McAfee Enterprise Security Manager

Windows Content Pack

February 3, 2016

Contents

1 Introduction

Monitoring of Windows devices is a critical part to ensuring environment security. There are specific Windows events that should be examined closer than other events. The Windows Content Pack focuses on these specific events and helps bring them to light through its included components.

2 Included Components

This section will detail the different components of the content pack.

2.1 Alarms

This content pack does not contain any alarms.

2.2 Correlation Rules

This content pack does not contain any correlation rules.

- Windows - Multiple System and Service Failures
- Windows - System or Service Failure with Malicious Activity

2.3 Reports

The reports included in this content pack have been designed to give a general overview into specific Windows events.

- Windows - System and Service Failure Report

2.4 Variables

This content pack does not contain any variables.

2.5 Views

The included views provide more details into service failures and expand on where they are originating from.

- Windows System and Service Failures

2.6 Watchlists

This content pack does not contain any watchlists.

3 Prerequisites

The Windows Content Pack requires at least one Windows Event Log - WMI data source added to the McAfee ESM.

4 Post-Installation Information and Configuration

See Knowledge Base article KB83783 to learn how to change the content pack components. (https://kc.mcafee.com/corporate/index?page=content&id=KB83783)

5 Use Case(s)

The purpose of this use case is to show a working example of how the components of the Windows Content Pack can be used.

5.1 Windows System and Service Events

Windows services should be monitored to ensure proper expected functionality. On the "Windows System or Service Failures" view, events signifying Windows service errors or failures are shown. Using this view events can quickly be drilled down to specific hosts or services that are having issues. From there, the issues can be investigated further on the host(s) experiencing the issue(s).

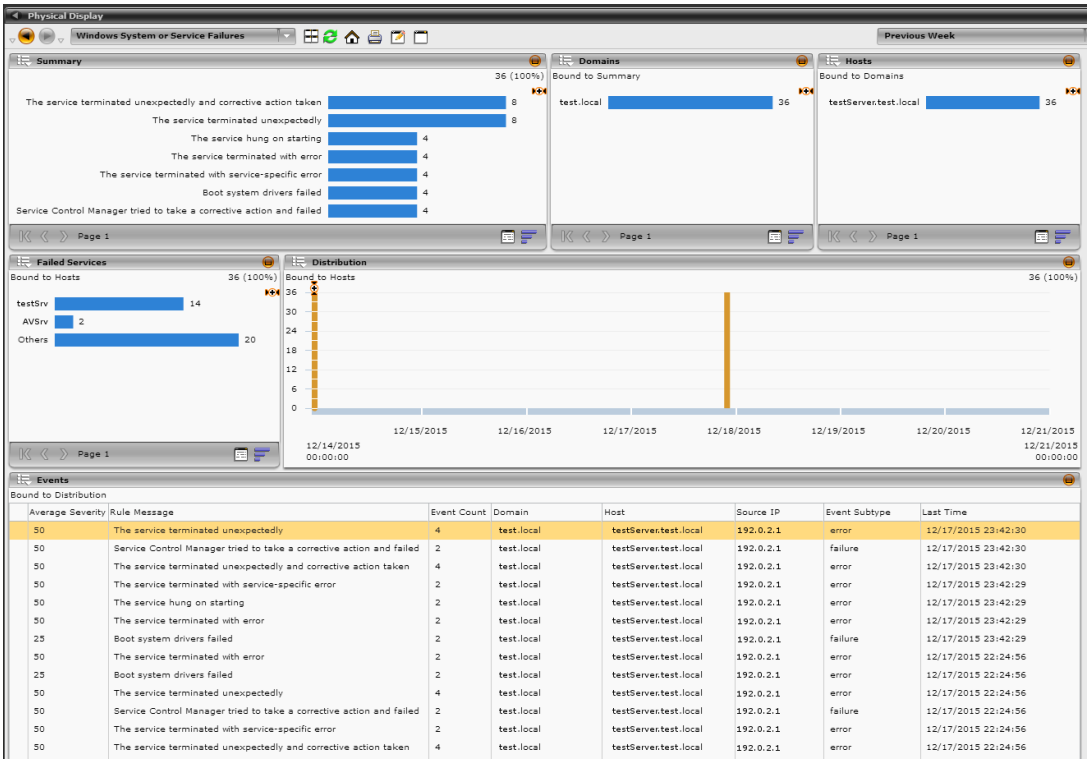

Image 5.1.1

6 Appendix A – View Details

6.1 Windows System and Service Failure View

The following image shows the “Windows System and Service Failure” View. This view shows all services or systems that have malfunctioned due to failure, configuration error, or user error. The specific reason for malfunction is determined by the reason or error codes WMI will supply. It is primarily filtered by Windows Event signatures with all of the view panes bound to each other in a left to right, and then top to bottom pattern.

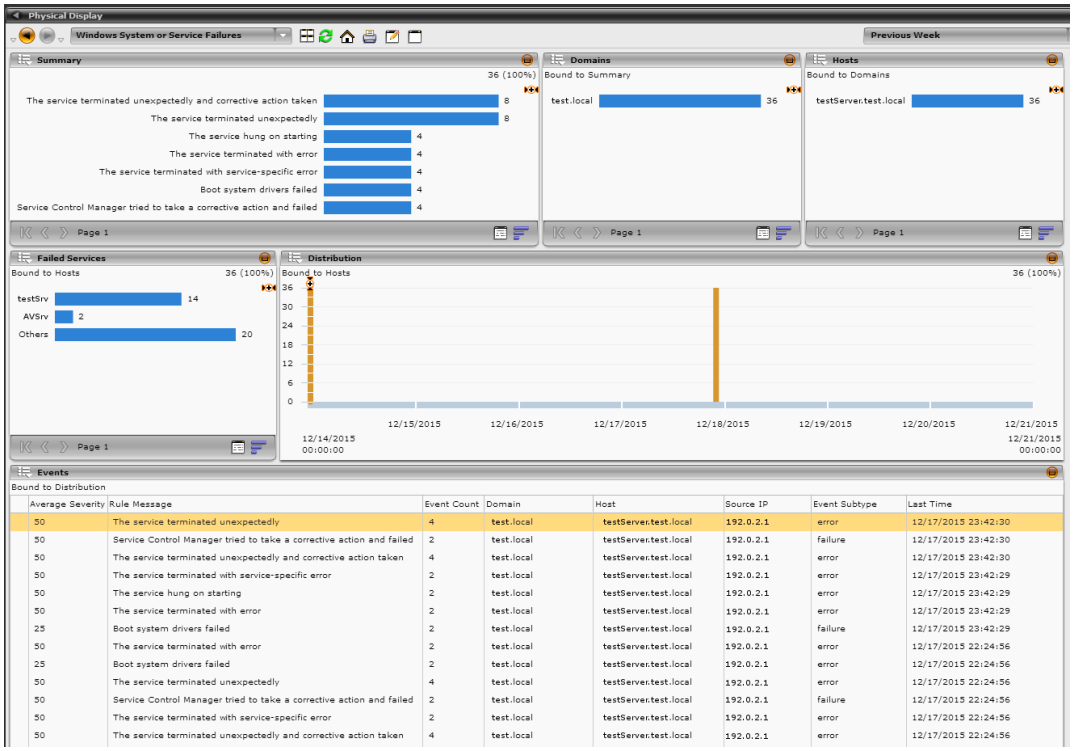

Image 6.1.1

7 Appendix B – Correlation Rule Details

7.1 Windows – Multiple System and Service Failures

This correlation rule triggers with multiple Windows service or system failure events.

Parameter Defaults:

- Time_Window: 10 minutes
- Number_of_Events: 15 events

7.2 Windows - System or Service Failure with Malicious Activity

This correlation rule is triggers when a malicious event and a Windows system or service failure event occurs on a single host.

Parameter Defaults:

- Time_Window: 10 minutes
- Number_of_Events: 1 event