LEMUEL OKECHUKWU

VEPH/20B/CY082

TASK 30A

**SIEM and SOAR Explained**

**TASK 30A:**

* Provide a detailed explanation of SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response), and explain its differences and which will you recommend
* Can you explain the concepts of true positive, true negative, false positive and false negative in cybersecurity, including how each method operates and the mechanisms they use to identify threats?

[](https://www.linkedin.com/pulse/what-main-differences-between-siem-soar-ina-nikolova-ph-d-)

SIEM (Security Information and Event Management) is a cybersecurity tool that collects and analyzes security data from multiple sources to detect and respond to security events in real-time. It provides a centralized view of an organization's IT security by consolidating data from various sources, including network devices, systems, and applications, making it easier to detect, manage, and respond to security events. SIEM tools are vital in today’s cybersecurity front line. They provide a centralized view of an organization’s IT security by collecting data from various sources, including network devices, systems, and applications. By consolidating this data into a single system, SIEM tools make it easier to detect, manage, and respond to security events.

SOAR (Security Orchestration, Automation, and Response) is an approach to cybersecurity that combines various security technologies to improve the efficiency and effectiveness of incident response processes. SOAR platforms integrate with a wide range of security tools, such as SIEM systems, intrusion detection and prevention systems (IDPS), and endpoint detection and response (EDR) solutions. They use automation, orchestration, and predefined incident response playbooks to handle repetitive tasks, allowing analysts to focus on complex threats.

**Components of SIEM:** A [SIEM solution](https://www.manageengine.com/log-management/top-siem-tools.html?source=siem-vs-soar) analyzes the log data to detect threats and helps you adhere to compliance standards. Its core components are:

* **Log collection**: Ingesting logs from servers, firewalls, workstations, databases, applications, cloud services, etc.
* **Parsing and categorizing**: Aggregating and processing raw logs collected from different sources into a standard format.
* **Correlation and reporting**: Finding patterns, spotting anomalies with use cases, assigning risk scores based on severity, and issuing alerts to the SOC team.

**components of SOAR**

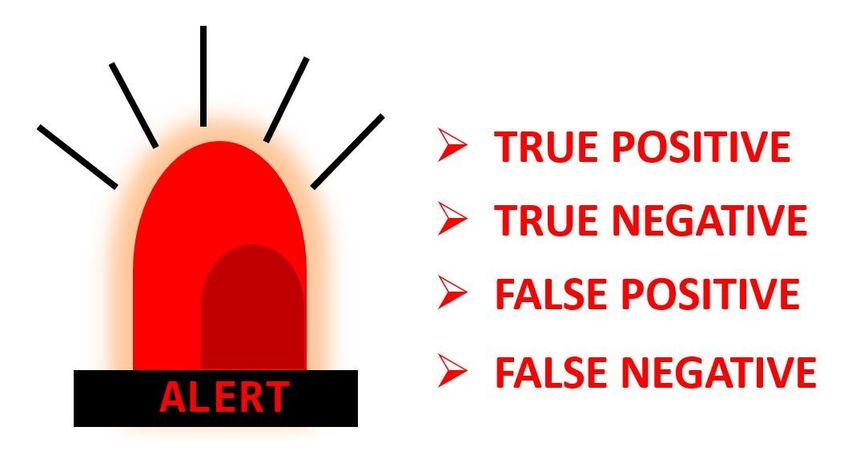
* **Ingest alerts**: Fetches threat feeds from SIEM, external threat intelligence, and other API-based platforms.
* **Orchestration and automation**: Automatically investigates threats by integrating with various associated tools and solutions.
* **Threat Response**: Implements a quick and automatic fix as instructed by a playbook or workflow.
* **Resolution**: Builds insights with advanced threat analytics and escalates if necessary by automatically assigning tickets for follow-up and further investigation by an analyst.

The key differences between SIEM and SOAR are:

* SIEM primarily focuses on collecting and analyzing security event data, while SOAR extends these capabilities through automation, orchestration, and predefined incident response playbooks.
* SIEM tools provide real-time analysis of security alerts, whereas SOAR combines data collection and other tools into a single solution.

Regarding which to recommend, it depends on the specific needs of an organization. SIEM is essential for organizations that need to collect and analyze security data from multiple sources to detect and respond to security events in real-time. SOAR is beneficial for organizations that want to improve the efficiency and effectiveness of their incident response processes by automating repetitive tasks and allowing analysts to focus on complex threats.

In conclusion, both SIEM and SOAR are indispensable cybersecurity tools catering to distinct functions. SIEM is crucial for real-time security event management, while SOAR enhances security operations through automation and orchestration.

[](https://www.linkedin.com/pulse/why-we-should-know-true-positive-negative-false-asif-ali)

Understanding true positive (TP), true negative (TN), false positive (FP), and false negative (FN) is crucial for evaluating the performance of a classification model or test. In cybersecurity, a true positive would correctly identify a threat, ensuring that security measures are triggered appropriately, whereas a false positive might trigger unnecessary alerts, potentially leading to resource wastage or user frustration. A false negative, on the other hand, could allow a threat to go undetected, posing a significant risk.

A true positive occurs when a security tool correctly identifies a threat or vulnerability, leading to appropriate action being taken to mitigate or eliminate it. For example, an intrusion detection system (IDS) correctly detecting and reporting an attempted cyber-attack would be considered a true positive.

A true negative happens when a security tool correctly identifies that there is no threat or vulnerability. This means the system has accurately determined that the activity observed is safe and does not require any intervention.

A false positive is when a security tool incorrectly identifies a threat or vulnerability where there is none. This can lead to unnecessary alerts and investigations, potentially overwhelming security teams and causing alert fatigue.

A false negative occurs when a security tool fails to identify a real threat or vulnerability, allowing it to go undetected. This can be particularly dangerous as it allows attackers to operate undetected, potentially leading to more severe consequences such as data breaches or unauthorized access to sensitive data.

These concepts are critical for evaluating the performance of security tools and strategies. Security operations (SecOps) teams rely on security information event management (SIEM) and extended detection and response (XDR) artificial intelligence to classify attacks based on their learning engines and process security telemetry over time. However, due to the vast amount of security telemetry messages received within SecOps, alert fatigue can affect the entire monitoring team.

Organizations should develop a strategy based on these four principles of classification models and the proper workflow for cybersecurity. This includes understanding the implications of each classification and developing appropriate responses, such as mobilizing escalation teams, contacting the press and customers, or possibly contacting their cyber insurance carrier.

To minimize false negatives and false positives, organizations need to ensure that their security tools are accurately configured and that their detection algorithms are robust. This involves continuous monitoring, updating security rules and policies, and implementing training for security teams to handle alerts effectively.

In summary, knowing about TP, TN, FP, and FN is essential for evaluating the effectiveness and reliability of tests and models, ensuring that decisions based on these evaluations are as accurate and informed as possible.