Information security is too complex to discuss within one report and you can enroll many different positions, so today I am going to focus on the thing I am personally interested in. This sphere is called Incident Response. The purpose of Incident response is to get several set of actions done if the intruder has already broken your perimeter and made a mess in it.

In this report I am going to cover 3 different aspects or you may say positions if you want to whose job is really necessary to react as it should be

1, Security operation center analyst

It is a person whose job involves lots of reading of different gibberish included into journal files of software in an organization to react reports from the specific software, which does the same automatically and determine whether it is really suspicious or even malicious or not.

Once the incident has happened and you got damaged you need to collect data analyze the preconditions that led to comprometation and improve your security further

2. Digital Forensics

As I already said you have to collect data, so there is a specialist that gets this job done, he collects and analyses journals finds indicators of comprometation in your corporate network. This person is in charge of isolation intruders, determine theirs gained access and capabilities, building the full model of the attack flow to detect exploited vulnerabilities and create a report with recommendations to prevent similar attacks in future

3. The third one in the workflow in a reverse engineer that cover the deep analysis of malicious binaries you have potentially gathered on step 2 of the investigation, it helps company to determine exactly what buglers have done to a system, the data extraction path and probably the author of the attack.