Commercial Intrusion Detection & Auditing: Installation, Integration & Use from the Security Professional's Prospective

Moderator
Jim Codespote
Technology, Security, & Interoperability Branch
National Security Agency
(410) 859-6214

Panelists

Dan Gahafer, CACI Inc.
Lawrence B. Suto, Strategic Data Command Inc.
Gordon Coe, AT & T

Abstract:

There are several intrusion detection and auditing products commercially available to help protect computer systems and networks. These products offer mechanisms such as signatures to detect misuse and intrusions, user profiles and real-time alerts and reporting. However, every product requires specific configuration for the particular network or system it protects. They are usually far from turnkey solutions and require much time and effort to install and to use. The panelists will discuss their experiences with planning, implementing, and maintaining their respective intrusion detection solutions. They will focus on product scalability, data analysis, ease of use, clarity of reports, and hurdles that had needed to be overcome before the product could be used operationally. The intent of the panel is to provide insight (war stories) to those attendees looking to implement a COTS intrusion detection solution from a non-vendor (customer) point of view. Dan Gahafer from CACI Inc. will discuss his experiences with the Haystack Labs Inc. Stalker product, Lawrence Suto from Strategic Data Command Inc. will discuss Science Applications International Corporation's (SAIC) Computer Misuse Detection System (CMDS) product, and Gordon Coe from AT&T will speak on Wheel Group Corporation's NetRanger Product.