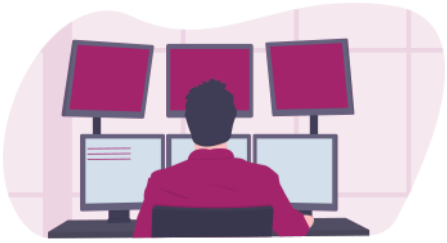
safe tech

Safe-Tech Adaptation is Innovation

The Cybersecurity services SOC NOC, are a necessity for every successful company

SOC-NOC

Security & Network Operation Center by Safe-Tech



The Cybersecurity services, SOC (Security Operation Center) and NOC (Network Operation Center) are a necessity for every company due to the current security threats that circulate through public and private networks. In recent years, administrations that lack sufficient resources have shown significant growth in Security incidents. These security breaches are one of the main causes of information loss, data corruption, economic losses, and the unavailability of computer infrastructure.

Safe-tech is an authorized distribution channel of a SOC-NOC that has the international certifications ISO20000-1 for the Management of IT Services and ISO 27001 for the management of Information Security and CERT that endorses them as an agency of response to security incidents.

These certifications guarantee the operation and delivery of the service at the highest quality under global standards. In addition, the SOC-NOC counts with a group of more than 20 Computer Security Specialists with global security certifications such as ITIL Version 4, Ethickal Hacker, and CISSP among others.

SOC-NOC BENEFITS:

- Real-time visibility of the consumption of infrastructure resources
- Real-time visibility of asset availability
- Real-time visibility of security threats Proactive response to security and continuity events
- Mitigation of security breaches
- Identification of opportunity areas
- Globally Certified Service

+1 (604) 565-5676 | sales@safetechsolutions.ca | http://safetechsolutions.ca | 8120 128th Suite 200 Surrey BC V3W 1R1

24/7 Security, 365 Days a Year

SOC-NOC Platform

Through the Security Platform, SOC-NOC integrates the most advanced technological tools and provides flexibility when enabling its services based on the specific needs of our clients:

- Integration Tool: Integration of logs and log files
- Availability Monitoring Tool
- Threat Intelligence Tool: Security monitoring
- Correlation and Analysis Engine: Next-Generation SIEM
- Automatic Alerts Enabler: Proactive alert system
- Ticket Tracking Tool: Help desk
- Visualization Interface: via web and DashBoards
- Advanced Analysis Tool: Monitoring in Deep Web and Dark Web
- Comprehensive Management System: Management system for operations in accordance with ISO20000-1 and ISO27001

Our services

AVAILABILITY AND HEALTH MONITORING

Do not wait for unavailability events to generate losses. With 24/7 Availability and Health monitoring, you can visualize your resource consumption and the availability of your service-enabling assets.

SECURITY MONITORING

Keep your assets protected against any security incident with 24/7 Security monitoring for the identification of potential threats and availability on your service-enabling assets.

ANALYSIS AND CORRELATION

Stay one step ahead of your attackers by using new generation technological engines. All the traffic of your corporate Network is analyzed and correlated in order to contrast the activity patterns of your organization vs. patterns contained in different logs throughout the world. This allows us to identify security events that have already occurred in different global locations and that could be present in your infrastructure.

MONITORING OF ADVANCED THREATS

Identify behavioural patterns of your infrastructure and its interaction towards malicious entities on the Web, Deep Web and Dark Web. This allows us to maintain the security of your company and adherence to the correct use of Internet resources.

CYBER DEFENCE

This service provides an effective cyber defence by identifying:

- Cyber incidents
- Vulnerabilities
- Targeted attacks
- Campaigns, phishing (web, domains, and applications)
- Information disclosure
- Programming code release
- Compromised credential identificationIllegal sale of products and services
- Unauthorized use of your brandNegative mentions that affect your infrastructure

PENETRATION TESTING

Make sure your assets are adequately protected by testing your network computer systems or web applications for vulnerabilities that an attacker could exploit.

VULNERABILITY ANALYSIS

Do not allow cybercriminals to take advantage of your weaknesses by identifying security gaps in the organization's monitoring and mitigation assets.

INCIDENT MANAGEMENT

Make sure security incidents have the least impact on your organization. Through our incident response team, we will provide you with appropriate treatment and response to avoid recurring problems of this nature.

safetech