ADVANCING THE ART OF THE POSSIBLE

A Selection of Cyber Security and Cyber Analytics Research Programs

Innovation is a focus at Noblis, whether we are delivering expertise on client-funded problems or advancing science and technology through our internally-funded Noblis Sponsored Research (NSR) program.

The NSR program is a vital part of corporate life at Noblis. Our research addresses our clients' most pressing mission challenges, resulting in sound, sustainable solutions with enduring impacts.

EMPOWERING THE ANALYTIC MISSION

Relying on closed or open source intelligence (OSINT) requires an automated solution for finding relevant data among the vast amounts of information and noise on the Internet and across enterprise document stores.

Versatile Ontology Research (VÖR) is a multi-functional system that enables analysts to collect, extract and discover information from a variety of open and/or closed source datasets. With user-defined input sources and a user-defined taxonomy, VÖR is the one-size-fits-all solution for law enforcement, homeland security and intelligence analysts, dramatically increasing their productivity by automating analysis and finding links in massive sets of documents.

EMPOWERING THE ANALYTIC MISSION PART 2

Understanding, categorizing and searching large amounts of data remains a challenging task for analysts. Noblis' VÖR system accomplishes this task for text documents, but there is no equivalent for visual media such as images and videos.

As part of our machine learning (ML) services, Noblis is developing a caption and object image labeling solution that combines image classification expertise with the practical experience of data analysts. Noblis' expertise in deep learning is applied for image classification to build an automated, image tagging software-solution to meet the growing demand from analysts, allowing them to search through unlabeled collections of images and videos using text-based retrieval methods.

ENHANCING DETECTION AND RESPONSE TO CYBER THREATS

Cyber security analysts face significant challenges detecting threats on modern networks. Alerts are frequent and must be triaged even if they are irrelevant, which consumes valuable analyst time. While commercial off the shelf solutions detect and counter common attacks, custom advanced analytic solutions are necessary to see patterns of advanced adversary activity.

Through the automated cyber analytics project, Noblis is improving cyber analysts' abilities to rapidly detect, analyze and respond to cyber threats through automation. Using a catalog of custom solutions, analysts are better equipped to detect non-obvious patterns, automate the analysis workflow and rapidly triage across data sources to reach conclusions faster. In one of the many Noblis-developed analytics, we use Common Crawl (open and free index of Web data) to backlink to possible sources of malware.

CREATING FABRICATED PERSONAS

Investigators face the two-sided problem of concealing and revealing the identities of online entities for missions ranging from domestic crime fighting to foreign counter-intelligence operations. To answer this challenge, fabricated personas can be constructed to conceal true identities; however, creating and maintaining these personas continues to be a challenge.

We have developed an entity, source and link obfuscation and assessment kit designed to create believably unique and mature personas that can defeat detection by adversaries and adequately meet diverse missions. The solution is designed to automate the creation of online personas in different social environments at different levels of service, commensurate with the requirements of the operating environment and adversary.

CURATING THE DARK WEB

A dynamic dark web repository that can store historical collections of information enables investigation of criminally inclined elements conducting acts against U.S. persons, organizations and/or infrastructure.

Our dark web collection program is creating a platform with the ability to scrape and archive the deep and dark web, without organizational attribution. This repository will be accessible through Noblis' VÖR system enabling far greater efficiency for analysts as they conduct their investigations.

MAKING A SMOOTH TRANSITION TO 5G

5G technology presents tremendous opportunities due to its significant improvements in speed, volume and latency, which will enable many new communication services. Along with these opportunities, there are security risks to consider. Agencies need hands-on, impartial assistance in navigating the complexities of 5G so that its vision becomes reality.

Through the SMART 5G project, Noblis is establishing an integrated 5G infrastructure to evaluate alternative architectures and conduct vulnerability research. This infrastructure, combined with Noblis' existing models, will allow us to explore areas of concern for agencies and identify, mitigate and exploit potential vulnerabilities.

MAPPING THE INTERNET'S ROUTING DATA

Improved Internet routing data displayed geographically, and network analytics based on this data are needed to analyze potential vulnerabilities and identify malicious hosts for cyber defensive and offensive systems.

Noblis has created a globally distributed solution to capture the Internet's routing topology in Internet Protocol version 4 (IPv4). This massive, frequently updated dataset has led to the development of analytics that can identify many major Internet routing components and test the data to classify potentially nefarious equipment, sites and actors.

AUTOMATING THE ANALYST WORKFLOW

Analysts need a dynamic way to correlate cyber threat information. Manual processes do not scale, and many tools do not provide context to allow analysts to pursue adversaries and find new information.

We combine automation, micro-service architecture, cutting edge ML and analysis support solutions into a unified vision to transform analysts' work processes and decrease time-to-action in conducting the threat hunting mission. By leveraging advances in technical architecture approaches and analytic methodology, the Noblis solution automates and simplifies the core time-consuming components of an analyst's workflow.

USING RECURRENT NEURAL NETWORKS FOR PASSWORD IDENTIFICATION

Brute force and random password guessing is a time-consuming task, delaying analysis of captured media.

Through our human generated password analytics project, Noblis is researching the use of recurrent neural networks (RNNs) to replace rule-based and brute force-based password guessing. RNNs have been shown to be useful in generating text in the context of character level natural language. Through training of these models, we are exploring more advanced means of gaining access to password-protected material.

USING DEEP LEARNING TO IDENTIFY ADVERSARIAL ACTIVITY

A constant challenge in applying ML techniques is acquiring, preparing and labelling data for training ML models. This situation is true in the cyber security domain, where "ground truth" needs to be established to accurately identify and profile hidden adversarial activities in a sea of noise.

Noblis is applying the power of generative adversarial network deep learning to problems in PCAP data generation and classification. This approach leverages our experience in modeling protocols from hidden protocol systems for covert traffic. Our research will serve as a strong classifier for suspicious network traffic and is important for code development for new cyber defense solutions and analytics.

noblis
For the best of reasons

noblis esi

answers@noblis.org • 703.610.2000
noblis.org • noblis-esi.com