The Analytics, Security & Forensics Company

IBM Partner and go to company for applications of artificial intelligence in cyber security, defense, security, forensics and analytics systems

Knowledgebase for Artificial Intelligence Forensics (KAIF) and IBM QRADAR Security Intelligence Integration Documentation

December 2016

Table of Contents

1 Introduction

This document is a description of the integration of KAIF and QRADAR using Inter-Process Communication (IPC) strategies via Device Support Model (DSM)/pipe. This satisfies all basic requirements for enabling KAIF and QRADAR to function as Software As A Service (SAAS).

2 Background

The continuous increase in growth of data on the Internet, public databases and distributed mobile systems calls for a robust software capable of handling and understanding complex data set as well as making sense out of meaningless data. KAIF Digital, Security, Forensics, and Incidence Response Software Platform applies techniques capable of harnessing intelligent data analysis capabilities essential for digital security and forensic analysis for electronic crime attacks, investigation and case analysis. This could range from day to day network security breach, counter-terrorism surveillance on Internet, mobility based systems, online fraud, online masking for impersonation and digital evidence recovery, collection and forensic analysis.

KAIF system uses a set of intelligent algorithms, methods and techniques deployed at operating system level of an ICT infrastructure to facilitate the discovery and recovery of digital evidence essential for digital security and forensic analysis.

3 KAIF and QRADAR Interoperability Framework

3.1 IBM Portfolio

Table 1: The IBM Portfolio indicating where KAIF compliments[1]

<table>
<tr><td colspan="4">Q Radar – SIEM, Flow, Forensics
KAIF</td></tr>
<tr><td colspan="4">Trusteer – Fraud Detection</td></tr>
<tr><td>People</td><td>Data</td><td>Application</td><td>Infrastructure</td></tr>
<tr><td>- Identity Access Management
- User Privilege
- Super Users etc</td><td>- Data at Rest
- Data in Motion</td><td>- DeSOps
- Dynamic – websites
- Fuzzing</td><td>- En Point Security
- IPS, IDS
- Mobile Solutions</td></tr>
<tr><td colspan="4">X Force: threat research, enhancing security</td></tr>
<tr><td colspan="4">Operating System Requirement: Linux</td></tr>
</table>

3.2 Value Added Components

KAIF adds value to QRADAR through its Machine Learning strategies for *profiling, clustering, classifying, summarising*, etc. as listed in Figure 1 to analyse the packet context and anticipate threats in real time and provide leads and intelligence for client to take necessary action.

While KAIF can be utilized as an integral part of QRADAR, one of its main advantages is that it produces a lean output that can be aimed at clients that have niche Cyber Security requirements. Integration of the two software products will ensure that they can be used and sold as a unified system based on client's needs.

[1] IBM/Intellas

3.3 KAIF – QRADAR Design Framework

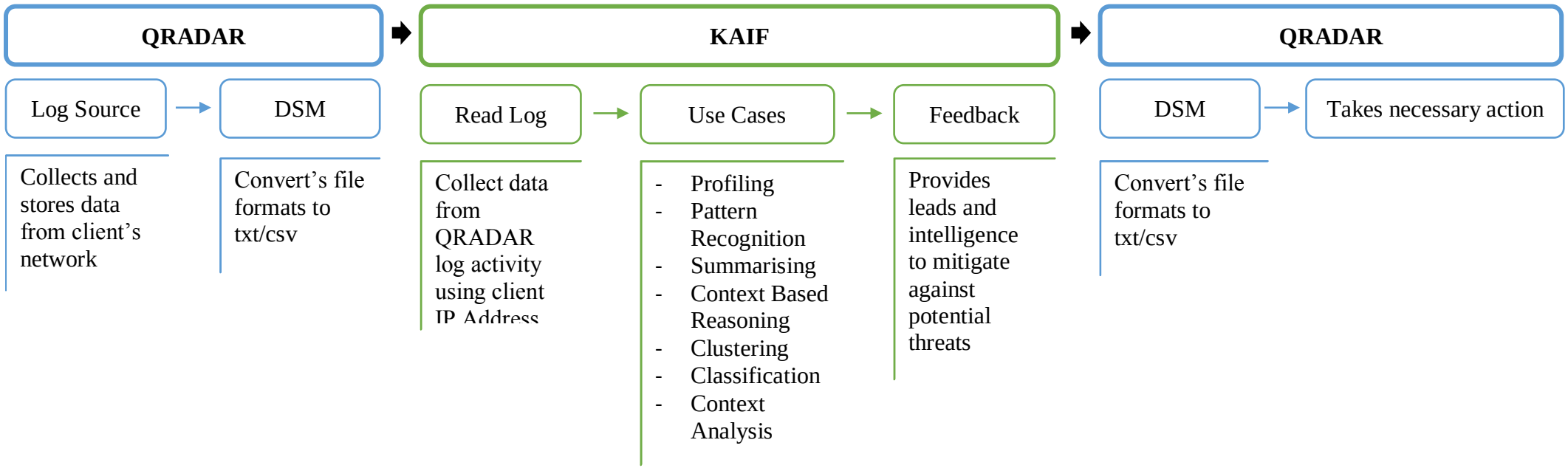

Figure 1: KAIF-QRADAR Design Framework

The KAIF-QRADAR Design Framework gives a brief overview of how KAIF would work in conjunction with QRADAR to provide a complete service to meet clients' needs. Data that is collected from the client's network and stored within QRADAR can be read and processed by KAIF via the DSM. KAIF can then provide leads and intelligence to mitigate against potential threat, which could then be transferred back to QRADAR through the DSM. Necessary action could be taken to detect and block the threats from the intelligence provided.

4 Data Flow Model

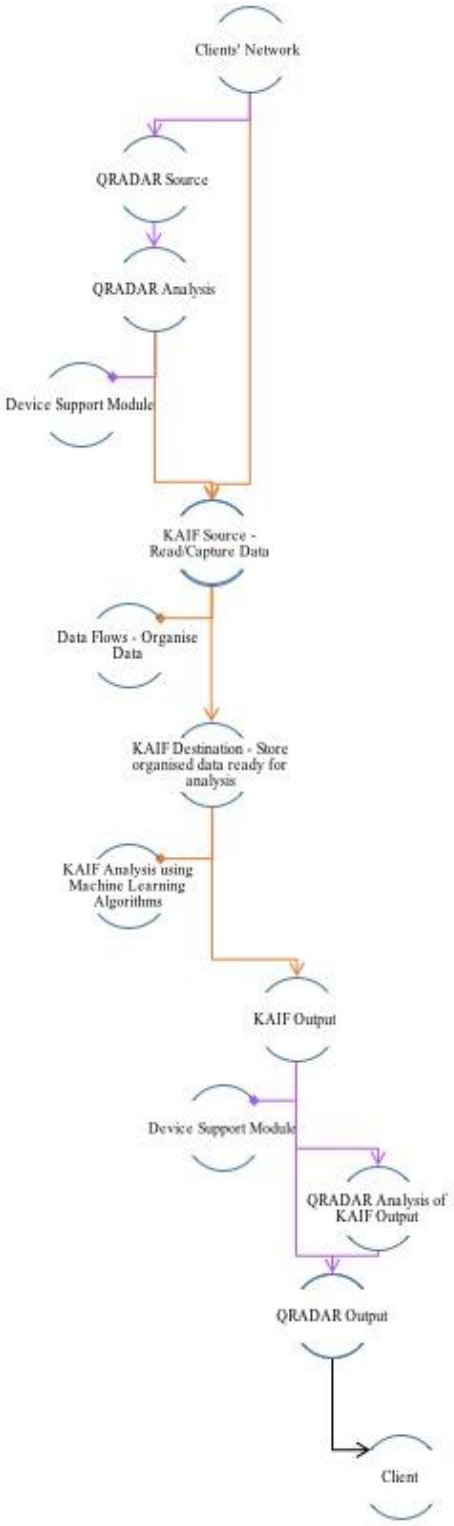

Figure 2: Data-flow model

The Data Flow Model provides a complete overview of how the data collected from the client's network is analysed through KAIF and QRADAR in order for the appropriate information to be sent back to the client. The different routes that could lead to different levels of analysis are highlighted.

5 Activities and Tasks

For the two software to work as one product as described above, the following tasks and requirements need to be completed and met:

- Testing large data set for client scenario thoroughly
- Complete full cycle of inter-process communication to ensure application of pipe works fully
    - Using log analysis/different attempts through QRadar
- Ensure that output that come from KAIF can be presented legibly through QRadar
- As part of integration service, model inter-process communication as a SAAS
- Develop Business Development strategy together with IBM to tap into strengths from both products
    - Launch KAIF as a IBM brand

6 Integration Support

6.1 Basic System Requirements

- Operating System – Linux
- Machine – Mac/PC
- File System – Flat files: xml, txt, vi edition, etc.

6.2 Deployment Model

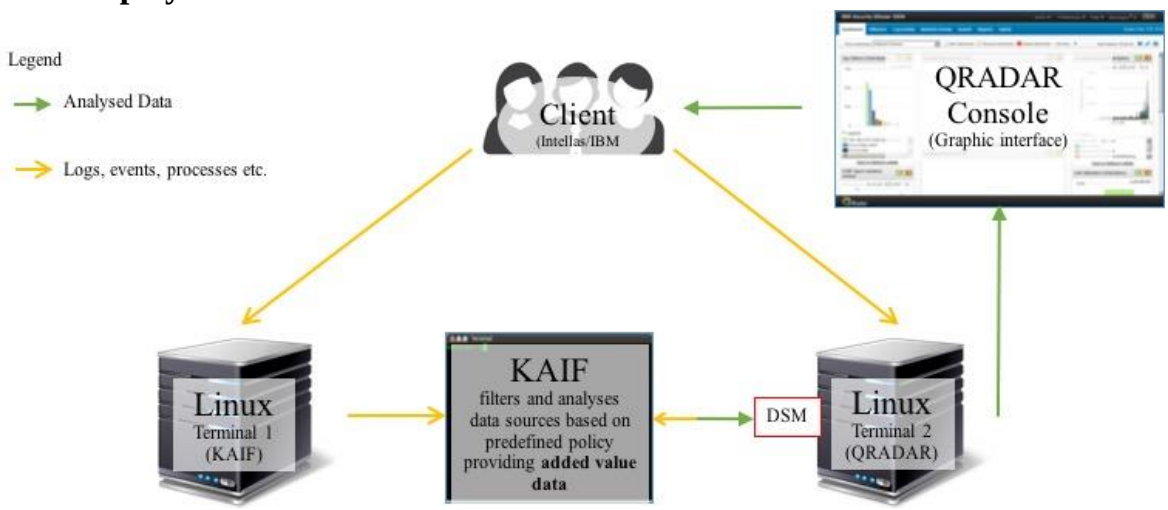

Figure 3: Deployment Model

KAIF/QRADAR integration provides Software As A Service (SAAS) in a cloud-based environment. In order to allow seamless transition of data it is necessary that both software are run on Linux. Network data in the form of log sources, locations, events, etc. can be read from a client's network by KAIF or QRADAR on terminals. KAIF filters data as it is collected from the client's network via the Linux terminal using *predefined policies*. It then analyses the data by *clustering, summarizing, profiling, classifying, etc*. as necessary using machine learning strategies. The analysed data is then formatted and sent to QRADAR through a DSM/*pipe* and displayed on the client's console in real-time.

7 Configuration

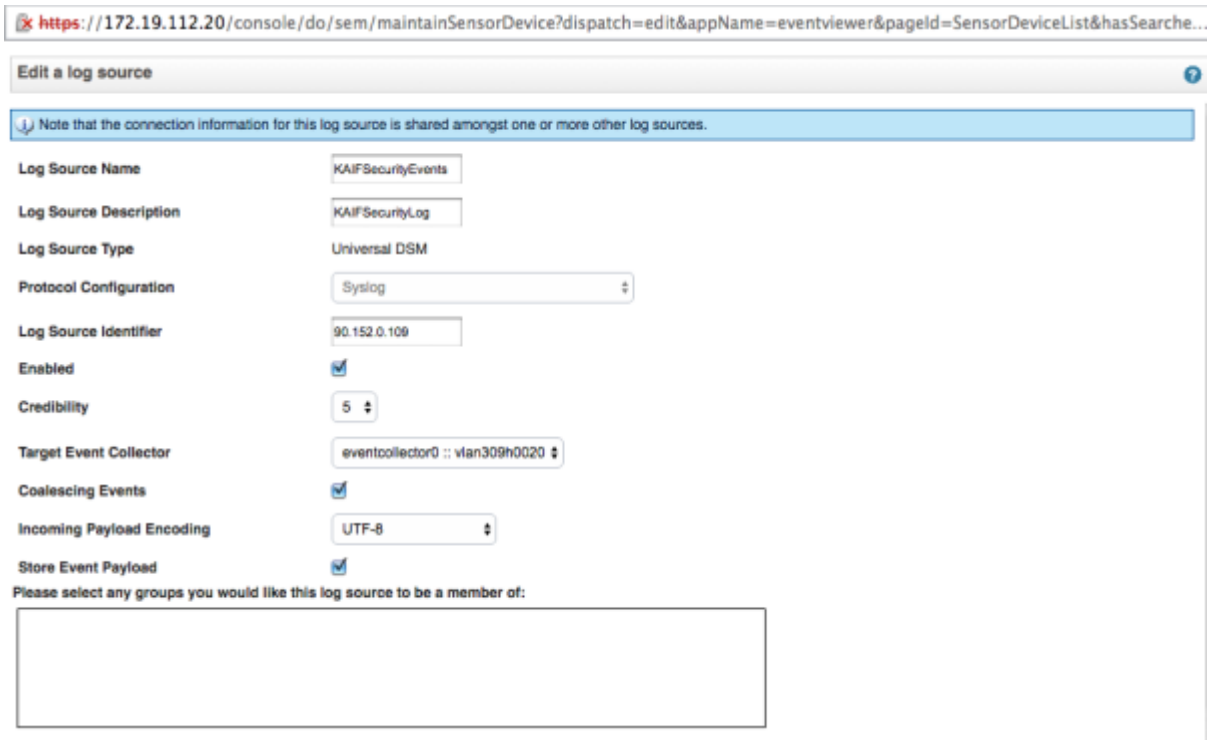

Figure 4: KAIF-QRADAR initial configuration

8 Conclusion

Integration of QRADAR with KAIF advances the capability of QRADAR and ensures that the services provided will be flexible to the client's needs. For those that require more in depth analysis, KAIF adds value to QRADAR through its machine learning strategies, and for others it targets niche aspects of Cyber Security, meeting a variety of clients' needs.

9 Further Work

KAIF-QRADAR integration is just the first step to building a product that can meet evolving client needs. Work will continue post the integration to continue to develop KAIF and improve and increase the services it can provide as part of the business development goals.