ASSIGNMEN
T-3

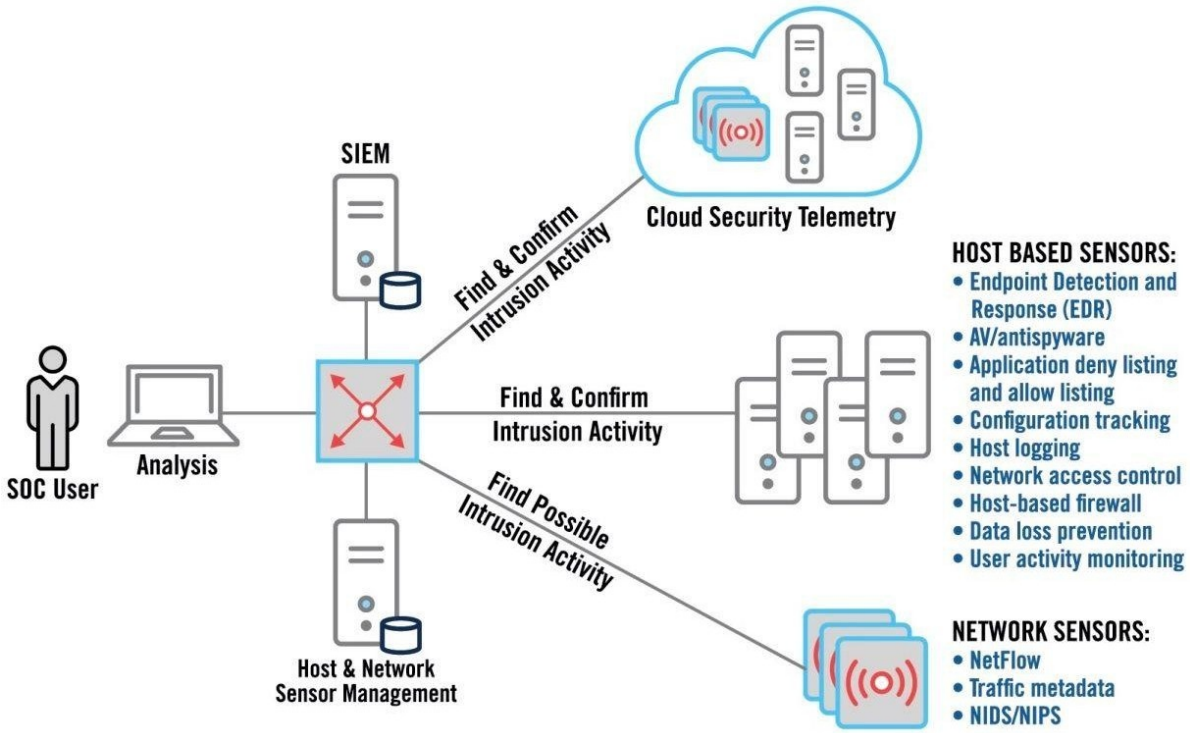
Name : shaik nihal ahmed

SOC and SIEM: The Role of SIEM Solutions in the SOC

Security teams building a security operations center face several commonchallenges:

- **Limited Visibility** – A centralized SOC does not always have access to all organizational systems. These could include endpoints, encrypted data, or systems controlled by third parties which have animpact on security.
- **White Noise** – A SOC receives immense volumes of data and muchof it is insignificant for security. Security Information and Event Management (SIEM) and other tools used in the SOC are getting better at filtering out the noise, by leveraging machine learning andadvanced analytics.
- **False Positives and Alert Fatigue** – SOC systems generate large quantities of alerts, many of which turn out not to be real security incidents. False positives can consume a large part of security

analysts' time, and make it more difficult to notice when real alerts occur.



TIER 1 – Event Classification

Tier 1 Analysts monitor user activity, network events, and signals fromsecurity tools to identify events that merit attention.

TIER 2 – Prioritization and Investigation

Tier 1 Analysts prioritize, select the most important alerts, and investigatethem further. Real security incidents are passed to Tier 2 Analysts.

TIER 3 – Containment and Recovery

Once a security incident has been identified, the race is on to gather more data, identify the source of the attack, contain it, recover data and restore system operations.

TIER 4 – Remediation and Mitigation

SOC staff work to identify broad security gaps related to the attack andplan mitigation steps to prevent additional attacks.

TIER 5 – Assessment and Audit

SOC staff assess the attack and mitigation steps, gather additional forensic

data, draw final conclusions and recommendations, and finalize auditingand documentation.