**Implementatieplan**

Project SecMon

Opdrachtgever: Arnim Eijkhoudt

Project: Project SecMon

Auteur: Christiaan Druif

Datum: 30 juni 2014

Versie: 0.3

Status: Final

# Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| Versie | Datum | Omschrijving | Auteur |
| 0.1 | 23-06-2014 | Concept versie | Christiaan Druif |
| 0.2 | 24-06-2014 | Concept versie | Christiaan Druif |
| 0.3 | 30-06-2014 | Final versie | Christiaan Druif |

Table of Contents

[Versiebeheer 2](#_Toc392098426)

[1. Inleiding 4](#_Toc392098427)

[2. De applicatie 5](#_Toc392098428)

[3. Requirements 6](#_Toc392098429)

[4. Installatie Linux distributie 7](#_Toc392098430)

[5. Installatie van SecMon 8](#_Toc392098431)

[6. De productieomgeving 9](#_Toc392098432)

[6.1. Situatie 1: Monitor Systeem 9](#_Toc392098433)

[6.1.1. Voordelen 9](#_Toc392098434)

[6.1.2. Nadelen 9](#_Toc392098435)

[6.2. Situatie 2: Op een router 10](#_Toc392098436)

[6.2.1. Voordelen 10](#_Toc392098437)

[6.2.2. Nadelen 10](#_Toc392098438)

# Inleiding

Dit document bevat het implementatieplan voor het project SecMon. Het document heeft als doel om aan de hand van stappen uit te leggen hoe de applicatie geheel functionerend op een Linux distributie geïnstalleerd kan worden. Tevens worden de voor- en nadelen van de applicatie benoemd voor de situaties waarin de applicatie gebruikt kan worden.

# De applicatie

De applicatie SecMon is een logfile parser waarbij gebruik wordt gemaakt van rule bestanden om de verschillende logfiles te parsen. De applicatie kan verschillende soorten logfiles gebruiken waaronder logfiles van iptables en o.a. van de Apache webserver. Aan de hand van de inhoud van de verschillende rule bestanden worden logfiles geparsed aan de hand van een gecreëerde reguliere expressie (regex). Deze regex wordt gebruikt om de logfiles te parsen, en als er een match optreedt, zal er een trigger plaatsvinden waarbij er één of meerdere automatische acties uitgevoerd kunnen worden. De hoeveelheid matches die moeten plaatsvinden voor een trigger is afhankelijk van de inhoud van het rule bestand.

De applicatie kan gebruikt worden op elke Linux distributie, dit komt in de requirements verder aan bod.

# Requirements

Onderstaand de requirements nodig voor de applicatie SecMon op een Linux distributie.

Er wordt onderscheidt gemaakt in de requirements voor en zonder web interface. De web interface is namelijk een optioneel. De applicatie werkt ook zonder web interface.

**Zonder web interface:**

* Een Linux Distributie
* Python 2.7

**Met web interface:**

* Een Linux distributie
* Python 2.7
* Web server (Apache, Nginx)

**Waarom zijn deze requirements nodig?**

**Linux Distributie:**

De applicatie moet op een besturingssysteem werken en is geprogrammeerd voor Linux. De applicatie is een manier geprogrammeerd dat het niet afhankelijk is van externe modules en is daardoor bruikbaar op een kale Linux distributie met Python 2.7 geïnstalleerd.

**Python 2.7**

Om de applicatie uit te voeren is er een Python interpreter nodig. De applicatie is geschreven zodat het optimaal werkt in Python 2.7. Deze versie van Python is gratis te downloaden van de officiële website van Python.

**Web server (Apache, Nginx)**

De web interface wordt op een webserver gehost. Het maakt in principe niet uit op welke webserver de web interface draait, zolang er ondersteuning is voor PHP. Apache en Nginx zijn voorbeelden van webserver waarop de web interface gehost kan worden, maar is geen verplichting.

# Installatie Linux distributie

Voordat de applicatie op een besturingssysteem kan draaien, moet er allereest een besturingssysteem geïnstalleerd worden. In dit hoofdstuk komt aan bod hoe een Linux distributie geïnstalleerd kan worden.

Er zijn verschillende Linux distributies beschikbaar waarop de applicatie kan functioneren. De applicatie werkt op een kaal systeem met Python 2.7 geïnstalleerd. In principe zou de applicatie dus op de meeste Linux distributies moeten werken.

Voor de installaties van een kale Linux distributie wil ik u graag verwijzen naar de officiële sites van de Linux Distributies, waar altijd een handleiding te vinden is van de installatie. Onderstaand een aantal handleiding van populaire Linux distributies:

**Ubuntu Server Edition:**

<http://www.ubuntu.com/download/server/install-ubuntu-server>

**Red Hat Enterprise 6:**

<https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Installation_Guide/Red_Hat_Enterprise_Linux-6-Installation_Guide-en-US.pdf>

**Gentoo:**

<https://www.gentoo.org/doc/en/handbook/handbook-x86.xml?part=1>

**Debian:**

<http://www.debian.org/releases/wheezy/i386/ch05.html.en>

De reden dat bovenstaand links zijn geplaatst naar de officiële handleiding van de betreffende Linux distributies is omdat de applicatie SecMon niet afhankelijk is van een specifieke distributie. Daarnaast is het alleen nodig om een kale Linux distributie te installeren en dat wordt uitgebreid en gedetailleerd beschreven in de officiële handleiding van de verschillende distributies.

# Installatie van SecMon

Onderstaand de installatie van de applicatie SecMon op een Linux systeem.

**Stap 1:**

Voor de applicatie SecMon is Python 2.7 nodig, deze moet geïnstalleerd worden. Dit is tevens de enige applicatie nodig voor het goed functioneren van SecMon, tenzij er ook gebruikt wordt gemaakt van de web interface. Dan is er een webserver nodig (bijvoorbeeld Apache of Nginx) en daarbij een PHP module.

**Stap 2:**

Download Python 2.7 op [www.python.org/ftp/python/2.7.6/Python-2.7.6.tgz](http://www.python.org/ftp/python/2.7.6/Python-2.7.6.tgz)

**Stap 3:**

Installeer de 2.7 versie van Python met behulp van de package manager van de gekozen distributie.

**Stap 4:**

Zet de applicatie op de server, dit kan doormiddel van een git clone of via (s)ftp.

**Stap 5:**

Kopieer de inhoud van de src map (de mappen core en custom) naar een map op het bestandssysteem. Dit kan bijvoorbeeld /var/secmon zijn.

**Stap 6:**

De applicatie kan nu gebruikt worden. Wel moet de applicatie nog geconfigureerd worden. Dit wordt in de handleiding beschreven.

# De productieomgeving

De applicatie kan op meerdere machines in een productieomgeving functioneren. Situatie één beschrijft de situatie waarin de applicatie op een apart systeem draait, waarin het aparte systeem functioneert als monitor systeem. De tweede situatie beschrijft de situatie waarin de applicatie draait op de router. De logs van het verkeer kunnen dan op hetzelfde systeem geparsed worden i.p.v. een ander systeem. De voor- en nadelen van beide omgevingen zullen beschreven worden.

## Situatie 1: Monitor Systeem

Het installeren van de applicatie SecMon betekent dat de applicatie op een apart systeem geïnstalleerd wordt. Dit zal waarschijnlijk op een virtuele machine gebeuren, maar kan ook op een fysiek systeem. De opzet is als volgt, de router waar het verkeer in het netwerk binnenkomt, logt het verkeer. Deze logfiles worden uitgelezen of doorgestuurd naar de SecMon applicatie op het andere systeem. De applicatie zal op basis van de inhoud van de logfile een actie ondernemen.

### Voordelen

De voordelen van de bovenstaand beschreven situatie zijn:

* Afhankelijk van andere processen die draaien op de machine, zullen er mogelijk meer resources beschikbaar zijn voor de applicatie.
* De applicatie draait op een minder kritische omgeving, wat de beheersbaarheid enigszins verhoogt.

### Nadelen

De nadelen van de bovenstaand beschreven situatie zijn:

* Er is constant verkeer tussen de router en het aparte systeem. Dit verhoogt het netwerkverkeer.
* Afhankelijk van de netwerksnelheid van de omgeving.

## Situatie 2: Op een router

Het installeren van de applicatie SecMon op de router waar het verkeer naar toe gaat is ook een optie. Net als bij de situatie van de applicatie op een ander systeem, heeft ook deze situatie voor-en nadelen. Deze zijn onderstaand beschreven. Het verkeer naar de router toe wordt gelogd in een logfile. De logfile kan uitgelezen worden door de applicatie en kan een actie uitvoeren indien nodig.

### Voordelen

De voordelen van de bovenstaand beschreven situatie zijn:

* Niet afhankelijk van het doorsturen van informatie vanuit andere systemen.
* Op deze manier wordt er geen extra netwerkverkeer gegenereerd.

### Nadelen

De nadelen van de bovenstaand beschreven situatie zijn:

* Mogelijk heeft de applicatie SecMon effect op de beschikbaarheid van resources waardoor er minder resources beschikbaar zijn voor de routing functionaliteiten.