SOC:OS

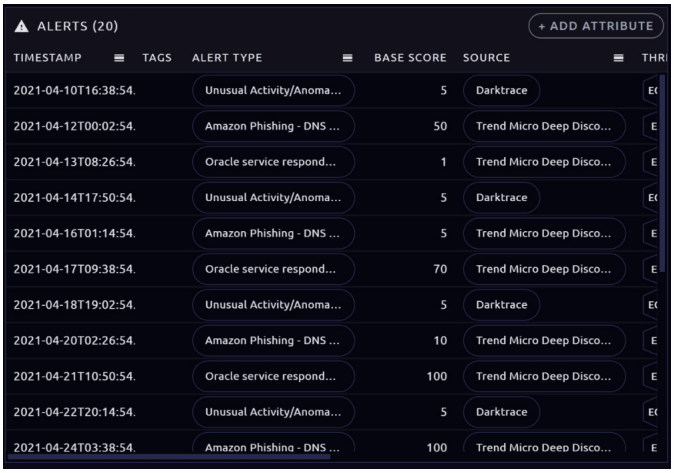
SOC.OS Release Notes

NEW DATA GRID FUNCTIONALITY, CLUSTER OVERVIEW PANEL, IMPROVED “SUGGESTED SEARCH” TERMS AND NEW INTEGRATION.

SEPTEMBER 2021

Data Grid

We've introduced the new Search functionality to the cluster page, allowing the visualisation and data view to be filtered using search queries. This means only the data the user is interested in will load, therefore reducing loading times.



Cluster Overview Panel

The new cluster overview panel surfaces the most prevalent alert types, and internal/ external entities in the cluster. The alert types and entities are ordered by the number of alerts they are associated with.

The overview of alert types shows the number of effected internal entities and the number of alerts associated with that alert type.

The overview of the internal/external entities in the cluster displays the number of alerts associated with each entity as well as the first and last seen date times.

Suggested Search

Updates to the API means that we've been able to improve suggested terms when performing searches on "Alert Type".

Integrations

We've improved the Actioned status of MS Azure Security Centre alert category "Antimalware action taken".

Wiki

- Tutorial page for the new Cluster Data View functionality
- Search help page updated with Basic Search explaining the SOC.OS chip search feature
- New ManageEngine integration page
- Further updates and improvements to MS Graph, Trend Micro Apex Central and Fortinet FortiAnalyzer integration pages

How can I help?

As ever, we're excited to continue to develop SOC.OS to meet your needs, and always welcome your input. Please continue to call us or email support@socos.io about defects and improvement suggestions, no matter how small or seemingly left field!

100 Avebury Boulevard,
Milton Keynes,
United Kingdom
info@socos.io
www.socos.io
@socos_cyber
@socoscyber