TELUS®

Security Information and Event Management

A better way to manage event data.

Organizations today must deal with two unfortunate realities: the rising number of increasingly complex security threats and the growing set of demanding and time-consuming compliance requirements.

- **Security threats.** Attacks are targeted, customized and increasingly focused on applications; an area where security is often insufficient. This represents a grave risk as proprietary business processes and confidential data are under constant siege. Many organizations have very limited visibility into the threats targeting their network.
- **Compliance requirements.** Industry and government regulations require that logs be collected, monitored and retained from a broad set of IT systems spanning multiple vendors and versions. To demonstrate due care, logs from hundreds of sources – thousands, in some cases – must be routinely reviewed for security breaches and compliance exceptions. This deep analysis and retention can represent thousands of person-hours and millions of megabytes.

TELUS Security Information and Event Management (SIEM) service deploys the right technology to meet your business and security needs. A log collection appliance will be deployed via cloud or on-premise to collect, aggregate and correlate data from your networking infrastructure, security and application sources. Correlated alerts are sent to our Security Operations Centre where they are analyzed for security relevance by highly skilled and experienced security analysts. They determine the legitimacy and impact of the threat. If warranted, your organization is alerted to begin deeper investigation and remediation of the security issue. Clients can access reports on all events, alerts and incidents 24/7 via an online interface.

Achieve compliance and security objectives.

TELUS SIEM is the most comprehensive, cost-effective way to understand your security, compliance or operational status. With our solution, your organization can:

Capture every event. All logs are retained in unaltered form to ensure forensic and legal validity.

Improve compliance. Logs can be retained as long as required by government and industry regulations.

Reduce cost. This cost-effective solution can collect and process terabytes of logs without requiring investment in a costly storage infrastructure

Identify problems early. Security threats are detected and understood from day one of deployment through the use of preconfigured reports and alerts.

Why TELUS for Security?

We work with each customer to:

- **Assess** your objectives, strategies, drivers, options, associated business and technical risks, and compliance, privacy and security requirements
- **Advise** on a complete end-to-end solution
- **Build** the solution by recommending, procuring and implementing the appropriate technologies
- **Manage** the ongoing effectiveness of your security environment

Through our proven methodologies, we help organizations reduce their security risk, ensure compliance to government and industry regulations, reduce costs of increasingly complex IT and security infrastructures and enable innovation by reducing the threat of security attacks. We provide the visibility, control and understanding organizations require to secure their networks.

future
friendly
enterprise

making more possible today

Visibility, Control and Understanding.

Managed service features:

Design

- Identification of critical log sources
- Development of correlation rules
- Creation of log acquisition methods for non-standard applications
- Planning for performance and capacity
- Planning for high-availability and redundancy

Implementation

- Project management
- Configuration of data sources
- Configuration of log collectors
- Onsite deployment of log collectors
- Verification of collection and correlation functions prior to management cutover

Management

- Alert monitoring and management
- 24x7 health monitoring of source devices and applications
- Ongoing security updates to the platform
- Ongoing maintenance updates to the platform
- Implementation of new correlation rules developed jointly with customer and TELUS security consultant
- 24x7 monitoring of real-time correlation alerts
- 24x7 proactive response to customers on critical threats and alerts
- 24x7 incident handling guidance

Storage and retention

- Retention of logs on the log collectors for near to mid-term retention requirements
- Long-term log retention via cost-effective offline storage (optional)
- Event viewing and reporting
- 24x7 access to real-time event browser
- 24x7 access to standard reports

Supported log sources

- Firewalls
- VPNs
- Intrusion detection systems
- Email security
- Routers and switches
- Wireless security
- Authentication systems
- Vulnerability scanners
- Directory servers
- Operating systems
- Mainframes
- Email servers
- Web servers
- Proxy and caching servers
- Databases
- Custom applications

GET THE BEST FOR YOUR BUSINESS.

See how TELUS Security Information and Event Management can help your organization.

Contact your TELUS Account Executive, call 1-866-GO-TELUS or visit **telus.com/businesssecurity**

future friendly enterprise

making more possible today