

Secure Associates

Intrusion Detection System

SA-IDS Overview

Secure Associates Intrusion Detection System (SA-IDS) provides a layer of defense, which monitors network traffic for predefined suspicious activities & patterns, and alerts system administrators when potential hostile traffic is detected.

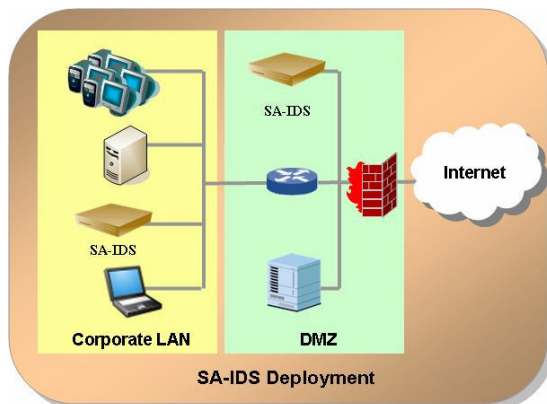
SA-IDS is capable of performing real-time traffic analysis and packet logging on IP networks. SA-IDS can perform protocol analysis, content searching/matching and detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.



Easy Installation and Configuration

SA-IDS software package consists of SA-IDS Console and proprietary MindStorm AnalyzerPro for security administrator on easy installation, configuration and on-going management.

With pre-configured rules, security administrators can perform optimal protection for the enterprise network in just a minute. SA-IDS also provide rules customization to fit enterprise specific security requirements.

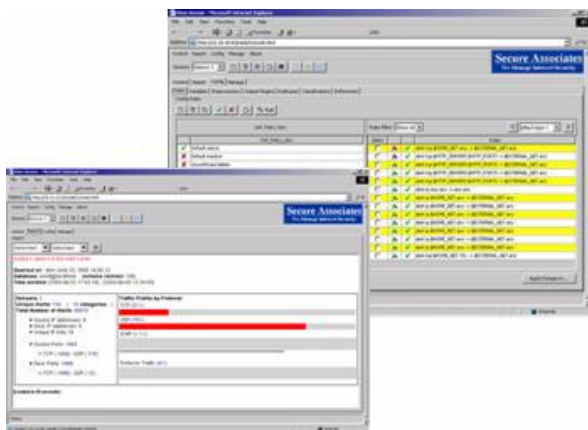


SA-IDS Features and Benefits:

- Web-Based Management GUI
- Automatic signatures/rules update
- Easy rules management and configuration
 - Default Rules Set
 - Customized Rules Set
- Easy to backup and restore IDS configuration
- Database management on data backup, restoration and purge.
- Automated attack response
- Alert when potential hostile traffic is detected
- Monitoring and analyzing network traffic for predefined suspicious, abnormal activities or patterns
- Security events/alerts consolidation and prioritization
- Reduce false positives
- Event knowledgebase for quick security response
- Advanced reporting
- Integrated with MindStorm for total security management.

Rules-based Detection Engine

SA-IDS utilizes rules-based detection engine that can be configured to detect both signature-based events for known and unknown security threats. Rules are used to scan packets at the IP protocol and the application to look for any attacks against the protocol. Out-of-the-box, SA-IDS includes over 2000 rule signatures. SA-IDS provides ease of use graphical user interface that allows customers to easy create their own rules and added to the ruleset on individual or groups of sensors.



Protocol Analysis and Detection Methods

SA-IDS provides several kinds of detection methods for detecting protocol anomalies. Stateful Inspection can detect port-scans, IP stack fingerprinting, TCP protocol anomalies and TCP evasion attacks. IP Defragmenter detects Denial of Service attacks and fragmentation evasion techniques. SA-IDS has a robust stream reassembly capabilities with the intent to let SA-IDS be able to handle performing stream reassembly for organization who need to track and reassemble more than 256 streams simultaneously. SA-IDS can provide full stream reassembly and stateful inspection for up to 64,000 simultaneous sessions.

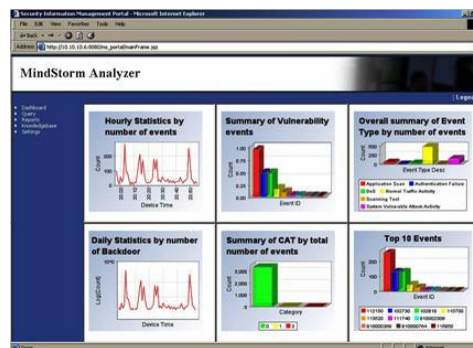
Event Severity and Prioritization

Each event detected by SA-IDS has been assigned a severity. This severity allow security administrator easy to identify the incident and take response action more effectively.

MindStorm AnalyzerPro

SA-IDS bundles with a comprehensive reporting and analysis tool, which provides a single console for security administrator to monitor and analysis SA-IDS events. MindStorm AnalyzerPro out-of-the-box comes with over 200 different kinds of pre-defined report templates including Real-time, Analysis, Technical and Management reports to target different levels of audiences within the organization.

MindStorm AnalyzerPro also provides real-time monitoring and alerting functionalities to allow security professionals easily to identify and respond to attacks and maintain a secure network proactively before security threats break-in.



Key Features and Benefits of MindStorm AnalyzerPro

- Real-time Alerts Monitoring and Incident Analysis
- Security Knowledgebase provides in-depth event information and recommended actions
- Out-of-the-box comes with over 200 report templates
- Easy Report Customization
- Report Scheduling and Auto Distribution
- Supports Multiple languages including English, Chinese (Traditional and Simplify) and Japanese version
- Advanced log query for analyzing large amount of raw data
- Advanced Data Management allows administrators to manage database without a DBA
- Policy-based Alert Response Module supports multiple notification methods and provides capability to integrate to Help Desk System