FALSE POSITIVE (FP)

FALSE NEGATIVE (FN)

TRUE POSIIVE (TP)

TRUE NEGATIVE (TN)

FALSE POSITIVE

TA false positive occurs when a security system incorrectly identifies a benign activity or event as malicious.
This can lead to wasted resources, as security analysts spend time investigating non-issues. It can also cause alert fatigue, where the sheer volume of false alarms leads to real threats being overlooked.

Example:
An intrusion detection system (IDS) flags normal network traffic as a potential data exfiltration attempt.

FALSE NEGATIVE

A false negative occurs when a security system fails to identify an actual malicious activity or event.
This is more dangerous than a false positive, as real threats go undetected and can cause significant damage without being noticed.

- **Example:**

Malware bypasses an antivirus program's detection, allowing it to infect the system without raising any alerts.

TRUE POSIIVE

A true positive occurs when a security system correctly identifies a malicious activity or event. True positives indicate that the SOC's detection mechanisms are functioning correctly, successfully identifying real threats.

- **Example**:

An intrusion detection system (IDS) alerts on an actual malware attack, and subsequent investigation confirms the presence of malware.

TRUE NEGATIVE

A true negative occurs when a security system correctly identifies benign activity as non-malicious. True negatives show that the SOC's systems are not generating unnecessary alerts for legitimate activities, thereby reducing the workload on analysts and avoiding alert fatigue.

- **Example**:

Normal network traffic from routine business operations is correctly identified as non-threatening, and no alerts are generated.