0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 6

31st March – 2nd April 2024

جامعـــــــة فيلادلفيـــــــا
Philadelphia University

Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

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.

User and Entity Behaviour Analytics (I)

- The User and Entity Behaviour Analytics (UEBA) was previously known as User Behaviour Analytics (UBA).

- UEBA uses large datasets to model typical and atypical behaviours of humans and machines within a network.

- Such baselines can identify suspicious behaviours, potential threats and attacks that traditional antivirus and malware scanners may not detect.

- This means UEBA can detect non-malware-based attacks because it analyses various behavioural patterns.

- UEBA also uses these models to assess the threat level, creating a risk score that can help guide the appropriate response.

User and Entity Behaviour Analytics (II)

- UEBA uses machine learning to identify normal behaviour and alert to risky deviations that suggest insider threats, lateral movement, compromised accounts and attacks.

- Entity can refer to IT systems, critical infrastructure, business processes, organisations, and nation-states.

- UEBA analyses the behaviour of these entities as well as individuals, though individuals are often able to act as or through such entities. To identify what a threat or attack is and what is normal use because

- For example; an attacker steals an employee’s password to log in, once inside, the attacker will not be able to mimic ‘normal’ behaviour and UEBA can detect this anomalous behaviour.

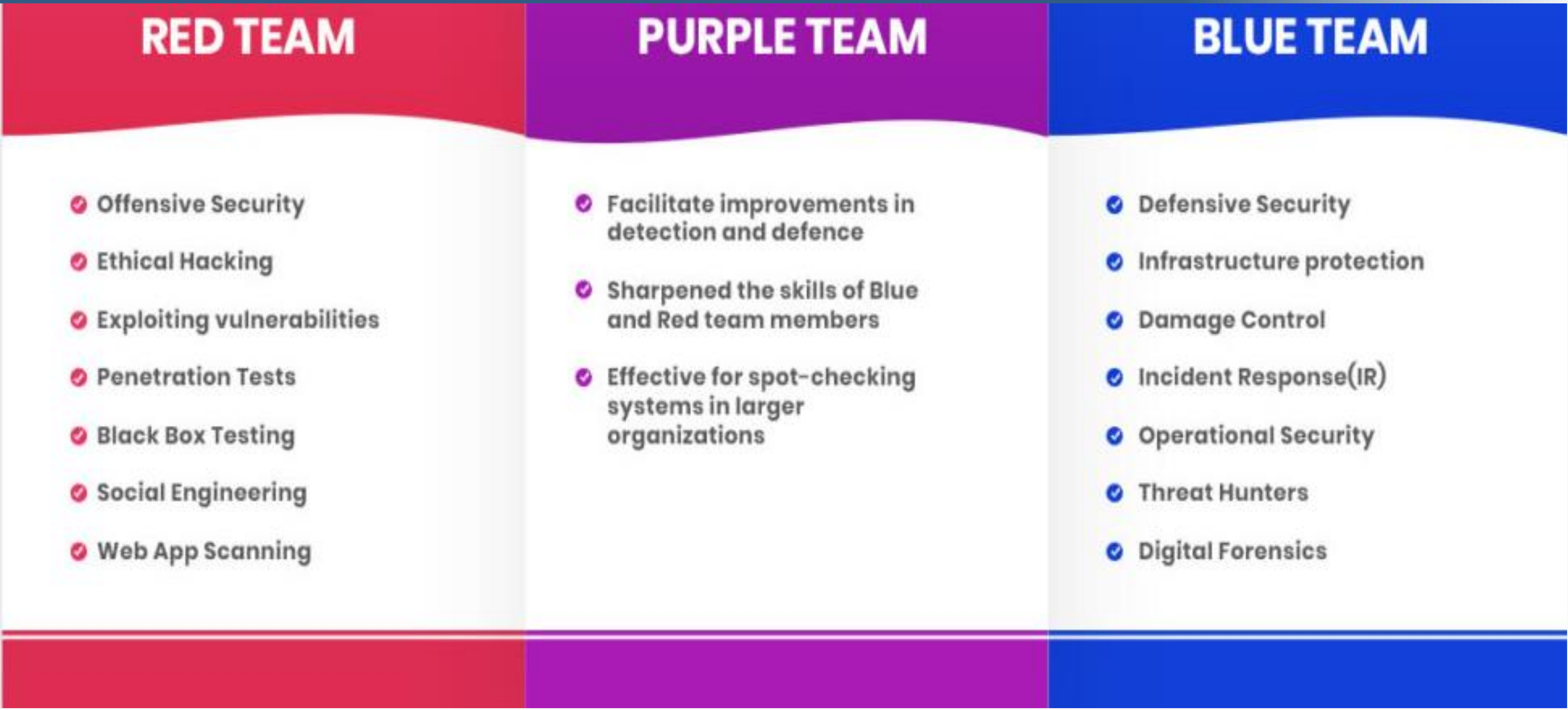
UEBA and SIEM

- UEBA and SIEM are often used together as UEBA relies on cross-organisational security data which is typically collected and stored by SIEM.
- UEBA can detect anomalous behaviours in real-time, it can issue an alert and request for a response to security analysts quickly.
- SIEM did not include behavioural analytics which meant they couldn’t monitor threats in real-time, UEBA was developed to address this.
- SIEM allows security teams to monitor threats in real-time and respond quickly to avoid attacks and address vulnerabilities making it much more effective at threat detection and analysis.
- It gives security teams the power to use sophisticated quantitative methods to gain insight into and prioritise efforts.

Red, Blue, and Purple Teams (I)

- Exercises and simulate attacks on enterprise systems and networks.
- Red teams are the adversaries, with the blue team the defendants.
- The “purple team” has entered the mix.
- The red team attacks and attempts to break the blue team's defences.
- Red teams use real-world cyber-attack techniques to exploit weaknesses in an organisation’s people, processes and technologies, without being noticed by the blue team.
- Blue team does the systems monitoring, threats and attacks detection and mitigation, network traffic, forensic and data analysis; and conducting performing vulnerability scans.
- The purple team usually or in fact, not a standalone separate team, but more a mix of blue and red team members.

Red, Blue, and Purple Teams (II)



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

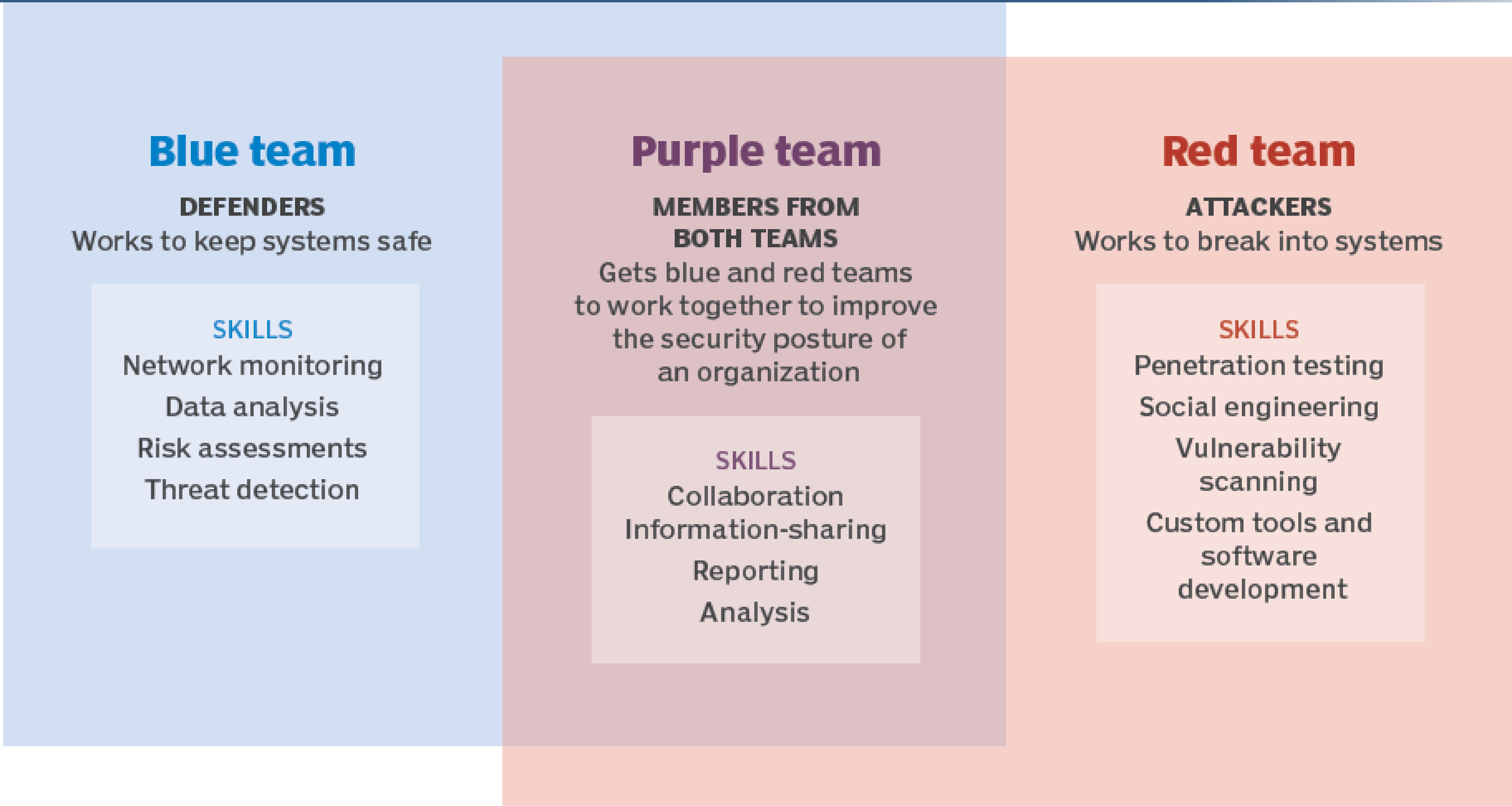
PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Red, Blue, and Purple Teams (III)



Blue team

DEFENDERS

Works to keep systems safe

SKILLS

Network monitoring

Data analysis

Risk assessments

Threat detection

Purple team

MEMBERS FROM BOTH TEAMS

Gets blue and red teams to work together to improve the security posture of an organization

SKILLS

Collaboration

Information-sharing

Reporting

Analysis

Red team

ATTACKERS

Works to break into systems

SKILLS

Penetration testing

Social engineering

Vulnerability scanning

Custom tools and software development

Indicator of Compromise (IoC)

- Indicators of Compromise (IoCs) are information about a specific security breach that can help security teams determine if an attack has taken place.
- IoCs help to identify and verify the presence of malicious software on a device or network, as an attack can leave behind traces of evidence.
- Obtaining IoCs can be by observation, analysis, and/or signatures.
- Observation: watching for abnormal activity or behaviours in systems or devices
- Analysis: determining the characteristics of the suspicious activity and analysing its impact
- Signatures: identifying known malicious software signatures

Types of IoCs (I)

- **Common types of IoCs**:
- Network-based.
- Host-based.
- File-based.
- Behavioural.
- Metadata.

- **Network-based IoCs**: such as malicious IP addresses, domains, or URLs. They can also include network traffic patterns, such as unusual port activity, network connections to known malicious hosts, or patterns of data exfiltration.

Types of IoCs (II)

- **Host-based IoCs**: are related to activity on a specific host, such as a workstation or server. Examples of host-based IoCs include file names or hashes, registry keys, or suspicious processes running on the host.
- **File-based IoCs**: include malicious files, such as malware or scripts used by an attacker.
- **Behavioural IoCs**: include different types of suspicious behaviour, such as unusual network traffic patterns or system activity, unusual logins or authentication attempts, or unusual user behaviour.
- **Metadata IoCs**: are related to the metadata associated with a particular file or document, such as the author, creation date, or version information.

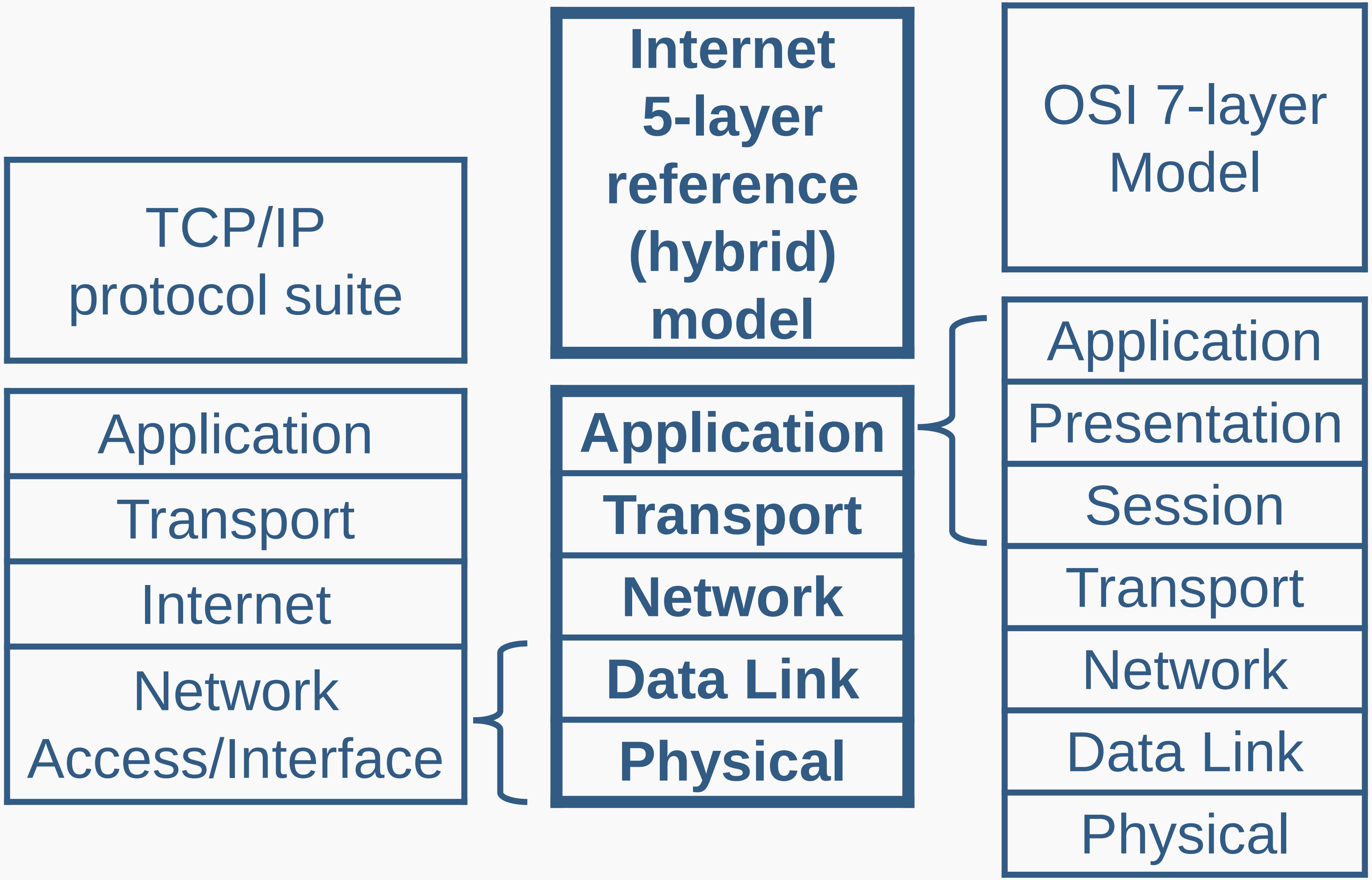
Indicators of Attack (IoA)

- Indicators of Attack (IoA) are the likelihood that a specific action or event may result in a threat.
- IoCs are similar to IoAs, but they are not exactly same.
- While IoA might indicate a high probability that an attack is planned to be launched, an IoC could be evidence of some unauthorised access to a network or system, such as the transfer of large amounts of data.
- IoC best practices include:
- Using automated and manual tools to monitor and analyse evidence of cyber attacks.
- Regular update of IoC procedures as new technologies and attack vectors emerge.
- What is the meaning of an attack vector, or threat vector?

Watching Attacks – Live Demo

- Kaspersky Cyber Threat Map
  - https://cybermap.kaspersky.com.
- Fortinet Cyber Attack Map.
  - https://threatmap.fortiguard.com.
- Oracle Internet Intelligence Map (*discontinued*).
  - https://map.internetintel.oracle.com.
- Digital Attack Map.
  - https://www.digitalattackmap.com.
- Checkpoint Cyber Threat Map
  - https://threatmap.checkpoint.com.

Computer Networks Layers



TCP/IP protocol suite

- Application
- Transport
- Internet
- Network Access/Interface

Internet 5-layer reference (hybrid) model

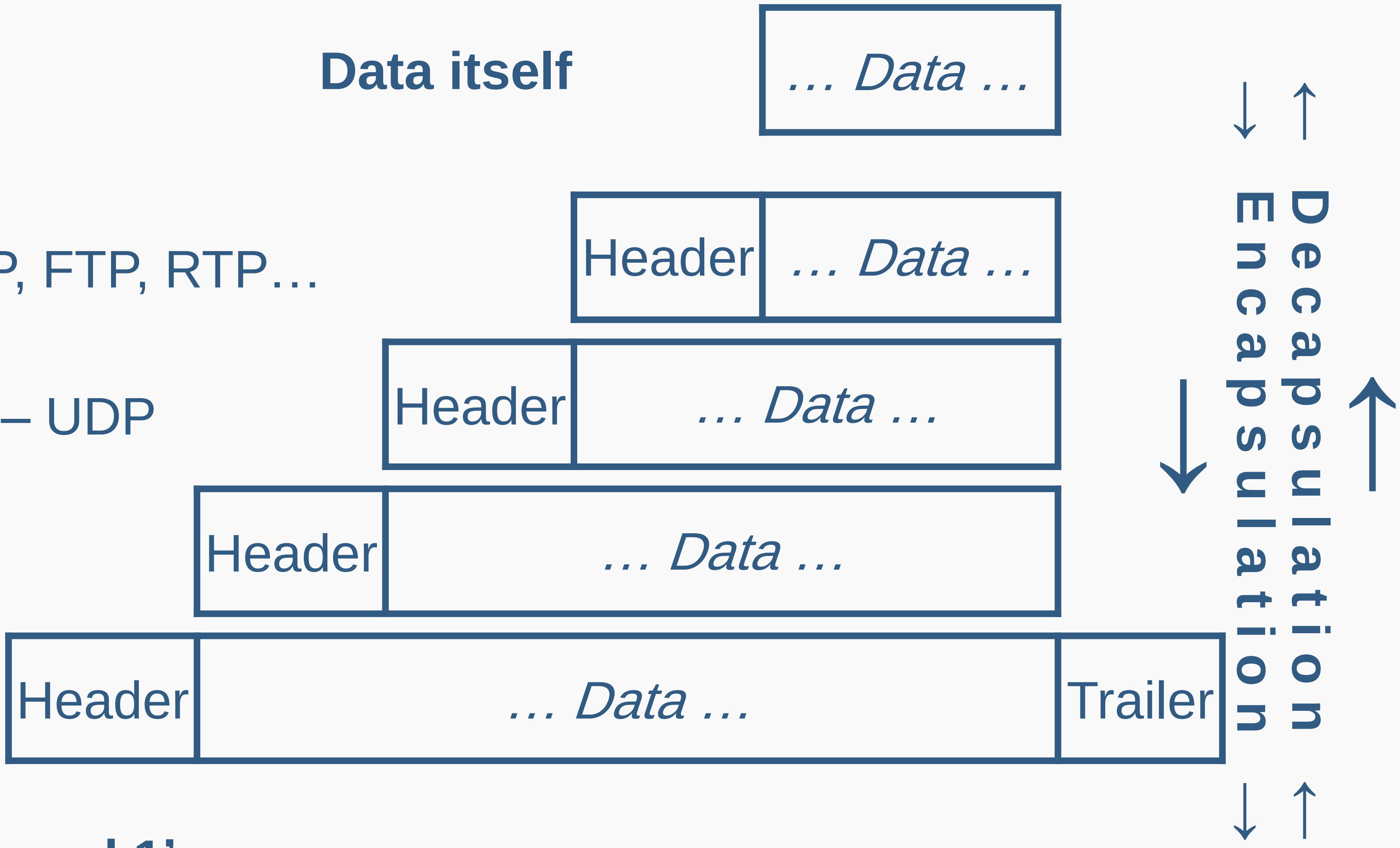
- **Application**
- **Transport**
- **Network**
- **Data Link**
- **Physical**

OSI 7-layer Model

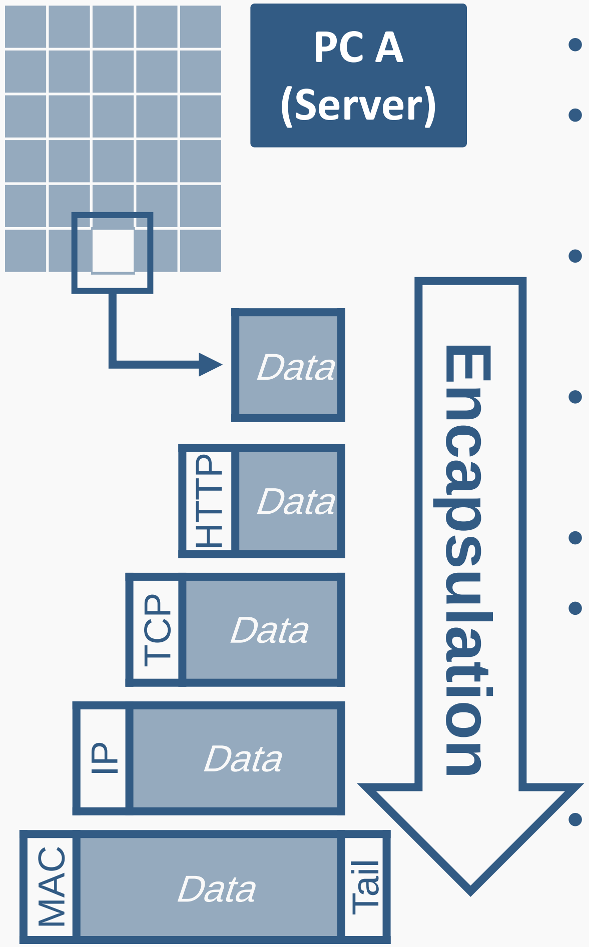
- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

Encapsulation and Decapsulation

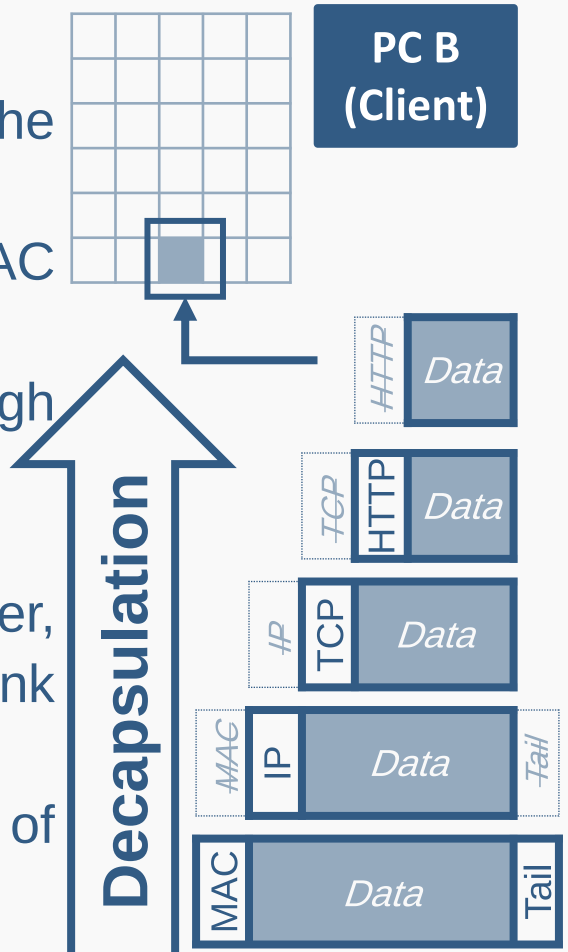
5-layer model		
Application	**Message**	HTTP, FTP, RTP…
Transport	**Segment**	TCP – UDP
Network	**Packet**	IP
Data Link	**Frame**	*MAC*
Physical	**… 0's and 1's …**	



Encapsulation and Decapsulation Example



- Server A sends a webpage to B, after B has requested it.
- The page is broken down into chunks.
- Each chunk is appended with headers then sent to B via the internet.
- HTTP header is added, then TCP, then IP, then the MAC header and trailer to create a “Frame”.
- The frame is converted to 0’s and 1’s, then A push it through the connecting media to B.
- B receives the bits and gather them into a frame.
- B removes the MAC header and trailer, then the IP header, then the TCP header, then the HTTP header, to get a chunk of the page. At the end B adds this chunk to the page.
- Each chunk is sent in such way to create a full display of the webpage.


PC B
(Client)
HTTP
Data
TCP
HTTP
Data
IP
TCP
Data
MAC
IP
Data
Tail
MAC
Data
Tail
Decapsulation