Senior Security Analyst

Who are we?

Have you ever wondered what makes trading and settlement possible in Canada? It's Fundserv—the online ecosystem that ensures every fund transaction is processed timely, accurately and securely. We're an online hub that electronically connects manufacturers, distributors, and intermediaries, enabling them to buy, sell, and transfer investment funds.

Our Culture & Values

Fundserv is guided by our four core values: Collaboration, Adaptability, Integrity, and Respect. Because above all else, Fundserv CAIRs:

- Collaboration
- Adaptability
- Integrity
- Respect

Benefits & Perks

Fundserv provides a comprehensive benefits plan that includes the following:

- Health care spending account
- RRSP with employer match
- Annual performance pay
- Fitness reimbursements
- Employee discount program
- Charitable donation matching
- Flexible hours & remote work options

To better support our employees during Covid-19, we've expanded our benefits:

- Virtual social events including escape rooms, online trivia & games
- Corporate-wide mental health days
- Subscription reimbursement for fitness, nutritional, and mental health apps

Location:

Downtown Toronto (remote until further notice)

Reports to:

Manager, Infrastructure Security

Department:

Infrastructure Security

Fundserv is an equal opportunity employer. We welcome and encourage applications from individuals with disabilities. Accommodations are available on request – please let us know how we can meet your needs.

The Opportunity

Fundserv is embarking on a multi-year, multi-million-dollar technology transformation program that focuses on currency, resiliency, security and agility. This ambitious transformation will completely redesign every façade of Fundserv's platform. We follow the Agile methodology principles, the collaborative practices of DevSecOps and will be leveraging the latest technologies and tools, such as a hyper-converged infrastructure, software-defined network, cloud, containers and APIs, enabling Fundserv to serve the industry better, and adapt to this ever-changing technology and investment landscape.

In this role you will:
The Security Analyst plays critical role at Fundserv. Responsible for analyzing and maintaining the security and integrity of Fundserv's network and systems infrastructure, this position requires an understanding of Information Systems as they relate to security and networks, systems, and sensitive data in a rapidly transforming hybrid environment. Working with Network, and Systems Support teams, the incumbent will Identify and help mitigate security issues, misconfigurations, and vulnerabilities related to Fundserv's on-prem and cloud infrastructure. The Security Analyst will apply their in-depth knowledge of operating systems, infrastructure and cloud providers, thinking like both an attacker and defender to help come up with proactive and preventative security measures to keep Fundserv technology secure in an ever-changing threat landscape.

- Investigate and advise on latest security related risk, threats and vulnerabilities security incident management, external security reviews and penetration tests to ensure infrastructure security posture is strong
- Collaborate on Information Security policies, standards, and baselines and contribute efforts to measure compliance.
- Monitor, assess, and preform network penetration tests, vulnerability assessment scans and risk assessment reviews.
- Define and report key security metrics to drive remediation trends.
- Provide pro-active network monitoring of security applications, devices and connectivity. Monitor for errors, tool availability and resolve issues.
- Manage operational workflows including Access Mgmt., Physical security, vulnerability remediation. Contribute to improvement/automation of processes.
- Report on findings and advise stakeholders in remediation activities as required.
- Document processes/procedures in accordance with Fundserv reporting standards.
- Collaborate with the IT Operations, architecture and project teams to engineer and implement security controls based upon policies, standards, and best practices.
- Facilitate and coordinate vulnerability assessment, reviews of assessment results, patching, and advice or conduct remediation activities related to BU OS, Middleware, Unix/Linux Servers, Storage, Databases, Appliances, Web Applications and Network Devices, malware tools, IDS/IPS, encryption, and other IT infrastructure technologies.
- Collaborate on and provide results and metrics for consistent reporting for governance purposes; collaborate and coordinate remediation plans and activities.
- Research and develop testing tools, techniques, and process improvements.
- Adequately explains, presents, demonstrates [when applicable] and documents the operational impact of a particular security loopholes or vulnerabilities.
- Analyze vulnerability results and recommend corrective action and hardening.
- Provide guidance and share knowledge with other members of the team.
- Understand the Scope of Work for engagements
- Proactively identify security risks and provide Security requirements and controls to mitigate these risks.
- Perform duties and tasks required in secure, organized and professional manner.

Why YOU are the person we're looking for

- Bachelor's Degree in Science, Engineering, or equivalent
- 4+ years progressive experience in IT Security
- CISSP, GSEC or other relevant certifications
- Demonstrated experience defining, maintaining and enforcing security best practices
- Working knowledge of industry-recognized tools, including: Middleware, Servers (Linux/Windows), Storage, Databases, Appliances, Web Applications, Network Security Devices, Cisco ACI, Nutanixs, Azure Cloud Platform, CyberArk, SCCM, Intune, Microsoft Endpoint Management, Palo Alto and Fortinet firewalls
- Broad understanding of the current cyber security landscape, with a background in networks & server/system management and Azure Cloud Security , and an in-depth understanding of Zero Trust and SASE security models
- Strong knowledge in Authentication, End Point Security, Internet Policy Enforcement, Web Content Filtering, Public Key Infrastructure (PKI), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions, VMs and common networking services and protocols (TCP/IP, SSH, FTP, DNS, DHCP, SMTP, SSL)
- Working knowledge of Information Security best practices, policies, standards, and baselines, including industry standards/guidelines from ISO 27001/27002, NIST, CIS, and OWASP

If this sounds like you, apply today at hiring@fundserv.com.