IT SECURITY ANALYST: $125.00/hour

Specific responsibilities can vary from position to position; their duties can include:

- Plan, implement and upgrade security measures and controls
- Protect digital files and information systems against unauthorized access, modification or destruction
- Maintain information security and monitor access
- Conduct internal and external security audits
- Manage network, intrusion detection and prevention systems
- Analyze security breaches to determine their cause
- Recommend and install appropriate tools and countermeasures
- Define, implement and maintain corporate security policies
- Security awareness training
- Coordinate security plans with outside vendors

Key technical skills include:

- Application Security Support
- Data Loss Prevention (DLP) scanning and reporting
- Endpoint Protection (Anti-Malware)
- Intrusion Detection
- Firewall monitoring and reporting
- Forensics Analysis
- Incident Response
- Penetration testing of network, applications, and infrastructure
- Security assessments of network, applications, and infrastructure
- Security Operations Center (SOC) Support Services
- Social engineering Penetration Testing
- Vulnerability and Threat Assessments, monitoring and reporting

IT SECURITY ENGINEER: $150.00/hour

Specific responsibilities can vary from position to position; their duties can include:

- Develop and carry out information security plans and policies
- Maintain security control systems (e.g., configuration, updates, etc.)
- Develop strategies to respond to and recover from a security breach
- Develop or implement open-source/third-party tools to assist in the detection, prevention, and analysis of security threats
- Awareness training of the workforce on information security standards, policies and best practices
- Implement protections
- Installation and use of firewalls, data encryption, and other security products and procedures
- Conduct periodic network scans to find any vulnerability
- Conduct penetration testing, simulating an attack on the system to find exploitable weaknesses
- Monitor networks and systems for security breaches, through the use of software that detects intrusions and anomalous system behavior
- Investigate security breaches
- The lead incident response, including steps to minimize the impact and then to conduct a technical and forensic investigation into how the breach happened and the extent of the damage

Key technical skills include:

- Expertise in anti-virus software, intrusion detection, firewalls and content filtering
- Knowledge of risk assessment tools, technologies, and methods
- Expertise in designing secure networks, systems and application architectures
- Disaster recovery, computer forensic tools, technologies and methods
- Planning, researching and developing security policies, standards, and procedures
- System administration, supporting multiple platforms and applications
- Expertise in mobile code, malicious code, and anti-virus software
- The IT security engineer should also have experience with and knowledge of:
- Endpoint security solutions, including file integrity monitoring and data loss prevention
- AWS and cloud platform as a service (PaaS) security
- Automating security testing tools
- Chef – a configuration management tool
- Git – a tool that helps track anomalous changes to files

HELPDESK PHONE SUPPORT	EMAIL THE HELPDESK	EMAIL SALES	EMAIL BILLING
225-761-0088 Option 1	helpdesk@tfmx.com	sales@tfmx.com	billing@tfmx.com

transformyx.com   225-761-0088

IT SECURITY ARCHITECT: $175.00/hour

Specific responsibilities can vary from position to position; their duties can include:

- Design, build and implement enterprise-class security systems

- Align standards, frameworks, and security with overall business and technology strategy

- Identify and communicate current and emerging security threats

- Design security architecture elements to mitigate risks as they arise

- Create solutions that balance business requirements with information and cybersecurity requirements

- Identify security design gaps in existing and proposed architectures and recommend changes or enhancements

- Training users in implementation or conversion of systems

Key technical skills include:

- Security architecture, demonstrating solutions delivery, principles and emerging technologies - Designing and implementing security solutions. This includes continuous monitoring and making improvements to those solutions, working with an information security team.

- Consulting and engineering in the development and design of security best practices and implementation of solid security principles across the organization, to meet business goals along with customer and regulatory requirements.

- Security considerations of cloud computing: They include data breaches, broken authentication, hacking, account hijacking, malicious insiders, third parties, APTs, data loss and DoS attacks.

- Identity and access management (IAM) – the framework of security policies and technologies that limit and track the access of those in an organization to sensitive technology resources.

CISO: $225.00/hour

Specific responsibilities can vary from position to position; their duties can include:

- Participate and provide consulting on executive-level initiatives such as program, plan, budget and policy review.

- Creation and maintenance of an industry-specific Information Protection Program.

- Implement and maintain an industry-specific compliance/security risk management framework.

- Establish and maintain key risk indicators, reporting, and monitoring as part of the measure and manage objectives of the Information Protection Program.

- Establish and maintain the Security Education, Training and Awareness (SETA) Program.

Key technical skills include:

- Over fifteen years of experience in cybersecurity and compliance

- Holds CISSP and other relevant security certifications

- Holds a master degree in related fields

- Specialization in industry-specific compliance and security risk management frameworks

- Served as CISO for more than seven years

IT SECURITY ENGINEER EXPERT: $225.00/hour

Cisco Certified Internetwork Expert (Security) and 10 years' experience

- Evaluate Customer technologies and architectures regarding infrastructure needs.

- Interface with management and vendors to develop and implement new solutions to meet business requirements.

- Design and manage the rollout of critical network infrastructures to support products and services, on both a strategic (long-term) and tactical (immediate term) level.

- Perform analytical, technical, cost analysis and CAPEX development work in the planning, design, installation and on-going administration and management of core data, broadband and softswitch (VoIP) networks.

- Ensure that network infrastructure is fully documented and performing as required for internal and customer SLA guarantees and expectations using specific metrics and measurements.

- Provide technical expertise and support to Operations in the ongoing maintenance and surveillance of related networks and applications.

- Provide technical expertise to Product Development to develop new product strategies and enhance existing product sets.

- Demonstrated in-depth knowledge of LAN/WAN support and engineering design for voice, data and video networks at Access,

- Aggregation, and Core network locations

- Thorough understanding of modern service provider TCP/IP data networks using standards and technologies including but not limited to MPLS, IS-IS, OSPF, BGP4, STP, RSTP, 802.1q, 802.1ah, SIP

- Superior knowledge, skills, and experience with Cisco routing hardware, software, protocols, softswitches, Session Border Controllers, firewalls, etc.

- Strong working knowledge of structured cabling systems, network facilities, electrical, UPS, etc.