SECONDARY RESEARCH

OpenSOAR: Security Orchestration and Automation Response platform

SECURITY OPERATIONS CENTER (SOC):

How this tool is of benefit to each of them? What do they need out of the dashboards?

Engineers:

• They need to build out orchestration and automation applications with workflows that integrated with their existing systems. Applications are user-designed templates for collecting, storing, and organizing the data.
• They should be able to create applications with a simple drag-and-drop interface where you can quickly automate tasks and create workflows to match your current incident response processes. There can be pre-configured sections/fields/workflows that facilitate the creation of new applications.
• There should be a completely customizable design that allows the engineers to create a fully or partially automated workflows.

Analyst:

• Aim is for a tool that gives them a comprehensive and interactive overview of their workload, priorities, team performance, and more.
• From the Dashboard visualizations, the analyst should be able to go straight to the corresponding data record and begin working from the record/incident view.
• Data displayed should be customizable using numerous reporting options and many different types of graphs charts and other visualizations.

Manager or Director:

• Reporting capabilities that enable the manager to effectively understand and communicate the true value of security operations to business leaders.
• Should be customizable to provide the optimal view providing a visual representation of key assets, teams, and activities
• Dashboards cards should be configured to enable the managers to rapidly visualize information such as workload by analyst and tier, the number and type of open tickets, Mean time to respond for specific threats, manual incident time per analyst, etc.
• Visualization provides managers the instant data they need to predict and recommend the changes necessary to continue mitigating next and existing risks
• They need to identify: Need for new or improved tools, where/if additional staff is needed, where/if training would be beneficial
• Generate any type of reports they need to generate for audits, compliance or presentation to upper management

Executive:

• The dashboards can be used by CISO/CSOs to provide an overall view of their security landscape and enable quick and efficient reporting to the board.
• They need an overview of the key performance indicators on their dashboard - how their teams are performing and look at the efficiency and effectiveness of the tools being used in the SOC.
• A few important views for the C-level: the automated vs. manual task, the level and types of incidence being handled most often, or the performance improvements in the meantime to respond.
• ROI calculators that allow the CISO to track their investments into the SOC and see the actual time and money saved.
• Measure performance and address weak points - make the operations profitable, efficient, and competitive.[1]

[1] https://swimlane.com/ and disucssions with Lead Security Engineer

OpenSOAR: Security Orchestration and Automation Response platform

EXISTING PRODUCTS AND THEIR SPECIFICS

DEMISTO: (Now Cortex SOAR, A Palo Alto Networks Company)

Demisto tool helps Security Operations Centers (SOCs) scale the capabilities of their human resources, improve incident response times, and capture evidence while working to solve problems collaboratively. The Demisto platform enables collaboration among analysts and intelligent automation using bots.[1]

Pro - Allows security engineers and security analysts to create custom widgets (a component of an interface on the dashboard, that enables them to perform a function or access a service)
Con - Does not allow the user to customize (say graphs) without coding. Some parameters on the reporting graphical interfaces have similar color that may need some customization for easier analysis.

- The UI is not very intuitive: There are no easy ways to jump to a particular topic on the incident report
- The reports generated based on different scenarios can be graphically more concise and informative [2]

About one year ago Demisto launched a mobile application for its SOAR Platform.

SWIMLANE

Swimlane helps organisations manage the growing number of alerts and notifications in their security systems. With Swimlane, business leaders can automate crucial and time-consuming incident response processes. The solution collects security data from almost all security platforms with minimal effort. Thus, it can automatically respond to alerts using playbooks and pre-set workflows.[3]

Swimlane does not have a mobile app yet.

PHANTOM by Splunk

The primary component of the Splunk SOAR system is the Visual Playbook Editor. The VPE allows developers and business teams to construct sophisticated yet simple Phantom Playbooks with drag-and-drop functionality. Even people without coding knowledge can build playbooks graphically while the VPE generates code behind the scenes in real-time. Splunk also offers canvas and function blocks so you can design specific automation processes for individual workflows. [3]

[1] https://www.networkworld.com/article/3088332/demisto-accelerates-security-investigations-through-automation-and-collaboration.html
[2] Discussion with the Lead Security Engineer
[3] https://www.em360tech.com/continuity/tech-features-featuredtech-news/top-10-soar-platforms/

OpenSOAR: Security Orchestration and Automation Response platform

ABOUT SOAR AND BEST PRACTICES:

Security orchestration, automation, and response (SOAR) solutions are valuable for everyone on a security team, from people on the front lines to managers and executives tracking reports and metrics from a birds-eye view, or even compliance and legal personnel working outside the security operations center (SOC).

Smarter:
With a SOAR platform in place, the users' skills and experience can be augmented by integrations with hundreds of threat intelligence feeds that provide valuable contextual information. The users (from engineers to executives) can use tools like link analysis to see visual representations of the connections between entities and incidents. Having the full story of each alert will make them even smarter when making decisions, which will result in less dangerous incidents slipping through unnoticed or without being remediated appropriately.

Faster:
By the time the engineer/analyst opens an incident report, it should already be enriched with the previously mentioned contextual data and threat intelligence. This enables them to assess every alert much faster by skipping the arduous manual steps of gathering data.

Wiser:
The users should have access to historical data from every previous incident to see how comparable cases have been handled in the past.

Customizable:
Enabling security analysts to visualize incident and indicator flows in a completely tailored manner, making it easier than ever to manage and automate incident response.[1]

[1] https://d3security.com/blog/how-soar-makes-a-security-analyst-more-impactful/