Protecting Your Business Security with Locum RealTime Monitor

By: Locum Software Services Limited

White Paper

Relative to MCP 19.0
We live in a world with increasing threats to system and information security. Governments and regulators around the world are responding by requiring increased vigilance, compliance, and reporting by businesses and government agencies. Protecting your business and customer information has NEVER been more important.

To meet these challenges, businesses are facing the urgent need to:

- Reduce the time to detect attempts to gain unauthorized access to sensitive information;
- Reduce business risks that can lead to severe consequences in terms of legal costs, loss of revenue, sanctions for regulators, severe client dissatisfaction and declining reputation;
- Improve compliance and reporting for management, regulatory agencies and auditors.

This paper focuses on Locum RealTime Monitor and how this security tool is designed to help you:

- Significantly reduce the risks and costs of inaction and non-compliance;
- Transform security into a highly visible resource;
- Assimilate your ClearPath MCP systems into your current SIEM infrastructure, further reducing costs and training.

Fully integrated and shipped with every Unisys ClearPath MCP operating environment, Locum RealTime Monitor’s full functionality can be activated through the purchase of a run-time software license. For evaluation purposes, a short-term trial license is available at no charge.
# Table of Contents

Introduction........................................................................................................................................ 4  
Benefits of Locum RealTime Monitor................................................................................................. 5  
What is Locum RealTime Monitor?...................................................................................................... 5  
How to Get Started................................................................................................................................ 8  
Implementing Locum RealTime Monitor.............................................................................................. 10  
Advanced Filtering Techniques............................................................................................................ 12  
Escalation of Alerts via Email or Syslog............................................................................................... 13  
RealTime Service.................................................................................................................................. 15  
An Example Client Scenario ................................................................................................................ 16  
Evaluating Your System....................................................................................................................... 24  
Best Practices....................................................................................................................................... 26  
Conclusion............................................................................................................................................. 27  
Licensing Requirements...................................................................................................................... 28  
About Locum.......................................................................................................................................... 28  
References........................................................................................................................................... 28
Introduction

Attempted breaches of information systems are becoming an ever increasing occurrence in today’s business environment. When businesses do not immediately detect attempts to access sensitive information, serious legal consequences and exceptional financial issues can result. In response to the increasing threat level, governments and regulators are enacting an ever increasing number of regulations covering compliance and the need for operational transparency. This is a worldwide phenomenon, and no organization is exempt. The regulations cover government, public, and private companies across all sectors including healthcare organizations, financial institutions and insurance, and indeed every company storing and accessing private consumer data.

In terms of security, the regulations aim to ensure the confidentiality, integrity, and availability of all electronic information companies create, receive, maintain, and transmit. Validation of compliance is usually achieved through security auditing, performed by internal or external auditors.

On ClearPath MCP systems, as on most systems, the primary source of audit data is the system event log. With busy systems, the system log can accumulate hundreds of thousands of records each day, and it is the sheer volume of information that can make timely alerting and auditing difficult. Moreover, as machines get faster, this volume is sure to increase, making the difficulty of identifying and isolating events increase proportionately if we have to use traditional retrospective log analysis.

In a world of increasing demands on budgets and staffing levels, it makes sense to automate processes. With security dependent on small numbers of staff, and with training budgets stretched thin, the only way to make the numbers add up and still protect your business in real time is to invest in software that can automate time and labor-intensive processes, freeing your staff up so that they can react to threats as they occur. The implementation of timeline graphs within RealTime Monitor also allows security administrators to be more proactive than reactive.

Locum RealTime Monitor addresses these very real issues and is designed to help mitigate the resultant risk. Locum RealTime Monitor is a ClearPath MCP security solution specifically positioned to assist ClearPath MCP clients to respond much more rapidly to unauthorized attempts at accessing sensitive information. Using event data related to the system logs, Locum RealTime Monitor classifies events as they occur, consolidates data from multiple systems and presents an immediate overall security assessment that is tailored exactly as per individual client business requirements.

Locum RealTime Monitor is the first Unisys-supplied real time product with relevance for both security administrators and auditors running all models of ClearPath MCP Servers. It is delivered as a pre-integrated and pre-tested solution. Locum RealTime Monitor is part of a suite of security products developed in partnership with Locum Software Services Limited, a company with a long history of security specialization and servicing customers around the world, headquartered in England.
Benefits of Locum RealTime Monitor

Locum RealTime Monitor is designed to provide the following business and operational benefits:

- Through automation, there is a substantial reduction in the time taken to detect attempted security breaches, so that exposure to additional business risks and costs is minimized
- Improved agility to react to dynamic security events
- Improved ability to manage the flow and priority of security information that is unique in each client environment
- Agile solution that is tailored to the unique requirements of ClearPath MCP clients
- Pre-integrated and pre-tested solution requiring minimal additional training for security administrators
- Tight integration with the MCP security architecture and high levels of automation, including the automation of security event reporting, provide a best-in-class security solution. This, in turn, can help elevate the productivity of staff involved in detecting and reporting on security events, and significantly reduce costs and improve levels of internal and external compliance without the need for additional staff
- Easy to use graphical interface for rapidly classifying which security events should be reported
- Improved risk management by increased security intelligence about the ClearPath MCP environment
- Fast 'out-of-the-box' operation, but is easily reconfigurable to provide adaptation for changes in security policies and tailoring as per each client’s specific needs
- Effective alert messages that can be saved for further scrutiny by auditors
- Timeline Graphs showing the rate of alerts allow security administrators to be more proactive than reactive
- Integration with existing Security Information and Event Management (SIEM) infrastructure, via SYSLOG format messages
- Optional use of RealTime Service. Run as a Windows Service program, the Service provides message escalation and forwarding functions and is designed to run automatically and unattended on a Windows server, without the requirement of a user interface

What is Locum RealTime Monitor?

Locum RealTime Monitor allows the monitoring in real time of security and system events on one or more ClearPath MCP systems. This incorporates flexible alert designation, together with routing of system and security events to meet all system monitoring needs. Locum RealTime Monitor consists of a Configurator, a Dashboard and a Service program which work together to offer the power and flexibility to create a monitoring environment that can be tailored to meet individual customers’ needs.

With options to keep the security administrator in touch with critical events, even when away from a workstation, and a choice of options to help display or further process the data, Locum RealTime Monitor gives total monitoring control over your ClearPath MCP systems.
Any system event that is loggable by MCP can be designated as an alert for Locum RealTime Monitor. Locum RealTime Monitor allows customers to choose which system events to monitor, either by selecting from a pre-defined list of generic security events grouped by functionality, or by designating specific system events by Sumlog major and minor types. Filtering can be applied to specific system events via the security relevance or successful result field of the log record.

More granularity in designating alerts can be attained by the use of advanced filtering which is available by the application of rules. For example, an event will only become an alert if it originated from a particular user or station, or if the text contains a specific subtext. See the Advanced Filtering Techniques section for more information.

Locum RealTime Monitor introduces the concept of activity codes, which are used to control monitoring actions. An activity code is the control structure that allows the customer to define the severity of each alert and what to do when the alert is received. This includes how the alert is displayed within the DashBoard, message forwarding using Syslog or via email to key members of staff, and/or other escalation actions. Activity codes group alerts which have the same severity, notification, and display requirements.

Figure 1: Locum RealTime DashBoard Alert Window

One specific alert may be associated with more than one activity code, so that, for example, two activity codes can be set up with the same set of monitored events, but different dispositions. For instance, if security violations reach a threshold level, the senior security administrator, who works at a secondary site, can be alerted to the problem via email or Syslog, while the operator currently in charge of monitoring the system simply sees the dial at 100%.
Alerts are forwarded to one or more instances of RealTime DashBoards running on Windows-based systems. Each dashboard has its own alert filters so that alerts can be configured independently, and each can display or forward alerts.

RealTime DashBoard displays alerts in one or more windows. By default, there is a separate window for each connection. However, each activity code may be configured to have its own alert window, so that the alerts may be grouped by severity, for example. Furthermore, each DashBoard can observe multiple MCP systems simultaneously, and alerts from several systems may be configured to be displayed in the same window. For example, you can define a window which shows all Red Alerts from multiple ClearPath MCP systems.

Locum RealTime Monitor also gives you the option to display RealTime Graphs within the RealTime DashBoard Main Window. RealTime Graphs are moving timeline graphs which show the rate of alerts per minute over a specified time period. The RealTime Graphs window is loaded automatically upon connection to a host, providing that the host has one or more windows defined. There is one graph per window, each showing the rate of alerts being sent to that window. Graphs are managed automatically when the state of a window changes. The graph will scale the Y axis automatically depending on the rate of alerts being displayed and the plot is updated once a minute. Each graph has set of radio buttons which can be used to adjust the scale to show different time periods. Each graph can be independently set. Figure 2 shows the RealTime Graphs tab within RealTime DashBoard.

Figure 2: The RealTime Graphs tab within the RealTime DashBoard Main Window
Multi-Factor Authentication (MFA) is available with RealTime Monitor, providing MCP programs the capability to enforce an extra layer of security on the user account. Conditions must be met for a successful log-on to trigger Multi-Factor Authentication; more information can be found in the RealTime Config and RealTime DashBoard Online Help files.

**How to Get Started**

Locum RealTime Monitor is delivered as part of every release of ClearPath MCP.

Locum RealTime Monitor comes ready for use 'out-of-the-box', and is easily configurable to meet the ever-changing needs of customers’ demanding environments. It is an optional priced feature and simply requires a software license key to activate. Without a license key you are restricted to using Locum RealTime Monitor with its 'out-of-the-box' settings. Limited duration trial licenses are available for download from Unisys at [http://www.unisys.com/locum](http://www.unisys.com/locum). However, to gain the most benefit from a short-term evaluation period, there is a certain amount of preparation required before a trial license is installed and activated.

Each customer’s audit requirements are unique and while the ‘out-of-the-box’ configuration provides a good starting point for monitoring MCP systems, it is unlikely that it will entirely satisfy these requirements. Customers should be familiar with the auditable events required by their local Security Policy document to determine how to configure Locum RealTime Monitor to best meet their auditing needs. A list of ‘out-of-the-box’ settings can be found in the Implementing Locum RealTime Monitor section.

Principally this involves deciding which events are to be designated as alerts, and what course of action should be taken for each.

In selecting system events for monitoring, the customer creates an alert filter. Each alert is assigned to one or more activity codes. It is the activity code that specifies in which window(s) alert messages are to be shown and just how those messages are displayed. Activity codes also allow customers to set required actions, such as the use of Syslog to send input to an SIEM package, or sending emails to alert key members of staff of abnormal levels of system events.
Figure 3: Edit Monitored Events dialog

Figure 3 shows the Edit Monitored Events dialog. The top pane displays a list of currently-defined activity codes, one of which must be selected before designating one or more alerts. The lower two panes allow the customer to designate alerts and to associate the alerts with the selected activity code. There are two mechanisms for doing this: Filter by Function and Filter by Log Record Type.

Filter by Function

If a broad spectrum of monitoring is required, customers can choose to filter system events by function. Locum provides a list of functions from which customers can select. These include giving the customer a comprehensive overview of all system events that fall within the purview of the selected functions.

Some examples are:

- Security Policy Changes
- Security Violations
- Logon Violations
- Password Changes
- Privileged Actions
- System Commands
- User Definitions
- User Validations
- User Suspensions
Filter by Log Record Type

Unisys *System Log Programming Reference Manual* provides all the information necessary to map system events to system log record types. It is the log record type, specified as a major and minor type that is used to designate an event as an alert. This allows the customer to filter the specific alerts they need to monitor by log record type. Alerts can be further filtered via the security relevance or successful result field of the log record, providing the customer with finely targeted alerts for precise monitoring of only those system events that are of interest.

The next step is to decide the disposition of the alert, or the course of action to be taken. This includes specifying how to display the alert, what icon or color scheme to use and which dials to associate the alert with. Locum provides three default activity codes, which can be customized to the customer’s requirements. For more information on how to create or modify alerts, refer to the Locum RealTime Config Online Help file.

**Implementing Locum RealTime Monitor**

There are four components to the RealTime Monitor installation:

- **LOCUM/SAFELIB** is a server library that runs on the MCP system. Its function is to handle the overall configuration and process the routing of alerts through the requested interfaces.
- **RealTime Config** is a Windows executable that allows the configuration of interfaces, alerts, and activity codes. RealTime Config is an MMC module, integrated with Unisys SecurityCenter.
- **RealTime DashBoard** is a Windows executable that acts as a collector to handle the display and forwarding of messages and the escalation of alerts.
- **RealTime Service** is run as a Windows Service program; as such it can be configured to be automatically initiated and to run unattended on a Windows server, without the requirement of a user interface. It provides all the message escalation and forwarding functions of RealTime DashBoard, but does not, and cannot, display incoming alert messages.

RealTime DashBoard, RealTime Service, RealTime Config and LOCUM/SAFELIB are provided with Unisys SecurityCenter. RealTime Config is a SecurityCenter module. Consult your SecurityCenter installation media for installation files and instructions on how to install the program and enter the run time key onto the MCP system. The RealTime DashBoard setup file (RTDsetup.exe) and the RealTime Service setup file are included amongst the files provided when you install the latest version of Unisys SecurityCenter and should be visible in the ‘INSTALLS’ share in your SecurityCenter directory. Run the setup packages and follow the instructions on screen in order to install RealTime DashBoard and RealTime Service.

LOCUM/SAFELIB is installed on the MCP system as part of a standard SecurityCenter installation. The Windows workstation software is not installed when the ClearPath MCP software is installed. SecurityCenter should be installed to the security administrator’s workstation, at which point RealTime Config will be installed automatically as a component.
Locum RealTime DashBoard should be installed where the data is to be collected and displayed. If you wish to use RealTime Service, it is usually preferable to install it on a Windows server. For greatest security and continuity, Locum recommends that RealTime Service be installed on the Windows environment of the ClearPath box.

The RealTime DashBoard Online Help file and the RealTime Config Online Help file contain detailed instructions on installation and set-up. For more information on the installation of RealTime Service, refer to the RealTime Service PDF manual.

Locum RealTime Monitor has a preconfigured 'out-of-the-box' configuration and when installed for the first time, it is immediately ready for use with this default configuration. Note that until you install a license key, you will only be able to use Locum RealTime Monitor in its default configuration. The default configuration consists of:

- 1 Config Interface
- 1 Alert Interface
- 3 Activity Codes

The Config Interface is configured in such a way that it is capable of connecting to any Windows workstation that is running RealTime Config. The Alert Interface is configured in such a way that it is capable of connecting to any Windows workstation that is running RealTime DashBoard.

The pre-configured activity codes are:

- Red Alert
- Amber Warning
- Information (green)

Each activity code is configured to display its alerts in its own default window.

In addition, the Alert Interface is configured to recognize certain events as alerts, and associates each with a particular activity code, as follows:

<table>
<thead>
<tr>
<th>Security Violations</th>
<th>Red Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon Violations</td>
<td>Red Alert</td>
</tr>
<tr>
<td>Security-Relevant System</td>
<td>Amber Warning</td>
</tr>
<tr>
<td>Privileged Actions</td>
<td>Amber Warning</td>
</tr>
<tr>
<td>Miscellaneous Security</td>
<td>Amber Warning</td>
</tr>
<tr>
<td>Abnormal Program Terminations</td>
<td>Information</td>
</tr>
<tr>
<td>Unsuccessful Password Changes</td>
<td>Information</td>
</tr>
</tbody>
</table>

Once you have a software license, it is recommended that, for security reasons, the two interfaces be reconfigured with specific IP addresses or workstation names so that each interface is dedicated to a specific workstation, therefore disallowing connection from elsewhere. It is acceptable for the two interfaces to be dedicated to the same workstation. You may also wish to increase the number of config and/or alert interfaces, depending on the number of security administrators there are, or areas and locations that are required to receive the alerts.
The alert designations and activity code definitions outlined above are for guidance only, and it is a further recommendation that they be amended appropriately to suit the local environment.

**Advanced Filtering Techniques**

Sometimes, the granularity provided by activity codes may not be sufficient to meet your auditing requirements. Advanced filtering offers finer granularity by means of Filter Rules, so that only alerts which meet specified criteria are delivered to the dashboard/collector. Configuration of Alert Filter Rules is performed by the means of the Table of Filter Rules which can be accessed via the Host Actions sub-menu of the Action menu on RealTime Config’s Menu Bar.

Note that Filter Rules are associated with a specified Alert Interface, not with the Activity Code associated with the event.

The Table of Filter Rules allows users to create rules which can later be applied to an event being monitored. Up to six conditions may be specified per rule. Specifying these conditions is achieved via the Filter Rule Configuration dialog, accessed via the Table of Filter Rules.

![Figure 4: The Filter Rule Configuration dialog](image)

Figure 4: The Filter Rule Configuration dialog
Each condition can filter alert messages on the basis of:

- Text
- Originating Usercode
- Originating Accesscode
- Originating Station

that:

- Contains
- Does not contain
- Begins with
- Ends with
- Equals
- Is not equal to

the appropriate Target text.

Assigning a rule to a monitored event is done via the List of Monitored Events dialog by clicking the Select Filter Rules… button.

**Escalation of Alerts via Email or Syslog**

One course of action for high priority alerts is to escalate to an email notification if specified thresholds are exceeded. The ‘Message escalation parameters’ and ‘Send by email’ sections on the Activity Code Configuration dialog in Figure 5 show the controls that are available for email notification. This requires that the Unisys Email Utility be installed to the ClearPath MCP environment.
A further option available within Message Escalation and Forwarding is to use Syslog to send alerts to another collector. Syslog is a computer data logging protocol widely used in Security Information and Event Management (SIEM) architectures. Most SIEMs will recognize and accept incoming messages that are in Syslog format. Using this mechanism, Locum RealTime Monitor becomes an agent that can deliver alerts generated on your MCP system to a collector situated and running on a different platform.

The Locum RealTime Monitor implementation of Syslog is based on the industry standard defined by RFC 5424.

Figure 6 shows the controls that are available for Syslog forwarding. For more information on Syslog severity codes, see Figure 15 and associated text in An Example Client Scenario.
The Activity Code Configuration dialog allows a combination of escalation methods to be set.

![Activity Code Configuration](image)

Figure 6: Activity Code Configuration – Forward to Syslog on the Message Escalation and Forwarding tab

**RealTime Service**

RealTime Service provides all the message escalation and forwarding functions of RealTime DashBoard but without displaying incoming alert messages. The functionality of RealTime DashBoard is unaffected by RealTime Service. You can have a mixture of RealTime Services and RealTime DashBoards within your RealTime Monitor configuration. RealTime Service is an NT service application that allows alert monitoring to be run unattended on any Windows server.

Via RealTime Service, alerts can be sent to Syslog, Email, File and/or the Windows Event Log. By using escalation parameters, you can specify that any subset of these actions should only take place if a specified number of alerts are received within a particular timeframe.
RealTime Service can be configured via the shortcut placed on the Windows Start menu by Locum’s installation process. The Configuration dialog can also be accessed through RealTime Config’s Action menu on the Menu Bar.

![RealTime Service Configuration dialog](image)

**Figure 7: RealTime Service Configuration dialog**

You can choose to change the Retry Interval and Report Interval, as well as selecting not to use Unisys Authentication Support. The Retry Interval determines how often (in minutes) the Service will attempt to open a closed connection. The Report Interval determines how often (in minutes) the Service will report on its status.

Three default connections will be listed in the Connections box. Double-clicking on a connection opens the Connection Details dialog where changes can be made.

Once a connection between RealTime Service (in a Windows environment) and LOCUM/SAFELIB (in the MCP environment) is established, security requirements will normally demand a logon process between the two. Locum recommends automatic logon using Authentication Support, which requires credentials to be entered via the Windows Control Panel.

The configuration of which messages the Service receives, and what methods are used, is done via the SafeLib Configuration dialog in RealTime Config.

The Service is started by accessing the Windows Services dialog from the Control Panel > Administrative Tools > Services option.

For more information on RealTime Service, refer to the RealTime Service PDF manual.

**An Example Client Scenario**

A company is concerned about possible security breaches of their MCP system and decides to use Locum RealTime Monitor to keep track of security and logon violations. When a threshold level of violations is reached, they want their security administrator to be alerted automatically. They also want to keep track of password changes, privileged actions and user suspensions, both in support of this and also to provide an audit trail for their user management policy.
RealTime DashBoard is installed on a Windows workstation and connections are created to the company’s MCP systems.

The security administrator runs RealTime Config and selects the active connection to the required ClearPath MCP system. From the Action menu, they select Host Configuration. From the SafeLib Configuration dialog (Figure 8), they select the alert interface that applies to the workstation on which they want to amend the alert filter, and then clicks the Reconfigure… button > Edit Alert Filter… option. The List of Monitored Events opens (Figure 9).

Figure 8: SafeLib Configuration dialog – Reconfigure… button > Edit Alert Filter… option

Figure 9: List of Monitored Events dialog
The security administrator needs to change the default monitored events, so clicks the Edit Monitored Events… button and opens the Edit Monitored Events dialog (Figure 10).

Figure 10: Activity Code 3 – Red Alert

The most important events that the company wants to monitor are security and logon violations, so the security administrator selects the Red Alert activity code (Figure 10), and then checks Security Violations and Logon Violations on the Filter by Functions list. They uncheck any other options and click Apply.

The security administrator moves onto the next most important events, which are password changes and privileged actions. They select activity code 2, Amber Warning (Figure 11), and check Password Changes and Privileged Actions from the Filter by Function list, uncheck any other options, and click Apply.
The lowest level of alerts is reserved for user suspensions. The security administrator selects activity code 1, Information (Figure 12), and ensures that only User Suspensions is checked on the Filter by Function list.
The security administrator then clicks OK, which closes the Edit Monitored Events dialog and returns them to the List of Monitored Events, where they can see at a glance which events are now being monitored (Figure 13).

Figure 12: Activity Code 1 – Information
The security administrator wants to make sure that when security and logon violations reach a certain level, they will be alerted automatically, so they make sure they have a monitored event selected that is assigned to the Red Alert activity code, then clicks the Edit Activity Codes… button on the List of Monitored Events. The Activity Code Configuration dialog opens.
Figure 14: Activity Code Configuration dialog – Email forwarding

The Message Escalation and Forwarding tab allows the security administrator to select how they want Locum RealTime Monitor to alert them when the threshold level for violations is reached. From the ‘Send by email’ dropdown menu, they can select Apply escalation parameters and then set the threshold level at the top of the dialog. If more than 20 messages are received within one minute, emails will be sent to their email address, but so that their inbox doesn’t get swamped with emails, they set a limit of no more than 2 email messages to be sent in any one minute period. They click OK and save the changes to the activity code.
The security administrator can also select Syslog as an escalation option by selecting ‘All messages’ if they wish all messages to be sent to Syslog, or ‘Apply escalation parameters’ if they wish the escalation parameters be applied. They then choose the desired severity level for that activity code and enter the hostname or IP address of the machine they wish to be alerted. This would typically be a computer running a Security Information and Event Management (SIEM) solution. Logging messages containing alert text will then be forwarded to the chosen machine. It is possible to specify a port other than the default, by un-checking the ‘Use Default’ checkbox and entering a value greater than 1024 (Figure 16). Clicking OK takes them back to the List of Monitored Events.

Figure 16: Forward to Syslog options within the Activity Code Configuration dialog
The security administrator clicks OK to close the List of Monitored Events and sits back to watch Locum RealTime Monitor as it provides a list of alerts, showing only those events needed to be monitored, allowing the organization to react promptly if their systems come under attack.

Figure 17: RealTime DashBoard – Customized display

**Evaluating Your System**

ClearPath MCP servers are inherently secure from many of the vulnerabilities that may afflict some other platforms. In addition, the MCP software allows the customer to impose a high level of security through its many and varied security features, such as its security policy options, and the deployment of the Secure Access Control Module (formerly InfoGuard).

However, the overall security of a ClearPath MCP server is dependent on:

- The security restrictions in force
- The level of privilege allowed on the system

The security restrictions in use on the system are generally governed by the Security Policy of the organization, which should be clearly defined in a security policy document. A security evaluation should be conducted to ascertain what restrictions are in force, and to determine whether those restrictions meet the requirements of the organization’s own security policy.

Irrespective of the security restrictions, the level of privilege should be predetermined and defined. Controlling the amount of privilege is perhaps one of the major challenges facing a security administrator. By its very nature privilege begets privilege, and generally bypasses the security restrictions that are enforced for non-privileged users.
In recent years, ClearPath MCP has introduced increasingly finer granulations of privilege allocation, which provide the security administrator with more precise control.

Any security evaluation should therefore quantify the amount and level of privilege defined on the system, enabling the security administrator to assess the risk of that privilege.

There are several tools available for the ClearPath MCP security administrator to conduct an evaluation of the security of the enterprise:

- Locum SafeSurvey, for assessing
- Locum SecureAudit, for audit reporting
- Locum RealTime Monitor, for alerting
- Logalyzer, for analysing system logs

Locum SafeSurvey

Locum SafeSurvey is a security assessment product for ClearPath MCP systems. It automates the process of risk identification based on system generated information, and therefore helps significantly in risk evaluation and risk management. SafeSurvey takes on-the-spot snapshots of system security, which with repeated use will identify trends over a period of time. These can be used to produce customized graphs and charts to display the data collected in ways that make it easy to understand at a glance. A summary version of SafeSurvey is fully integrated and shipped with every Unisys ClearPath operating environment; its full functionally can be activated through the purchase of a run-time software license.

Locum SecureAudit

Locum SecureAudit is an event-based auditing tool which analyses data from both single and multiple system logs and produces a wide range of retrospective security-relevant reports. It enables the security administrator or auditor to focus on specific events and conduct forensic investigations using a time-based reporting mechanism. Used in conjunction with Safe Survey, it facilitates the analysis and evaluation of ClearPath MCP systems. The data collected by Locum SecureAudit can be used to produce customized reports, graphs, and charts to display the data collected in ways that make it easy to understand at a glance. A summary version of SecureAudit is fully integrated and shipped with every Unisys ClearPath MCP operating environment; its full functionally can be activated through the purchase of a run-time software license.

LOGANALYZER

SYSTEM/LOGANALYZER is a Unisys-supplied utility program that analyses system log entries and produces a report consisting of all entries that correspond to parameters that are set. Whilst mainly an operations tool, Logalyzer can be useful in retrieving security information concerning events that have happened on the system. Logalyzer is included in every Unisys ClearPath MCP operating environment.

Trial Licenses

Free trial licenses are available for Locum SafeSurvey and Locum SecureAudit at www.unisys.com/locum, under the Evaluation Licenses section. Follow the links for each product to download an evaluation license key. Contact your sales representative for more information about licenses.
**Best Practices**

Once a ClearPath MCP system is evaluated, and the necessary changes and enforcements put in place, there remains a need for continual vigilance. Periodic repeated evaluation should be performed and the tracking of any changes to or violations of policy is an absolute necessity. Locum RealTime Monitor offers the ability to track such changes as soon as they happen, and to escalate the alert action as the security administrator sees fit.

The Locum RealTime Monitor product is designed as a security tool. Although most events on the system are capable of being monitored, including non-security relevant events, the routing of alerts should be to a security destination rather than an operation destination.

Each of the pre-defined functional alerts has security relevance. The following table recommends a priority for each of the functional alerts. Note that these are recommendations only and the importance of each will naturally vary from site-to-site, depending on such factors as the type of workload being run on each ClearPath MCP server and the security policy in force throughout that company.

<table>
<thead>
<tr>
<th>Event</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal Program Terminations</td>
<td>Low</td>
</tr>
<tr>
<td>COMS Cfile Changes</td>
<td>Low</td>
</tr>
<tr>
<td>DMSII Database Events</td>
<td>Low</td>
</tr>
<tr>
<td>Guardfile Activity</td>
<td>Medium</td>
</tr>
<tr>
<td>Logon Violations</td>
<td>High</td>
</tr>
<tr>
<td>MCS Initializations</td>
<td>Low</td>
</tr>
<tr>
<td>Miscellaneous Events</td>
<td>Medium</td>
</tr>
<tr>
<td>Password Changes</td>
<td>Low</td>
</tr>
<tr>
<td>Privileged Actions</td>
<td>Medium</td>
</tr>
<tr>
<td>Role Based Access Control</td>
<td>Medium</td>
</tr>
<tr>
<td>Security Policy Changes</td>
<td>High</td>
</tr>
<tr>
<td>Security Violations</td>
<td>High</td>
</tr>
<tr>
<td>System Commands</td>
<td>Medium</td>
</tr>
<tr>
<td>Unauthorized File Accesses</td>
<td>High</td>
</tr>
<tr>
<td>User Definition Changes</td>
<td>Medium</td>
</tr>
<tr>
<td>User Suspensions</td>
<td>High</td>
</tr>
<tr>
<td>User Validations</td>
<td>Low</td>
</tr>
<tr>
<td>UserDataFile Changes</td>
<td>Medium</td>
</tr>
</tbody>
</table>

In addition to these general recommendations, an evaluation of the system may highlight other events of concern; events that are not covered by the functional alerts in the above table. It is then that finer granularity is needed.
Finer granularity may be achieved by configuring events by major/minor type. In this way, any loggable event on the system can be designated an alert. The *System Log Programming Reference Manual* gives a full list of all loggable events. Caution should be exercised however, in designating alerts in this manner, in terms of numbers of events selected and frequency of those events. For example, designating File Open events (major 1, minor 5) or File Close events (major 1, minor 6) as alerts would probably be counterproductive in that the frequency of such events would flood the collector and overwhelm all other alerts, as well as being a significant overhead on the system.

The use of Filter Rules also offers finer granularity in filtering events, ensuring that only alerts which meet specified criteria are delivered to the dashboard/collector. Configuration of Alert Filter Rules is performed by means of the Table of Filter Rules. For more information, see the *Advanced Filtering Techniques* section.

Some event records are marked by MCP with a result indicator which shows whether or not the event is security-relevant. The RealTime Config client has a check box whereby the list of security-relevant events is displayed. This may help in fine-tuning the filter selection.

As with many other things, security issues are continually evolving. More threats and vulnerabilities become exposed over periods of time. In addition, each MCP release may introduce new logging entries and events. Because of these, regular and periodic security review should be undertaken, and as a result, the configuration of Locum RealTime Monitor should be amended accordingly.

**Conclusion**

The power of Locum RealTime Monitor to help mitigate risks comes from its configurability and flexibility. One collector (dashboard) can monitor multiple ClearPath MCP systems and one ClearPath MCP system can be monitored from multiple dashboards. This allows the possibility of different views of the same ClearPath MCP system from different points, for example, a system security viewpoint versus a network security viewpoint. Each dashboard can be configured with different windows so that the dashboard can look at different events. All output is color-coded by system (defined when the connection is configured) as well as an icon for the activity code. You can even capture the events listed in a window by saving the output to a text file.

Locum RealTime Monitor comes as a pre-integrated, pre-tested solution at no additional costs, other than that of the software license to upgrade the client’s security infrastructure, offering security at an affordable price. To activate Locum RealTime Monitor, contact Unisys or your MCP system supplier and order style CSP10xxx-LRM (xxx represents a software pricing group – 10 through 160 in increments of 10).

Further information can be obtained either through the Locum Software Services website [http://www.locumsoftware.com/realtime_monitor.html](http://www.locumsoftware.com/realtime_monitor.html), by calling +1 (203) 434-2909 or +44 (0)1246 570-300, or by emailing sales@locumsoftware.com.
Licensing Requirements

To use RealTime Monitor in full-feature mode, you must have a Unisys-supplied license key (style xxx-LRM-LRM) that is compatible with the version of LOCUM/SAFELIB that is installed. For example, if the version of LOCUM/SAFELIB is 18.43.0926, key 591-LRM-LRM is required. This key will be valid on any MCP level between 581 and 601 providing it is used with the 18.0 level of LOCUM/SAFELIB.

To obtain pricing or order license keys, contact your system supplier or Unisys representative.

Note that Try & Buy keys are available to allow a short evaluation period of the software. Try & Buy keys offer full functionality for a limited time and are available online at www.unisys.com/locum.

About Locum

Locum Software Services Limited is a company that has specialized in security solutions for ClearPath MCP systems for over 30 years, with many customers around the world, primarily in the financial sector. Its flagship product is Safe & Secure, a proactive security solution that builds on and significantly enhances the standard MCP security. In recent years, Locum has forged a mutually beneficial partnership with Unisys; together delivering a suite of security products that includes Locum SafeSurvey, Locum SecureAudit and Locum RealTime Monitor.

References

- System Log Programming Reference Manual (form number 8600 1807)
- System Software Utilities Operations Reference Manual (form number 8600 0460)
- Locum RealTime DashBoard Online Help
- Locum RealTime Config Online Help
- Locum RealTime Service PDF Manual
- SecurityCenter Help File (form number 4310 9263)

For more information visit www.locumsoftware.com
©2019 Locum Software Services. All rights reserved.