



DTIC-AI • 6721 John J. Kingman Road, Suite 0944 • Fort Belvoir, VA 22060-6276 • Commercial 703.767.9120 • DSN 427.9120 • Fax 703.767.9119 • E-mail iaic@dtic.mil

DTIC Sponsored IACS: AMPTIAC • CBAC • CPMA • DACS • HSIAC • IATAC • IRIA • MSAC • MTIAC • NTIAC • PAC • SURVAC • WSTIAC
Military Sponsored IACS: ARMIAC • CEIAC • CRBTIAC • CTIAC • DTRIAC • EIAC • HEIAC • SAIVAC • SMIAC

[Archives](#)



Data and Analysis Center for Software (DACs)



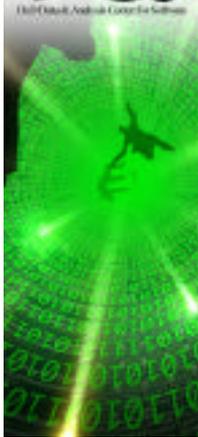
Automated Intrusion Detection Environment – Advanced Concept Technology Demonstration

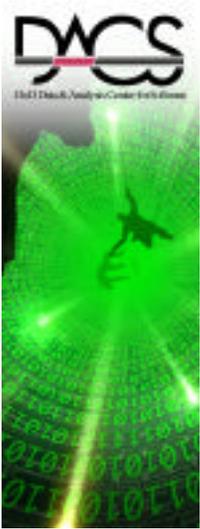
The DACs was recently made aware of a July, 2001 letter of appreciation which was sent by Mr. Don C. Eddington of the Center for Advanced Technology, an office of the Defense Information Systems Agency, to the Air Force Research Laboratory – Rome Research Site. This letter outlined the efforts put forth by Mr. Philip Zaleski and Mr. Stephen Kelly of ITT Industries – Advanced Engineering and Sciences, for their role in the preparation and execution of the final demonstration of the Automated Intrusion Detection Environment – Advanced Concept Technology Demonstration (AIDE-ACTD).

[Continued on Story 2](#)

Please visit our Web site at <http://iac.dtic.mil/dacs> or send us an E-mail at dacs@dtic.mil

[Visit the Archives section for past stories...](#)





Data and Analysis Center for Software (DACs)



Please visit our Web site at <http://iac.dtic.mil/dacs> or send us an E-mail at dacs@dtic.mil

[Visit the Archives section for past stories...](#)



Data and Analysis Center for Software (DACS)

DACS

Story 1

Story 2

Automated Intrusion Detection Environment – Advanced Concept Technology Demonstration (continued)

The AIDE-ACTD is a tool which is designed to normalize and correlate network and host-based intrusion events from disparate Government off-the-shelf (GOTS) and Commercial off-the-shelf (COTS) sensors at a government facility. With this information, the AIDE-ACTD can prioritize the events and display them on a single user interface, while making the information available to a hierarchical management structure. The AIDE-ACTD was born out of the preliminary work from DACS TAT#6, which is the Air Force Enterprise Defense (AFED) task currently in progress at AFRL-RRS. A close relationship and frequent technology transfer with AFED helped to build the AIDE ACTD into a successful system that was proven to correlate network intrusion events across various GOTS and COTS sensors, thereby streamlining a facilities' administrative tasks. It was outlined in Mr. Eddington's letter that, as part of the core development team, Mr. Zaleski and Mr. Kelly were an integral part in the overall success of the AIDE-ACTD final demonstration. Specific areas mentioned were preparation, test script generation, performance enhancement, and site hardware and software configuration. During the dry run and final demonstration of the AIDE-ACTD, both Mr. Zaleski and Mr. Kelly participated in daily status teleconferences, kept the automated reporting structure in place, and collected metrics from the AFRL-RRS site. After the final demonstration, Mr. Zaleski and Mr. Kelly helped to analyze the data that was collected, provided results for the test report, and assisted in the out-brief to the Office of the Secretary of Defense. Mr. Eddington closed by saying that these efforts were vital to the overall success of the AIDE-ACTD program, and looked forward to their positive contributions in the future Information Assurance AIDE Forum and Pilot Services. It's important to note that the AIDE-ACTD is currently in the technology transfer phase with the DISA Joint Programs Office (JPO).

Without the work that has been accomplished on DACS TAT#6, the AIDE-ACTD would not have been able to meet it's goal to be a tool that the DoD could use to help protect its' information infrastructure.

Please visit our Web site at <http://iac.dtic.mil/dacs> or send us an E-mail at dacs@dtic.mil

[Visit the Archives section for past stories...](#)