SECURLOG |
EVENT LOG MONITORING

DataComm

SecurLog (Security Event Log Monitoring Agent), is part of DataComm's complete suite of security services and is designed to resolve the challenges of monitoring critical security event logs generated by Windows servers.

SecurLog utilizes specialized monitoring agent and an event alerting process to monitor mission-critical servers' event viewer logs in real-time for policy and security violations, manage complex rule-sets, and maintain logs required by regulators for critical devices. This service keeps your staff informed of critical events occurring on your servers without expensive applications, time-consuming installations, and extensive training.

Our solution is designed to be deployed with low upfront investment costs, no annual software or hardware maintenance subscription fees and rapid deployment with minimal impact to your organization.

DATACOMM'S SECURLOG DELIVERS:

- A dedicated team of security experts
- 24x7x365 log monitoring
- Immediate Critical Alert notification and incident response
- Real- time alerting & notification
- Compliance reporting to meet GLBA, HIPAA, and SOX acts
- An augmented view of changes on your internal network
- Comprehensive Monthly Reporting

DATACOMM'S SECURLOG PROVIDES THE MEANS TO:

- Determine unauthorized access attempts and other policy violations
- Monitor critical servers or Domain Controllers exclusively and set alerts
- Understand server and network activity in real-time
- Log Windows Security Events or critical security events
- View system activity including: logins, user and group account creations and deletions, scheduled tasks, service installations, security incidents, and more…
- Monitor unauthorized Active Directory access permissions
- Log domain access, policy modifications, and user account changes

3 KEY INGREDIENTS

- **Comprehensive Event Collection** - Collects application, system, & security event data on critical Windows devices.
- **Real-time Alerting & Notification** - Alerting allows you to set the specific criteria on Windows devices for which you need to be notified.
- **Compliance Logging & Reporting** - Generate predefined reports to meet HIPAA, GLBA and SarbanesOxley requirements.

The average cost of an attack originating from inside an organization is over $167K, which includes viruses, insider abuse of network access and system penetration.

CSI/FBI Computer Crime and Security Survey Network World

SECURLOG |
EVENT LOG MONITORING

DataComm

How it Works

DataComm's SecurLog deployment staff will assist in the installation of the agent on critical servers. SecurLog will then collect, in real-time, the policy and security events accumulated in the Windows Event or Security Event Log. SecurLog then correlates this information to our filter policies. When a critical event is detected, SecurLog will trigger an alert to be sent through our service ticketing system. DataComm's technical staff then investigates and responds to these alerts

STEP 1 - MONITORING

SecurLog makes the task of monitoring more intuitive byremoving the trivial events that are primarily only informational. Our solution enables you to tighten security policies as necessary. SecurLog Provides Real-Time Detection & Response to the following policy and security events:

- User Account created/deleted
- User Account enabled/disabled
- User Account changed
- Computer Account created/deleted
- Group created/deleted
- Group Changed
- Domain Policy Modified
- A Service was installed
- Scheduled Task Created

STEP 2 - NOTIFYING

With the trivial events cast aside, SecurLog notifies you of critical events that occur on machines monitored with a SecurLog agent. SecurLog keeps track of when events occurred (outside or during operating hours) on each server or domain controller. Once analyzed, the events that are detected and categorized in SecurLog event Alert List, will trigger an alert to be sent via our ticketing system and you will be notified through e-mail or phone call.

STEP 3 - REPORTING

DataComm stores and sends out Windows Monthly Domain Oversight Reports which contain Windows Critical Event data. These reports are stored for purposes of network auditing and more recently to comply with various regulations such as HIPAA, GLBA and Sarbanes-Oxley. DataComm provides reporting and long-term data retention in these ways:

- Email service tickets of critical events
- Monthly archival reports with incident response logs
- Retention of reports and all service tickets for 2 years

A COMMON MISCONCEPTION

Most people think computer break-ins occur only from external sources; malicious individuals trying to break into the network in an attempt to obtain confidential information or financial gains.

The truth is, however, that 70% of attacks originate from the inside. Lack of effective security event log monitoring gives malicious users or naive employees the keys to your data network and exposes your institution to countless business risks.