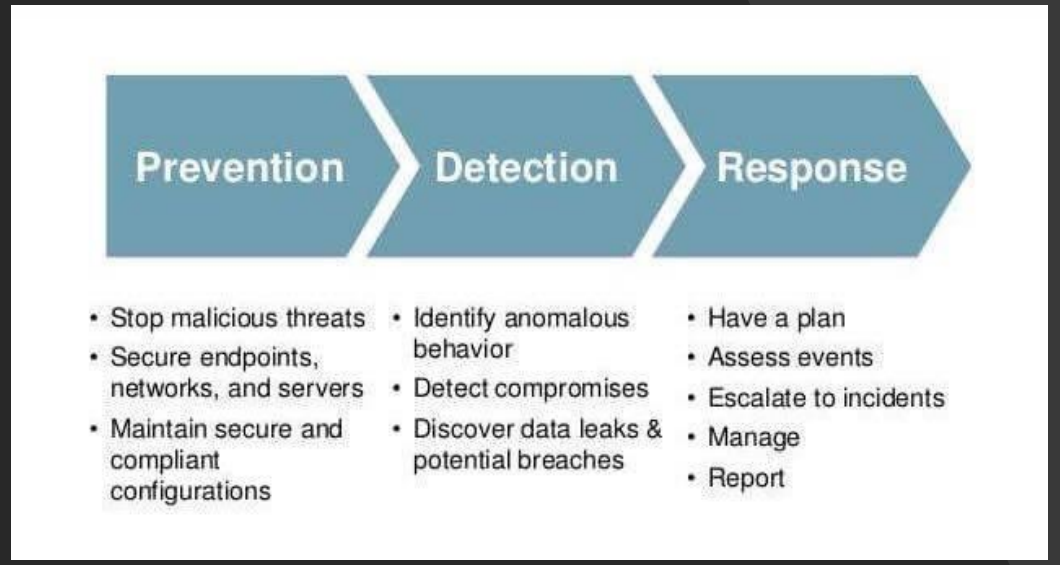
IT SECURITY

DEVELOPING AN OPERATIONAL MODEL OF COMPUTER SECURITY

The process of developing an operational model of computer security is divided into 3 phases as below:

- Prevention
- Detection
- Response



Stage 1 - Prevention

Early stage of the development process includes creating the Security Policies, Security Awareness, and Access Controls.

Security Policies

Security Awareness

Access Controls

Stage 1 - Prevention (Security Policies)

- 2 questions needs to be answer
  - “What” needs to be documented?
  - “What” needs to be protected?

- All the responsibilities of each authorised individual such as the management and employees will be mentioned separately in the security Policy.
- Another aspect of the security policy statement would be the responsibility to review and audit, enforcement and implementation of future projects related to the IT.
- The written policy needs to be consistent, concise, clear and coherent to give easy understanding for the management.

- If the policy is difficult to understand, it will creates issues in the subsequent enforcement and implementation of the policy, while the process of review and audit will be inefficient.

- Security Awareness Program will be held in the organisation to increase more awareness after designing and implementation of the IT system.
- This program will be cover topics such as:
  - ✓ Reporting process for any sort of security violation,
  - ✓ Different uses of security measures,
  - ✓ The awareness of security itself.

- The program purpose mentioned as below:
- Helping the employees and the management to get a complete guide about the importance of security aspects,
- Having all employees to participate and work in aa a team in discussing all issues faced by the organisation,
- Introducing a new reward system for those staff members who will perform a great security practice.

Stage 1 - Prevention (Security Awareness)

Stage 1 – Prevention (Access Control)

- There should be a proper management, responsible members or IT experts who can have the access to the systems in maintaining the security control systems.
- It is important for IT experts to have the ability in accessing and handling particular software within the organisation.
- In maintaning a proper access control system, user accounts will be created which will recognise each user based on several method below:

  ✓ Identification
  ✓ Authentication
  ✓ Authorisation

Identification

- The unique identification used will include different information of the user such as the network, hardware, software application, client and person’s information.
- The user will be bound to show their proper identification with the help of the proposed identification in order to get know who they are and what is their designation within the organisation.
- These identifiers will be unique and they will never be shared with the other staff members.

Authentication

- Most commonly used item is the **password**. This type of authentication is commonly known as single authentication or one-factor authentication. But this is a weak form of authentication as many a times user forgets their passwords.
- The authentication can comes in the form of **token, smart card or an identity card**. This type of authentication is known as multilevel or two-factor authentication which mainly used in offices and more reliable than the one-factor authentication.
- The strongest form of authentication is called **“Biometrics”** which using the DNA of a person, retina pattern or a finger print scanner.

Authorisation

- In this stage, only certain members who have been authenticated and identified are allowed to make use of some resources within the organisation.
- Some restrictions will be imposed to those members who are not authorised for the use of certain sites or software.
- Authorisation will help limiting only certain user on specific software.
- It provides specific access rights or privileges to the resources, which is related to information security and computer security in general and to access control in particular.

Stage 2 - Detection

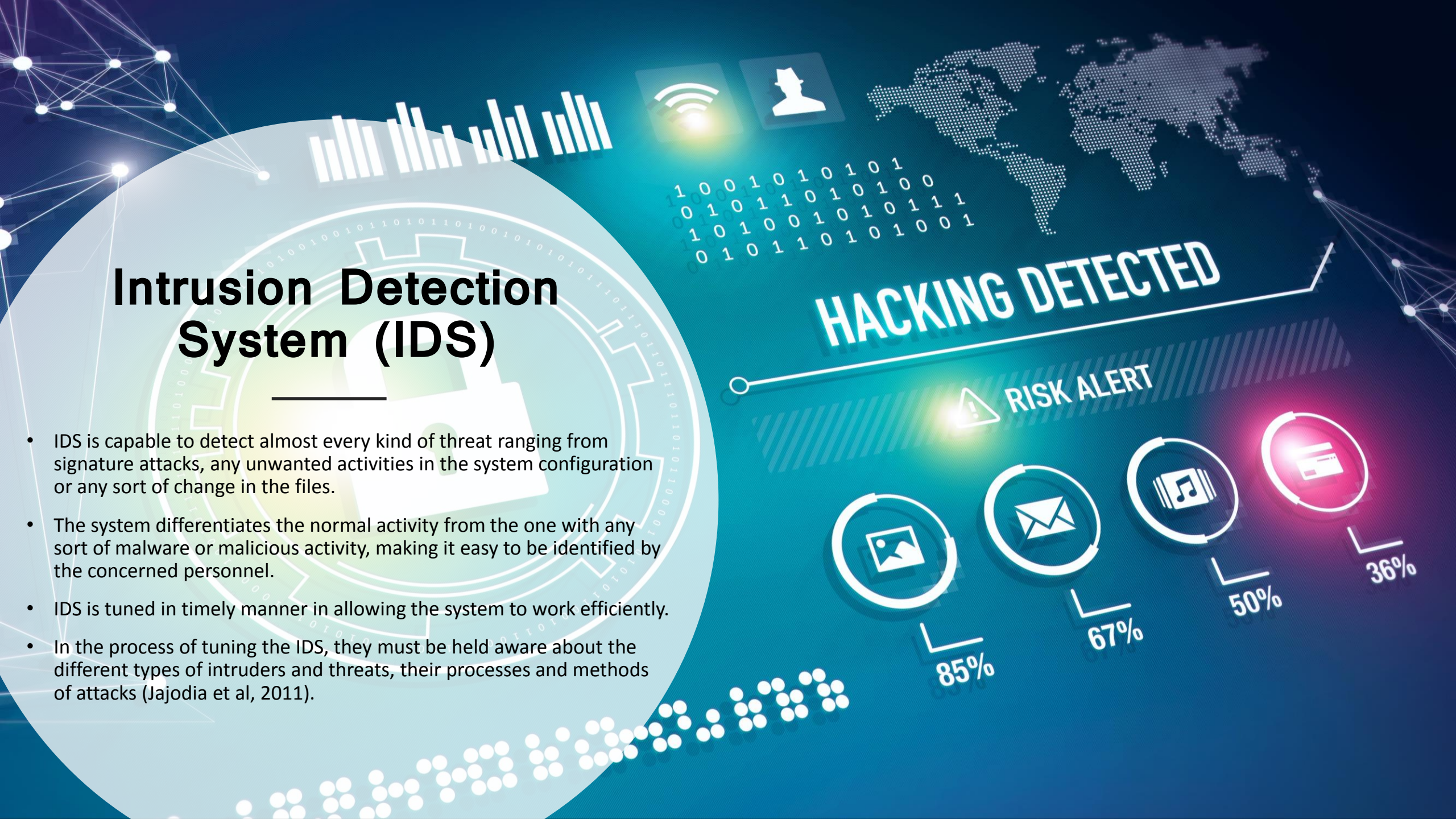
If the system fails to detect any threat, it could lead to some critical issues to the computer security system.

Therefore, it is very importance for an organization to have layered security defense strategy in ensuring the threat detection if the first system failed to do so.

One of the most intelligent system used for security threat detection is the Intrusion Detection System (IDS).

Intrusion Detection System (IDS)

- IDS is capable to detect almost every kind of threat ranging from signature attacks, any unwanted activities in the system configuration or any sort of change in the files.
- The system differentiates the normal activity from the one with any sort of malware or malicious activity, making it easy to be identified by the concerned personnel.
- IDS is tuned in timely manner in allowing the system to work efficiently.
- In the process of tuning the IDS, they must be held aware about the different types of intruders and threats, their processes and methods of attacks (Jajodia et al, 2011).



Honeypots

HONEYPOTS ARE AN ADVANCED COMPUTER ANTI-HACKING SYSTEMS WHICH ARE USED BY MANY COMPANIES IN ORDER TO PREVENT HACKERS ATTACK OR DIAGNOSE THEIR SYSTEM MORE EFFECTIVELY AND EFFICIENTLY.

BY USING HONEYPOTS, NEW TRICKS CAN BE LEARNT FROM THE HACKERS ON HOW ARE THEY HACKING INTO THE SYSTEM.

IT HELPS TO STOP HACKING ACTIVITIES INTO THE SYSTEM.

Stage 3 – Response

- This is the most important stage after the detection phase.
- Once the system has detected the threats, there must be timely response to that alarm.
- There must be an advance planning for that incident and the concerned personnel needs to response in a well manner to it.
- It is a disaster to make a plan and develop different strategies and make decisions when the attack has already occurred, so in response to that there should be a pre-plan strategy made to resolve the issues.

THE END