SOC:OS

SOC.OS Release Notes

VISUALISATION PERFORMANCE IMPROVEMENTS, AGENT STATUS INDICATOR AND SOC.OS WIKI

JUNE 2021

Visualisation performance improvements

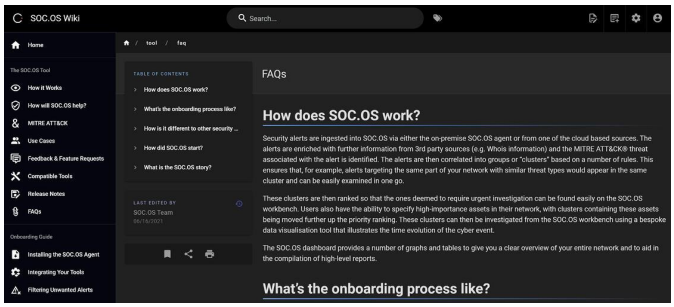
No more long waits for loading those clusters with hundreds or thousands of entities. New cluster visualisation driven from ElasticSearch gives a smoother and faster experience.

Agent status indicator

Status indicator now works with the latest version of the SOC.OS agent, giving you visibility in the SOC.OS UI when the agent is online or offline.

SOC.OS Wiki and help pages

Our help and documentation resource is rapidly taking shape, and has been deployed in beta. Keep an eye out for a full launch coming very soon.



What's new? (Non-UI)

- AlienVault OTX enrichment are now more reliable, with better identification of URLs to be submitted for look up
- Performance and usage monitoring implemented to drive UI improvements in future development
- Improved monitoring to enable alerting for agent downtime to SOC.OS team and allow future proactive alerting to users
- Enable multiple instances of the same source, eg monitor multiple AWS GuardDuty accounts within a single SOC.OS instance

Bug Fixes

- Fixed a number of bugs and inconsistencies introduced in the recent UI upgrade to introduce search
- Issue with Wallboard Users being forced to use MFA resolved

Source Systems

- New integrations of source systems:
- Microsoft O365 Defender
- Microsoft Azure Advanced Threat Protection
- Cisco Meraki
- Improved existing integrations:
- Trend Micro Deep Discovery threat mappings improved
- Entity identification for all Microsoft tools improved
- Entity identification for FortiAnalyzer improved

How can I get involved?

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