1. Career Opportunities: Specialist; Cybersecurity Systems (2891)

Requisition ID **2891** - Posted **02/05/2024**

Job Summary

Responsible for protection of system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. This includes designing and managing computer security architecture and developing cyber security designs as per the established security requirements.

Key responsibilities.

- To design, implement and enforce IT Security Policies to ensure alignment with related corporate policies.
- To understand and provide expert advice on the ICT security risks facing information assets.
- To be responsible for the technical IT security strategy, proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- To be responsible for forensic investigation of IT security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- To coordinate regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Implement technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks
- To administrate and monitor using specific IT Network Security applications including [but not limited to] the company -wide antivirus, email encryption, Data Loss prevention, file screening, server audit, and host protection systems. This requires continuous re-assessment of suitability for purpose and making or recommending any required changes.
- Run various assessment tools to obtain insight on security posture and create various reports for management and stakeholders.
- Provide remediation consultation to global teams to support enterprise risk reduction efforts
- Monitoring of all IT assets on configuration integrity in order to proactive manage the bank's environment.
- Engineer, implement and monitor security measures for the protection of computer systems, networks and information assets.
- Identify and define system security requirements standards of the bank.
- To be responsible for regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Hardening of all IT assets before promoted to production environment. Formal checklist will be used for installation/changes of any configuration in the bank's environment for a new/existing setup.
- Help enhance and maintain current hardening standards for all information assets this includes but not limited to servers, workstations, databases, audio visuals and network devices.
- Support penetration testing activities and exercises.

- Recommend through assessment-based findings, outcomes, and propositions for further system security hardening enhancement.
- Reviewing configuration API and PKI of the bank to ensure its compliance to the established standard on regular basis.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters as per the SAT program.
- Monitor internal and external policy compliance and cybersecurity framework is being complied by both vendors and employees.
- Implement new technology on the network security and ensure security hardening and effectiveness of the control. Implement and Ensure compliance of Cybersecurity framework amongst the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff knows his or her duties during such an incident.
- Prepare and report all security incidents to the ICT Management or as directed by line manager.
- Real time monitoring of network user activities.
- Work with different units in the department to reduce systems configurations risk.
- The CRDB Bank Management may assign other responsibilities as needed.

Qualifications

- Bachelor's degree in computer systems technology or related academic field.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, etc.
- At least 3 years of general ICT Security experience in banking environment.
- Expert knowledge of current IT cyber security issues
- Management of a complex IT Infrastructure within large enterprise level organization.
- Contingency and Disaster Recovery Planning.
- Up to date knowledge of technical applications
- Ability to think ahead and anticipate problems, issues, and solutions
- Experience providing IT focused Enterprise Architecture and strategy.
- Windows Operating systems and Active Directory Management
- Anti-Virus domain infrastructure

Deadline 14th February 2024

To Apply, **CLICK HERE**

2. Career Opportunities: Specialist; Cyber Threat Hunting (2890)

Requisition ID **2890** - Posted **02/05/2024**

Job Summary

Responsible for protection of system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. This includes designing and managing systems security architecture and developing cyber security designs as per the established security requirements. Ensuring security minimum requirements and best practices are applied consistently across existing and new systems.

Key Responsibilities

- To implement and enforce Cyber security Policies to ensure alignment with related corporate policies.

- To understand and provide expert advice on the Cyber security risks facing information assets.
- Responsible for the technical Cyber security strategy – proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- Responsible for forensic investigation of Cyber security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- To coordinate regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Implement technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
- To administrate and monitor the infrastructure using specific Cyber security applications including [but not limited to] the company -wide antivirus, email encryption, Data Loss prevention, file screening, server audit, and host protection systems. This requires continuous re-assessment of suitability for purpose and making or recommending any required changes.
- Run various assessment tools to obtain insight on security posture and create various reports for management and stakeholders.
- Provide remediation consultation to global teams to support enterprise risk reduction efforts.
- Monitoring of all IT assets on configuration integrity in order to proactive manage the bank's environment.
- Engineer, implement and monitor security measures for the protection of computer systems, networks and information assets.
- Identify and define system security requirements standards of the bank.
- To be responsible for regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Hardening of all IT assets before promoted to production environment. Formal checklist will be used for installation/changes of any configuration in the bank's environment for a new/existing setup.
- Help enhance and maintain current hardening standards for all information assets this includes but not limited to servers, workstations, databases, audio visuals and network devices.
- Support penetration testing activities and exercises, including self-capacity to perform penetration testing.
- Recommend assessment-based findings, outcomes, and propositions for further system security hardening enhancement.
- Reviewing configuration APIs and PKIs of the bank to ensure its compliance to the established standard on regular basis.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters as per the SAT program.
- Monitor internal and external policy compliance and cybersecurity framework is being complied by both vendors and employees.
- Implement new technology on the network security and ensure security hardening and effectiveness of the control. Implement and Ensure compliance of Cybersecurity framework amongst the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff knows his or her duties during such an incident.
- Prepare and report all security incidents to Management or as directed by line manager.
- Real time monitoring of network and systems user activities.
- Work with different units in the department to reduce systems configurations risk.
- The CRDB Bank Management may assign other responsibilities as needed.

Qualifications

- Bachelor's degree in computer systems technology or related academic field.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, etc.
- At least 3 years of general ICT Security experience in banking environment.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.

- Expert knowledge of current IT cyber security issues
- Management of a complex IT Infrastructure within large enterprise level organization.
- Contingency and Disaster Recovery Planning.
- Up to date knowledge of technical applications
- Ability to think ahead and anticipate problems, issues, and solutions
- Experience providing IT focused Enterprise Architecture and strategy.
- Windows Operating systems and Active Directory Management
- Anti-Virus domain infrastructure

Deadline 14th February 2024

To Apply, **CLICK HERE**

3. Career Opportunities: Manager; Cyber Threat Hunting (2889)

Requisition ID **2889** - Posted **02/05/2024**

Job Summary

Responsible for protection of system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. This includes designing and managing systems security architecture and developing cyber security designs as per the established security requirements. Ensuring security minimum requirements and best practices are applied consistently across existing and new systems.

Key Responsibilities

- Formulate and update threat hunting strategies to stay ahead of evolving cyber threats.
- Manage Threat Intelligence through incorporation of threat intelligence into threat hunting processes to identify potential cyber risks.
- Supervise and lead a team of threat hunters, providing guidance and support.
- Deploy and manage advanced threat detection tools and techniques.
- Conduct regular incident response drills and simulations.
- Collaborate with SOC teams to integrate threat hunting findings into overall incident response and mitigation efforts.
- Conducting post-incident analysis to identify areas for improvement and lessons learned.
- Collaborate with external cybersecurity communities, organizations, and law enforcement agencies to share threat intelligence and enhance the Bank's cyber resilience.
- Responsible for the technical Cyber security strategy – proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- Responsible for forensic investigation of Cyber security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- To coordinate regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Implement technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
- Run various assessment tools to obtain insight on security posture and create various reports for management and stakeholders.
- Provide remediation consultation to global teams to support enterprise risk reduction efforts.

- Monitoring of all IT assets on configuration integrity in order to proactive manage the bank's environment.
- Engineer, implement and monitor security measures for the protection of computer systems, networks, and information assets.
- Identify and define system security requirements standards of the bank.
- To be responsible for regular security testing with high quality reporting. Responsible for the subsequent hardening of IT systems based on results of regular tests.
- Help enhance and maintain current hardening standards for all information assets this includes but not limited to servers, workstations, databases, audio visuals and network devices.
- Support penetration testing activities and exercises, including self-capacity to perform penetration testing.
- Reviewing configuration APIs and PKIs of the bank to ensure its compliance to the established standard on regular basis.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters as per the SAT program.
- Monitor internal and external policy compliance and cybersecurity framework is being complied by both vendors and employees.
- Implement new technology on the network security and ensure security hardening and effectiveness of the control. Implement and Ensure compliance of Cybersecurity framework amongst the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff knows his or her duties during such an incident.
- Prepare and report all security incidents to Management or as directed by line manager.
- Real time monitoring of network and systems user activities.
- Work with different units in the department to reduce systems configurations risk.
- The CRDB Bank Management may assign other responsibilities as needed.

Qualifications

- Bachelor's degree in computer systems technology or related academic field.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, etc.
- At least 5 years of general ICT Security experience in banking environment.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.
- Technical handling interaction with vendors, contractors, and other stakeholders
- Expert knowledge of current IT cyber security issues
- Management of a complex IT Infrastructure within large enterprise level organization.
- Contingency and Disaster Recovery Planning.
- Up to date knowledge of technical applications
- Ability to think ahead and anticipate problems, issues, and solutions
- Experience providing IT focused Enterprise Architecture and strategy.
- Windows Operating systems and Active Directory Management
- Anti-Virus domain infrastructure

Deadline 14th February 2024

To Apply, **CLICK HERE**