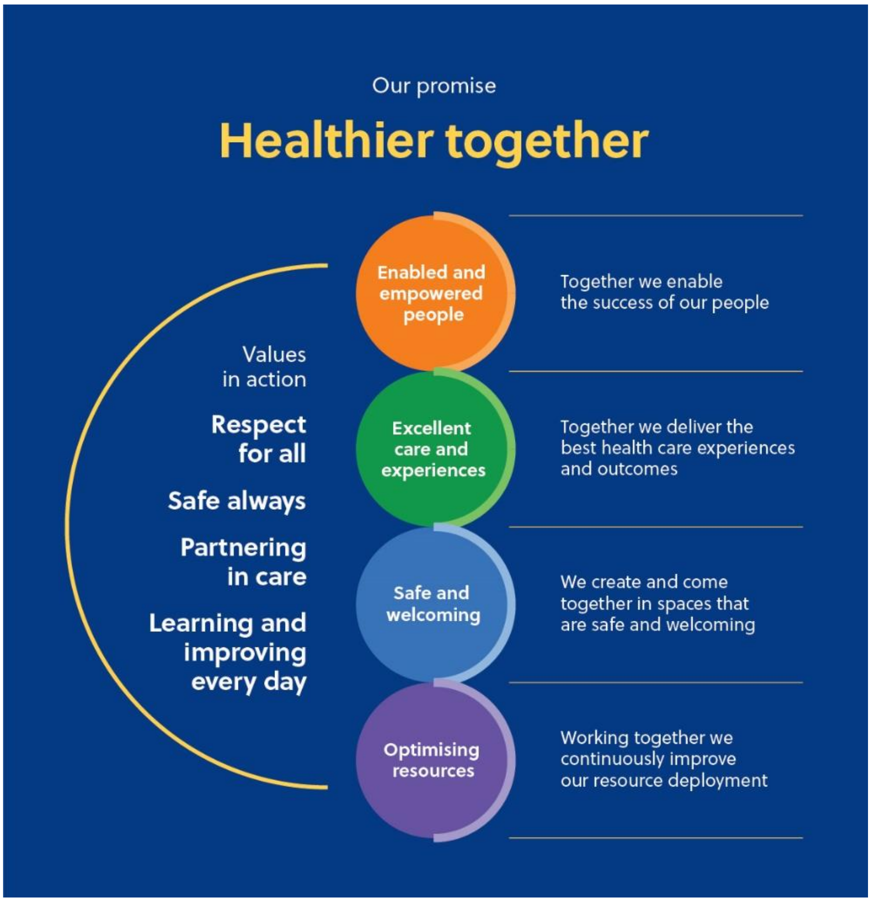
POSITION DESCRIPTION

Position Title:	**Senior Cyber Security Engineer**
Award Classification:	**HS4 or as negotiation**
Award / Agreement Name:	**HEALTH AND ALLIED SERVICES, MANAGERS AND ADMINISTRATIVE WORKERS (VICTORIAN PUBLIC SECTOR) (SINGLE INTEREST EMPLOYERS) ENTERPRISE AGREEMENT 2021-2025**
Position Reports to:	**Associate Program Director – Cyber Security**

EASTERN HEALTH – HEALTHIER TOGETHER

Eastern Health is one of Melbourne's largest metropolitan public health services. We provide a comprehensive range of high-quality acute, sub-acute, palliative care, mental health, drug and alcohol, residential care, community health and statewide services to people and communities that are diverse in culture, age and socio- economic status, population and healthcare needs



Our promise

Healthier together

Values in action

Respect for all

Safe always

Partnering in care

Learning and improving every day

Enabled and empowered people — Together we enable the success of our people

Excellent care and experiences — Together we deliver the best health care experiences and outcomes

Safe and welcoming — We create and come together in spaces that are safe and welcoming

Optimising resources — Working together we continuously improve our resource deployment

1. POSITION PURPOSE

The Senior Cyber Security Engineer will be responsible for leading the development and implementation of advanced threat detection and response strategies to safeguard Eastern Health from emerging cyber threats and attacks on its information and ICT infrastructure systems. This role is critical in designing and overseeing robust security architectures, deploying cutting-edge security technologies, and conducting comprehensive vulnerability assessments to proactively detect and respond to sophisticated cyber security threats. The Senior Cyber Security Engineer will lead and coordinate cyber security incident response efforts, perform in-depth root cause analysis, and provide strategic direction for effective containment and remediation measures. Additionally, this position will support technical and non-technical changes related to cyber security at Eastern Health, promote a culture of security awareness, and ensure compliance with relevant security standards and regulations. The role also involves collaborating with cross-functional teams to enhance the organization's overall cyber security posture and continuously drive improvements in security processes and controls.

2. MAJOR DUTIES AND/OR RESPONSIBILITIES

The Senior Cyber Security Engineer fulfills the following tasks:

- **Security Architecture and Design:** Design and oversee the implementation of robust security architectures and solutions. This includes evaluating and deploying cutting-edge security technologies, ensuring integration with existing systems, and conducting regular security health checks.

- **Advanced Threat Detection and Response:** Lead the development and implementation of advanced threat detection and response strategies. This includes creating and refining use cases, enhancing detection rules, and integrating new data sources into SIEM and SOAR tools to identify and mitigate sophisticated cyber threats.

- **Incident Management:** Oversee and coordinate cyber security incident response efforts. This involves conducting thorough investigations, analysing root cause, and implementing effective containment and remediation measures.

- **Vulnerability Management:** Lead comprehensive vulnerability assessments and penetration testing. Develop and execute remediation plans to address identified vulnerabilities and ensure the security of the organization's IT infrastructure.

- **Threat Intelligence and Hunting:** Stay updated with the latest threat intelligence and lead proactive threat-hunting activities. Identify emerging threats, analyse attack patterns, and develop and implement strategies and technical security controls to mitigate potential risks.

- **Security Awareness and Training:** Develop and deliver security awareness programs and training sessions for employees. Promote a culture of security awareness and ensure that staff are knowledgeable about best practices and emerging threats.

- **Collaboration and Communication:** Collaborate with cross-functional teams, including IT, business units, and external partners, to ensure the implementation of effective security measures. Communicate security risks, incidents, and recommendations to stakeholders clearly and concisely.

- **Compliance and Governance:** Ensure compliance with relevant security standards, regulations, and frameworks. Develop and maintain security policies, procedures, and guidelines to align with industry best practices and organizational requirements.

- **Continuous Improvement:** Continuously evaluate and improve security processes, technologies, and controls. Identify areas for enhancement, implement innovative solutions, and stay abreast of industry trends and advancements in cyber security.

3. SAFE PRACTICE AND ENVIRONMENT

Occupational Health and Safety

Eastern Health is committed to provide and maintain a working environment for all staff that is safe and without risk to health. All staff are to take care of their own health and safety and the health and safety of any other person who may be affected by your acts or omissions at the workplace. Understand responsibilities and accountabilities to yourself and others in accordance with OH&S legislation and Eastern Health policies and promote a working environment that is congruent with these guidelines. This includes staff reporting of all clinical and OHS incidents and near misses, in particular those related to Occupational Violence, Manual Handling and Slips, trips and falls.

Staff are required to comply with all state legislative requirements in respect to the Occupational Health and Safety Act 2004 and the Workplace Injury Rehabilitation and Compensations (WIRC) Act 2013.

4. TRAINING AND DEVELOPMENT

Relevant, practical and timely education should direct, facilitate, enhance and support the professional growth and practice of employees in a health environment characterised by change. All programs should endeavour to promote evidence-based practice, a problem solving approach and to be competency based.

You are expected to participate in the personal development process on an annual basis.

5. QUALITY

As a staff member of Eastern Health staff are required to comply with Eastern Health performance standards and participate in continuous monitoring and improvement as part of your role. You are also required to comply with legislation, professional standards and accreditation standards.

As a staff member employed by Eastern Health services you must have and maintain the appropriate skills and knowledge required to fulfil your role and responsibilities within the organisation. In addition, you must ensure that you practice within the specifications of this position description, and where applicable within the agreed scope of practice.

You are responsible for ensuring safe high quality care in your work. This will include complying with best practice standards, identifying and reporting any variance to expected standards and minimising the risk of adverse outcomes and patient harm. In addition, you will ensure that service and care is consistent with the EH approach to patient and family centered care.

6. CONFIDENTIALITY

Any information obtained in the course of employment is confidential and should not be used for any purpose other than the performance of the duties for which the person was employed. Staff are bound by the Information Privacy Act 2000 and the Health Records Act 2001.

7. EQUAL EMPLOYMENT OPPORTUNITY

You agree to adhere to the Equal Employment Opportunity policies and practices of the Health Service. Discriminatory practices, including sexual harassment, are unlawful. The Health Service will not tolerate discriminatory behaviour and any such conduct may lead to the invoking of the Disciplinary Policy and Procedure, which may result in termination of employment.

8. PERFORMANCE DEVELOPMENT

A Performance Review, that includes agreed targets, will occur three (3) months from commencement and then annually on the basis of the duties and responsibilities outlined in this position description. This is an opportunity to review personal and the allocated work unit's service performance, facilitated by the setting of objectives/goals and ongoing evaluation of performance and achievement. Objectives will be developed annually, documented, discussed and agreed with the immediate line manager, who will act as the assessor. The incumbent is expected to demonstrate and show evidence annually of on-going self and allocated work unit's service development.

9. EASTERN HEALTH'S PROMISE

Our promise to our communities, patients, consumers and staff is that we will be **HEALTHIER TOGETHER**. Bolder than a vision for the future, our promise calls us to action. We know that working together is the only way we can achieve what is necessary for a healthier future.

Our values are ones in action and are the behaviours that matter most.

- Respect for all
- Safe always
- Partnering in care
- Learning and improving everyday

Learning from the challenges of the past and looking to the future, we understand that we are building towards a more engaged, more reliable, always safe health service in partnership with our people to improve every day.

9. ATTACHMENTS

- Attachment 1 Key Selection Criteria

10. ATTACHMENTS

- Attachment 1 Key Selection Criteria

11. NOTE

Statements included in this position description are intended to reflect in general the duties and responsibilities of this position and are not to be interpreted as being all-inclusive.

Prior to accepting any offer of employment, prospective employees will be required to read and commit to the Eastern Health Code of Conduct, including (but not limited to) issues of Occupational Health and Safety, Equal Opportunity and Confidentiality.

Vaccination against infectious disease is a mandatory requirement of this role. An offer of employment is conditional on you providing evidence that you are currently vaccinated against COVID-19, prior to commencing employment.

Signed: ____ Date: ____/____/____

Manager

INCUMBENT STATEMENT

I ______________________________________(Incumbent Name) have read, understood and accepted the above Position Description and associated Attachments.

Signed: ____ Date: ____/____/____

ATTACHMENT 1

KEY SELECTION CRITERIA

Position Title:	**Senior Cyber Security Engineer**
Award Classification:	**HS4 or by negotiation**
Award / Agreement Name:	**HEALTH AND ALLIED SERVICES, MANAGERS AND ADMINISTRATIVE WORKERS (VICTORIAN PUBLIC SECTOR) (SINGLE INTEREST EMPLOYERS) ENTERPRISE AGREEMENT 2021-2025**
Position Reports to:	**Associate Program Director – Cyber Security**

Essential

Candidates will be evaluated based on their ability to perform the above-mentioned duties while demonstrating the skills and competencies necessary to be highly effective in the role. These skills and competencies include:

- Degree in Computer Science, Information Security, or a related field.
- 7+ years of experience in cyber security, especially in cyber-security architecture, engineering and operations role.
- Certified Information Systems Security Professional (CISSP), The GIAC Certified Incident Handler (GCIH) or equivalent - Preferred
- Knowledge of security, risk and control frameworks and standards such as ACSC Essential 8, NIST, MITRE ATT&CK & ITIL.
- Technical expertise in network security, system and cloud security knowledge, firewalls, intrusion detection, web application security, IoT Security, vulnerability scanning, and malware protection.
- Strong knowledge of common vulnerabilities and exploitation techniques.
- Practical experience with threat hunting, cyber security incident handling, red teaming and penetration testing
- Proficiency with at least one scripting language (e.g., Perl, Python, PowerShell).
- An understanding of business needs and a commitment to delivering high-quality, prompt, and efficient service to the business.
- Understanding organizational mission, values, and goals and consistently applying this knowledge.
- Strong decision-making capabilities, with a proven ability to weigh the relative costs and benefits of potential actions and identify the most appropriate one.
- An ability to effectively influence others to modify their opinions, plans, or behaviors.

Desirable but not essential:

- Previous experience working in a health environment or Victorian government agency.
- An understanding or experience in project management or Agile BA methodologies.
- Experience writing User Stories with Acceptance Criteria for Security Testing.
- An understanding or experience in secure software development methodologies.