0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 3

10th to 12th March 2024

جامعة فيلادلفيا
Philadelphia University

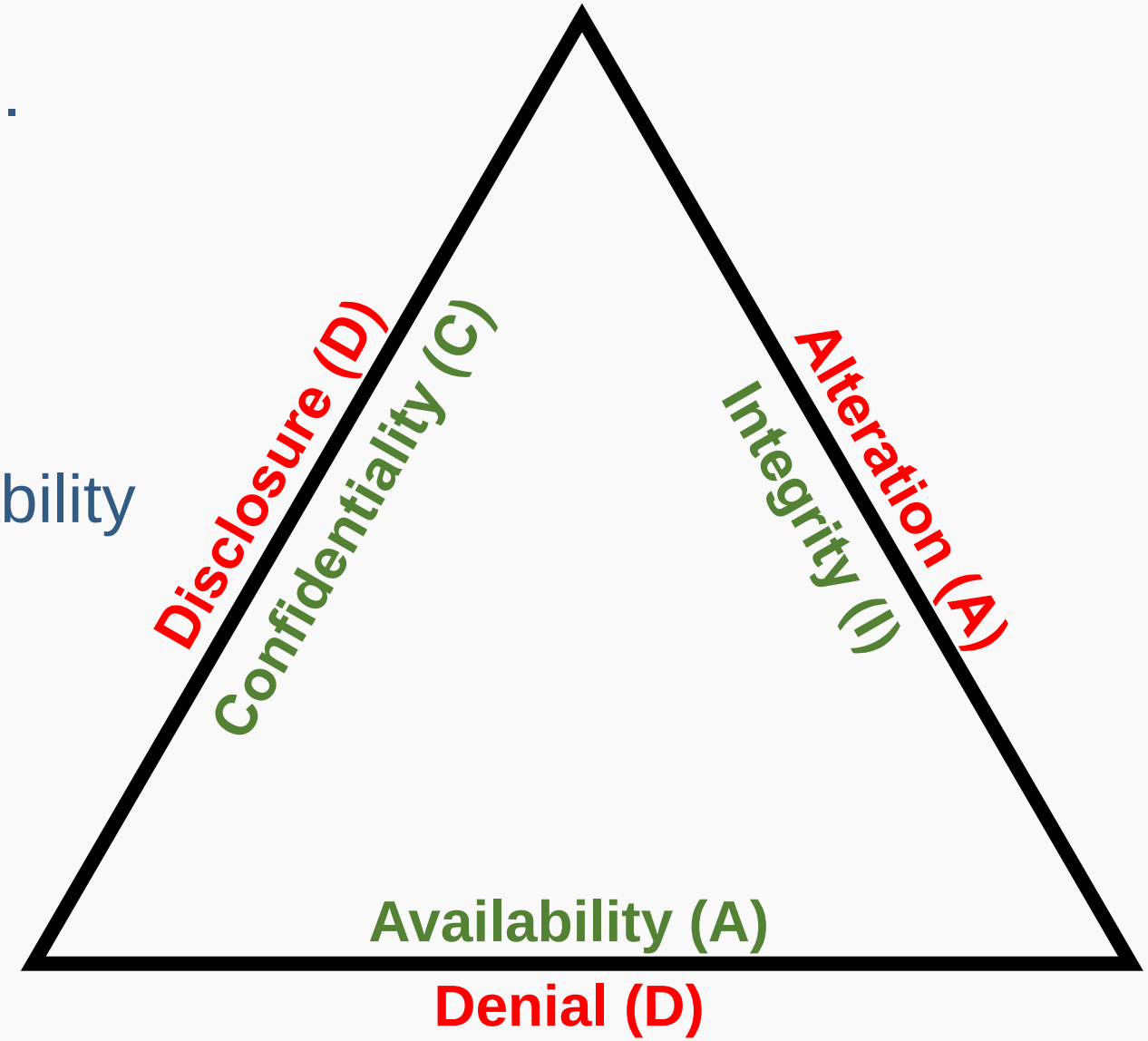
Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

General Module Overview

- Computer networks and security revision.
- Security operations, Security Operations Centre (SOC), and Network Operations Centre (NOC).
- IT Services management, and Incidents management.
- Security incidents, and incident response.
- Technical forensics of networks, malware and other computing related matters.
- Intrusion Detection Systems and Intrusion Protection Systems; IDS and IPS.
- Snort and Snort integration with other vendors.
- Wireshark and network traffic analysis.
- Cyber Threat Intelligence (CTI).

Security Goals: CIA and DAD triads

- **C**onfidentiality: authenticated and authorised parties only have access.
  - ***D****isclosure abuses Confidentiality.*
- **I**ntegrity data may be modified by authorised parties.
  - ***A****lteration abuses Integrity.*
- **A**vailability to guarantee the obtainability and accessibility of a systems and services.
  - ***D****enial abuses Availability.*
- See triad to the right.



Gold Standard

- The chemical symbol of gold in the periodical table is "**Au**".
  - Suggested by Kohnfelder (2022).
- **Authentication**: high-assurance determination of the identity of a principal.
- **Authorisation**: reliably only allowing an action by an authenticated principal.
- **Auditing**: maintaining a reliable record of actions by principals for inspection.
- A **principal** is any reliably entity: a person, an organisation entity, an application, a service, a device, an object, or any other agent with the power to interact with a computing system.

Confidentiality (C) – Disclosure (D)

- Simply to keep a system or piece of information ***confidential***, where only unauthorised people or objects cannot ***disclose***.
- Intruder may be passive: listen only, or active: listen and modify.
- Confidentiality can be achieved by cryptography algorithms, using keys.
  - Encipher or Encrypt (E): converting plaintext (P) to ciphertext (C).
  - Decipher or Decrypt (D): recovering ciphertext (C) to plaintext (P).
- Secret Key Cryptography (Symmetric). Using only ONE key (K).
  - The key is secret, but the algorithm is or at least can be public.
  - E.g.: Advanced Encryption Standard (AES).
- Public Key Cryptography (Asymmetric). Encryption key and decryption key are NOT the same.
  - Two keys: public and private. Encrypting using one, decrypting using the other.
  - E.g.: Rivest, Shamir, Adleman (RSA).

Integrity (I) – Alteration (A)

- To guarantee that a system or piece of information is ***integral*** and cannot be ***altered*** by unauthorised people or objects.
- Integrity check can be done using something called one-way function; Checksum, Hash Functions, or Message Digests (MD).
- The input is computed to produce an output, where it is extremely difficult or impossible to find the input from the output.
  - A little change in the input will produce a significant difference in the output.
- This concept can be used to check copies of the same data storage, where both must have the same exact value.
  - A message “HEY”, assuming H=8, E=5, and Y=25. 8+5+25=38.
  - Changing it to “HAY”, and assuming A=1, 8+1+25=32. $32 \neq 38$.
- Thus, intentional tampering or just innocent change can be sensed.

Availability (A) – Denial (D)

- The assurance of an ***available*** service, system, or piece of information and not ***denied*** getting to.
- While, in general, Confidentiality and Integrity has to be 100% guaranteed, any less will abuse these two goals.
- Availability may not be 100% achieved but attempts to.
- Denial of Service (DoS) attacks are the usual way to stop or reduce availability.
  - Resources are consumed or get busy, or at least reduce access to. A resource can be a Bandwidth, a CPU, a Memory, an Energy source…etc.
- Main attacking way; flooding the victim a huge number of messages.
  - Distributed DoS (DDoS); many attacking sources.
- Other non-flooding DoS; for example, spoofing an identity and send a single message indicating a cancel or session ending communication.

Security Operations Centre (SOC)

- A centralised function within an organisation employing people, processes, and technology.
- Such centre’s job is to continuously monitor and improve an organisation's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents.
- A hub or central command post, across an organisation's IT infrastructure, including its networks, devices, appliances, and information stores.
- The SOC is responsible for the security of the IT infrastructure and all the data on it.

Telemetry

- Telemetry is data collected from a network environment.
- Such data can be analysed to monitor the health and performance, availability, and security of the network and its components. In order to respond quickly and resolve network issues in real-time
- The proliferation of threats is placed by collecting context from diverse sources.
- SOC is the correlation point for every event logged within the organisation that is being monitored.
  - For each of these events, the SOC must decide how they will be managed and acted upon.

SOC Staff and Organisational Structure

- The security team monitor, detect, investigate, and respond to cyberthreats around the clock.
- The team acts as the central point of collaboration in coordinated efforts to monitor, assess, and defend against cyberattacks.
- The SOC is usually led by a SOC manager
- Incident responders,
- SOC Analysts (levels 1, 2 and 3)
- Threat hunters and incident response manager(s).
- The SOC reports to the CISO, who in turn reports to either the CIO or directly to the CEO.
  - Who are the CISO, CIO, and the CEO?

CIO and CISO

- Chief Information Officer (CIO) is a corporate executive in charge of IT strategy and implementation in an organisation.

- Chief Information Security Officer (CISO) is senior-level executive, who oversees the organisation's information, cyber, and technology security, responsible for developing and implementing the information security programme.
  - CISO most likely report to the CIO.
- Chief Technology Officer (CTO).
  - CTO look outwards, CIO looks inwards

- Chief Executive Officer (CEO). The highest-ranking person in a company

SOC Architecture

- Governance, Risk and Compliance (GRC) systems.
- Application and database scanners.
- Intrusion Prevention Systems (IPS).
- User and Entity Behaviour Analytics (UEBA).
- Endpoint Detection and Remediation (EDR).
- Threat Intelligence Platforms (TIP).

SOC Functions

1. Take Stock of Available Resources.
2. Preparation and Preventative Maintenance.
3. Continuous Proactive Monitoring.
4. Alert Ranking and Management.
5. Threat Response.
6. Recovery and Remediation.
7. Log Management.
8. Root Cause Investigation.
9. Security Refinement and Improvement.
10. Compliance Management.

SOAR General Definition

- Security Orchestration, Automation, and Response (SOAR).
- SOAR collects threat-related data from a range of sources and automate the responses to the threat.
- A collection of security software solutions and tools for browsing and collecting data from a variety of sources.
- SOAR then uses a combination of human and machine learning to analyse this diverse data to comprehend and prioritise incident response actions.
- Three software capabilities
  1. Threat and vulnerability management.
  2. Security incident response.
  3. Security operations automation.

SOAR Deeper Explanation

- The term was originally coined by Gartner (gartner.com).
  - Also defined the three capabilities.
- Threat and vulnerability management (**Orchestration**) covers technologies that help amend cyber threats
- While security operations automation (**Automation**) relates to the technologies that enable automation and orchestration within operations.
- SOC teams are looking for today:
  1. Automating Repeated Response Workflow.
  2. Save Time for Higher Priority Triage Tasks.
  3. Easy Standardised Response to follow.

Benefits of SOAR

- Sometimes SOC teams struggle with connecting different systems and collecting data from them. This may result in many *error-prone* manual processes, with the lack in the highly skilled talent to solve for all of this.
  - An increased probability of missing an alert that matters, wasting time and resources due to manual processes, and slow response times due to lack of standardised response capabilities.
- All resulting in minimising the impact of security incidents of all types, maximising value of existing security investments, and an overall reduced risk of legal liability and business downtime, achieve this:

1. Consolidate process management, technology and expertise.
2. Centralise asset monitoring.
3. Enrich alerts with contextual intelligence.
4. Automate response and perform inline blocking.