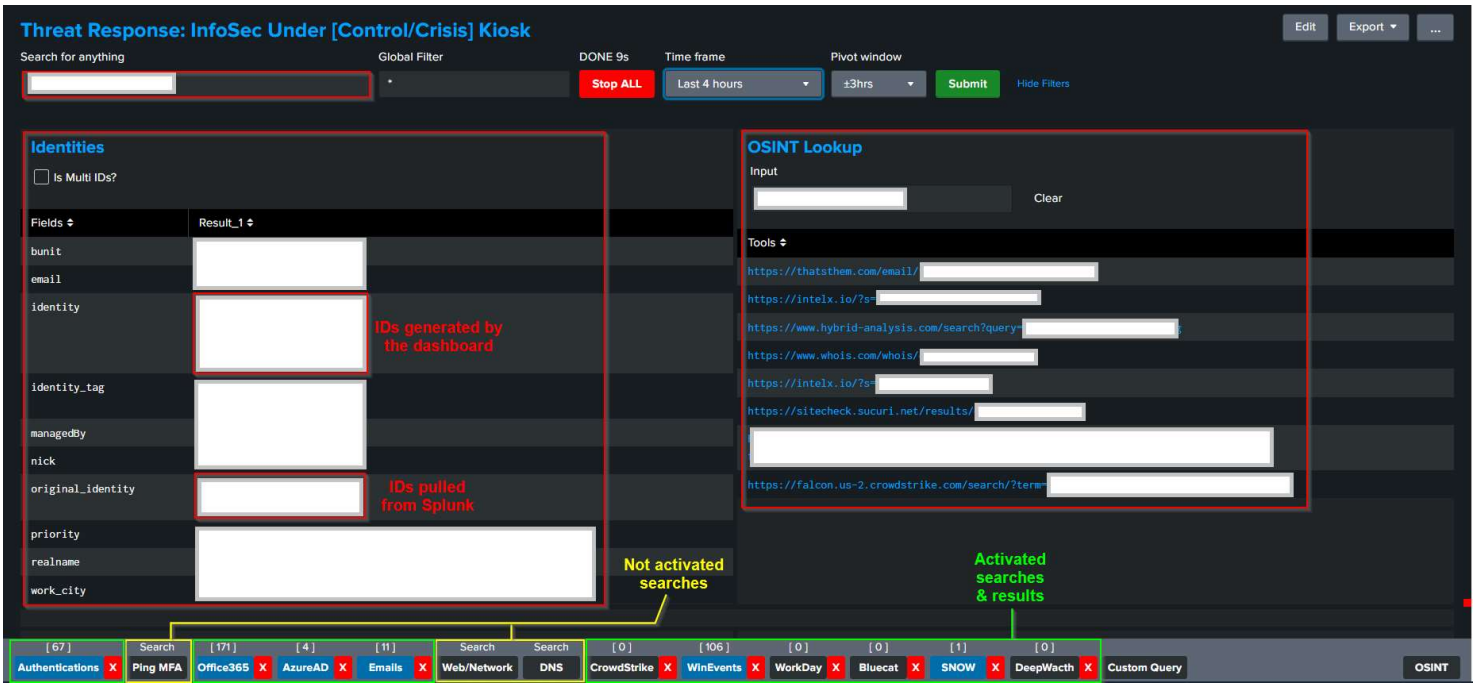
Log Source buttons: The Log Sources that you want to perform searches on. Some scenarios with the Log Source buttons:

- If none of the Log Source were selected, it will search on all sources.

- If the keyword were filled, clicked on any of the buttons will run a search on that Log Source.
- If you want to search on just a few specific Log Sources, **select the Log Sources first** before entering the keyword.

Sub search status: status of each individual search, also display result's count when it's done.

Search Results Sample



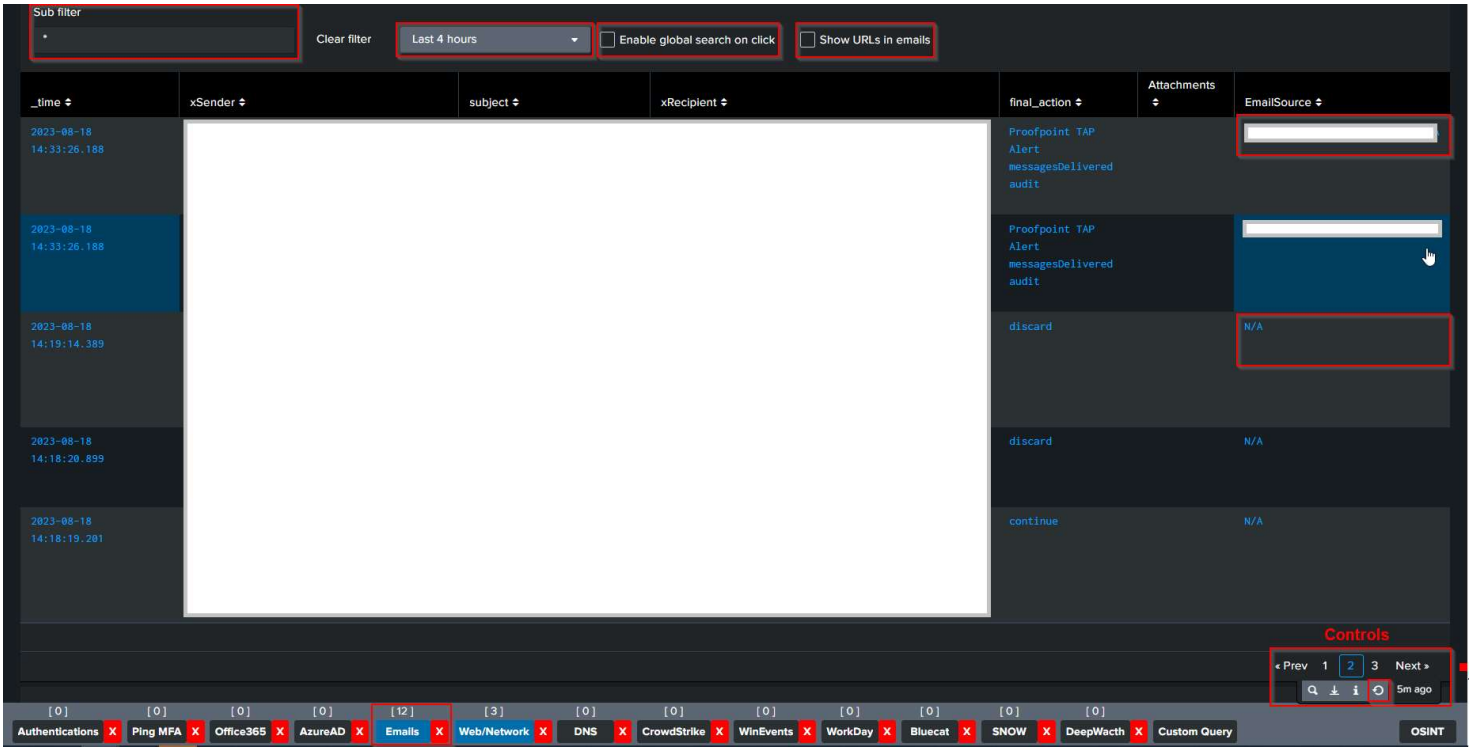
Identities: information in this panel are pulled from the "identity_lookup_expanded" lookup table in Splunk. This panel will not be displayed if the input was not a User ID or User ID was not found. It also generates legacy addresses (@<old_domainname>) to extend the searches.

OSINT Lookup: Links are generated automatically based off the input.

Not Activated Searches: in this example, the "**Ping MFA**", "**Web/Network**" and "**DNS**" were not selected/activated when the initial search run. Click on the buttons will activate the addition searches.

Activated Searches & Results: top numbers are the count of the results, panels with **0 result will be hidden**. Click on any buttons will jump to/expand that particular panel. Click on the "**X**" button will disable that source for the next search of the same session.

Panel Sample



Most of the panels are very similar in general, the sample here is from the “Emails” panel as it has a bit more “extras” to the others.

Sub Filter: apply a local filter to this particular panel. This filter takes free-text input, wildcard, AND/OR operators, “key=value” or an advanced input (see below). Clicking on (almost) any of the clickable items in the panel will populate the sub filter with a “key=value” automatically, it also populates the OSINT Lookup with that clicked item. You can add more filters by typing in or just click on other items to filter further.

Timeframe: this timeframe allows you to apply an individual timeframe for this panel without effecting other panels, in case you want to extend or narrow down just this panel.

Enable Global Search on Click: when this is selected, clicking on any clickable items in the panel with launch a new search for that particular item in a new tab. The timeframe for the new search is within **± X hours** of the clicked event, with **X** is the selected “**Pivot Window**” mentioned earlier.

Show URLs in Emails (only available for Emails panel): show all URLs in the emails, all URLs are clickable items.

EmailSource (only available for Emails panel): if this column is not “N/A”, clicking on it with bring you to the RAW source of the email. You **MUST** be logged-in in TAP first for this to work.

Controls: you can navigate between pages, refresh the panel, open the panel's result in Splunk search, etc. here

Advanced Sub Filter: this sub filter is designed to be “injectable”; You can write an extended query inside of this filter. For example, using this as a sub filter:

** | stats count AS final_action values(xSender) AS xSender BY subject | sort BY final_action*