Formula Consultants

IDS-2200

Intrusion Detection System

Product Description

Formula Consultants Incorporated

P.O. Box 544
Anaheim, California 92815

714/778-0123
714/778-6364 (Fax)

sales@formula.com
www.formula.com

Highlights

IDS-2200 brings intrusion detection to your OS 2200 system.

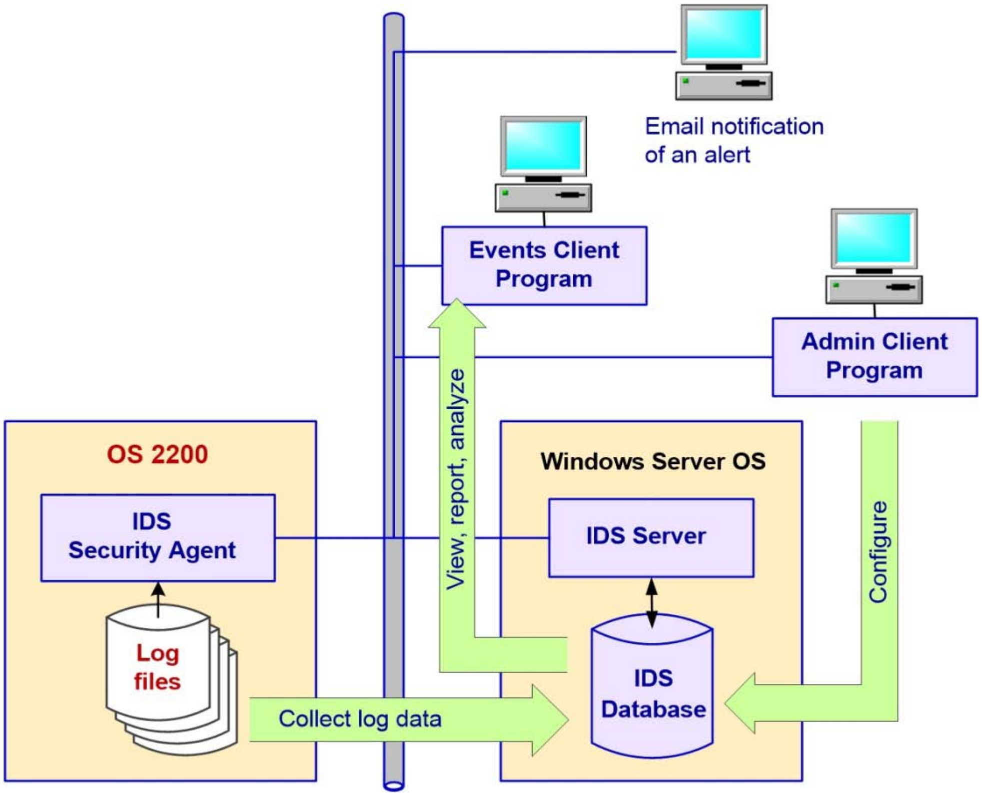
IDS monitors key system logs for activity or events related to security. Administrators define thresholds of anomalous activity which will generate alerts. User activity, which violates pre-defined rules or thresholds, triggers IDS to terminate the user session and / or suspend user signon privileges, while alerting security administrators.

Administrators use convenient GUI presentations to review relevant log data in the IDS database, and monitor the overall internal security environment for the OS 2200 site.

Release Status	Current release: IDS-2200 2R2
Installation	Standard installation w/ COMUS and SOLAR for OS 2200 components Familiar Windows installation techniques for server, client components
Log Data	Continuously gathers security related log data from EXEC, comm., web, etc.
Detects unauthorized use	Detects anomalous or unauthorized user access of system resources Notifies relevant security staff Can terminate the session and/or disable the user's signon privileges
Database	Stores security related log data in dedicated, server-based database
Viewing Data	Authorized users view log data via a client GUI program
Defining "Rules" for Alerts	Administrators use a GUI wizard to define alerts. Anomalous or unauthorized access, detected in logs is programmed to notify administrators, and, optionally, restrict that user's access.
Secure Transmission	AES 128 bit encryption for all inter-component communications Optional SSL encryption

Overview

IDS-2200 Components



IDS Security Agent

The IDS Security Agent collects log data from the OS 2200 EXEC and other subsystems. It sends the log data to the IDS Server.

IDS Server

The IDS Server, hosted on a Windows Server platform, continuously receives log data from the IDS Security Agent, and stores it in the IDS Database, under Microsoft SQL Server.

Based on “rules” pre-defined by administrators, IDS immediately detects anomalous or unauthorized access of OS 2200 system resources. When activity is detected which matches a configured “rule,” IDS generates an alert, sending an email notification to staff. Depending on the configuration choices for that alert, IDS can terminate the user session and / or deactivate that user's signon privileges. (Not shown on the diagram.)

The IDS Server implements interfaces, where IDS client programs connect with the IDS Server, to configure, manage, and operate IDS-2200.

IDS Database

The collector module within the IDS Server receives the log data from the OS 2200 system, and stores it in the IDS Database.

IDS Admin Client

Administrators use the IDS Admin Client to complete the installation of IDS. They also use it to configure the operating characteristics of IDS, especially to define the alerts which will detect unauthorized access.

IDS Events Client

Authorized users, such as security analysts and administrators, use the IDS Events Client to review the overall operation of IDS. They view security events and alerts. They have additional tools for monitoring the OS 2200 security environment.

Email Recipients

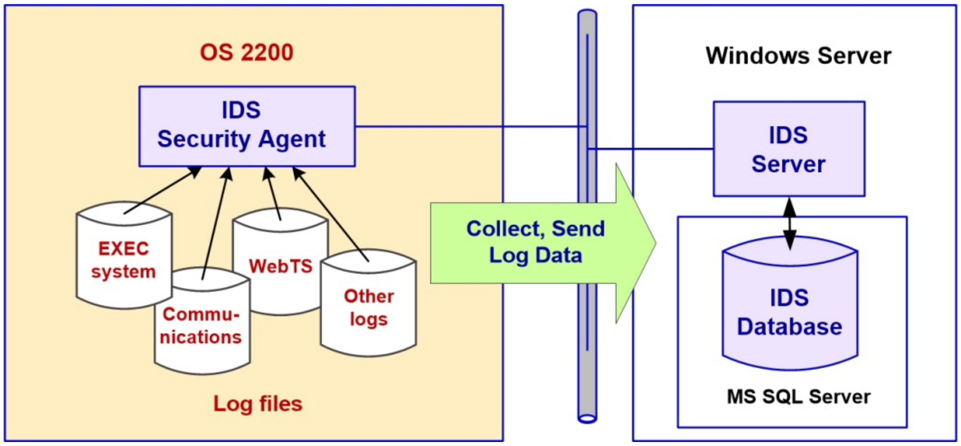
When security administrators define alerts, they can configure the email address of one or more staff members who will be notified when that particular alert is triggered. These recipients do not need to be IDS users.

IDS-2200 in Action

Log Information Gathered by IDS

IDS-2200 gathers security related system information from a variety of sources originating on the Unisys OS 2200 enterprise server.

IDS-2200 2R2 Security Agent Installation and Administrator Guide



IDS gathers OS 2200 system logs:

- User authentication events
- File authentication events
- ACR authentication events
- Privilege authentication events
- CPFTP events
- EXEC events

IDS gathers communications logs:

- CMS
- CPComm/CPCommOS
- SILAS

IDS gathers web enablement logs:

- WebTS

IDS gathers logs for BIS (MAPPER) events.

In a future release, IDS will gather client-server logs:

- OLTP
- UniAccess
- CITA

Configuring IDS-2200

Core IDS Objects

IDS 2R2 Admin Client User Guide, "Configuring IDS Objects and Parameters," page 2-2

To complete the installation of IDS-2200, administrators use the IDS Admin Client program to configure the key IDS objects.

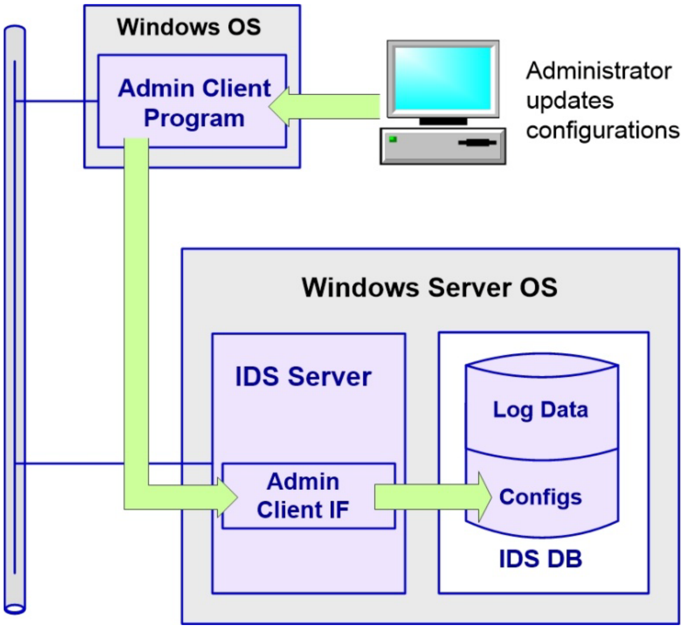
- the OS 2200 agents which will be collecting log data, and
- the users who will be permitted to use IDS functions.

Defining Alerts in IDS

IDS 2R2 Admin Client User Guide, "Defining Alerts," page 2-9

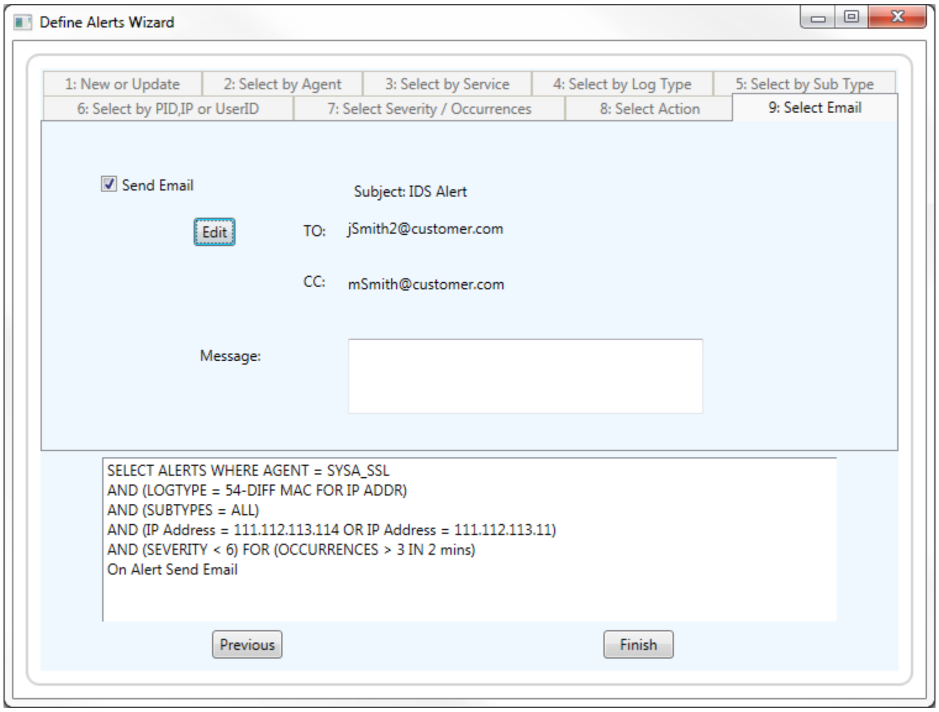
An alert is a set of conditions within the security events which, when detected, will trigger additional action. Administrators configure follow-on actions appropriate to the security event detected, including:

- recording the alert in the database,
- notifying a staff member(s) via email,
- (potentially) terminating the user's session, and
- (potentially) deactivating the user's signon privileges.



Security administrators and their management first plan their monitoring and enforcement regime. What kinds of unauthorized use of system resources do they want to detect? Which of these should generate specific alerts to individuals who can take further action? Which of these security events should trigger automatic restrictions for the user detected?

Next, the security administrator uses an IDS-2200 GUI tool within the IDS Admin Client to define the alerts. The tool is implemented as a "wizard."



☑ Send Email

Subject: IDS Alert

TO: jSmith2@customer.com

CC: mSmith@customer.com

Message:

```
SELECT ALERTS WHERE AGENT = SYSA_SSL
AND (LOGTYPE = 54-DIFF MAC FOR IP ADDR)
AND (SUBTYPES = ALL)
AND (IP Address = 111.112.113.114 OR IP Address = 111.112.113.11)
AND (SEVERITY < 6) FOR (OCCURRENCES > 3 IN 2 mins)
On Alert Send Email
```

It presents a GUI with a series of tabbed data entry panels. Each panel focuses on an attribute or a condition to be associated with the alert. As the administrator makes choices presented in the GUI panels, the alert generator is formulating the SQL commands which will operate against the IDS database of consolidated log data.

For example, the alert can be focused on a log type or sub-type. It can be focused on an individual workstation ID. It can stipulate the kind of restriction to be placed on the user involved in the security event. When conditions trigger this alert, it can be configured to automatically send an email message to one or more recipients, who do not need to be registered users of IDS-2200.

After IDS has been installed, it is continuously updating the IDS database, running under Microsoft SQL Server, and hosted on a Windows server platform.

Security administrators engage in a combination of proactive and responsive/reactive activities.

Proactive - Reviewing IDS Events and Alerts

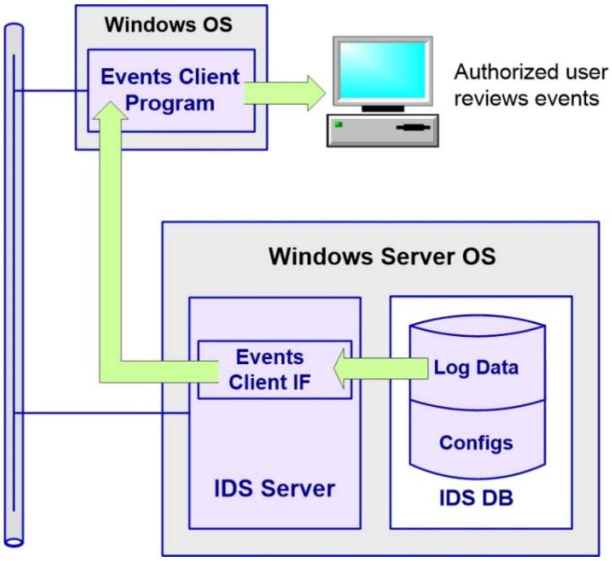
Security administrators and analysts continue to monitor risk conditions and define new alerts to detect these risk conditions. They use the GUI display capabilities to review the security events. They may select events based on a time period, log types/subtypes, the event severity, or on other event attributes. The events appear in a list. Highlighting an individual event produces a detailed display of that event.

IDS 2R2 Events Client User Guide,
Section 2, Using the Events Client

Events Client users can also view both events and alerts on the same screen, with alerts in the upper window and events in the lower window. Details for a highlighted alert or event appear in a frame on the right within each window.

In addition to viewing selected prior events, the security analyst or administrator can choose the option to "Track Current." In this setting, the system dynamically displays all new events in real time as they occur.

Analysts can also use the Events Client to scan the ports on the OS 2200 system, and to trace the route to a specific IP address.



Responsive / Reactive

When an alert triggers an automatic action, it generates an email to all recipients, configured within that alert. Depending on the conditions of the security event, and actions taken toward the user's session and/or privileges, the administrator might place additional restrictions on that user. Or, the administrator might restore the user's privileges. Security administrators use their analysis to make recommendations to management.

Product Documentation

The IDS-2200 documentation set:

- *IDS-2200 2R2 Release Announcement*
- *IDS-2200 2R2 Security Agent Installation and Administrator Guide,* FP-101107-005
- *IDS 2R2 Installation and Configuration Guide for Windows Platforms,* FP-101108-003
- *IDS 2R2 Admin Client User Guide,* FP-101109-003
- *IDS 2R2 Events Client User Guide,* FP-101110-003
- *IDS 2R2 Quick Start Notes*
- *FCI Products Release Tape Recreation Instructions*

To learn more about the format and interpretation of specific OS 2200 system log records, types and sub-types, refer to the Unisys documentation on that topic, in two volumes:

- *OS 2200 System Log Operations and Support Reference Manual Volume 1: Introduction Through Error Log Type 629 ClearPath OS 2200 Release 15.0* 7831 0315-025
- *OS 2200 System Log Operations and Support Reference Manual Volume 2: Error Log Type 801 Through Type 17650 ClearPath OS 2200 Release 15.0* 3839 6347-006

Refer to documents related to the OS 2200 release level appropriate to your site.

For additional information, refer to Unisys documentation which describes the implementation, configuration and administration of security features in OS 2200.