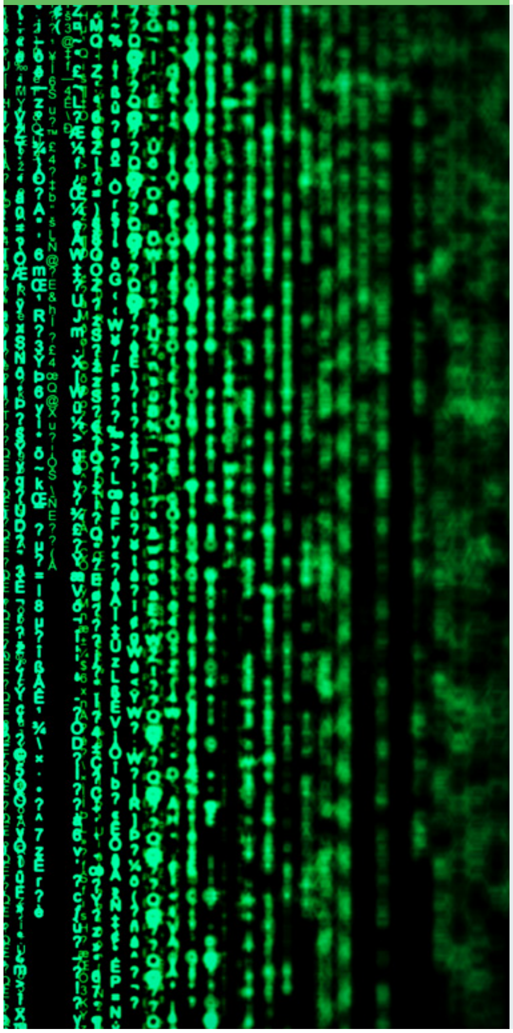
Insight

The Evolution of Cyber Innovation

By Paul Ritchey and Lee Trossbach, ICF



Abstract

In a fast-moving field, ICF continues to drive innovations that address and anticipate challenges in monitoring, detection, and protection from cyber threats. Through its own work and partnerships with other research leaders, ICF has established itself as a pioneer in developing the technologies that underpin current and future cybersecurity capabilities. Here, we present some of ICF's contributions to the cyber innovation narrative, concluding with our views on future development trends.

Withstanding the Test of Time—Intrusion Detection Framework

When a U.S. Army customer contracted with ICF to assist in detecting and identifying malicious network traffic, no one could have anticipated the development of an intrusion detection framework that would still be in place more than a decade later.

The ICF team saw an opportunity to improve the efficiency and scalability of a system that has consequently been able to withstand exponential growth in size and sources of data along with increased bandwidth speeds. ICF's architecture anticipated the limitations of centralized processing by introducing cluster-based processing that established redundancy, supported easy scaling, automated load balancing, and allowed for deployment of improved analysis tools.

Always learning and applying best practices to new implementations, ICF will continue to build on the proven success of its intrusion detection framework. Future developments will reflect continuing needs for scaling—from network bandwidth and utilization along with the processing power required for new tools—and flexibility, compilation of data from disparate sources, and full operational fallback.

ICF has demonstrated its commitment to cyber innovations through its client work and the leadership role it plays in the research and development (R&D) community.

Looking Ahead to a Whole New World—Oculus Rift

Published in December 2015 in ***Evolution of Cyber Technologies and Operations to 2035***, ICF's chapter titled "The Application of Virtual Reality for Cyber Information Visualization and Investigation" paints a picture of the working environment for a future cyber analyst:

> *Shortly after putting on the VR [virtual reality] headset, she is surrounded in virtual space by virtual monitoring tools and displays from network sensors around the world. In the virtual environment created for her, she can see panels of related information surrounding her in a starscape-like fashion. Peripheral indicators can be views with a quick look, and primary indicators and active windows are ahead of her in a windshield-like interface.*
>
> *The system she monitors manages intelligence information, providing intelligence analysts the ability to view, monitor, interact with, or modify the information. She has been assigned specifically to defend the system—not just against attacks, but also from adversaries intent on extracting information.*
>
> *She physically gestures an open hand and motions her arm from right to left "swiping" an active window into view. Her VR headset detects the motion instantly, presenting this morning's most pressing indicators of malicious activity.*

Performing cyber analysis and investigation in a virtual reality environment represents a paradigm shift in the way this work is accomplished. Without the limitations of a monitor and traditional interactive devices (e.g., mouse, keyboard), analysts can surround themselves with the data and tools needed to do their jobs. Using a head-mounted display (such as the Oculus Rift or HTC Vive) and graphics powered by computer, game console, or smartphone, VR display peripherals create a new reality (full immersion) that fills the visual field. Analysts can:

- Work with large primary displays akin to a windshield or multiple monitor setup.
- Bring in or out of view supporting data on all sides and additional walls of information.
- Interact with and swap displays based on gestures.

The ICF Cyberlab created a proof-of-concept prototype that was demonstrated to the cybersecurity research community at the October 2015 CyberSci Summit. Through actual use of an Oculus Rift headset (Development Kit 2), attendees were able to gain a better understanding of the possibilities of virtual analysis in an immersive VR environment. Moving outside the research and development community, ICF was recently awarded a project that will use and continue to build on the virtual analysis concept to develop cornerstone capabilities that will provide foundations for advanced analysis capabilities in VR.

Patents to Protect Innovative Solutions

ICF has introduced two patentable methodologies that represent original contributions to the information technology field and demonstrate the leading-edge role the company has played in the evolving cybersecurity story.

1. **Method and Apparatus for Visualizing Network Security Alerts**
   Applied to the world of Intrusion Detection System alerts, real-time visualization allows for graphical representation of abstract data in intuitive ways to improve understanding and speed response. When network events are presented on a 3-D graph leveraging a comprehensive methodology, analysts can quickly identify outliers and patterns to help prioritize investigation decisions. As networks continue to grow in size and complexity, effective cybersecurity will require innovations and capabilities to translate overwhelming amounts of data into meaningful, actionable information.
2. **Method and Apparatus for Monitoring Network Traffic**
   As described in the ICF patent application, network security systems rely on the ability to screen and monitor network traffic in order to identify unauthorized or malicious activity that may be considered harmful. In particular, network security systems seek to identify unwanted network usage while the usage is occurring or is about to occur so that appropriate action may be taken in response. In addition to identifying unwanted network usage, network security systems may record information about the unwanted network usage, attempt to prevent/stop the unwanted network usage, and/or report the unwanted network usage to appropriate personnel.

   One embodiment is a system that collects data from monitored network traffic. The system inputs, in parallel, the data through a neural network. The system compares an output of the neural network—generated in response to the inputted data—to at least one predetermined output. If the output of the neural network corresponds to at least one predetermined output, the system provides a notification relating to the data.

Looking Ahead

ICF has demonstrated its commitment to cyber innovations through its client work and the leadership role it plays in the research and development (R&D) community. From this unique perspective, we are able to identify trends for future developments:

1. **NoSQL Solutions**

   Massive growth in the amounts of data being collected and monitored requires systems supporting structured and semistructured data for analytics, processing, and visualization.

2. **Machine Learning**

   Automation still has limitations in the cybersecurity world, requiring human intervention for identification and prioritization of malicious events. As machine learning matures, we anticipate more application of machine learning techniques to alleviate analyst workloads.

3. **User Interface**

   A pending paradigm shift completely changes how we interface with our computer systems and (more importantly) our data is validated by the interest we see in head mounted display-enabled VR environments.

4. **Data Visualization**

   As the amounts of data processed continue to grow, new techniques for quickly and reliably analyzing the data using new, revolutionary data visualization techniques become more important than ever.

Successful defense against increasingly diverse and complex cyber threats will require cooperation and collaboration by industry, government, and academia. Industrial players bring funding and data for testing; government entities bring inside knowledge of the intelligence and defense communities; and academia offers outside-the-box thinking unbound by corporate or organizational requirements. Contributions from each perspective represent the ideal combination to tackle future challenges.

About the Authors

Paul Ritchey is a Technical Director with ICF and has more than 15 years of experience working in the cybersecurity field. The early portion of his cybersecurity career was focused on utilizing Government-Off-The-Shelf and Open Source software solutions to develop a highly scalable intrusion detection system (IDS) architecture. Mr. Ritchey's work with several other individuals led to an IDS implementation that has proven highly effective and scalable. Once the project was transitioned into the operational environment, Mr. Ritchey led a growing team of computer-security software development experts who supported this system for a 24x7 Department of Defense Computer Network Defense Service Provider (CNDSP). After returning to research and development several years ago, Mr. Ritchey now manages a team of researchers, developers, and analysts who are conducting basic and applied research into new areas of network traffic analysis, securing ad hoc networks, and developing other cybersecurity-related tools.

About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with more than 5,000 professionals focused on making big things possible for our clients. We are business analysts, policy specialists, technologists, researchers, digital strategists, social scientists, and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at **icf.com**.

Lee Trossbach is a Technical Director at ICF. He has been with the company since 2004. He has over a decade of experience in technical and operational duties relating to Defensive Cyber Operations (DCO). Mr. Trossbach graduated with a Bachelor of Science (double major) degree in Business Administration and Computer Information Systems. For the past several years he has studied and researched data visualization and immersive technologies, both professionally and casually. He has a patent relating to visualization of network security alerts.

For more information, contact:

ICF Cybersecurity
cyber@icf.com

icf.com/cyber

Any views or opinions expressed in this white paper are solely those of the author(s) and do not necessarily represent those of ICF. This white paper is provided for informational purposes only and the contents are subject to change without notice. No contractual obligations are formed directly or indirectly by this document. ICF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.