Using the eR&D Approach to Pilot Deployment and Assessment in DHS

AJ Risko
Luanne Goldrich
Nykia Jackson
Johns Hopkins University
Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
aj.risko, luanne.goldrich, nykia.jackson
@jhuapl.edu

Robert Gatlin*
Brian Gattoni*
Department of Homeland Security
4601 Fairfax Drive
Arlington, VA 22203
robert.gatlin,
brian.gattoni@hq.dhs.gov

Richard Linger
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831
lingerr@ornl.gov

*The opinions expressed in this article are the author’s and do not necessarily represent the position of the United States, the Department of Homeland Security, or any other entity

ABSTRACT
This paper describes the success of the Hyperion Tool’s pilot deployment and assessment in a Department of Homeland Security’s (DHS) cyber center using the embedded research and development (eR&D) methodology/approach detailed in [1]. The eR&D methodology ensures the eR&D Team is tightly coupled with operational stakeholders to seamlessly and continuously identify operational requirements from stakeholders, discover R&D projects that may apply to the requirements, filter the R&D projects to select the applicable R&D technologies, then integrate the selected technology into the operational environment. This pilot deployment and assessment served as a “proof of concept” of the eR&D approach by demonstrating a stakeholder’s articulated requirements could be matched with newly developed technologies. Specifically, a DHS cyber center identified the need for a malware analysis tool that would automatically identify malware with little to no malware analyst interaction. The eR&D Team then took this requirement and discovered and filtered the Hyperion Tool as developed by Oak Ridge National Laboratory (ORNL) as a newly developed technology that could address this need and proposed a pilot deployment and assessment for integration into the DHS cyber center’s workspaces. The eR&D process helped to close an operational gap by connecting the research and operational communities.

1. INTRODUCTION
One of the primary objectives of DHS’s eR&D Team is to perform analyses of research (AoR) so as to identify, discover, filter, and integrate R&D investments into operational systems and programs. This is achieved through the identification and application of new, innovative technologies that improve mission capabilities of supported operators and analysts. As such, the eR&D Team does not actually carry out traditional R&D functions but rather focuses on seeking out and interfacing with federally funded R&D projects. Further, in that the eR&D Team serves as an enabler of operations, it has both a unique understanding of current stakeholder operations as well as a R&D perspective that helps with addressing current or future needs.

1.1 Technology Transition
The discussion of integrating R&D into operations must include an overview of work done in the technology transition space and the low probability of success due to the inherent problems encountered in this space. One of the primary functions of the eR&D Team, in addition to performing an AoR, is to help close the age-old gap between research and operationally fielded technology, metaphorically known as the Valley of Death (see Figure 1). Numerous studies [2] [5] have been performed and reports written on the difficulties and challenges of technology transition in government-funded R&D and approaches to overcoming those challenges.[3]
To maximize the potential for a proposed methodology to operate as intended and increase probability of the selected technology’s successful integration into the operational environment, the eR&D Team has developed a process to initiate and facilitate the relationship between the operations and research community. The tools employed for each cycle of the eR&D process help narrow the Valley of Death by moving either the start or finish lines of the technology transition process, helping to close the gap in the disconnect between the two communities.

1.2 eR&D Process
The eR&D Team constructed a comprehensive four-phase approach [1] (see Figure 2) to allow the researchers to elicit R&D requirements from the stakeholders seamlessly on a continuous basis; clarify challenges in the problem space; give the researchers immediate access to the tactical environment in which the analysts and operators work; and enhance the likelihood of a successful implementation and integration into the operational environment.

In the Identify cycle, the eR&D Team collaborates with operational areas within the organization to determine and elicit the operational, or stakeholder, R&D requirements. There are four phases in the eR&D Identify process: elicitation (through embedded participation), analyze requirements, stakeholder feedback and requirements validation. These phases are elements of a cyclical process. The eR&D Team meets annually with the operational teams to ensure a comprehensive set of R&D requirements is gathered; requirements submission by the operational teams is also encouraged throughout the year. As stakeholder feedback is adjudicated and these requirements are refined and validated through the Identify process, the requirements are fed into a repository (REQcollect, described in Section 1.3) where they can be stored, queried, categorized, prioritized, archived and maintained over time. As progress is made in the Identify cycle, it enables movement or activity in the other cycles.

In the Discover cycle, the team is outwardly facing and is tasked with discovering ongoing research projects that are being conducted across the cybersecurity spectrum including universities, consortiums and other research organizations of interest. There are three phases in the Discover process: exposure, investigation, and summary. The Discover cycle, like the Identify cycle, is ongoing -- it is accomplished once for each relevant project identified. There may be many projects in this process simultaneously.

The team discovers technologies by collaborating with other cybersecurity organizations, attending conferences, and researching potential projects. Once an accurate, concise summary of a project is written, an AoR document is initiated and the Discover cycle feeds the technologies into the repository. Note the Discover cycle is driven by a detailed knowledge of the R&D requirements elicited during the Identify cycle.

As the Identify and Discover cycles are executed, validated requirements and technologies are added into the repository; the built-in Google-like correlation algorithm in the Filter cycle automatically finds closely related or similar requirements with technologies that will potentially satisfy the requirements (eR&D Filter process phase 1 – automatic matching), in whole or in part. Once matches are provided, the Filter cycle continues; the eR&D Team uses its unique knowledge of the requirements and operational environments of the stakeholders to further examine the top matches from a perspective of what would likely satisfy the stakeholder’s operational requirements. If this process results in more than one viable technology, the eR&D Team consults with the stakeholder to determine which project is the best candidate to satisfy their requirements.

Once reasonable matches are suggested from the automated algorithm during the Filter cycle, the eR&D Team selects candidate technologies (matches) that are relevant for high-priority requirements (eR&D Filter process phase 2 – select matches) and subsequently promoted to the stakeholder. Note the output of the filter cycle may be an empty set. This would mean no technology/project was found for a given requirement, i.e., the automated matcher did not find any matches or the ones found were eliminated by the eR&D Team as irrelevant. In this case, impromptu discovery must be conducted if the requirement is of high priority or the stakeholder needs dictate that an R&D input is essential. This is discussed in the next cycle, Integrate.

Lastly, the Integrate cog turns as the eR&D Team facilitates the integration of filtered/matched technologies to the stakeholder; appropriate subject matter experts (SMEs) are involved with the research team. There are four phases in the Integrate process: investigate, initiate, increment, and integrate. The eR&D Team guides the technology and stakeholders through the integration, and ultimately relinquishes the technology to the stakeholder. As the Integrate cycle is executed, lessons learned and important process improvement information are fed back into the repository.
When a project has been selected to move forward, work on the AoR plan begins. The AoR plan is a high-level assessment of what it means to integrate a specific technology for a specific stakeholder. An AoR may contain a target recommendation, plan, status report(s) and a final report. It is a useful compilation of the artifacts produced in each phase of the integration process and resides in a central location. At this stage, SMEs from the stakeholder organization become actively involved in detailing the functional needs of the technology in order for it to satisfy the stakeholder’s requirements. This early interaction is key to developing a system that allows the eR&D Team to meet its goal of helping stakeholders take advantage of advances in technology research. This interaction results in requirements and acceptance test criteria by which the technology will be evaluated when the integration is complete.

2.1 Pilot Deployment

In that the goal of DHS’s eR&D Team is to discover and filter newly developed technologies for possible integration into operational environments based upon identified stakeholder requirements, the requirement for a tool that could help address an automated malware analysis capability was articulated by the DHS cyber center. Specifically, this requirement originated from a change request that was submitted by the DHS cyber center for capability enhancements in the area of improved malware analysis. Based upon this identified need/requirement, the eR&D Team then used REQcollect to discover possible technologies/capabilities that could address the DHS cyber center need. At this point, four potential technologies/capabilities were discovered using REQcollect and additional requirement details were sought out from the DHS cyber center, which included the need/requirement for an automated dynamic and static malware analysis tool/engine. Consequently, of the four potential technologies/capabilities discovered, three of them were demonstrated to the DHS cyber center and further input on their needs was garnered and applied during filtering. Based on the above eR&D methodology of identification, discovery, and filtering, the Hyperion Tool was down-selected for integration into the DHS cyber center through a pilot deployment to assess its ability to meet malware analysts’ needs as well as satisfy the “static analysis engine” requirement.

2.2 Description

The Hyperion System/Tool as developed by Oak Ridge National Laboratory (ORNL) is a new technology built for malware detection and analysis that employs rigorous semantic methods to automatically compute malware behavior and classifies it for analyst’s understanding and action. Further, the Hyperion Tool is intended to capture and reuse malware analyst’s expertise to leverage this scarce resource across a given organization such as the DHS cyber center. Specifically, Hyperion provides a new approach to malware analysis through two key capabilities unavailable in other technologies currently used by malware analysts.

First, Hyperion employs the mathematical foundations of denotational semantics to compute the full functional behavior of software. The behavior is essentially an “as-built” specification of the software, and is computed without the need to execute potentially malicious code. The behavior is represented as a set of disjoint cases that covers the behavior space and reveals both legitimate and malicious functionality.

Second, malware analysts can define Behavior Specification Units (BSUs) that capture their expertise in recognizing malicious content (e.g., key logging or data exfiltration) for use in automatically analyzing computed behavior. BSUs are very general and widely applicable representations of potentially malicious (or legitimate) behavior that are independent of particular code implementations. Hyperion provides a simple language for specifying BSUs. Once defined, a BSU can be applied over and over to the computed behavior of other malware to determine if the behavior is present, thereby sharing expertise and reducing effort otherwise required to manually identify malicious content (see Figure 3 below for BSU definition and description).

### Figure 3, BSU Definition and Description
3. ASSESSMENT METHODOLOGY

3.1 Overview
As approved by the DHS leadership, the pilot deployment and evaluation of Hyperion was conducted as an Early Operational Assessment (EOA) in that an EOA provides both verification and validation of system capabilities based upon stated stakeholder objectives and articulated operational needs. Also, an EOA was specifically chosen due to the fact that as an assessment, it helps keep the focus on mission needs, helps provide some level of risk reduction, and provides a limited operational effectiveness and suitability progress report so the stakeholder can make an informed decision on whether to pursue future development and/or refinement of a given capability. To support the EOA, a Hyperion Assessment Team was formed to plan, coordinate, and execute the pilot deployment and assessment of Hyperion on DHS’s behalf. This Hyperion Assessment Team included the ORNL Development Team and the Johns Hopkins University Applied Physics Laboratory (JHU/APL) Test and Evaluation Team. The Hyperion Assessment Team held regular meetings with DHS malware analysts as well as DHS leadership to discuss the testing process, gather additional requirements and feedback, schedule reviews and updates, reveal any system issues, and share ideas on technical direction and requirements.

3.2 Hyperion Pilot and Assessment Objectives
As a pilot deployment and for assessment purposes, Hyperion was provided to the DHS cyber center to demonstrate and assess it in a real-world, operational environment. Based upon discussions with the malware analysts and DHS leadership, the following four objectives were defined by the Hyperion Assessment Team:

1. Determine the throughput and performance of Hyperion in analyzing potentially malicious software samples.
2. Assess the ability of Hyperion to completely and accurately compute the behavior of a software sample under operational conditions without executing the code (i.e., through static analysis).
3. Determine if the DHS cyber center derived BSUs could accurately capture malicious attributes in computed behavior in comparison to behavior observed through manual analysis.
4. Assess the ability of Hyperion to leverage the BSUs created to detect malicious behavior in software samples collected from security incidents provided by the DHS cyber center customers.

Likewise, the DHS cyber center’s malware analysts described the following user needs for Hyperion:

1. Automatically compute and classify behavior for malware libraries at machine speeds.
2. Help (analysts) conduct detailed, deep dive analysis of specific malware samples.
3. Leverage and reuse malware analyst’s expertise through definition of malware Behavior Specification Units (BSUs).
4. Compute the same behavior for a malware sample no matter how its control flow is obfuscated.

3.3 Assessment Scope
The Hyperion EOA was broken down into the following four parts: Part 1 (Verification of Hyperion Capability); Part 2 (Validation of Manual and Hyperion Analysis); Part 3 (Validation of BSU Definition/Application); and Part 4 (Analysis and Reporting of Results). The specifics are contained below:

Part 1: Verification of Hyperion Capability
The EOA provided verification that assessed the Hyperion Tool against stated objectives/requirements. As such, a description of each of the five phases of Part 1 of the assessment is provided along with its purpose.

Part 1, Phase 1: Simple Programs
- Description: Assessment of Hyperion analysis of simple programs with known behavior.
- Purpose: The purpose of this phase was to verify the correctness of Hyperion analysis output. This was accomplished by analyzing simple, understandable executables and then manually comparing the Hyperion analysis results to the source code for the simple programs.

Part 1, Phase 2: Malicious Programs
- Description: Assessment of Hyperion analysis of randomly selected malware executables.
- Purpose: The purpose of this phase was to verify the stability and performance speed of Hyperion. This was accomplished by analyzing a set of real-world malicious programs and then checking to see if Hyperion produced analysis results in an acceptable amount of time for all of the programs.

Part 1, Phase 3: Benign Programs
- Description: Assessment of Hyperion analysis of known benign executables.
- Purpose: The purpose of this phase was to verify the stability and performance speed of Hyperion. This was accomplished by analyzing a set of real-world benign Windows 7 programs and checking to determine if Hyperion produced analysis results in an acceptable amount of time for all of the programs.

Part 1, Phase 4: BSU Classification
- Description: BSU classification of selected executables.
- Purpose: The purpose of this phase was to ensure that BSU classification correctly classified known behavior in selected executables.

Part 1, Phase 5: DHS Cyber Center Binary Samples
- Description: Assessment of Hyperion Analysis using selected binary samples from the DHS cyber center’s malware repository/library.
- Purpose: The purpose of this phase was to exercise Hyperion analysis on the DHS cyber center’s provided binary samples.

Part 2: Validation of Manual and Hyperion Analysis (Deep Dive)
- Description: A comparative analysis was made between partner-provided malware samples that compared analysis
results produced by the DHS cyber center’s malware analysts and the Hyperion system.

- **Purpose:** The purpose was to compare results between manual and Hyperion-produced analysis as well as to further refine Hyperion capabilities to support deep-dive analysis.

**Part 3: Validation of BSU Definition/Application**

- **Description:** the DHS cyber center’s malware analysts created and applied BSUs based upon characteristics of prior malware received and analyzed.
- **Purpose:** The purpose was to help malware analysts define BSUs that capture their expertise in recognizing malicious content (e.g., key logging or data exfiltration) for use in automatically analyzing the computed behavior. Once a BSU is defined by Hyperion, it can be applied to the computed behavior of other potential malware samples to determine if the defined behavior is present, and thereby leverage an analyst’s expertise while saving time normally required for manual analysis.

**Part 4: Analysis and Reporting of Results**

- **Description:** The Assessment Team collected all data from the testing events including assessment results, problems/discrepancies, enhancement requests, and user perspectives.
- **Purpose:** The purpose of this was to analyze and report on the data collected to provide the sponsor with a perspective of Hyperion’s ability to satisfy both sponsor objectives as well as operational/user needs.

### 4. RESULTS AND WAY FORWARD

The purpose of this paper was to demonstrate how the eR&D approach worked as described. This pilot deployment also demonstrated that the eR&D approach produces better fielded and more capable products for stakeholders. eR&D Approach Finding 3: The overall eR&D Approach of identifying, discovering, filtering, and integrating technologies/capabilities as captured in REQcollect worked as intended during this “proof of concept”.

**eR&D Approach Finding 1:** The overall eR&D Approach of identifying, discovering, filtering, and integrating technologies/capabilities as captured in REQcollect worked as intended during this “proof of concept”.

**eR&D Approach Finding 2:** For most newly developed technologies/capabilities, a partner for further development and production must be sought out by the developer so as to enable further refinement of the technology/capability. This results in a better fielded and more capable product for the stakeholder.

**eR&D Approach Finding 3:** During the filtering part of the eR&D Approach, it is important to actively dialogue with the stakeholder of the need/requirement to get additional details so as to narrow the field of eligible technologies/capabilities.

**eR&D Approach Finding 4:** Integration of new technology or capabilities in support of a given entity’s requirements is still difficult due to real-world operational mission considerations so adaptability by all stakeholders during pilot deployment is a must.

**eR&D Approach Finding 5:** As part of the selection process, a transition partner for the selected eR&D technologies should be identified. A successful pilot of a gap filling technology will quickly become obsolete without a transition partner to invest in and improve the fledgling capability.

### 4.3 Future/Recommendations

The pilot deployment and assessment of the Hyperion Tool was determined to be a success especially in the area of Transition to Practice (TTP) in DHS for its cyber center. ORNL, the developer of Hyperion, has partnered with R&K Cyber Solutions, LLC for further development, production, and distribution. Hyperion has also been provided to other US Government agencies for pilot programs and actual integration into their cyber operations centers. In regards to the overall eR&D Approach, it is recommended that other “proofs of concept” get implemented and tested to further refine and hone the eR&D approach.

### 5. SUMMARY

This paper described the success of the Hyperion Tool’s pilot deployment and assessment in a DHS cyber center using the embedded research and development (eR&D) approach incorporating the four processes of identify, discover, filter, and integrate. The outlined approach as a “proof of concept” demonstrated that the eR&D Team in working with a real-world stakeholder (i.e., a DHS cyber center) was able to elicit identified operational requirements and then look for and discover potential technological solutions. Further, the eR&D Team then filtered from the possible technological solutions the Hyperion Tool for integration through both a pilot deployment and assessment into DHS cyber center workspaces. Consequently, the eR&D approach allowed the eR&D Team to forge relationships with the stakeholder, which gave the eR&D Team immediate access to the operational environment in which the DHS cyber center malware analysts work as well as closed the gap between the research and operational communities. Thus, by tracking and documenting research that is funded by Federal agencies and departments, the eR&D Team is able to discover, filter, and integrate research projects and new technologies that best fulfill the identified R&D requirements of its stakeholders. Continuing to follow the eR&D process will ensure that DHS receives the innovative technology that it needs to accomplish its mission in an efficient and timely manner.
Further, this eR&D approach for transitioning technology helps facilitate successfully traversing the Valley of Death between the research and operational communities by linking both the producers and consumers of research technologies. Thus, the eR&D approach helps build a bridge across the Valley of Death by more effective communication and translation of user needs and research technologies.

6. REFERENCES


Appendix A

Specific recommendations that apply to the DHS cyber center regarding the Hyperion Tool are as follows:

Recommendation 1: Workflow Integration needs to be updated in the DHS cyber center to include the use of the Hyperion Tool and its resultant capabilities. This will require working with the DHS cyber center’s malware analysts to integrate Hyperion into operational workflows to include developing plans as well as implementing requirements for this purpose. The requirements needing resolved deal with compatibility of data formats and interfaces and usability improvements, and are relatively straightforward to implement. Of particular interest with the overall workflow is the integration of BSU classification findings along with the automated malware reporting process.

Recommendation 2: The Hyperion Tool can and should be improved. Hyperion’s technology can be extended for broader use and increased automation to better leverage analyst capabilities so the DHS cyber center requirements for evolution of the next-generation Hyperion system should be collected. These requirements focus on achieving the full potential of the Hyperion technology to satisfy mission objectives.

Recommendation 3: BSU libraries should be established so as to help reduce the asymmetric advantage of adversaries in regards to cyber operations. Further, the DHS cyber center should establish a BSU working group as well as create collaboration procedures for sharing BSU knowledge and libraries across US government agencies.

Recommendation 4: Hyperion capabilities need to be documented better along with additional training needs to occur in the DHS cyber center. As such, Hyperion embodies unique functionality that requires better explanation, and continued training will help the DHS malware analysts. This is necessary because Hyperion is a new technology with substantial capabilities that are somewhat unfamiliar to malware analysts, organizational leadership, and acquisition personnel. Thus, a need exists to better articulate these capabilities at several levels of abstraction for wider understanding.

Recommendation 5: Hyperion should be used to help “triage” malware feeds. Hyperion technology can be applied to prioritize and categorize “big data” malware streams so there is a need to develop requirements and specifications, and implement a “proof of concept” Hyperion-variant for this purpose. Accordingly, a vision has emerged within the DHS cyber center for a fast, pared-down Hyperion system to analyze “big data” malware streams with BSUs to identify the typically small portion requiring further analysis.