1. 应急响应就是对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，保证计算机信息系统与网络免遭破坏。

主要功能：

① 因为出现安全问题后采取应急响应措施，事先做好准备。

② 安全事件具有突发性，复杂性与专业性的特点，防止组织体系及协调机制方面存在不知道、不规范的问题。在事件确发生后采取措施，力图将事件所造成的损失降到最小。

2. 审计：即记录和分析用户使用信息系统过程的中的相关事件

主要功能：

① 安全审计可监控来自信息内部和外部的用户活动，对与安全有关的活动的相关信息进行识别，记录，存储和分析，对突发事件进行识别，记录，存储和分析，对突发事件进行报警和响应，还能对系统事件的记录，为事后处理提供重要依据，为网络犯罪行为及泄密行为提供取证基础。

② 同时，通过对安全事件的不断积累并且加以分析，能有选择性和针对性地对其中的对象进行审计跟踪，以保证系统的安全。

扫描全能王 创建

3. 主要作用：获得证据，打击违法犯罪

其它作用：

①排除故障：取证工具和技术可以用来排除计算机和网络之间的故障。

②日志监控：实时取证过程，需要监视各种日志文件，分析和关联各种系统的日志记录，从而帮助在应急响应中的事件处理，识别违反安全策略的事件，实施审计等。

③数据恢复：从系统中恢复丢失的数据，包括偶然和故意删除的数据以及由于其它原因删除的数据。

④数据提取：帮助从加密的、隐含的，分散的文件系统区域提取和还原数据。

⑤完善策略：调查用户违反安全策略的行为。

4. 电子证据的特点：

①数字性 ②技术性 ③脆弱性 ④多态性 ⑤人机交互性 ⑥复合性

5. 步骤主要包含：①收集 ②检查 ③分析 ④报告

①收集阶段，就是辨认、标志、记录、集中与具体事件相关的数据，并保护数据的完整性

②检查阶段，利用合适的取证技术和工具从收集来的数据中发现和提取信息，同样需保证数据完整性

③分析阶段，要根据特定问题和需求对检查阶段得到的数据进行进一步的调查

④在报告阶段，根据分析结果，描述事件发生，决定采取哪种行动，提出安全策略，改正指南等建议。

扫描全能王 创建