(* = Poster Board is available upon request)

C2/C41/CYBER

2020

Arytic is a Next-Gen Artificial Intelligence Hiring Platform
Arytic is a Next-Gen Artificial Intelligence Hiring Platform. It is an intelligent machine that leverages inputs from applicants and hiring organizations to determine alignment or fit in the areas of psychometrics or personalities, skills, jobs, cultures and teams. It can be tailored for the culture and employment rules of a specific organization, such as the Department of Defense. It will revolutionize the hiring process, ensuring that newly hired DoD civilian talent is highly compatible to support the global warfighting mission of the DoD. Arytic has demonstrated a significant return-on-investment from creating the first-time fit, thereby enhancing retention and limiting personnel turnover.

Entrap Hunt Tool
The Entrap Hunt Tool leverages advanced malware detection methods using system and process behavior monitoring. This gives cyber defenders more granular visibility into system activity that analysis of system logs cannot. Entrap uses the MITRE ATT&CK model to detect tactics and techniques of advanced persistent threats to enable zero-day detection. With this hunt tool cyber defenders can remediate compromises and threats on a system faster.

Plasticity Disinformation Toolkit
Plasticity's Disinformation Toolkit helps intelligence analysts find the "needle" in the "haystack" of publicly available information like social media, news, and the dark web. The toolkit improves content searching and automatically flags content that may be disinformation, bot activity, or a coordinated narrative by a state/non-state actor. Intelligence analysts can then analyze or translate content and easily generate aggregate reports to pass up the chain of command. Plasticity's tool helps analysts — who have remained relatively constant in numbers over the years — keep up with the exponentially growing quantity of online content.

2019

The Athena Project
The Athena Project grew from experiences in the military where reports written did not translate to reports read, let alone lessons learned. The Athena Project has a unique ability to: • Collect and signify narrative stories of a human (complex) system at scale
• Reduce the cognitive bias in human system mapping through AI tools
• Identify the emerging trends and risks associated with a given human system.

The tools used to accomplish this enable key decision makers within organizations to understand complex environments. The Athena Project's dynamic capacity and capability provide the space and insights for better decisions about critical strategic and operational outcomes.
Private Cloud Technologies Include Edge Compute Solutions

(* = Poster Board is available upon request)

Awnix provides an "Emporium of Compute Products and Services" including but not limited to centralized private cloud base on OpenStack and/or K8s. Awnix also is offering edge compute products and services that are designed to enable emerging markets like 5G and grow existing markets like IoT. Simply put Awnix works with a range of Telco and Gov clients to produce comprehensive cloud solutions with heavy focus on security and innovation.

Handheld, 105+ Language Translation Device
AVAILABILITY, ACCURACY AND TRUST in a translator (whether human or machine) is a critical factor when conversing with foreign nationals. The problem though, there has NEVER been, nor will there EVER be, enough linguists, at all the places, at all the times, that operationally a linguist is critically needed. In this world of “flex” operations, Teams can find themselves in one geographic location today speaking Arabic and then tomorrow a mere 10 km’s away speaking a dialect of French. TRANSL8-LITE provides a handheld device capable of ACCURATELY translating 105 languages and dialects, utilizing our patented Global Awareness (GA) Artificial Intelligence (AI) platform with an output for translated audio streams in both native voice and in native text format.

Advanced Cyber-Threat Detection and Analysis
Anneal Initiative’s cyber-intelligence methodologies facilitate high-impact computer network defense. Anneal’s automated processes deep data-mine classified threat indicators and make secure large-scale correlations with network data. This detects & identifies sophisticated threats targeting networks months or years earlier than other methods. Anneal’s collaborative intelligence analysis processes combine threat knowledge (intent & TTPs) with network vulnerability & consequence knowledge to build targeted risk analysis & cybersecurity strategies.

Borsetta’s Patent-Pending Technology Connects Physical Assets to our AI Asset Management Platform to Secure Real-time Information and Process Intelligent Actions via a Trustworthy Edge Network Today the collection, processing, and dissemination of data across all domains is overly burdensome and slow. In order to win tomorrow every asset must be trusted to connect, share, filter and learn in real time. So, how do we bridge the gaps between disparate assets and networks across all domains? Borsetta’s mission is to secure a hyperconnected world with trust, where every asset, device or object has the capability to self-authenticate, transact, sense its environment, transmit secure real-time information and process intelligent actions via a trustworthy edge network.

2018

Communication system for a definable/decentralized community with multiple levels of access based on assigned authorities/permissions.
OneRoom is a cloud-based communication/user engagement platform transforming how different groups of people (stakeholders), the organizations to which they belong and its partners, connect and communicate. OneRoom recognizes the unique role, tasks, goals and communication needs of each audience. OneRoom streamlines communication by replacing paper documentation, phone/robo calls, text messages and the need for using multiple applications, with an easy-to-use, intuitive interface that prioritizes communicaiton, allows quick and easy task execution. OneRoom empowers users by giving

them control; allowing them to manage tasks and information better, faster and easier to help them be more organized and successful.

We Separate IT From OT and Make OT INVISIBLE on the Internet!

Secure-IoT provides a physical and cyber security solution to end the threat of vulnerable endpoint operational devices. With SC-IoT technology, organizations can employ consistent security solutions with centralized management across the extended network. Secure-IoT is a managed service platform that protects the Operational Technology (OT) of enterprises by providing secure, private networks and managed communications, ensuring safe operations without compromise. Control Systems and devices (i.e., things) that run inside our Virtual Enclaves become invisible to hackers & accessible only to authorized users.

Time, Expense, Referral, Data Sharing

Our software enables secure data collaboration among teams or coalitions.

Entrap - Zero Day Protection

The future of antivirus technology is signatureless. Entrap detects and prevents against existing and future (zero-day) computer viruses, ransomware and other malware. Our approach uses complex mathematics used and proven in genetic analysis and DNA sequencing. Our team has analyzed the behavior of thousands of malware samples to recognize malicious behavior in programs in real time. This technology provides the best defense against zero-day exploits and virtually eliminates the need for frequent signature updates.

Digital Maps and Data Science

Modern intelligence teams rely on strategic information to ensure the success of their mission. Without the ability to effectively communicate this information their missions may be put at risk. To solve this, our team has developed a mobile geospatial intelligence system. The system has been designed over years of research and includes best practices in the fields of digital mapping and data science. We have designed the system in a rugged case so that it may be easily shipped to any location and can support hundreds of concurrent users. This exciting innovation is nearly complete and we look forward to learning about your key requirements to bring it over the finish line.

Intelligent Integrator - Secure (iIntegrator-Secure)

Legacy IT Consulting and custom integration efforts have compelled businesses to take one of three courses of action; (1) stop your DevOps innovation efforts and concentrate on an integration, (2) depend on legacy processes where knowledge is leveraged by an isolated few, or (3) pay hundreds of thousands of dollars and 12 to 24 months of development for an IT Consulting giant to create a custom integration. Why? What if there is an easy-to-use solution that unifies data integration and knowledge-based decision making at the Line-of-Business user level? The solution? iIntegrator – Secure is a paradigm shift in enterprise level knowledge-based decision-making for organizations of all sizes.

Information Defense - from Internal and External Threats

Information, documents, plans, etc are under threat of being leaked or stolen by internal actors, or by

being destroyed by external actors, often ransomware. PA File Sight detects users copying files (more than simply opening them with Word), and can also protect documents on file servers from ransomware-infected user computers that might attempt to encrypt files on the server. Both situations can send real-time alerts and block the user from accessing any further files on the server.

STARTTM Sensor Network
A rapidly deployable wireless sensor network that leverages communication link quality between nodes to detect intruders. The nodes can be placed or tossed in the desired area without the need for extensive planning. Once deployed nodes form a self-healing selfconfiguring mesh network for communication and sensing. When the nodes detect a change in communication link quality they trigger a camera to verify the intrusion using image recognition software. The system can be monitored remotely via a secure web interface.

Channel Statistics Dependent Frequency Hopping
Wireless digital communication systems are subject to interference when more than one signal is transmitted at the same frequency. In order to avoid signal degradation, the military uses frequency hopping, changing the frequency throughout signal transmission. This technology is an improved frequency hopping algorithm. The algorithm uses the capability to measure the bit error rate (BER) at the receiver. The frequency hopping pattern is then changed with respect to the BER at that frequency. Frequencies with high BER are likely experiencing more interference and are therefore used less by the transmitter, and frequencies with lower BER are used more.

Secure IoT Manufacturing System
The use of the Internet of Things (IoT) is gaining interest in manufacturing systems because it allows such systems to improve their efficiency. Unfortunately, the use of IoT creates cybersecurity vulnerabilities, which could ultimately sabotage and introduce defects into the manufacturing system. One group of possible sabotage attacks is the defect injection (DI) attack. This attack causes objects to be fabricated with deformed geometry, weak material composition, and other flawed characteristics. The presented technology is a method to detect compromised machines in IoT-enabled manufacturing systems. The method uses energy consumption and voltage measurements to identify compromised machines.

2017

REAPR (Reactive Electronic Attack Portable Radio)
Kerberos International, Inc. (“Kerberos”) and Southwest Research Institute (“SwRI”) are developing a low cost, small SWaP, efficient and effective multi-mode Electronic Warfare (EW), Electronic Support (ES) and Electronic Attack (EA) system that is capable of identifying and disrupting (jamming) adversary RF signals/transmissions in the V/U/SHF frequency range without disrupting Blue Force communications, weapons systems or data networks.

Flight Controller Testbed for Rapid Design, Simulation and Validation Capabilities This technology provides an organic and modular hardware system and software environment for rapid development of guidance, navigation and control (GNC) algorithms for automatic and intelligent control of Unmanned

(* = Poster Board is available upon request)

Aerial Systems (UASs). The hardware, software, and ground station modules are designed tosupportsingleormultipleUASs. ScalabilityofsystemsallowssupportingabroadrangeofUASs including swarm flights.