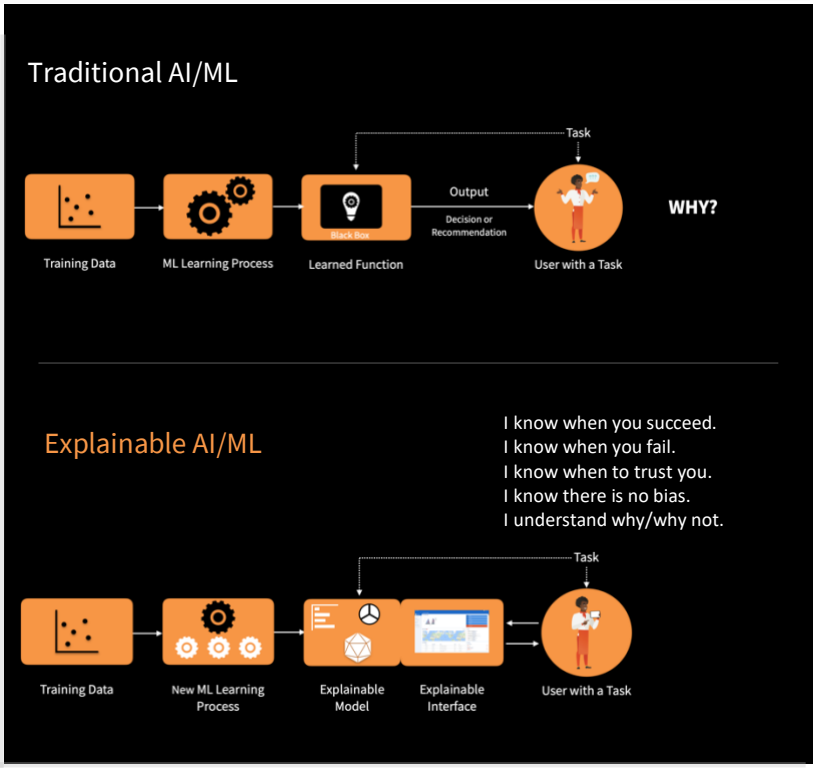
DeepSense – Explainable AI for the Tactical Edge

ZIGHRA
Smart Identity Defense

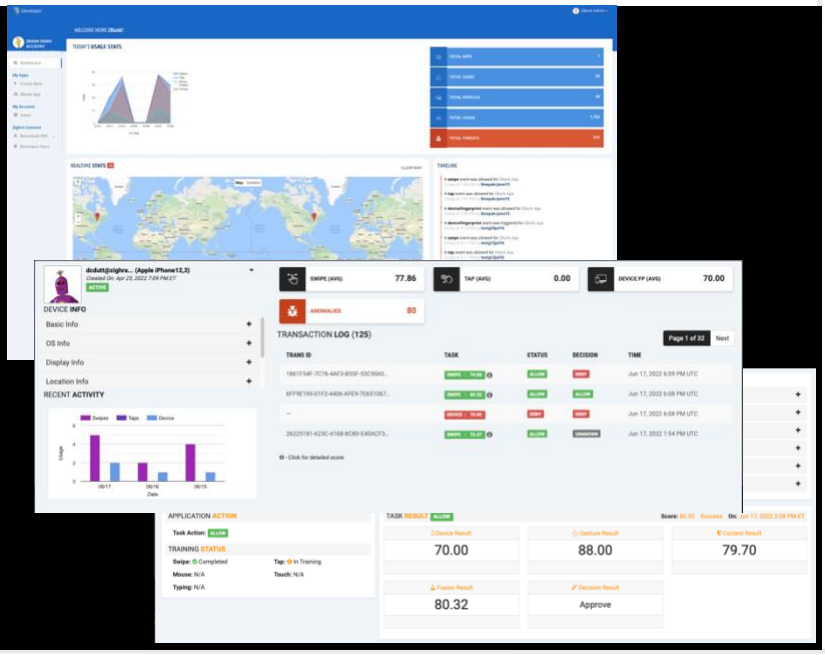
Government departments face persistent cyber threats from fraud groups working in association with nation states. From stealing intellectual property, to collecting intelligence that risks undermining nations' IT systems and capabilities. To minimize the cyberthreat it is essential that organizations adopt the strongest form of continuous AI powered situational awareness and behavioural intelligence solutions for securing data, devices, and users including employees, partners, and contractors. However, the effectiveness of traditional AI systems is limited by the machine's current inability to explain their decisions and actions to human users. Explainable AI/machine learning will be essential if future business decision makers and warfighters to understand, appropriately trust, and effectively manage an emerging generation of AI capabilities.

AI POWERED SITUATIONAL AWARENESS & BEHAVIOURAL INTELLIGENCE

Human operators need to understand, appropriately trust, and effectively manage these AI powered machines. Zighra provides novel automated, real-time situational awareness and triage of behavioural compromise alerts using explainable AI/ML. This will dramatically increase security analyst effectiveness and efficiency and dramatically reduce the risks and costs of attacks. Our patented method leverages real-time, fine-grained knowledge of the real user behaviour and the system processes they are legitimately using to discover threat behaviour that is using their credentials but cannot be attributed to the real user. Zighra collects various types of data from endpoints and user activity to detect behavioural threats. These includes sensor data from touches, taps, swipes, clicks, scrolls and mouse movements, the associated sensor data from accelerometer, gyroscope and orientation sensors amongst others, context data, and network. The AI engines on the platform then learn a behavioural profile of the user from these data and feature extractions in the form of a ML model which is used to detect any anomalies. Enterprises can now leverage sensor fusion and analytics across all their applications and services, strengthening cyber security while maintaining access control.



CYBER SECURITY THROUGH SENSOR FUSION ANALYTICS



KEY BENEFITS

- Sensor analytics platform for IM teams and warfighters to understand, appropriately trust, and effectively manage an emerging generation of cognitive machines.
- Visual explainable AI/ML interface that explains the rationale of why the system made specific decisions and insights into the models.
- Reduce administrator fatigue by reducing the false alerts and improved situational awareness for incident awareness and analysis
- Ensure collected data can be processed, exploited, filtered, and disseminated to facilitate decision making process tactically, operationally, and strategically.
- Red button – remotely shutdown endpoints if required.
- Flexible deployment for on-premise, cloud or on-device. Support for mobile, web, workstations and IoT.

info@zighra.com
+1 613-663-9090
www.zighra.com