Enhancing Healthcare Ecosystem Cybersecurity: The Role of BAE in the SECANT Project

The BAE module plays a crucial role in the SECANT project as it is responsible for identifying and analyzing behaviors within complex ICT infrastructures to detect potential cyber threats and attacks. The module uses machine learning and advanced analytics to analyze large amounts of data and identify specific behavior related to specific threats that could indicate a security breach. By detecting these threats early on, the BAE module enables security professionals to take proactive measures to mitigate the risk of a successful cyber attack.

The main objective of the SECANT project is to develop a holistic framework for cyber security risk assessment that enhances digital security, privacy, and personal data protection within complex ICT infrastructures in the healthcare ecosystem. To achieve this, the SECANT project leverages automated threat detection forms that are addressed to CERTs/CSIRTs, with the BAE module being a key component. The SECANT project aims to promote situational security awareness as a priority within complex ICT infrastructures, such as the healthcare ecosystem.

The infrastructure where the BAE module will be tested will be provided by the Karolinska Institutet, which will facilitate the collection and analysis of data from multiple sources. This infrastructure will enable the BAE module to collect data from a variety of internal and external sources, including observable events that have happened on an organization's internal network and vulnerability databases.

The healthcare ecosystem is a prime target for cybercriminals due to the sensitive nature of the data it holds. Thus, the importance of accurate and timely cyber security intelligence data cannot be overstated. The BAE module's ability to detect malicious behavior in complex ICT infrastructures will enable security professionals to take proactive measures to mitigate risks and safeguard personal data protection within the healthcare digital world from cyber threats.

The BAE module will work in conjunction with the Threat Intelligence Module (TIM), which is responsible for identifying, gathering, enriching, and sharing Cyber Threat Intelligence (CTI) data. The TIM module comprises four distinct sub-components that facilitate different functionalities, including data gathering, analysis, correlation, dynamic taxonomy allocation, and storage. The BAE module will communicate with SECANT's Interoperability Layer (IPL) to provide data such as logs and alerts of existing devices within the organization. The IPL module will facilitate the collection of data from internal sources by gathering data directly from the devices (logs from legacy devices) and the Technical Vulnerability Impact Assessment module (TVIA). A simple data flow representing the BAE mechanisms can be seen in fig1.

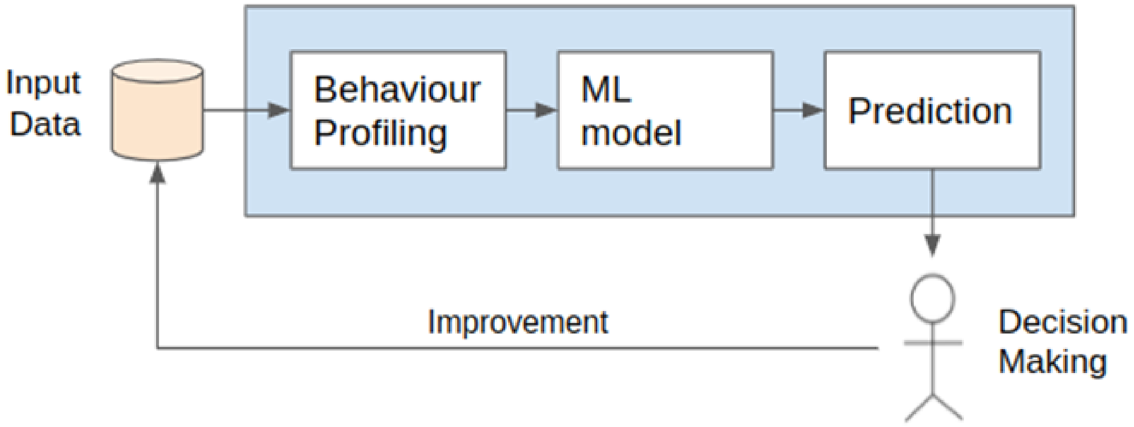

fig1: BAE data flow.

The BAE module will play a critical role in the SECANT project's efforts to collect, analyze, and interpret vast amounts of data from various sources to identify potential threats, vulnerabilities, and attack patterns. By leveraging machine learning and advanced analytics, the BAE module will enable security professionals to take proactive measures to mitigate risks and safeguard the healthcare digital world from cyber threats. The SECANT consortium takes into account the importance of accurate and timely cyber security intelligence data and has a rigorous and thorough strategy to gather, enrich, and share accurate CTI data. The BAE module will be a key component in the SECANT project's efforts to achieve this objective.