Compendium
of
Anomaly Detection and Reaction Tools and Projects

MP 99B0000018R1
Version: 2.0d
May 17, 2000

by Leonard J. LaPadula
The MITRE Corporation
Bedford, Massachusetts

Table of Contents

Section **Page**

Introduction

This document is a compendium of anomaly detection and reaction (ADR) automated tools and research projects. In the first appendix to this document you will find an explanation of what we mean by "anomaly detection and reaction". In the second appendix you will find a description of the attributes used to describe the tools and projects.

In the descriptions of tools and projects, we have used the unverified claims of the vendors and projects, paraphrasing what they have written to ensure a uniform style of presentation. In some cases, some other source of information was used; these cases are noted individually.

A compendium of this type cannot cover all ADR tools and projects: there are too many of them and the population changes rapidly. For the commercial off-the-shelf (COTS) products, we started this compendium in the latter half of 1998 by focusing on major vendors and tools [1]. At that time we included products from vendors in three groups—primary, secondary, and other. These groups were defined on the basis of information provided in a Hurwitz Group white paper [2]. Primary providers were those vendors with the highest revenues as reported in the white paper. Secondary providers were those with comparable, competitive tools or systems, as identified in the same paper. Other providers were added to the compendium as we discovered additional tools from searching available sources of information. See the first version of this compendium for fuller discussion of these points and identification of the primary, secondary, and other providers.

We now add to this compendium without regard to current revenues of providers. Rather, we include any commercial products of any vendor that appear to be released, fully supported offerings relevant to anomaly detection and reaction.

For government off-the-shelf (GOTS) products, we have included all that we could get information about. The research and development projects we have reported are projects funded, directly or indirectly, by the U.S. government; we have not attempted to discover what research and development efforts may be underway by vendors.

The remainder of this document is organized as follows:

- Commercial Off-the-Shelf Products
- Government Off-the-Shelf Products
- Research and Development

Section 2

Commercial Off-the-Shelf Products

AntiSniff, Version 1.0 (July, 1999)

Vendor	LOpht Heavy Industries, Inc.
Type of Tool	Network Scanner
Description	AntiSniff is a new class of proactive security monitoring tool. It has the ability to scan a network and detect whether or not any computers are in promiscuous mode. This is often a sign that a computer has been compromised. With AntiSniff, administrators and security teams can finally get a handle on who is watching network traffic at their site.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT A stripped down command line only version will be released for Unix systems
Target Platforms	Any computer attached to AntiSniff's network
Network Topologies	Ethernet
Methods of Detection	Various tests are performed. Currently version 1.0 of AntiSniff performs three classes of tests: Operating System specific tests, DNS tests, and network latency tests3. Each test can stand on its own for determining a machine's state or be used in conjunction with the other tests included in the suite. AntiSniff V1.0 is designed to work on local network segments in a non-switched environment. In switched environments but its functionality will be limited. Projected AntiSniff V2.0 will also work across routers and switches.
Sources of Data	Observations
Reports	Reports tab of interface shows results of tests in tabular and graphical form.
Reactions	Alerts: console alarms or e-mail

AutoSecure Access Control (for Windows NT or for UNIX)

Vendor PLATINUM technology, inc.

Type of Tool System Monitor
(System Monitor for Access Control)

Description PLATINUM's AutoSecure Access Control for Windows NT (ACWNT) extends to the Windows NT platform the same kind of proactive access control security that AutoSecure Access Control for UNIX (ACX) provides for UNIX platforms. ACWNT also provides a central point for the administration of security of mixed UNIX and Windows NT environments.

Native Windows NT provides ACL (access control list) protection for files and directories in NTFS only. AutoSecure ACWNT extends this protection to FAT, HPFS and CDFS files systems. When any user, including the administrator, requests access to a file, the ACWNT authorization engine checks the access privileges granted to that user and either permits or denies access. Access to sensitive system resources can thus be tailored to a user's specific functional needs.

PLATINUM's AutoSecure ACX is a comprehensive security management solution that provides mainframe-level protection for distributed UNIX environments. It protects enterprise-wide information assets from unauthorized access, modification, or destruction. It does this from within the operating system without modifying the operating system kernel code. This is done by intercepting calls to the system and making a decision to grant or deny access based on rules defined in the AutoSecure Access Control database. If access is granted by AutoSecure it is then passed on to the system.

AutoSecure ACX enables control of the root user, prevents Trojan horses and backdoors, provides audit trails, protects configurations, and provides many other powerful security features.

The product includes ACXpert, a Windows 95/NT graphical user interface, which gives you point-and-click icons, pull-down menus, and the ability to drag and drop desktop items for the easy administration of AutoSecure database classes and records. AutoSecure ACX can easily scale to support any size network from departmental systems to enterprise-wide environments. ACX is scaled with the use of a Policy Model Database(PMDB). The PMDB is a management database that pushes rules out to subscribing systems. PMDB's can be set up in a hierarchical fashion to allow grouping of like systems. The same version of ACX is used no matter what size the network is. Each systems has a

	copy of ACX installed and PMDB's are used to manage groups of systems. PMDS is included as part of the software product and runs on UNIX or NT system that ACX is installed on. ACX on NT provides a GUI that can be used to manage a mixed environment of UNIX and NT systems. A Motif-based GUI is provided for UNIX-based ACX; it provides a single point of management for a group of UNIX systems. The ACX products operate on any network running TCP/IP.
Architecture	Sensor Sensors—Director (when Windows NT is employed as Manager)
Agent/Sensor Platforms	Windows NT UNIX (HP-UX, AIX, and Sun Solaris).
Director Platforms	Windows NT AutoSecure AC can administer NTs and UNIXs on the same network
Methods of Detection	Pattern matching (monitors access attempts)
Reactions	Alerts: • An ACX can send an ordinary e-mail to a specified recipient (anywhere). • An ACX can provide an alert at the system on which it is running through its normal user interface. • Notifications of attempted security violations, in a proprietary format, can be sent from an ACX to a Windows NT ACX acting as Manager for a collection of ACXs (subscribers). The Manager, in turn, can then use either or both of the above two alert methods to propagate that notification.
Update Method	NA
Communications	
Special Features	Maintains accountability by storing all user activity in a detailed log.

AutoSecure Policy Compliance Manager

Vendor	PLATINUM technology, inc.
Type of Tool	Security Compliance Scanner
Description	PLATINUM's AutoSecure Policy Compliance Manager identifies potential security problems in your system and provides reports and scripts to correct them. It can be customized to generate high-level or very detailed reports, for areas as specific as a single server or as broad as your entire enterprise. PLATINUM's AutoSecure Policy Compliance Manager (AutoSecure PCM) checks your operating systems, network, user accounts, passwords, directories, and file systems. AutoSecure PCM uses a four-phase approach to securing your system: • The Audit phase identifies potential problem areas. • The Analyze phase provides details on the specific weaknesses identified. • The Correction phase uses system-generated correction scripts, modified as required to conform to your security policy, to correct the problems and establish your "security baseline" — the security standard for your organization. • The Monitor phase compares the current status of your system against the security baseline and reports any reduction in security, as well as new security gaps that may have developed over time.
Architecture	Sensor
Agent/Sensor Platforms	Open VMS UNIX Windows NT
Target Platforms	
Methods of Detection	Pattern matching
Sources of Data	
Reports	Report of weaknesses identified
Reactions	Produces report
Update Method	
Communications	Security audit information transmitted across the network is encrypted.
Special Features	All security audit information can be sent to management consoles for consolidation.

BlackICE Defender

Vendor	Network ICE
Type of Tool	System Monitor
Release Date	August 1999
Date of This Entry	February 8, 2000
Description	BlackICE Defender is a host-based intrusion detector designed for use on home or small business systems. It scans all inbound and outbound Internet traffic for suspicious activity. It provides shutoff and traceback capability for suspected attacks.
Architecture	Sensor
Agent/Sensor Platforms	Windows 95/98/NT
Network Topologies	Connection to the Internet via DSL, ISDN, cable, or standard modem.
Methods of Detection	Pattern matching in TCP/UDP packet and on IP addresses
Sources of Data	Network packets
Reports	BlackICE Defender offers on-screen viewing of alerts through a flashing icon in the system tray and through the User Interface.
Reactions	Can automatically block all traffic coming from a suspected intruder.
Update Method	Users can update the product by selecting "Download BlackICE Update" in the "BlackICE Utilities" menu. A new update is available every few weeks. Defender comes with free upgrades for 1-year. After that, upgrades will cost an annual fee of $19.95.
Notes	The BlackICE product line includes BlackICE Pro, BlackICE Sentry, and BlackICE Defender.
Source of Information	http://www.networkice.com/Products/BlackICE/blackice

BlackICE Pro

Vendor	Network ICE
Type of Tool	System Monitor
Release Date	May 10, 1999
Date of Entry	October 11, 1999
Description	BlackICE Pro is a host-based intrusion detector, providing intrusion detection, identification, and protection service on networked workstations and servers. Using a network monitoring engine, BlackICE Pro reacts to suspicious activity (shut off access, traceback) and can also report to the ICEcap management console (*see* separate entry for ICEcap).
Architecture	Sensor (or Agents-Director when used with ICEcap)
Agent/Sensor Platforms	Windows 95/98/NT/2000 workstation or server
Director Platforms	*See* ICEcap
Network Topologies	TCP/IP networks (any 10 or 10/100 Ethernet adapter; gigabit Ethernet coming soon; any Microsoft-compatible WAN connection)
Methods of Detection	Pattern matching (over 200 signatures)
Sources of Data	Network packets
Reports	Event reports
Reactions	Blocks access from detected intruder Notifies the ICEcap management console about the event Gathers information about intruder using backtracing features
Update Method	
Communications	
Special Features	"Collective awareness technology" informs other workstations/servers of attack (*see* separate entry for ICEcap)
Notes	The BlackICE product line includes BlackICE Pro, BlackICE Sentry, and BlackICE Defender.

BlackICE Sentry

Vendor	Network ICE
Type of Tool	Network Monitor
Release Date	1999
Date of This Entry	February 8, 2000
Description	BlackICE Sentry uses Active Packet Monitoring technology to detect suspicious activity and reports it to an ICEcap Management Console. This stand-alone agent provides visibility in areas where BlackICE Pro cannot be installed. BlackICE Sentry actively monitors remote workgroups, sensitive server clusters, and networked mainframe computers for suspicious activity. It records information, including data gathered from backtracing, in logs for use in prosecuting hackers.
Architecture	Agent
Agent/Sensor Platforms	Windows NT, workstation or server
Target Platforms	Particularly oriented toward protecting nonWindows systems
Network Topologies	TCP/IP on Fast Ethernet subnets
Methods of Detection	Pattern matching (Network ICE maintains a database of currently over 300 signatures)
Sources of Data	Network packets
Reports	See ICEcap
Reactions	Sends data to ICEcap Management Console
Update Method	unknown
Communications	unknown
Special Features	
Notes	The BlackICE product line includes BlackICE Pro, BlackICE Sentry, and BlackICE Defender.
Source of Information	http://www.networkice.com/Products/BlackICE/blackice

Centrax 2.3

Vendor	CyberSafe
Type of Tool	Network Monitor System Monitor Vulnerability Scanner
Release Date	1st Quarter 2000
Date of This Entry	April 5, 2000
Description	Centrax integrates host- and network-based intrusion detection, network node intrusion detection, vulnerability assessment, and audit policy management under one interface. Combining each of these capabilities under a common interface provides a capability to detect threats coming from both inside and outside the protected network.
Architecture	Agents—Director
Agent/Sensor Platforms	Windows NT Workstation or Server 3.51 or 4.0 (Windows NT Target Agent) SUN Solaris (Solaris Target Agent) Windows NT Workstation or Server 4.0 (Network Target Agent)
Director Platforms	Windows NT Workstation or Server 4.0 (Command Console)
Network Topologies	TCP/IP
Target Platforms	Same as Agent Platforms
Methods of Detection	Pattern matching • Host-based agents analyze audit data generated on their hosts • Network agents analyze network packets
Sources of Data	Network packets and audit data
Reports	Centrax can generate more than 14 types of standard reports, including statistical reports by user or target, activity reports by user or target, login session reports, enterprise activity summary reports by user or target, enterprise failed logon activity reports by user or target, enterprise browsing activity reports by user or target, enterprise virus activity reports by target, network activity reports by source or destination, and network statistics by source or destination.
Reactions	Alerts: • Pager • E-mail • SNMP traps Responses: User-specifiable for each alert; user can elect to

- Disable an account
- Shutdown the computer
- Log out the user
- Run a Tripwire scan
- Do nothing

Update Method

Communications All transmissions of audit policies, collection policies, and counter-measure responses are encrypted.

Special Features Each activity signature has its own properties, such as response to the alert associated with the signature. The response property is user-definable.

Support for either MS Access or SQL Server as the back-end database is available with Centrax 2.3.

Centrax 2.3 can automatically start a Tripwire scan in response to a threat and can run scheduled Tripwire scans.

Notes Centrax 2.3 can monitor over 300 types of threats and attacks

Source of Information CyberSafe web site

Computer Misuse Detection System (CMDS™)

Vendor ODS Networks, Inc.

Type of Tool System Monitor

Release Date The tool has been available since before 1998. It was developed by Science Applications International Corporation (SAIC); ODS Networks, Inc. acquired the tool from SAIC in September 1998. ODS Networks now refers to the product as the CMDS Enterprise system.

Description CMDS provides both intrusion detection and sophisticated misuse detection in a single system. The CMDS Enterprise security software profiles user behavior, identifies suspicious activities, detects intrusions and misuse of resources, and analyzes data generated from hosts, servers, firewalls, intrusion detection systems, routers and a wide variety of applications. Installed on hosts and workstations, CMDS provides a way to watch for intrusions even in switched networks. CMDS detects and thwarts attempted logins, file modifications, Trojan horse installation, changes in administrative configurations and many other signs of intrusion. In addition, CMDS constantly monitors for the difficult to detect problems like socially engineered passwords, trusted user file browsing, and data theft that might indicate industrial espionage. CMDS supports a wide variety of operating systems and application programs.

Architecture Sensors-Director

Agent/Sensor Platforms Target machines:

- Sun Solaris 2.5 or Higher
- HP/UX 10.x
- DG/UX B2 with Security Option 4.12
- Trusted Solaris 1.x
- Windows NT 4.0

Firewalls:

- ANS Interlock
- Raptor Eagle
- CYBERSHIELD

Other sources of audit data can be used, according to vendor.

Director Platforms Sun Solaris 2.5 or Higher
HP/UX 10.x
DG/UX B2 with Security Option 4.12

Methods of Detection
Pattern matching
Statistical deviation detection

Sources of Data
Audit data

Reactions
Alerts: CMDS generates Warnings and Real-Time Alerts when a network user’s behavior matches a pre-defined threat signature - whether by engaging in activity which is “out-of-profile,” or when an attack signature is detected. Whenever CMDS detects an alert condition, a red CMDS Alert window is displayed on-screen. In Real-Time mode, Alerts display as they are generated. In Batch or On-Demand mode, Alerts will display when processed.

Update Method
unknown

Communications
Director – Sensor communications method unknown.

Special Features
With a CMDS-equipped system, you decide which statistical categories of computer behavior and what threshold of activity in each category will trigger a security alert. You can customize the CMDS Manager to meet the particular security requirements of your network.

CMDS uses an expert system called CLIPS, a knowledge-based system. The CMDS expert system is defined by a set of CLIPS rules that detect only what you tell it to detect. The CMDS server communicates pertinent information from the audit records to the expert system as the data is processed in real-time.

A CLIPS programmer can easily modify CMDS to add or modify attack signatures by adding rules or changing statistics. Statistical categories are determined at run time by a text file that you may edit to meet your requirements.

CyberCop Monitor

Vendor	Network Associates, Inc.
Type of Tool	System Monitor
Release Date	1999
Date of Entry	October 8, 1999
Description	CyberCop Monitor is a host-based intrusion detection tool, providing both real-time packet analysis and system event anomaly detection. CyberCop Monitor's architecture is compatible with high-speed and switched network environments and will run on NT and UNIX Platforms. Host based traffic is monitored along with system events and log file activities.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT 4.0 running SP4 Vendor claims availability for Sun Solaris 2.5, 2.6, HP-UX and AIX in U.S. English from Q3 1999 onwards
Methods of Detection	Pattern matching
Sources of Data	System event logs, system alerts, and network packets ("Sentry" packet analysis) entering the Sensor platform
Reports	Various forms of analytical reporting from a central, enterprise console or directly from each installed server to enable, providing details and resolution advice. 20 predefined reports provided with the product.
Special Features	Developed under the Microsoft Management Console user interface, both CyberCop Monitor and Console integrate to provide a graphical interface for local/remote reporting and remote installation. Monitor is a "snap-in" to the NAI Security Management Interface (SMI) (*see* NAI web-page description: http://www.nai.com/asp_set/products/tns/ccmonitor_features.asp)

CyberCop Scanner, Version 2.5

Vendor	Network Associates, Inc.
Type of Tool	Vulnerability Scanner
Description	CyberCop Scanner discovers security weaknesses in networked environments. It performs evaluations of Intranets, Web Servers, Firewalls and Screening Routers by scanning them and performing tests to discern whether they are vulnerable to intrusions or attacks from hostile users, and identifies what those vulnerabilities are.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT Linux (expected)
Director Platforms	NA
Target Platforms	Any system running TCP/IP
Methods of Detection	Pattern matching
Sources of Data	Responses to probes, including data that it is able to download
Reports	Four selectable formats: HTML ASCII Rich Text Format (RTF) Comma delimited
Reactions	NA
Update Method	FTP site is maintained by vendor. In the future, Scanner will be able to automatically download updates to its Module Database periodically or on-demand.
Communications	NA
Special Features	The 420+ scans built in to the Scanner are grouped in modules, stored in a Module Database. There are about 22 modules, each of which focuses on a type of network resource such as firewall, router, and gateway. Up to 10 different scans can be run simultaneously, the specific number depending on the resources available on the Scanner platform. Scanner can also use a fake DNS server to check for the DNS server cache-corruption (overflow) vulnerability. Network Associates provides software for setting up the fake server. Scanner comes with CASL (a scripting language) that allows users to create specialized network packets for vulnerability testing.

CyberCop Server

Vendor Network Associates, Inc.

Type of Tool System Monitor

Release Date 1999

Description CyberCop Server protects a server through automated detection and response, acting as a complement to existing firewalls. CyberCop Server operates 24 hours a day, 7 days a week, in real time. It offers the following features:

Real-Time Monitoring: Using patented “watchdog-in-a-box” technology, CyberCop Server immediately detects intrusions and tampering such as illegal user substitution to superuser, illegal Web site content modification, illegal network interloper, and illegal login.

Automated Responses: When such detections are made, CyberCop Server automatically issues programmed responses such as login termination, terminating process, paging or sending e-mail to the webmaster, and generating an SNMP trap. In addition, CyberCop Server can even invoke external customized Active Response Modules to repair damage or increase the prevention in other cooperating products.

Architecture Sensor

Agent/Sensor Platforms Windows NT 4.0, Sun Solaris 2.5 and 2.6, HP (expected), AIX (expected)

Director Platforms NA

Target Platforms Same as sensor

Methods of Detection Pattern matching

Sources of Data The tool focuses on 5 layers: network, system, application, x, and y. It uses data from each of the layers; for example, network packets, system events, and application logs.

Reports Server can write to the system log and to the Tivoli Enterprise Console (via ARM [*see* Special Features below])

Reactions Alerts: e-mail, SNMP traps, and paging

Responses: Terminate offending processes, Terminate offending login connections, and Disable/shun offending accounts.

Update Method same as scanner

Special Features ARM (Active Response Module): CyberCop Server can interface with other security applications or corporate applications for customer responses to security events. Available ARMS: Cisco Pix, Tivoli Management Environment, and Fixit, which can repair illegal content changes immediately.

CyberCop Sting

Vendor	Network Associates, Inc.
Type of Tool	Decoy
Release Date	Late 1999
Date of Entry	October 8, 1999
Description	CyberCop Sting presents the appearance of an enticing target to potential intruders, while normal users will generally be unaware of its existence. CyberCop Sting logs intrusive behavior using analysis tools to collect and log evidence of attack source and techniques, whether attacks are from insiders or outsiders. CyberCop Sting emulates a virtual network on a single machine. It can be configured to provide virtual network services and profiles of different devices. It simulates the IP stacks to “fake-out” OS fingerprinting by port scanners (one of a hacker’s most useful tools) by emulating more than one virtual network layer.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT
Target Platforms	CyberCop Sting emulates NT and Solaris servers and Cisco routers
Reactions	Silent alarms, SNMP alerts, paging, and e-mail
Special Features	A redirect feature of Sting sends an attacker to a “live jail server” for evidence collection.
Additional Information	CyberCop Sting is available as a standalone product, as part of the CyberCop Intrusion Protection suite (it is an extension of CyberCop Monitor), and as part of Network Associates’ ActiveSecurity solution, which integrates firewall, intrusion protection, antivirus, and helpdesk products around a secure Event Orchestrator.

Database Scanner 1.0

Vendor	Internet Security Systems
Type of Tool	Vulnerability Scanner
Description	Database Scanner is the first security risk assessment solution for database management systems. With Database Scanner, anyone can establish a database security policy, run an audit, and present all of the security risks and exposures in easy-to-read reports.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT
Director Platforms	NA
Target Platforms	Microsoft SQL Server Sybase Adaptive Server (to be released January 1999)
Methods of Detection	Pattern matching
Sources of Data	Database configuration parameters, permissions, password file, etc. Key areas checked: • Year 2000 Compliance • Passwords, logins and users • Configuration • Installation hot fixes and service packs • Permission Control
Reports	Vulnerability reports, with suggested fixes
Reactions	NA
Communications	NA

Dragon Intrusion Detection System, Version 3.2

Vendor Network Security Wizards

Type of Tool Network Monitor

Release Date August 20, 1999

Description Dragon is a packet based intrusion detection system. It collects packets and analyzes them for a variety of suspicious activities that may indicate network abuse or intrusions. Information is organized to facilitate forensic and analytic analysis of network activity. Dragon collects event data into its own database, which can be accessed by the Dragon analysis tools. These tools process the collected data and produce flat log files, summary information, activity graphs, and replays of network sessions. Dragon sensors also have ‘plug ins’ which allow them to communicate with a central management node.

Architecture Agents-Director (Dragon agents send data to a Dragon-Master server)

Agent/Sensor Platforms UNIX

Director Platforms UNIX

Network Topologies Ethernet 100BaseT

Methods of Detection Pattern matching

Sources of Data Network packets

Reports Flat log files, summary information, activity graphs, and replays of network sessions

Reactions Dragon sensors support SNMP and SYSLOG protocols. SNMP traps can be sent to up to six different network management stations.

Update Method New attacks are published for Dragon customers. Dragon can be configured to automatically download the latest attack signatures.

Communications All communication is encrypted using Blowfish and sent over an ICMP protocol.

Special Features Users can add signatures: signatures are described on one line that defines which way the traffic is going, which port to search for, the name of the attack signature, and the ASCII or binary data that is unique to the attack.

In many cases Dragon sensors can be deployed without static IP addresses or any open ports. This makes detection of and attacks on the sensor almost impossible.

Source of Information http://www.network-defense.com/

Enterprise Security Manager

Vendor	AXENT Technologies, Inc.
Type of Tool	Security Compliance Scanner
Description	Enterprise Security Manager is the reliable, cross-platform, enterprise scaleable, security management framework. Enterprise Security Manager features extensive operating system support, dynamic configuration capabilities, integrated reporting, and open framework. The manager/agent architecture means you can set up domains within your organization to easily group users with similar security profiles. The manager/agent concept, which relies on client/server technology, also means less networking bandwidth is used during security checks. The manager simply instructs each agent to perform the specified security check. Once completed, the agent sends the resulting data to the manager. Only data that is absolutely necessary gets sent between managers and agents. This is a vast improvement over other products which constantly probe the systems across the network in order to get security information. You can drill down into problem areas and correct faulty security settings in your enterprise. All agents can be run manually or on a schedule.
Architecture	Agents-Director
Agent/Sensor Platforms	IBM AIX HP-UX Sun OS Sun Solaris Digital Ultrix Digital OSF/1 Digital UNIX Silicon Graphics Motorola SVR3.2 Motorola SVR4.0 NCR Unix Sequent MS-DOS Windows Windows NT (client and server) Novell NetWare Novell IntranetWare Open VMS

Director Platforms	UNIX systems compatible with X-Window Windows 3.x/95/NT
Target Platforms	See list of agents above
Methods of Detection	Pattern matching
Sources of Data	System parameters
Reports	Graphical view of high-level security posture with drill-down capability
Reactions	None
Update Method	Unknown
Communications	All network communication is authenticated and scrambled using a proprietary algorithm.
Special Features	Enterprise Security Manager's hierarchical approach makes it easily scaleable to your enterprise network. Enterprise Security Manager managers control groups of agents called domains. Enterprise Security Manager super managers control groups of managers for higher level reporting and data consolidation. No matter how large your enterprise, Enterprise Security Manager can be configured to cover it all. Capability to correct faulty settings (this does not appear to be done automatically; thus, it is not listed as a reaction capability)

Expert™ 4.1

Vendor Symantec

Type of Tool Analyzer

Specific Type: Risk Management Tool, which includes network mapping, vulnerability scanning, and risk analysis capabilities

Description A network security and risk management tool, Expert is the first product that can measure and manage network security risk and perform a meaningful business impact analysis. Expert identifies assets and critical business functions most at risk to a company and assesses the potential business impact and financial losses in the event of a network attack or failure. Expert enables one to make intelligent business decisions about network security posture and to protect one of an organization's most vital assets—its information.

Expert can preform the following general functions

- Identify Network Resources
- Identify Vulnerabilities and Safeguards
- Risk and Business Impact Analysis
- Predictive Risk Modeling

Identify Network Resources: Expert uses standard TCP/IP networking protocols to discover network devices such as computers, routers, hubs, and printers, then scans the network to obtain detailed information about the devices and the services that run on them. Expert then creates a canvas and graphically displays the information.

Identify Vulnerabilities and Safeguards: Expert identifies known vulnerabilities inherent in the network under analysis and provides a comprehensive listing of those associated with its specific components and systems. Expert uses non-intrusive network auditing to establish this network security baseline. In addition to detailed vulnerability reports, Expert can provide safeguard recommendations as part of its analysis capability.

Risk and Business Impact Analysis: The user of Expert inputs business objectives, tasks, and assets. Assets are identified as information objects. Using the results of the previous functions, Expert's Business Impact Analysis report identifies the risk incurred by objectives, tasks, and assets.

Predictive Risk Modeling: Expert can model additions or changes to the network using "what if" analysis. It will identify changes to the risk levels of business network functions based on proposed modifications. Expert can model networks as well (*see* special features below).

Architecture	Sensor
Agent/Sensor Platforms	Windows 95, 98, and NT, version 4.0 or later
Director Platforms	NA
Target Platforms	(Vendor) Virtually any system
Methods of Detection	Network discovery: Expert uses services such as ping, SNMP, TCP port scan, traceroute, and Microsoft Networking.
Sources of Data	Scanned systems and user inputs
Reactions	Alerts: graphical change-alerts (changes in network topology)
Reports	Expert provides managerial (summary) reports and technical (detailed) reports on system components, vulnerabilities, and safeguards.
Update Method	Updates and fixes distributed on floppy disk.
Communications	Expert uses TCP/IP and Microsoft Client for Networks
Special Features	Expert provides capability to value information assets as a basis for risk analysis. One can model network risk off-line with Expert by drawing networks, defining objectives, tasks, and assets, listing vulnerabilities and safeguards, and developing network security policies.

HackerShield

Vendor BindView Development Corporation (acquired Netect, Inc. 3/2/1999)

Type of Tool Vulnerability Scanner

Description HackerShield protects against both internal and external hackers. It finds vulnerabilities by probing operating systems and the network. After each scan, HackerShield prepares a report of what vulnerabilities are on your servers, where they are, and how to close them. It can close some of them automatically.

HackerShield maps your network to create an inventory of your servers, workstations, and other IP devices. Using this map, it probes each device for programs that contain security holes that could be exploited over the Internet or intranet. HackerShield uses a database of known hacker techniques to scan firewalls, web servers, mail servers, database servers, file servers, routers, and other IP devices. It can find vulnerabilities in Unix, Windows NT, and Windows 95/98 operating systems as well.

HackerShield scans the operating system and internal configuration of each NT server. It checks for missing OS patches, specifically ones relevant to security. It also checks the integrity of key system files, fire directory permissions, and registry values and permissions in NT servers and workstations.

Architecture Sensor

Agent/Sensor Platforms Windows NT server or workstation

Director Platforms NA

Target Platforms Firewalls, web servers, mail servers, database servers, file servers, routers, and other IP devices, and Unix, Windows NT, and Windows 95/98 operating systems.

Methods of Detection Pattern matching

Sources of Data Various, responses and operating system data

Reactions Reports
Some automatic fixes

Update Method (PC Week
http://www.zdnet.com/pcweek/stories/news/0,4153,371687,00.html)
Automatic monthly updates via PGP’d e-mail.
New checks and fixes are sent to customers using secure broadcast technology that updates the database, without requiring reinstallation; this is done via the RapidFire Updates™ system.

Communications

Special Features	(PC Week) Can automatically fix many vulnerabilities.

ICEcap

Vendor	Network ICE
Type of Tool	Anomaly Detection and Reaction Director
Release Date	1999
Date of Entry	December 20, 1999
Description	ICEcap is a security management console that centralizes information from BlackICE and ICEscan agents distributed on a network. ICEcap can automatically deploy BlackICE on the network with a single command and uses a scalable, centralized reporting structure. Collective Awareness™ operates with a BlackICE Pro full deployment to not only alert an administrator to attacks but to propagate the information to every BlackICE Pro on the network.
Architecture	Director
Director Platforms	Microsoft Windows NT 4.0, workstation or server Microsoft Windows 2000
Target Platforms	*See* BlackICE Pro
Sources of Data	BlackICE Pro sensors BlackICE Sentry agents
Reports	Provides predefined reports and capability for user to define reports.
Reactions	Alerts: • alarms to an SNMP manager • e-mail message • pager message
Communications	
Special Features	ICEcap ships with Microsoft Access but can be configured to use Microsoft SQL Server 6.5 or 7.0 for database storage. The ICEcap database schema is also available for developers who wish to design their own applications or reports to work off the ICEcap database.

ID-Trak

Vendor Internet Tools, Inc.

Type of Tool Network Monitor

Description ID-Trak is an advanced network-based intrusion detection system developed to protect enterprise specific mission-critical resources from internal or external intruders.

A patent pending technique called Stateful Dynamic Signature Inspection (SDSI) is employed to monitor attack signatures. A knowledge base of over 200 attack signatures is currently distributed with ID-Trak. New attack signatures can be added in to the knowledge base in real-time.

Customized attack signatures can be added to detect unauthorized access to sensitive corporate data. Once an attack is detected, the administrator can define a set of actions to be performed ahead of time such as logging the attack, stopping the attacker session, sending an alarm and storing the complete application session for later analysis. The stored log of the attack can be used for conviction of the attacker or to define new attack signatures.

Detection of over 200 well-known Internet attacks.

Architecture Sensor

Sensor Platforms Windows NT

Target Platforms Any system on ID-Trak’s Ethernet segment employing TCP/IP

Methods of Detection Pattern-matching

Sources of Data Network packets (ID-Trak puts its NIC into promiscuous mode)

Reports ID-Trak can do session capture in the form of a text file. If, for example, a potentially malicious user telnets to a server, ID-Trak can detect that user’s login name and password and then create a text file that contains everything in the session.

ID-Trak can generate HTML or e-mail reports

Reactions Alerts:

- Internal alerting within the user interface
- Firewall-1 OPSEC messages
- SNMP traps to SNMP managers already running on the network

Responses:

- Log attack
- Terminate connection

- An administrator-defined application can be run with a command line argument

Update Method

Customers can download (or receive in e-mail) an individual attack signature that can be imported into the system and activated in real time. This does not require installing anything or restarting the system.

Customers can create their own attack signatures, such as search strings for ASCII or hex patterns at offsets or anywhere in a stream, values that can be extracted and evaluated in real time, and keywords that refer to ports, addresses, or header and payload sizes. ID-Trak provides a toolkit that allows this expansion of the list of predefined network- and data-centric signatures.

Communications

ID-Trak supports SAMP, Suspicious Activity Monitoring Protocol, in order to stop non-TCP attacks that it cannot itself reset.

ID-Trak employs Firewall-1 authentication: Firewall-1 manager exports a certificate, which is copied to ID-Trak, and each is provided the IP address of the other; the Firewall-1 OPSEC API then handles communications with ID-Trak securely.

Special Features

- Attack signatures can be added and customized in real time
- ID-Trak can make selected network servers unavailable during specified times

Internet Scanner

Vendor	Internet Security Systems (ISS)
Type of Tool	Vulnerability Scanner
Description	ISS's Internet Scanner™ … focuses on the single most important aspect of organizational network risk management – identifying and addressing technical vulnerabilities. Internet Scanner performs scheduled and selective probes of your network's communication services, operating systems, key applications, and routers in search of those vulnerabilities most often used by unscrupulous threats to probe, investigate, and attack your network. Internet Scanner then analyzes your vulnerability conditions and provides a series of corrective action, trends analysis, conditional, and configuration reports and data sets. Internet Scanner consists of three integrated modules for scanning intranets, scanning firewalls, and scanning web servers.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT 4.0 (Service Pack 3 required) IBM AIX 3.25 and higher HP-UX 9.05 and higher Sun Solaris 2.3 and higher Sun Solaris x86 2.4 and higher SunOS 4.1.3 and higher Linux 1.2x (with kernel patch) and higher
Director Platforms	NA
Target Platforms	Internet Scanner has the ability to scan any network device with an IP address. This includes routers, printers, PC's, firewalls, workstations, etc.
Methods of Detection	Pattern matching
Sources of Data	Responses to network probing
Reports	Vulnerability reports, sometimes include hot links to online vendor and patch resources
Reactions	
Update Method	Updates free to licensed customers, not automated.
Communications	NA
Special Features	User can select or customize scans to perform (called choosing or customizing a "policy")

Intruder Alert

Vendor

AXENT Technologies, Inc.

Type of Tool

System Monitor and Network Monitor with NetProwler Add-In (“Network Monitor” qualified — AXENT describes it as follows: “Intruder Alert includes Net*Prowler* technology to spot-check network traffic, which expands Intruder Alert’s monitoring capabilities to catch packet-based network attacks!” Also: “The NetProwler technology is the capability for Intruder Alert to put a Network Interface Card into “Promiscuous” mode. It is an audit-collection utility [that] can detect groups/types of network segment-based attacks, and feeds the corresponding events into readable audit logs.” [Author’s Note: I don’t understand these statements on Net*Prowler*.])

Description

Using a centralized graphical interface, you can control monitoring and responses throughout the entire network from a single management console. You can use the interface from any desktop (Windows 95, Windows NT or the most popular UNIX platforms) and can monitor combined data from devices that operate on most platforms including UNIX, NT and NetWare. You can also expand Intruder Alert’s monitoring capabilities by tying it into leading framework systems such as Tivoli, HP/OpenView and BMC.

Architecture

Agents-Director

Agent/Sensor Platforms

Windows NT
(Alpha in Spring ’98)
NetWare® 3x and 4x
UNIX

- AIX 3.2.5 & 4.X on RS/6000
- AT&T GIS (NCR) 2.3 & 3.0 on x86
- Digital UNIX/OSF1 3.0 or later on DEC Alpha-AXP
- Digital UNIX 3.2 or greater on Alpha
- HP-UX 9.05 & 10.01 or later
- HP-UX 11.0 on HP 9000/7xx & 8xx
- IRIX 5.3 & 6.2 on SGI (Indy)
- Solaris 2.4, 2.5, and 2.6 on Sun SPARC
- SunOS 4.1.3_U1 & 4.1.4 or later on Sun SPARC
- SVR4 on Motorola 88000

Director Platforms

Interface: Windows NT/95
Manager: Windows NT, NetWare 3.x-4.x, and UNIX (see Agent Platforms)

Target Platforms	Same as agent platforms
Methods of Detection	Pattern matching
Sources of Data	Audit logs from monitored systems Network packets
Reactions	Alerts: at console (Director), e-mail, pager (from STVDB) Responses: disable user’s account, stop a program from running, block access to a system (from STVDB)
Update Method	
Communications	Agents must be registered to a manager before they can be configured. Each time communications occurs between manager and agent, a password exchange and verification takes place. Every session is encoded using a special key. Intruder Alert includes uses a Diffie-Hellman key exchange, which is negotiated each time a manager contacts an agent, or an agent contacts a manager. Also, Intruder Alert uses “Blowfish,” a highly secure encryption algorithm that contains a built-in, symmetric key algorithm.
Special Features	

IP-Watcher

Vendor	En Garde Systems, Inc.
Type of Tool	Network Monitor
Description	IP-Watcher is a network monitoring tool which can be used to inspect the data being transferred between two hosts. IP-Watcher can monitor all connections on or passing through the subnet on which it is operating, allowing an administrator to display an exact copy of a session in real time, just as the user of the session sees the data. It features a simple interface which displays all the sessions it “sees” and statistics about your network. IP-Watcher can monitor any connection on a TCP port.
Architecture	Sensor
Agent/Sensor Platforms	
Director Platforms	
Methods of Detection	Packet monitoring via IP-Hijacking
Sources of Data	
Reactions	(Vendor) Responses: • Kill a connection • Send a message to the client side • Take over a connection
Update Method	
Communications	
Special Features	

IRIS (INTOUCH Remote Interactive Supervisor)

Vendor Touch Technologies, Inc.

Type of Tool Anomaly Detection Support Tool (Vendor calls it a Session Observation Tool)

Description Through viewing of network packets, IRIS can observe Telnet, RLOGIN, LAT, FTP, and URL accesses.

The IRIS tool enables the user to:

- Watch sessions in real time
- Take screen snapshots
- Record sessions for later review

Architecture Sensor

Agent/Sensor Platforms OpenVMS

Director Platforms NA

Methods of Detection NA

Sources of Data Network packets

Reactions NA

Update Method

Communications

Special Features

Kane Security Analyst for Novell

Vendor	ODS Networks, Inc.
Type of Tool	Vulnerability Scanner
Description	The Kane Security Analyst for Novell is a NetWare 3.x and 4.x NDS security assessment tool that analyzes your network for security exposures and provides detailed report cards and charts to illustrate where security can be improved. This workstation-based product compares your server against Intrusion Detection’s proprietary NetWare security methodology and delivers a set of reports and recommendations for the security weak spots it discovers. The KSA security features span six major security areas: • User Account Restrictions • Password Strength • Access Control • System Monitoring • Data Integrity • Data Confidentiality
Architecture	Sensor
Agent/Sensor Platforms	
Target Platforms	
Methods of Detection	Pattern matching
Sources of Data	System data, various
Reports	Yes, *see* Description
Update Method	
Communications	
Special Features	

Kane Security Analyst for Windows NT

Vendor	ODS Networks, Inc.
Type of Tool	Vulnerability Scanner
Description	The Kane Security Analyst for Windows NT is a network security assessment tool that analyzes a Windows NT domain, server, or workstation for security exposures and presents the results in reports. It assesses the overall security status of Windows NT networks and reports security in six areas: password strength, access control, user account restrictions, system monitoring, data integrity and data confidentiality.
Architecture	Sensor
Agent/Sensor Platforms	Microsoft Windows NT 3.51 or later
Target Platforms	
Methods of Detection	Pattern matching
Sources of Data	System data, various
Reports	Yes, *see* Description
Update Method	
Communications	
Special Features	The Kane File Rights is an interactive tool included with the KSA that allows users to investigate rights and privileges associated with various users, groups and directories.

Kane Security Monitor for Windows NT

Vendor	ODS Networks, Inc.
Type of Tool	Infraction Scanner[1]
Description	The Kane Security Monitor (KSM) is an intrusion detection system based on event log analysis for Windows NT networks. The KSM provides a centralized collection facility for event logs. An event log analysis at the centralized location forms the basis for reporting and graphing security events. The KSM can monitor thousands of workstations and hundreds of servers, 24 hours a day, 7 days a week.
Architecture	Agents-Director
Agent/Sensor Platforms	Windows NT, Workstations and Servers, Intel-based systems only
Director Platforms	Windows NT, Workstation or Server, Intel-based systems only
Target Platforms	Windows NT, Workstations and Servers
Methods of Detection	Pattern Matching
Sources of Data	Windows NT security log, applications log, and systems log
Reactions	Alerts: e-mail, pager, fax, voice mail, and forward an alert to the HP OpenView, IBM’s TMG, or Computer Associates Unicenter by delivering alarms to these management systems consoles as SMTP alerts
Update Method	
Communications	Agents are “registered” to a KSM Auditor Service as they are installed and configured. Each time communications occurs between manager and agent, a security verification process takes place.
Special Features	

[1] The vendor claims, on its web pages, that the tool is a monitor providing real-time alerts. I consider it a scanner because the detection engine examines logs from the systems it is protecting; thus, it appears that the tool is periodically scanning the historical data.

NetBoy Suite of Software

Vendor NDG Software Inc.

Type of Tool Suite of Monitors (see descriptions below)

Description The NetBoy Suite comprises EtherBoy, WebBoy, GeoBoy, and PacketBoy

WebBoy: WebBoy is a complete Internet/Intranet monitoring package. It provides statistics on standard Web traffic including URLs accessed, cache hit ratios, Internet protocols and user defined protocols.
To aid the security conscious administrator, WebBoy provides a configurable alarm mechanism to enable monitoring and notification of unusual network activity.

EtherBoy: EtherBoy gives you affordable real-time multi protocol network monitoring on your IBM compatible PC. It provides insights and answers to a large number of network management and usage questions.
Because EtherBoy is totally passive, no additional load is placed on your network resources. It is an ideal addition to your desktop based management station, or as a laptop based portable network probe.

GeoBoy: GeoBoy is a geographical tracing tool capable of tracing and displaying routes taken by traffic traversing the Internet. GeoBoy allows you to locate Internet delays and traffic congestion.
GeoBoy resolves geographical locations from a series of cache files which can be updated and customized by the user.

PacketBoy: PacketBoy is a packet analyzer/decoder package capable of decoding many of the commonly used LAN protocols. Protocols which can be decoded include TCP/IP, IPX (Novell NetWare), AppleTalk, Banyan and DECNET protocol suites. Multiple captures can be loaded and saved to disk.
To aid the security conscious administrator, PacketBoy provides a configurable capture trigger to automatically start packet capture when unusual or undesirable network activity occurs. It is an ideal addition to your desktop based management station, or as a laptop based portable network probe.

Architecture Sensor

Agent/Sensor Platforms PC (Win 95/98/NT)

Director Platforms	none
Methods of Detection	various
Sources of Data	various
Reactions	
Update Method	
Communications	
Special Features	

NetProwler

Vendor	AXENT Technologies, Inc.
Type of Tool	Network Monitor
Description	See Intruder Alert
Architecture	Add-on to Intruder Alert, Version 3.1

NetRanger

Vendor Cisco (through acquisition of WheelGroup)

Type of Tool Network Monitor

Description The NetRanger system includes two components: Sensor and Director. NetRanger Sensors, which are high-speed network "appliances," analyze the content and context of individual packets to determine if traffic is authorized. If an intrusion is detected, such as a SATAN (System Administrators Tool for Analyzing Networks) attack, a ping sweep, or if an insider sends out a document containing a proprietary code word, NetRanger sensors can detect the misuse in real-time, forward alarms to a NetRanger Director management console for geographical display, and remove the offender from the network.

NetRanger Sensor: NetRanger Sensor can monitor almost any type of TCP/IP network, including Internet connections, LAN segments, and the network side of dial-in modem pools. The Sensor contains the NetRanger real-time intrusion detection engine, which examines each individual packet, including its header and payload, as well as its relationship to adjacent and related packets in the data stream. When the Sensor detects a policy violation, it sends an alarm to the NetRanger Director console.

NetRanger Director: NetRanger Direct monitors the activity of multiple NetRanger Sensors located on local or remote network segments. It provides a geographically oriented GUI to help operators pinpoint the location of an attack.

Architecture Agents-Director

Methods of Detection Pattern matching

Analyzes the attack and reports such items as the attacking IP address, the type of attack, the destination address and port, the time and length of the attack.

Sources of Data Network packets

Reactions Alerts: pager, e-mail, reports details to a centralized management system (Director)

Responses: NetRanger can be configured to automatically shun or eliminate specific connections by changing Access Control Lists (ACLs) on Cisco routers.

Update Method

Communications NetRanger uses a UDP-based application-level communications protocol that authenticates the communication and guarantees alarm delivery.

Special Features

Automatically transfers Event and IP session logs to an archive device.
Provides stage data to a relational database for subsequent analysis.
Scalable, capable of multi-tier operation
Provides analysis to reveal potential network configuration errors.
The system’s network security database (NSDB) allows a technician instant access to specific information about the attack, hotlinks, and potential countermeasures. Because the NSDB is an HTML database, it can be personalized to a user to include operation-specific information such as response and escalation procedures for specific attacks.

NetRecon, Version 2.0

Vendor	AXENT Technologies, Inc.
Type of Tool	Vulnerability Scanner
Description	NetRecon runs on a Windows NT workstation and probes your networks and network resources. Traditionally such probes execute network vulnerability checks individually, which results in a shallow view of specific vulnerabilities and takes a long time to complete. By contrast, NetRecon's unique UltraScan™ technique allows it to immediately display vulnerabilities as they are detected and quickly perform deeper probes. This makes it easy to understand the ramifications of security problems so you know which ones are the most important. Unlike conventional network probing techniques, UltraScan™ is not just IP-based, but exploits multiple protocols and methods to detect vulnerable network resources. Such a capability is essential since most networks contain sensitive resources that can be accessed in non-IP ways, like NetWare.
Architecture	Sensor
Agent/Sensor Platforms	Intel-based PC, Windows NT 4.0
Director Platforms	NA
Target Platforms	Network devices: servers, workstations, routers, webservers, and firewalls NetRecon runs on Windows NT, but can probe virtually any kind of network system or device. This includes UNIX servers, Windows NT servers, NetWare networks, Windows 95 and 3.x workstations, mid-range systems, mainframes, routers, gateways, webservers, firewalls, name servers, and many more.
Methods of Detection	Various common probes to find ways to break into the network Uses multiple network protocols, not just IP, to find network resources (e.g., NetWare)
Sources of Data	Responses from probed systems
Reports	Graphically displays progress and results in real-time Produces network vulnerability report—HTML report and expert advise on fixing vulnerabilities
Reactions	None
Update Method	Soon (reference date: 12/9/1998) you will be able to download the latest NetRecon Tune-up Pack, which includes the latest NetRecon probe modules.

Communications	NA
Special Features	

NetSonar

Vendor

Cisco Systems

Type of Tool

Vulnerability Scanner
Network Mapper

Description

NetSonar automates the process of auditing a network's security posture through its comprehensive vulnerability scanning and network mapping capabilities.

NetSonar is a network measurement and analysis tool. With it, you can perform these tasks:

- Scan your network to compile an electronic inventory of systems and services.
- Probe for and confirm network vulnerabilities using rules. You can also add your own rules to probe for vulnerability conditions that you define.
- Manage the results of your scans and probes.
- View and organize scan and probe results in a browser.
- Generate charts and reports based on the results of your scans and probes.

Network mapping compiles a detailed electronic inventory of network resources—includes device, device type, operating system, and operating system version.

Using a network security database, NetSonar identifies vulnerabilities in the following categories:

- Network TCP/IP hosts
- UNIX hosts
- Windows NT hosts
- Web servers
- Mail servers
- FTP servers
- Firewalls
- Routers
- Switches

Architecture

Sensor

Agent/Sensor Platforms

Pentium (166 MHz minimum) with Solaris x86 V.2.5x or V.2.6
Sun SPARC Solaris with V.2.5x or V.2.6

Director Platforms

Methods of Detection

Pattern matching ("rules")
Network probing (e.g., ping)

Sources of Data	Results of probes
Reactions	Produces reports
Update Method	
Communications	
Special Features	(Vendor’s User’s Guide) NetSonar has four main components: a Graphical User Interface , a Network Mapping Tool , a Vulnerability Assessment Engine , and a Report Wizard . Additionally, NetSonar provides the Network Security Database (NSDB), an HTML database that explains the nature and meaning of vulnerabilities NetSonar detects.
Notes	Requires Java on sensor platform: JRE 1.1.5 provided; JDK™ 1.1.5 supported

Network Flight Recorder, Version 2.0.2 (Commercial)

Vendor Network Flight Recorder, Inc.

Type of Tool Anomaly Detection Support Tool

Release Date 1999 (commercial version)

Description NFR watches traffic on its network and records what the user has told it to record. The NFR system is intended to run on a workstation or PC with a hard disk sized appropriately for the amount of data the user expects to gather and retain. NFR can, for example, maintain statistics about Web surfing activity through a firewall, or records about who logged into a mainframe, when, and for how long. NFR stores the data and lets the user browse it, automatically archives or purges it, and keeps it secure against alteration.

Access to the NFR's data store uses a Web browser that supports Java and Secure Sockets Layer. NFR is end-user programmable. Included with it are a number of recording packages that gather basic statistics, watch firewalls, and track user activity. If a user has a specific requirement to watch something, the NFR can be programmed, through a graphical interface, using NFR's internal programming language to implement that requirement.

Architecture Sensor

Agent/Sensor Platforms BSD/OS 3.x on Intel
FreeBSD 2.2.x on Intel
HP-UX 10.20 on PA RISC
OpenBSD 2.3 on Intel
RedHat Linux 4.x on Intel
RedHat Linux 5.x on Intel
Slackware Linux 3.x on Intel
Solaris 2.5 on SPARC
Solaris 2.5.1 on SPARC

Interface Platforms The Graphical User Interface can be run on the sensor platform or on a different machine on the network that meets these requirements

- screen resolution of at least 800 x 600
- supports one of the following web browsers
  - Microsoft Internet Explorer 3.02 or higher
  - Netscape Communicator 4.0 or higher
  - Netscape Navigator 3.01 or higher

Target Platforms NA

Methods of Detection NA; however, user can add own code to incorporate intrusion detection functionality. Also, on March 1, 1999, NFR, Inc. announced a new partnership with L0pht Heavy Industries, Inc.. L0pht will be writing filters for NFR to provide anomaly detection functionality; these filters, NFR, Inc. said, will be provided to users on a regular monthly basis, beginning early in the second quarter of 1999.

Sources of Data Network packets (on Ethernet, Fast Ethernet, or FDDI network)

Reports

Reactions

Update Method

Communications

Special Features

NOSadmin for Windows NT, Version 6.1

Vendor	BindView Development Corporation
Release Date	Version 6.1 announced in June 1999
Type of Tool	Vulnerability Scanner (Vendor calls it a “query engine”.)
Description	NOSadmin checks on more than 600 areas of risk to Windows NT security and allows you to easily perform the detailed analysis to pinpoint security holes and why they exist. NOSadmin comes with over 500 reports that automatically identify risks to the security and integrity of your enterprise, including storage analysis, server integrity, and security holes. NOSadmin for Windows NT has a new technology called Active Extensions which allows you to quickly close security holes, enforce standards, and implement security policies across the enterprise.
Architecture	Director
Director Platforms	Windows NT
Target Platforms	Windows NT servers within an NT domain
Methods of Detection	Pattern matching
Sources of Data	Registry entries, permission settings, configuration parameters, and so forth
Reports	Security analysis reports; over 500 prepackaged reports included
Reactions	ActiveAdmin feature provides user a way to fix problems: Vendor’s Datasheet states “Active Extensions bring BindView’s award winning ActiveAdmin functionality to Windows NT management. ActiveAdmin allows you to close security holes and enforce standards and security policies across the enterprise, without leaving the BindView console.”
Update Method	
Communications	
Special Features	Query capability: NOSadmin provides a query-based interface for building custom queries for issues specific to a network. Scalability: Multiple query engines can work together in a domain.

POLYCENTER Security Compliance Managers

Vendor	COMPAQ, DIGITAL Products and Services
Type of Tool	Security Compliance Scanner
Description	(Vendor – paraphrased) The POLYCENTER Security CMs for a variety of platforms are software tools that a security or system manager uses to establish a custom security analysis and reporting system to manage the security of a network of distributed systems. With these tools, the security manager can implement and maintain a security standard for the nodes in a distributed computing environment that is consistent with corporate security policy. Security managers define tests to examine the settings of operating system parameters that are relevant to the security of the system. These tests ensure that the operating system parameters comply with the organization's security policy. Using POLYCENTER Security CM's menu interface, these tests are grouped into inspectors, which are run regularly to test for compliance with the security policy. Compliance Managers are available for AIX, HP-UX, SunOS, ULTRIX, Solaris 2, Digital UNIX, NetWare, and OpenVMS nodes.
Architecture	Agent
Methods of Detection	Check system parameters against preset values
Sources of Data	Predefined policy
Reactions	E-mail reports to predefined distribution lists Create scripts that set parameters to match policy
Update Method	
Communications	
Special Features	Can generate special reports to POLYCENTER SRF, an ADR Director

POLYCENTER Security Intrusion Detector for Digital UNIX, Version 1.2A

Vendor COMPAQ, DIGITAL Products and Services

Type of Tool System Monitor

Description POLYCENTER[TM] Security Intrusion Detector for Digital UNIX[R] (POLYCENTER Security ID) is a real-time security monitoring application for the Digital UNIX operating system. It performs knowledge-based analysis of the output of the audit subsystem to recognize and respond to security-relevant activity. Violations such as attempted logins, unauthorized access to files, illegal setuid programs, and unauthorized audit modifications are automatically detected and acted upon. This frees the system or security manager to tackle more important end-user problems.

Most security breaches involve a series of actions. Instead of looking at each action individually, POLYCENTER Security ID looks at the whole picture. Using a case method modeled after criminal investigations, POLYCENTER Security ID assigns an agent to monitor the suspect and file evidence to the case. By analyzing each security event within the context of a case, POLYCENTER Security ID can distinguish between real threats and innocent behavior and, therefore, POLYCENTER Security ID will not kick legitimate users off the system or trigger false alarms.

Security ID can be configured to take countermeasures against intruders without human intervention. Security managers can work from the Manager’s Graphical User Interface or from the Digital UNIX command line.

Architecture Sensor

Methods of Detection Pattern matching

Sources of Data Audit subsystem

Reactions (STVDB)

Alerts: e-mail

Responses: automatic countermeasures include resetting event auditing if it was modified, re-enabling of audit data generation, and shutting down an offending process

Update Method

Communications

Special Features

POLYCENTER Security Intrusion Detector for OpenVMS VAX and OpenVMS Alpha, Version 1.2a

Vendor COMPAQ, DIGITAL Products and Services

Type of Tool System Monitor

Description POLYCENTER [TM] Security Intrusion Detector (ID) for OpenVMS [TM] (formerly DECinspect[TM] Intrusion Detector) is a security tool that constantly monitors suspicious or hostile activity and reports any such activity to the security manager.

POLYCENTER Security ID operates in real time, processing audit events from the OpenVMS Audit Server as they occur and notifying the security manager via electronic mail. Furthermore, POLYCENTER Security ID can be configured to take countermeasures against intruders without human intervention.

Security managers can use this version of POLYCENTER Security ID from the DCL command line. If they are running OpenVMS VAX[TM] Version 5.3 or higher but less than Version 6.0, security managers can also use this version of POLYCENTER Security ID from within the POLYCENTER Security Compliance Manager for OpenVMS menu system.

http://www.digital.com/info/SP4127/

Architecture

Methods of Detection

Sources of Data

Reactions

Update Method

Communications

Special Features

POLYCENTER Security Reporting Facility (SRF)

Vendor COMPAQ, DIGITAL Products and Services

Type of Tool ADR Director

Description POLYCENTER SRF software is designed to run on one or more nodes to support the centralized collection and management of compliance information from POLYCENTER Security CM installations, which can include AIX[R], HP[R]-UX, SunOS[R], ULTRIX[TM], Solaris 2, Digital UNIX[R], NetWare[R], and OpenVMS[TM] systems. It provides centralized management for distributed POLYCENTER Security CM client nodes. POLYCENTER SRF extracts data from tokens sent by nodes running POLYCENTER Security CM and maintains this data in a relational database for management reporting. POLYCENTER SRF can provide management reports for networks of AIX, HP-UX, SunOS, ULTRIX, Solaris 2, Digital UNIX, NetWare, and OpenVMS nodes.

Architecture Director

Methods of Detection

Sources of Data

Reactions

Update Method

Communications

Special Features

PréCis 3.0

Vendor

Litton PRC

Type of Tool

System Monitor
(Audit Management Toolkit)

Description

PréCis provides a robust, host based audit management and misuse detection toolkit. Audit agents on each monitored workstation process audit logs and create alerts based on security relevant events. Alerts are pushed to the PréCis Monitor Tool in near real time, and are correlated with other security events at the manager level through the use of our Security Indications and Warning (SI&W) technology. SI&W provides a "network" view of anomalous behavior employing a technique that uses statistics in combination with rules.

PréCis maintains the original "native" audits from each monitored workstation which are transferred to the manager in off-peak times. Native audits are maintained for potential use in criminal prosecution.

PréCis agents also reduce and consolidate native audit events into a standard audit format. These "normalized" audits are stored in a relational data base at the PréCis manager to facilitate review and reporting what has transpired on your network.

The Version 3.0 server provides a new Configuration Tool that allows the user to reconfigure agents from a central location.

Architecture

Agents-Director

Agents are system monitors (audit review and collection). PréCis agents are installed on network nodes where audit source files are produced. Their primary role is to perform timely preprocessing of native ("raw") audits, so that near real-time information can be derived. Their secondary role is to move audits efficiently to a central location for analysis and archiving.

Director is a suite of tools, such as PréCis Monitor Tool, residing on the server portion of the architecture.

Agent/Sensor Platforms

HP-UX
Windows NT
Sun Solaris
SCO CMW+

Director Platforms
HP-UX
Sun Solaris

Methods of Detection
Pattern matching (Agents and Director)
Statistical deviation detection (Director)

Sources of Data
Audit data in monitored systems

Reactions
Alerts: generated by both Agents and Manager, displayed by Manager

Agents produce first-level alerts based on recognition of single events or a combination of events (e.g., a use of privilege command)

The Notification Services component of the Manager has a configurable rule-based capability to analyze the incoming audit stream and recognize unusual behavior patterns or site specific security policy violations not discernible by agents.

Update Method
Users can create rules to match their own site security policies or employ PRC to implement their policy. In addition, PRC provides and maintains a default set of “indicators” which will be expanded as necessary and provided under our standard maintenance agreement. These indicators are not templates of activity representing specific attack profiles.

Communications
The agent manager interface provides authentication for connections and non-repudiation support for data transfers.

Special Features
The PréCis Audit API library is intended for use by any application wishing to generate audits directly into an agent, rather than write them to a file. This API library can be used by an application resident on the same node as an agent or it can be used by a remote application to pass audits to an agent on another node, where they can be further processed.

Notes
In an e-mail from Doug Allpress, PréCis Product Manager, 11/30/98, he stated that “…recently, PréCis was selected by the U.S. Air Force for their Theater Battle Management Core Systems (TBMCS) program. PréCis provides audit management and intrusion detection for TBMCS.”

ProxyStalker 1.0

Vendor	Network Associates, Inc., Trusted Information Systems Division
Type of Tool	System Monitor
Description	ProxyStalker 1.0 is currently the only intrusion detection system providing real-time monitoring and configuration checking for NT systems running the Microsoft Proxy Server. Developed in cooperation with Microsoft, ProxyStalker's security monitoring can detect security breaches by insiders or outsiders by comparing logs of system activities against its database of potential types of misuse. When tampering occurs, ProxyStalker can respond by ending the session, terminating the user's privileges, and even repairing illicit changes. In addition, alarms are sent via e-mail or to a report detailing the identity of the violator, as well as when, where and how the violation occurred.
Architecture	Sensor
Agent/Sensor Platforms	Microsoft Windows NT Server v4 with Service Pack #3 installed NTFS running Microsoft Proxy Server v2.x
Director Platforms	NA
Methods of Detection	Pattern matching
Sources of Data	System logs
Reactions	Alerts: send SNMP traps, report to administrators via e-mail Responses: restart critical processes, repair configuration changes made illegally, kill offending processes and logins, disable and shun user account logins
Update Method	
Communications	
Special Features	Using a wizard GUI, ProxyStalker asks a few simple policy questions then installs and runs constantly in the background

RealSecure™ 3.1

Vendor	Internet Security Systems (ISS)
Type of Tool	Network Monitor (RealSecure Engines) Infraction Scanner (RealSecure Agents)
Release Date	1999
Date of Entry	December 1999

Description

RealSecure™ is an integrated network- and host-based intrusion detection and response system. It enables administrators to

- Automatically monitor network traffic and host logs
- Detect and respond to suspicious activity
- Intercept and respond to internal or external host and network abuse

The components of the RealSecure 3.1 family are:

- RealSecure Network Engine. This is the RealSecure engine that looks at all the traffic on a single segment.
- RealSecure System Agent. The system agent is a detection module that monitors the operating system log files for signs of unauthorized activity. Like the network engine, it can take action automatically to prevent further system incursions.
- RealSecure Management Console. The console provides the capability to manage network engines and system agents from the same user interface. Both types of detectors use the same alarm formats, report to the same database, and use many of the same reports. This module is bundled at no charge with the network engine and the system agent.
- RealSecure Manager for HP OpenView. This is a plug-in module for existing HP OpenView systems that allows such systems to manage RealSecure network engines securely. (Management of system agents is not officially supported in this release.)

The detector components—Network Engine and System agent—and the OpenView plug-in are all licensed separately.

The RealSecure Network Engine captures all packets from a local network segment and examines each of them for signs of network abuse, malicious intent, or suspicious activity. Users can customize the system by defining connection events, fine-tune existing signatures, establish traffic masking filters, and specify a response for every network event.

Each RealSecure System Agent installs on a workstation or host, examining that system's logs for tell-tale patterns of network misuse and breaches of security. Like the RealSecure Network Engine, RealSecure

System Agent sends an alarm to the RealSecure Management Console or third party network management console when it detects evidence of improper usage. Based on what is discovers, RealSecure System Agent also automatically reconfigures RealSecure Network Engine and select firewalls to prevent future incursions.

The RealSecure Management Console provides three basic services:
1) Real-time alarm display — RealSecure Management Consoles provide a single view of threat activity across an enterprise network. The consoles sort alarm data from all active engines by user-defined criteria and provide extensive on-line assistance for each detected event.
2) Data management — RealSecure Management Consoles collect databases from active engines into a single data store which can be exported to an enterprise database system. RealSecure's built-in reporting system generates reports from this collected database, including pre-defined reports designed to support staff ranging from technical network managers to high-level executives. RealSecure supports custom and user-generated reports, all launched from the RealSecure user interface.
3) Engine configuration — The RealSecure Management Console adjusts the configuration of every engine in an enterprise network with the push of a button. RealSecure's grid-based configuration tool allows administrators to specify which signatures are active, what response should be taken for every event, which user-defined connection events should generate alarms, and how incoming traffic should be masked for optimal use by an incident response team.

Architecture
Agents-Director
- Agents are the RealSecure Network Engine and the RealSecure Agent
- Director is the RealSecure Management Console or the RealSecure Manager for HP OpenView

Agent/Sensor Platforms
RealSecure Engine runs on a dedicated workstation:
- Windows NT 4.0 with Service Pack 4 or higher, on a Pentium II 300 MHz or better
- Solaris SPARC 2.5.1 and 2.6
- Solaris x86 2.5.1 and 2.6
- Linux

RealSecure Agent: Windows NT 4.0 with Service Pack 4 or higher, on a Pentium II class machine

Director Platforms
RealSecure Management Console: Windows NT 4.0 with Service Pack 4 or higher, on a Pentium II 200 MHz or better

RealSecure Manager for HP OpenView: HP OpenView versions B.05.01 (Sun Solaris 2.5.1 or 2.6) or B.05.02 (Windows NT 4.0 with SP3)

Network Topologies

RealSecure operates on

- Ethernet networks (10 Mbps)
- Fast Ethernet networks (100Base-T only, 100 Mbps),
- FDDI (100 Mbps)
- Token Ring networks (4 Mbps to 16 Mbps)

Target Platforms

RealSecure filters and monitors any TCP/IP protocol and interprets many network services including web surfing, e-mail, file transfer, remote login, Chat, and Talk.

RealSecure also monitors and decodes Microsoft CIFS/SAMBA traffic for Windows networking environments.

Methods of Detection

Pattern matching

Sources of Data

Network packets (Engines)
System logs (Agents)

Reports

Engines and Agents send reports of detected anomalies to RealSecure Manager

Reactions

- Email an administrator
- Terminate an attack automatically
- Reconfigure a Check Point Firewall-1 to reject traffic from the attacking source address or notify a Lucent Managed Firewall Security Management Server (SMS)
- Send an alarm to the management console indicating that the event occurred
- SNMP trap for an off-the-shelf management platform
- Log the event, including date, time, source, destination, description, and data associated with the event
- View the session or record for later playback
- Execute a user-specified program

Update Method

Updates are posted on the ISS web site (http://www.iss.net) and users are notified of new software via e-mail.

Communications

Engines to Managers communications in version 2.0 use a secure channel for passing messages between engine and console. This channel guarantees:

- Reliability — Delivery is guaranteed with no retry logic required by the caller, subject to the availability of the communications path.
- Privacy — Data is securely encrypted to prevent unauthorized disclosure.
- Integrity — Data cannot be modified in, added to, or deleted from the

	data stream without the receiving entity detecting the corruption and aborting the session. • Authentication — Each end of the connection is sure that it knows uniquely who the peer is, and that there is no party in the middle proxying the data stream. Option: The Network Engine can use a second network interface card connected to a secure network for out-of-band communications with the management console.
Special Features	Operates over any adapter card capable of supporting promiscuous mode Provides capability for the user to create signatures for the network engines using regular expression string matching

Retriever™ 1.5

Vendor Symantec

Type of Tool ADR Director (vendor calls it a Network Security Management Tool)

Release Date 1999

Date of This Entry February 18, 2000

Description Retriever provides capabilities to preserve the availability of network services and to protect the reliability and confidentiality of critical information. Retriever automatically discovers network components, unobtrusively identifies vulnerabilities, provides safeguard and policy recommendations, and performs customizable network audits. Thus, Retriever helps develop a baseline security level for implementing best-practice security policies that can be monitored and enforced as frequently as desired without interfering with network performance. Specifically, Retriever

- Discovers and maps the network, creating an inventory of systems, services and network components
- Identifies vulnerabilities and establishes a network security baseline
- Recommends safeguards
- Audits the network, verifying that vulnerabilities are secured
- Runs scheduled network scans and provides visual alerts to any changes on the network, to help enforce security policy
- Enables predictive (“what if”) network modeling off-line to reduce security risk prior to integration

Architecture Director

Director Platforms Windows 95/98
Windows NT 4.0 (SP3)

Network Topologies TCP/IP networks

Target Platforms

Sources of Data

Reports Retriever can produce about 16 different reports on network and vulnerability discovery and recommended safeguards.

Update Method The vulnerability and safeguard databases, as well as the scan and audit engines, are updated approximately six times per year. These updates can either be downloaded from the L-3 website or obtained on CD.

Special Features Retriever’s modem discovery capability uses an inputted list of phone numbers to search for modem tones to allow identification of unauthorized modems.

Retriever lists all known vulnerabilities that may apply in the discovered network without running hacking scripts, performs a non-intrusive network audit, and uses the results to establish a network security baseline.

L-3 Network Security plans to make Retriever CVE-compatible[2] by the end of first quarter 2000. The CVE numbers would appear in the vulnerability reports produced by Retriever and would have hyperlinks to the CVE website.

Source of Information http://www.L-3Security.com/products/retriever/#features on February 7, 2000.

[2] The Common Vulnerabilities and Exposures (CVE) database lists publicly-known security problems and assigns a unique identifier to each problem. The security problems are of the type that potentially can be exploited by network crackers.

SAFEsuite Decisions 1.0

Vendor	Internet Security Systems (ISS)
Type of Tool	ADR Director (Vendor) Decision Support System (DSS)
Description	SAFEsuite® Decisions is a security decision support application. It collects and integrates security information derived from multiple sources and locations including Check Point FireWall-1™, Network Associates' Gauntlet Firewall™, ISS' RealSecure™ intrusion detection and response system, and ISS' Internet Scanner™ and System Scanner™ vulnerability detection systems. SAFEsuite Decisions automatically correlates and analyzes this cross-product data to indicate the security risk profile of the entire enterprise network. For example, vulnerabilities found by Internet Scanner and intrusion events detected by RealSecure will be correlated to provide high value information indicating specific hosts on the network that are both vulnerable to attack and that have been attacked. Built on SAFELink, ISS' automated data collection and report distribution technology for multiple sources and destinations, SAFEsuite Decisions provides comprehensive scheduled report execution, enabling ongoing overviews of changing security conditions.
Architecture	Director (this tool only) Agents-Director is the overall architecture for deployed system (see Concept of Operation below)
Director Platforms	Windows NT 4.0 with SP3 (multiple platforms may be required; see latest vendor information)
Concept of Operation	SAFEsuite Decisions distributes security information to users, based on analysis of security data available from a variety of sources deployed throughout a network infrastructure. 1) Data collection—Data is securely moved from the local data store (log files, local databases, etc.) of security products (vulnerability assessment, intrusion detection, and firewall products) into a central, enterprise database. This data collection step includes several sub-steps: data extraction from the source system, secure transfer of the data over the network, and the insertion of the data into the central database. 2) Data analysis—Once the data is available in a central database,

	analysis of the data can be performed, providing consolidation[3] and correlation[4] of the data. The analysis identifies security status and trends that could not easily be discerned without the use of the centralized data repository. 3) Information Distribution—Once useful security status information and trends have been determined, information is made available to users who can employ it to have a positive impact on the security posture of the enterprise.
Methods of Detection	Various, depending on agents employed
Sources of Data	Various, including ISS's Internet Scanner, ISS's Security Scanner, ISS's RealSecure, Check Point FireWall-1™, and Network Associates' Gauntlet Firewall™
Reactions	Provides reports, push or pull
Update Method	
Communications	Employs SAFELink for transmission of security information from the agents
Special Features	
Note	According to the vendor, this information is preliminary, as of December 7, 1998.

[3] For example, when intrusion event data is consolidated from many RealSecure engines deployed throughout the enterprise network, consolidated analysis can be performed. This indicates which hosts are most frequently attacked, when most attacks are being launched, and what attacks are most frequently used.

[4] For example, vulnerability data is correlated with intrusion events to indicate those hosts or groups of hosts that are both vulnerable to a specific attack and have been attacked.

SecureNet PRO, Version 3.0

Vendor MimeStar, Inc.

Type of Tool Network Monitor

Release Date 1997

Last Update May 25, 2000

Description Overview: SecureNet PRO is an enterprise-scalable network monitoring and intrusion detection system. It captures, analyzes, and reconstructs all TCP/IP activity on a network in real-time. It is capable of monitoring, analyzing, or logging any network transmission for purposes of user activity logging and attack detection.

Architecture Sensor

Platforms MimeStar announced on April 24, 2000 that SecureNet PRO is available for the Linux operating system, on (recommended) 400 MHz Pentium.

Methods of Detection Pattern matching; over 290 included attack signatures for detecting exploitation attempts; state-based application level protocol decoding of major network protocols (including HTTP, FTP, Finger, SMTP, Rlogin, TFTP, POP3, NNTP, RPC, NetBIOS, SMB, and others)

Sources of Data Network packets

Reports A custom report generation engine allows one to create detailed reports of network activity in both text and HTML format. Reports can be sorted, grouped, and filtered according to specified report generation criteria.

Reactions

- TCP Session Termination allows any TCP network data stream to be terminated
- Real-time logging of TCP session content or individual data packets
- E-mail notification of detected network attacks

Update Method

Communications All communications between SecureNet PRO software components are encrypted using industry-grade encryption methods. (128 bit Blowfish, 56 bit DES, and Triple DES encryption); all transmissions between SecureNet PRO components are also validated using the industry-standard MD5 (Message-digest 5) algorithm

Special Features Multiple network intrusion detection engines may be centrally managed from a remote graphical administrative console. A single intrusion detection engine may be simultaneously managed by multiple remote administrative consoles, allowing multiple administrators to monitor the security of a network concurrently.

Security Configuration Manager for Windows NT 4

Vendor	Microsoft Corporation
Type of Tool	Security Compliance Scanner
Description	(from Windows NT Server White Paper, Nov 1998, downloadable from Microsoft web site) Microsoft Security Configuration Manager is a Microsoft Management Console (MMC) snap-in tool designed to reduce costs associated with security configuration and analysis of the Windows NT operating system. The Security Configuration Manager allows you to configure security for a Windows NT-based system, and then perform periodic analysis of the system to ensure that the configuration remains intact. The Security Configuration Manager supports two modes of security analysis for Windows NT-based systems: configured system analysis and unconfigured system analysis. • Configured system analysis refers to situations where the system has already been configured using a security configuration file prior to performing the analysis. In this case, the baseline configuration has already been imported into a database and an analysis can be performed against that same database. This type of analysis can be used to answer the question: What security relevant system parameters have changed since the last time this machine was configured? • Unconfigured system analysis refers to situations where the system has not been configured with the baseline configuration. This type of analysis can be used to answer questions such as, How do current system settings compare with this baseline configuration? What system settings would change if I were to apply this configuration? In this case, the baseline security configuration file is imported into a database prior to performing the analysis. If you later want to configure the system with the baseline configuration, the created database can be used. In both cases, the end result is a database that contains both configuration information as well as analysis results.
Architecture	Sensor
Agent/Sensor Platforms	Windows NT 4
Director Platforms	NA
Target Platforms	NA
Methods of Detection	Pattern matching
Sources of Data	Policy database

Reports	The tool reports differences between actual configuration and described configuration settings in database
Reactions	NA
Update Method	
Communications	NA
Special Features	

SeNTry – Enterprise Event Manager (Replaced by "One Point Solution: Windows NT Security" sometime in 1999)

Vendor	Mission Critical Software (http://www.missioncritical.com/eem/eem.htm)
Type of Tool	System Monitor
Description	SeNTry EEM collects information from many NT sources, including log entries, application events, and SNMP traps, applies filters to exclude events the user considers unimportant, and forwards the important events to a central collection point. SeNTry EEM issues alerts for critical conditions that the user defines, classifies each event, and stores the information in a central ODBC-compliant database for future analysis and reporting.
Architecture	Agents-Director
Methods of Detection	Pattern-matching
Sources of Data	NT event logs
Reactions	SeNTry Monitor module displays status of targets and a global status indicator SeNTry Alert Gatherer Service (SAGS) module sends e-mail alerts via its Mail Application Program Interface (MAPI) System can be configured to set off SNMP traps with management via an SNMP management utility
Update Method	
Communications	Agent to director via named pipes, data in the clear
Special Features	

SessionWall-3, Version 4.0

Vendor	PLATINUM technology, inc.
Type of Tool	Network Monitor
Release Date	February 9, 1999
Description	SessionWall-3 Release 3 (V1R3) is designed to be used as a standalone or complementary product. It includes a world-class intrusion detection and service denial attack detection engine, an extensive URL control list of more than 200,000 categorized sites, a world-class Java/ActiveX malicious applet detection engine as well as a virus detection engine. It complements all popular "firewalls" to extend application-specific protection, provide intrusion detection, and audit the current settings. SessionWall-3 also interfaces with FireWall-1 using the OPSEC interface. SessionWall-3 provides the surveillance, intelligence, controls, and interfaces required to protect a company's networks from both external and internal intrusion and abuses. SessionWall-3 achieves these capabilities by a combination of very sophisticated network surveillance, scanning, blocking, detection, response, logging, alerting and reporting capabilities into an easy to use integrated package.
Architecture	Sensor
Sensor Platforms	Windows 95/98 Windows NT 4.0/5
Network Topologies	Ethernet Token Ring FDDI
Methods of Detection	Pattern matching (Vendor refers to "rules": "These rules specify the patterns, protocols, addresses, domains, URLs, content, etc. and the actions to be taken should these be encountered.")
Sources of Data	Network packets
Reactions	Alerts: • Audible tone • E-mail • Page • Fax • Log entry Responses: • Send SNMP trap to NMS • Execute custom DLL or command

Update Method For attack database: download from website

Communications

Special Features New rules can easily be added or the existing rules can be changed using menu driven options. All network activity that is not associated with a rule is identified for statistical and real-time analysis, often identifying the need for additional rules.

SFProtect - Enterprise Edition

Vendor	Hewlett Packard
Release Date	August 1999
Type of Tool	Vulnerability Scanner Security Compliance Scanner
Description	SFProtect is a vulnerability analysis tool for the NT operating system and the major applications that run on that system (i.e., web and database servers). SFProtect includes IntelliFix technology to close security holes discovered by the analysis. [http://literature.hp.com:80/litweb/pdf/5968-7019E.pdf]
Architecture	Agents-Director
Agent/Sensor Platforms	Windows NT
Director Platforms	Windows 95, 98, or NT
Network Topologies	TCP/IP Network
Target Platforms	Windows NT
Methods of Detection	Pattern matching
Sources of Data	Data values on target platform
Reports	HTML-based reports of analysis
Reactions	SFProtect can perform regularly scheduled audits with e-mail notification if problems are found
Update Method	unknown
Communications	unknown
Special Features	IntelliFix technology (see Description above)

SilentRunner

Vendor Raytheon Systems Company

Release Date Unknown

Entry Date September 28, 1999

Type of Tool The author was unable to determine the type of tool from the product literature available at the time of this entry. The vendor calls the tool a *Discovery, Visualization, and Analysis System*

Description This tool appears to be a network discovery tool that can provide graphical depictions of the network and its activity. In addition, it appears to be able to incorporate data from other sensors as input to its analysis engine.

See the vendor description at URL:
http://www.raytheon.com/rsc/c3/cpr/cpr_021/cpr21.htm
(working on date of entry)

Comment The author was unable to provide the usual tool information for this tool at the time of this entry. Identification of this tool has been included in this compendium because the author believes it may be able to process and display anomaly data.

SMART Watch

Vendor WetStone Technologies, Inc.

Type of Tool System Monitor (System Integrity Checker)

Release Date June 8, 1998

Date of This Entry February 21, 2000

Description SMART Watch actively monitors a Windows computer system, detecting changes to watched resources and reporting via e-mail or pager to the system administrator. SMART Watch uses self contained, silent operation, “waking up” when a change in the file system is detected. Thus, it does not depend, as do some other techniques, on polling or integration into the system’s scheduler. Operating system level changes tell SMART Watch when to verify if a resource is still intact. If a resource has changed or been deleted, SMART Watch can respond within milliseconds. In the case of a file modification or deletion, SMART Watch can restore the content of the affected file immediately.

SMART Watch uses cryptographic signatures to determine when the content of a resource has changed. It can be configured to use either MD5 or SHA-1 hash algorithms. SMART Watch also uses encryption to securely store resource information, thereby preventing malicious changes to signatures. This privacy mechanism also prevents unauthorized users from determining what resources are being watched.

Architecture Sensor

Agent/Sensor Platforms Windows 95, 98, NT (4.x and 5.x)

Methods of Detection Changes in watched resources.

Reactions Alerts by e-mail or pager.

Source of Information http://www.wetstonetech.com/products.htm

Stake Out™ I.D.

Vendor	Harris Communications
Type of Tool	Network Monitor
Description	Stake Out is an intelligent agent designed to monitor TCP/IP based network for suspicious behavior. It detects system probes and attacks including SATAN, “Ping O’ Death”, TCP SYN flooding, and other prevalent exploitations of operating system vulnerabilities in real time. Stake Out™ is available in two versions: Stake Out™ Workstation and Stake Out™ Enterprise. Stake Out™ Workstation • Stand-alone system which can monitor traffic on a network segment and includes Motif-based interface for configuration and alert display • For small networks with few segments or for remote sites where response to an intrusion alert must be coordinated with staff local to the attacked system Stake Out™ Enterprise • For companies with large wide-area networks • Security plug-in for network management systems • Incident response teams can rely on immediate intrusion alerts • Powerful graphical interface allows Help Desk monitoring of network security • As an attack progresses to its target, each agent in its path will log and announce the activity in real time.
Architecture	Sensor
Agent/Sensor Platforms	
Director Platforms	
Methods of Detection	Pattern matching
Sources of Data	Network packets
Reactions	Alerts: paging and/or e-mailing system administrators (Enterprise version) Responses: Output to any SNMP compliant network management system (such as Harris Network Management, Sun NetManager, HP OpenView, etc.)
Update Method	

Communications	Uses encrypted inter-process communication

Stalker, Version 2.1

Vendor Network Associates, Inc., Trusted Information Systems Division

Type of Tool System Monitor

Description Stalker provides the highest level of intrusion detection for both Windows NT and UNIX systems. Because Stalker runs at the system level, it can terminate unauthorized actions immediately and notify the network manager by email, pager or phone.

By comparing system audit logs against TIS' patented database of potential types of misuse, Stalker can detect security breaches made by insiders or outsiders. When tampering occurs, alarms are sent via email or to a printed report file detailing the identity of the violator, as well as when, where, and how the violation occurred.

Stalker can be configured to run 24 hours a day in an automated, unattended mode, and is capable of managing multiple and differently configured servers from a single management station.

Stalker has three main functions:

MISUSE DETECTOR With Stalker's Misuse Detector, all intruders, whether insiders or outsiders, can be immediately pinpointed. This unique, patented technology identifies many system attacks, exploitations, and vulnerabilities, with new misuses added as discovered.

TRACER/BROWSER Stalker's Tracer/Browser ensures the complete investigation of security events via audit trails, extracting the trail of events as needed. Automatic reports can be generated on a regular basis to monitor for policy violations, and ad-hoc queries can be performed to aid investigation or policy enforcement.

AUDITING Stalker provides ongoing monitoring and management of audit trail data within the environment—and even enables a continuous audit of an entire network. Stalker's audit controls and storage manager configure and manage all auditing, allowing an administrator to choose the events to record and place in long-term storage for later use if needed.

Architecture Sensors-Director

Agent/Sensor Platforms Sun Solaris 2.4, 2.5, and 3.6, and Sun OS 4.1.3 with BSM
IBM AIX 4.1.4, 4.2, and 4.3, and AIX 3.2.5

	HP UX 10.20 and HP UX 9.05 SCO UnixWare 2.1
Director Platforms	Sun Solaris 2.4, 2.5, and 3.6 IBM AIX 4.1.4, 4.2, and 4.3 HP UX 10.20
Target Platforms	See sensor platforms
Methods of Detection	Pattern matching
Sources of Data	Audit trails
Reactions	Alerts: e-mail, pager, phone Responses: terminate process
Update Method	
Communications	
Special Features	

System Scanner 1.0

Vendor	Internet Security Systems
Type of Tool	Vulnerability Scanner Infraction Scanner
Description	System Scanner™ enables system administrators to take control of their security practice by proactively seeking out internal system vulnerabilities. A comprehensive host based security assessment and intrusion detection tool, System Scanner identifies and reports exploitable system weaknesses. System Scanner assesses file permissions and ownership, network services, account setups, program authenticity, operating system configuration and common user-related security weaknesses such as guessable passwords to determine the current security level and to identify previous system compromises.
Architecture	Agents-Director
Agent/Sensor Platforms	*See* Target Platforms
Director Platforms	<not specified at vendor's web site; probably same platforms as for agents>
Target Platforms	Servers running AIX, HPUX, IRIX, Linux, Solaris, SunOS, or Windows NT Server Desktop systems running Windows 95, 98, or NT Workstation
Methods of Detection	Pattern matching (uses vulnerability database)
Sources of Data	System data
Reports	Report of scan identifies relative severity, suggested fixes, and vendor resources for patches and updates; reports can be sent to Central Console
Reactions	NA
Update Method	Updates free to licensed customers, not automated.
Communications	<not specified at vendor's web site>
Special Features	

T-sight™

Vendor En Garde Systems, Inc.

Type of Tool Analyzer and Responder
(vendor) Intrusion Investigation and Response Tool

Release Date 2000

Date of This Entry April 28, 2000

Description T-sight is designed to work as a supplement to an intrusion detection system. T-sight enables the user to take control of a suspicious connection once an alarm has been set off (either T-sight's alarm or/and an IDS alarm). T-sight alarms can be configured for certain types of activities; these are defined by the user and not by a database—the usual method for automated intrusion detection products.

T-sight also allows the user to examine active connections and transactions in real-time. It provides capability to review connections and transactions, and offers reporting and graphing features.

Architecture Sensor

Agent/Sensor Platforms Windows NT
Windows 2000

Network Topologies TCP/IP

Methods of Detection T-sight monitors a variety of protocols, the data for which is interpreted by Handlers. Version 1.0 ships with Handlers for

- Telnet
- DNS
- Rlogin
- Rsh
- FTP
- HTTP
- SMTP
- Finger

These Handlers define a number of transactions for each protocol and specify alarms defined by the user. A Handler works by reviewing packet data and reporting transactions as well as any alarms triggered to T-sight.

Sources of Data Network packets

Reports Graphical charts can be generated over specific time slices of the packet data. Types of charts include alarms triggered, protocols used by machine, services used by host, and hosts listed by transaction.

Reactions Alerts: message to the user
Responses: takeover or terminate a connection

Communications

Special Features

Notes

Source of Information

Section 3

Government Off-the-Shelf Products

The following products are described in this section:

Automated Security Incident Measurement (ASIM)

Joint Intrusion Detection System (JIDS)

Network Intrusion Detector (NID)

Network Security Monitor (NSM)

Automated Security Incident Measurement (ASIM), 2.0

Provider Air Force Information Warfare Center (AFIWC/AFCERT)

Type of Tool Infraction Scanner (in batch mode)
Network Monitor (in real-time mode)

Description (from NSA Database) Automated Security Incident Measurement. Monitors network traffic and collects information on targeted unit networks by detecting unauthorized network activity. The ASIM real-time alarming capability is implemented using a pop-up window under the X Window System. ASIM can also detect one Network Layer activity: SATAN scans.

(from CyberStrike Roadmap: Part 2) The ASIM software consists of a suite of Borne shell scripts, configuration files, and compiled C-code programs. The C-code programs constitute the engine which captures, filters, and analyzes Ethernet and FDDI[5] packets. The effect is to monitor and analyze TCP/IP[6] traffic for suspicious activity. ASIM Version 2.0 can operate in batch or real-time modes. In batch mode, it collects traffic for a 24-hour period, then analyzes it for suspicious activity. Detected probable incidents can be viewed at the site where the engine is located or the data can be transmitted, DES[7]-encrypted, to AFCERT for analysis. In real-time mode ASIM identifies strings and services that could indicate attempts at unauthorized access and immediately creates an audio alert or spawns an alert process created by the user.

(ASIM User’s Guide) ASIM Version 2.0 runs on a Sun Sparc5 workstation under Solaris 2.5.1 (preferred operating system), Solaris 2.5, or Solaris 2.6, or on an IBM-compatible PC under Linux V2.0. In either case, a dedicated workstation is required, located at the boundary of the security domain(s) to be protected. A security domain is defined as an IP domain (e.g., the domain 132.47).

ASIM software components include compiled C code (executable) programs used to capture data, Borne shell scripts used to analyze captured data, configuration files used to define what data will be captured, and log files which contain the captured data.

[5] Fiber Distributed Data Interface

[6] Transport Control Protocol/Internet Protocol

[7] Data Encryption Standard

	The ASIM Central software consists of c-code (received transmissions and populate database) and Java GUI for operator access to database.
Architecture	Agents-Director
Agent/Sensor Platforms	Sun Sparc5 workstation under Solaris 2.5.1 (preferred operating system), Solaris 2.5, or Solaris 2.6, or IBM-compatible PC under Linux V2.0. In either case, a dedicated workstation is required, located at the boundary of the security domain(s) to be protected.
Director Platforms	Sparc 5000 running Solaris 2.6, with Oracle database (referred to as ASIM Central)
Target Platforms	Platforms in security domain of sensor
Methods of Detection	Pattern matching
Sources of Data	Network packets
Reports	In real-time mode: real-time alert reports sent from agent to ASIM Central (AFCERT) (up-channeled every 10 minutes)
Reactions	Alerts: e-mail, on-screen
Update Method	
Communications	DES-encrypted transmission of logs from ASIM software to ASIM Central (at AFCERT)
Special Features	

Joint Intrusion Detection System (JIDS), Version 2.0.3

Provider	DISA Information Assurance Support Environment (IASE)
Type of Tool	Network Monitor
Description	(Provider) JIDS version 2.0.3 offers a security manager a suite of tools that help detect, analyze, and gather evidence of intrusive behavior occurring on an Ethernet or Fiber Distributed Data Interface (FDDI) network using the Internet Protocol (IP).
Architecture	Sensor
Agent/Sensor Platforms	SunOS 4.3.1 Solaris 2.5.1 and 2.6 HP-UX 10.10 (including TAC-4) RedHat Linux 4.2
Methods of Detection	Pattern matching
Sources of Data	Network packets
Reports	
Reactions	Alerts: real-time alerts
Update Method	
Communications	
Special Features	Intrusive behavior can be detected and analyzed with JIDS using any one of the three operating models: retrospective intrusion analysis, real-time intrusion detection, and statistics gathering. Retrospective Analysis analyzes previously collected traffic for evidence of intrusive behavior. Real-time Detection processes live data and signals the presence of possible intrusive activity Statistics Gathering collects either packet headers for statistical analysis, collects statistics on who is speaking to whom, or collects statistics on which hosts are providing what services

Network Intrusion Detector (NID), Version 2.1

Provider Lawrence Livermore National Laboratory

Type of Tool Network Monitor

Description (from Provider) NID is a suite of software tools that help detect, analyze, and gather evidence of intrusive behavior on Ethernet and FDDI networks using the Internet Protocol (IP). NID is hosted on a single, network-connected Unix workstation. It collects packets or statistics that cross a user-defined security domain. NID provides detection and analysis of intrusions from individuals not authorized to use a particular computer, and from individuals allowed to use a particular computer but who perform either unauthorized activities or activities of a suspicious nature on it. NID uses attack signature recognition, anomaly detection, and a vulnerability risk model. NID is available for use by all authorized

- Department of Energy offices, national laboratories & facilities
- Department of Energy Contractors who directly support DOE
- U.S. Government civilian agencies

NID was formerly known as the Network Security Monitor (NSM) and was originally developed at the University of California at Davis.

The DoD version of NID (called JIDS) is available to DoD entities and DoD contractors at the DISA INFOSEC Tools Distribution site

Architecture Sensor

Agent/Sensor Platforms HP-UX 10.10
Solaris 2.5.1 and 2.6
SunOS 4.1.3
Red Hat Linux 5.1

Methods of Detection Pattern matching

Sources of Data Network packets

Reports

Reactions Alerts: real-time alerts

Update Method

Communications NID provides an interface for secure communications

Special Features NID has three common operating models:

1 Retrospective intrusion analysis: analyze previously collected traffic for evidence of intrusive behavior

2 Real-time intrusion detection: process live data and signal the presence of possible intrusive activity

3 Statistics gathering: generate statistics based on packet headers, connections, or services

Network Security Monitor (NSM)

Type of Tool Network Monitor

Description Network Security Monitor no longer exists as a discrete tool/system. According to the ASIM User's Guide:

"ASIM evolved from a program called Network Security Monitor (NSM), which was originally designed and built by the cooperative efforts of the Lawrence Livermore National Laboratory and the University of California (Davis Campus) for the U.S. Air Force Cryptologic Support Center and the U.S. Department of Energy. The original design document, if one exists, is not presently available to the current development team, which is tasked with providing enhancements and improvements to the usability, functionality, and reliability of NSM (now ASIM), as well as providing for real-time monitoring capabilities for the program. Through study and analysis of the existing source code and functional testing, it is apparent that NSM was originally designed to be a batch process utilizing a compilation of software tools available at the time. Since then, new tools and features have been added at various times. New script files have been written, and previous ones modified as fitted each individual user's needs. This evolutionary growth process continues to this day.

The current design of ASIM is such that C programs (also known as executables) (except for ASIMwatch, which is a Java language program), Bourne shell scripts (also known as scripts), and files (such as configuration files, log files, and transcript files) work together to provide the functionality and flexibility that the ASIM tools provide."

Section 4

Research and Development

This section has information on the following projects:

- Air Force Enterprise Defense (AFED)
- Automated Intrusion Detection Environment (AIDE) Advanced Concept Technology Demonstration (ACTD)
- Autonomous Agents for Intrusion Detection (AAFID)
- Common Intrusion Detection Director System (CIDDS)
- Common Intrusion Detection Framework (CIDF)
- DARPA Intrusion Detection Evaluation
- Distributed Intrusion Detection System (DIDS)
- Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD)
- Extensible Prototype for Information Command and Control ($EPIC^2$)
- Graph-based Intrusion Detection System (GrIDS)
- Lighthouse
- Next-Generation Intrusion Detection Expert System (NIDES)
- Outpost
- Projects at Air Force Research Laboratory, Rome Location
- Spitfire

Air Force Enterprise Defense

Researcher Air Force Research Laboratory (AFRL), Rome Location

Type of Tool ADR Director

Date of Information 1/3/2000

Description Air Force Enterprise Defense (AFED) is an outgrowth of the EPIC^2 project. AFRL, in cooperation with Air Combat Command (ACC) and other Air Force MAJCOMS, has defined the goal of AFED to be to move EPIC^2 concepts closer to operational use. AFRL is developing a prototype system, using concepts and lessons learned from EPIC^2, which it will deliver to ACC, AMC, AFSPACECOM, and others, for operational testing. The first increment is expected to be delivered near the end of January 2000.

Initially, AFED will consist of UNIX-based database servers and PC-based analysts’ workstations for visualization with lightweight clients. The servers incorporate an Oracle database, which will serve a function similar to its role in EPIC^2. It accepts “raw” inputs from a variety of sensors. A second Oracle database, hosted on an NT server, provides warehousing for “cooked” data—inputs into the first Oracle database that have been refined by some processing.

Sensors send their outputs directly to the main server. Access to those outputs and the “cooked” data on the secondary server occurs through triggers, scheduled events, or directed queries from analysts’ workstations.

Architecture Agents-Director

Features Current planning calls for incorporation of the following categories of EPIC2 functionality:

- Intrusion Detection—both network- and host-based
- Change Management / Policy Enforcement
- Vulnerability Assessment
- Mission Readiness / Situational Assessment
- Common Enterprise Picture (IA + Network Management)
- Visualization

The planned sensors are

- NetRadar
- ASIM
- AXENT ITA and ESM
- Internet Security Scanner
- Sidewinder

Additional Commentary

The AFED PMO has been working with CITS NMS/BIP to develop the spiral transition process to turn AFED over to ESC in FY02.

The expected relationship of AFED to Outpost is that Outpost will provide a major feed of host-based sensed data to AFED. Although there are points of similarity between the two, AFED would be expected to operate on a larger scale than Outpost, with heterogeneous sensors feeding into an echeloned hierarchy.

Automated Intrusion Detection Environment (AIDE) Advanced Concept Technology Demonstration (ACTD)

Researcher STRATCOM is the Operations Manager, AFRL is the Execution Manager, and DISA is the overall Program Manager for this ACTD

Type of Tool ADR Director

Architecture Agents-Director

Note The current implementation of the objective tool is EPIC^{2}. See the description of EPIC2 for information about the current properties of the objective tool.

Description This 5-year technology demonstration program focuses on the detect and react portions of the defensive information operations model. The goal is to integrate data from network management and information protection systems in order to provide automated integrated tactical warning and attack assessment. To achieve the goal, the program has set three objectives:

- Create an architecture for the sharing, integration, analysis and warning of IW attacks
- Incorporate current and maturing intrusion sensing tools in conjunction with expert systems technology for the management of distributed systems
- Correlate intrusion events at local agency, CINC, and Joint command levels to tighten the detection grid and increase the success of identifying IW threats

Additional Commentary News article *Strategic Command testing cyberwarfare 'early warning system'* by Navy Journalist 1st Class Michael J. Meridith, United States Strategic Command Public Affairs

OFFUTT AIR FORCE BASE, Neb. (AFPN) February, 1999-- U.S. Strategic Command is preparing to test a next-generation intrusion detection system that could provide early warnings of cyberattacks against the Department of Defense.

The test is part of an $11 million Advanced Concept Technology Demonstration which speeds up the normal acquisition process by allowing warfighters to test prototype technologies.

The first phase of this five-year ACTD, which was tested in September, involved bringing together information from intrusion detection sensors at several different sites during a mock cyberattack. This provided information operations personnel a more complete view of the scope of the cyberattack than was previously available, making defensive planning that much easier.

"This year, we want the system to help analyze that data," explained David Ellis, a senior member of USSTRATCOM's ACTD team. "It will put the pieces together and advise the user of their relative significance. In essence, the system will put everything in one place and tell us if there's a systematic series of attacks."

After this summer's demonstration, the ACTD will undergo an intense development process to prepare it for it's final test in 2000. That demonstration will put into place an automatic reporting mechanism that will pass information about cyberattacks among the 27 participating sites, providing a consolidated defense against cyberattacks.

Ellis said that if this ACTD proves itself, it will become an essential component in DOD's information defense arsenal.

"We need the ability to detect an attack as soon as it occurs," he explained. "And we need to be able to quickly determine the scope of it. Our information systems are so globally interconnected that it's easier for a potential adversary to launch a cyberattack rather than by other conventional methods."

April 26, 2000: The following information was provided by Dwayne Allain, in an e-mail, dated April 25, 2000. to the Infosec e-mailing list, in response to a query about the use of the CVE (Common Vulnerabilities and Exposures: see footnote 2) database in government projects:

"The AIDE ACTD at AFRL Rome is attempting to normalize sensor signatures with CVE signatures in the AIDE database and to report CVE information as part of the AIDE interface. Additionally they are providing a link to the CVE website via the AIDE web browser for those events that are detected by the deployed sensors.

Autonomous Agents for Intrusion Detection (AAFID)

Researcher	AAFID Group, COAST Laboratory, Purdue University
Type of Tool	This project is experimenting with a distributed architecture, within which various types of autonomous agents can be accommodated
Description	This project is investigating the utility of a distributed architecture that uses small, independent entities, called Agents, to detect anomalies. The architecture is expected to have advantages such as scalability, efficiency, fault-tolerance, and configurability. The project builds systems that use the architecture and measures their performance and detection capabilities. A complete specification of the AAFID architecture is given in the reference (next item). The first prototype of a system that uses the architecture, called AAFID2, has been released to the public.
Architecture	Agents-Director
Agent/Sensor Platforms	Systems that can run Perl 5 code
Director Platforms	UNIX systems Windows NT is planned
Target Platforms	Systems that can host Agents
Methods of Detection	Various, depending on functionality of Agent
Sources of Data	Various, depending on functionality of Agent
Reports	
Reactions	
Update Method	
Communications	
Special Features	Development of the system uses the object-oriented programming features of Perl5, which makes code reuse easy. The infrastructure of AAFID2 (see Description below) includes most of the facilities needed for developing new entities—monitors, transceivers, or agents. AAFID2 also includes semi-automatic code-generation tools for developing agents.
Reference	Balasubramaniyan, J., J. O. Garcia-Fernandez, E. H. Spafford, and D. Zamboni, 1998, *An Architecture for Intrusion Detection using Autonomous Agents*, COAST TR 98-05, Department of Computer Sciences, Purdue University.

Common Intrusion Detection Director System (CIDDS)

Researcher Air Force Information Warfare Center (AFIWC), /EA

Type of Tool Anomaly Detection and Reaction Director

Date of Information 12/20/1999

Description The heart of the CIDDS is a software program using an Oracle relational database to assimilate data from each of the CITS NMS/BIP tools to realize hierarchical implementation of AF intrusion detection. CIDDS provides the following capabilities:

- Collection of data from computer security products
- Mass storage of data from computer security products
- Capability to design and launch queries on the stored product data to correlate data received from selected combinations of sensors or all sensors
- Features(e.g. whois, nslookup, and analyst notepad) to assist analysis of network data received from computer security products
- Secure communications with child CIDDS and, where appropriate, computer security products
- Maintain configuration information on child CIDDS and, where appropriate, computer security products
- Mechanism for reporting both up and down the enterprise-wide intrusion detection hierarchy
- GUI to provide a computer security products analyst with an efficient, easy -to-learn interface to fully use the CIDDS capabilities

CIDDS will intelligently integrate data from ASIM and the CITS NMS/BIP sensors:

- Sidewinder firewall
- AXENT ITA
- AXENT ESM
- Cisco Router information

Architecture Sensors-Director

Agent/Sensor Platforms See descriptions of the sensors listed above: AXENT ITA and AXENT ESM are described in this compendium; Sidewinder and Cisco information can be found on the world-wide web.

Reference AFIWC, May 20, 1999, *Air Force Intrusion Detection: ASIM/CIDD,* unnumbered PowerPoint presentation, Air Force Information Warfare Center (AFIWC)/EA, San Antonio, Texas.

Comment As of November 22, 1999, CIDDS had apparently successfully been installed at ACC, AMC, and AFSPACE under a pilot program.

Common Intrusion Detection Framework (CIDF)

Researcher Consortium

Type Effort to develop standards

Description (Project) The Common Intrusion Detection Framework (CIDF) is an effort to develop protocols and application programming interfaces so that Intrusion Detection products can interoperate and components of them can be reused in other systems.

This effort was initiated by Teresa Lunt while she was at DARPA/ITO (the Information Technology Office of the Defense Advanced Research Projects Agency). It began as part of the Information Survivability program with a focus on allowing DARPA projects to work together. It has since broadened significantly with participation from a number of companies and organizations. Most contributors are from the U.S., but there is also international participation.

Stuart Staniford-Chen (stanifor@cs.ucdavis.edu) and Brian Tung (brian@isi.edu) are the coordinators of the CIDF effort.

DARPA Intrusion Detection Evaluation

Researcher	MIT Lincoln Laboratory, Information Systems Technology Group
Type of Tool	Testing and evaluation standards
Project's Description	The Information Systems Technology Group of MIT Lincoln Laboratory, under Defense Advanced Research Projects Agency (DARPA) Information Technology Office and Air Force Research Laboratory (AFRL/SNHS) sponsorship, is collecting and distributing the first standard corpus for evaluation of computer network intrusion detection systems. We are also coordinating, with the Air Force Research Laboratory, the first formal, repeatable, and statistically-significant evaluation of intrusion detection systems. This evaluation will measure probability of detection and probability of false-alarm for each system under test. These evaluations will contribute significantly to the intrusion detection research field by providing direction for research efforts and an objective calibration of the current technical state-of-the-art. They are intended to be of interest to all researchers working on the general problem of workstation and network intrusion detection. The evaluation is designed to be simple, to focus on core technology issues, and to encourage the wide participation. We have tried to eliminate security and privacy concerns, and we are providing data types that are used commonly by the majority of intrusion detection systems. Data for this first evaluation will be made available in the spring and summer of 1998. The evaluation itself will occur in the fall. A follow-up meeting for evaluation participants and other interested parties will be held in December to discuss research findings. Participation in the evaluation is solicited for all sites that find the task and the evaluation of interest. There are two parts to the intrusion detection evaluation. The first part is an off-line evaluation. Network traffic and audit logs collected on a simulation network will serve as input to intrusion detection systems under test. These systems will process data in batch mode, trying to find the attack sessions in the midst of normal activity. The second part of the evaluation is conducted in real-time. Systems will be delivered to AFRL and inserted into their network test-bed. Again, the job of the detection system is to find the attack sessions in the midst of normal background activity. Some systems may be tested in off-line mode, some in real-time mode, and some in both modes.

Additional information available at:
http://www.ll.mit.edu/IST/ideval/index.html

Distributed Intrusion Detection System (DIDS)

Researcher
University of California, Davis

Type of Tool
Infraction Scanner (host manager—see Description below)
Network Monitor (LAN manager—*see* Description below)

Description
(from COAST) This intrusion detection system aggregates audit reports from a collection of hosts on a single network.
DIDS extends the network intrusion-detection concept from the local area network environment to arbitrarily wider areas, with the network topology being arbitrary as well. The generalized distributed environment is heterogeneous, i.e. the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers. The architecture for DIDS consists of the following components: a host manager (a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager, placed at a single secure location, that receives reports from various host and LAN managers and processes these reports, correlates them, and detects intrusions.

Architecture
Agents-Director

Agent/Sensor Platforms
Claims to be able to deal with heterogeneous systems; no current information is available about which systems or LANs agents have been written for.
As of 1991 (*see* Reference below) the host manager was implemented for Sun SPARCstations running SunOS 4.0.x with the Sun C2 security package and the LAN manager was a subset of UC Davis' Network Security Monitor.

Director Platforms
Not specified; 1991 paper (*see* Reference below) indicates it is an expert system written in Prolog

Target Platforms
As for agent/sensor platforms

Methods of Detection
Pattern matching

Sources of Data
Audit logs for hosts
Network packets for LANs

Reports
Apparently (*see* Reference below), the expert system (Director) provides a report on the security state of the monitored system.

Communications
(Reference) "High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of

CMIP management tools as they become useful. The architecture also provides for bi-directional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors."

Special Features DIDS correlates reports from both host and network monitoring using an expert system.
(COAST) Unique to DIDS is its ability to track a user as he establishes connections across the network, some perhaps under different account names.

Reference Snapp, S. R. et alia, 1991, "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture and An Early Prototype", *Proceedings of the 14th National Computer Security Conference*, pages 167-176, October 1991.

Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD)

Researcher	SRI International / Computer Science Laboratory
Type of Tool	Unclear from web-pages description, but apparently uses both statistical deviation detection and pattern matching

Description

(from Project) SRI Project 1494, Contract Number F30602-96-C-0294, DARPA ITO Order No. E302, 28 August 1996 through 27 August 1999. Phillip Porras and Peter Neumann are leading a project to develop EMERALD, a distributed scalable tool suite for tracking malicious activity through and across large networks. EMERALD introduces a highly distributed, building-block approach to network surveillance, attack isolation, and automated response. The approach is novel in its use of highly distributed, independently tunable, surveillance and response monitors that are deployable polymorphically (sic) at various abstract layers in a large network. These monitors demonstrate a streamlined intrusion-detection design that combines signature analysis with statistical profiling to provide localized real-time protection of the most widely used network services on the Internet. Equally important, EMERALD introduces a framework for coordinating the dissemination of analyses from the distributed monitors to provide a global detection and response capability to counter attacks occurring across an entire network enterprise. Also, EMERALD introduces a versatile application-programmers' interface that enhances its ability to integrate with the target hosts and provides a high degree of interoperability with third-party tool suites.

EMERALD is a successor system to NIDES that considerably extends the NIDES concept to accommodate network-based analyses and to dramatically increase interoperability and ease of integration into distributed computing environments. This effort includes extending components for profile-based analysis, signature-based analysis, and localized results fusion with automated response capability. In addition, we are considerably extending our results analysis capability to facilitate hierarchical interpretations of our distributed monitoring units, which will enable cross-platform analysis at various layers of abstraction, and successive refinement of the resulting analyses within increasingly broader scopes. We are also developing an accompanying set of exportable API that will permit interoperability between EMERALD components and network monitoring facilities.

Architecture Appears to be some sort of distributed-agent architecture; unclear from web-pages description

Methods of Detection Perhaps pattern matching and statistical deviation detection; unclear from web-pages description

Special Features (Project) EMERALD provides a hierarchically composable analysis scheme, whereby local analyses are shared and correlated at higher layers of abstraction.

Note In response to a question about availability, Phil Porras sent the author the following information on November 25, 1998:

"Plans for EMERALD's general release are still being formed. There has been no discussion of making it Government off-the-shelf. At some point, hopefully by this summer or sooner, we will begin to release free (and unsupported) versions of EMERALD on the Internet (possibly with some registration restrictions). There are certain funding agencies who have access to our software and who we do support, but we try to keep that list small to minimize the impact to our research efforts."

Extensible Prototype for Information Command and Control (EPIC^2)

Researcher Air Force Research Laboratory, Rome Location

Type of Tool ADR Director

Description (from Project) The Extensible Prototype for Information Command and Control (EPIC^2) provides a framework for interoperability, integration, and coordination of intrusion control tools. It gives the user a powerful capability for detection and discovery of information security problems, assessment of vulnerabilities, and visualization of the information protection situation. EPIC^2 normally carries out these operations automatically. It gives the user a powerful capability to control and integrate the output from a variety of systems.

Functional goals for EPIC^2 are:

- Integrate, coordinate, and visualize
  - Network topology
  - Network management
  - Vulnerability information
  - Intrusion events
- Provide intrusion control capability to
  - Analyze intrusion events
  - Locate and defensively counter sources of attack
  - Assess impact of attack and extent of damage
  - Recover from attack
  - Report attack, damage, and actions taken

Architecture Agents-Director

Agent/Sensor Platforms Various: potentially any system that can use at least one of three bridging methods to communicate with the Director

Director Platforms Sparc Ultra I, running Solaris 2.5.1

Target Platforms Various: depends on agents employed

Methods of Detection Various: depends on agents employed

Sources of Data Various: depends on agents employed

Reports Various: reports can be scheduled, operator-initiated, or Director-initiated

Reactions Various: depends on agents employed and policy established in EPIC^2 Director

Special Features

Bridging allows interfacing to a wide variety of agents. Three bridging methods are possible (embedded, wrapped, and proxied coding) so that most systems can be interfaced to the EPIC^2 Director.

Graph-based Intrusion Detection System (GrIDS)

Researcher University of California, Davis

Type of Tool Analyzer

Description (Project, 1997) GrIDS is designed to detect large-scale automated attacks on networked systems. The mechanism that we propose is to build activity graphs which approximately represent the causal structure of large scale distributed activities.

The nodes of an activity graph correspond to hosts in a system, while edges in the graph correspond to network activity between those hosts. Activity in a monitored network causes graphs representing that activity to be built. These graphs are then compared against known patterns of intrusive or hostile activities, and if they look similar a warning (or perhaps a reaction) is generated.

The GrIDS project is part of UC Davis's Intrusion Detection for Large Networks project, which is funded by ARPA.

Methods of Detection Activity Graphs

Sources of Data (Project Design Document, 1997)

- Host-based IDS with some appropriate interface
- TCP wrappers to give host-reports of connections
- Network sniffers along the lines of NSM or NID to give network reports of connections and to provide non-TCP connection coverage

Reactions Alerts

Lighthouse

Researchers The MITRE Corporation, Software Engineering Institute of Carnegie Mellon University, Lincoln Laboratories; sponsored by U.S. Air Force.

Type of Research Intrusion Detection Technology

Date of Information January 19, 2000

Description This Air Force Information Assurance (IA) program includes both research and prototyping. As the research produces usable operational concepts, prototypes are developed and integrated into the functional and operational infrastructure, initially in a laboratory environment and subsequently in operational testbeds. The infrastructure for the current laboratory environment is provided by Outpost.

Selected research topics are directed toward satisfying Air Force IA requirements as documented in publications produced by IA TPIPT, CITS NMS/BIP, CI MAP, and such. CSAP21 and EPIC2 provide guidance for functional integration of prototyped capabilities. The integrated prototypical capabilities are intended to fit within the IP operational architecture developed by AFCA/AFCIC (the IP Working Group).

In addition to the development of prototypes to operate on the Outpost infrastructure, which is the bulk of the project, the project is addressing testing strategies and the state of the practice. *See* the SEI report, reference below.

Period of Performance Started in FY99, continuing in FY00.

References Allen, J., A. Christie, W. Fifthen, J. McHugh, J. Pickel, E. Stoner, December 1999, *State of the Practice of Intrusion Detection Technologies*, Technical Report CMU/SEI-99-TR-028, ESC-99-028, Carnegie Mellon, Software Engineering Institute, Pittsburgh, Pennsylvania.

Next-Generation Intrusion Detection Expert System (NIDES)

Researcher SRI International / Computer Science Laboratory

Type of Tool System monitor
(Project) NIDES can also operate in batch mode, for periodic batch analysis of audit data.

Description (Project) NIDES is a comprehensive intrusion-detection system that performs real-time monitoring of user activity on multiple target systems connected via Ethernet. NIDES runs on its own workstation (the NIDES host) and analyzes audit data collected from various interconnected systems, searching for activity that may indicate unusual and/or malicious user behavior. Analysis is performed using two complementary detection units: a rule-based signature analysis subsystem and a statistical profile-based anomaly-detection subsystem. The NIDES rule-base employs expert rules to characterize known intrusive activity represented in activity logs, and raises alarms as matches are identified between the observed activity logs and the rule encodings. The statistical subsystem maintains historical profiles of usage per user and raises an alarm when observed activity departs from established patterns of usage for an individual. The alarms generated by the two analysis units are screened by a resolver component, which filters and displays warnings as necessary through the NIDES host X-window interface.

Architecture Sensors-Director

Agent/Sensor Platforms

Director Platforms SunOS, 4.1.3 or Solaris 1.1, with X-Window interface

Target Platforms SunOS, 4.1.3 or Solaris 1.1
Non-Sun hosts can be made targets by using the audit data customization facility provided with the NIDES release. To monitor non-Sun targets in real-time, the host must support TCP/IP and have a connection to the NIDES host to support data transfer.

Methods of Detection Pattern matching
Statistical deviation detection

Sources of Data Audit data

Reactions Alerts: e-mail and (Project) PopUp Messages (?)

Outpost

Researcher The MITRE Corporation

Type of Tool Intrusion Detection Infrastructure

Date of Information January 19, 2000

Description Outpost is an infrastructure on which sensors, analyzers, reporters, directors, and so forth can interoperate to provide situation awareness, reaction, remediation, and reconstitution capabilities, and decision support.

The infrastructure consists of an Oracle database, host-based agents written in Java, an open API, and a central control station. From the control station—the Outpost server—probes are downloaded to the host-based agents, which run the probes and report the results. Probes can be written in Java, but more typically would be written in C or C++ to enable them to access the level of data needed. Probes are written in accord with the open API. The Outpost agent deletes the probe after it has run. Probes can be scheduled by an administrator to ensure an adequate refresh rate of the data stored in the Oracle database—the repository for all reports from the probes.

Since probes are written in Java, a degree of platform independence has been achieved for the infrastructure. The use of XML for sending probe results to the Outpost server also contributes to openness and interoperability.

Outpost generally will operate on any network up to WAN size for the current implementation. Scaling to larger networks should be possible by cascading servers.

Architecture Agents-Director

Communications The Outpost server communicates with probes using HTTP over SSL.

Special Features Downloaded executables are signed using PK technology so that the Outpost probes can authenticate them as legitimate downloads from the Outpost server.

Additional Commentary Outpost provides the infrastructure for the Lighthouse project.

Projects at Air Force Research Laboratory (AFRL), Rome Location

Researcher	AFRL
Types of Projects	Various projects related to anomaly detection and reaction
Date of Information	January 2000

Description

AFRL at any given time has numerous efforts underway to explore new approaches and new technologies. During fiscal year 1999, the following projects were underway, many expected to continue well into fiscal year 2000. The projects listed here, arranged by area, are individually described in Appendix 3.

- Intrusion Detection
  - Process Control Approach to Indication and Warning Attack on Computer Networks
  - ATM Sentinel Intrusion Detection
  - Detection of Data Corruption Attacks in Information Warfare Environment
  - Database Security
  - A New Integrated Approach to Intrusion Prevention, Detection, and Response
  - Data Classification and Data Clustering Algorithms for Intrusion Detection in Computer Networks
  - Distributed Agent Information Warfare Framework
- Damage Assessment and Recovery
  - Damage Assessment, Data Recovery and Forensics
  - Demonstrating Information Resiliency
  - Trusted Recovery from Information Attacks
  - Automated Resource Recovery Agent
- Forensic Analysis
  - Damage Assessment, Data Recovery and Forensics
  - OMNI SLEUTH – Computer Forensics System
  - Synthesizing Information from Forensic Investigation
- Analysis and Decision Support
  - Interactive Information Protection Decision Support Systems (IIPDSS) ATD
  - Extensible Prototype for Information Command and Control (EPIC2)
- Anomaly Detection Support Tools
  - Audit Workbench

Spitfire

Researcher MITRE

Type of Tool Intrusion Alert Manager

Description Spitfire integrates intrusion event capture, display, and analysis for the defensive IW operator. Using a relational database, operators can analyze incident data in real time or retrospectively. Spitfire was originally built to handle the event stream from the NetRanger suite of intrusion detection and monitoring equipment. It has since been expanded to allow independent or complementary input from the RealSecure network monitor.

Spitfire allows client users to selectively display incidents and to run queries on the incident data stored in the database and on vulnerability and tools information databases provided with the system.

Architecture Director, implemented in client/server architecture:

- Client: GUI providing access to data stored on server
- Server: Provides access to Oracle database that stores the intrusion alerts and vulnerability and tool information

Agent/Sensor Platforms NA

Director Platforms Client: Windows 95 Windows NT 4.0
Server: PC or UNIX

Target Platforms NA

Methods of Detection NA

Sources of Data Incident alerts provided by sensor systems; for example, NetRanger and RealSecure alerts

Reports Various, results of queries on database

Reactions NA

Update Method NA

Communications Client-server communications employ SQLnet.

Special Features Provides access to vulnerabilities and tools database via intrinsic help screens

Notes The Spitfire prototype is available to Government sponsors, but is not supported conventionally.

List of References

1. LaPadula, L. J., March 1999, *Compendium of Anomaly Detection and Reaction Tools and Projects*, MP 99B0000018, The MITRE Corporation, Bedford, Massachusetts.

2. Hurwitz Group, Inc., March 1998, *Information Security: Assessing Risks and Detecting Intrusions*, White Paper viewable at http://www.summitonline.com/security/papers/hurwitz3.html on November 2, 1998.

Appendix A

What We Mean by Anomaly Detection and Reaction

One can fashion protection against cyber-intruders within a spectrum of techniques. At one end of the spectrum is the method of detecting intruders. In this method, one uses intrusion detection tools to watch what is going on in the network to discover suspicious events. If perfect intrusion detection and reaction systems were available, there might be no need for any other measures to protect against cyberattack. At the other end of the spectrum is the method of ensuring that all the components of the network, including firewalls, routers, servers, and workstations, are equipped to fully repel any attack. In this method, one does not try to detect intrusive connections coming from outside one's network since they can do no harm. In theory, even a denial of service attack can be thwarted in this way because the components of the data communications infrastructure would be smart enough not to carry the traffic that would cause the denial of service. Of course, it is a good question to ask how to make the components so smart. In practice, neither end of this spectrum will provide the best protection for investment made. In practice, one needs to be prudent. One should properly set up and configure the components of one's network using current best practices and one should provide state of the art intrusion detection.

Doing these things is not a one-time chore. Network topologies tend to be dynamic. Often it is difficult to control the comings and goings of hosts on a network, especially in large networks. The job of properly setting up and configuring components often requires skilled personnel, who are in short supply. In addition, new cyberattacks may demand new protections or responses.

Prudent, affordable, continuous protection of one's network involves monitoring the network for anomalies of various kinds, whether they are suspicious textual strings in a network packet or undesirable values for important keys in NT registries. Moreover, it involves correcting detected anomalies, whether that means terminating a connection or reconfiguring a server.

We call an automated system that performs or assists in such tasks an anomaly detection and reaction (ADR) system. Besides checking network packets for suspicious strings, or monitoring a user's behavior looking for deviations from an established pattern, the ADR system checks components of the network for errors of omission, misconfigured applications, and errors in system parameters. When the ADR system finds an anomaly, it reacts, generally by trying to fix the anomaly. Its response may be restricted to issuing an alert for certain anomalies. For others, it may be able to fully correct the problem. In some cases, it may be able to provide ancillary information that will assist an administrator in correcting the anomaly. What it can do will be determined by the state of the art, the budget, and the information operation to be protected.

Besides budgetary considerations, the extent of the protection domain determines the needed capacity of the ADR system for that domain. Moreover, networks tend to grow, thereby extending the scope of interest for an ADR system. Thus, scalable ADR systems are needed, not only so that the same basic system can serve domains of different size, but also so that the same ADR system can accommodate significant growth in the domain it protects.

Appendix B

Product and Project Description Attributes

Automated tools are described using the attributes described in the next table. In the tool descriptions, the acronym "NA" is used for an attribute that is "not applicable" for a particular tool.

Table B-1. Explanation of Tool Attributes

Attribute	Explanation
Name of Product	Self-explanatory.
Vendor	For GOTS, this category is called "Provider".
Type of Tool	We recognize the following types of tools (listed alphabetically): • Analyzer: An analyzer receives inputs from a variety of sources (e.g., intrusion detectors, vulnerability scanners, and so forth), possibly from widely disparate and distributed sources, and performs analysis on the aggregated data to discover one or more things such as widely distributed attacks, distributed but coordinated attacks, patterns of vulnerabilities, and so forth. • Anomaly detection and reaction director (ADRD or ADR Director): An ADRD integrates the functionality of two or more ADR tools; these tools may be of the same type or of different types. For example, an ADRD may integrate the functionality of many, identical network monitors or it may integrate the functionality of a system monitor and a vulnerability scanner. The ADRD provides an interface for managing ADR tools and their interactions. Products in this category may range widely in degree of integration. At a minimum, a system in this category provides a single interface to two or more instances of the same type of tool or to two or more types of tools that are interrelated at least via the view presented to the user. Very capable ADRDs include intrasystem communications among multiple instances and types of tools and may include within them the functions of other types of tools, such as analysis engines. • Anomaly detection and reaction support tool (ADRST or

Attribute	**Explanation**
	ADR Support Tool): This kind of tool does not itself perform anomaly detection or reaction functions but gathers information that could be used to detect anomalies. Tools of this type might collect audit data from hosts or data from network packets, store the data in a database, and make it available in some user-friendly form. • Decoy: A decoy tool or system provides, simulates, or emulates a computer system or network system to provide a target for a cyber attacker, whether an insider or an outsider. Tools of this type would typically collect data about intrusive activity, providing alerts and reports, possibly collecting evidence to be used in legal action, and so forth. • Infraction scanner: An infraction scanner periodically looks for evidence of infractions, including intrusions by outsiders and violations of policy by insiders. • Network monitor: A network monitor looks for evidence of attempted misuse or intrusion in real time by examining data from network packets. • Network scanner: A network scanner looks for evidence of network conditions that might provide an intruder or attacker an exploitable entrée into the network or the systems on the network. • Responder: A responder takes actions to mitigate the effects of an intrusion or other anomaly. A responder does not itself discover the problem; thus, it is activated by some other agent, such as an ADR Director. • Security compliance scanner: A security compliance scanner periodically examines the settings of system parameters that are relevant to the security of the system to ensure that they comply with a preset policy. • System monitor: A system monitor looks for evidence of misuse and intrusion in real time by examining data from the target system and/or data in network packets entering the system. • Vulnerability scanner: A vulnerability scanner periodically looks for vulnerabilities that might make a system susceptible to exploitation.

Attribute	**Explanation**
Architecture	We characterize the architecture of the tool as one of the following: • Sensor: A Sensor is a software/hardware component that one adds to a system such as a server or workstation to provide anomaly detection and reaction functions specific to that system or the domain in which the system is located. An ADR Sensor can operate independently of other ADR capabilities to protect the system or domain. It may also provide exported data or reports that can be used by other IDR capabilities. In addition, it may operate under the management of an ADR Director. • Agent: An Agent is a software/hardware component that one adds to a system such as a router to provide anomaly detection and reaction functions specific to the domain of the Director under whose management it operates. An ADR Agent never operates independently; it is designed to work cooperatively with an ADR Director. • Director: A Director is a software application or a software and hardware ensemble that performs storage, analysis, reporting, and/or command and control functions. It can be implemented on a stand-alone system or it can share a platform with other applications**,** running “independently” of the system on which it is installed, such as a server that hosts several different functions. An ADR Director controls or interacts with ADR Agents or Sensors within its domain. *See* description of ADR Director under Type of Tool above. • Sensors-Director: self-explanatory • Agents-Director: self-explanatory
Agent/Sensor Platforms	This attribute identifies the platform, both hardware and software, on which the agent or sensor executes.
Director Platforms	This attribute identifies the platform on which the director executes.
Target Platforms	This attribute identifies the platforms that are monitored, probed, scanned, etc., by the ADR capability being described.
Methods of Detection	We categorize all known methods of detection as one of the following types: • Statistical Deviation Detection: In this approach the ADR

Attribute	**Explanation**
	tool looks for deviations from statistical measures. A baseline of values is defined for subjects and objects such as users, groups, workstations, servers, files, and network adapters. One can use historical data, simple counting, or expected values to establish the baseline. As activities being monitored occur, the ADR tool updates a list of statistical variables for each subject or object of interest. For example, the engine might count the number of files read by a particular user over a given period. This method treats any unacceptable deviation from expected values as an intrusion. For example, when the number of files read by a particular user over a given period exceeds the expected value for that period, the ADR tool declares a potential anomaly. • Pattern Matching: ADR tools use a pattern matching technique for monitoring activity as well as for checking configuration parameters, preset policy, and so forth. When monitoring activity, the ADR tool compares activity to stored patterns that model attacks. Known attacks or types of attacks are modeled as patterns of data. Patterns can be composed of single events, sequences of events, thresholds of events, or expressions using AND and OR operators[8]. This method treats any activity that matches a pattern as a potential anomaly. For checking current settings, parameters, and so forth, the ADR compares the value of some data item to a predetermined value that can represent a known vulnerability, a configuration setting, an element of a security policy, and so forth.
Sources of Data	Self-explanatory.
Reports	Self-explanatory.
Reactions	We generally group reactions into the two classes “alerts” and “responses”.

[8] Negation could also be used but it might introduce computational complexity since it could require looking for “everything but this event.”

Attribute	**Explanation**
Update Method	This attribute describes the method used by the vendor or provider of a tool to update patterns or algorithms used for detection, scanning, analysis, etc.
Communications	This attribute comments on the communications used by the tool to communicate among its parts or with other ADR capabilities, covering the security aspects such as authentication and data encryption.
Special Features	Special features are capabilities not usually found in a tool of the type being described.
Description	This attribute gives a description of the tool, as stated by the vendor or provider whenever possible. If the source of the description is other than the vendor or provider, the source is identified.

The attributes just described are adapted in obvious ways to describing research projects.

Appendix C

Projects at Air Force Research Laboratory, Rome Location

The summary descriptions that follow are based on information provided by AFRL in September 1999. Projects are grouped by subject

- Intrusion Detection
- Damage Assessment and Recovery
- Forensic Analysis
- Analysis and Decision Support
- Anomaly Detection Support Tools

Descriptions of projects addressing more than one of these areas appear in each of the subject areas addressed.

Intrusion Detection

Process Control Approach to Indication and Warning Attack on Computer Networks

Investigating model-based intrusion detection techniques at the system level to detect coordinated IW attacks by correlating and fusing Indications & Warning (I&W) values from component-level intrusion detection techniques (low level intrusion detection sensors).

AFRL Program Manager: John Feldman

Estimated date of completion: October 1999

ATM Sentinel Intrusion Detection

Focused on intrusion detection at the data link layer of the OSI reference model.

AFRL Program Manager: N. Peter Robinson

Estimated date of completion: June 2000

Detection of Data Corruption Attacks in Information Warfare Environment

Data characterization, i.e., modeling sets of data items, will be used to construct a family of constraints and allow the system designer to associate predicates that govern the way the data in the set can change over time. If the predicates are not true at a given point in time, one is in a good position to declare an information attack whose target is one of the items in the characterized set.

AFRL Program Manager: Joe Giordano

Estimated date of completion: January 2000

Database Security

Focusing on intrusion confinement by isolating likely suspicious actions before a definite determination of intrusion is made.

AFRL Program Manager: Joe Giordano

Estimated date of completion: September 30, 1999

A New Integrated Approach to Intrusion Prevention, Detection, and Response

Research on a number of facets of the problem, focused on investigating computer models describing relationships between observable evidence and intrusion scenarios, examining techniques for detecting intrusions into networks, and investing automated tuning mechanisms for evidence gathering.

AFRL Program Manager: William Maxey

Estimated date of completion: April 2000

Data Classification and Data Clustering Algorithms for Intrusion Detection in Computer Networks

Developing a data classification and clustering algorithm specially tailored for intrusion detection in information systems.

AFRL Program Manager: William Maxey

Estimated date of completion: March 2000

Distributed Agent Information Warfare Framework

Research on distributed intelligent agents to monitor and analyze network traffic and host-level activity in support of multi-hypotheses fusion.

AFRL Program Manager: Bob Vaeth

Estimated date of completion: September 30, 1999

Damage Assessment and Recovery

Damage Assessment, Data Recovery and Forensics

Developing data recovery and damage assessment concepts, to provide a framework for development of a comprehensive system to aid the computer forensic analyst.

AFRL Program Manager: Bob Vaeth

Estimated date of completion: December 1999

Demonstrating Information Resiliency

The objective is real time resumption of information processing capability using proactive techniques for recovery of critical data.

AFRL Program Manager: Glen Bahr

Estimated date of completion: June 2000

Trusted Recovery from, Information Attacks

Investigating recovery techniques in three models: hotstart, warmstart, and coldstart; also determining algorithms to achieve trusted recovery from information attacks on databases.

AFRL Program Manager: Joe Giordano

Estimated date of completion: October 1999

Automated Resource Recovery Agent

The goal was to advance the state of the art in recovery and defense of computer systems resources after and during an attack by developing techniques to quickly bring systems back online. The focus was to maintain system operations by monitoring and recovering critical resources.

AFRL Program Manager: Joe Giordano

Estimated date of completion: May 1999

Forensic Analysis

Damage Assessment, Data Recovery and Forensics

Developing data recovery and damage assessment concepts, to provide a framework for development of a comprehensive system to aid the computer forensic analyst.

AFRL Program Manager: Bob Vaeth

Estimated date of completion: December 1999

OMNI SLEUTH – Computer Forensics System

Extending an existing intrusion detection framework to provide forensic agents and an investigative user interface.

AFRL Program Manager: John Feldman

Estimated date of completion: December 1999

Synthesizing Information from Forensic Investigation

Research into five key methodologies for assisting computer forensic specialists: information archive, preservation and organization, information type identification, semantic identification techniques, evidence mining techniques, and evidence viewing techniques.

AFRL Program Manager: John Feldman

Estimated date of completion: May 2000

Analysis and Decision Support

Interactive Information Protection Decision Support Systems (IIPDSS) ATD

This ATD will plan and program for development and fielding of an interactive, adaptable data correlation capability with integrated decision support for analyzing network activity from multiple sensors. It will provide technology to assist operators in prioritizing alarms, to automatically clear false alarms via expert analysis, to automate post-incident data collection, and to provide step-by-step recommended courses of action for dealing with alerts and incidents.

AFRL Program Manager: Mike Nassif

Estimated date of completion: unknown

Extensible Prototype for Information Command and Control (EPIC2)

This project describes some key advantages of a data-centric, expert system architecture, the EPIC2, lessons learned from the deployment of EPIC2 in the Air Expeditionary Forces (EFX98) exercise, and an integration plan for EPIC2 under the Technical Cooperative Program (TTCP).

AFRL Program Manager: Chet Maciag

Estimated date of completion: unknown

Anomaly Detection Support Tools

Audit Workbench

Developing a programming system, or framework, for processing and analyzing audit trails generated by host operating systems.

AFRL Program Manager: Brian Spink

Estimated date of completion: May 2000

Credits

The production of this compendium was sponsored in fiscal year 1999 by the Air Force MOIE Project, 039974820T, C2 Protect, Tactical Environment Task and in fiscal year 2000 by the Air Force MOIE Project, 0300749900, Intrusion Detection Systems Research.

This document was produced with the assistance of RoboTech, a technical document template.