Paper SAS524-2017

Adding a Workflow to Your Analytics with SAS® Visual Investigator

Gordon Robinson and Ryan Schmiedl, SAS Institute Inc.

ABSTRACT

Monitoring server events to proactively identify future outages. Looking at financial transactions to check for money laundering. Analyzing insurance claims to detect fraud. These are all examples of the many applications that can use the power of SAS® Analytics to identify threats to a business. Using SAS® Visual Investigator, users can now add a workflow to control how these threats are managed. Using the administrative tools provided, users can visually design the workflow that the threat would be routed through. In this way, the administrator can control the tasks within the workflow, as well as which users or groups those tasks are assigned to. This paper walks through an example of using the administrative tools of SAS Visual Investigator to create a ticketing system in response to threats to a business. It shows how SAS Visual Investigator can easily be adapted to meet the changing nature of the threats the business faces.

INTRODUCTION

Analytics is only as good as the decisions that it enables. The key to making the right decisions is ensuring that the right information is given to the right people at the right times.

Environments in which analytics are used can often be highly regulated. This can result in the necessity to be able to document and record the processes that were followed in handling data and the decisions made from the output of the analytics performed.

This paper will use an Insider Threat solution as the focus of how workflow can be applied and used to help direct the decisions that are made in relation to the outputs of analytics.

The paper will use the business problem of Insider Threat as an example of a solution that can use SAS Visual Investigator, which will be able to use the workflow functionality to enhance the offering. It will look first at what an insider threat is and how threats are identified. It will then discuss the workflow capabilities of SAS Visual Investigator and talk about how this can be applied to the insider threat business problem.

WHAT IS INSIDER THREAT?

The last 10 years have seen an emergence of cyber-attacks and security measures being put in place by both organizations and individuals to try to prevent insider threats. This ranges from businesses putting in firewalls and implementing two-factor authentication right down to individuals installing anti-virus software to protect their PCs at home.

It is predicted that cybercrime will cost the world $6 trillion a year[1] annually by the year 2021. In addition, it is predicted that over $1 trillion will be spent globally on cybersecurity over the next four years.

The statistic that might surprise a lot of people in relation to cybercrime is that 60%[2] of all cybercrime is perpetrated by individuals who are known to the organizations involved. A lot of people associate cybercrime with the high profile hacking cases that have taken place in recent times.

[1] http://cybersecurityventures.com/cybersecurity-market-report/

[2] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF

Some really high profile instances of insider threats that most people will remember include the following:

- Edward Snowden, the founder of WikiLeaks, is quite possibly the best known case. He was a former CIA employee and a former US government contractor who stole and leaked classified information from the National Security Agency (NSA).
- The Panama papers are another more recent example. The employee who leaked this information has never been publicly identified[3]. He cited income inequality as his reason for leaking the papers.

Not all insider threat cases are malicious. Approximately one third of the incidents of insider threat were carried out by inadvertent actors. These are individuals who unwittingly allow access to corporate data and networks by providing access to third parties or by not following security procedures.

The other side of this is the malicious insiders. This could be employees, contractors, or anyone with access to internal data and systems. These individuals purposely set out to steal data or to cause harm to the associated organization.

"In 2017, the insider threat epidemic begins"[4] - James Scott

A recent Institute for Critical Infrastructure Technology (ICIT) study highlighted that the threat faced by organizations from insiders was likely to grow over the coming years. For example, terrorist organizations are expected to try to radicalize airport employees as a means to enabling terrorism.

As these threats grow, organizations will be forced to invest more in trying to identify threats as quickly and efficiently as possible.

USING ANALYTICS TO DETECT THREATS

SAS Analytics for insider threat deterrence is based on the following four distinct analytic domains that look at data from different perspectives:

- Rules test all behaviors and activities against a predefined set of algorithms or business rules that can detect known types of risk behaviors based on specific patterns of activity or defined actions.
- Anomaly detection, such as clustering techniques, determines baseline behaviors for both individuals and groups and patterns of activity to define what's normal for each, measuring variations from the norm.
- Predictive modeling and data mining uses historical data or large amounts of transactions to predict future behavior and potential risks, as well as to detect new or emerging threat behaviors.
- Network or link analysis goes beyond data visualization to calculate the statistical significance between connections or transactions in the data and determines inferred relationships.

The combination of powerful data aggregation, a hybrid analytical approach, and a powerful technology platform enables organizations to assume a more proactive and contextually aware security posture. This approach is critical to circumventing a potential terrorist plot, thwarting an espionage mission, reducing fraud transactions, and addressing other complex threats.

All of the approaches above can be used to trigger alerts whenever a threat is detected. These alerts can be fed into SAS Visual Investigator to allow an analyst to triage them. In triaging the alert, the analyst will be able to make a decision as to whether the alert merits further investigation. If further investigation is required, then the analyst can instantiate the creation of a case.

---

[3] https://en.wikipedia.org/wiki/Panama_Papers

[4] http://icitech.org/icit-brief-in-2017-the-insider-threat-epidemic-begins/

WORKFLOW WITHIN SAS VISUAL INVESTIGATOR

SAS Visual Investigator introduces the ability to add workflow to the cases that are modeled within a solution.

The workflow functionality is based on the industry standard Business Process Model and Notation (BPMN). Whilst not yet supporting all of the BPMN tasks, events, and gateways, it provides enough capabilities to enable the modeling of almost all of the workflows that will be required for solutions on top of SAS Visual Investigator.

BPMN COMPONENTS

SAS Visual Investigator supports the following BPMN tasks, events, and gateways:

- Start Event
- User Task
- REST Service Task (custom to SAS Visual Investigator)
- Script Task
- Exclusive Gateway
- End Event

Start Event

Each workflow within SAS Visual Investigator will have one start event (see Figure 1). In the process of starting the workflow it is possible to pull values from the associated case and store these values within process variables. For example, if the case has the value “High” in a risk column, then this can be passed in to the workflow and stored within a process variable. Process variables are used within conditions that control the direction the workflow takes and the tasks that result from this.

Figure 1. A Start Event

User Task

A user task (see Figure 2) within a workflow is something that is assigned to either a group or a user within SAS Visual Investigator. If the task is assigned to a group, then members of that group will be able to claim it. Claiming tasks prevents multiple members of the group from working on the same task at the same time.

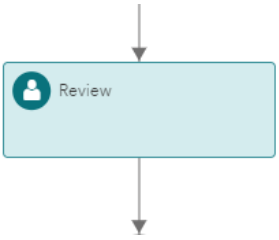


Figure 2. A User Task

When adding a user task to a workflow, the designer will be able to set the options that will be presented to the user performing the task to mark it as completed. For example, if the task is a review task then the user might be presented with the following options:

- Accept
- Reject

Associated within each of the options will be some configuration that will set both process variables and values within the associated case. Using the example above, if the user selects the Accept option then this might result in a column within the case being set to "Accepted". In addition, it might result in a process variable being set to Accepted. This variable might be used within a subsequent exclusive gateway to control the direction of the workflow.

Rest Service Task

REST service tasks (see Figure 3) can be used to allow the workflow to interact with external systems. This allows process variables to be sent to the service being called through either the query string or the body of the message. The use of the REST service task is a powerful feature to allow for SAS Visual Investigator to be integrated into an organization's enterprise.

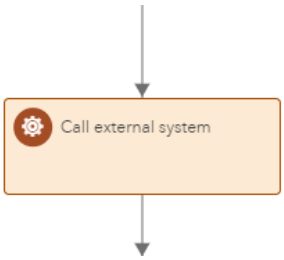


Figure 3. A REST Service Task

Script Task

Script tasks (see Figure 4) allow the workflow designer to incorporate some custom JavaScript code. The normal use of this would be to manipulate and set process variables that are used to control the flow of the process.

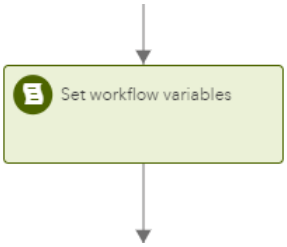


Figure 4. A Script Task

Exclusive Gateway

Exclusive gateways (see Figure 5) can be thought of as “if” conditions within a workflow. They allow conditions to be created that will be used to determine the direction the workflow takes. Only one arrow out of an exclusive gateway will be followed.

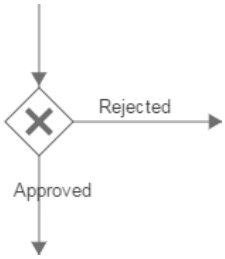


Figure 5. An Exclusive Gateway

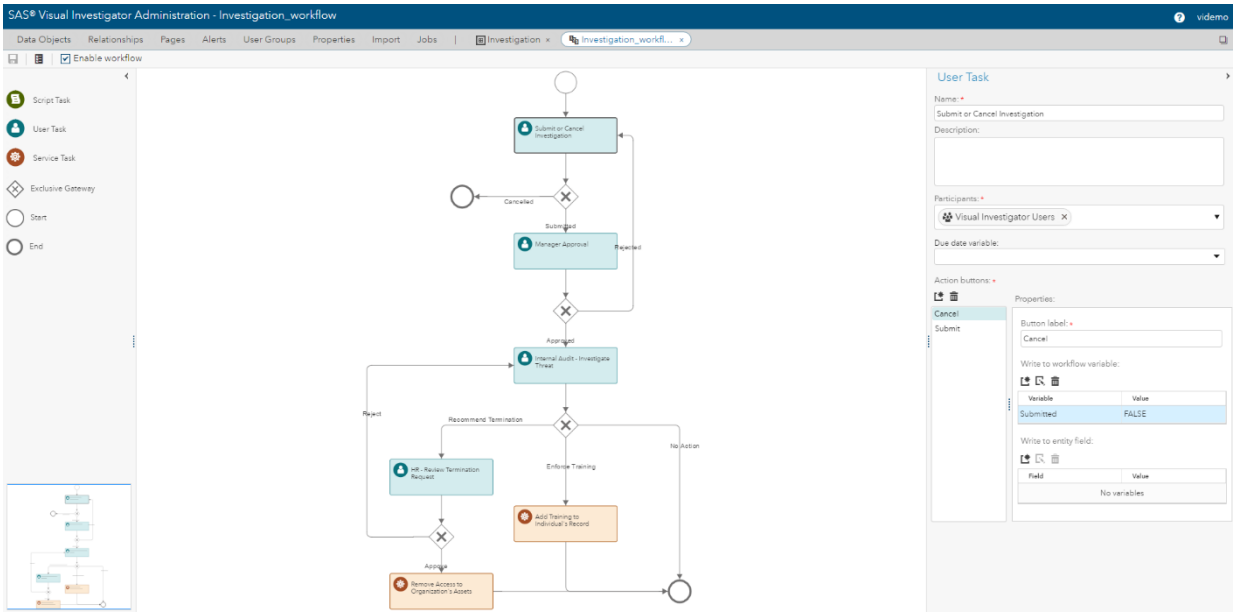
End Event

A workflow can have multiple end events. These end events (see Figure 6) denote that the workflow has reached a point at which it can be thought of as complete.

Figure 6. An End Event

ADMINISTRATION

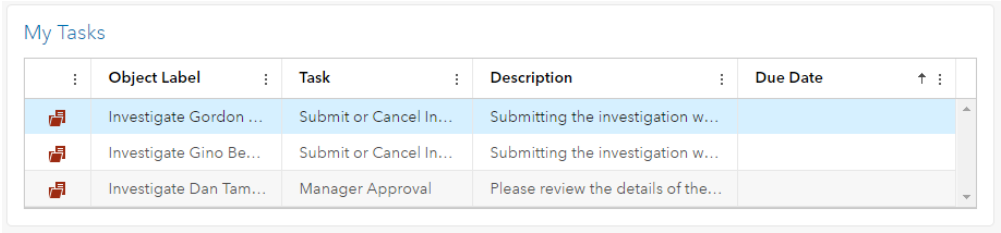
The Administration section of SAS Visual Investigator now provides access to a workflow designer (see Display 1Display 1. Workflow Designer within SAS Visual Investigator). This access has been integrated into the product to allow for tight integration between the workflow and the underlying data. Values need to be pulled from the entities into process variables within the workflow. The flip side is that the workflow needs to be able to write back to the associated entity to allow for states to be set.



Display 1. Workflow Designer within SAS Visual Investigator

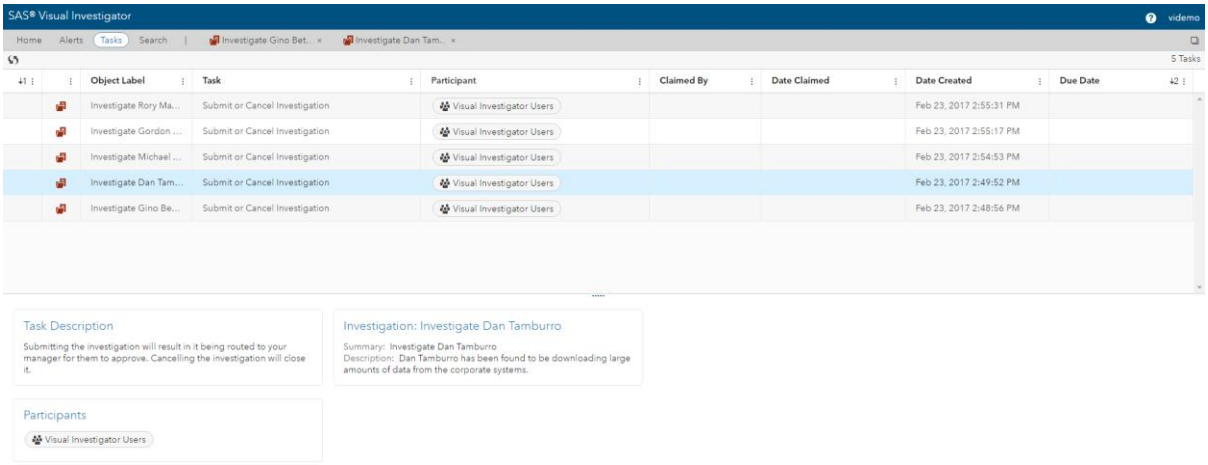
ACCESSING WORKFLOW TASKS

There are two ways that a user of SAS Visual Investigator can access their tasks. The first way is through the homepage. A new homepage control has been added that allows users to quickly access the tasks that they have claimed (see Display 2).Display 2. My Tasks Section on Homepage



Display 2. My Tasks Section on Homepage

The second way that users can see the tasks is through the new Tasks tab. The tasks tab allows a user to see all of the tasks that are assigned directly to them, or to a group to which they belong (see Display 3).

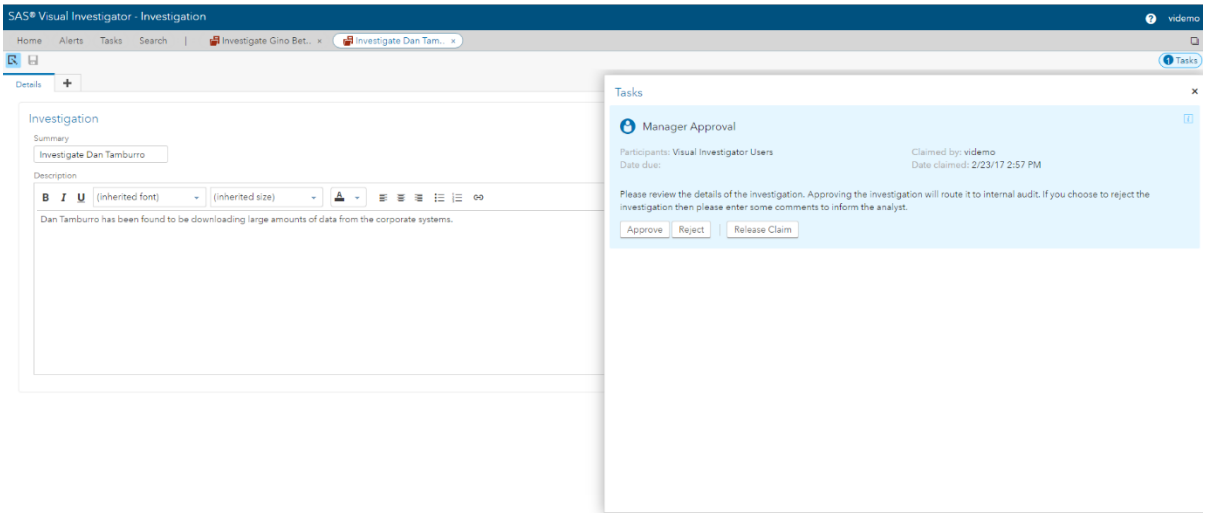


Display 3. Task Listing within SAS Visual Investigator

Selecting a task within the grid allows the user to see some details about it in the pane below. This includes a description of the task to be performed along with some details of the associated object.

COMPLETING WORKFLOW TASKS

Opening an object that has an associated workflow task will now result in a new toolbar button appearing. This button shows the count of tasks that are currently outstanding on the object. If the user clicks on the button, then a pane will slide in showing details of the tasks (see Display 4).



Display 4. Tasks Pane When Viewing an Object

From within this task pane, the user will be able to claim the tasks. Once the tasks have been claimed, the options for completing the task will be available.

APPLYING WORKFLOW TO AN INSIDER THREAT SOLUTION

Now that we have an understanding of the workflow capabilities of SAS Visual Investigator, we can start to look at how this could be applied to the Insider Threat solution.

As mentioned earlier, SAS uses a hybrid analytical approach to generate alerts on employees and contractors within an organization. These alerts are routed to analysts to triage and potentially investigate further.

If an analyst decides that an alert is worth further investigation, then they will create an investigation object. The creation of the investigation will result in a workflow being instantiated (see Figure 7).

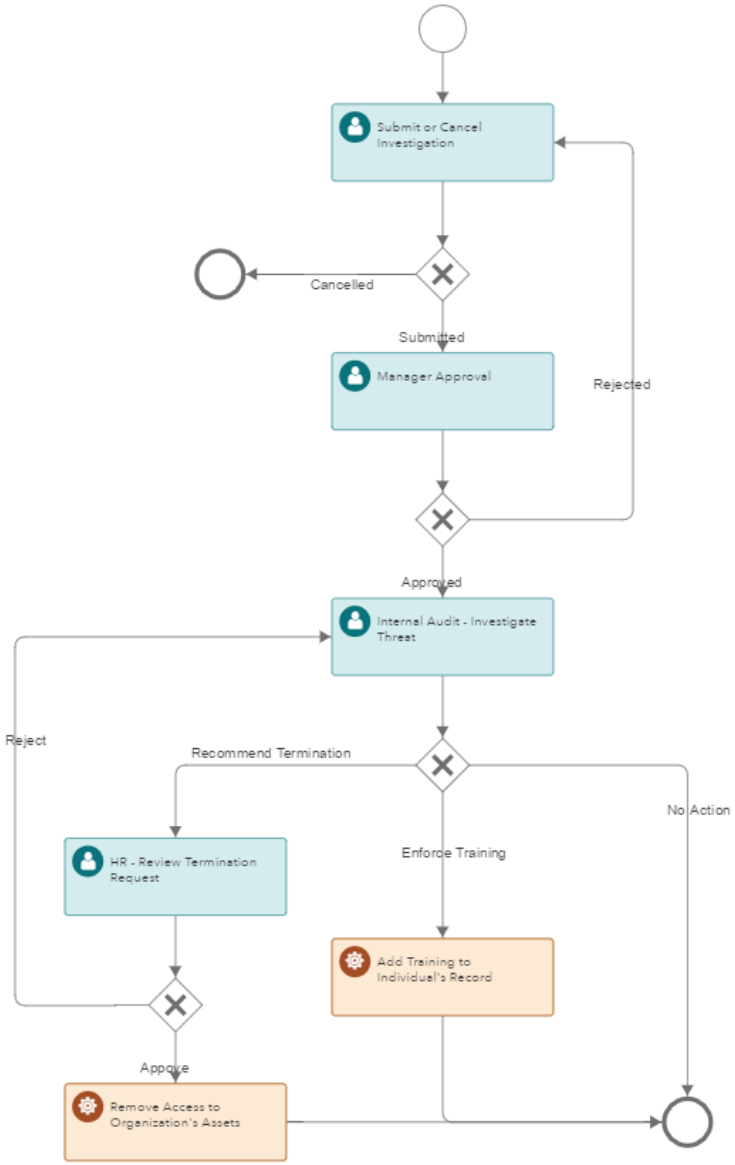


Figure 7. Insider Threat Workflow

The investigation object allows an analyst to document their findings into the possible threat. The analyst can use the insight capabilities of SAS Visual Investigator to do so. This allows them to snapshot any visualizations that they have generated, insert any images they might have found and to add supporting text.

Once the analyst has completed the documentation of their findings, they will be able to submit the investigation to their manager for review. The manager would have the option of approving or rejecting the investigation.

If the manager rejects the investigation, then they will fill in details of why they have done so and send it back to the analyst. The analyst then has the option of entering more information into the investigation and resubmitting it, or to cancel it. Canceling the investigation would result in the workflow being completed and therefore no further tasks being required. Submitting it again with more information would result in the manager reviewing it again.

If the manager approves the investigation, then it is routed to the Internal Audit team. The Internal Audit team is responsible for performing deeper investigations into the actions of individuals within the organization. This team will look at the information provided to them by the analyst and make a decision on how to move forward.

There are a number of options open to this team in relation to the investigation are the following:

- Recommend Termination – In this case the investigation is routed to the HR team. Once the HR team confirm the termination, a service task is used to automate the removal of access to the organization's resources.
- Require Training – If the case is found to not be malicious then the auditor might enforce that the individual involved takes a training course to make them aware of corporate security policies. This would use the service task capabilities to automatically add the details of the training to the individual's records.
- No Action – The auditors might find, after further investigation, that there was justification for the actions of the individual and that no further action is required.

CONCLUSION

The workflow functionality within SAS Visual Investigator supplements its alert triage capabilities by allowing resulting cases to be created and managed. Having both of these functions handled within a single application reduces the cost and support burden that comes with running multiple applications.

As we have seen from the example of the Insider Threat solution, the workflow capabilities of SAS Visual Investigator allow it to manage the tasks associated with cases along with allowing it to integrate with other systems by making external REST calls.

SAS plans to build on the workflow capabilities of SAS Visual Investigator in the future by extending the support for BPMN tasks, events, and gateways.

REFERENCES

SAS. 2017. "Using Analytics to Proactively Deter Insider Threats." Accessed February 14, 2017. https://www.sas.com/en_us/whitepapers/using-analytics-to-deter-insider-threats-107092.html.

CyberSecurity Ventures. 2017. "Cybersecurity Market Report." Accessed February 14, 2017. http://cybersecurityventures.com/cybersecurity-market-report/.

IBM. 2016. "Reviewing a year of serious data breaches, major attacks and new vulnerabilities." Accessed February 14, 2017. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF.

Wikipedia. 2017. "Panama Papers." Accessed February 14, 2017. https://en.wikipedia.org/wiki/Panama_Papers.

ICIT. 2017. "ICIT Brief: In 2017, The Insider Threat Epidemic Begins." Accessed February 14 2017. http://icitech.org/icit-brief-in-2017-the-insider-threat-epidemic-begins/.

RECOMMENDED READING

- *SAS® Visual Investigator 10.2: Administrator's Guide*
- *SAS® Visual Investigator 10.2: User's Guide*

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Gordon Robinson
SAS Institute Inc.
+1 984 789 7548
gordon.robinson@sas.com