Today, in countries across the world, operations such as the digitalization of critical infrastructure and public services, through the use of computer networks, has revealed the security problems of cyber space. Used for the transferring and storing of highly critical data, any weaknesses and vulnerabilities located on these computer systems have the potential to cause tangible and intangible costs and losses on the country concerned. With the concept of cyber security growing in importance globally, countries have developed strategies, launched awareness-raising activities, and organized campaigns to have maximum information security level. In what is an ongoing process, it has been revealed that countries are finding it necessary to create computer security incident response teams, in order to protect their national cyber security. Cyber incident response teams are for the early identification of threats to national security that may occur in cyberspace, and to reduce the effects of any attack that may be encountered. In this study, we examined in detail the policies being implemented for the creation of cyber incident response teams and the qualifications team members should have. In addition, the cyber incident response teams created in developed countries around the World, and the properties and activities of these teams, are investigated.
The study is concluded by examining the development of cyber incident response teams in Turkey, and presenting
recommendations for Turkey.