|  |  |
| --- | --- |
|  | **I-ISMS Revision** 1 |

**NP Factory, Ltd.**

**Plant Floor**

**Industrial Information System Management System**

Guide to Windows System Monitoring

Nathan Pocock

https://our.intranet/path/to/document.docx

|  |  |
| --- | --- |
| **I-ISMS Revision** 1 (19) | **Industrial Information System Management System**  Guide to Windows System Monitoring  Editor: *Nathan Pocock*  Authors: *Nathan Pocock* |

**Monitoring**

PRIVATE

|  |  |
| --- | --- |
| 05d - Guide To Windows Monitoring.Docx  Version: 1 Revision 19  Pages: 1 | Path: C:\Users\nathan pocock\OneDrive\wgu-capstone\templates\05d - Guide to Windows Monitoring.docx  Keywords: monitor, audit, log, admin, analyze, review  Last Saved by Nathan Pocock on 9/16/2016 4:26 PM |
|  | **NP Factory, Ltd.**  [Company Address]  Plant Floor  I-ISMS  704-491-5840  Manager Pocock |

Executive Summary

A guide to preparing Windows systems for monitoring using the OSSEC tool.

Revision History

|  |  |  |
| --- | --- | --- |
| Revision | Author | Date |
| Initial creation | Nathan Pocock | 16-Sep-16 |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[1 Instructions 1](#_Toc461806748)

[2 Overview 1](#_Toc461806749)

[3 Installing OSSEC Server 1](#_Toc461806750)

[3.1 Downloads 1](#_Toc461806751)

[3.2 Installation 1](#_Toc461806752)

[4 Deploying OSSEC Agents 1](#_Toc461806753)

[4.1 Download auto-ossec 1](#_Toc461806754)

[4.2 Deploy auto-ossec to the ossec server 1](#_Toc461806755)

[4.3 Deploy auto-ossec to Windows computers 1](#_Toc461806756)

[4.3.1 Initial setup 1](#_Toc461806757)

[4.3.2 Actual deployment 1](#_Toc461806758)

[5 Monitoring Systems 1](#_Toc461806759)

[5.1 Accessing Logs 1](#_Toc461806760)

[5.2 Monitoring systems discipline 1](#_Toc461806761)

[6 Responding to Alerts 1](#_Toc461806762)

[7 Other Considerations 1](#_Toc461806763)

Figures

**No table of figures entries found.**

# 

# Instructions

This page provides quick instructions for using this guide:

1. Read the Overview to learn about OSSEC
2. Install OSSEC Server
3. Deploy OSSEC Agents
4. Learn how/when to Monitor systems for changes

Finally, delete this page.

# Overview

Each computer system on the network must be continuously monitored for unauthorized changes, such as virus infections, malware attacks, or back-doors being exploited. Systems can be monitored automatically by intrusion detection systems, such as OSSEC[[1]](#footnote-1).

OSSEC is a Server that runs on a Linux server. Agents run on the Windows computers and report changes back to the server. Personnel must monitor the server to see if any changes have occurred.

This guide will help you to install the server, deploy the agents to the Windows computers, and see how to monitor the system.

# Installing OSSEC Server

A dedicated Linux server is needed. This can be a physical or virtual computer; you decide based on the hardware you have available. This guide assumes a Linux O/S is generally available for you.

Recommendation: Download the pre-built appliance.

## Downloads

Download the following components from [http://ossec.github.io/downloads.htm](http://ossec.github.io/downloads.html):

* Either the Virtual Appliance (preferred) or the Server/Agent
* Web UI
* Agent Windows

## Installation

The Virtual Appliance is the preferred installation method. Simply open the virtualization container (VMware or VirtualBox, etc.) and then “import” the downloaded \*.OVA file. The logins are:

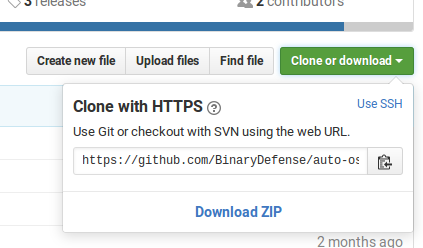
* user/\_0ssec\_
* root/\_0ssec\_

More details are available in the readme: <http://ossec.wazuh.com/vm/ossec-vm-2.8.3.README>

# Deploying OSSEC Agents

Deploying the Windows agents is not so easy. Use the “Auto-Ossec”[[2]](#footnote-2) project to help simplify the deployment process.

## Download auto-ossec

1. Go to <https://github.com/binarydefense/auto-ossec>
2. Click the green “Clone or download” button
3. Click the “Download ZIP” link:   
   
4. Save the file in an easily-accessible location, e.g. Desktop/USB stick.

## Deploy auto-ossec to the ossec server

The following instructions assume physical access to the Linux OSSEC server, whether is via the virtualization user-interface, or a remote connection:

1. Login to the OSSEC server
2. Copy the files downloaded in *Download auto-ossec*, above.
3. Follow the instructions in section “Linux Automatic Installation” on the GitHub page: <https://github.com/binarydefense/auto-ossec>

## Deploy auto-ossec to Windows computers

The following instructions will create a script that you can simply run from each Windows computer (manually) to easily install the OSSEC agent.

**Note**: if the plant-floor network is a domain and group-policies are an option, then consider using IT to help create a deployment policy to push to all computers.

### Initial setup

1. Store the Windows-based OSSEC files on an existing network share, or create a one.  
   Files include: auto\_ossec.exe and ossec-agent-win32-2.8.3.exe
2. Identify the IP-address of the share and keep a note of it.
3. Open Windows notepad and create a new file called deploy-ossec.bat and save it to the network share. Place the following text into  
      
   auto\_ossec.exe 1.2.3.4/0  
      
   Note: replace 1.2.3.4 with the actual IP-address noted in step 2.

### Actual deployment

Go to each Windows based computer and then:

1. Open Windows Explorer
2. Either, browse the network share or type it in directly into the address bar, e.g. [\\1.2.3.4\sharename\](file:///\\1.2.3.4\sharename\)
3. Right-click on the “deploy-ossec.bat” file and then choose “Run as administrator”
4. Enter the administrator credentials and click OK.

# Monitoring Systems

## Accessing Logs

To view the OSSEC logs:

1. Open a browser and go to the following URL:   
   <http://1.2.3.4/>
2. Login with the credentials specified in *Installation*, above.

## Monitoring systems discipline

The user-interface should be checked daily by two or more people.

# Responding to Alerts

Some alert notifications may be expected, such as changes to the file-system whenever windows updates occur. In that situation, since Windows update should be disabled (see [05c - Guide to Windows Hardening.docx](05c%20-%20Guide%20to%20Windows%20Hardening.docx)) this should be a cause for concern, except when somebody has manually requested Updates etc.

Unexpected alerts should be investigated.

Seek assistance from IT when additional skills/knowledge is necessary/

# Other Considerations

The monitoring solution herein does not provide 100% coverage. It does provide a significant visibility at the operating system level only. Also consider the following as part of a more holistic view of the plant-floor systems:

1. **Endpoint-protection**: consider an anti-virus/malware system that provides a centralized framework  
   Recommendation: consider Symantec Endpoint Protection deployment.
2. **Network on the wire traffic**: consider the actual traffic-patterns that a network intrusion detection system could identify.  
   Recommendation: consider purchasing a NIDS appliance or deploy the Security Onion virtual appliance in a VMWare/VirtualBox and then configure the network switch to mirror ports to the VM.
3. **Firewall**: check the logs to see where traffic is being blocked  
   Recommendation: check the firewall log frequently; better yet, configure the firewall to send logs to a centralized server such as the Security Onion recommendation.
4. **Industrial devices**: each device requires monitoring; check the manuals/vendors to see how to monitor the device’s log activities.  
   Recommendation: if possible, forward the logs to a centralized server; if not possible then create a batch file script that will automatically open a browser URL to an appropriate log; repeat for other logs. For example, consider this batch file:   
   @echo off  
   iexplore http://device1/  
   iexplore https://device2:port/  
   iexplore <https://device3:port/path/to/file.html>  
   The execution of the above script forces the user to see the device’s log and close it, before seeing the next, and the next, and so on. It would be advisable to put this batch file into the STARTUP folder of the Windows START menu.

1. http://ossec.github.io/index.html [↑](#footnote-ref-1)
2. https://github.com/binarydefense/auto-ossec [↑](#footnote-ref-2)