Undergraduate Certificate in Advanced Security Operation Center Management

Incident Response and Handling

Incident Response and Handling is a critical component of any effective cybersecurity strategy. This section will explain key terms and vocabulary related to Incident Response and Handling in the context of the Undergraduate Certificate in Advanced Security Operation Center (SOC) Management.

* **Incident**: An incident is any event that could lead to unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. Examples of incidents include malware infections, phishing attacks, and unauthorized access to sensitive data.
* **Incident Response**: Incident Response is the process of identifying, investigating, containing, and mitigating incidents to minimize their impact on an organization.
* **Incident Handling**: Incident Handling is the practice of managing incidents in a structured and consistent manner to ensure a timely and effective response.
* **Incident Response Plan (IRP)**: An IRP is a written plan that outlines the steps an organization will take to respond to incidents. It should include procedures for detecting, analyzing, containing, and mitigating incidents, as well as procedures for communicating with stakeholders and reporting incidents to authorities.
* **Incident Response Team (IRT)**: An IRT is a group of individuals who are responsible for responding to incidents. The IRT should include representatives from different departments, such as IT, security, legal, and public relations.
* **Incident Response Lifecycle**: The incident response lifecycle is a series of stages that an organization goes through when responding to incidents. The stages include preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.
* **Preparation**: Preparation involves developing and maintaining an IRP, training IRT members, and ensuring that the necessary tools and resources are in place.
* **Detection and Analysis**: Detection and analysis involves identifying and investigating incidents to determine their scope and impact.
* **Containment**: Containment involves taking steps to prevent the spread of incidents and minimize their impact.
* **Eradication and Recovery**: Eradication and recovery involves removing the cause of incidents and restoring affected systems to a secure state.
* **Post-Incident Activity**: Post-incident activity involves conducting a post-incident review to identify lessons learned and making improvements to the IRP and other security controls.
* **Computer Incident Response Team (CIRT)**: A CIRT is a team of experts who are responsible for responding to computer security incidents.
* **Computer Security Incident Response Team (CSIRT)**: A CSIRT is a team of experts who are responsible for responding to computer security incidents and providing guidance and assistance to organizations.
* **Incident Classification**: Incident classification involves categorizing incidents based on their severity and impact. Common classifications include low, medium, high, and critical.
* **Incident Prioritization**: Incident prioritization involves determining which incidents should be

addressed first based on their severity and impact.
* **Incident Notification**: Incident notification involves informing stakeholders, such as employees, customers, and law enforcement agencies, about incidents.
* **Incident Coordination**: Incident coordination involves working with other organizations, such as service providers and law enforcement agencies, to respond to incidents.
* **Lessons Learned**: Lessons learned are insights and recommendations that are identified during post-incident reviews. They can be used to improve the IRP and other security controls.
* **Tabletop Exercise**: A tabletop exercise is a simulated incident response exercise that is conducted in a low-stress environment. It is used to test the IRP and train IRT members.
* **Full-Scale Exercise**: A full-scale exercise is a simulated incident response exercise that is conducted in a high-stress environment. It is used to test the IRP and train IRT members in a realistic setting.

In conclusion, Incident Response and Handling is a critical component of any effective cybersecurity strategy. Understanding key terms and vocabulary is essential for developing and maintaining an IRP, training IRT members, and responding to incidents in a structured and consistent manner. By following the incident response lifecycle, classifying incidents, prioritizing incident response, notifying stakeholders, coordinating incident response, and learning from incidents, organizations can minimize the impact of incidents and protect their information and information systems.