

Intrusion DETECTION

From intrusion detection to intrusion prevention.

These days, companies require an effective Intrusion Detection System (IDS) for logging attempts made by outside hackers to penetrate the company's public and private network segments and hosts. Log reports should be regularly reviewed by technical personnel to identify real threats and decide whether action needs to be taken or if upper management should be notified.

IDS Methodology

SEC's proven methodology for implementing and managing an effective IDS solution is as follows:

- Work closely with company IT personnel to identify hosts and network segments that house critical assets and warrant monitoring, including server hosts, Internet gateway, screened subnets (DMZ) for publicly accessible servers, network segments that will allow for the capture of most or all user traffic, and any other critical network areas
- Strategically deploy OS and network sensors and implement a central management console to gather data from all deployed sensors and store in a centralized database. Consolidate data for alert review/notification and report generation.
- Execute a 30-day trial period for initial implementation of the IDS software to build a database of logs for review so that we can determine the difference between normal business related traffic and non-business related traffic, make changes to the configuration to weed out false positives, and tune the system to provide meaningful alerts and reporting data.

- Communicate any Trojans or suspicious network activity found so that corrective actions can be taken.
- Establish an alerting process, such as e-mail and paging notifications, and develop a policy for notifying designated management personnel that can delegate corrective actions.
- Communicate with change control management board to address any future IDS sensor deployments to account for the addition of critical server hosts or changes in the network architecture.

We are an ISS Premier Partner and are well versed in the design, deployment, and management of ISS products, including the Real Secure product suite and Internet Scanner. Additionally, we are experienced in the design, deployment and management of open-source IDS solutions, such as SNORT.

SEC provides security consulting and technical services in addition to performing internal and external vulnerability assessments and security audits. We have a thorough understanding of the challenges that companies face in securing the integrity of their business and network environments. Consequently, our engineers are actively involved in leading industry-related newsgroups and organizations to stay current on the latest vulnerability concerns and hacking methods used to exploit enterprise networks. We are mindful of these concerns and apply our knowledge, experience, and expertise to every security solution we design and implement.