



SECOS™

SECOSHIELD™

INTRUSION DETECTION SYSTEM

"Currently a best kept secret, SecoShield definitely deserves wider recognition. With emphasis on ease of use, this quick-to-install, simple-to-use IDS will make a fine addition to any security policy, especially in a network where performance is paramount."
SC Magazine, July 2002

SecoShield - Network Intrusion Detection and Response System

SecoShield v3.1 is a network-based, real-time, 'reactive' intrusion detection and response system that provides unmatched security performance. Leading the industry with the most comprehensive event detection, SecoShield offers misuse detection (one of the world's largest attack signature databases), anomaly detection (threshold, statistical, and protocol rules), and policy-based detection that controls both internal and external behavior. It also offers stateful inspection and customized flood and port scanning detection.

SecoShield v3.1 analyzes activities across your network providing early warnings of unauthorized activity, with features that allow it to terminate an attack before any damage has occurred. SecoShield's strong performance capabilities permit sensors to be placed anywhere the administrator considers to be a risk, on either side of the firewall, or even within the demilitarized zone (DMZ). Unlike some IDSs, SecoShield v3.1 detects packets at the MAC-level of the protocol stack, allowing real-time detection without degradation. It also employs statistical analysis to flag abnormal behavior, such as Denial-Of-Service (DOS) attacks.

Another unique feature of SecoShield v3.1 is that it registers dropped packets, which can be the precursor to an attack, thus alarming administrators to possible intruders before any damage has occurred.

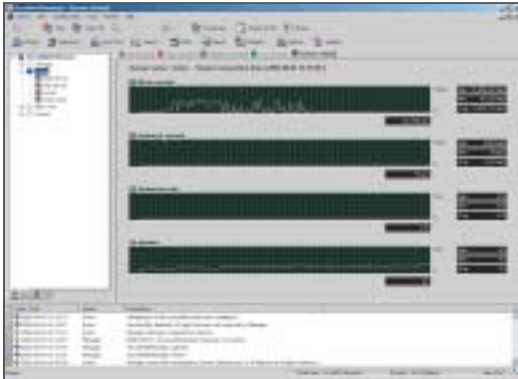
Secos has established a license agreement with SecurityFocus™ to access their globally collected and analyzed Vulnerability Database. Our detection signatures are established by vulnerabilities gathered by more than 1,300 sensors in more than 105 countries. These vulnerability-based signatures are updated within 24 hours of discovery from anywhere in the world, allowing SecoShield to detect any type of verified hacking pattern. There is also an option for user threat definition, which is coupled with a policy editor, allowing for more detailed user input.

SecoShield performance goes beyond simple detection. It has the ability to automatically react against intrusions and to reconfigure other security systems, such as Check Point's FireWall-1®. In addition, it can notify enterprise management systems (e.g. Network Management System (NMS), System Management System (SMS), Enterprise Security Management (ESM)) using SNMP traps.

HIGH PERFORMANCE AND SCALABILITY AT ONE LOW COST

- Supports multiple network interfaces
- Single sensor can monitor multiple connections or segments
- Modest sensor hardware and multiple interfaces can recognize sustained sensor monitoring performance in excess of 600 Mbps
- Gigabit capable
- Supports major operating system (OS) environments
- Supports remote management
- Multi-processor, multi-threaded engine

REAL-TIME MONITORING



- Real-time performance statistics
- Display packet loss rate

GRAPHICAL USER INTERFACE



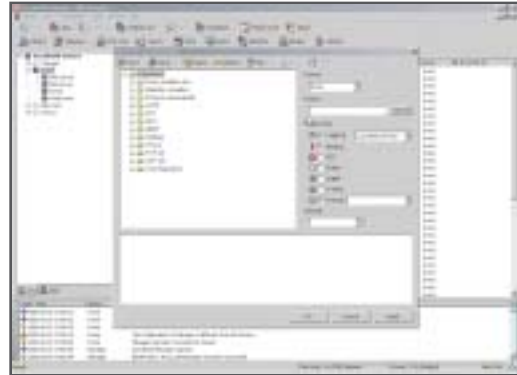
- Fast, intuitive windows GUI
- Event log - high, medium, low severity views
- Audit logs
- Network traffic information, sensor packet loss ratios

MISUSE DETECTION



- Live Updates
- Customizable signatures

RESPONSE CAPABILITIES



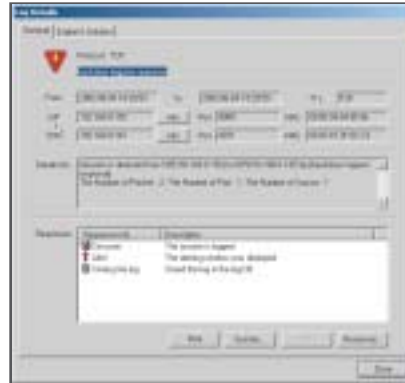
- ACTIVE responses
- Digest audit logs, detailed detection information, e-mail, and window alerts

CUSTOMIZABLE REPORTS



- Easy, powerful, accurate real-time reporting tools
- Exports data to all major file types (.xls, .txt, .html, etc.)
- 15 standard text and 5 graph reports

FULL SESSION RECONSTRUCTION



- Advanced forensic documentation
- Source destination and event details
- Protocol structure and values
- Packet content in binary and ASC II values

Technical Specifications

SecoShield v3.1 Management Console (recommended)

Processor	Dual PIII 800Mhz, 256K cache
Memory	512Mb
Hard Drive	At least 20 Gb Internal SCSI
Network Interface	Fast Ethernet/Gigabit Interface 1 EA
Operating System	Windows NT 4.0 (SP6) or Windows 2000

SecoShield v3.1 Sensor (recommended)

Processor	Dual PIII 800Mhz, 256K cache
Memory	512Mb
Hard Drive	At least 8 Gb Internal SCSI
Network Interface	Fast Ethernet/Gigabit Interface 3 EA
Operating System	Windows NT 4.0 (SP6) or Windows 2000

Platforms

Windows NT 4.0 (SP6) or Windows 2000
Solaris (SPARC) 2.6, 7.0, 8.0
Linux Red Hat 7.1 and Kernel v2.2 or higher

About Secos

Founded in 1997, Secos is dedicated to the development of effective, globally focused technology, offering network, transaction, content, and system security. Our products meet the challenges of today's information security marketplace by providing compatibility, integration, and reliability essential to conducting secure online business. Secos provides the most powerful new technologies for security management, adding intelligence and efficiency to security without affecting the performance of the networks they protect.

For complete product listings and trial downloads, visit www.secos.com.

For more technical information on Secos products, please contact us at support@secos.com.
For a Secos sales associate, please contact us at sales@secos.com or call us at 949.794.0021.

18301 Von Karman Ave., Suite 460
Irvine, CA 92612 USA
Phone: 949.794.0021
Fax: 949.794.0027
www.secos.com

