SOC Survey Results

- A survey was distributed to all **SOC analysts**.
- We got nearly **60 responses** – which is great!
- We grouped the results for **“Worst Part of the Console”**and put on Post-It notes for analysis.

Worst part of console

Led by the UX designer, dev, analysts and others help affinitize (organize info on the post-it notes in to categories) the **“Worst Part of the Console”** data to uncover themes.

Worst part of console Themes from Affinity

- Integrate the web app in console
- Speed up the search results
- Reduce need to manually tune
- Better system than CAG displays nows
- Integrate scripts in to console
- Shun does not always work
- Correlation is slow and confusing
- Manual parts of IR emails
- Console loads slowly
- No SSO authorization
- Inability to input special characters
- Too many popups
- Tool page is complicated and cluttered
- Prefer new tabs over windows
- A lot of clicks to do one process
- Poor descriptions and naming

Worst part of console Themes from Affinity

- Alert-centric rather than event-centric
- A lot of unused space
- Not all info displayed is useful
- Inconsistent
- Want cross sensor alerts
- Need faster FSM Grepper
- Attach tickets over time
- Attach more info to tickets than alerts
- Info is strangely distributed, i.e notes
- None of the info is cross referenced
- Disorganized
- Prefer a dark UI
- Not enough automation
- Show IPs in last 10 tickets
- Tickets slow to load
- Ability to create multiple tickets

From these high level themes, we can develop a **“To Do” list** of features and items we would like correct and redesign in the new console.

This is a great **starting point to improve** the interface using our users’ feedback.

Worst part of console Highest frequency in Survey

- Slowness
- Bright colors/interface
- Old/dated design
- Cannot create multiple tickets for one client

Worst part of console

	Recommendations
Slowness	Reduce the slow load time of console, tickets and more by increasing performance, eliminating elements not needed on the interface and implementing scripts in to console.
Bright colors/interface	Updating design to implement a dark theme/design. Make sure that dark interface is consistent throughout.
Old/dated design	Through research, prototyping and performing usability tests, we will create a new design that the analysts will enjoy using.
Multiple tickets for one client	Permit the ability for more than one ticket to be written at once for a client. Do not repaint the screen when analyst wants to create another ticket.

Worst part of console Medium frequency

- Opens windows instead of tabs
- Not single sign on
- Slow correlation
- Not enough automation

Worst part of console Small frequency

- Would like more context/history on alerts
- Inability/inconsistency on handling of special characters
- Too many pages/tools. Finding things can be hard.
- Things lack descriptions. Tool tips would help.

Best part of console

Highest frequency

- Grease Monkey scripts
- Auto associating tickets
- Alert research
- It gets things done

Best part of console

Medium frequency

- Adding notes at different levels (IP, alert, sensor)
- CAG screen
- User friendly
- WERT
- Event notifier

Best part of console

Small frequency

- Templates for emails
- Simplicity – all in one place
- Easy to scroll though
- Easy to learn

If you could change one thing...

- Speed
- Script integration
- Email
- Alert and CAG screen

What can you not live without?

Highest frequency

- Grease Monkey Scripts
- WERT
- Notes

Medium frequency

- Data Session rebuild
- Webapp

Additional comments

Every step of the ticketing and research **process** uses **analyst's time** very **inefficiently**. It's **too hands on** for any analyst to be able to **perform multiple tasks** in addition to monitoring/ticketing well.

Eliminate the **slow access/loading** of console because it really **affects monitoring** greatly.

Thank you for the initiative about this matter to **help us further** in our daily task.