**SKILLS MAP - INCIDENT INVESTIGATION MANAGER/FORENSIC INVESTIGATION MANAGER/THREAT INVESTIGATION MANAGER**

**Job Role**

The Incident Investigation Manager/Forensic Investigation Manager/Threat Investigation Manager plans and oversees the performance of security response via post-incident analysis of intrusion, attack, loss or breach and the identification of root causes. He/She provides guidance on the use of investigation methodology to capture evidence to produce legally defensible results and conclusions. He applies analysis across a variety of data sets to develop knowledge of internal and external information vulnerabilities and to uncover hidden insights, patterns and connections. He proposes mitigation techniques and countermeasures as well as develops cyber security solutions to prevent future attacks. He develops security requirements and standards. He presents threat intelligence reports to senior leaders. He is required to be on standby with on-call availability with varied shifts including nights, weekends and holidays.

He thinks strategically and adopts a forward-looking perspective in anticipating threats and planning pre- or post-incident analyses. He is adept at dealing with complexity, and is an articulate and developmental leader in his team.

### Critical Work Functions and Key Tasks / Performance Expectations

<table>
<thead>
<tr>
<th>Critical Work Functions</th>
<th>Key Tasks</th>
<th>Performance Expectations (For legislated / regulated occupations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop an incident response strategy</td>
<td>Develop a threat intelligence strategy to protect systems from unauthorised access or cyber attacks</td>
<td></td>
</tr>
<tr>
<td>Establish digital forensic investigation and threat analysis policies and standards for the organisation</td>
<td>Establish guidelines to performing threat analysis and investigations</td>
<td></td>
</tr>
<tr>
<td>Develop threat mitigation and prevention processes and policies, refreshing them where required</td>
<td>Implement processes and guidelines to collect threat intelligence, analyse data, create intelligence reports and maintain records</td>
<td></td>
</tr>
<tr>
<td>Abuse senior management on major information security related risks</td>
<td>Implement mechanisms to improve threat threat detection and incident response times</td>
<td></td>
</tr>
<tr>
<td>Implement incident response strategy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond to security incidents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversee cyber threat analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversee forensic investigations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage department</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Technical Skills & Competencies

<table>
<thead>
<tr>
<th>Skills &amp; Competencies</th>
<th>Level</th>
<th>Generic Skills &amp; Competencies (Top 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Forensics</td>
<td>Level 6</td>
<td>Communication Advanced</td>
</tr>
<tr>
<td>Cyber Incident Management</td>
<td>Level 6</td>
<td>Developing People Advanced</td>
</tr>
<tr>
<td>Cyber Risk Management</td>
<td>Level 4</td>
<td>Problem Solving Advanced</td>
</tr>
<tr>
<td>Security Assessment and Testing</td>
<td>Level 4</td>
<td>Resource Management Advanced</td>
</tr>
<tr>
<td>Security Governance</td>
<td>Level 5</td>
<td>Sense Making Advanced</td>
</tr>
<tr>
<td>Security Strategy</td>
<td>Level 5</td>
<td>Stakeholder Management Level 5</td>
</tr>
<tr>
<td>Threat Intelligence and Detection</td>
<td>Level 6</td>
<td></td>
</tr>
</tbody>
</table>

**Programme Listing**

For a list of Training Programmes available for the Infocomm Technology sector, please visit: [www.skillsfuture.sg/skills-framework/ict](http://www.skillsfuture.sg/skills-framework/ict)