Committed to Caring for You

The Health Services Authority is responsible for the provision and administration of primary and secondary levels of healthcare services and public health functions for residents of the three Cayman Islands through a 127-bed hospital on Grand Cayman, a 18-bed hospital in Cayman Brac, a satellite outpatient clinic in Little Cayman and four District Health Centers on Grand Cayman offering the most comprehensive range of inpatient and outpatient services in a single health system in the Cayman Islands.

We invite applications for the following position:

JUNIOR SECURITY OPERATIONS CENTRE (SOC) ANALYST

Salary range: CI$49,800 - CI$66,984 per annum

The Junior Security Operations Analyst is responsible for supporting the mitigation of security threats to HSA's IT and digital infrastructure, through pro-active monitoring for any anomalies, performing prompt investigation and supporting the implementation of timely actions.

Primary Responsibilities: The successful candidate is required to perform a Level 2 Investigation into security anomalies or alerts, this will include analysis of a wide range of data (including system longs, packet capture files etc.), correlation of findings from previous investigations, open-source intelligence research in known exploits and publicly reported vulnerabilities, the preparation of a report and timely escalation of confirmed issues to the Management Team. Under guidance of the SOC Manager, implement actions to mitigate confirmed threats in real time and/or liaise directly with the relevant IT Department to advise of the mitigation actions required. Support continuous improvement through conducting product research into new tools for the Security Operation Centre Team and to prepare a brief for the manager's review and consideration. Achieve assigned SLA and KPIs and report to the SOC Manager.

Qualifications and Experience: The successful candidate must have a relevant Bachelor of Science degree in one of the following: Cyber Security, Computer Science, Business Systems, Information Technology (or equivalent) and at least one relevant, internationally recognized certification: COMPTIA Security+, COMPTIA Network+, EC Council Certified Ethical Hacker or GIAC Security Essentials Certification. This role requires the post-holder to have at least one (1) year of relevant work experience within one of the following fields: Cyber Security, IT Security Operations or Network Operations. Candidates with less than one (1) year of relevant work experience will be considered; however, will be required to sit a 2-hour exam and achieve a pass mark of at least 80%. The post-hold must be an excellent communicator verbally and in writing, possess strong analytic, critical thinking and research skills. The ability to learn complex topics and apply the knowledge to work assignments.

A remuneration and benefits package, commensurate with experience and qualifications will be offered to the successful candidate.

NOTE: Incomplete applications will not be considered. All applicants must complete and submit an HSA Application Form via e-mail to hsa.jobs@hsa.ky using pdf format. Log on to our website at www.hsa.ky to access the Application Form and Job Description.

Application deadline: December 8, 2024

Committed to Caring for You

Job Description

Job title	*Junior Security Operations Centre (SOC) Analyst*	**Job Holder**	*Vacant*
Reports to	*SOC Manager*	**Section**	*IT*

Background Information

The Cayman Islands Health Services Authority ("HSA") provides and administers health care services and public health functions for residents of the Cayman Islands in accordance with the National Strategic Plan for Health.

Services are delivered primarily through the 127-beds at the Cayman Islands Hospital (the country's principal health care facility), and the 18-beds at the Faith Hospital on Cayman Brac. Ancillary services are offered at district health centres, and clinics for dental and ophthalmologic care. Residents of Little Cayman can access care through the Island's clinic which is a purpose-built facility.

HSA is committed to the cyber security protection and safeguarding of its digital systems, services and the data entrusted to us, for the continuity and assurance of our service delivery, the quality and effectiveness of our day-to-day operations, risk management and compliance with laws and regulations.

Job purpose

HSA's essential IT and digital systems and services provided are across multiple sites in Grand Cayman, Cayman BRAC and Little Cayman. HSA's IT and Technology environment supports a large and diverse user community and critical in-patient and out-patient services. The Security Operations Centre (SOC) Team is responsible for safeguarding HSA's IT and digital systems and services from cyber security disruptive events and data breaches.

The SOC Team will be the primary contact for any suspected security incident and for leading the Incident Response in accordance with our SLAs, playbooks, processes, and practices. HSA is a 24/7/365 organisation and given that cyber threats can occur at any time, as such, the Security Operations Centre will evolve to operate 24x7x365 through a combination of the SOC Team working extended hours and weekends and an outsourced arrangement.

The SOC Team will be the primary contact for any suspected security incident and for leading the Incident Response in accordance with our SLAs, playbooks, processes, and practices.

The Junior Security Operations Analyst role is part of the SOC Team.

The Junior Security Operations Analyst will be responsible for supporting the mitigation of security threats to HSA's IT and digital infrastructure, through pro-active monitoring for any anomalies, performing prompt investigation and supporting the implementation of timely actions.

The Junior Security Operations Analyst will undertake continuous investigation of correlated security event feeds and the appropriate triage and escalation in case of an identified security incident.

Daily, the Junior Security Operations Analyst will be assigned security events to analyse, investigate, report on findings, take mitigating actions and/or make improvement recommendations. Continuous learning will be an important aspect of the role, as the cyber threat landscape continues to evolve, and novel attack types are a regular occurrence. This role requires a high degree of sharing and collaborative working with colleagues both within the SOC Team and the wider IT Department.

The Junior SOC Analyst will be required to nurture effective working relationships with his peers and colleagues in other Departments.

Dimensions

- This graduate entry level role will be part of the Security Operations Centre (SOC), which is part of the IT Department.
- Full training will be provided for the successful candidate so that they can proficiently undertake the role, i.e., 6 weeks of formal role-based, on-the-job training.
- The other roles within the SOC comprise of Security Operations Centre Manager, Security Operations Centre Analysts, and Information Security Manager.
- The SOC Manager and or his/her delegate will be responsible for the day-to-day management and assignment of tasks to the Junior Security Operations Analyst.
- The Junior Security Operations Analyst will be required to work 37.5 hours per week; however, flexible working is required as the SOC Team operates based on two shifts: (1) normal business hours shift and (2). extended weekday shift and weekend shift. The preference of the SOC Team will be considered when the shift schedule is being prepared.
- The normal business hours shift will be office based and the extended weekday and weekend shift based on working from home.

Duties and responsibilities

- Monitoring security anomalies across a range of detection systems and performing Level 1 Triage Investigation and document findings, in accordance with the Department’s standard operating procedures.
- Perform Level 2 Investigation into security anomalies or alerts, this will include analysis of a wide range of data (including system logs, packet capture files etc.,.), correlation of findings from previous investigations, open-source intelligence research in known exploits and publicly reported vulnerabilities, the preparation of a report and the timely escalation of confirmed issues to the Management Team.
- Under the guidance of the SOC Manager, implement actions to mitigate confirmed threats in real-time and / or liaising directly with the relevant IT Department to advise of the mitigation actions required.
- Continuously research and conduct appraisals into the latest cyber security threats, apply the indicators of attack (IoA) and indicators of compromise (IoC) to the Level 1 Triage and Level 2 Investigation, and share learning with your colleagues.
- Operate in conformance with the Department’s established standard operating procedure, key performance indicators (KPIs) target, change control protocol and quality standards.
- Under the instruction and guidance of the SOC Manager, to support incident response action plan.
- Supporting continuous improvement through conducting product research into new tools for the Security Operation Centre Team and to prepare a brief for the SOC Manager’s review and consideration.
- Achieve assigned SLA and KPIs and report to the SOC Manager.
- Undertake activities to complete Training Plans for continuous learning.

Qualifications, Experience & Skills Requirement

Education and Experience Requirements:

The post-holder must have a relevant Bachelor of Science Degree, one of these subjects; Cyber Security, Computer Science, Business Systems, Information Technology (or equivalent), and must have at least one relevant, internationally recognised certification:

- COMPTIA Security+
- COMPTIA Network+
- EC Council Certified Ethical Hacker
- GIAC Security Essentials Certification

This role requirements the post-holder to have at least one (1) year of relevant work experience working within one of the following fields:

- Cyber Security
- IT Security Operations
- Network Operations

Candidates with less than one (1) year of relevant work experience will be considered, however, the candidate will be required to sit a **2-hour exam** and achieve a pass mark of at least 80%.

The post-holder must be an excellent communicator verbally and in writing.

The nature of the work requires that the post-holder possesses strong analytic, critical thinking and research skills.

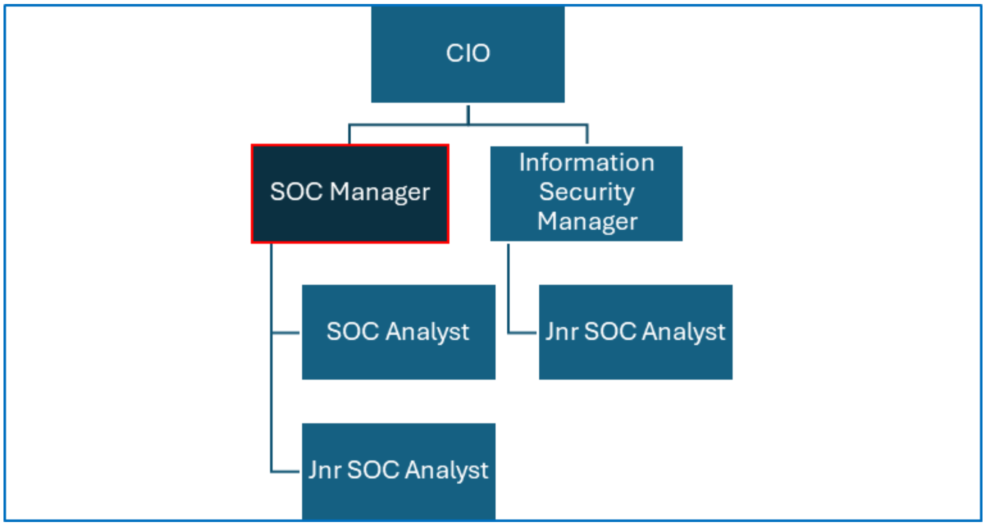
The ability to learn complex topics and apply the knowledge to work assignments.

Skills and abilities:

- ✓ Strong analytical, attention to detail and critical thinking
- ✓ Excellent report writing skills and effective verbal communicator
- ✓ Comfortable working in high-pressure environment
- ✓ Highly motivated to learn new frameworks/skills and take on responsibility
- ✓ Intuitive and keen instincts to pre-empt attacks
- ✓ Ability to collaborate and strong teamworking skills
- ✓ Ability to think creatively and problem solve
- ✓ Ability to conduct research into security issues and products as required
- ✓ Highly self-motivated and comfortable working alone or with a team of peers or senior persons and with third parties
- ✓ Ability to manage his/her time to ensure that process SLAs and deadlines are met
- ✓ Ability to effectively prioritize and execute tasks in a high-pressure environment.
- ✓ Must be able to meet performance goals to include, on call support, helpdesk security support, Incident Management solving

- ✓ Proficiency in the use of Microsoft Office 365 Products.

Reporting Relationship



Other Working Relationships

- All H.S.A Staff
- Outside Vendors

Decision Making Authority and Controls

This post does not have any delegated authority.

This role will require the post-holder to immediately escalate all security issues to the SOC Manager and the CIO.

Working conditions

- Required to work 37.5 contracted hours per week; however, flexible working is required.
- The SOC Team operates on the basis two shifts:
  (1) normal business hours shift and
  (2). extended weekday shift and weekend shift.
- The preference of the SOC Team will be considered by the SOC Manager when the shift schedule is being prepared.
- Normal office working environment or working from home.
- The Junior SOC Analyst is required to be on-call in the event of a security incident.

Physical requirements

The position requires the incumbent to sit for extended periods, and repetitive tasks with few breaks. On-call availability. Dexterity of hands and fingers to operate a computer keyboard, mouse and to handle other computer components.

Problem/Key Features

To deliver its mandate of cyber safeguarding the organisation’s digital systems and data from cyber-attacks, the SOC Team are reliant on advanced best-in-breed AI security systems and native security systems for insight into any indicators of attack and or indicators of compromise. Security warning alerts can occur at any time of the day or any day of the week, meaning that urgency and priorities can change unexpectedly.

In addition, the SOC Team are required to be available outside of normal business hours to investigate, analyse and take action to prevent/mitigate all attacks as a matter of urgency and in accordance with operating procedures and protocols.

The post holder is required to be mature, flexible and can work with changing priorities and under pressure.

Evaluation Metrics

- Improvement in the Security Maturity of the HSA
- Security Audit Compliance
- Incident Response times (Performed within RTO and RPO guidelines)
- Number of incidents avoided per day
- Number of investigation reports per day
- Number of data breaches avoided per day

Prepared by:	Interim CISO
Date Prepared:	20th May 2024
Approved by:	*Chief Information Officer*
Date approved:	
Reviewed:	
Next Review	