

Position: Senior Systems Administrator, Security Operations
Reports to: Manager, Security Operations and Compliance
Contract type: Indefinite; Full Time

The Chartered Professional Accountants of British Columbia (CPABC) is seeking a highly organized and analytical individual with excellent attention to detail for the Senior Systems Administrator role. We are proud and honoured to have been recognized as one of BC's Top Employers for a fourth consecutive year in 2023. Come join a collaborative network of like-minded professionals and take the first step towards an exciting opportunity by applying to the position.

Job Summary

Reporting to the Manager Security Operations and Compliance (MSOC), the Senior Systems Administrator, Security Operations (SSASO) role will focus on CPABC's IT security, with the two primary areas of responsibility being security & compliance, and ongoing security operations. Working alongside the MSOC and Security Analyst (SA), the SSASO will be responsible for helping to ensure CPABC meets our compliance requirements and configuring and supporting our security systems and tools.

Key Responsibilities:

Security and Compliance

- Review our security alerts and log files, along with daily reviews of the SIEM dashboard and logs.
- Utilize our cloud security posture management tools to monitor, analyze and report on the security of our cloud infrastructure, identifying potential misconfigurations and recommending solutions as appropriate.
- Research, recommend and assist in the implementation of new technologies to support CPABC's security and privacy needs, ensuring IT policies are implemented and adhered to.
- Perform security risk assessments on new and existing applications and infrastructure, making recommendations for security risk reduction & mitigation.
- Participate in compliance reviews (e.g. PCI's SAQ-D questionnaire review, penetration testing, security reviews, etc.) to help ensure the organization remains PCI and FOIPPA compliant.
- Participate in the development, maintenance, and periodic testing of CPABC's Disaster Recovery Plan and procedures.
- As a key member of the Cybersecurity Incident Response Team (CIRT), work alongside our IT Operations team to perform remediation tasks while participating in periodic response plan tests.
- Define and implement alerting and monitoring standards for CPABC systems and services / applications, fine-tuning alerts and responding to incidents while maintaining responsibility for monitoring the systems and applications.
- Maintain awareness of current PCI requirements as well as emerging threats and vulnerabilities, deploying hotfixes, patches, firmware releases and configuration changes as necessary.
- Contribute to the revision of security policies and procedures, including the development and maintenance of an IT Sec Ops' procedures manual.
- Work with our 24x7 SOC service provider

Ongoing Security Operations

- Support CPABC's other Systems Administrators with the management and configuration of the organization's Mobile Device Management solution.
- Configure Endpoint detection rules, configurations, hardening and documentation.
- Recommend, design, and participate in the implementation and management of CPABC's security solutions, including those within the M365 environment (e.g. anti-malware and anti-spam, HIPs, Windows Firewall, Azure Active Director, Microsoft Endpoint Manager, Microsoft Cloud App Security, etc.).
- Perform patches and upgrades of OS, applications, and devices, as required.
- Employ various practices such as OS hardening, patch-level scanning, PCI-compliance scanning, etc.



- Participate in the integration of cloud services (e.g. Azure, AWS, Office 365, DRaaS, etc.).
- Configure, administer, and support enterprise-class security solutions (e.g. Device Control, SIEM).
- Provide Tier 2 support and backup coverage for CPABC's other Systems Administrators and Technical Support Specialists.
- Other duties and responsibilities as may be assigned from time to time.

Key Requirements:

Key Requirements

- MCSE Server Infrastructure certification is required;
- Seven (7) plus years of relevant, related working experience;
- Five (5) plus years of experience in the following areas:
 - Configuring and maintaining enterprise-class anti-malware and firewall solutions;
 - Working with threat monitoring and management tools.
 - Working with enterprise-class virtualization technologies
 - Working with general IT infrastructure technologies physical and virtual
- Three (3) plus years of PCI-DSS implementation and maintenance experience
- A deep, thorough knowledge of security principles, solutions, and implementation
- A fair knowledge of SIEM systems
- Prior experience with IT auditing
- Proven experience with Windows Server 2012/2016, Active Directory, DNS and MS SQL (2012/2016);
- Experience working with Linux-based systems including OS management
- Experience working with incident response plans and disaster recovery plans.
- Ability to quickly identify and analyze problems and recommend appropriate solutions;
- Excellent interpersonal and communication skills, both verbally and written;
- Ability to work collaboratively as a key member of a team and independently with minimum supervision;
- Diplomatic, tactful and professional approach;
- Proven ability to prioritize competing requirements and deadlines under pressure;
- Ability to periodically work overtime and outside of normal business hours, as required.

Nice to Haves

The following items would be considered an asset, but are not required:

- VMware VCP-DCV certification or equivalent Microsoft certification;
- A+ certification;
- Experience working with AWS or Azure;
- Experience or understanding of FOIPPA;
- CISSP, CISA or GSEC certification;
- PCI Internal Security Assessor (ISA) qualification.

If this job outline describes you, please email your **résumé** to HRCPABC@bccpa.ca by **Wednesday, March 15, 2023**.

We thank in advance all candidates who respond; however, only those selected for interviews will be contacted.

Why join our team? CPABC offers an entrepreneurial environment with a competitive compensation package. At CPABC we live our core values:

- *We Are Open*
- *We Work Together*
- *We Communicate*



- *We Improve Every Day*
- *We Are Professional*
- *We Laugh and Celebrate*

About CPABC

The Chartered Professional Accountants of British Columbia (CPABC) is the training, governing, and regulatory body for over 39,000 CPA members and 6,000 CPA students and candidates. CPABC carries out its primary mission to protect the public by enforcing the highest professional and ethical standards and contributing to the advancement of public policy. CPAs are recognized internationally for bringing superior financial expertise, strategic thinking, business insight, and leadership to organizations. CPABC is proud to have been presented with a fourth consecutive BC Top Employer award in 2023.