# Lab Activity #2: Investigate Incident Detection and Analysis Tools

## Purpose: Assess and Document Incident Detection & Analysis Tools for Windows 8.1 Workstations.

1. Assess and document the uses of the Windows 8.1 *Windows Defender* utility as part of the incident response process.
2. Assess and document the uses of the Microsoft Baseline Security Analyzer (MBSA) tool to detect and analyze software and configuration vulnerabilities in Windows 8.1 systems during the incident response process.

## Overview:

There are many different types of tools which perform automated detection and analysis of known threats (Cichonski, Millar, Grance, & Scarfone, 2012). For this activity, we will focus upon assessing and documenting two such tools which can be used in the **detection and analysis phase** of the Incident Response Process (as defined in NIST SP 800-61r2).

First, we will examine the host-based anti-virus (malware detection) and host-based intrusion detection and prevention capabilities that are built into Windows 8.1 in the Windows Defender utility. This tool can be used to detect threats to confidentiality of information, threats to system integrity, and threats to system availability. Windows Defender also provides **containment, eradication, and recovery** capabilities that can automatically return Windows 8.1 workstations to known-good states (restoring system integrity) by removing or quarantining files that have been infected by malware. Windows Defender is usually configured to start during the workstation boot process and runs in the background to provide real-time threat detection and response.

Microsoft Baseline Security Analyzer (MBSA) is a scanning tool that can be used to analyze system configuration parameters and detect when the parameter settings are outside allowable ranges or if combinations of settings will result in vulnerabilities that can be exploited by attackers. This tool examines the system registry and other configuration files and compares the settings for key parameters to a system security configuration baseline established by the operating system vendor, Microsoft. MBSA is run on-demand and can also be run on a scheduled basis using the operating system’s task scheduler.

**Reference**

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST SP 800-62 rev. 2). http://dx.doi.org/10.6028/NIST.SP.800-61r2

## Situation Report:

Recent contracts with the Departments of Defense and Homeland Security have imposed additional security requirements upon the company and its SCADA lab operations. The company is now required to comply with NIST Special Publication 800-171 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.* The company must also comply with provisions of the Defense Federal Acquisition Regulations (DFARS) including section 252-204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting.* These requirements are designed to ensure that sensitive technical information, provided by the federal government and stored on computer systems in the Sifers-Grayson SCADA lab, is protected from unauthorized disclosure. This information includes software designs and source code for Industrial Control Systems for which Sifers-Grayson is providing software support and maintenance. The contract requirements also mandate that Sifers-Grayson report cyber incidents to the federal government in a timely manner.

The engineering and design workstations in the Sifers-Grayson SCADA Lab were upgraded from Windows XP to Windows 8.1 professional three years ago after the lab was hit with a ransomware attack that exploited several Windows XP vulnerabilities. A second successful ransomware attack occurred three months ago. The company paid the ransom in both cases because the lab did not have file backups that it could use to recover the damaged files (in the first case) and did not have system backups that it could use to rebuild the system hard drives (in the second case).

The SCADA Lab is locked into using Windows 8.1. The planned transition to Windows 10 is on indefinite hold due to technical problems encountered during previous attempts to modify required software applications to work under the new version of the operating system. This means that an incident response and recovery capability for the lab must support the Windows 8.1 operating system and its utilities.

## Your Task

Prepare draft incident response guidance to be included in the Sifers-Grayson *Incident Responder’s Handbook*. Your draft guidance will explain the use of Windows Defender and Microsoft Baseline Security Analyzer and then describe how each could be used as part of an incident response process.

You will create two separate procedures. The first will explain how to configure and use Windows Defender to detect and analyze malware and detect, block, and analyze intrusion attempts. The second will explain how to configure and use Microsoft Baseline Security Analyzer (MBSA) to scan for vulnerabilities arising from misconfigurations of system parameters.

## Instructions

## Instructions

### Part (a): Using Windows Defender to Detect and Analyze Threats

1. Investigate the use of Windows Defender to detect and analyze potential viruses, spyware, and other forms of malware. Your investigation should include researching best practices for configuring and using the scanning, detection, and analysis capabilities for this host-based anti-malware software. At a minimum, your research should address the following
   1. Update requirements for anti-virus definition files
   2. Configuration requirements to enable real-time scanning
   3. Procedures for conducting full system scans
   4. Fast or quick scan for high vulnerability areas of the system
   5. Removable media scanning
   6. Reviewing scan results including reviewing any quarantined files or detected malware
2. Identify how the tool could be used during the incident response and recovery process (it may be useful in more than one phase). Typical uses include:
   1. Detecting malware at the point of entry to the system (e.g. in an email message or web page)
   2. Detecting intrusion attempts in real-time
   3. Analyzing files and file systems to detect and identify malware
   4. Quarantining files suspected of carrying threat payloads
   5. Deleting Infected Files
   6. Scanning removable media

### Part (b): Using Microsoft Baseline Security Analyzer (MBSA) to Detect and Analyze System Vulnerabilities

1. Investigate the use of *MBSA* to detect vulnerabilities in a Windows 8/8.1 system. As you do this, identify appropriate sources of information (e.g. Windows Help, Microsoft Technet, etc.) for instructions for configuring MBSA to scan a Windows 8/8.1 system. Using those sources, research how MBSA performs the following tasks:
   1. Scan single or multiple computer systems
   2. Check for Windows administrative vulnerabilities
   3. Check for weak passwords
   4. Check for Internet Information Services (IIS) administrative vulnerabilities
   5. Check for SQL administrative vulnerabilities
   6. Check for security updates (missing updates)
   7. Copy, save and print scan reports
2. Identify how the tool could be used during the incident response and recovery process (it may be useful in more than one phase). Typical uses include:
   1. Identify and report on recommended remediation steps for vulnerabilities
   2. Identify and report on specific vulnerabilities by CVE numbers
   3. Detect and analyze weak passwords
   4. Detect and analyze misconfigured system parameters
   5. Analyze impacts of multiple (cascading) vulnerabilities
3. Write a *guidance document* that identifies the tool, explains the capabilities it provides, and then lists and briefly describes the recommended uses identified under item #2. Add a list of resources that can be consulted for additional information. Next, summarize the procedures required to perform the tasks listed under item #1 (do not provide step-by-step instructions). Close your guidance document with a Notes / Warnings / Restrictions section that answers the question “Is there anything else the incident responder needs to be aware of when using this tool?”

### Finalize Your Deliverable

1. Using the grading rubric as a guide, refine your incident response guidance. Your final products should be suitable for inclusion in the organization’s *Incident Responder’s Handbook*.
2. As appropriate, cite your sources using footnotes or another appropriate citation style.
3. Use the *resources* section to provide information about recommended readings and any sources that you cite. Use a standard bibliographic format (you may wish to use APA since this is required in other CSIA courses). Information about sources and recommended readings, including in-text citations, should be formatted consistently and professionally.
4. Your submission file for this assignment should start with a title page which lists the following information:

* Lab Title and Number
* Date
* Your Name

1. The **CSIA 310 Template for Lab Deliverable.docx** file is set up to provide the required title page and two *incident response guidance* templates. Use the first template for your “Windows Defender” guidance. Use the second procedure template for your “MBSA” guidance.