INVESTIGATION

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Related Jobs Titles

Persons working in this Specialty area may have job titles similar to:

- Computer Crime Investigator
- Special Agent

Tasks

Professional involved in this Specialty perform the following tasks:

- Analyze computer-generated threats
- Assist in the gathering and preservation of evidence used in the prosecution of computer crimes
- Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion
- Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects
- Conducts large-scale investigations of criminal activities involving complicated computer programs and networks
- Determine and develop leads and identify sources of information in order to identify and prosecute the responsible parties to an intrusion
- Develop an investigative plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet
- Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, etc.)
- Employ IT systems and digital storage media to solve and prosecute cybercrimes and fraud committed against people and property
- Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
- Examine recovered data for information of relevance to the issue at hand
- Fuse computer network attack analyses with criminal and counterintelligence investigations and operations
- Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action
- Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations
- Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration
- Identify elements of proof of the crime
- Identify outside attackers accessing the system from the internet or insider attackers, that is, authorized users attempting to gain and misuse non-authorized privileges
- Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations
- Prepare reports to document analysis
- Process crime scenes
- Secure the electronic device or information source
- Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence

KSAs

Experts in the Specialty Area have the following Knowledge, Skills, and Ability:

- Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, search and seizure laws, civil liberties and privacy laws, etc.), statutes
- Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones
- Knowledge of legal governance related to admissibility (Federal Rules of Evidence)
- Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Knowledge of seizing and preserving digital evidence (e.g., chain of custody)
- Knowledge of social dynamics of computer attackers in a global context
- Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code)
- Knowledge of types and collection of persistent data
- Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data
- Skill in evaluating the trustworthiness of the supplier and/or product
- Skill in preserving evidence integrity according to standard operating procedures or national standards
- Skill in using scientific rules and methods to solve problems