FORMING AN INCIDENT RESPONSE TEAM: A STEP-BY STEP GUIDE

Author – Andrew Smith

February 2024

When it comes to cybersecurity, being prepared for potential incidents is crucial. One of the key components of an effective incident response plan is a well-formed incident response team (IRT). An IRT is a group of dedicated individuals who are trained to handle and respond to security incidents in an organization.

Forming an IRT requires careful planning and consideration. In this guide, we will outline the steps you need to go through to form an incident response team.

Step 1: Identify Team Objectives and Scope

The first step in forming an incident response team is to clearly define the objectives and scope of the team. This involves identifying the goals and responsibilities of the team, as well as determining the scope of incidents the team will handle. It is important to align the objectives of the team with the overall goals and mission of the organization.

Step 2: Define Team Roles and Responsibilities

Once the objectives and scope of the team are established, the next step is to define the roles and responsibilities of each team member. This includes identifying key positions such as incident response coordinator, technical analysts, communication specialists, and legal advisors. Clearly defining the roles and responsibilities will ensure that each team member knows their specific duties and tasks.

Step 3: Assess Skill and Expertise

After defining the roles and responsibilities, it is important to assess the skill and expertise of potential team members. This involves evaluating their technical knowledge, experience in incident response, and any relevant certifications or training they may have. It is important to have a diverse team with a range of skills and expertise to effectively handle different types of security incidents.

Step 4: Establish Communication Channels

Effective communication is essential during incident response. Establishing communication channels within the team and with other stakeholders is crucial for timely and accurate information sharing. This includes setting up dedicated communication tools, such as secure messaging platforms or incident management systems, and defining communication protocols for different types of incidents.

Step 5: Develop Incident Response Procedures

Developing incident response procedures is a critical step in forming an incident response team. These procedures outline the step-by-step process for detecting, analyzing, containing, eradicating, and recovering from security incidents. The procedures should be well-documented, regularly reviewed, and updated to reflect changes in technology, threats, and regulations.

Step 6: Train and Exercise the Team

Training and exercising the incident response team is essential to ensure their readiness and effectiveness. Team members should undergo regular training sessions to enhance their skills and knowledge in incident response. Additionally, conducting simulated exercises and tabletop drills will help the team practice their response procedures and identify areas for improvement.

Step 7: Establish Relationships with External Entities

An incident response team does not operate in isolation. It is important to establish relationships with external entities such as law enforcement agencies, incident response organizations, and industry peers. These relationships can provide valuable support, resources, and information sharing during security incidents.

Step 8: Continuously Monitor and Improve

Forming an incident response team is not a one-time task. It requires continuous monitoring and improvement. Regularly assess the team's performance, update procedures based on lessons learned from past incidents, and stay informed about emerging threats and best practices in incident response. This will ensure that the incident response team remains effective and adaptive to changing cybersecurity landscape.

By following these steps, you can form a robust and effective incident response team that is well-prepared to handle security incidents and protect your organization's assets.