



McAfee Enterprise Security Manager

Data Source Configuration Guide

Data Source: CyberArk PIM

Feb 14th, 2013



Important Note:

The information contained in this document is confidential and proprietary.

Please do not re-distribute without permission.



Table of Contents

1	Revision History	4
1.1	Revision Details	4
2	Introduction	5
3	Prerequisites	5
4	Data Source Configuration Details	5

4.1	CyberArk PIM Version X Configuration	5	Error! Bookmark not defined.
4.2	CyberArk PIM Version Y Configuration		Error! Bookmark not defined.
4.3	McAfee Receiver Configuration	9	
5	Troubleshooting		Error! Bookmark not defined.

1 Revision History

1.1 Revision Details

Revision Version	Author	Date	Description
1.0	Carlos Krystof	Feb 14th, 2013	Config guide

2 Introduction

This guide details how to configure the CyberArk PIM product to be able to send Syslog data in the proper format to the McAfee Enterprise Security Manager SIEM releases 9.0.2 and 9.1. It is applicable for CyberArk PIM.

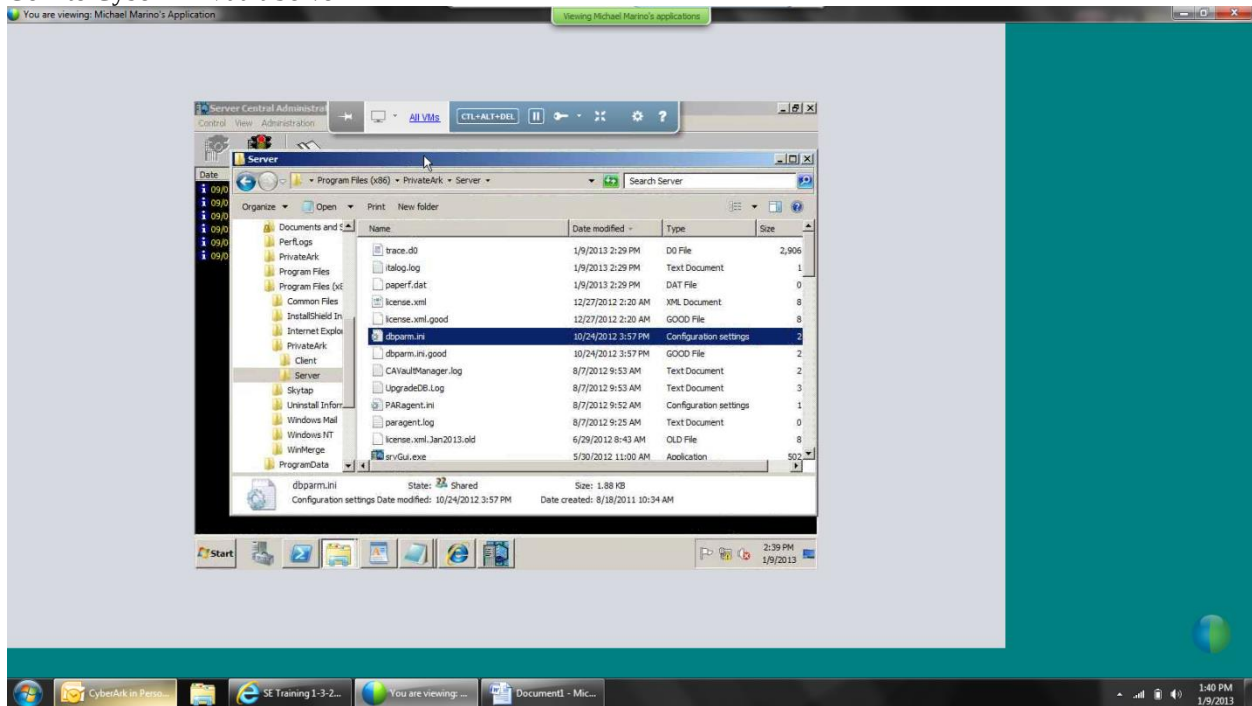
3 Prerequisites

In order to configure the CyberArk PIM Syslog service, appropriate administrative level access is required to perform the necessary changes documented below.

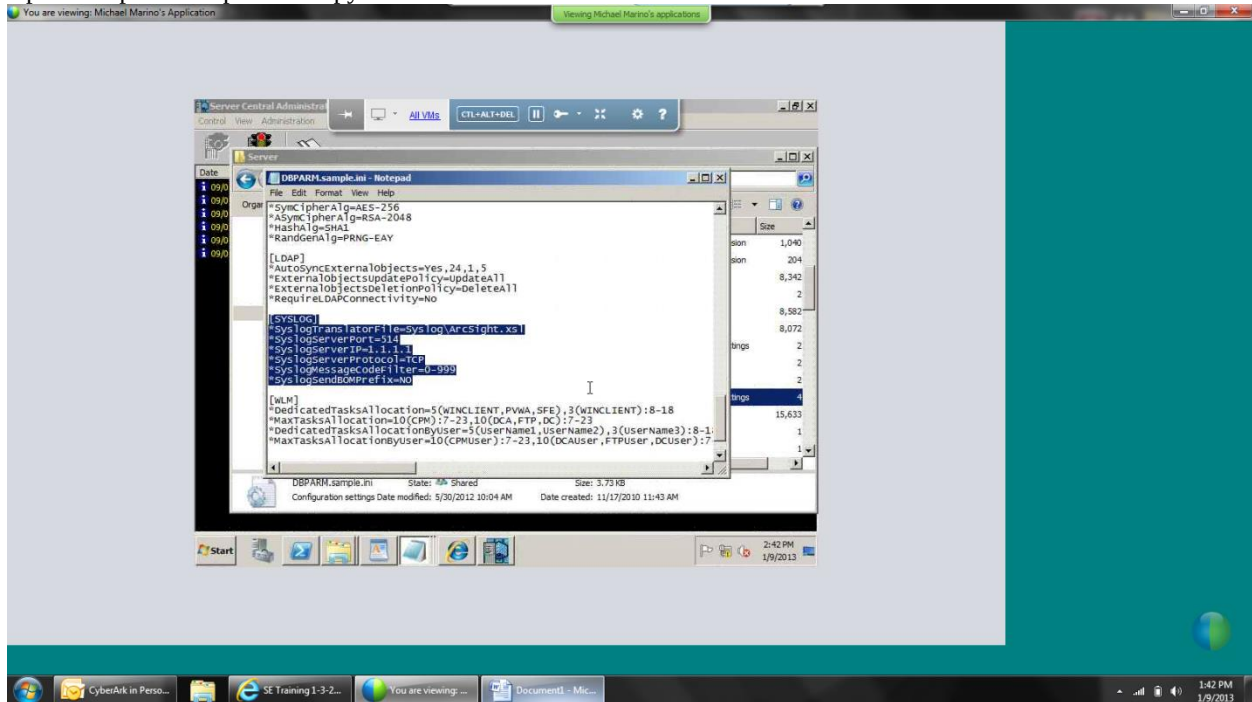
4 Data Source Configuration Details

4.1 CyberArk PIM Configuration

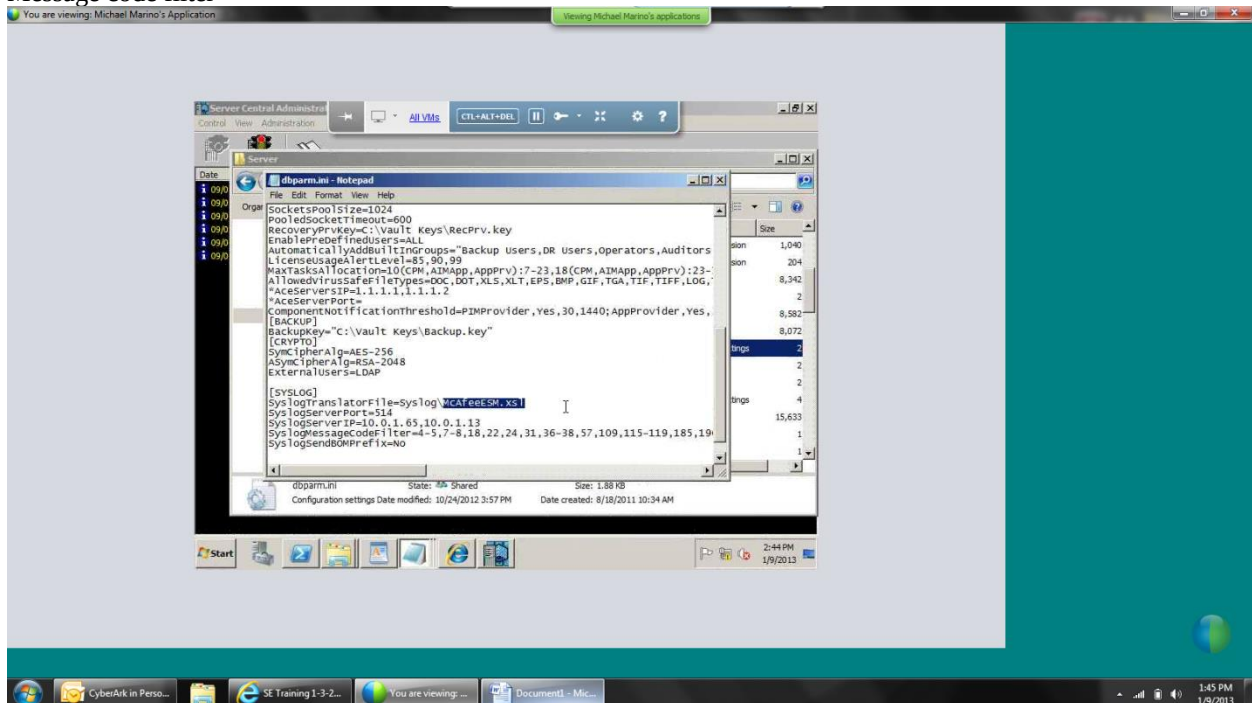
Go into CyberArk Vault Server



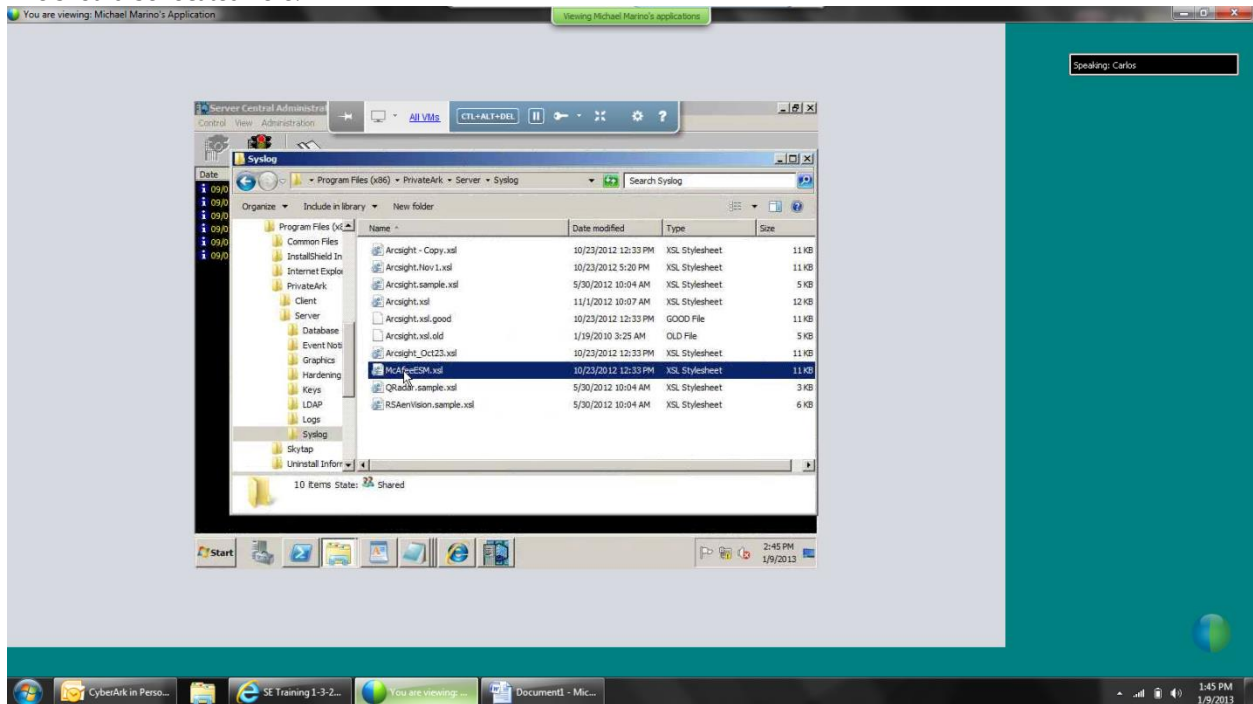
Open "DBparm.sample.ini" copy SYSLOG section



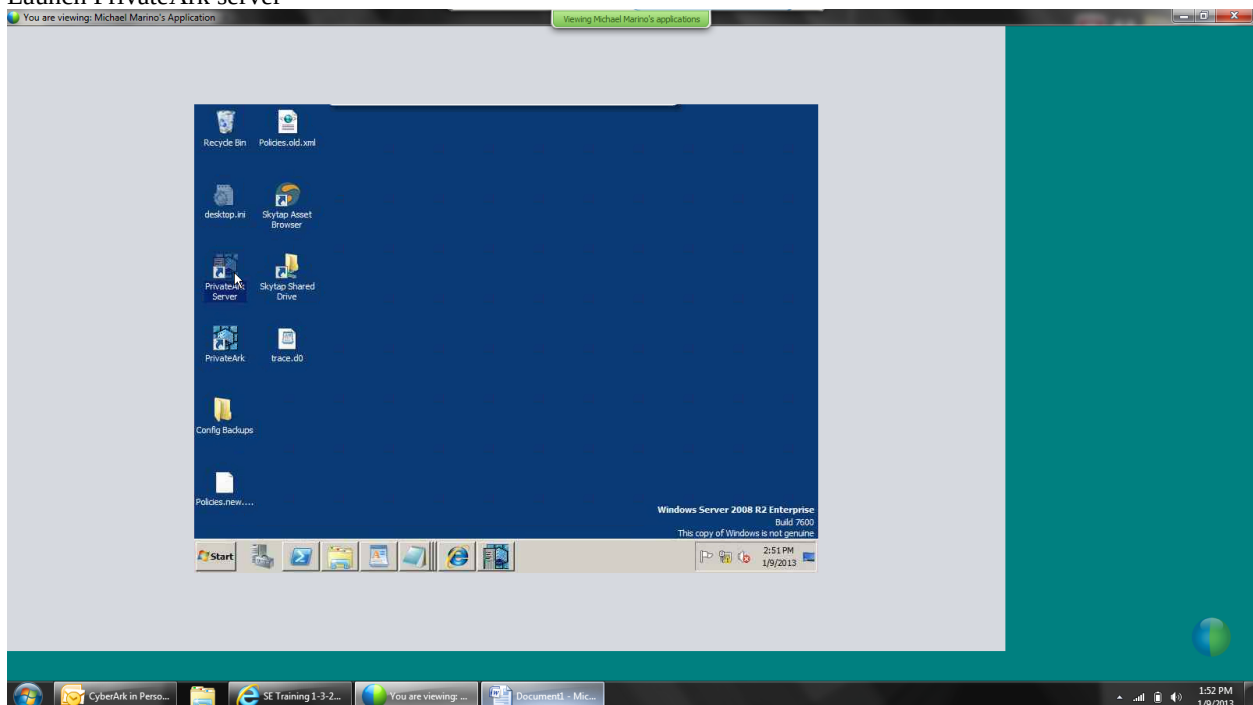
Copy to bottom of dbparm.ini
Rename McAfee
Enter port number
Enter IP address
Message code filter



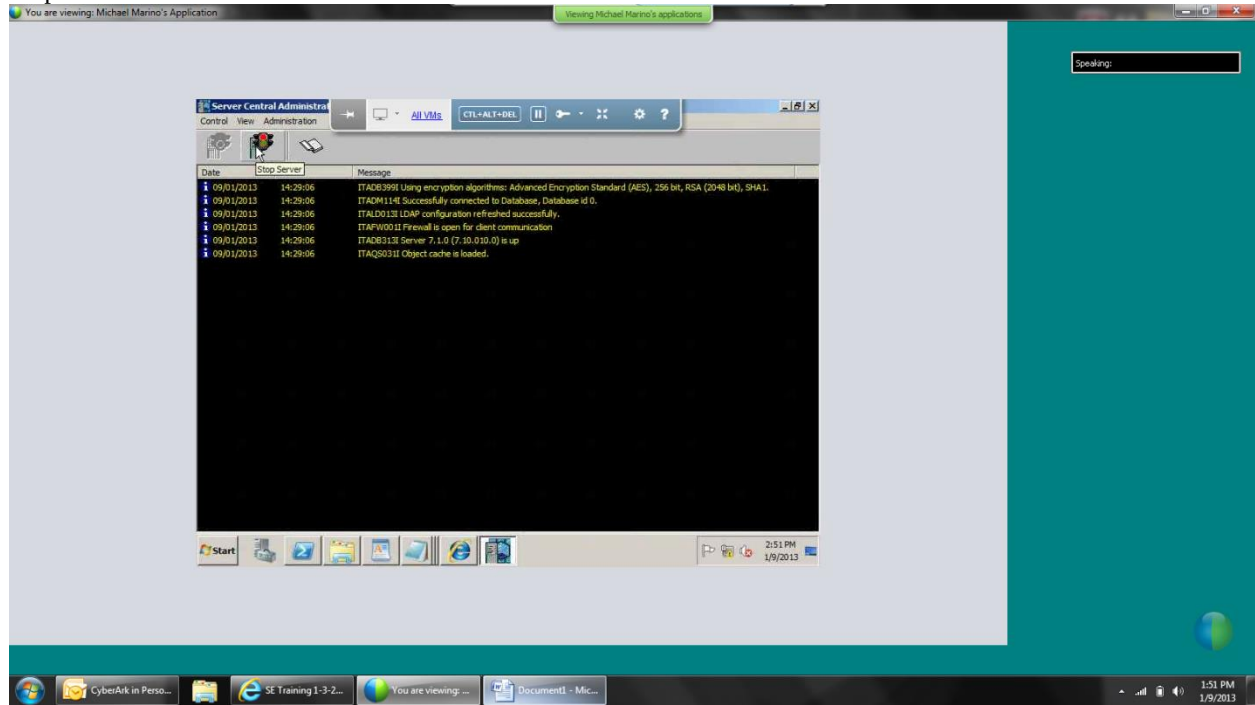
This syslog directory is the location of CyberArk parsers.
File should be located here:



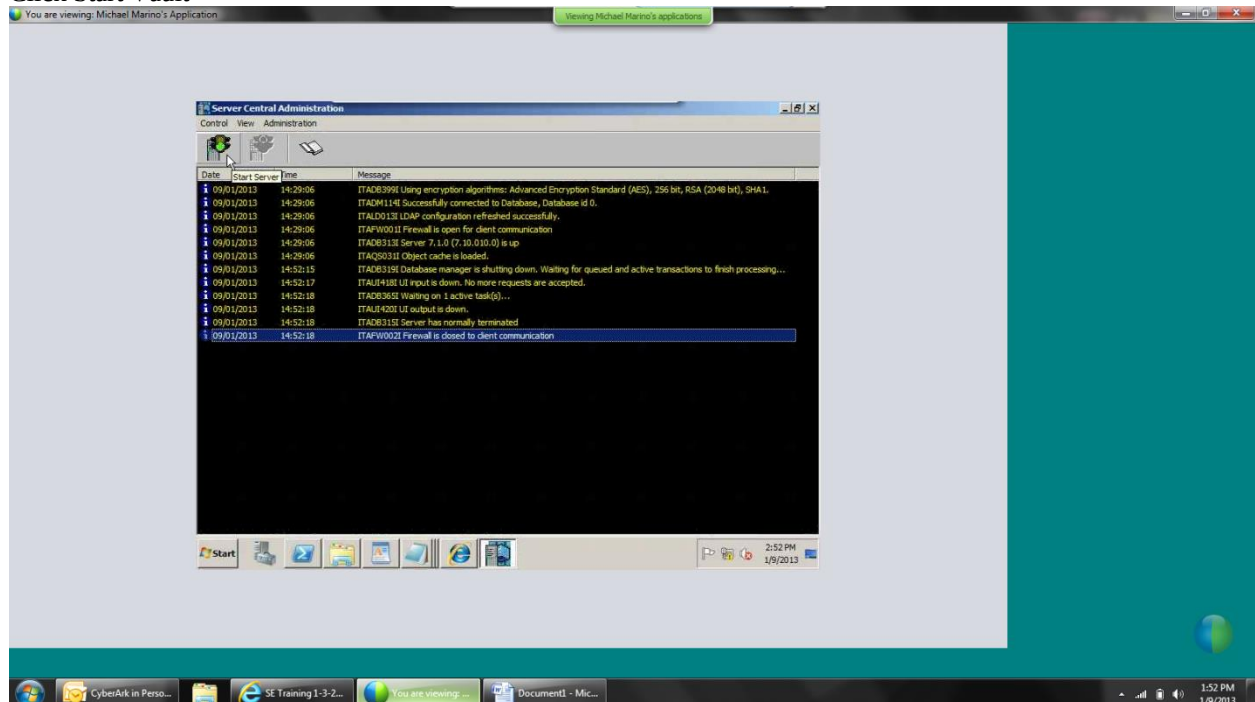
Launch PrivateArk server



Stop Vault



Click Start Vault



4.2 McAfee Receiver Configuration

After successfully logging into the McAfee ESM console the data source will need to be added to a device in the ESM hierarchy. In order to create a new data source to a McAfee Receiver from the [Data Source Long Name] device that you have just configured, follow these steps:

1. Select the receiver you are applying the data source setting to.
2. Select the Receiver properties.
3. From the Receiver Properties listing, select 'Data Sources'
4. After selecting the Receiver, select the Add Data Source icon.

Once you select the option to add a data source, you are taken to the Add Data Source menu. The general options for adding a data source are shown. As you select different options, additional parameters may show. Each of these parameters will be examined in more detail.

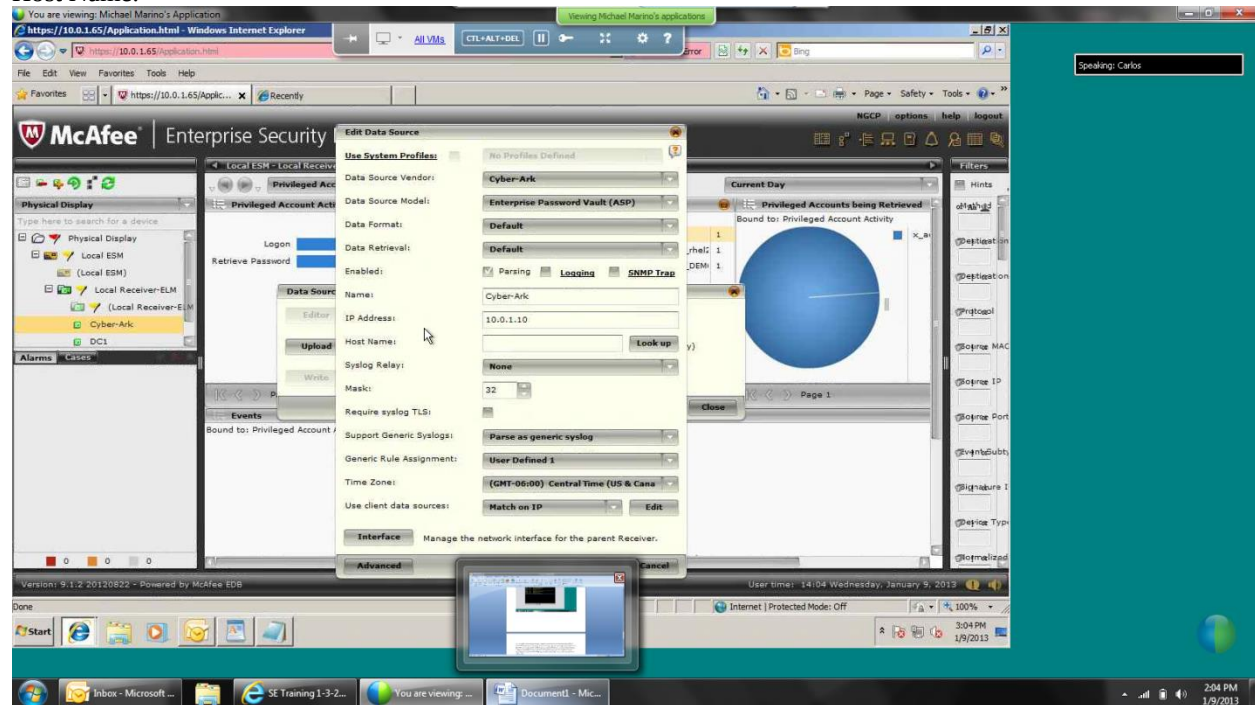
Select new Data Source and enter the following:

Data Source Vendor: CyberArk

Data Source Model: Enterprise Password Vault (ASP)

IP Address:

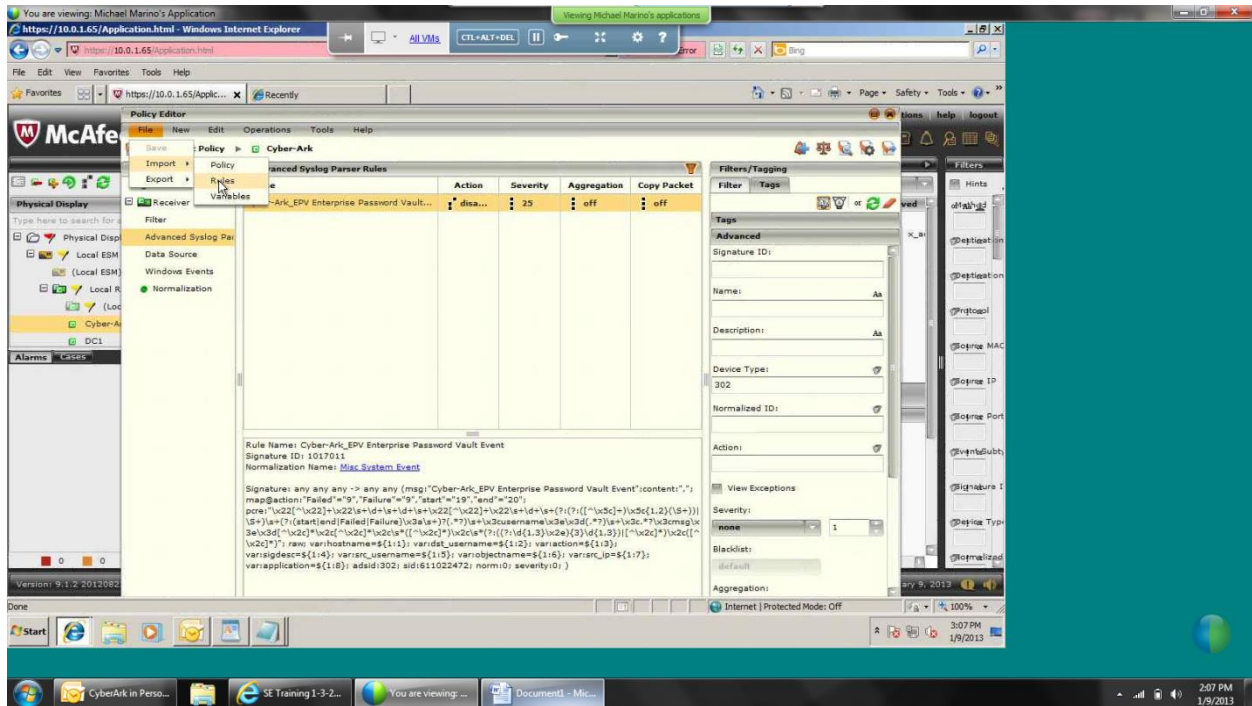
Host Name:

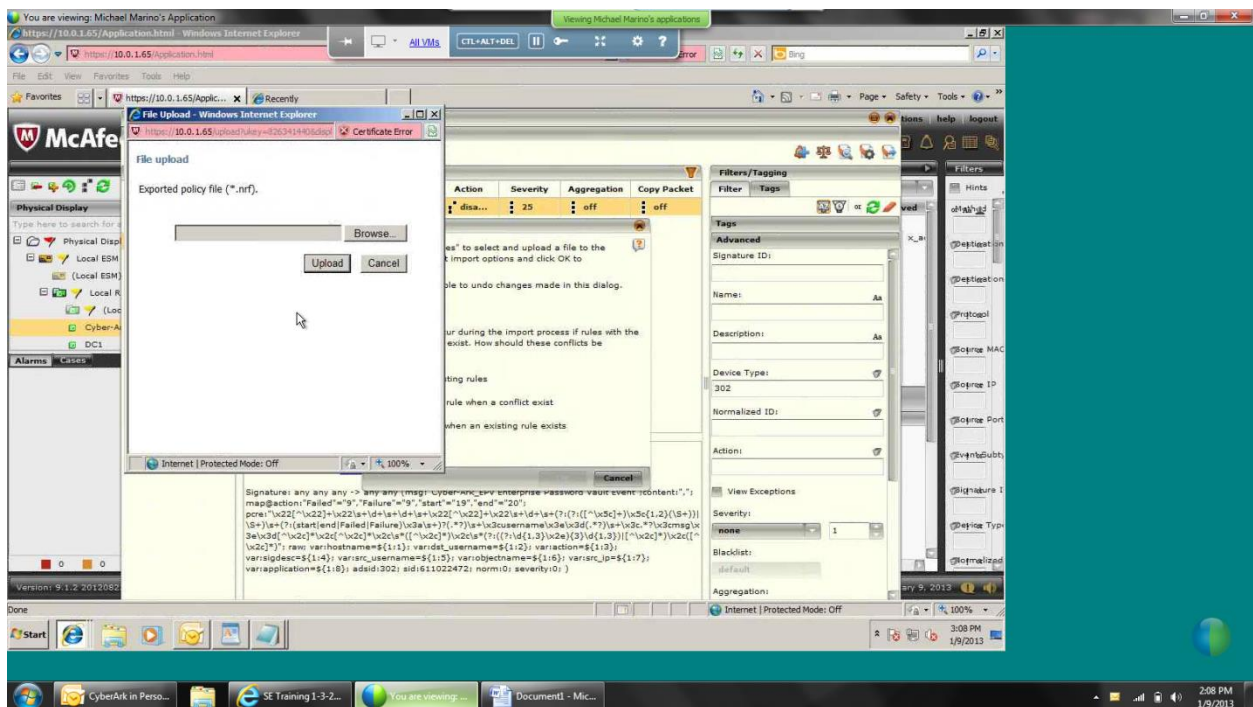
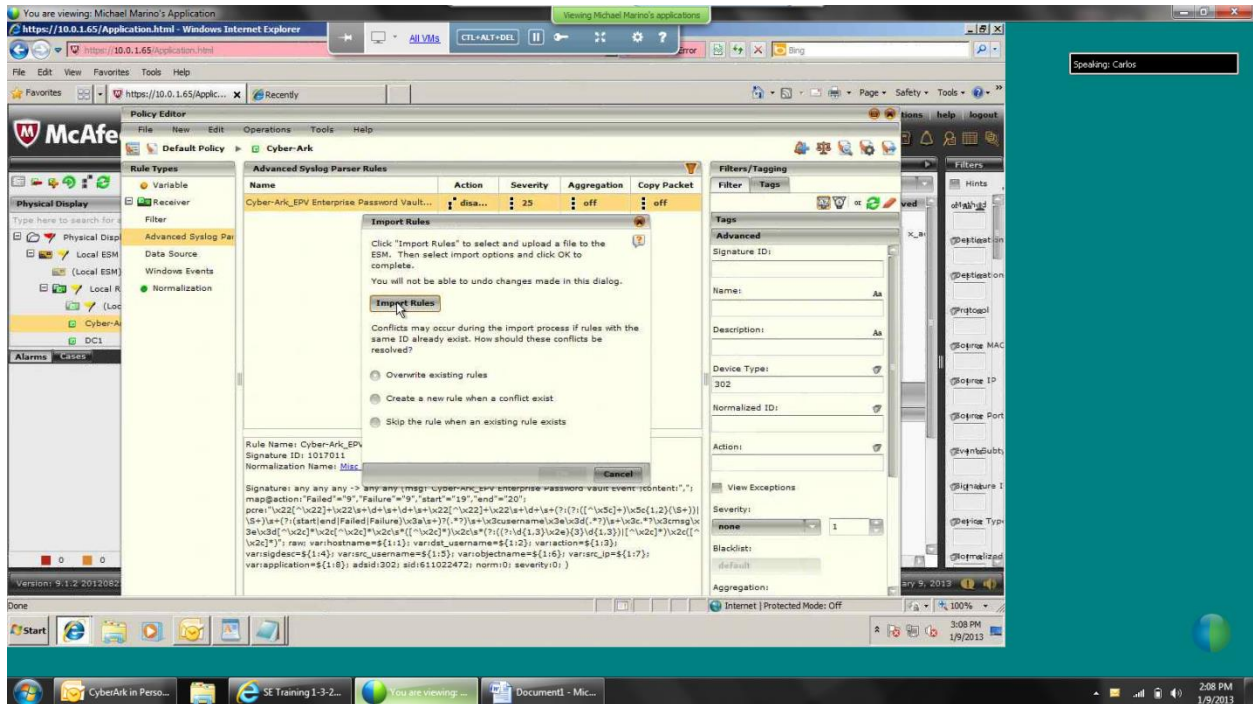


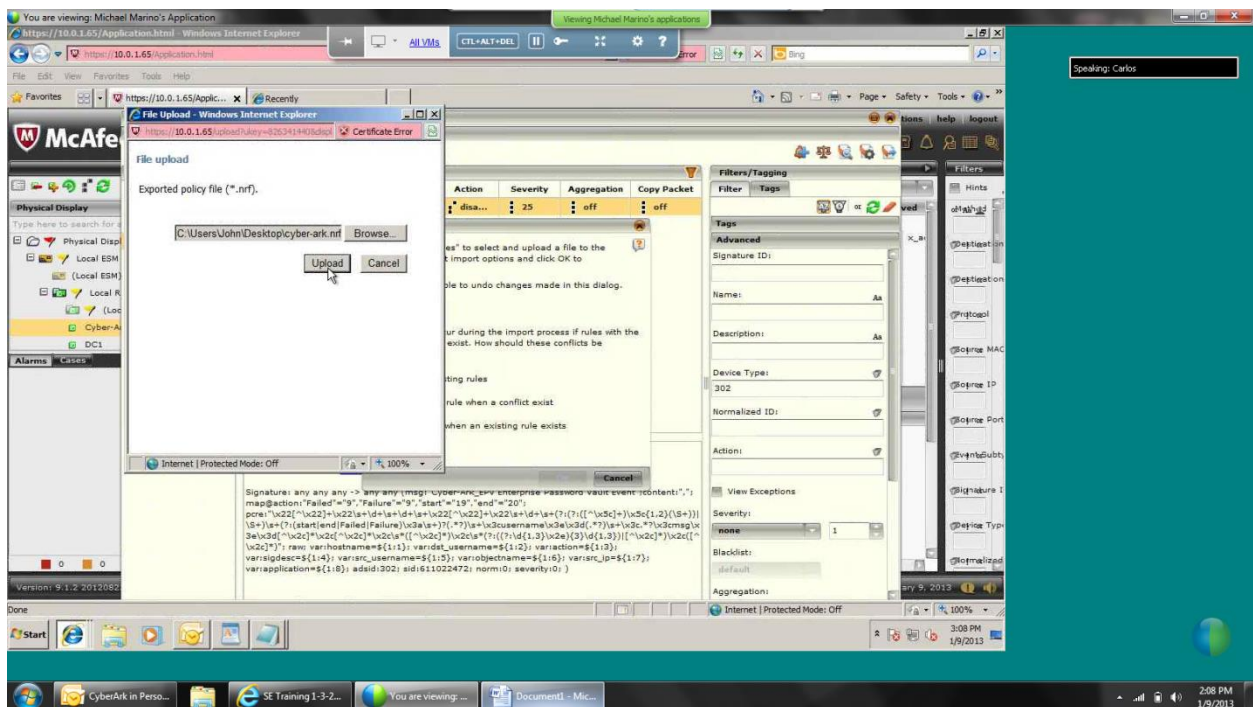
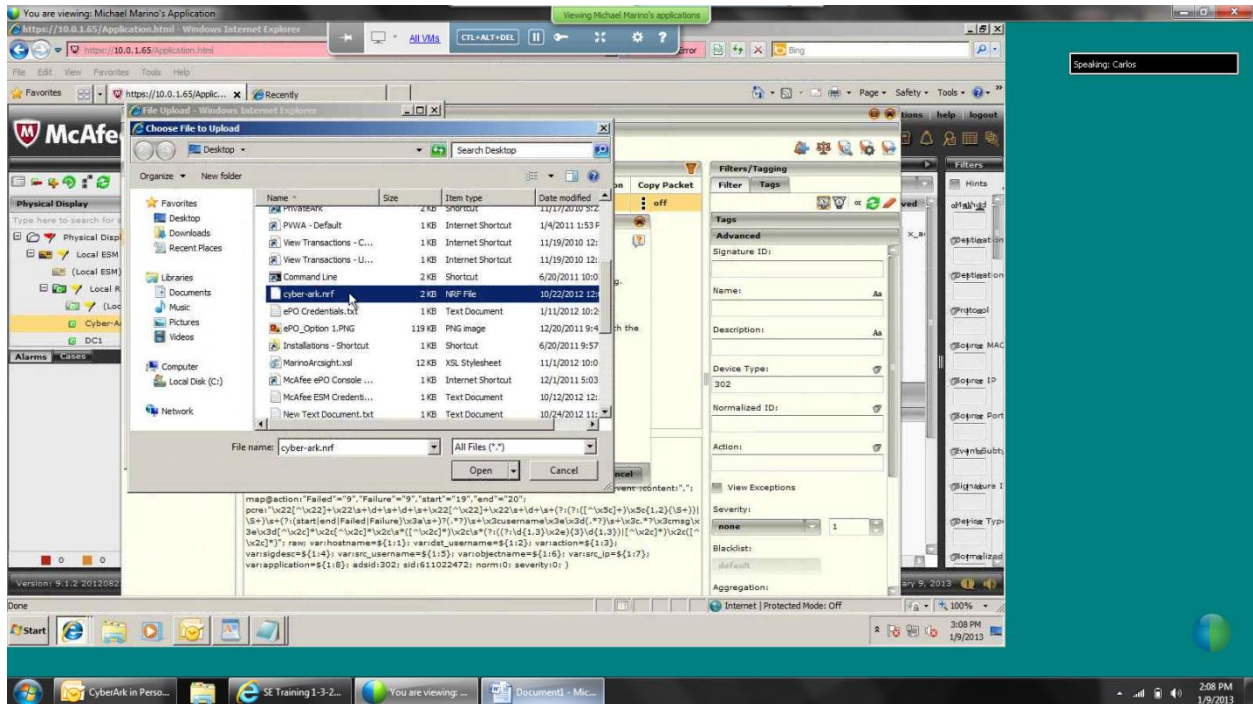
You will need to go to the policy manager, make sure your data source is selected, and go to file → Import → Rules. Browse to the .nrf rule, and import it. Next, select the Advanced bar near the bottom of the window on the right, clear the filter, scroll to the bottom, and select “user defined” from the Origin drop down. Click the green arrows near the top of the filter to run the query. You should see your imported rule in the window now. Enable the new rule, and roll policy.

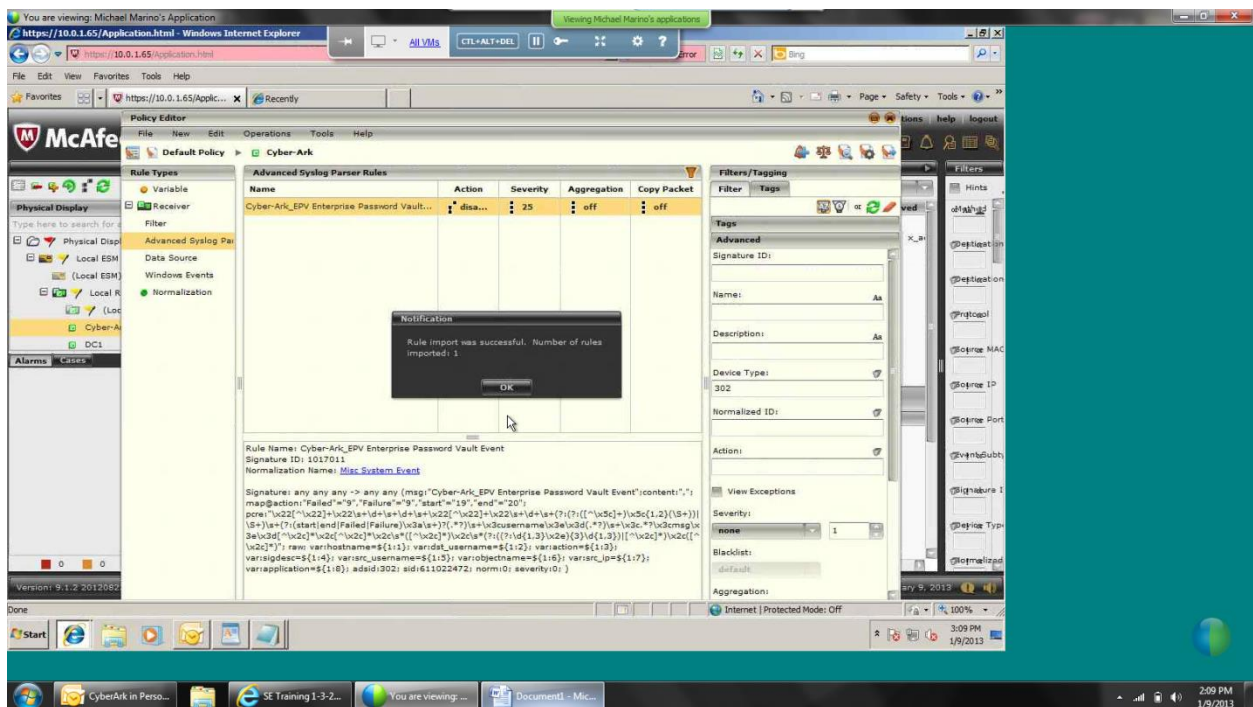
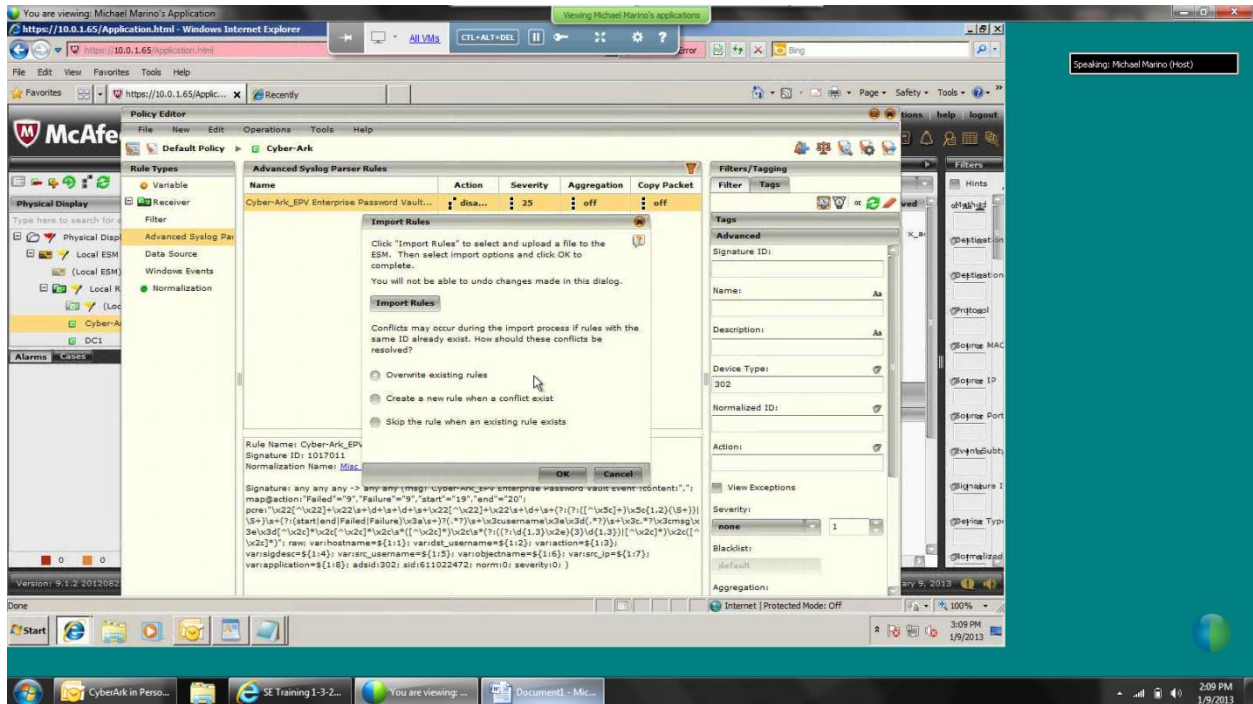


cyber-ark.nrf





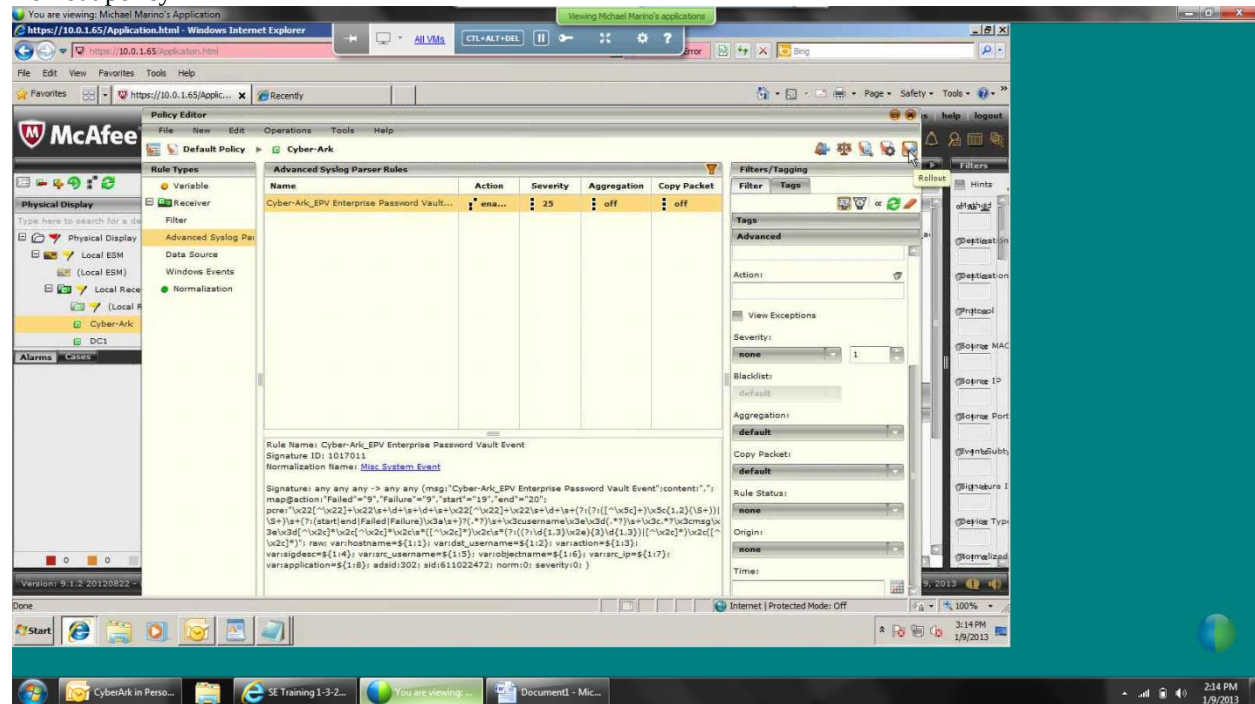




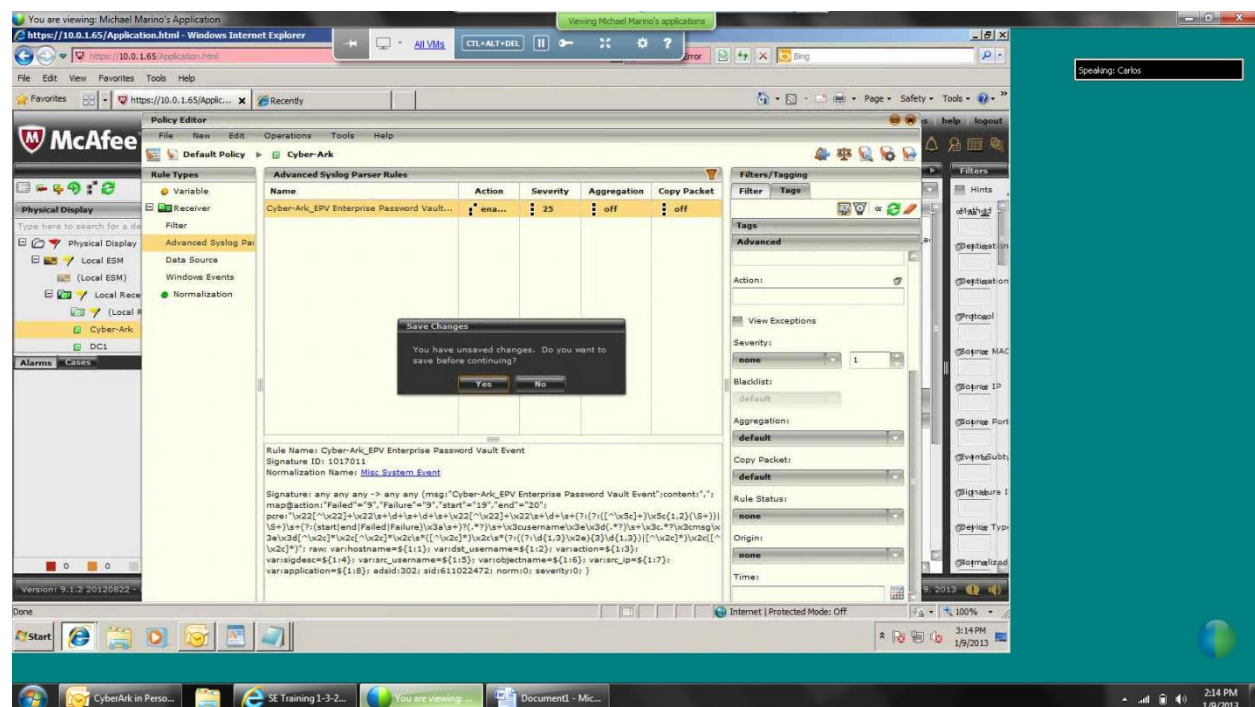
Enable Policy

[illegible]

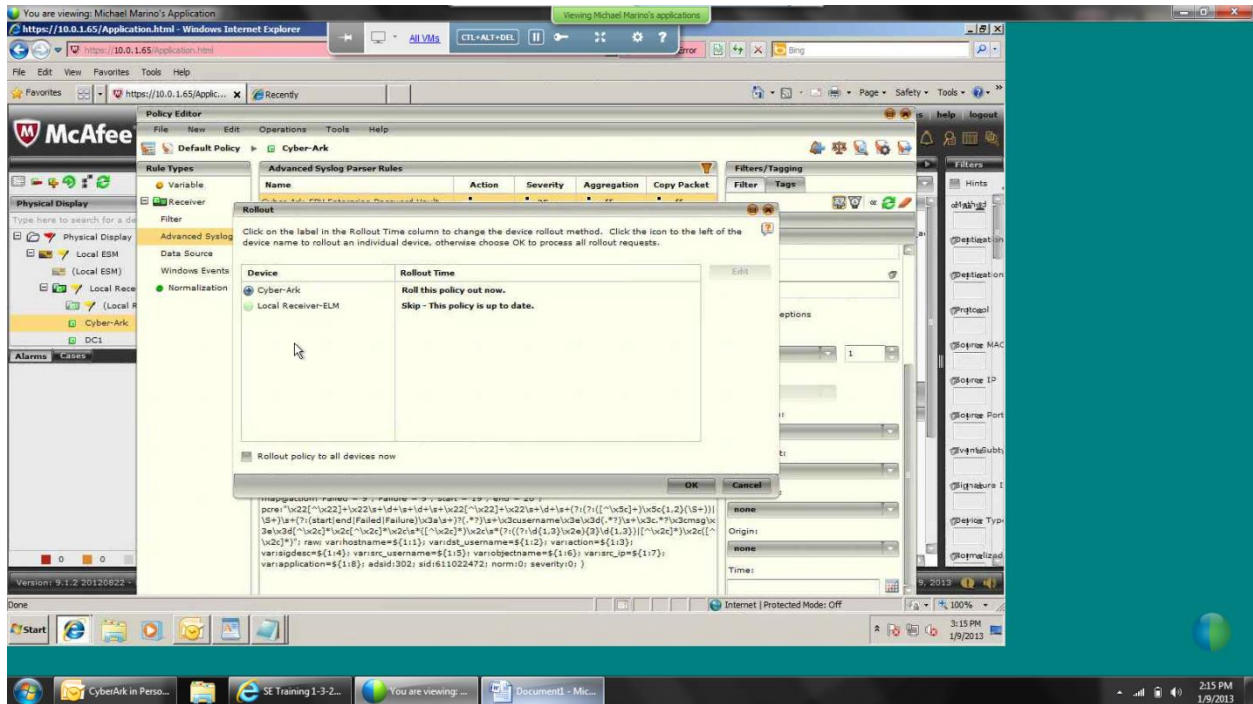
Roll out policy



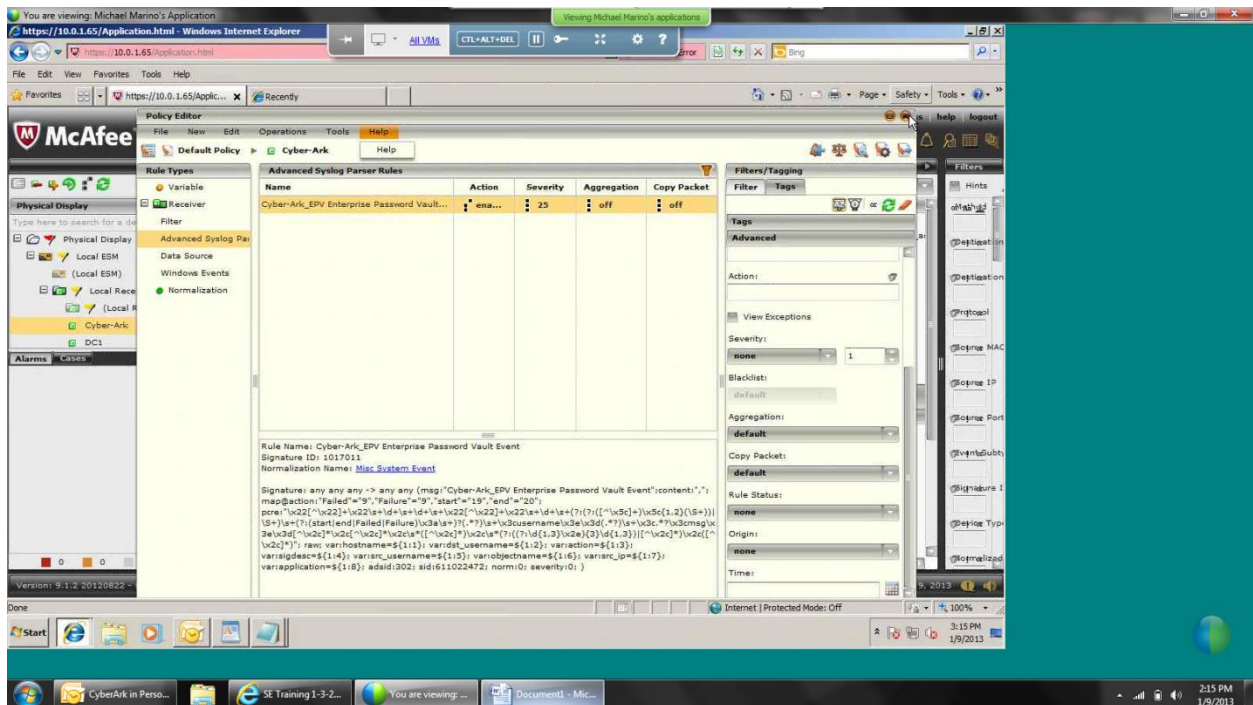
The screenshot shows the McAfee Policy Editor interface. The 'Advanced Syslog Parser Rules' table is visible, showing the rule 'Cyber-Ark Enterprise Password Vault' with an action of 'enable', severity of 23, aggregation of 'off', and copy packet of 'off'. The rule details on the right show the rule name, signature ID (1017011), and a complex signature string. The interface also includes a left sidebar with 'Physical Display' and 'Alarms' sections, and a top menu bar with 'File', 'New', 'Edit', 'Operations', 'Tools', and 'Help'.



This screenshot is similar to the one above, but with a 'Save Changes' dialog box open in the center. The dialog box contains the text: 'You have unsaved changes. Do you want to save before continuing?' with 'Yes' and 'No' buttons. The background interface remains the same, showing the rule configuration for 'Cyber-Ark Enterprise Password Vault'.

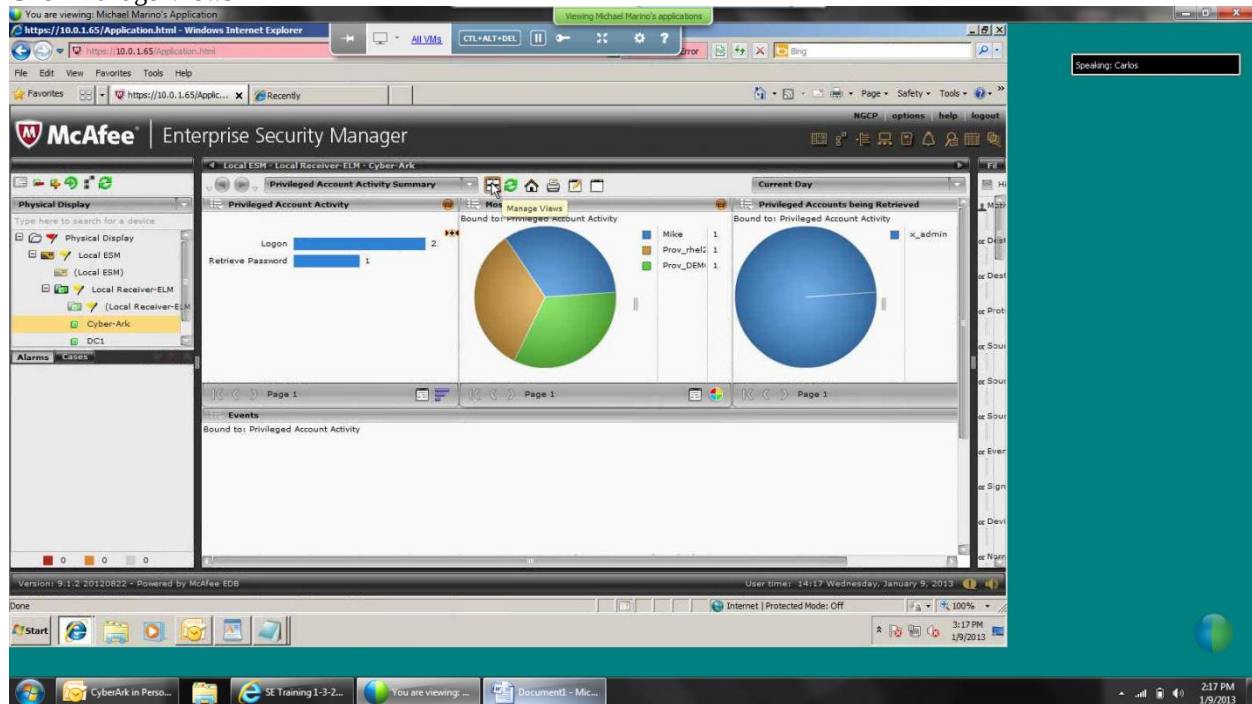


Close policy editor



5 Dashboards

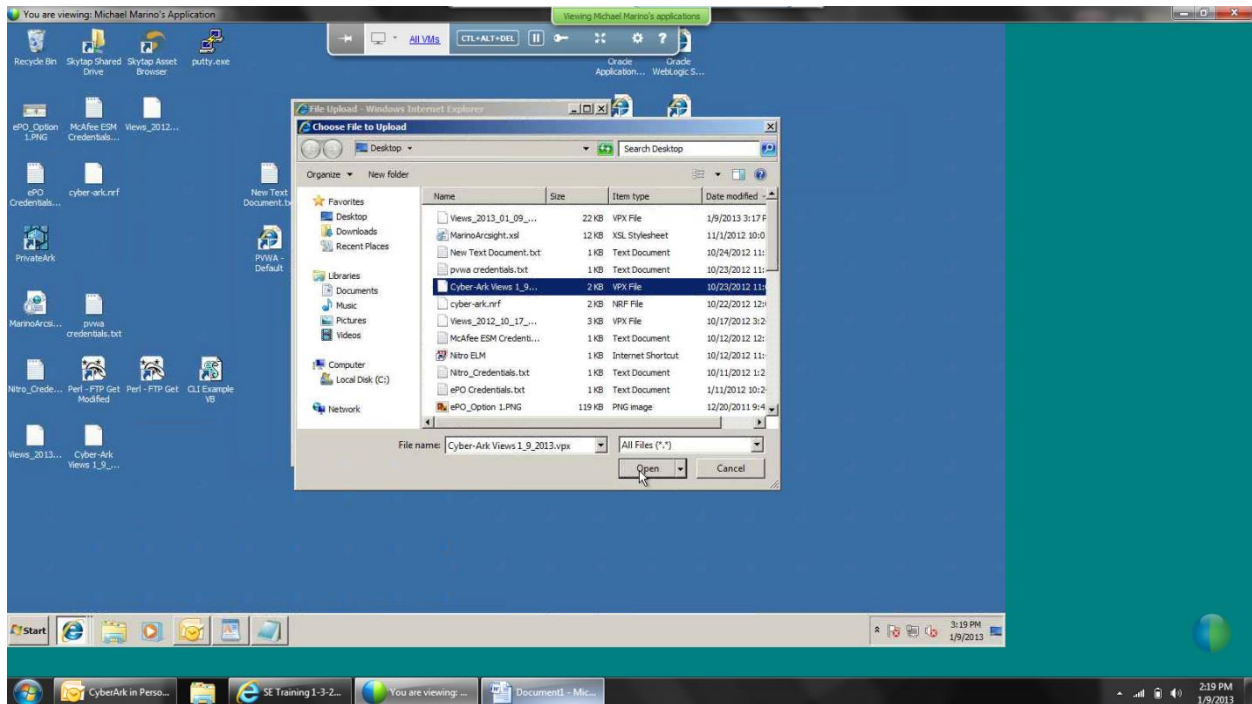
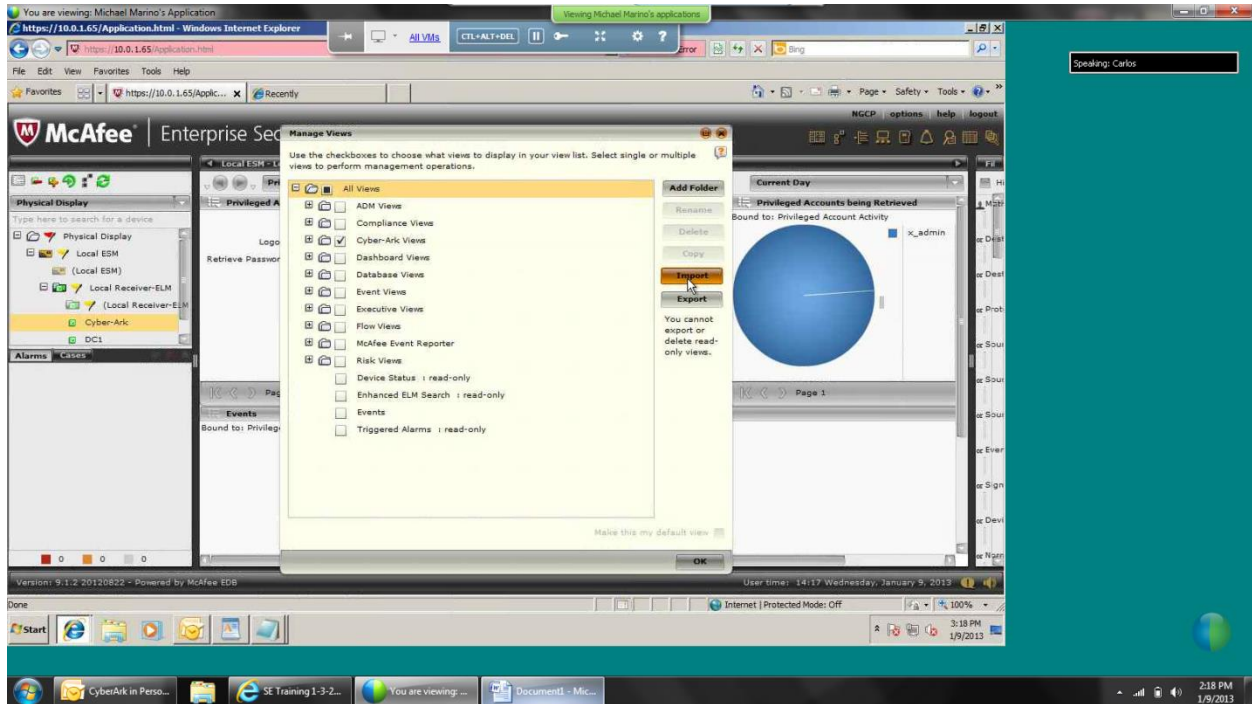
Import Dashboards:
Click Manage Views

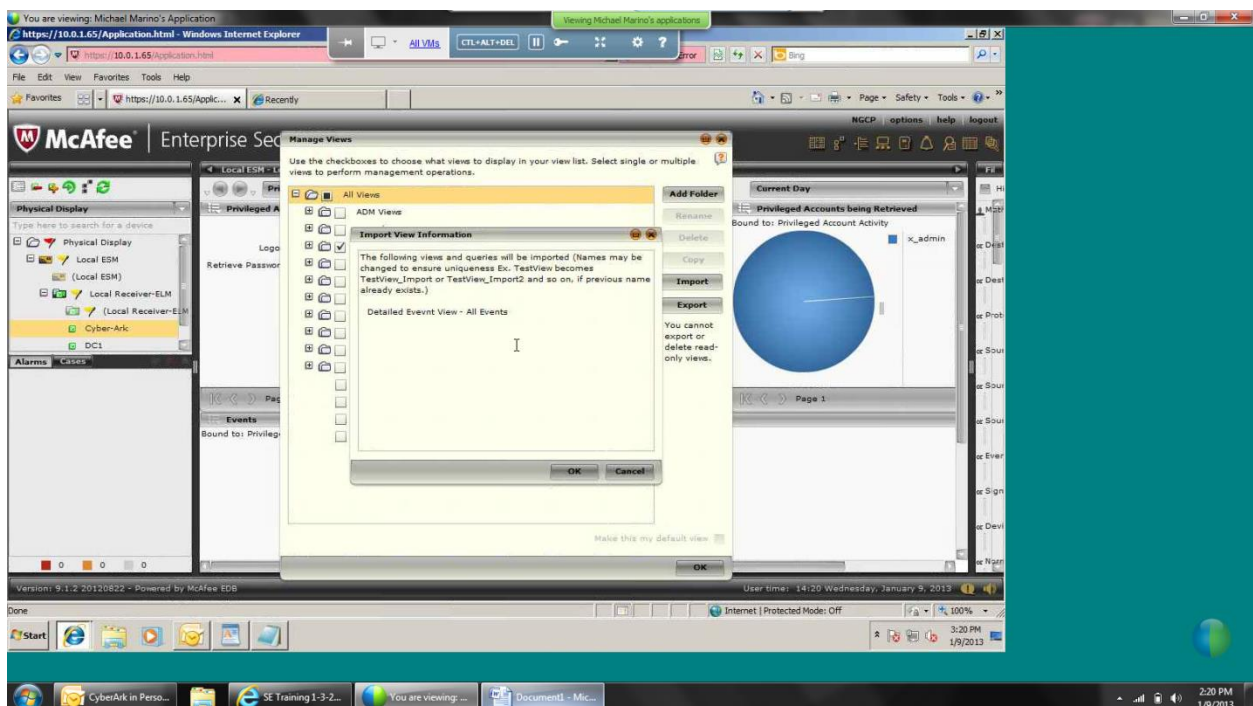
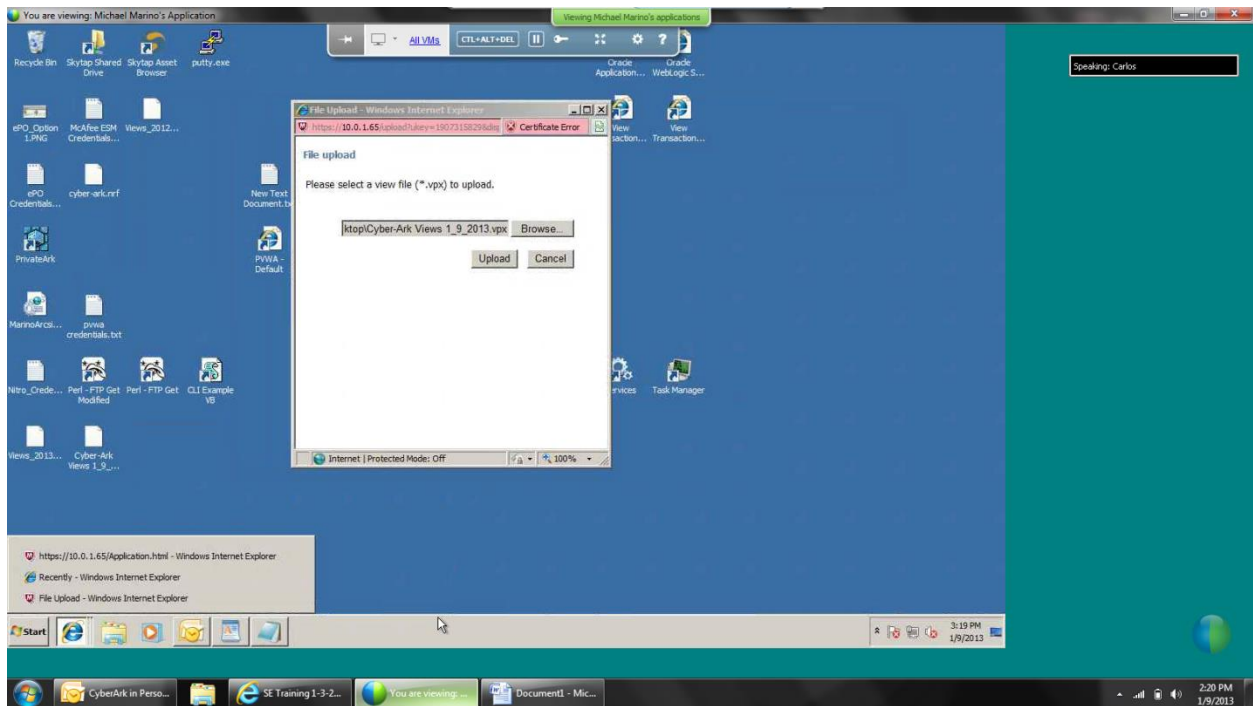


Select Import: Import file: Cyber-Ark Views 1_9_2013.vpx

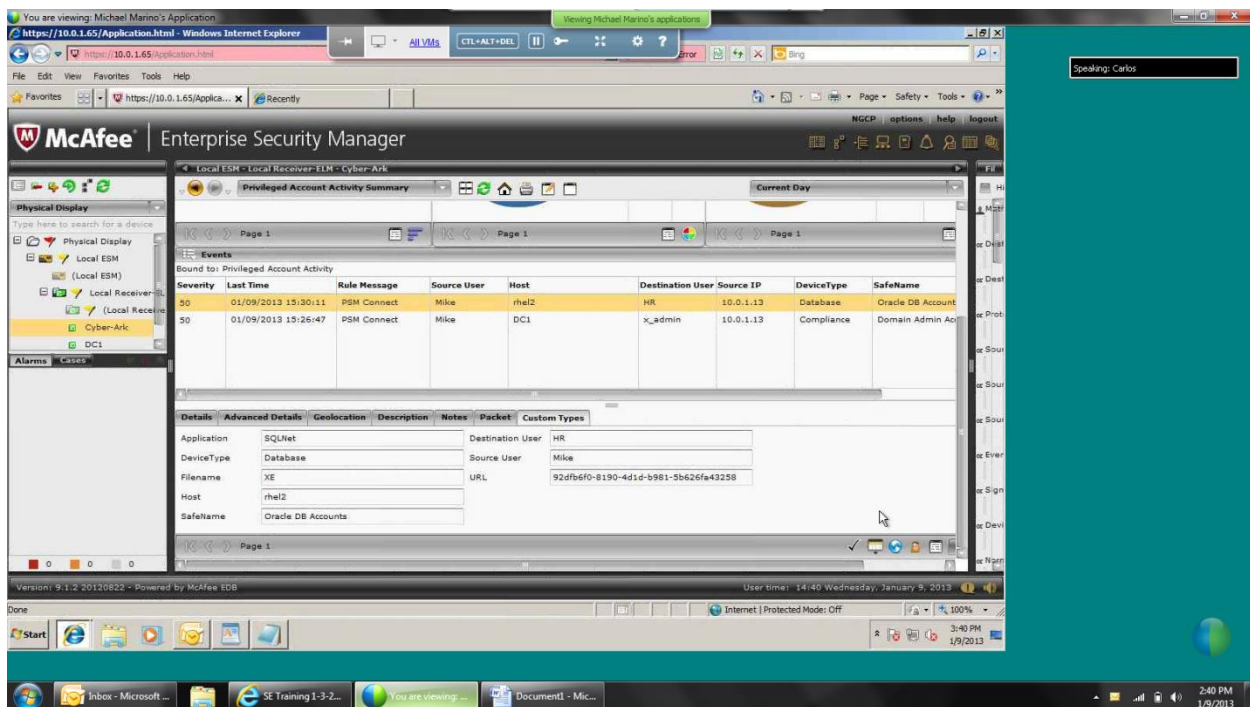
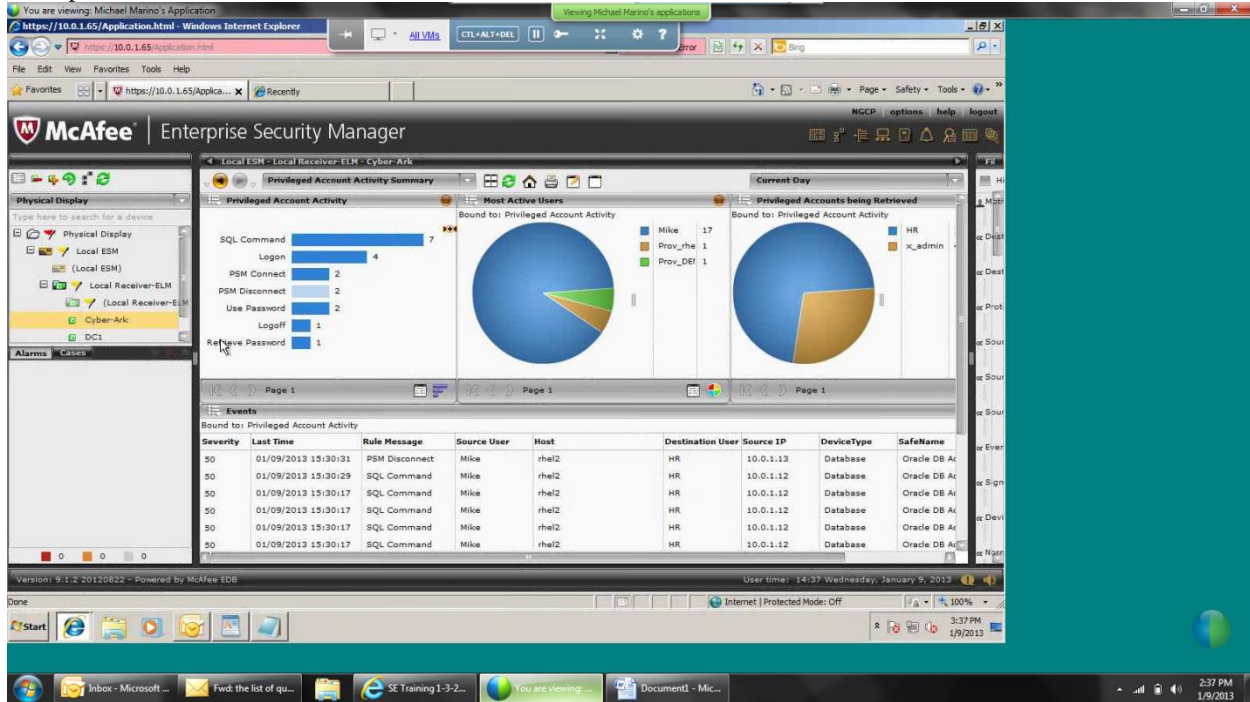


Cyber-Ark Views 1_9_2013.vpx





Examples



You are viewing: Michael Marino's Application

https://10.0.1.65/Application.html - Windows Internet Explorer

Viewing Michael Marino's applications

McAfee Enterprise Security Manager

Local ESM - Local Receiver-ELM - Cyber-Ark

Privileged Account Activity Summary

Current Day

Events

Bound to Privileged Account Activity

Severity	Last Time	Rule Message	Source User	Host	Destination User	Source IP	DeviceType	SafeName
30	01/09/2013 15:30:29	SQL Command	Mike	rhel2	HR	10.0.1.12	Database	Oracle DB Account
30	01/09/2013 15:30:17	SQL Command	Mike	rhel2	HR	10.0.1.12	Database	Oracle DB Account
30	01/09/2013 15:30:17	SQL Command	Mike	rhel2	HR	10.0.1.12	Database	Oracle DB Account
30	01/09/2013 15:30:17	SQL Command	Mike	rhel2	HR	10.0.1.12	Database	Oracle DB Account
30	01/09/2013 15:30:17	SQL Command	Mike	rhel2	HR	10.0.1.12	Database	Oracle DB Account

Details

Application: SQLNet

DeviceType: Database

Filename: XE

Host: rhel2

SafeName: Oracle DB Accounts

Destination User: HR

Source User: Mike

URL: 92dfb6f0-8190-4d1d-b981-5b626fa43258

Message_Text: select first_name,salary from employees

Version: 9.1.2 20120822 - Powered by McAfee EDB

User time: 14:40 Wednesday, January 9, 2013

Internet | Protected Mode: Off

3:40 PM 1/9/2013

Inbox - Microsoft ... SE Training 1-3-2... You are viewing ... Document1 - Mic...

You are viewing: Michael Marino's Application

https://10.0.1.65/Application.html - Windows Internet Explorer

Viewing Michael Marino's applications

McAfee Enterprise Security Manager

Local ESM - Local Receiver-ELM - Cyber-Ark

Privileged Account Usage

Current Day

Events

Bound to Privileged Account Activity

Severity	Last Time	Rule Message	Source User	Destination User	Host	Source IP	DeviceType	SafeName
30	01/09/2013 15:30:09	Use Password	Mike	HR	rhel2	components.test.net	Database	Oracle DB
30	01/09/2013 15:26:44	Use Password	Mike	x_admin	cyber-ark-demo	components.test.net	Compliance	Domain A
30	01/09/2013 14:34:20	Retrieve Password	Mike	x_admin	cyber-ark-demo	components.test.net	Compliance	Domain A

Details

Application:

DeviceType: Database

Domain:

Host: rhel2

SafeName: Oracle DB Accounts

Destination User: HR

Source User: Mike

Subject: (McAfee ePO Ticket ID: Event sent to McAfee)

Version: 9.1.2 20120822 - Powered by McAfee EDB

User time: 14:42 Wednesday, January 9, 2013

Internet | Protected Mode: Off

3:42 PM 1/9/2013

Inbox - Microsoft ... SE Training 1-3-2... You are viewing ... Document1 - Mic...

