**Understanding the differences between SIEM and IDS**

**Concept of SIEM**

Security Information and Event Management or SIEM is a collection of different services and tools which are used to view the information security of the organization. SIEM provides two types of services which are anomaly detection and threat detection. Anomaly detection refers to the detection of anomalies in network traffic. Threat detection on the other hand refers to the detection of threats. These services are provided by SIEM using different types of techniques.

Anomaly detection uses statistical analysis to detect anomalies. Threat detection uses machine learning algorithms to detect different threats. Both methods rely on analyzing network traffic over time. When an anomaly occurs, the algorithm detects the anomaly. When a threat occurs, the algorithm detects the threat. Although SIEM performs anomaly detection and threat detection, it does not perform reverse engineering which refers to the process of identifying the source of a packet.

**Concept of IDS**

Intrusion Detection System, also known as IDS is a type of system that is associated with monitoring the network traffic for the detection of any kind of malicious activities. When any malicious activities are identified, it immediately gives an alert.IDS identifies the source of a packet. IDS can help the administrator to find out the root cause of the problem.IDS does not perform reverse engineering. However, IDS can identify the source of a packet. So, IDS can help the administrator to find out the root cause of the problem.IDS helps the administrator to detect threats.

**SIEM vs IDS - their dissimilarities**

Technology is increasing at an exponential rate with each passing minute, and so is the rate of cyber threats and different types of cyber attacks. Presently, there is an increased rate of growth in cyber attacks. With the increase of these attacks, new technologies and tools have been introduced to minimize their risk and effects. It is important to have a clear understanding of them and their method of operation.

SIEM and IDS both are related to the domain of cybersecurity. Both are mainly introduced as a solution to cyber crimes. But there are various points and features that separate the two in terms of meaning, method of operation, etc. Given below are some of them.

1. One of the most fundamental differences between SIEM and IDS is that SIEM is used as a preventive action and IDS is used to direct any kind of suspicious activities and generate alerts in case of finding suspicious activity.SIEM is not responsible for monitoring the entire network traffic.

2. The second difference between both these technologies is their ability and disability to find the root cause of a particular type of threat. SIEM lacks the ability to determine the root cause of a problem due to the fact that it does not perform reverse engineering. On the other hand, IDS generally identifies the source packet and therefore can easily detect the root cause of the problem.

3. The working procedure of IDS is a passive one.IDS can’t prevent any attack. Nor can it prevent the attack from exploiting the data. On the other hand, SIEM tools suggest users take necessary actions to prevent the attack from spreading and exploiting.

In order to completely protect the overall organization environment against any kind of malpractices and cyber crimes, both of these tools work together. The primary function of IDS is to detect any kind of threats, violations, or malicious activities and inform them about them. SIEM is given the alert and notification about the possible threats and to further the administrator about it and suggest suitable measures to prevent it and minimize its effect, if any.

**References**

1.<https://www.logsign.com/blog/ids-vs-siem-what-is-the-difference/>

2.<https://www.comodo.com/difference-between-siem-and-ids.php>

3.<https://hackcontrol.org/blog/siem-vs-ids/>

4.<https://www.bitlyft.com/resources/from-ids-and-ips-to-siem-everything-you-need-to-know>

5.<https://www.reddit.com/r/cybersecurity/comments/rms7a3/difference_between_siem_and_ids/>

6.<https://blog.cygilant.com/blog/making-sense-of-information-security-technologies-ids-ips-utm-and-siem>

7.<https://www.upguard.com/blog/siem-vs-ids>