APPENDIX ONE:
Job Description

POSITION TITLE:	Cyber Security System Engineer
LOCATION:	Information Technology Solutions, Tauranga
REPORTS TO:	Infrastructure and Service Delivery Manager

POSITION SUMMARY

Working with the latest technologies, the Cyber Security System Engineer's primary focus is to work with internal Craigs Investment Partners (CIP) teams and 3rd party specialist security service providers to monitor, detect and respond to events impacting the security of CIP.

CIP's ICT services encompass an infrastructure inclusive of Virtual and physical Desktops, Server, Application, Network and Telecommunications and WAN/SDWAN areas. The role's responsibilities cover Cyber Security across all of these service areas to ensure maximum protection and ultimately availability of ICT services to the business users in alignment with the IT SLA with the business.

The Cyber Security System Engineer will work closely with the other members of the Infrastructure and Service Delivery Team and overall Technology Department, supporting the administration, management, monitoring and compliance of information security policies and procedures, and reporting of all computing security issues within CIP.

The role contributes to the ongoing development of information security procedures and processes in accordance with defined policy and supports the network services for CIP including identifying risks, tracking and driving remediation.

The Cyber Security System Engineer will also involve working with 3rd party Vendors to ensure the CIP's Cyber Security Roadmap is being developed and met.

KEY RESPONSIBILITIES

- Exploit security tools to continuously improve the detection, prevention and analysis of security incidents
- Perform event correlation, monitoring, research, assessment and analysis:
    - Triage alerts received from CIP monitoring tools and third-party security providers. Track and escalate remediation activities to ensure timely resolution
    - Investigate security incidents, actual or suspected, to contain and understand the extent of any impact. Invoke the Security Incident Response Plan if necessary. Perform root cause analysis and recommend security improvements to prevent recurrence
- Contribute to standards defining requirements to meet operational security needs, such as security event logging and monitoring agent implementation/maintenance:
    - Work with the other team members to ensure these operational security standards are communicated and met across CIP

- Maintain compliance with our control framework, standards, and policies

- Act as a security subject matter expert to advise our Technology team and the wider business to build awareness and accountability:
    - Providing input on any identified current technology architecture vulnerabilities, weaknesses and possible upgrades or improvements
    - Raise awareness among product team members from other disciplines about security operations and operational concerns as a key consideration of product development
    - Communicate at all levels across Craigs to promote individual and business wide information security
- Keep informed as to emerging security threats that have the potential to impact CIP and implement/recommend mitigating strategies
- Utilise available threat intelligence sources to inform and improve attack detection techniques
- Define requirements to automate and continuously improve the efficiency of threat detection, alerting and response
- Maintain security operations playbooks and runbooks in support of the Security Incident Response Plan
- Assist in the planning, design, deployment of new cyber control systems
- Assist with installing, configuring and maintaining critical security infrastructure and software patches
- Assist with monitoring and reporting on Security compliance to Australian and New Zealand legislation and regulators
- Assist in the delivery of minor information security projects & initiatives across Craigs Investment Partners
- Support & Escalations:
    - Respond to incidents assigned through the Service Desk / Cyber monitoring process
    - Provide Technical leadership in any Cyber Security events
    - Maintain accurate incident records and notes in the service desk system in line with SLA / Cyber forensic requirements.
    - Ensuring all Cyber issues and events are logged in the Service Desk system and categorised correctly
    - Follow all Infrastructure and Service Delivery Team processes as required
- Be involved in, support and deliver the strategic goals of the organisation's IT Department and Infrastructure Team
- Support of organisation's WAN, LAN and (Server) Infrastructure and security:
    - Liaise with 3rd party Vendors to perform Network and Hardware troubleshooting to isolate and diagnose common network problems and ongoing development.
    - Liaise with 3rd parties for resolution of faults, where necessary.
    - Assist with operational duties as allocated.
- Undertake Procurement and Asset Management as required for provision of ICT services in the organisation.

- Back-up and Disaster Recovery services:
    - Work with other members of the Infrastructure and Service Delivery team to ensure CIP's IT services are documented, managed and tested in conjunction with the Craigs Business Continuity Plan and aligned with the Craigs Investment Partners Cyber Security policies and procedures.
- On-call duties as Rostered:
    - Afterhours support as documented in the Craigs IT SLA document. After-hours support requires availability within the timelines provided in the SLA document.
    - Available outside of normal working hours as required for operational duties (including but not limited to BCP tests, server upgrades, patch installs, project work etc).
- Continuous Improvement:
    - Process improvements and recommendations to enhance Infrastructure and Service Delivery operations
    - Prepare, update and/or contribute to user guidelines, processes, and policies, and other related documentation
    - Involvement in the Infrastructure and Service Delivery Team's continuous improvement plan
- General Duties and Responsibilities:
    - Operate within the parameters of the NZX rules and regulations and CIP procedures and policies.
    - Maintain a high level of competence with Craigs Investment Partners' systems.
    - Maintain the core competencies as set down by the firm from time to time.
    - Complete all Company educational requirements as required for the role as set by the Company.
    - Act professionally, ethically and work co-operatively and constructively within the framework of the company structure.
    - Any other tasks as requested by your manager.

APPENDIX ONE:
Job Description

PERSON SPECIFICATION

Qualifications	• Bachelor's degree in Computer Science, Information Systems, or equivalent education or work experience • Advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP or CASP and/or SIEM-specific training and certification (desirable) • Hold DoD-8570 IAT Level 2 baseline certification (Security+ CE or equivalent) at start date (desirable)
Knowledge/Experience	• 4+ years of prior relevant experience • Financial services experience (desirable)
Key Skills and Attributes	• Advanced understanding of TCP/IP, common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements. • Hands-on experience analyzing high volumes of logs, network data (e.g. Netflow, FPC), and other attack artifacts in support of incident investigations • Experience with vulnerability scanning solutions • In-depth knowledge of architecture, engineering, and operations of at least one enterprise SIEM platform (e.g. Microsoft Sentinel, ArcSight, QRadar, LogLogic, Splunk) • Excellent time management and organisational skills • Strong written and verbal communication skills • Ability to work well under pressure • Problem solving skills