ANALYGENCE

SUCCESS STORY

Department of Homeland Security

ANALYGENCE is a trusted partner for mission support, cyber solutions, and management services. We specialize in achieving the goals and needs of government, military, and industry partners by leveraging our diverse backgrounds, applying our extensive management consulting expertise, and customizing solutions for each and every client. We recently completed a cutting-edge cyber support contract for the Department of Homeland Security (DHS) to assist the National Cybersecurity and Communications Integration Center (NCCIC) in meeting a critical mission requirement to provide the detection and analysis of sophisticated malware that existing anti-virus products and network security software cannot detect, integrate enhanced detection capabilities into the existing Hunt and Incident Response (IR) Team (HIRT) baseline tools and applications, and validate efforts for advanced malware detection and analysis.

ANALYGENCE worked with the NCCIC and the Office of the Chief Technology Officer (OCTO) to develop enhanced tools to evaluate malware in potentially infected networks and systems. Due to the volume and complexity of the files to be reviewed, coupled with the pace and sophistication of attacks, the NCCIC required the integration of the output of multiple analysis tools into a single analytic report, allowing them to accelerate their processes and workflow. Our team completed deliverables that included a robust and automated toolset to detect and analyze files, provided alerts when malware was detected, and produced reports detailing the malware technical characteristics.

In addition, ANALYGENCE assisted the OCTO in a scientific validation of a proposed Secure Internet Access and File Transfer (SIAFT) Architecture by integrating a version of the analytic platform defined in the SIAFT draft security architecture in a lab test environment and producing an output report. Upon Government approval of the analytic platform and validation approach, our team constructed the platform in our lab environment, beginning with the creation of the controlled environment in which the test platform would be constructed and installed. Development of the test platform included the integration of a number of commercial malware detection and analysis tools and availed itself to the storage hardware, network devices and processing hardware in the environment to house large malware data sets, process the data, and store results. The resulting environment and platform were developed and validated independent of external network connectivity and other devices as to ensure safety and high levels of cyber hygiene in the work environment. Resulting reports from each of the integrated malware tools used in the validation task were combined, using the conversion software and malware description language specifications used in the earlier IR Toolset upgrade effort. The final task was the development of a Proof of Concept (PoC) system with a live test scenario of the process. ANALYGENCE applied an agile development methodology to the development, integration, and deployment of the PoC platform. Upon completion of the PoC demonstration, our team installed the platform in a live operational setting to test the efficacy of the overall solution and provided multiple demonstrations for DHS customers. Finally, we developed and then delivered to the Government the lab test system in standalone mode to diagnose problems in the operational system.

ANALYGENCE.COM

CONTACT US

6811 Benjamin Franklin
Drive
Suite 170
Columbia, Maryland 21046

1433 Hooper Avenue
Suite 119
Toms River, New Jersey
08753

(301) 830-6092
bd@analygence.com

DUNS #: 964747732
Cage Code: 65G01