

31-5-2024

Versie: 1.0

# Technisch Ontwerp

## Projectgroep

ICTAISc

## Docent

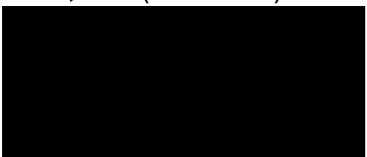


## School en Opleiding

Windesheim Zwolle HBO-ICT Software Engineering, Business IT Management & Infrastructure Design & Security

## Student

Bark, Ivan (s1169347)



Geen vertrouwelijke behandeling gewenst.

## Versiebeheer

Versie	Datum	Omschrijving	Opmerkingen
0.1	23-4-2024	Eerste opzet	N.v.t.
0.5	6-5-2024	Uitwerking tools	N.v.t.
1.0	16-5-2024	Afronding	N.v.t.

## Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
	Docent	1.0	31-05-2024	Oplevering

## Inhoudsopgave

1. Inleiding .....	3
2. Machines.....	4
2.1. Skylab .....	4
2.2. SIEM .....	4
2.2.1. Splunk.....	4
2.2.2. LogRythm .....	4
2.2.3. Trellix .....	5
2.2.4. Wazuh .....	5
2.3. Pfsense .....	5
2.4. Metasploitable .....	6
3. SIEM.....	7
3.1. Wazuh.....	7
3.1.1. Agent.....	7
3.1.2. Server (cluster) .....	7
3.1.3. Indexer .....	8
3.1.4. Dashboard .....	8
3.1.5. Implementatie .....	8
3.2. Instellingen .....	9
3.2.1. Policy monitoring (NIET) .....	9
3.2.2. OSquery (NIET) .....	9
3.2.3. System inventory (WEL).....	9
3.2.4. Vulnerability detector (WEL).....	9
3.2.5. File integrity monitoring (WEL) .....	9
4. Bibliografie .....	10

## 1. Inleiding

---

Winfra vital verzorgt de levering van gas en elektriciteit aan klanten in Noordwest Overijssel. De infrastructuur van Winfra vital wordt gezien als een vitale infrastructuur dat met uitval grootschalige maatschappelijke ontwrichting kan veroorzaken, hierdoor is het van belang dat de veiligheid hiervan nauwlettend in de gaten wordt gehouden.

Inlichtingendiensten hebben gewaarschuwd dat vitale infrastructuren steeds meer aandacht krijgt van overheidsactoren. Deze actoren zijn instaat om niet alleen de technische zwakheden te verkennen, maar richten zich ook op kantoorautomatisering en het personeel. Door een snelle digitalisering van deze sector is een structurele aanpak van cybersecurity vereist namelijk: security by design.

Dit document dient als technisch ontwerp. In het document wordt onze inrichting toegelicht. Er zal worden ingegaan op de gebruikte machines en op de opbouw en structuur van de SIEM.

## 2. Machines

---

In dit hoofdstuk wordt geschreven welke machines worden toegepast. Er wordt een toelichting gegeven van elke machine en voor welke reden elke machine word toegepast.

### 2.1. Skylab

Skylab is een omgeving welke kan worden ingezet om meerdere virtuele machines in te stellen en tegelijkertijd te laten draaien. In deze omgeving kunnen alle machines uit dit hoofdstuk worden toegepast. De huidige omgeving waarin wordt gewerkt is in het beheer van Windesheim. De servers die worden gebruikt in Skylab zijn van het bedrijf VMWare.

### 2.2. SIEM

SIEM, oftewel Security Information en Event Management, word took toegepast. De SIEM zal draaien op een Skylab VMWare server met Ubuntu Desktop 22.04. Ubuntu is voor gekozen, vanwege de uitgebreide support, documentatie en het hoge aantal gebruikers. Verder is het een sterke en gemakkelijk te gebruiken desktop omgeving.

Voor het daadwerkelijk instellen van de SIEM zijn er meerdere opties en meerdere aanbieders. Mogelijke aanbieders zijn: Splunk Enterprise Secury, LogRythm SIEM, Trellix Enterprise Security Manager en Wazuh. (Gartner, n.d.)

De verschillende opties en aanbieders zullen hieronder verder worden toegelicht.

#### 2.2.1. Splunk

Splunk is een van de grootste aanbieders van SIEM implementaties. Ze zijn voornamelijk gefocust op efficiëntie, en snelheid van het detecteren van bedreigingen. Een paar van hun klanten zijn: Heineken, Lenovo, Puma en Bosch. (Splunk, n.d.)

Een voordeel van Splunk is dat het geavanceerde capaciteiten heeft voor real-time threat detection en snelle respons, dit komt door de continue monitoring en notificatie functionaliteit. Daarnaast heeft het features voor user-based activity tracking, risk scoring en uitgebreide data analytics, deze features geven IT-professionals de mogelijkheid om beveiligings dreigingen snel te identificeren en geeft het de mogelijkheid om uitgebreide forensische data in te zien. (SubRosa, n.d.)

#### 2.2.2. LogRythm

LogRhythm is een SIEM-product voor zakelijk gebruik. Het wordt ingezet om beveiligingsloggegevens te verzamelen van software binnen een organisatie, waaronder netwerkbeveiligingscontroles, besturingssystemen en gebruikersapplicaties. Dit SIEM-tool analyseert de data om mogelijke tekenen van kwaadaardige activiteiten te identificeren, zodat menselijke of geautomatiseerde processen aanvallen in uitvoering kunnen stoppen of kunnen helpen bij het herstel van succesvolle aanvallen. SIEM-platformen zoals die van LogRhythm genereren ook gedetailleerde rapporten over beveiligingsincidenten, die gebruikt kunnen worden om naleving van beveiligingsvoorschriften, wetten en andere vereisten te documenteren. (Scarfone, 2015)

### 2.2.3. Trellix

Trellix Enterprise Security Manager is een uitgebreide SIEM-oplossing die ontworpen is om beveiligingsoperaties te verbeteren door middel van realtime monitoring, snelle dreigingsdetectie en geautomatiseerde respons. Belangrijke kenmerken zijn:

- **Geavanceerde Dreigingsdetectie:** Identificeert en reageert in realtime op complexe bedreigingen.
- **Integratie en Datacorrelatie:** Verzamelt en verrijkt gegevens uit verschillende bronnen voor uitgebreide analyse.
- **Geautomatiseerde Naleving:** Vereenvoudigt naleving met geautomatiseerde monitoring en rapportage.
- **Schaalbare Architectuur:** Ondersteunt grootschalige dataverwerking voor grote ondernemingen.

(Trellix, n.d.)

### 2.2.4. Wazuh

Voor het te implementeren SIEM is besloten om de Wazuh open-source security platform toe te passen.

Wazuh is een gratis en open source SIEM-platform dat it-infrastructuur bewaakt, verdachte activiteiten detecteert en helpt bij beveiligingsincidenten. Wazuh stelt de gebruikers in staat om aan de hand van dashboards en visualisaties snel inzicht te krijgen in de huidige beveiligingsstatus. Het biedt ook meerdere functies zoals log- en eventbeheer, vulnerability detection, security configuration assessment (SCA) en vereenvoudigt het bijhouden en demonstren van regelnaleving op frameworks zoals PCI DSS, NIST 800-53, GDPR, TSC SOC2 en HIPAA. (Wazuh, n.d.)

Wazuh is gekozen vanwege zijn open-source karakter, real-time dreigingsdetectie, brede beveiligingsfuncties en eenvoudige integratie, daarnaast is ervoor gekozen wegens eisen vanuit de opdrachtgever. Het dient als volledige oplossing voor het beveiligen van onze netbeheerder IT-infrastructuur en geeft directe waarschuwingen voor potentiële bedreigingen. (Wazuh, n.d.)

Wazuh wordt verder toegelicht in het volgende hoofdstuk.

## 2.3. Pfsense

pfSense is een open-source firewall- en routerplatform dat veel wordt gebruikt in netwerken vanwege zijn robuuste beveiligingsmogelijkheden en flexibiliteit. Het biedt uitgebreide functionaliteiten zoals verkeersfiltering, VPN-ondersteuning, en netwerkmonitoring. Door de open-source aard is pfSense kosteneffectief en wordt het continu verbeterd door een actieve community.

Het platform is zeer geschikt voor zowel kleine bedrijven als grote ondernemingen vanwege de schaalbaarheid en de brede compatibiliteit met verschillende netwerkhardware. Het wordt toegepast om netwerken te beschermen tegen ongeautoriseerde toegang en om een veilige en betrouwbare netwerkarchitectuur te waarborgen. Dankzij de uitgebreide functies en de hoge mate van aanpasbaarheid, wordt pfSense vaak gekozen voor complexe netwerkbehoeften binnen de ICT-sector. (Baselier, n.d.)

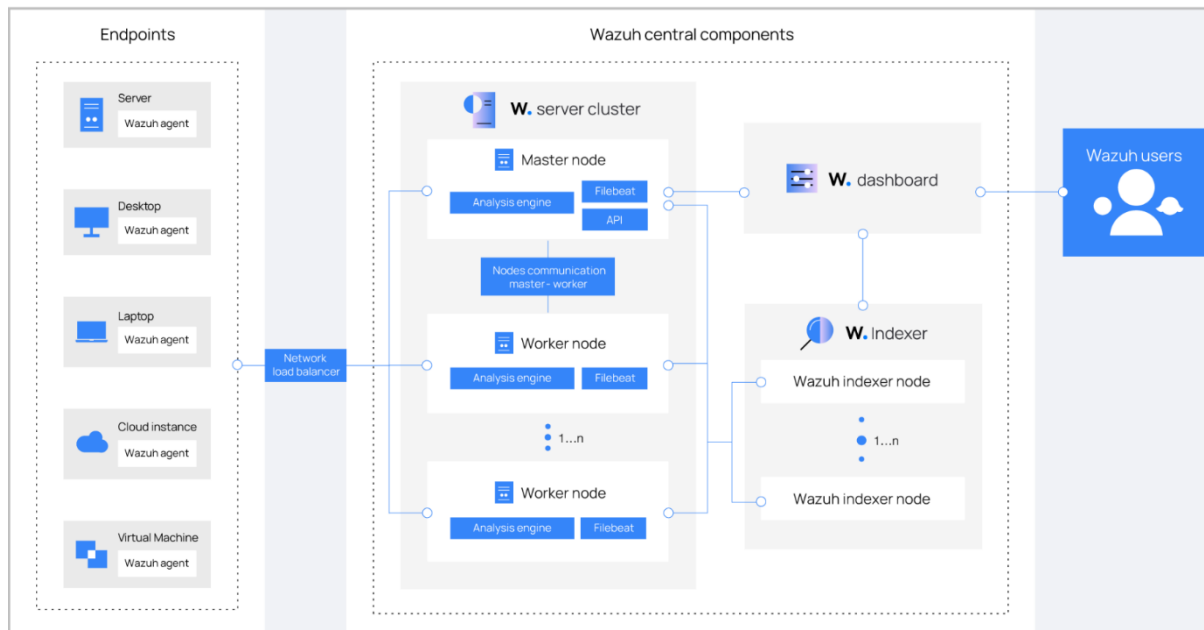
## 2.4. Metasploitable

Metasploitable is een virtuele machine speciaal ontworpen voor veiligheidstesten. Specifiek voor het testen en oefenen van pentesten en kwetsbaarsheidscans. Oorspronkelijk gemaakt door rapid7, dezelfde ontwikkelaars van de populaire penetratietesttool metasploit. Metasploitable is een oefenomgeving (virtuele machine) met veel intentionele kwetsbaarheden. Zo kunnen gebruikers praktijkervaring opdoen zonder echte systemen in gevaar te brengen.

De virtuele machine is gebaseerd op Ubuntu Linux en bevat zoals eerder benoemd opzettelijk verschillende kwetsbaarheden zoals: verouderde software, slechte wachtwoorden, etc. hierdoor dient het als uitstekend hulpmiddel voor de projectgroep om vaardigheden te ontwikkelen.

## 3. SIEM

### 3.1. Wazuh



Figuur 3.1: Schematische weergave Wazuh (Wazuh, n.d.)

Wazuh is een open-source implementatie van een SIEM. Het bestaat uit vier onderdelen: De Agent, Server, Indexer en de Dashboard. Elk individueel onderdeel wordt hieronder uitgelegd en is hierboven gevisualiseerd.

#### 3.1.1. Agent

De Wazuh Agent is de scanner van de SIEM. Elke agent binnen de organisatie behoort op elk individueel machine geïnstalleerd te worden. Deze machines worden ook wel Endpoints genoemd. Elke agent verbindt hiermee met de voor hen aangegeven server

#### 3.1.2. Server (cluster)

De Wazuh Server is het centrale onderdeel van de SIEM. De server verzamelt en beheert al het verkeer en de verbindingen tussen elk onderdeel. Wanneer het aantal machines te groot is, kan de server opgesplitst worden in meerdere kleinere sub-servers. Al deze sub-servers worden dan weer verbonden met een centrale server. Deze centrale server wordt dan de Cluster genoemd.



### **3.1.3. Indexer**

De Indexer analyseert en evalueert alle data welke de Agents versturen. De Indexer is 1 op 1 verbonden met de server. Elke server heeft dus ook maar 1 Indexer, mits de server fungeert als Cluster.

### **3.1.4. Dashboard**

De dashboard visualiseert alle bevindingen en analyses die de Agents, Servers en Indexers maken. Per netwerk is maar 1 dashboard. Deze is verbonden ofwel met de enkelvoudige Server, of de centrale Cluster. In de dashboard staan alle verbonden Agents en hun instellingen weergegeven. Sommige instelling zijn ook aan te passen in de dashboard. Alle instellingen staan op de Server zelf.

### **3.1.5. Implementatie**

De Server, Indexer en Dashboard staan allemaal op dezelfde machine: Een Ubuntu 22.04 Desktop Virtuele Machine met 4 CPU cores en 8GB RAM op 192.168.1.104. Er is gekozen om de Wazuh te installeren op de Ubuntu 22.04 Desktop machine want voor het installeren behoren veel lange commando's uitgevoerd te worden. Deze zijn alleen te kopiëren van binnenin de machine zelf. Daarom was het nodig om Wazuh te installeren op een machine met een webbrowser, om zo de commando's te kopiëren en te plakken.

De agent is geïnstalleerd op de enige aanwezige machine: Een Metasploitable3 Windows Virtuele Machine draaiende op 192.168.1.106.

## 3.2. Instellingen

### 3.2.1. Policy monitoring (NIET)

Policy monitoring checkt of machines & applicaties voldaan aan voor gedefinieerde set van regels. Onder deze instelling behoort ook de SCA (Security Configuration Assessment) welke controleert of iedere service de juiste configuratie heeft. Policy monitoring is alleen nodig voor de 'Securityconsultant' om best practices te implementeren. We focussen ons nu voornamelijk op het monitoren en analyseren van events voor eventuele hacks. Wanneer de SIEM goed voldoet aan die basis criteria, moet gekeken worden naar deze instelling. Het heeft voor ons een te lage prioriteit om tijd te stoppen in het zoeken en toepassen van deze configuratie regels.

### 3.2.2. OSquery (NIET)

Voor deze instelling is de open-source package nodig genaamd OSquery. Dit zet een besturingssysteem om tot een krachtige relationele database. Deze database kan dan verkent worden met SQL functies. Deze instelling is erg handig voor het snel verkennen van het systeem en alle draaiende processen.

Om deze functionaliteit toe te voegen aan de Wazuh gaat wel veel geschatte tijd kosten welke we niet hebben. Deze functionaliteit word ook al grotendeels vervuld door de 'System inventory' & 'Vulnerability detector' instellingen. Voor nu laten we dus deze instelling uit. Wanneer meer tijd over is kan gekeken worden naar het instellen van OSquery.

### 3.2.3. System inventory (WEL)

Met system inventory scant de Agent automatisch wat voor services & applicaties er allemaal draaien op de machine. Hierdoor wordt in kaart gebracht welke software waar draait. Deze informatie helpt met het uitvoeren van de taken van actoren 'Vulnerability manager' & 'Security architect'

### 3.2.4. Vulnerability detector (WEL)

De vulnerability detector schept nog wat bovenop de system inventory instelling. Het evalueert en detecteert kwetsbaarheden in applicaties en operatie systemen. Deze worden weergegeven en evalueert aan de hand van CVE (Common Vulnerabilities and Exposures) score. Hierdoor word ook meteen duidelijk welke kwetsbaarheden aanwezig zijn op de machine en welke CVE daarbij hoort. Hierdoor kan de kwetsbaarheid gemakkelijk geïdentificeerd en gepatched worden. Ook deze setting helpt de actoren 'Vulnerability manager' & 'Security architect' met het uitvoeren van hun taken.

### 3.2.5. File integrity monitoring (WEL)

Deze instelling scant en analyseert cruciale bestanden om te controleren of ze nog steeds legitiem zijn. Het fungeert hiermee als een soort van antivirus welke in observatie modus staat. Deze instelling helpt ons met het nog beter scannen en monitoren van de machine.

## 4. Bibliografie

---

- Baselier, J. (sd). *PfSense – Open-Source Firewall*. Opgehaald van <https://jarnobaselier.nl/pfsense-open-source-firewall/>
- Gartner. (sd). *Security Information and Event Management (SIEM) Reviews and Ratings*. Opgehaald van Gartner: <https://www.gartner.com/reviews/market/security-information-event-management>
- Scarfone, K. (2015, November 18). *LogRhythm's Security Intelligence Platform: SIEM product overview*. Opgehaald van TechTarget: <https://www.techtarget.com/searchsecurity/feature/LogRhythms-Security-Intelligence-Platform-SIEM-product-overview>
- Splunk. (sd). *Splunk Enterprise Security*. Opgehaald van Splunk: [https://www.splunk.com/en\\_us/products/enterprise-security.html](https://www.splunk.com/en_us/products/enterprise-security.html)
- SubRosa. (sd). *Maximizing Cybersecurity: A Comprehensive Guide to Using Splunk as a SIEM*. Opgehaald van Subrosacyber: <https://www.subrosacyber.com/blog/using-splunk-as-a-siem>
- Trellix. (sd). *Trellix Enterprise Security Manager*. Opgehaald van Trellix: <https://www.trellix.com/products/enterprise-security-manager/>
- Wazuh. (sd). *Architecture*. Opgehaald van Wazuh: <https://documentation.wazuh.com/current/getting-started/architecture.html>
- Wazuh. (sd). *The Open Source Security Platform*. Opgehaald van Wazuh: <https://wazuh.com/>