The examination is designed to demonstrate that cyber-security professionals have sufficient knowledge and skill in key areas to successfully conduct network security functions. The closed-book exam contains 65 multiple choice questions.

Exam content areas
The exam is broken down into five content areas as follows:

<table>
<thead>
<tr>
<th>Major Content Groupings</th>
<th>Exam Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Protect Infrastructure</td>
<td>7%</td>
</tr>
<tr>
<td>II. Event/Incident Detection</td>
<td>17%</td>
</tr>
<tr>
<td>III. Triage &amp; Analysis</td>
<td>28%</td>
</tr>
<tr>
<td>IV. Respond</td>
<td>40%</td>
</tr>
<tr>
<td>V. Sustain</td>
<td>8%</td>
</tr>
</tbody>
</table>

Key areas covered under these major headings are as follows:

**Protect Infrastructure**
- Assist constituents with correcting problems identified by vulnerability scanning activities
- Implement changes to the computing infrastructure (to stop or mitigate an ongoing incident, to stop or mitigate the potential exploitation of a vulnerability, or as a result of postmortem reviews or other process improvement mechanisms)
- Provide constituents with guidance in best practices for protecting their systems and networks.

**Event/Incident Detection**
- Monitor networks and information systems for security.
- Analyze the data or indicators from the networks and systems being monitored
- Enter event/incident reports received from the constituency into the incident management knowledgebase.
- Collect incident data and intrusion artifacts (e.g., malware, logs) to enable mitigation of incidents.
- Perform initial, forensically sound collection of images for forensic analysis and investigation.
- Identify missing data or additional sources of information and artifacts.

**Triage & Analysis**
- Categorize events using the organization’s standard category definitions.
- Perform correlation analysis on event reports to determine if there is affinity between two or more events.
- Prioritize events (includes determining scope, urgency, and potential impact).
- Assign events for further analysis, response, or disposition/closure.
- Determine cause and symptoms of the incident.
- Analyze intrusion artifacts and malware (e.g., malware, source code, Trojan horse programs) to understand their purpose and/or to identify the specific vulnerability.
- Perform vulnerability analysis.
- Determine the risk, threat level, or business impact of a confirmed incident.
Respond
• Develop an incident response strategy and plan to limit incident effect and to repair incident damage.
• Perform real-time incident response tasks (e.g., direct system remediation) to support deployable incident response teams.
• Determine the risk of continuing operations.
• Change passwords.
• Improve defenses.
• Remove the cause of the incident.
• Validate the system.
• Identify relevant stakeholders that need to be contacted or that may have a vested interest or vital role in communications about an organizational incident.
• Identify the appropriate communications protocols and channels (media and message) for each type of stakeholder.
• Coordinate, integrate, and lead team responses with other internal groups (e.g., IT, management, compliance, legal, human resources), according to applicable policies and procedures.
• Provide notification service to other constituents (e.g., write and publish guidance or reports on incident findings) to enable constituents to protect their assets and/or detect similar incidents.
• Report and coordinate incidents with appropriate external organizations or groups in accordance with organizational guidelines, policies, and procedures.
• Serve as technical experts and liaisons to law enforcement personnel (e.g., to explain incident details, provide testimony).
• Track and document incidents from initial detection through final resolution.
• Assign and label data/information according to the appropriate class or category of sensitivity
• Collect and retain information on all events/incidents in support of future analytical efforts and situational awareness.
• Enter information (shift change transitions, current state of activity) into an operations log or record of daily operational activity.

Sustain
• Perform risk assessments on incident management systems and networks.
• Run vulnerability scanning tools on incident management systems and networks.

Exam Registration Instructions
1. Email certification-info@sei.cmu.edu for a link to the SEI’s testing portal. Follow the link to access the SEI’s testing services.
2. Create a personal account and follow the instructions for new users of the testing system.
3. After logging in, click “Register for Exam” at the top of the page.
4. On the “Exam Registration” page, click on “CERT-Certified Computer Security Incident Handler.”
5. Click on “Buy Now” next to CERT-Certified Computer Security Incident Handler. (Clicking “Buy Now” does not obligate you to purchase the exam.)
6. On the “Select Testing Center” page, use the drop-down menus at the top of the page to tailor the search for a testing center by country, state, Zip code, etc.
7. On the “Date and Time Selection” page, schedule a testing session by selecting a date and starting time. After scheduling the test session and acknowledging that you have read the “no-shows and cancellations” policy, click the blue “Select” button.
8. On the “Shopping Cart” page, if everything appears correct, click the blue “Check Out” button.
9. On the “Checkout” page, provide the appropriate billing and payment information, and click the blue “Submit” button. The credit card charge is then processed.
10. After the exam has been purchased, you will receive an email that confirms the purchase and provides important information about the testing session, including a candidate authorization code that you will need in order to take the exam.