Implementation and Analysis of a Security Incident and Event Management System

by
Anna Heinzman

Prepared for

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

Anna Heinzman — Date: 4.18.16

Jim Scott — Date: 4-19-16

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

April 2016

Acknowledgements

I would like to thank my employer, Projetech, for giving me the opportunity to complete a project with them and for teaching me most of what I know now in the year I have worked with them. I am grateful to get the chance do a real world project for my Senior Design. I would specifically like to thank my manager, Tyler Caldwell, for assigning me this project and giving me guidance throughout the semester and with my entire time at Projetech.

Table of Contents

Section **Page**

List of Tables and Figures

No. **Page**

Abstract

In all applications, everything you do is piped into a log file somewhere. These log files contain pertinent error data and other information a network administrator needs to know. However it can be a very tedious task to go through and manage log files manually. Tools called Security Incident and Event Management Systems (SIEM) are a popular way to manage log files. They manage, report and alert on log files based on the company's configuration and are a highly customizable software to tailor to a particular company's infrastructure. I will be implementing Event Tracker, a SIEM produced by Prism Microsystems, at Projetech. This will span three datacenters and over 400 virtual servers. My goal is to improve uptime for better SLA's and overall give a much deeper look and understanding as to what is going on in our infrastructure.

1. Introduction

1.1 Company Description

Projetech is a small Cincinnati based company that offers the IBM software Maximo over the Cloud. (Software as a Service, SaaS). We have over 400 virtual servers of a dozen different types including, application servers, web servers, database servers, etc. These are spanned over three clouds, two production cloud environments in Washington DC and Dallas, TX, along with one development cloud here in Cincinnati.

1.2 Problem

Currently at Projetech we have a variety of ways to monitor and look into our infrastructure. We have a server health monitoring tool that checks on things such as CPU and storage, a vulnerability scanning tool, and an intrusion detection system. With all of that we are still missing something to take an even deeper look into our network. We still experience several issues within our network that we were unable to anticipate. Since we are a cloud company who offers SaaS, we have SLA's with our clients that promise to offer a 99.99% uptime with their production applications. Therefore, we need to do everything possible to ensure uptime and overall client satisfaction.

Issues such as database backup errors, IIS communication errors, and other Maximo related issues that we experienced were not being monitored, and could be completely missed unless someone were to look into the log files. In addition, while automation and scheduling tasks to run at night is great for efficiency it is often not checked on the next day, and we are left to assume things went well. Clients could lose

data due to a mistake on a file replicator service failure at 2:00am, and we wouldn't know until they call us. That does not make Projetech look good which could harm our reputation which is becoming more important as we are a growing company, and are starting to go after bigger clients.

1.3 Solution

One tool that we had yet to integrate into our network is a Security Incident and Event Management System (SIEM). Since a lot of our current issues are based on software and services, and not so much the back end infrastructure, this seemed like a good tool to look into. This will look into log files that are generated by the software and send an alert to the relevant contact on our team. We will also be able to create scheduled reports to make it easy to spot strange occurrences in our servers. This is going to give us a deeper insight into our infrastructure, and give us a better understanding of the patterns and trends that exist.

I will be inputting various log files for all relevant applications, including but not limited to: Windows Event Viewer, Maximo, IIS, SQL, Oracle, DB2, DataSplice, Nagios, and WebSphere. I will also be creating reports and alerts based on the needs of the three teams of the technical side of Projetech (Developers, Network/Security, and Customer Support). I will need to set up ways to notify the relevant team lead on reports and alerts.

Once I have all of the above completed, I will be able to take a closer look at the information we now have easy access to. I would like for this to result in an overall

percent reduction of errors across our network, and create a general awareness of what is going on in our network.

1.4 User Profile

1.4.1 Application Title

Security Incident and Event Management System – Event Tracker

1.4.2 Potential Users

Infrastructure team at Projetech consisting of:

- Network Administrator
- Head of Security
- Network and Security Analyst

1.4.3 Software and Interface Experience

Current software and tools that need to be monitored are: Maximo, WebSphere, DB2, Oracle, DataSplice, MS SQL, IIS, and Windows Services. All team members will need a good amount of experience with all listed software in order to troubleshoot.

1.4.4 Experience with Similar Applications

Currently we have other tools to improve our infrastructure and uptime in place, these all have different functions, however do have similarities. All users will have experience with an Intrusion Detection and Vulnerability scanning tool called Nessus. A server health monitoring system which runs Nagios through a web UI called Opsview. Lastly we have a systems management tool called Tivoli Endpoint Manager which handles real time scans, Windows server patching, and a few small automated tasks.

1.4.5 Task Experience

All users should have a general understanding of the existing infrastructure and common security measures taken at the company. Since the three users will be notified about a variety of incidents in log files, they need to know troubleshooting steps to take to resolve any issues with priority to SLA-affecting issues.

1.4.6 Frequency of Use

This tool will always be scanning certain log files and pulling files to report on in a scheduled manner. Frequency of Use for me to be the Event Tracker Admin will be a few hours a week. On top of that the team will use it when they receive an alert or report. Since we are planning for this to become a developed tool in our security toolkit, Frequency of Use for all team members will be at least moderate.

1.5 Budget

Component	Cost
Event Tracker Yearly Fee	$15,000
Labor ($20/hr for 300hrs)	$6,000
Total	**$21,000 / yr.**

Table 1, Budget

1.6 Gantt Chart

Below is my schedule that I set for myself at the beginning of this semester. I wanted to give myself plenty of time to work on the initial configuration as a good foundation will help the project succeed. Some tasks have been simpler than expected so I was able to spend more time on research and more difficult issues I have faced and leaving me within my schedule so far.

Task Mode	Task Name	Duration	Start	Finish
	Initial Configuration and Design	25 days	Mon 8/17/15	Fri 9/18/15
	Configuring Master Console	5 days	Mon 8/17/15	Fri 8/21/15
	Configure Relay Servers	5 days	Mon 8/24/15	Fri 8/28/15
	Install Agent on all Servers	15 days	Mon 8/31/15	Fri 9/18/15
	Development Implementation	40 days	Mon 9/21/15	Fri 11/13/15
	Windows Event Viewer	10 days	Mon 9/21/15	Fri 10/2/15
	Develop Basic Reports and Alerts	8 days	Wed 9/30/15	Fri 10/9/15
	Meetings with Technical Contacts	3 days	Mon 10/12/15	Wed 10/14/15
	Consume Additional Log Files	8 days	Wed 10/14/15	Fri 10/23/15
	Create Alerts and Reports based on new logs files	15 days	Mon 10/26/15	Fri 11/13/15
	Creating Implementaion Guides	7 days	Thu 10/8/15	Fri 10/16/15
	Document Issues and Resolutions	5 days	Mon 11/9/15	Fri 11/13/15
	Production Implementation	60 days	Mon 11/16/15	Fri 2/5/16
	Configure Log File Consumption in Production	13 days	Wed 12/16/15	Fri 1/1/16
	Develop Weekly and Daily Reports	15 days	Mon 1/4/16	Fri 1/22/16
	Develop Production Alerts	20 days	Mon 1/4/16	Fri 1/29/16
	Configure Pager Duty for Mission Critical errors	5 days	Mon 2/1/16	Fri 2/5/16
	Document Issues and Resolutions In Production	5 days	Mon 2/8/16	Fri 2/12/16
	Analysis	25 days	Mon 2/15/16	Fri 3/18/16
	Reports on Common Errors and Threats	10 days	Mon 2/15/16	Fri 2/26/16
	Meet with Technical Contacts to work on Resolutions	5 days	Mon 2/29/16	Fri 3/4/16
	Percent Reduction of Error Count	20 days	Mon 3/7/16	Fri 4/1/16

Figure 1, Gantt Chart

2. Discussion

2.1 Defining SIEM

A SIEM is a combination of security event management (SEM) and security information management (SIM). SEM focus on real-time monitoring of security events and a SIM is focused on historical analysis of log files to help with investigations and reporting. There are many uses of a SIEM, including: data collection and aggregation, event correlation, reporting, alerting and forensics.

2.2 Technical Elements

2.2.1 Datacenters and Servers

At Projetech we have three datacenters. Two production environments where our SLA's with our clients say that we have 99.99% uptime. In order to keep this we need to have less than .01% of unscheduled downtime. These two datacenters are located at Dallas Texas and Washington DC. These are managed by us through vCenter but the equipment is purchased through IBM Softlayer. In addition to those datacenters, we have one development datacenter in Cincinnati Ohio where we manage all hardware and networking.

We have close to 400 servers of varying servers within our infrastructure. Application servers take up a majority of the servers. In addition we have Web servers, Database servers (SQL, Oracle, and IBM DB2), Domain Controllers, Mobile Application Servers, Sandboxes, and servers for our numerous tools in our network.

We will be creating a Master Event Tracker Server in our Development Cloud. We will then have two relay servers in our two Production Clouds which will pipe all files to the Master server. All systems will have to be managed in their appropriate local server. Then once they are added, we can manage everything through the Master server.

2.2.2 Network Diagram

Below is a basic network diagram for the SEIM. It shows how the application will be accessed, as well as how it is split up throughout the different datacenters. As mentioned, the master server is located in our Cincinnati datacenter, with two relays in both of our production datacenters.

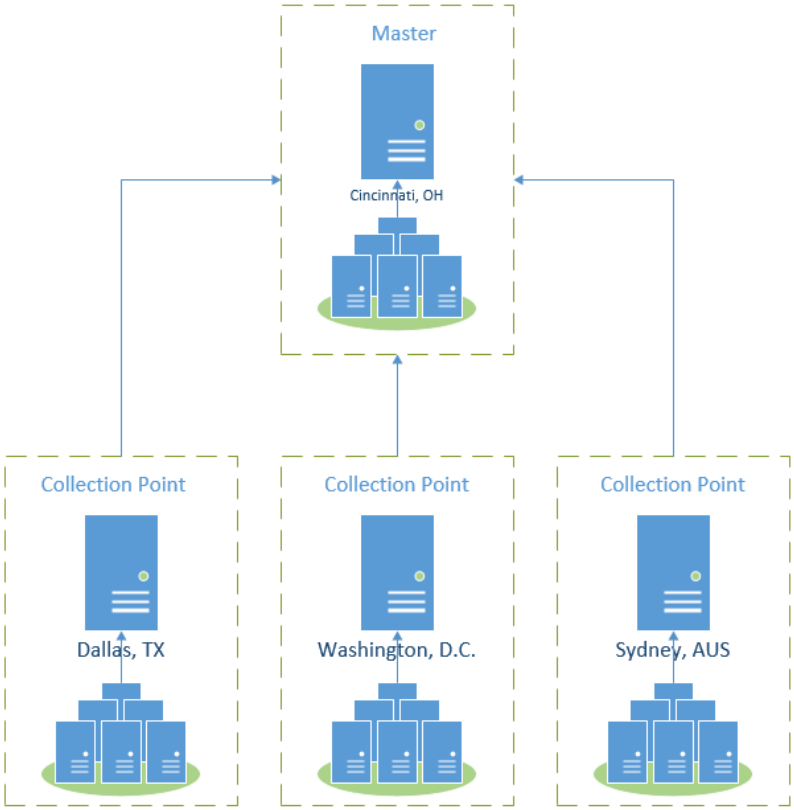

Figure 2, Network Diagram

2.2.3 Firewall

In order for Event Tracker to pull log files from all servers port 14505 must be opened on all servers with the agent installed. This allows Event Tracker to communicate between agents and Relay/Master Servers.

2.2.4 Log Retention

All Event Tracker Files are to be considered “Operational Data”. Per Projetech policies, Operational Data must be retained for 90 days and then deleted. This will be completed though “Event Vault”, a tool within the Event Tracker application Control Panel. A rule will be set to purge all logs older than 90 days which needs to be verified every week.

2.2.5 Alerts and Reports

The main functionality of Event Tracker is the Alerting and Reporting tasks. Alerts will scan log files in real-time and when a specified string is produced by a log file it will then send an email to certain team members. Reports can be scheduled daily/weekly/monthly at any time. These will pull the log files and scan them and create a report that has a count of strings or codes. These will be used to find patterns through the network. These can also be scheduled to email team members for ease of access.

2.3 Testing

2.3.1 Overview

This section will go into the methods of testing that was completed in order to ensure that all components are operational and functioning as expected. The objective of this is to verify that all components are working and there are not false alerts, alerts that don't email or reports that are not being generated as intended. In addition to that, there needs to be testing on user access and other system operations.

2.3.2 Requirements

1. All authorized users should have access to the system
    a. Usernames should be formatted first initial, last name (ex. aheinzman)
    b. Passwords should be pulled from Active Directory
    c. Unauthorized users should not be allowed into the system
    d. The administrator should be able to add users as needed
2. Alerts should be sent out immediately after an error string is found
    a. Alerts should be sent to authorized users
    b. Alerts should be emailed less than a minute from the time the string was found
3. Reports should be emailed Daily/Weekly/Monthly as needed
    a. Reports should be emailed exactly at the scheduled time
    b. Reports should be emailed or accessed by authorized users

2.3.3 Test Report

Req. #	Item	Test Case	Input	Expected Output	Actual Output	Pass/Fail
1	1a, 1b	1	aheinzman, *AD Password*	Log in to system	Log in to system	P
	1c	2	Anna, PASSWORD123	Failure to Log in	Failure to Log in	P
	1d	3	Add user	user added	user added	P
2	2a	4	Add email as action	Email received	Email received	P
	2b	5	Error String Located	Email received	Email received	P
3	3a	6	Report Time	Email received	Email received	P
	3b	7	Add email as action	Email received	Email received	P

2.3.4 Testing Screenshots

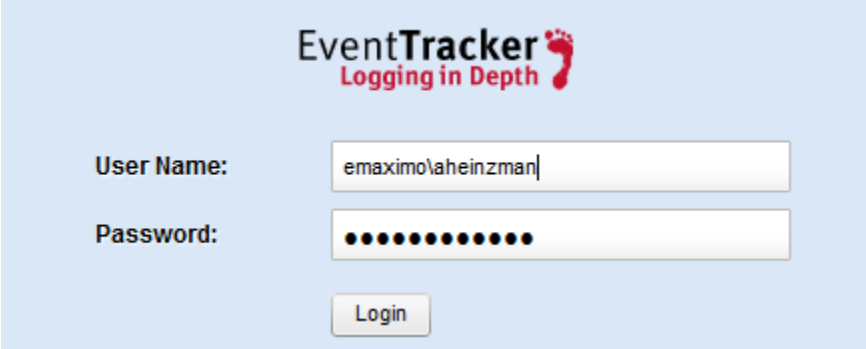

Image 1

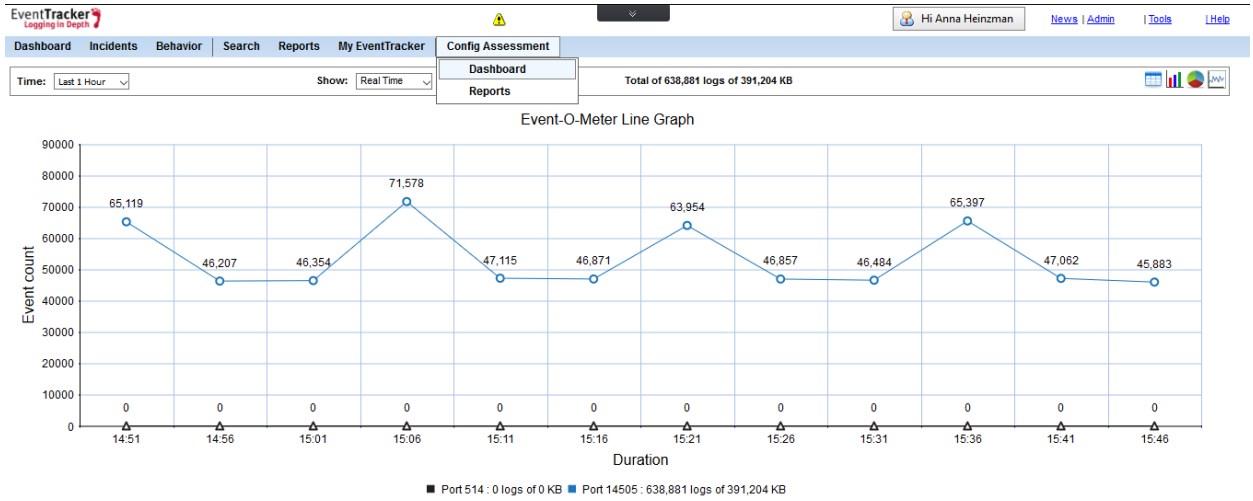

Image 2

Image 1 and 2 show a user putting in valid credentials and being taken to the landing page of Event Tracker

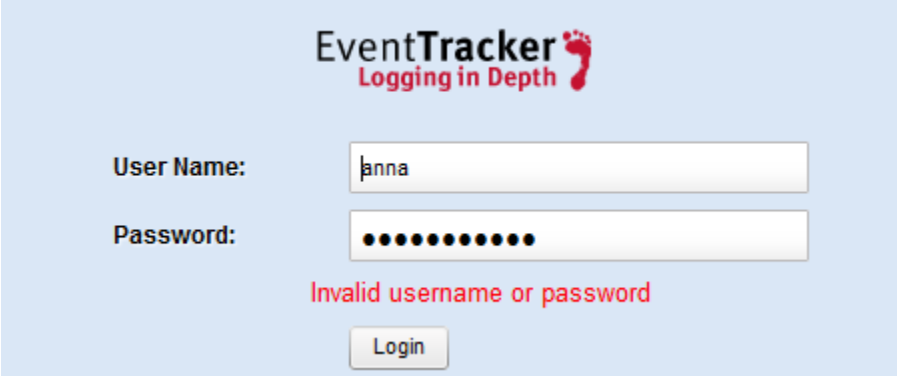

Image 3 - *shows the error message received when invalid credentials are used*

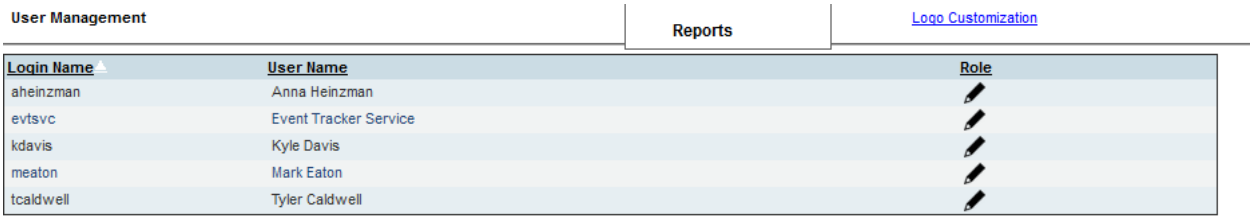

Image 4 – *list of authorized users*

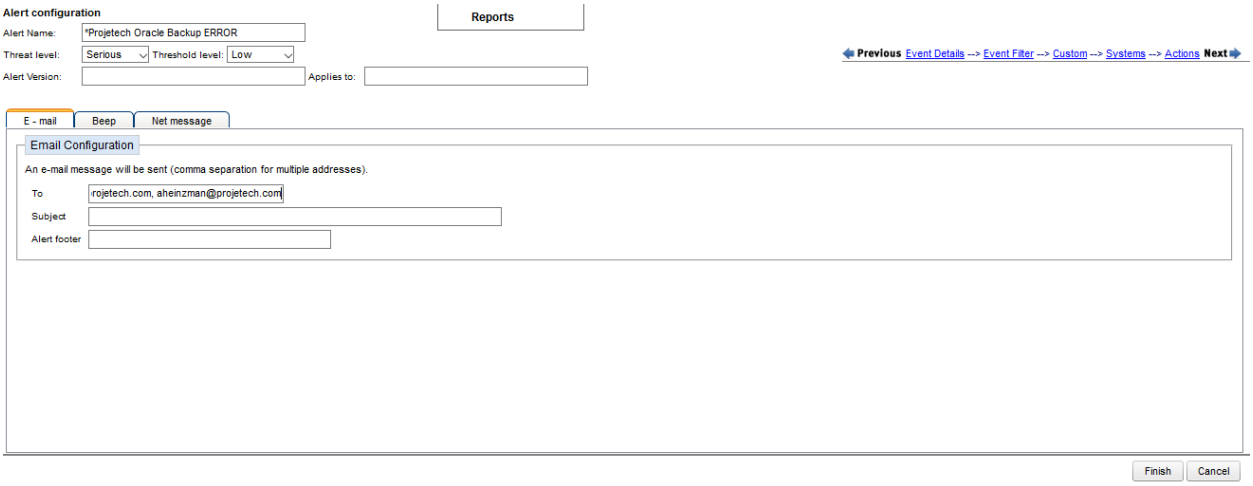

Image 5 – *List of emails alert is to be sent to*

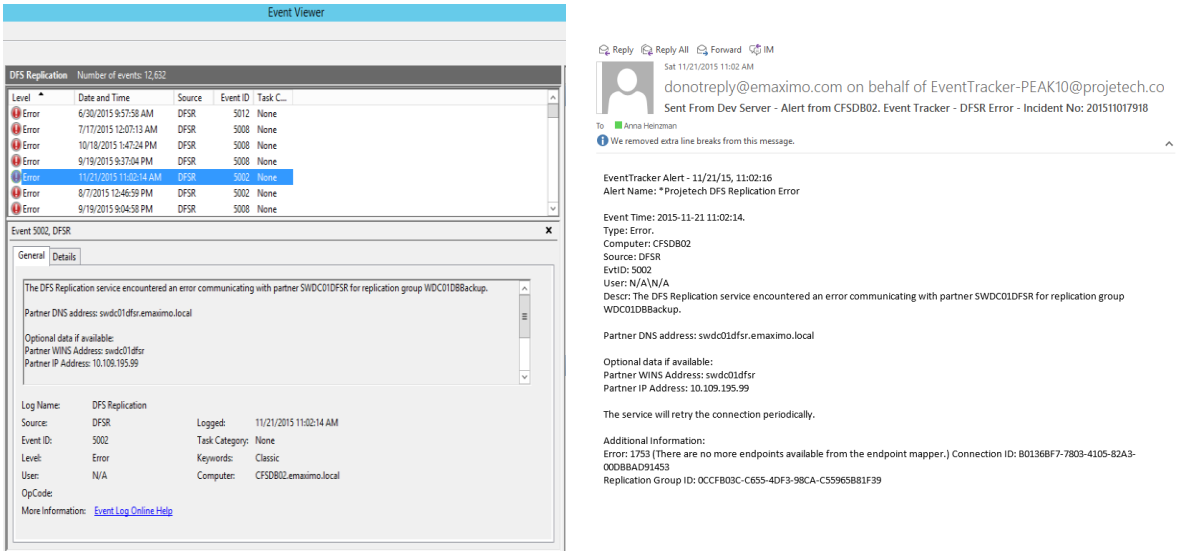

Image 6 – *Time of error and corresponding email*

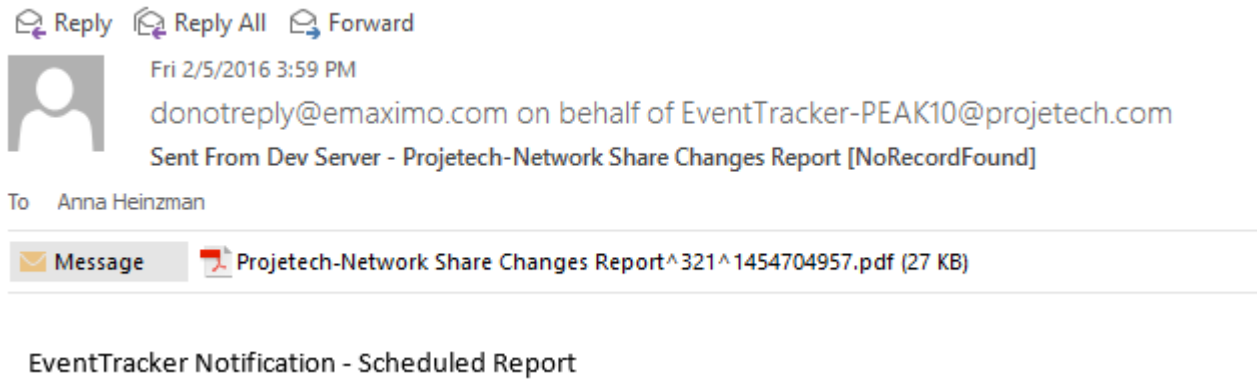

Image 7 – *an email is sent out at the schedule time, 3:59pm*

3. Conclusion

So in conclusion, we chose Event Tracker in order to try to get a deeper look into what was going on in our infrastructure. Some errors were not being caught by our current tools we have in place like a server health monitoring system, and a configuration manager, Tivoli Endpoint Manager (TEM). A SEIM, specifically Event Tracker, is the tool we needed for this and has already proven to be useful for what we currently have configured. I have only really done a small portion of what Event Tracker is capable of and I am looking forward to seeing what I can do in the coming semester and also all throughout my time at Projetech.

Bibliography

"Security Information and Event Management: Business Benefits and Security, Governance and Assurance Perspectives." ISACA. 2010. Accessed December 1, 2015. https://hazima.files.wordpress.com/2014/10/siem-business-benefits-and-security-governance-and-assurance-perspectives_whp_eng_1210.pdf.

"Pricing Comparison." Event Tracker. Accessed December 1, 2015. https://www.eventtracker.com/pricing/comparison/#.