



Driver Sensors

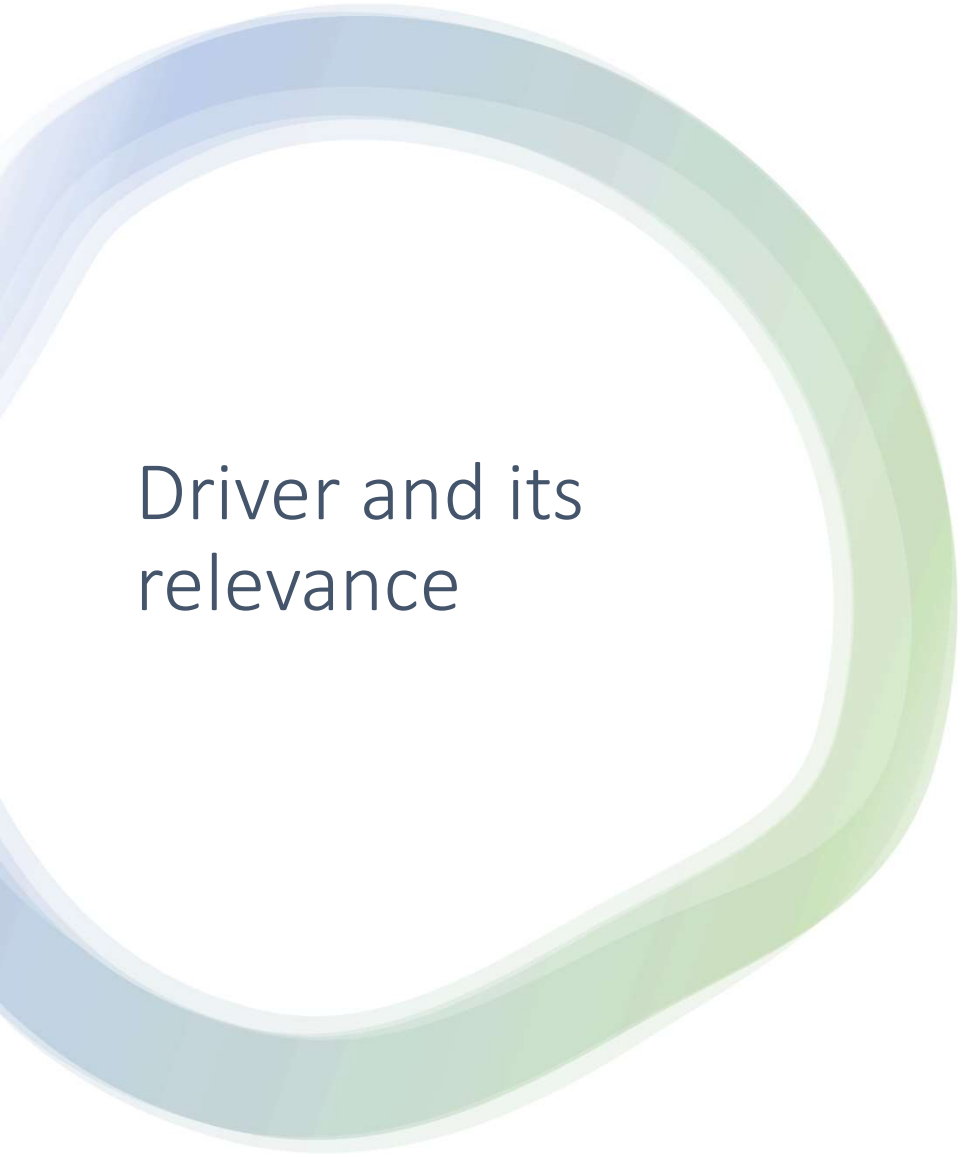
Group P1T12

João Costa (99088)

João Marques (99092)

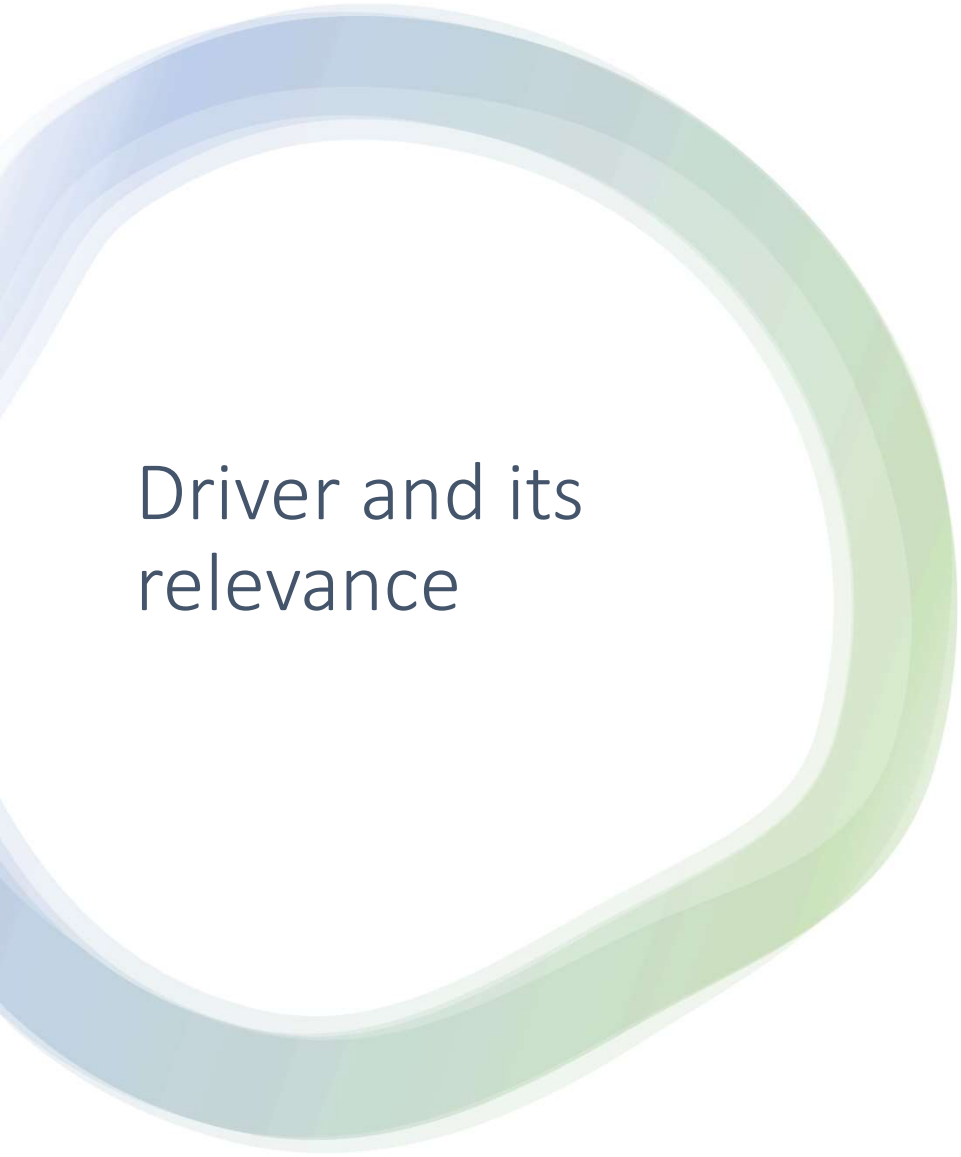
Security and Management of Information Systems

2023/2024



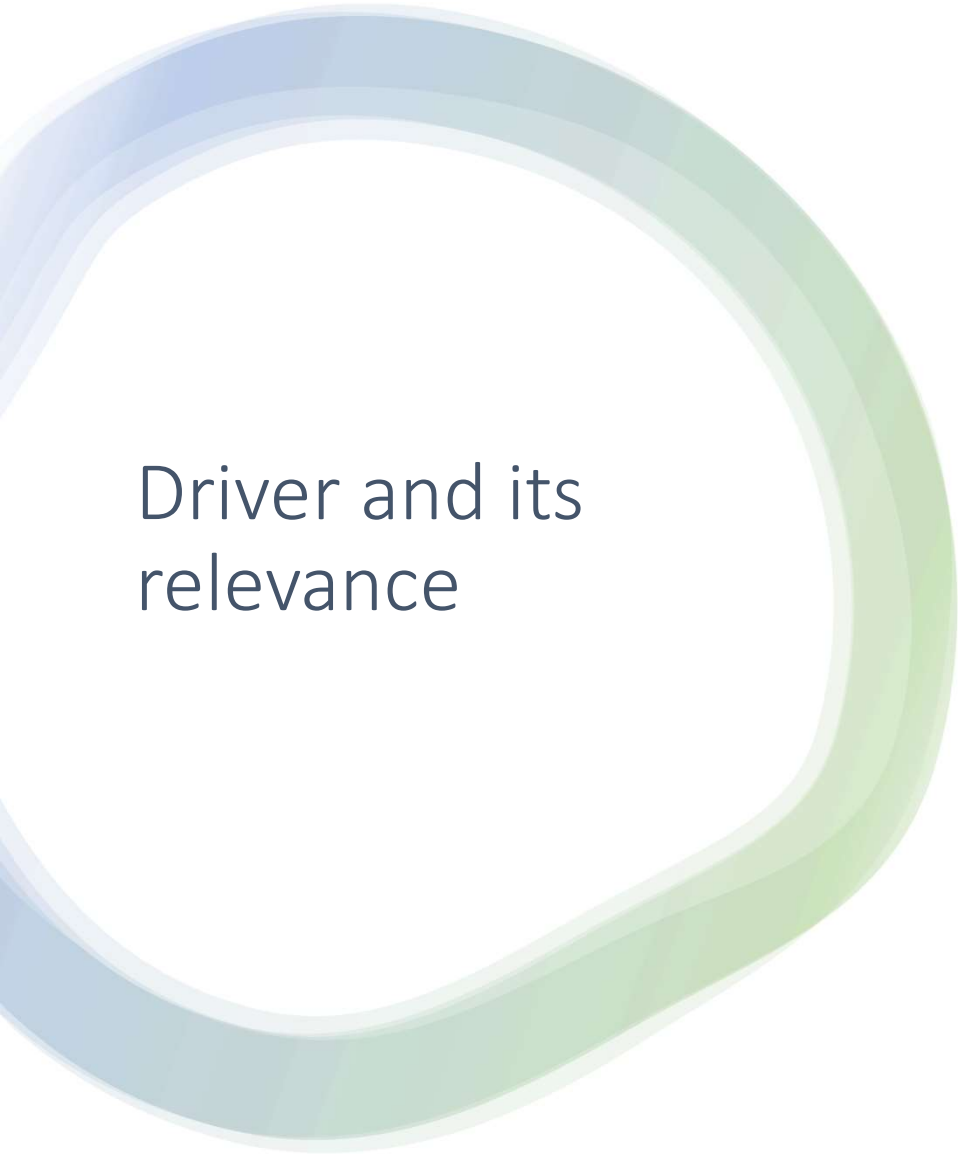
Driver and its relevance

- Definition: Sensors provide real-time data and insights into various aspects of an information system's environment.
- Importance: Continuous monitoring and data collection are essential for detecting anomalies, identifying potential security threats, and ensuring the smooth functioning of the system.



Driver and its relevance

- Network Intrusion Detection Sensors: Monitor network traffic for suspicious activity.
- Environmental Sensors: Measure temperature, humidity, etc., in data centers to prevent equipment damage.
- Endpoint Sensors: Monitor activity on individual devices for signs of malware or unauthorized access.
- Integration: Sensors are integrated into managed security services and tailored monitoring solutions.



Driver and its relevance

- Governance: Roles and responsibilities for managing sensor infrastructure, data retention policies, and ethical use.
- Risk Management: Assessing risks associated with deploying sensors, including data breaches and reliance on outdated data.
- Compliance: Compliance with regulations such as GDPR, ensuring data protection, privacy, and security standards are met.

Examples of real cases

- Equifax Data Breach (2017) [1]:
 - Overview: Massive breach exposing personal information of 147 million people due to security infrastructure failure.
 - Sensor Implementation: Various sensors in place but failed to detect breach early.
 - Response: Revamped security measures, invested in advanced intrusion detection sensors, improved network monitoring.
 - Outcome: New sensor infrastructure enabled early breach detection, thwarted attempted breaches, maintained customer trust.
- Target Data Breach (2013) [2]:
 - Overview: Significant breach during holiday shopping season, resulting in theft of credit card information from over 40 million customers.
 - Sensor Gap: Lack of effective endpoint sensors allowed malware to remain undetected for weeks.
 - Impact: Failure to detect breach early led to data exfiltration and significant consequences.

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