Phase II Final Summary Report: WhyViz: Transforming Cyber Data into Human-Centered Visualizations

Proposal Number: F2-8842

Topic Number: AF SBIR Solicitation 15.1 (AF151-015)

Contract Number: FA8650-16-C-6711

Summation

The goal of WhyViz was to conduct a formal evaluation of the effects of various visualizations on the performance of cyber analysts analyzing data in the early stages of cyber incident handling, i.e., detecting malicious activity, and conducting preliminary analysis and identification of an event. These analysis tasks are accomplished in real-time, under high volume data intensity, where decisions must be made in seconds in order to avoid alert queue overflow which could result in malicious activity going unresolved.

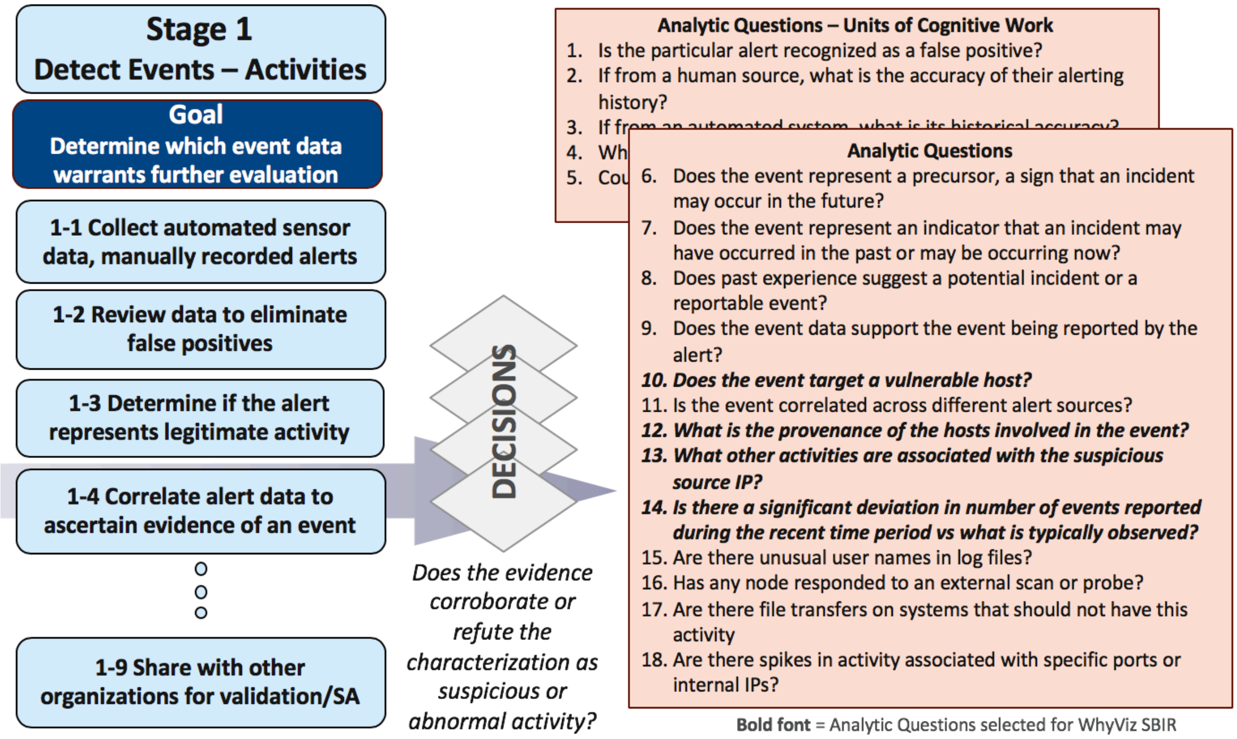
In Phase II of the WhyViz project, we applied the results of knowledge elicitation activities conducted during Phase I and used cognitive design processes to iterate the design of different visualizations that addressed the scope of analytic requirements within WhyViz. To answer our research questions, we designed two online experiments to better facilitate participation by actual cyber defenders. One experiment focused on detecting malicious activity; the second on the potential technical impact of a categorized event.

WhyViz executed a complete product development process to produce different visualizations (Dashboard, Integrated and Alpha-numeric representations) that addressed the cognitive requirements of the selected analytic tasks. Using the Visual Analytics Science and Technology Challenge (VAST) 2011 MC-2 data set, we began by isolating segments that presented activity for visualization, and established ground truth for the resultant security visualizations. WhyViz identified and implemented methods to transform low-level cyber data into meaningful visualization attributes, and demonstrated methods for security data cataloging as a prerequisite to data transformation and visual encoding. We enhanced the VAST 2011 data set to (a) include NetFlow emulation, derived from PCAP data, and (b) extend the applicability of VAST 2011 to real-time analysis context by addressing inconsistencies in time formatting. Using human-centered design principles, we iterated and reviewed different visualization prototypes for each experiment. We then verified designs using diverse data samples before instantiating those designs using the Data-Driven Documents (D3) JavaScript library.

We also refined the experiment design and developed a web application to execute the experiment and collect metrics needed to evaluate the effect of different cyber visualizations on cyber defender performance (speed, accuracy). Standard instruments (Modified Cooper-Harper, System Usability Scale) were incorporated to collect subjective measures of workload and usability. The visualization prototype and experiment execution software were instantiated in a Microsoft Azure cloud instance. We validated the statistical analysis methods used to evaluate experimental data and conducted operational pilots to verify the experiment system. After remediating issues identified during the pilots, we recruited and selected participants, and conducted training and experiment sessions using our cloud-based system. Experiment participants were practitioners with recent, hands-on experience as cyber defenders, and college students studying cyber security who participate in cyber competitions.

DISTRIBUTION STATEMENT A. Approved for public release: 88ABW Cleared 10/04/19; 88ABW-2019-4344.

WhyViz produced a re-usable experiment management system for the evaluation of security visualization prototypes within a relevant operational context. The project also identified a set of minimally essential cyber information relevant to the early stages of the cyber incident handling, and investigated and demonstrated data aggregation techniques for managing visualization display space in cyber incident handling analysis.



Stage 1
Detect Events – Activities
Goal
Determine which event data warrants further evaluation
1-1 Collect automated sensor data, manually recorded alerts
1-2 Review data to eliminate false positives
1-3 Determine if the alert represents legitimate activity
1-4 Correlate alert data to ascertain evidence of an event
1-9 Share with other organizations for validation/SA
DECISIONS
Does the evidence corroborate or refute the characterization as suspicious or abnormal activity?

Analytic Questions – Units of Cognitive Work

1. Is the particular alert recognized as a false positive?
2. If from a human source, what is the accuracy of their alerting history?
3. If from an automated system, what is its historical accuracy?
4. Wh
5. Cou

Analytic Questions

6. Does the event represent a precursor, a sign that an incident may occur in the future?
7. Does the event represent an indicator that an incident may have occurred in the past or may be occurring now?
8. Does past experience suggest a potential incident or a reportable event?
9. Does the event data support the event being reported by the alert?
10. ***Does the event target a vulnerable host?***
11. Is the event correlated across different alert sources?
12. ***What is the provenance of the hosts involved in the event?***
13. ***What other activities are associated with the suspicious source IP?***
14. ***Is there a significant deviation in number of events reported during the recent time period vs what is typically observed?***
15. Are there unusual user names in log files?
16. Has any node responded to an external scan or probe?
17. Are there file transfers on systems that should not have this activity
18. Are there spikes in activity associated with specific ports or internal IPs?

Bold font = Analytic Questions selected for WhyViz SBIR

A summary view of of the WhyViz Goal-Directed Task Analysis for Stage 1 the DoD Cyber Incident Handling Life Cycle. The GDTA identifies 1) the goals a cyber defense decision maker must achieve in order to accomplish a mission; 2) the decisions that must be made in order to accomplish these goals; and 3) the specific information that is needed to support these decisions. This understanding of these cognitive requirements formed the basis of the visualizations and data transformations developed in Phase II, and the formal study to evaluate the impact of those visualizations on cyber analyst performance.

Anticipated Benefits

The WhyViz project has made several significant contributions to the continued development of security visualization capabilities. We identified inconsistencies in concepts and terms which inhibit more meaningful discourse within the security visualization community and between other domains interested in security visualization capability. We introduced the use of “visualization objectives” as a means to achieve more robust requirements definition for security visualization design. We investigated data aggregation techniques for managing visualization display space in cyber incident handling analysis. By continuing to share these and other project outcomes through conference presentations and peer-reviewed publications, we hope to continue to expand and refine both the knowledge and practice of cognitive engineering and user-centered design principles for cyber security visualizations.

WhyViz produced a re-usable experiment management system for the evaluation of security visualization prototypes within a relevant operational context. This “Off the Shelf” experiment delivery system can be used to support other user interface design evaluation and data visualization evaluation efforts, or for evaluation of visualizations within existing tools. At present, there is no standard evaluation framework for cyber security visualizations. The framework used in WhyViz to evaluate the visualizations is a potential evaluation framework for cyber defense visualizations. We will seek to make the WhyViz exemplar available to other researchers and developers.

WhyViz also identified a set of minimally essential cyber information relevant to the early stages of cyber incident handling and general cyber defense. This essential set of information and the related transformations have utility beyond cyber security visualizations. Security vendors have two related new offerings: a) security automation and orchestration, the latter term describing the coordination among / across automated and human activities; and b) cognitive security, which includes layering AI, such as natural language processing and machine learning, on top of security automation and orchestration. Organizations are beginning to invest in security automation and artificial intelligence (AI) technologies to close the gap caused by the workforce shortage and the increased threat landscape. Security automation and orchestration efforts are affecting not just the detection of events, but incident response activities as well. Insight from the cognitive engineering and visual design processes used in WhyViz are highly relevant for these security automation and orchestration offerings. WhyViz identified several of the repetitive data-processing tasks that can be automated, as well as several tasks that appear in different stages of the incident handling lifecycle, enriched through additional data fusion and correlation processes. Specifically, the minimally essential cyber information and the related transformations could provide a baseline of capabilities for these technologies.