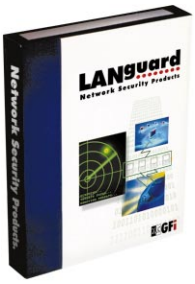


LANguard

Security Event Log Monitor

Intrusion detection using NT/2000 event logs

Many companies mistakenly assume that unauthorized access is only attempted by external parties. Actually, the majority of corporate security threats stem from internal sources, such as users accessing confidential data. Of course, your network provides for security, but many 'backdoors' exist. A firewall offers no protection against attacks from within the company. Furthermore, how can you verify that your firewall is actually blocking out all external attacks?

LANguard S.E.L.M. does this by monitoring the security event logs of all your Windows NT/2000 servers and workstations and alerting you to possible intrusions/attacks in real time. Because LANguard S.E.L.M. is not a network-based IDS, it is not impaired by switches, IP traffic encryption or high-speed data transfer, as are traditional intrusion detection products.

Respond quickly to important events without spending hours examining logs

LANguard S.E.L.M. powerfully expands the basic audit and reporting facilities found in Windows NT/2000 to enable administrators to meet daily business needs. LANguard S.E.L.M. notifies you of critical security events in real time and provides tips for interpreting events in the context of other activity and recommended courses of action. Through LANguard S.E.L.M.'s pre-built event viewer filters, you can quickly check for any high security events on a daily basis and examine medium and low security events on a weekly or monthly basis. Use LANguard S.E.L.M.'s report module for in-depth investigations and trends analysis.

Key features & benefits

- Intrusion detection the right way!
- Network-wide analysis of security logs made easy
- View reports on key security information happening on your network
- Intelligent analysis of security events
- Advanced filtering of security events using the LANguard S.E.L.M. Event Viewer
- Email-based alerts: Send alerts to an email inbox, pager or mobile phone
- No impact on network performance
- Detect web server intrusion/defacement

Intrusion detection the right way!

Many 'network-based' intrusion detection products are difficult to deploy because they work by sniffing network traffic. Switches, traffic encryption (IPsec & SSL) and the sheer high speed of today's networks make network-based IDS products "go blind".

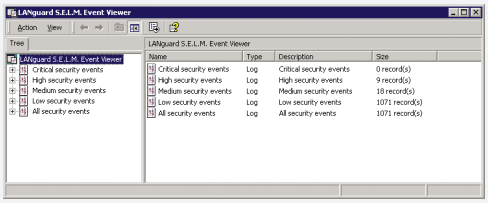
In addition, network-based IDS tools can only look at the bytes of packets sent over the network and therefore can only monitor for attacks/patterns recognizable at the network level - a system that is soon outdated as these patterns are constantly changing. Only a host based IDS can monitor attacks within the context of operating system objects like user accounts, groups and files.

LANguard S.E.L.M. analyses Windows NT/2000 event logs and is not impaired by switches, IP traffic encryption or high-speed data transfer. Since LANguard S.E.L.M. is based on security logs, it can detect vital events relating to an attack, such as failed logons, account lockouts, and more.

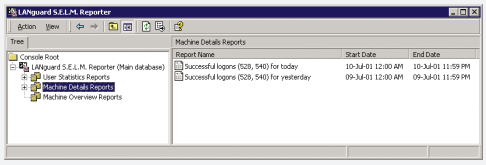
Network-wide analysis of all security event logs made easy!

If you are already using the Windows NT/2000 security logs for analysis, LANguard S.E.L.M.'s automated network-wide analysis has a number of advantages over manual security event log analysis:

- Provides real time monitoring and notification
- Solves fragmented audit trails by consolidating all security events in a single database
- Allows central archiving of events for reporting and backup
- "Translates" the often cryptic descriptions to clear concise explanations and suggestions for action
- Removes "noise" events that make up a large ratio of all security events
- Solves the problem of security log files being tampered with.



A network-wide view of all security events
LANguard's Event Viewer provides a single view of all security events on all your machines, and also offers advanced filtering capabilities.



A partial list of events that LANguard S.E.L.M. monitors:

- Kerberos & NTLM authentication events
- Rights usage and assignments
- Workstations being accessed remotely
- Attacks using local user accounts
- Logon failures occurring in your network
- Accounts getting locked out
- Expired user accounts
- User accounts being created
- Successful logon of an administrator outside office hours
- Account password changes
- Global and local group members being added
- New trusted domain
- User account changed
- Audit log cleared

Insider hacking represents about 70% of all malicious attacks and causes $1 billion of damages each year to US businesses
- Business Week, December 2000

LANguard Security Event Log Monitor is approved by The NSS Group

Requirements

Windows 2000 Pro or server or Windows NT server to run LANguard S.E.L.M.

Servers & clients to monitor must be running Windows NT or Windows 2000

View reports on important security information happening on your network

Use LANguard S.E.L.M.'s powerful reporter to identify key security trends. LANguard S.E.L.M. includes a number of standard reports, which you can customise. LANguard S.E.L.M. also allows you to create custom reports from scratch. Here are a few of the reports included with LANguard S.E.L.M.:

- All failed logons
- Users who failed to logon due a bad username or password for yesterday, past week or month
- All account lockouts for yesterday
- Initial daily logon time for each user for yesterday, past week or month
- Which computers users log into
- Possible security log tampering for today, yesterday, past week or month
- Failed object access events

Intelligent analysis of security events

LANguard S.E.L.M. sifts through all the "noise" in your security logs and just notifies you of the critical events by prioritizing events according to:

- Type of event
- Security level of each computer
- Whether event occurred during normal operating hours
- Role of computer (workstation, member server or domain controller)

LANguard S.E.L.M. also takes into account the differences in how events are logged on NT computers as compared to Windows 2000. Once LANguard S.E.L.M. has analysed events, it categorizes them into 4 different categories: critical, high security, medium security and low security events.

Advanced filtering of security events using the LANguard S.E.L.M. Event Viewer

The Windows 2000 standard event viewer has limited features, and can only view one computer at a time. LANguard's Event Viewer provides a single view of all security events on all your machines, and also offers advanced filtering capabilities. For example, you can filter based on user, computer, PC security level, and more. It also includes a condition builder to enable you to make advanced filters on a combination of these variables.

Email-based alerts: Send alerts to an email inbox, pager or mobile phone

After an intrusion is detected, LANguard S.E.L.M. can alert one or more people by email. Because you can configure multiple email addresses, you can easily set up alerts to be sent to a pager or a GSM phone. Simply direct the email alert to an email-to-pager or email-to-SMS gateway service or to locally installed gateway software. Alerts can be configured based on security level.

Detect web server intrusion/defacement

LANguard S.E.L.M.'s special features for object access auditing allow you to detect web server intrusion and defacement as well track access to critical files on internal servers.

No impact on network performance

LANguard S.E.L.M. has a very efficient event log collector agent, allowing real time collection of security events without impacting network performance. You can adjust the event collection frequency for each computer according the computer's security level and role.

Download your evaluation version from http://www.gfi.com/lanselm

www.gfi.com

GFI Software USA, Inc.
105 Towerview Court
Cary NC 27513,
USA
Tel +1 (888) 2-GFIFAX
Fax +1 (919) 388-5621
sales@gfiusa.com

GFI Software Ltd. UK
5, Princeton Mews
167-169 London Road
Kingston-upon-Thames
Surrey KT2 6PT, United Kingdom
Tel +44 (0)20 8546-0640
Fax +44 (0)20 8546-0741
sales@gfi.co.uk

GFI Software GmbH
Stresemannstrasse 364
22761 Hamburg,
Germany
Tel +49 (0)40 306810-0;
Fax +49 (0)40 306810-10
info@gfigmbh.de

GFI Asia Pacific
Post Office Box 494
HINDMARSH SA 5007
Australia
Tel +61 8 8424-3100
Fax +61 8 8424-3199
sales@gfiap.com

GFI Software Ltd
GFI House
San Andrea Street
San Gwann SGN 05
Malta
Tel: +356 21382418
Fax: +356 21382419
sales@gfi.com