Your Trusted Cyber Security Partner

Cyber Security Threat Protection: Strengthen Your Defences!

A proactive approach to cyber security is essential to locating and identifying your system's potential vulnerabilities before hackers can exploit them. Cover-All offers Cyber Security services and technology solutions in partnership with CyberWolfe. Our Cyber Security Operations Centre located in Cover-All's Data Centre can help you strengthen security and regulatory compliance.

COVERALL
Managed Cloud and IT Services

CyberWolfe
Innovative Cyber Security Services

1-833-268-3788

Maintain Security and Compliance Standards

Technology is an essential component of providing positive customer experiences. Yet a business is estimated to fall victim to a ransomware attack every 11 seconds. The cost of these attacks is estimated at approximately $6 trillion, which can seriously impact customer trust and profitability. As the sophistication of corporate information technology environments increases, so does cyber security criminals' ability to adapt quickly to develop new ways to penetrate corporate and public systems.

Cyber security must be built on the foundation of trust and resilience. Our strategic partnership with CyberWolfe gives us the ability to provide our clients with innovative zero-trust cyber security and risk mitigation solutions that offer proactive cyber security defences. With a proven track record of providing over 300 Canadian-based businesses with solutions to meet their unique business needs, our threat intelligence specialists are ready to help your business identify risks and maintain security and compliance standards. We can help mitigate the risk of data breaches, including:

- ✓ Ransomware
- ✓ Malware
- ✓ Phishing
- ✓ Denial of Service

Trusted Managed Cyber Security Operation Centre Services

Cover-All's Cyber Security Operations Centre offers a complete range of cyber security services to ensure you maintain security and regulatory compliance and protect your brand reputation.

Log Management is essential in ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Our team can perform routine log analysis to identify security incidents, policy violations, fraudulent activity, and operational problems.

Managed Monitoring is the process of continuously observing an IT system to detect data breaches, cyber threats, or other system vulnerabilities. Our team can monitor and provide your IT team with proactive cyber security alerts to network usage anomalies, thereby allowing your team to investigate and determine if a threat exists so they can take decisive action.

Managed Detection and Response (MDR) is a managed cyber security service that provides intrusion detection of malware and malicious activity in your network and assists in rapid incident response to eliminate those threats with succinct remediation actions. Our highly skilled security analysts use specialized technology to uncover threats, extending the tools available to your IT team.

Active Threat Hunting is the process of proactively searching through networks or datasets to detect and respond to advanced cyber threats that evade traditional security controls. Our experienced cyber security analysts will proactively search for and identify security incidents or threats currently deployed that automated detection methods did not identify. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defences.

Vulnerability Management helps to proactively review for flaws in your code or design that may compromise the security of an endpoint or network. This includes checking for, identifying, and mitigating vulnerabilities.

E-mail monitoring provides a wealth of information on individual users and departments to help prevent a security compromise or the loss of sensitive information.

Endpoint security management is a policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources. Our team can utilize endpoint security management tools to manage and control computing devices requesting corporate network access.

Threat assessment evaluates events that adversely affect operations and/or specific assets. Our team is highly trained in evaluating security threats and will evaluate historical information, a primary source for threat assessments. A comprehensive threat assessment considers actual, inherent, and potential threats.

Security awareness training is a strategy IT security professionals use to prevent and mitigate user risk. An IBM study found that 95% of cyber security breaches resulted from human error. Our security awareness training can help employees understand their role in helping combat information security breaches.

Shared Visibility allows organizations to identify, assess, monitor, and respond to cyber threats. Our team can provide network visibility, helping you detect policy issues and cyber threats to protect and prevent service-impacting issues.

Integration Intrusion Detection Systems (IDS) analyze network traffic for signatures that match known cyberattacks. An IDS uses integrated intrusion signatures to identify potentially malicious activities capable of damaging your network. Intrusion Prevention Systems (IPS) also analyzes packets but can also stop the packet from being delivered based on what kind of attacks it detects — helping stop the attack. Our intrusion prevention systems work by scanning all network traffic, helping to prevent threats, including:

- ✓ Denial of Service (DoS) attack
- ✓ Distributed Denial of Service (DDoS) attack
- ✓ Various types of exploits
- ✓ Worms
- ✓ Viruses

User Behaviour Analytics (UBA) is a cyber security process that helps to detect insider threats, targeted attacks, and financial fraud. Our team can analyze patterns of human behaviour and apply algorithms and statistical analysis to detect meaningful anomalies from those patterns to detect potential threats.

We also offer penetration testing, vulnerability assessments, and ransomware protection.

Our cyber threat intelligence specialists are ready to help. Call us at 1-833-268-3788 to discover how we can mitigate your organization's cyber security risks.

Managed Mainframe Services
Mid-range and Open Systems Services
Managed Cloud Services
Cyber Security Services
Co-Location Services
Backup & Recovery/DR Services
Cloud & IT Consulting Services

Call to discover how we can help your business!

Visit our website

https://www.coverallmcits.ca/

Follow us on LinkedIn

1-833-268-3788