

## Security Event Log Monitor

### Check your security

Windows 2000 is eminently capable of keeping track of events that concern the security of a system and the files contained in it. Every system has a separate Security Event log file especially for that purpose. But the word “every” imposes a limitation on exercising simple and correct control. The product reviewed here, GFI’s LANguard Security Event Log Monitor, allows you to keep a security watch on a large and diverse Windows environment.

Security is becoming an increasingly important part of everyday life, not least in computer system environments. One or more firewalls and all kinds of virus scanners protect our systems as well as possible against the outside world. The time has now come to make the inside world secure as well. Unfortunately, not everybody who works at a company can be trusted. This is not necessarily because of malice. In environments with hundreds of systems, it’s easy to make a mistake and somebody can accidentally try to access a certain system or file. There’s no problem provided that an incident doesn’t become the norm. Only a report covering a certain period of time reveals whether an incident really was just an incident. Accountants and above all EDP auditors are keen to see how safe a company is over prolonged periods of time. Windows enables an administrator to set the conditions that must be satisfied to copy an entry to the security log. In Windows 2000, you can find and set the Audit Policy values by following the path Control Panel -> Administrative Tools -> Local Security Policies. These settings make it possible to monitor user behavior. The log registers successful/unsuccessful log-ons and successful/unsuccessful accessing of network drives. It is also possible to keep track of attempts to access certain directories or individual files. In Windows 2000 Explorer, you can select Security in Properties in a folder or file

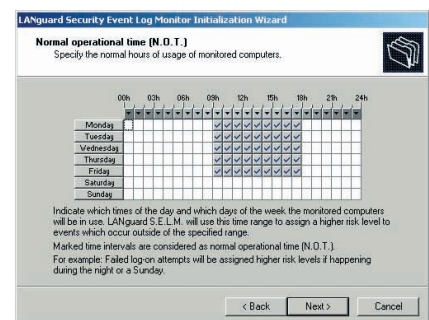
by clicking the right-hand mouse button. Advanced and Auditing can then be activated. Using Add, you can add a user or a group in the Name field. Your selection can be made complete with preferred quantities like Access, Failed and Successful. It is advisable to use at least a group as the unit to be monitored. Selecting a particular person or account can lead to legal and other problems. A logical group to select is Everyone.

#### Problem

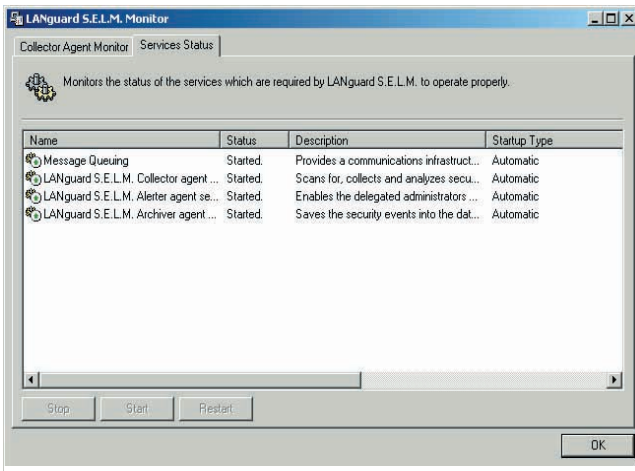
All well and good. But with the above settings, the log file will quickly become full. The default size of these files is not very large. If the size approaches the maximum, the oldest reports will be overwritten. What’s more, there is sometimes default cyclic overwriting after a certain number of days. So if the administrator wants to check the log files for suspect actions, he must do so very regularly and for each individual system. If “somebody” cleans up the log file, however, there will be nothing left to check. Moreover, Microsoft does not always give the clearest of explanations of events, and, even worse, the numbers and IDs of similar types of events differ in Windows NT and Windows 2000. This is not exactly helpful in the mixed environments that are commonplace nowadays. So while a Windows implementation allows you to monitor and save a temporary report on just about everything, it lacks tools for

Production information	
<b>GFI LANguard SELM</b>	
<b>Manufacturer</b>	GFI
	http://www.gfi.com
<b>Price</b>	From \$450,- for 5 servers. From \$125,- for 5 workstations.
<b>Rating</b>	+ Easy to install; once set up SELM monitors the network 24 hours a day, 7 days a week; built-in security intelligence. - A number of systems may be skipped on the initial network inventory; changes to network system configuration have to be made manually.

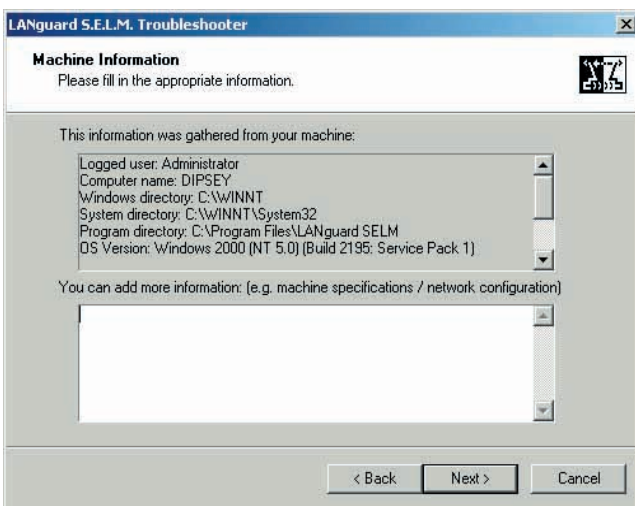
systematically and thoroughly monitoring a large computer base in its entirety. GFI tackled this problem and came up with the LANguard SELM package. The defined goal was real-time monitoring of all Windows NT and 2000 systems in a network. Whenever necessary, the application must generate an alarm to alert the correct person or persons. There was also recognition of the need for a reporting capability covering the combined actions across all computers. The reports need to be transparent and savable over a prolonged period of time and must be editable. To watch over a complete network with LANguard SELM, the software needs to



▲ **Figure 1:**  
**Normal working hours**



◀ **Figure 2:**  
**Services on the Security Station**



◀ **Figure 3:**  
**System information**

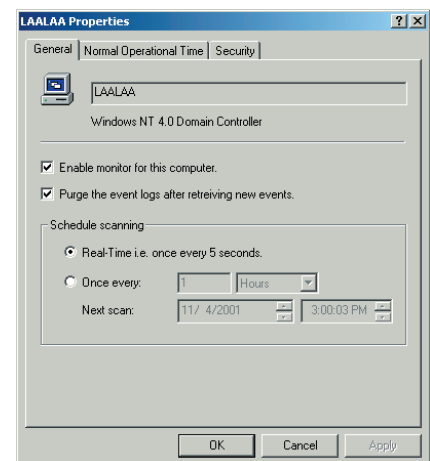
be installed on one system only. It is advisable to install the package on a system that is as secure as possible. This means protected by software and also located at a place with good physical security. There's nothing like a lack of evidence when a crime has been committed. Installation takes place satisfactorily, although the system does have to be restarted in connection with DLLs. This should not be a problem, however, because it is preferably a separate security system. After installation, you must make known to LANguard SELM all systems to be monitored. The package is capable of automatically registering all known systems, i.e. those that are active. Systems can be added and deleted manually. Before starting, it is important to have a good overview of all systems requiring monitoring. Which systems are switched off? What about additions, deletions and

changes? Changes are particularly important, because when SELM sniffs out systems in the network, it detects the type at the same time. A distinction is made between Windows NT and 2000 Server or Workstation/Professional and whether the system is a domain controller. Consequently, the upgrade of PC1234 from NT to 2000 also necessitates a modification in SELM. This is because SELM "translates" the reports in the security log to a similar text for both NT and 2000 computers, while the IDs for identical events between these operating systems are different. To fetch information from the configured systems, SELM uses a Collector Agent to collect events with a standard Win32 API from the systems. The gathered data goes to a database. The database choice is between Access and SQL Server. Separate software does not need to

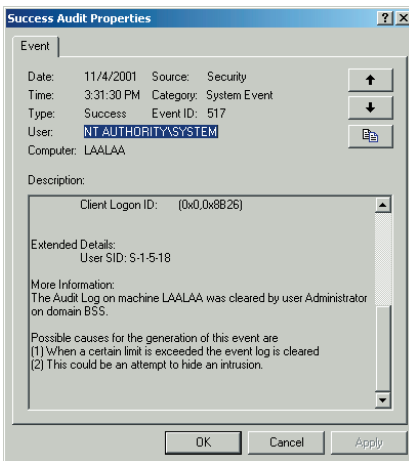
be present for Access, but it obviously does for SQL. Besides the reports built into SELM as standard, an ODBC link theoretically makes it possible to create any type of report in, say, Crystal Reports. Another part of SELM, the Alerter Agent, compares the fetched data with a table that includes rules for determining the seriousness of an event. SELM allocates four levels of seriousness, i.e. Low, Medium, High and Critical. If an event is recognized as critical, a designated person or application will be alerted by SMTP via such means as an SMS message or pager call. It is possible to set the frequency of interrogation of a certain system. SELM will as standard scan a server - and certainly a domain controller - more often than it will scan a workstation. The normal working hours for a system can also be set. Setting these hours means that SELM will not watch the computers outside normal working hours! An event not immediately worrying during normal working hours will certainly be a cause of concern if it occurs outside those hours. Finally, the security level of the entire system can be set according to the Low, Medium, High and Critical statuses.

**Practical**

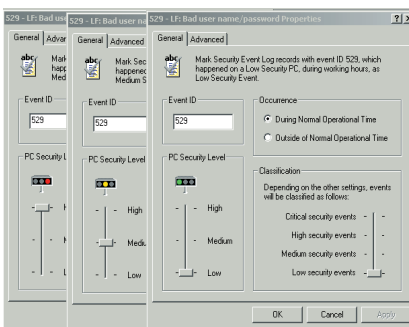
Let's briefly return to the question of working hours, with the help of an example. Windows NT will record a network connection to a shared directory as a 528 event of type 2. An identical action under



▲ **Figure 4:**  
**Settings of monitored systems**



▲ **Figure 5:**  
**Message if event log is cleaned up**



▲ **Figure 6:**  
**Example of standard report**

LANguard Security Event Log Monitor & Reporter			
Users who failed to logon for any reason today			
11/4/2001 12:00:00AM to 11/4/2001 11:59:59PM			
Event IDs covered: 529, 530, 531, 532, 533, 534, 535, 536, 537, 539			
Domain	User Name	Total Events	%
DIPSEY	Yogi	4	100.0%
<b>Total</b>		<b>4</b>	<b>100.0%</b>

▲ **Figure 7:**  
**Same event, different level**

Windows 2000 makes this a 514 event. These are entirely normal events during normal working hours, certainly if the share is on a server. The situation becomes a little different when a share is accessed on a different workstation. As a rule, a user has no business being on a colleague's system. This occurrence may be a break-in attempt, for example, with the aim of assuming somebody else's identity. If this event happens to occur outside normal working hours, the SELM alarm will be generated. SELM considers network log-ons to workstations far more suspicious than a similar

log-on to a server. It classifies these events accordingly. A consequence of this method is naturally that overtime periods must be properly documented and communicated. If they are not, the system may call the administrator in the middle of the night on account of a probable break-in, whereas in fact somebody is simply working longer hours. The administrator can modify the normal working hours of the systems beforehand and reset them later.

SELM uses a number of standard rules to register unsuccessful log-on attempts, blocked accounts, actions after working hours, workstation-to-workstation access, changes to audit policies, security file clean-ups and the accessing of selected files. Depending on the context in which any of these events occurs - e.g. on what type of computer, at what time and similar - the event will be categorized as Critical or lower. In the case of a Critical event, the warning mechanism will be activated and a message will be sent via SMTP. The administrator has a choice of a number of built-in reports to be kept informed also of events of a lower class. The reports include "Yesterday's High Security Events", "Last Week's Medium Security Events" and "Last Month's Low Security Events". Generation of these

reports creates an excellent overview of what has occurred at non-critical level. The reports are ideal for the EDP auditors, too. Running SELM on a separate computer has already been suggested. Besides this condition, there is another crucial condition for meeting the wish to get reports over longer periods of time. This concerns the degree of data protection. Besides a good backup schedule, comprising complete and incremental backups, the data can be protected through replication. A package like NSI's Double Take, capable of replicating at file level, could be helpful.

**Levels**

Monitoring systems obviously comes with a price tag. The administrator responsible for system security must definitely consider the cost. SELM allows the setting of the frequency of sys-

tem interrogation. The higher the system ranks in the security scale - High and, obviously, Critical - the more frequently the system will need to be interrogated. The highest frequency offered by SELM is once every five seconds. If you use this value, SELM will cause a significant network and CPU load, both on the monitored system and on the SELM system. Based on numerous implementations, the supplier has developed a schedule that strikes a good balance between extra load and integrity. With this schedule, the collector visits high-security domain controllers once every minute. At the other end of the scale, low-security level workstations are interrogated only once a day.

An extremely useful feature of SELM - one that even plays an active security role - is how it handles security event files located on the monitored systems. SELM classifies the cleaning up of these log files as a Critical event because Windows keeps track of such actions, even if Auditing has been deactivated. On the systems monitored by SELM, the collector will clean up the event log after it has been read. This automatically means that an unauthorized party cannot obtain via the event log any information that can be used "against the system".

**Conclusion**

LANguard SELM is a tool that can relieve administrators of a great deal of work in these turbulent times. The product installs easily and has MMC plug-ins for fast and simple access. It takes a while to get used to the structure of several screens for the various tasks, but familiarization is fast. Most of the work lies in the preparations that must be made before SELM can do its work. A security plan has to be set up for the network (ITIL helps here). An extensive inventory of all systems and their roles must be compared with the plan to ensure the existence of clear security levels. Then a detailed analysis must be made of the objects that must be monitored with Windows Audit and the target subjects (users and groups) and, finally, the related access types. Once this has been done, LANguard SELM can monitor everything and systematically raise alarms as and when necessary. ▲