# The data that can be analyzed and used to enhance cyber security

Data collection is critical component in cyber security as security data is used in Security Operations to detect, investigate and respond to security incidents. This data allows your security team to create a clear picture of organization's infrastructure and help them to make their security planning and apply the security solutions accordingly to protect organization data.

**Example of Data sources in Cyber Security are:**

### 1- Logs and event data:

Logs are the data generated by various devices, applications, systems within organization as record. These records contain information that is valuable for organization Security Operation team to completely visualize the activites and behavior of their networks and system and monitor them for any incident. The logs are then centralized in single location where SOC team apply their security solutions such as SIEM (Security Information and Event Management) to check for alerts so security team can detect and respond to the situation accordingly.

### 2- Hosts and Endpoint data:

Endpoints are the components and devices in organizations such as servers, firewalls, IPS/IDS, honeypots that generates logs as the security information. These logs generated are sent to SIEM as centralized location for logs collection and processing to detect and respond cyberattacks. This Data Includes Timestamps, Endpoint ID, User, Process, Source IP, Destination IP, actions taken by endpoint etc.

### 3- Threat Intelligence feeds:

Threat intelligence feeds are the valuable information about current and emerging cybersecurity threads, that help organizations to enhance their existing cybersecurity structure by staying informed about the current risks and vulnerabilities present on internet. These feeds help security experts to patch-up their security solutions capabilities to detect and respond to the new threads. This include Commercial Feeds, IOCs (IP Addresses and Domain Names), Threat Actors and TTPs (Tactics, Techniques, and Procedures), CVEs (Common Vulnerabilities and Exposures).

### 4- Network Traffic Data:

Network traffic data is a valuable source of information for SOC analysts, helping them identify potential threats, detect anomalies, and respond to security incidents.

This Data includes Raw Packets, Header Information, NetFlow or IPFIX, Deep Packet Inspection (DPI) which SOC analysts use to investigate about the security incident over the network.

## 5- Security alerts and incidents:

Security alerts and incidents are the notifications generated by SIEM solutions when it detects any malicious activity on endpoint devices on organization's network. These alerts are alarmed to bring attention to potential security incident. Security analyst can use these alerts to visualize the breach and enabling timely investigation and response.

Alerting makes it possible for people to keep up with the information that matters most to them.

## 6- Vulnerability scan:

Vulnerability scanning is a crucial aspect of cybersecurity, and a SOC plays a key role in monitoring and responding to security incidents. These logs contain information about the vulnerabilities exist in organization network and the severity level of them so that how Security analyst can remediate according to vulnerabilities so they can be safe from cyberattacks. This includes Outdated software versions, unpatched systems, weak passwords, misconfigured settings, open ports without proper restrictions.

## Conclusions:

Cyber security relies on the analysis of diverse data sources such as logs, endpoint information, threat intelligence feeds, network traffic data, security alerts, and vulnerability scans. These sources enable security teams to detect, investigate, and respond to security incidents effectively, enhancing overall organizational security posture.