Kroger Security Information and Event Management Upgrade

By

Patrick McDonald

A Proposal Submitted to
The Faculty of the School of Information Technology
In Partial Fulfillment of the Requirements for
The Degree of Bachelor of Science
In Information Technology

Patrick M McDonald — Date 4/22/14

Mark Stockman, Faculty Advisor — Date 4/20/14

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2014

ACKNOWLEDGEMENTS

I would like to thank Professor Stockman for all the help and guidance during my projects and during my tenure at the University of Cincinnati. I would also like to thank Professor Kumpf for sharing his wisdom and guidance with me. As well as to Professor Scott for helping me get my internship with Kroger. Lastly I would like to thank everyone in the Corporate Information Security Department at Kroger for letting me work with them and learn from them.

Table of Contents

List of Figures

ABSTRACT

The Corporate Information Security (CIS) Department at Kroger is responsible for the security of information assets. The department is currently in need of a new Security Information Event Management (SIEM) System. Current systems are restricted to six gigabytes of data it can collect, and delayed collection times. Kroger currently uses Fifty Four servers to run the log collections. CIS is changing to a SIEM software called QRadar. The new system uses fewer servers, and allows for event retention. QRadar also allows for real-time data collection. With the use of collection agents, logs are collected automatically and forwarded to one main collection server. Overall, the new collection system has improved the company's security, and also keep it HIPAA and PCI compliant.

INTRODUCTION

In today's world, an attack on a company's network is almost guaranteed; The only problem is you never know how or when. To help prevent serious attack and mitigate damage to your network or your data you need to have a sense of situational awareness. "Situational awareness refers to the collective real-time under-standing within an organization of its security risk posture. Security risk measures the likelihood that an attack might pro-duce significant consequences to some set of locally valued assets" (Amoroso, 2011). A good way for a company to help keep its security awareness is to implement a Security Information and Event Management product.

Security Information and Event Management (SIEM) is the combination of Security Information Management and Security Event Manager. The purpose of implementing a SIEM product on a network is to help with incident response and government regulation compliance. SIEM's are used to analyze system logs, thus enabling the ability to track when data on the network changes. Most SIEM's can be setup to send automated alert or reports when a flagged log type shows up in collection. SIEM's can collect from a number of devices within a network for example servers, routers, and applications. "SIEM can be the central logging solution in the enterprise and most have the ability to also provide canned reporting for regulatory compliance and other security standards"(Woody, 2013). Having a SIEM running and checking a large network like Kroger's network is a tremendous asset and it needs to be upgraded.

PROBLEM NEED

Kroger's current SIEM, known as Tivoli Compliance Insight Manager(TCIM), was announced that it will no longer be supported by IBM. This gives Kroger the chance to look into

new software and replace TCIM with a more modern SIEM solution. Currently, TCIM has a few issues that should be solved with the new software. At present TCIM logs collected and reports generated are not done at real-time; each system must be sent a request for a system log and then respond. This process adds about hour delay for the logs to make it back to TCIM and then be reported. TCIM collection of logs can only collect up to 2GB of logs on a single TCIM gem database. This requires Kroger to have 54 servers with TCIM to collect from every essential device.

The new solution needed to be able to collect logs without collection limits. The solutions need to have real-time reporting. It should also support audit packages beyond the next two years. The software also needs to give the opportunity to merge multiple existing audit environments; this way Kroger can audit data in a more effective manner. In addition, the solution must maintain its current record of regulatory compliance. Further, it needs to be able to collect audit data from Kroger's existing technologies and store this data in a secure, compliant format in order to produce necessary reports and alerts. Moreover, this program must allow Kroger to maintain its current audit procedures and policies. Finally, the new solution must offer a support model that can accommodate Kroger's SLA's.

SIEM SELECTION

To help with selecting the best suited SIEM software available, Kroger used a third party company, Gartner. Gartner researched most of the available SIEM products on the market today. Using Kroger's product requirements, Gartner rated each product by its ability to execute over completeness of Kroger's vision. Next, Gartner produced a report and a graph that divides all the products into four different sections. The best section is known as the magic quadrant. Kroger

then selected the top six products in the magic quadrant for further selection research. It was from these six selected products that QRadar was chosen.

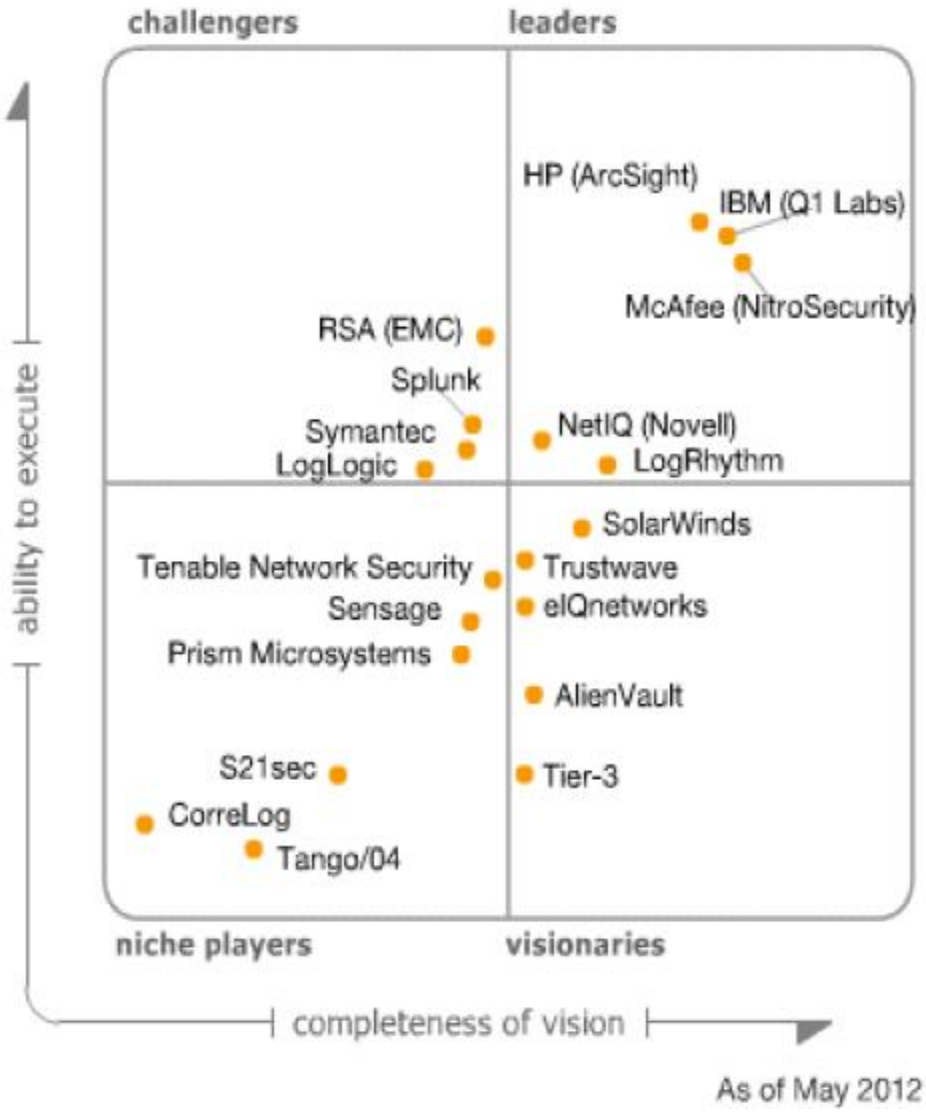

Figure 1 Magic quadrant

SOLUTION

The solution is the implementation of QRadar as the replacement for TCIM. QRadar is a SIEM software product owned by IBM. "IBM® Security QRadar® is a high-performance

system for collecting, analyzing, archiving and storing large volumes of network and security event logs"(Malliaroudakis, 2013). It was QRadar that best met all of Kroger's needs. QRadar offers real-time collection of system logs by applying agents on the servers from which we collect logs. With over 2,500 stores with fuel centers and pharmacies, Kroger needs to put an agent on each server. Implementation of an agent on each server is necessary not only for real-time collection, but for security as well. Currently, stores cannot talk to other stores, and divisions cannot talk to other divisions.

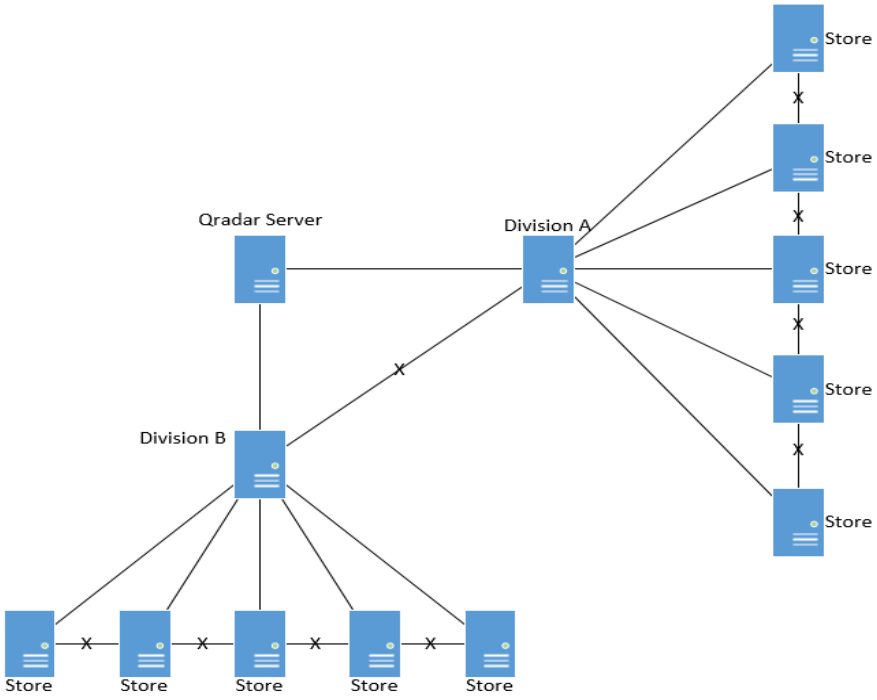

Figure 2 Collection Restriction

QRadar does not restrict the amount of logs it can collect, unlike TCIM. When, and if, QRadar hits its limits, it will setup a backlog so that no packets are dropped and all logs coming in will be processed. Being IBM's newest SIEM product, it is guaranteed to be supported beyond the next 2 years. QRadar also maintains regulatory compliance by keeping Kroger safe

from fees and fines. QRadar will also be able to collect audit data from Kroger's existing technologies and store this data in a secure, compliant format in order to produce necessary reports and alerts.

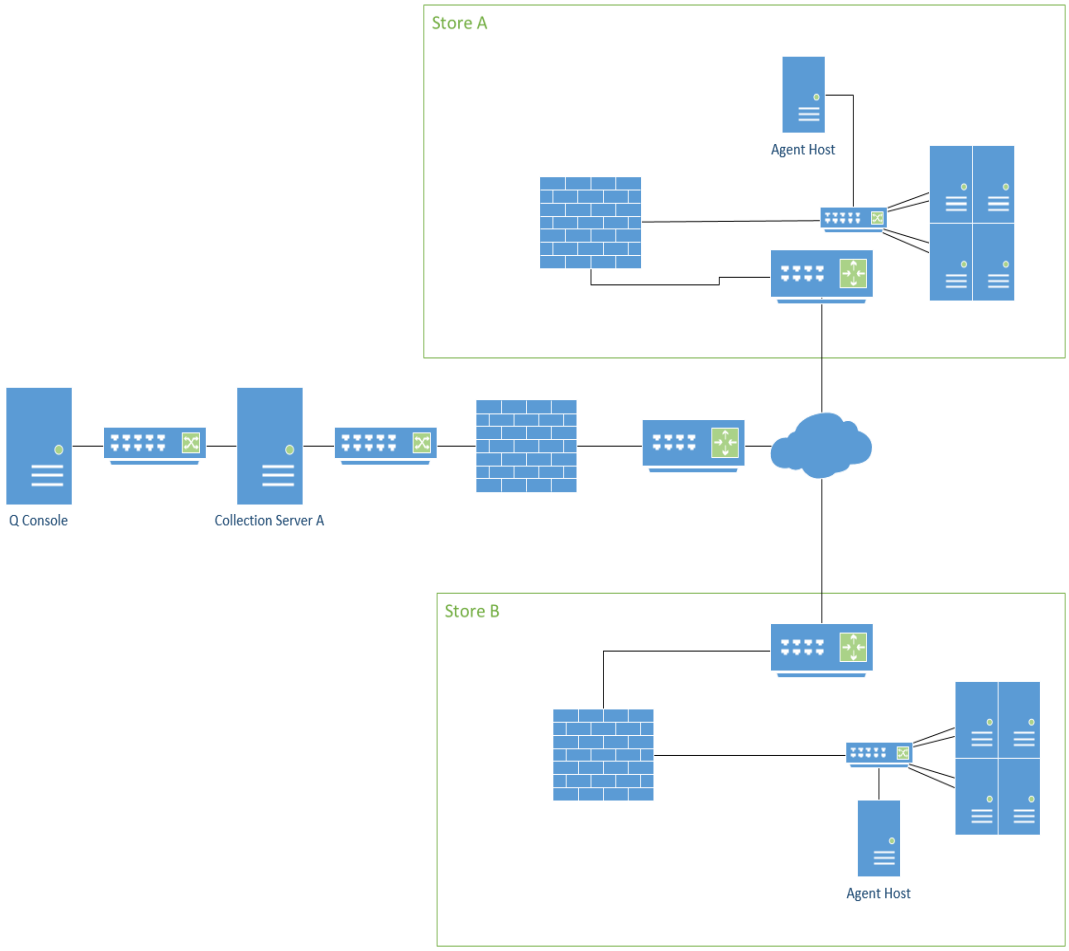

Figure 3 Network Diagram to Stores

QRadar will only need to be one server; unlike its predecessor, which was taking up 54 servers. QRadar will also allow Kroger to maintain its current audit procedures and policies. There will be some work to parse the logs for QRadar; although it can parse most operating systems and devices, QRadar will not be able to parse the programs that have been internally

designed by Kroger. In the past, Kroger had many programs developed to fit their needs, because third party options did not meet Kroger's requirements. I have been working with a team at Kroger in the Corporate Information Security (CIS) department, to help verifying current reporting and auditing servers. Kroger is currently collecting over 2,000 servers, ranging from windows servers to IBM mainframes. QRadar also has an easy to use dashboard that is customizable to its user. The following graphs illustrate what is currently going on in the network.

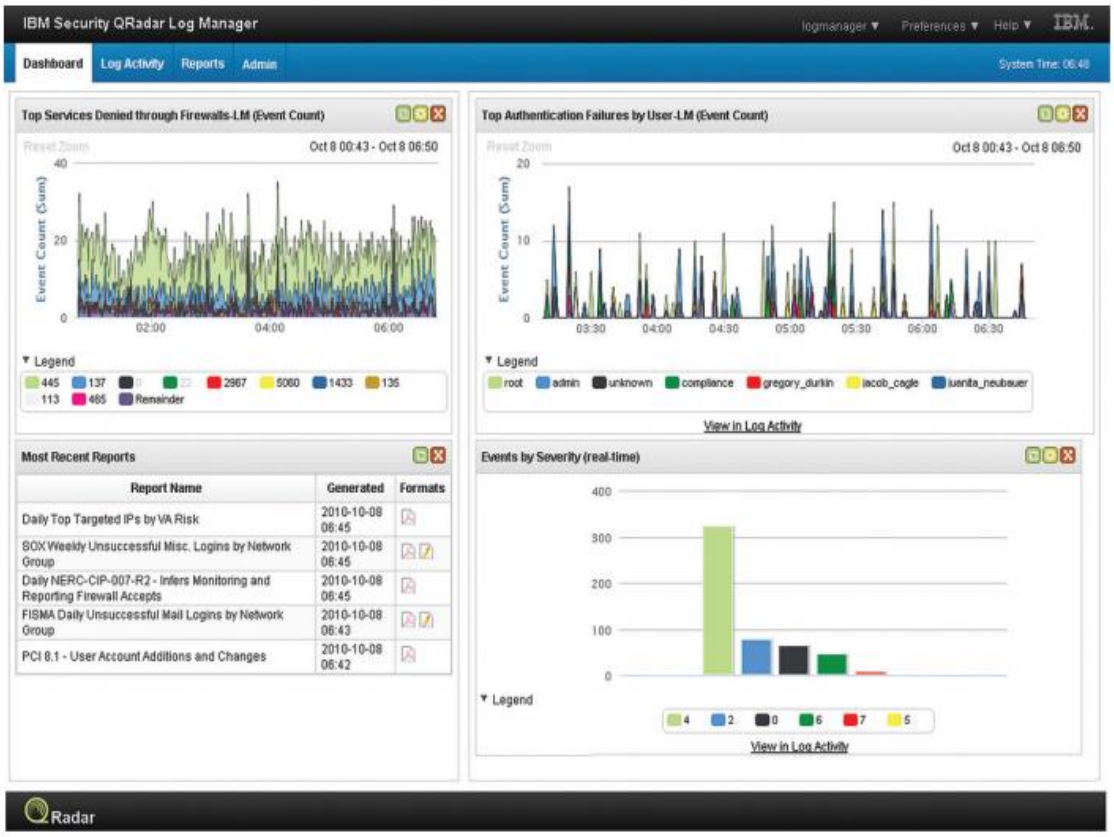

Figure 4 Basic QRadar Dashboard

As you can see in figure 2 most actions or services are denied by the firewalls, Authentication failures, Events, and recent reports generated. These are just a few of the configurations that can be imported into a user dashboard.

TECHNICAL AREAS

The technical areas involved with this project are Networking and Database. Networking is involved because the new SIEM will be collecting logs from thousands of servers, security devices, applications, and operating systems from across the network and from all over the country using TCP, UDP, FTP and SFTP protocols. We have also had to put in a request with the networking team to make sure that the correct ports we use for collection are open on the firewalls. These system logs will be checking and making sure that all devices are staying secure and are compliant to U.S. Regulations. A database is used because all logs will be collected and stored in a database for auditing purposes. Logs will need to be archived for a set time by regulatory standards until they can be removed.

USER PROFILE

The primary users of QRadar are going to be its administrators--with the possible addition of Data Owners, Desktop support, and Network Administrators in the future. QRadar administrators are able to add and remove sources for log collection, search criteria, and reports. When additional groups and users are allowed to use QRadar, they will have restrictions, which let them have access to information available to their group.

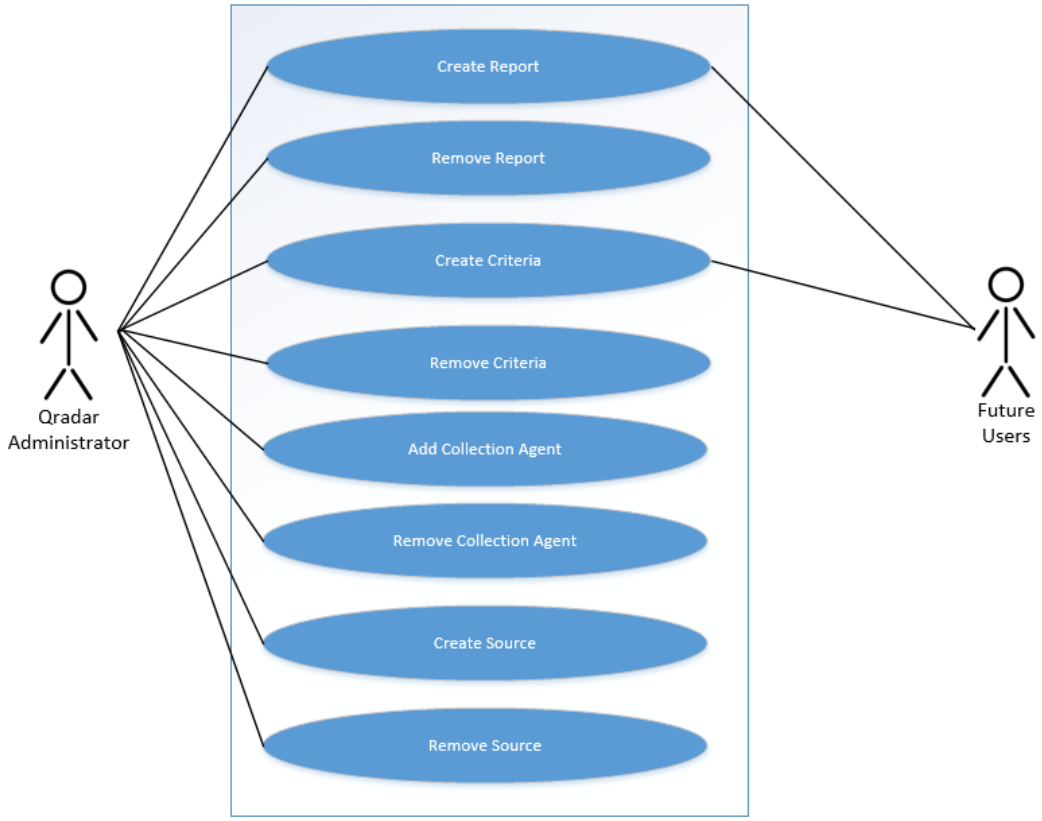

Figure 5 Use case diagram

BUDGET

Initially quoted to be about 1.2 million dollars, the final cost has been determined to be $750 thousand dollars. The final cost includes price of software, servers, storage, and salary cost of everyone working on the project. Also included in the price plan that Kroger has purchased with IBM, IBM will provide eighty hours of on location support. We have had a QRadar specialist to help with our system upgrade and answer all our questions.

SCHEDULE

As of now, the major portion of the project has a deadline to be finished by the end of the December. Additional users besides the QRadar administrator will be considered after the main portion of the project is completed. The primary objective due by February is to get all necessary servers that require auditing moved over to QRadar from TCIM.

1			Pharmacy	46 days	Mon 9/30/13	Mon 12/2/13
24			Mainframe	20 days	Mon 9/30/13	Fri 10/25/13
39			AIX - Compliance	20 days	Mon 10/7/13	Fri 11/1/13
55			Micro$oft - Compliance	10 days	Mon 11/11/13	Fri 11/22/13
62			Microsoft SQL - MSSQL Auditing	10 days	Mon 11/11/13	Fri 11/22/13
69			Fuel Center Auditing - Microsoft	20 days	Mon 11/4/13	Fri 11/29/13
76			Active Directory (New)	2 days	Mon 11/18/13	Tue 11/19/13
81			Database Auditing	30 days	Mon 11/11/13	Fri 12/20/13
117			Linux OS Auditing	10 days	Mon 11/18/13	Fri 11/29/13
124			Store VM Stack Logs	5 days	Mon 11/25/13	Fri 11/29/13
129			Microsoft OS Auditing - Non Fuel	10 days	Mon 11/25/13	Fri 12/6/13
136			Production Readiness	3 days	Mon 12/16/13	Wed 12/18/13

Figure 6 Tentative Project Schedule

AGENT TESTING

When trying to find what agent we wanted to use to collect logs for QRadar on Kroger's remote systems we had a few choices. The first and best option would be to use WinCollect. WinCollect was designed to work with QRadar and one agent can collect from 200 different sources. An issue found with WinCollect is that if you have to many agents it will start to cause issue with QRadar because WinCollect uses only one port and would start to bog down QRadar. IBM has promised that they are currently working on a patch that would fix the issue caused by multiple WinCollect agents. Another issue we are having with WinCollect is that it cannot currently host on a windows XP environment. Although it is able to collect form XP, this is an

Issue because Kroger Fuel centers current operate with a windows XP environment and our department is not sure when they plan on changing over to windows 7. We are also using a agent called Adaptive Log Exporter (ALE). ALE is the predecessor to WinCollect. ALE can be hosted on a windows XP system. ALE also has a device limit of 20 different sources. This is not so much of any issue as of right now because each xp environment only contains about 6-7 devices. The main issue with ALE is that it is no longer supported by IBM. All and any configuring has to be done through document searching and finding everything we can off the Internet. Other than not being supported we have decided to go with ALE until fuel centers upgrade to a windows 7 environment. We had also tested an agent called Snare. As a team we decided to not use Snare for a few reasons, cost, support, and feel. With Snare to use the features we wanted we would have to pay a fee for each agent and we were using. The second reason was because of support. We did not know the company very well that owns Snare and wanted to be sure they could provide good and long lasting support for the agent. With Snare we could not get that guarantee. Third reason for not going with Snare was it seemed out dated more than ALE. Even though we are using a console to setup these agents the setup of snare was off putting and slightly more complicated.

SYSTEM TESTING

For collecting form fuel centers and using ALE we had to construct a special script to automatically add each device at a store to the agent. We then had to work with the system owners that are in Denver, Colorado to make sure all necessary ports are open for agents to connect and report to QRadar. Working with people over such great distance can cause a few issue of their own in communication. With the IBM AS/400 iSeries servers was slightly easier

with the AS/400 team located in our building. I scheduled multiple meeting with the AS/400 team to talk about getting reporting setup to work with QRadar. Because of the age of the AS/400 iSeries they don't support SFTP so we had to use FTP to a second server in which QRadar will pick up the logs. Logs cannot be directly transferred to QRadar console. They must go to the collection servers and then to the console.

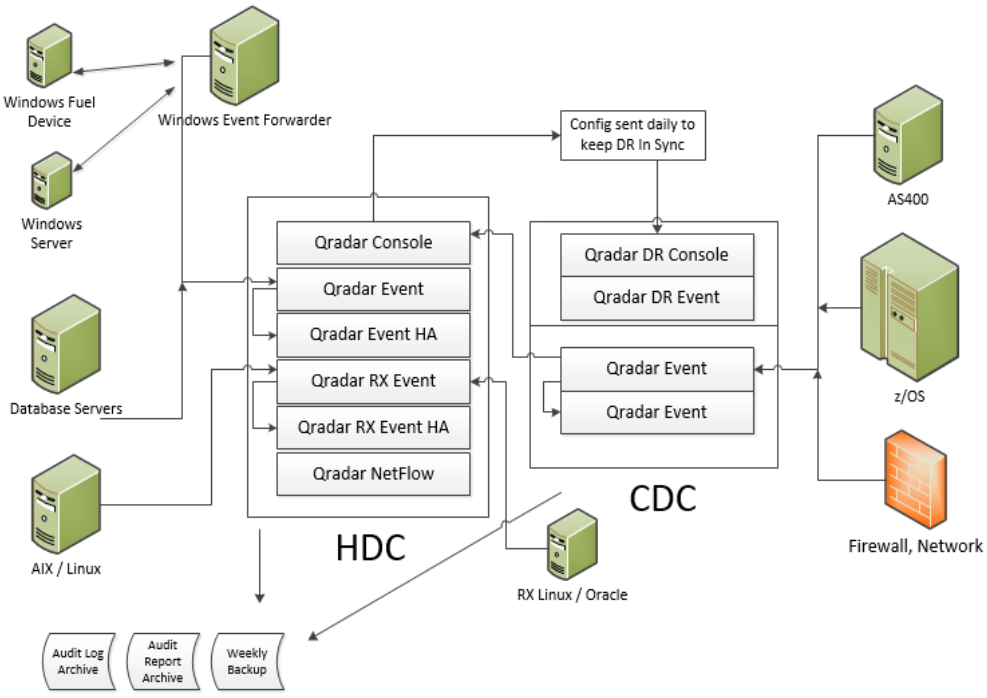

Figure 7 Network Diagram of QRadar

DELIVERABLES

Currently in production in QRadar we have all AS/400 iSeries from IBM sending logs and QRadar generating reports similar to TCIM's. In pilot testing, we also have the fuel centers, SQL servers, Kroger pharmacy applications. We are collecting from 2-3 fuel centers from each division around the country. After about two more weeks of pilot testing, we will have the fuel

center team role out the log collections to the rest of the 2500 fuel center servers. All systems in QRadar that are in production will continue to report to both TCIM and QRadar to make sure data we have data integrity. The reports that we generate in QRadar must match the reports coming from TCIM. After one year of comparing the reports we will then have system owns shutdown the collection services for TCIM. As additional deliverable for the project I have also started work on a run book that will explain the setup of every system in QRadar. It currently contains log sources and types, collection agents, reports, and custom parse rules. The run book will need to be updated as the system grows.

CONCLUSION

The current setup with TCIM is insufficient in terms of scalability and reliability. The movement to QRadar will not only help with current collection issues, but it will also help improve response time when someone tries to tamper with a device or data within Kroger's organization. Considering the amount of work needed for setting up the parse rules, configuring collection agents, and carrying over everything from TCIM to QRadar-- this project is significant enough for a senior design project.

WORKS CITED

Amoroso, E. (2011). *Cyber attacks*. Burlington, MA: Butterworth-Heinemann. Retrieved from http://proquest.safaribooksonline.com.proxy.libraries.uc.edu/book/-/9780123849175

Woody, A. (2013). *Enterprise security: A data-centric approach to securing the enterprise*. Birmingham, UK : Packt Publishing. Retrieved from http://proquest.safaribooksonline.com.proxy.libraries.uc.edu/book/-/9781849685962?bookview=overview

Malliaroudakis, G. (2013, July 14). *IBM security QRadar log manager*. Retrieved from www-03.ibm.com/software/products/us/en/qradar-log-manager

Gartner. (2013). Retrieved from www.gartner.com/technology/home.jsp

IBM security QRadar log manager. In (2013). Somers, NY: IBM COrporation. Retrieved from http://public.dhe.ibm.com/common/ssi/ecm/en/wgd03020usen/WGD03020USEN.PDF