# Module 1 - Note

# Cybersecurity Incident Detection and Response!

* Prepare for cyber security incident.
* Set up Info sec environment.
* Analise risks and complex malware attack
* Visualize information about cyber-attacks.
* Apply countermeasures.

# 6 phases of cybersecurity detection and incident response

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lesson Learned

# Security Operations Centres (SOCs) – Evolution

# MSSP – Managed Security Service Provider

A third-party security service provider that helps company to achieve security goals by providing network security solution to prevent and mitigate security threat. A MSSP focussing on security implementation.

# Common cyber threat types

Phishing Attack = Social engineering Attack

Man in the Middle Attack (MITM)

Denied of Service Attack (DOS)

SQL Injection