COMPREHENSIVE CYBER FORENSICS SERVICE

Product brochure

THE PROBLEM

Cyberwarfare, along with information warfare, have evolved into the fifth domain of warfare (with space, air, sea and land being the other four domains). In this era of mass on-line communication, states, governments, corporations, organizations, individuals and targets ranging from state infrastructures to home appliances face serious cyber threats.

Cybersecurity is currently an essential need in the context of national security as well as in everyday life as cyberterrorism, hacking, on-line fraud, denial of service, malware, ransomware, website defacing, social media manipulation and other threats have become a real and present danger.

One of the most important activities within the broad context of cybersecurity is Cyber Forensics. The term "Cyber Forensics" refers to the employment of investigative, analytical and technological tools and structured procedures with the intention of collecting, recording and retaining evidence of damaging and/or malicious offensive activities and incidents concerning computers and computer systems. Recently, this activity has been applied more and more frequently to cyberattacks.

The objectives of cyber forensics are:

- To determine what actually happened and the identity of the perpetrators
- To assess the damage sustained and the corrective action required
- To analyze and understand the opponent's tactics and tools
- To draw lessons and conclusions for the development of future defenses and countermeasures
- To present the evidence in the context of legal proceedings

Organizations seeking to protect their information, computer systems and operations/services will benefit from a comprehensive cybersecurity system that includes either in-house or outsourced cyber forensics services.

THE SOLUTION

ACS offers CCFS – Comprehensive Cyber Forensics Service.

CCFS is an in-house or outsourced cyber forensics service consisting of three primary elements, or stages: preventive/real-time cyber forensics, real-time cyber incident management tools and post-event investigative cyber forensics. Additionally, a complete training package is provided.

By incorporating CCFS in their comprehensive cybersecurity systems, organizations will be provided with a complete cyber forensics solution that offers preventive action support, real-time incident management capabilities and post-event investigative tools.

KEY FEATURES & MAJOR ADVANTAGES

Key Features & Major Advantages:
- A complete cyber forensics service:
- Cyber forensics laboratory
- Preventive & real-time cyber forensics systems
- Cyber incident management systems & tools
- Post-event investigative tools & procedures
- Complete training package
- Cyber forensics laboratory:
  - Design & setup
  - Maintenance & supervision
  - Future upgrading
  - Preventive & real-time cyber forensics systems:
  - Collection & analysis of history data
  - Incident detection system
  - Compilation of a pre-event database for real-time incident detection
  - Compilation of a database for post-event investigation
- Cyber incident management systems & tools:
  - On-site CERT (Cyber Emergency Response Team)
  - On-going CERT management
  - Cybersecurity incident analysis
  - Training for CERT personnel
- Post-event investigative tools & procedures:
  - On-site forensics services
  - Covert investigations
  - Mobile forensics
  - Legal assistance

- Complete training package:
  - Data mining
  - Mobile forensics
  - Network forensics
  - Specific training activities adapted to the client's needs & requirements