**Unit 10 Case Study  
IBM-QRADAR-Intellas-KAIF Integration**

**https://static.s123-cdn-static-d.com/uploads/4501025/normal\_6273becb6cdde.pdf**

This case study demonstrates concepts and principles of data parsing using a Pipe/DSM (Device Support Module) as an API for enabling data sharing and connectivity on an internet/web based distributed platform.

Reading

QRadar collects data about network activity and can provide monitoring services. KAIF(Knowledgebase Artificial Intelligence Forensics) is a platform that uses algorithms and other technologies to identify intelligence and data analysis opportunities for use in cyber security and forensic analysis of cyber-attacks.

The example provides a description and method for how the two platforms can be connected via an API to supply data about network activity collected by QRadar into KAIF to use advanced analytics to intelligently identify cyber security breaches and risks. These are then presented back to the organisation and KAIF through the API. The data pipe line between the two solutions is made possible by the API.

**Reflections**

This example shows how using an API to move data between two separate software solutions can be implemented to result in a better overall solution. The data pipe line from QRadar to KAIF is made possible by utilising an API to transfer network traffic data which is high in volume and complexity. This presents it to a solution able to analyse the data and provide greater insight back to the organisation than would be possible without this additional machine learning integration.