Highlight

Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPS) monitor computer systems and networks to detect unauthorized attempts to access and use the systems and networks, as well as abuse of existing privileges. When intrusions are discovered, IDPS log all activity related to the breach, make the appropriate notifications, and take the appropriate countermeasures to limit the magnitude of the breach.

To assist emergency responders in selecting the right IDPS for their jurisdiction, Science Applications International Corporation (SAIC) prepared an application note for the System Assessment and Validation for Emergency Responders (SAVER) Program. The Intrusion Detection and Prevention Systems Application Note provides information on the operational usage of these systems.

All reports in this series will be placed in the SAVER section of the Responder Knowledge Base website (https://www.rkb.us/saver) as they become available. Information on other technologies evaluated by the SAVER Program can also be found on the website.