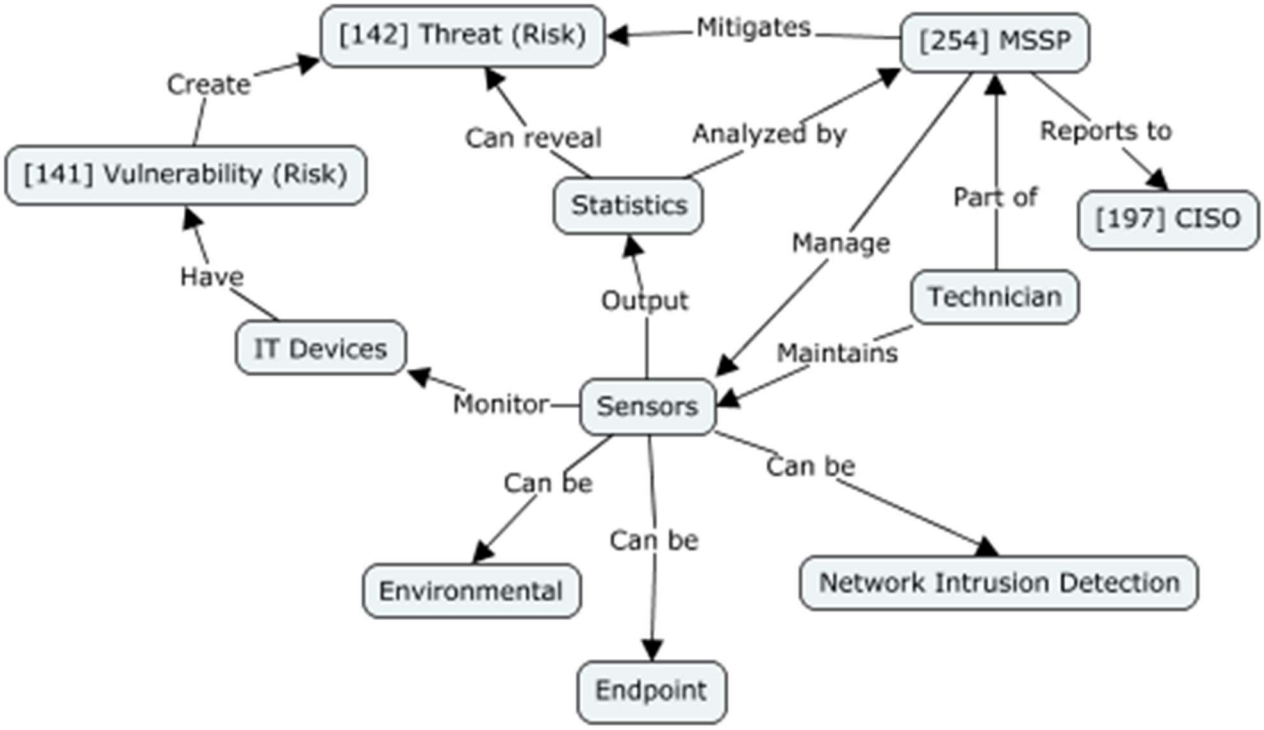
1 – Concept Map – Driver



Concept	Definition (one sentence per concept)
[141] Vulnerability (Risk)	Weakness of an asset or control that can be exploited by one or more threats.
[142] Threat (Risk)	Potential cause of an unwanted incident, which can result in harm to a system or organization.
[197] CISO	Senior-level executive responsible for developing and implementing an information security program.
[254] MSSP	Provides outsourced monitoring and management of security devices and systems.
Statistics	Analytics on the data supplied by the sensors.
Sensors	Devices that provide real-time data about an information system's environment.
Technician	Qualified personnel that repair and upgrade the sensors.
IT Devices	Devices that receive and send information that needs to be protected.
Environmental (Sensor)	Type of sensor that monitors activity on individual devices for signs of malware or unauthorized access. Also known as Host-Based sensors.
Endpoint (Sensor)	Type of sensor that measures environmental factors such as temperature, humidity and fire.
Network Intrusion Detection (Sensor)	Type of sensor that monitors network traffic for suspicious activity.

2 – Description of the driver and its relevance

Sensors provide real-time data and insights into various aspects of an information system's environment. They fulfill the need for continuous monitoring and data collection within information systems, gathering data on parameters such as network traffic, system performance, environmental conditions, and user behavior. This continuous monitoring is essential for detecting anomalies, identifying potential security threats, and ensuring the smooth functioning of the system.

There are several types of sensor products available for different purposes in information systems security and management. These include network intrusion detection sensors, which monitor network traffic for suspicious activity; environmental sensors, which measure temperature, humidity, and other environmental factors in data centers to prevent equipment damage; and endpoint sensors, which monitor activity on individual devices for signs of malware or unauthorized access.

Sensors are often integrated into managed security services, where third-party providers offer continuous monitoring and threat detection services to organizations. Additionally, consulting services are offered to help organizations design and implement sensor-based monitoring solutions tailored to their specific security needs.

Effective governance ensures that sensor data is collected, stored, and analyzed in accordance with organizational policies and legal requirements. This includes defining roles and responsibilities for managing sensor infrastructure, establishing data retention policies, and ensuring that sensor data is used ethically and responsibly. Risk management is crucial as sensors can introduce risks such as data breaches if they are not properly secured. Organizations need to assess the risks associated with deploying sensors, including the risk of unauthorized access to sensor data, the risk of false positives or false negatives in threat detection, and the risk of reliance on outdated or inaccurate sensor data.

Compliance with regulations such as GDPR is critical when using sensors to collect and analyze data in information systems. Organizations must ensure that sensor data is collected and handled in compliance with relevant regulatory requirements, including data protection, privacy, and security standards. This involves implementing appropriate security controls, conducting regular audits of sensor systems, and maintaining documentation to demonstrate compliance.

3 – Examples of real cases

In 2017, Equifax, one of the largest consumer credit reporting agencies, suffered a massive data breach that exposed the personal information of approximately 147 million people. This breach occurred due to a failure in their security infrastructure, but it also highlighted the importance of effective sensor-based monitoring. Equifax had various sensors in place, but they failed to detect the breach in its early stages. [1]

After the breach, Equifax revamped its security measures, including its sensor systems. They invested in advanced intrusion detection sensors and improved their network monitoring capabilities. With the new sensor infrastructure, Equifax was able to detect and thwart several attempted breaches, thus preventing potential data leaks and maintaining the trust of their customers. This case demonstrates how effective sensor-based monitoring can prevent future breaches and protect sensitive information.

In 2013, Target Corporation, one of the largest retail chains in the United States, suffered a significant data breach during the holiday shopping season. Hackers gained access to Target's network through a third-party HVAC vendor and installed malware on the company's point-of-sale systems. The breach resulted in the theft of credit card information from over 40 million customers.[2]

One of the key failures in Target's security infrastructure was the lack of effective endpoint sensors. These sensors could have detected the presence of malware on the compromised systems and alerted Target's security team. However, due to inadequate monitoring, the malware remained undetected for several weeks, allowing the hackers to exfiltrate sensitive data.

The Target breach shows the importance of comprehensive sensor-based monitoring in retail environments. If Target had implemented robust endpoint sensors and continuously monitored their systems for suspicious activity, they could have detected the breach much earlier and mitigated its impact. This failure serves as a cautionary tale for organizations, emphasizing the critical role of sensors in detecting and responding to security threats effectively.

4 – References

[1] https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html accessed on 2/5/2024
[2] https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/ accessed on 2/5/2024
[3] https://standards.ieee.org/beyond-standards/why-are-sensors-the-key-to-iot-cybersecurity/ accessed on 3/5/2024