Forensics and CSIRT Plan

ISSC 498

 The 899th Communications Squadron (899 CS) will always have a Tiger response team on hand in the event of a computer security incident. The response team will fill the same role as a computer security incident response team (CSIRT) Their responsibilities will include supporting and coordinating an appropriate and time sensitive response to any security event or incident (Ruefle, 2007). The main goal of the CSIRT is to limit and control any damage that can result in events while providing effective guidance for response and steady recovery activities in addition to preventing any future security mishaps from taking place. The team will consist of 10 subject matter experts that are available 24-7/365. The key with responding to security incidents is to limit any further damage while protecting critical information, assets and systems.

 The 899 CS Tiger response team will work with the organizations security analysts, incident handlers, network and system administrators, human resources and public affairs staff, information security officers and other managers in the organization to help coordinate and manage the incident response process for the 899 CS. The tiger team will have an incident tracking database to record data about all reported incidents as well as the actions taken to resolve the incident (Ruefle, 2007). A checklist will be created and include the following the impact of the incident, the technical cause of the incident, potential threats resulting from the incident, solutions and workarounds, estimated downtime, implementation of response strategies, collaborating with outside entities to include law enforcement agencies and establishing a repository to track vulnerability information to develop lessons learned to enhance security posture and incident response management for the 899 CS (Ruefle, 2007). Also, the Tiger response team will work with the Computer Forensics team to investigate the security incident or attack. The forensics team will be readily available and will begin their evaluation immediately, gathering facts, details of the incident. The Forensics team will collect any evidence or information form the systems, storage devices and network. In addition, he Forensics team will thoroughly analyze the collected evidence and information they will use all available tools and techniques while documenting every step and establishing time frames to complete their investigation. When the forensics team have completed their investigation a summary of findings will be presented to leadership and the head of the IT staff along with recommendations and strategies to prevent future attacks and incidents.

References

Ruefle, R. (2007, January 24). Defining Computer Security Incident Response Teams. Retrieved March 20, 2020, from <https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams>