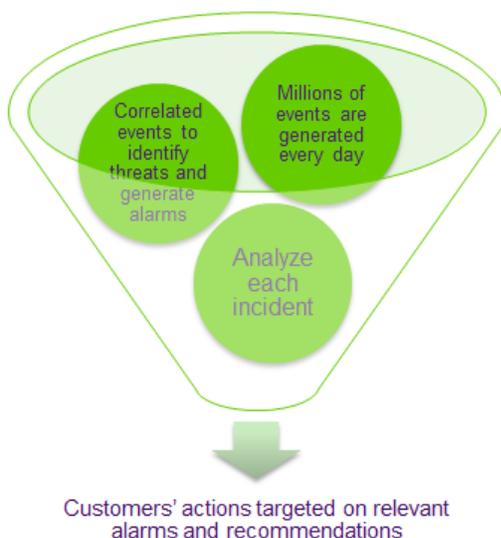# TELUS Managed SIEM.

Supporting better visibility and compliance.

Protecting networks from increasingly sophisticated and concealed security threats, as well as demonstrating those efforts to regulators has become a challenge for organizations overwhelmed by the sheer volume of data available to monitor.

Data in the form of logs are collected through multiple devices on a network. These logs, or records of events, include everything from log-on attempts, configuration changes and system errors. They are tracked through network systems like routers, servers and applications as well as security devices like firewalls and intrusion prevention systems.

Logs can provide clues into security events happening on the network, but to be effective, seemingly unrelated systems and network events need to be aggregated, correlated, rationalized and filtered for specific known threats, user behavior anomalies and other suspicious conditions.

Although many security threats will leave traces of evidence or 'Indicators of compromise', network and IT administrators are challenged with too much disparate data to review and analyze, and do not have time to comb through multiple logs and correlate significant events. Consequently, many security threats go undetected.

Correlated events to identify threats and generate alarms

Millions of events are generated every day

Analyze each incident

Customers' actions targeted on relevant alarms and recommendations

How a SIEM can help

A Security Information and Event Management (SIEM) solution brings efficiency and automation to monitoring security threats by collecting, aggregating and correlating data from a broad set of IT systems spanning multiple vendors and versions. They enable IT staff to focus specifically on potential threats, breaches and suspicious behaviors that could impact the stability of their organization.

TELUS | Business

Challenges with traditional SIEM solutions

Many organizations have made substantial investments in SIEM technologies only to find they did not live up to the promises as advertised. Many SIEM deployments have been ignored or abandoned due to the following challenges:

- High initial capital expenditure.
- Rerouting event information from multiple data sources to the SIEM was time and resource intensive. Deployments were slower than expected.
- Fine tuning alerts and alarms to reduce the noise and produce actionable intelligence was challenging.
- SIEM did not provide visibility into the organization's public and private cloud assets.
- Lack of experienced staff available to manage the solution.

Why choose our Managed SIEM solution

The TELUS Managed SIEM service is different. It is a cloud-based solution, hosted in Canada. It provides you the visibility to detect and prevent potential threats and demonstrate regulatory compliance, while removing the long deployment timelines and challenges of traditional SIEM technologies. Our solution offers:

Better Log Collection, Monitoring and Response	- Broader visibility with a variety of use cases - 24x7x365 log collection and infrastructure monitoring with correlation on logs from all TELUS Managed Security Services. - Real time notification based on severity via telephone, email or reports
More Advanced Security Monitoring on all data	- Monitoring of alarms - Near real-time notification of potential threats and triage - Continuous tuning of Use Cases - Prescriptive response to alerts - Analysis and alerting with recommended actions
More personalized reports through our web accessible Managed Security Services Portal, for example:	- Top Attackers Summary - Summary of top attackers by Origin Host - Top Suspicious Login Summary - Account Management activity - Compliance user Audit failures - New Account Activity - Privileged user activity summary
Ongoing support	- Monthly tuning, action reviews and recommendations meetings

Organizations will benefit from TELUS Security expertise developed over years managing SIEM solutions for similar customers and internally on our own network. You will receive 7x24 monitoring without hiring, training and retaining a full time security staff. And, our flexible payment model provides predictable monthly fees without the up-front capital costs of purchasing and deploying equipment on premise.

GET THE BEST FOR OUR BUSINESS.
See how TELUS Managed Security Information and Event Management can help your organization. Contact your TELUS Account Executive, call 1-866-GO-TELUS or visit telus.com/BusinessSecurity

TELUS | Business