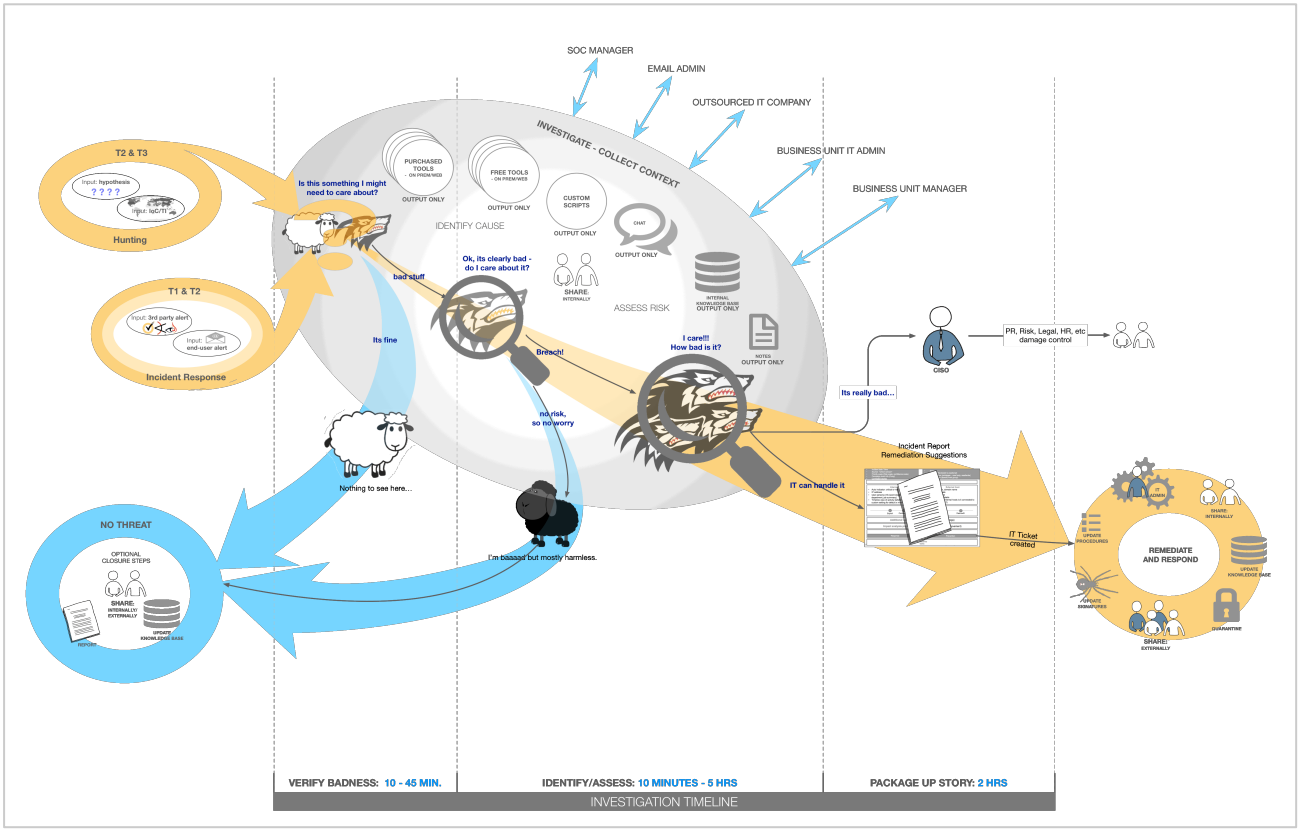
BRASSHILL
RESEARCH & DESIGN

WHITE PAPER

Turbocharge your Analysts

Process/Workflow Optimization



Change is the one constant in any operations center, whether it is security operations, Incident Response, or any other IT focused team. Workload, staffing and budget changes are just a few of the changes that business units cope with regularly. With change, comes the need to modify business and operational processes, preferably in a way that allows for long term planning.

One solution to quickly incorporate change is to hire more staff or buy more tools. A more long term but ultimately more effective solution is to make changes to the underlying processes that support the business and operational goals of the team. This type of change in itself can be quite a process, taking time away from other more urgent tasks.

We can help. By understanding your current practices and processes at the goal and task level we can build a picture of where are your current bottlenecks, inefficiencies, and pain points. This research is then used collaboratively with your team to design new processes and workflows that meet your changing needs and help your analysts by making them more efficient and engaged.

A more hostile threat environment brings challenges

In many security operations and incident response centers we see ongoing efforts to improve both the team's business processes and the actual analyst workflows/tasks to manage ever-changing workload and staff levels. Some of the common stumbling blocks are:

- Large numbers of un integrated information-gathering tools being used, which can lead to inefficient and error prone processes
- Variations in work processes and applications used among analysts
- The need for tailoring tasks to different levels of expertise vs. keeping staff engaged and able to advance in their proficiencies

Without doing a detailed analysis of what is currently happening and what the end goals are, creating new processes and making organizational changes to address inefficiencies cannot be validated or measured for their success.

How we can help

At a high level, our solution is to support your process improvement/change efforts by helping you evaluate your current practices against desired results, then generate suggestions of how to achieve those results through identifying roadblocks, pain points, and gaps in the current practices. With detailed insights into the problems you are trying to address you will have an improved ability to evaluate planned changes.

Outlined below are some of the issues teams may face, and how we can help solve these issues.

Issue: Lack of detailed description of current processes and desired changes, or lack of time to research and generate these descriptions.

Solution: Without a detailed starting point, identifying the best areas for change can be challenging. We can conduct stakeholder interview summaries based on semi-directed interviews with management and senior analysts and then summarize this information to give you that starting point.

These interviews are extremely useful to help detail and refine out both the end goals for a group, as well as aligning all the stakeholders to an agreed-upon direction. To execute, we start with a list of questions for our interviews, talk to each stakeholder and suggested expert, and then do a synthesis of the results to present to the stakeholder group as a whole.

Issue: Finding the time to articulate a detailed and clear understanding of the tasks, roles, and goals of the team to inform and validate changes.

In general, the tasks and goals of a team are known at a high level for tracking and assignment purposes. Understanding in detail what goes into each task to achieve each goal, and how these tasks can vary from analyst to analyst is important to know when instituting change, but it can be time consuming to extract this information.

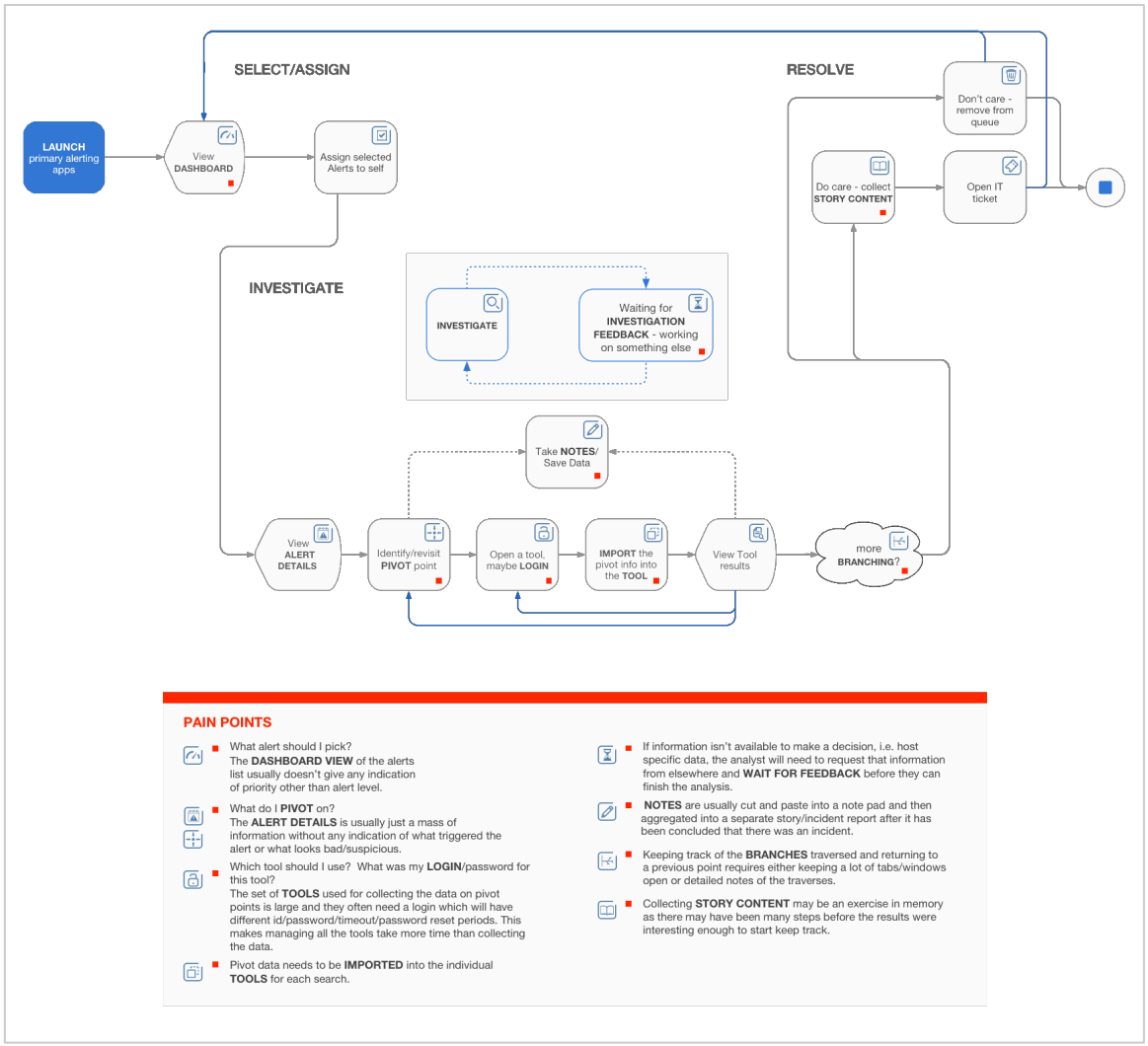
Solution: An audit of all the current processes and practices can give you that clear understanding and confidence that the changes you make will affect your team positively.

Auditing current processes can take advantage of a number of different techniques used in user research, such as contextual interviews (interviewer watches and listens as analyst performs tasks), semi-directed interviews (interviewer has a list of questions but allows 'floating' from that list), and group sessions to identify tasks, roles, goals, and other tribal knowledge. A number of deliverables are produced from this stage that play a key role in later stages.

Issue: Making sure the team has a voice in the changes being made in a constructive and collaborative manner.

Solution: Collaborating with your team to analyze the current workflow along with the desired processes to identify areas of improvement is a good way to make sure all stakeholders have a voice in what ends up being the 'fixit' list. With this participation, the changes should be more appropriate and the acceptance of those changes will be much higher.

Example of 'High-Level Alert to Resolution' Workflow (before fixing)



Issue: Planning changes so that they can be staged and will be accepted when they are rolled out.

Solution: Team collaboration to develop improved workflows along with the roadmaps to push those changes allow all affected stakeholders a voice in the process and can bring both insight and innovation to the exercise.

This step is a combination of identifying new workflows, what are the 'best of' tools and techniques available, how to apply them to the 'fixit' list, and how to address what is missing, whether it is creating a tool; buying a tool; changing a process; or using a new technique. Again, when done as a collaborative exercise, using all the previously collected information, it stands a much better chance of succeeding. A roadmap laying out how and when the changes can be incorporated, as well as how to measure the success of the changes is also developed.

Next Steps

The solution outlined above will provide valuable research that you and your team will be able to use as a touchstone going forward. What it doesn't address is what to do next if you have concluded that some new tools need to be created or integrated. We can help. For information on how we can help with this step, see the details of our Tool Design Strategy service (brasshill.com)