

————— **TIME TO ACTION : DECISIVELY REDUCED**

Security Information And Event Management

Elevated operational efficiency and security empowering informed decision-making and proactive incident management

We've got eyes on it.

Who is watching your infrastructure?

Accelerate your response to cyber incidents with Decisive's cutting-edge detection tools, reducing time to action and minimizing potential damage. Our solution ensures swift identification and remediation of threats, safeguarding your assets with efficiency and precision.

>30,000

SIEM Investigations Performed by the DGI SOC in 2023

>10,000,000,000

Events analyzed per month by DGI SIEM

24/7/365

Eyes on glass monitoring



A platform, not a tool.

Decisive's approach to security monitoring combines multiple industry leading technologies and our own special sauce to provide customized surveillance with proactive detection, allowing you to identify suspicious and malicious traffic as it occurs.

Our tailored approach gives you a single point of integration for all logging activity, flexible deployment, rules and alerting tuned to your specific environment, and around the clock triaged escalations of potential security incidents.

Decisive's SIEM platform provides you with comprehensive network visibility—including users, applications, and infrastructure. Integrations with your existing security controls as well as powerful add-on services to enhance capability make the Decisive SIEM service a force multiplier.

The Decisive SIEM solution does not stop there, allowing for automated response actions across various technologies to stop threat actors in their tracks, and minimize damage.



Service Details:

- Decisive SIEM uses a combination of **best-in-class products** to achieve unique results.
- Ability to **ingest logs across your hybrid environment**; cloud, colo, on-prem.
- Decisive can provide managed SIEM **on premises or in the cloud** for SIEM as a Service (SIEMaaS).
- Hosting provided by **data sovereign** Canadian cloud.
- **Premium threat intelligence** provides a critical data source for correlation against your logs.
- SOAR playbooks to **automate investigative work** for 24/7 monitoring team .
- Additional playbooks which allow for **response actions on common infrastructure** such as firewalls, endpoint security, and active-directory.
- Monitoring runbook for **transparent operations**.
- **Detailed post-mortems** for high priority incidents.
- Custom **secure ingestion pipeline** for your log data.
- Dedicated **Technical Account Manager**.
- **vCISO support** to assist with decision making.

Our Partners:



Our Credentials:

- SOC 2 Type 2
- ISO27001
- ISO27017/ISO27018
- Secret Cleared

Embrace the Importance of Data Resiliency

Decisive Group has you covered

An essential element of data resiliency is the concept of visibility into an organization's network infrastructure. Understanding and maintaining visibility into the flow of data within a network is pivotal for proactive risk management and swift response to potential threats. This visibility empowers businesses to identify anomalies, detect security breaches, and mitigate risks before they escalate into major incidents. In essence, a transparent and well-monitored network serves as the first line of defense, providing a comprehensive understanding of the organization's digital footprint. Decisive Group's Managed SIEM service provides this visibility, coupled with centralized 24/7 monitoring by a team of skilled cyber security analysts.



Prepare Respond Recover

You need the confidence that comes with knowing you are prepared when your data is threatened.



Secure Backup



Managed SIEM



Disaster Recovery



Managed Firewall

How to contact us



1 (855) 336-3700



inquiry@decisivegroup.com



118 Iber Road, Suite 105,
Ottawa, ON K2S 1E9