



PROJECTPLAN

Deis, Sekariya S.

2 maart 2025

Versiebeheer

Versienummer	Datum	Auteur	Veranderingen
<0.1>	<02/03>	<Sekariya>	<Opbouwing document>
<0.2>	<02/03>	<Sekariya>	<Inhoud bijgevuld>
<0.3>	<17/03>	<Sekariya>	<Feedback verwerkt>

Inhoudsopgave

Introductie.....	3
Relevantie.....	3
Belanghebbenden	3
Communicatie	3
Deadline	3
Projectopdracht	4
Opdracht	4
Doelstelling	4
Scope.....	4
Randvoorwaarden.....	4
Onderzoeksvragen	5
Eindproducten.....	6
Project-aanpak en planning	7
Aanpak	7
Planning	8
Leeruitkomsten	8
Communicatieplan	9
Project risico's	10

Introductie

In de huidige digitale wereld is het essentieel om IT-infrastructuren continu te monitoren en proactief te beheren. Problemen zoals prestatieverlies, netwerkbedreigingen en systeemstoringen kunnen aanzienlijke gevolgen hebben voor bedrijven en gebruikers. Traditionele monitoringtools bieden vaak reactieve oplossingen, wat betekent dat problemen pas worden aangepakt zodra ze zich voordoen.

In dit project wordt een AI-gestuurde infrastructuurmonitoring ontwikkeld om proactief beheer mogelijk te maken. Door gebruik te maken van geavanceerde monitoringtools, wordt een uitgebreide monitoringomgeving gecreëerd.

Relevantie

Dit project is relevant voor bedrijfs infrastructuur omdat het een AI-gestuurde monitoringoplossing biedt die helpt bij proactief beheer, schaalbaarheid en beveiliging binnen een omgeving. Grote organisaties hebben complexe IT-systemen die continu moeten worden bewaakt om prestatieproblemen en beveiligingsdreigingen te voorkomen. Door het combineren van verschillende monitoring-systemen met AI-analyse, biedt dit project inzichten, voorspellingen en geautomatiseerde incidentdetectie, wat stilstand vermindert, kosten bespaart en naleving ondersteunt.

Belanghebbenden

De belanghebbenden in dit project zijn met name de docenten die betrokken zijn bij dit project.

Communicatie

Tijdens deze onderzoeksstage zal de communicatie plaatsvinden via verschillende kanalen:

- Persoonlijke ontmoetingen
- Microsoft Teams voor online vergaderingen.
- E-mail voor formele berichten en afspraken.

Deadline

De deadline is op 22 Juni 2025

Projectopdracht

Dit project draait om het bouwen van een slimme monitoringoplossing voor IT-infrastructuren, die niet alleen real-time data verzamelt, maar ook voorspellingen kan doen en slimme inzichten kan bieden. Door gebruik te maken van verschillende tools, wordt een systeem opgezet dat problemen signaleert voordat ze echte schade aanrichten.

Opdracht

Het doel van dit project is het opzetten van een AI-gestuurde monitoringomgeving die continu IT-systemen analyseert en problemen proactief aanpakt. Dit gebeurt door een combinatie van verschillende monitoringtools, en een overzichtelijk dashboard dat direct inzicht geeft in de status van de infrastructuur.

Doelstelling

Het implementeren van een monitoringsysteem

- IT-systemen in real-time monitort en analyseert.
- Anomalieën herkent en mogelijke problemen voorspelt.
- Beveiligingsbedreigingen detecteert en rapporteert/meldt.
- Flexibel en schaalbaar is binnen een Kubernetes-omgeving.

Scope

Deze sectie beschrijft de grenzen en focus van het onderzoek. Het definieert wat er wordt onderzocht, welke aspecten worden bestudeerd, en waar de grenzen liggen van het onderzoeksveld.

Tot het project behoort:	Tot het project behoort niet:
Implementatie van een monitoringsysteem.	Monitoring van applicatiespecifieke prestaties buiten de infrastructuur.
Integratie van AI om voorspellingen en automatische samenvattingen te maken.	Het bouwen van een volledig op maat gemaakte AI-oplossing.
Focus op zowel prestatie-monitoring als beveiliging.	

Randvoorwaarden

De randvoorwaarden voor het project omvatten technische, organisatorische en tijdsgebonden beperkingen die van invloed zijn op de uitvoering en het eindresultaat.

- 1. Technologische beperkingen:**
 - Alleen open-source tools en frameworks worden gebruikt.
- 2. Organisatorische beperkingen:**
 - Het project moet haalbaar zijn binnen de gestelde tijd.
 - De oplossing moet eenvoudig te begrijpen en te beheren zijn.
- 3. Beveiligingsbeperkingen:**
 - Er moet rekening worden gehouden met best practices voor cybersecurity.
 - De oplossing moet voldoen aan basis GDPR- en compliance-vereisten.

Onderzoeksvragen

De onderzoeksvragen vormen de kern van het project en zijn gericht op het vinden van een passende oplossing voor het project.

Hoofdvraag:

"Hoe kan een AI-gestuurd monitoringsysteem het beheer van IT-infrastructuur verbeteren en welke technologieën bieden de beste combinatie van prestaties, beveiliging en schaalbaarheid?"

Deelvragen:

1. Welke methoden en technieken zijn het meest geschikt voor het voorspellen van systeemfouten en dreigingen?
2. Hoe kan AI worden ingezet om automatisch rapporten en waarschuwingen te genereren op basis van verzamelde gegevens?
3. Welke uitdagingen spelen een rol bij de implementatie van beveiligings- en monitoringoplossingen in een dynamische IT-omgeving?
4. Wat zijn de voordelen en nadelen van het combineren van verschillende monitoring- en beveiligingstechnieken binnen één infrastructuur?

Onderzoeksmethoden:

Binnen het project wordt gebruikgemaakt van verschillende onderzoeksmethoden om relevante informatie te verzamelen en tot onderbouwde conclusies te komen. De volgorde van deze methoden wordt aangehouden op basis van de deelvragen hierboven.

Methode	Context	Deelvraag
Available product analysis	Identificeer bestaande oplossingen die het probleem (of een deel daarvan) dat u met uw oplossing probeert op te lossen, kunnen oplossen.	<u>1</u>
Literatuuronderzoek	Maak een zoekplan en identificeer relevante trefwoorden. Materiaal zoeken en beoordelen. Binnen de bronnen.	<u>2</u>
Community research	Zoek naar het probleem waarmee u worstelt in een online community waarvan u weet dat u deze kunt vertrouwen.	<u>3</u>
Best good and bad practices	Organiseer activiteiten gericht op het delen van ervaringen. Afhankelijk van uw onderwerp zijn er mogelijk veel beste, goede en slechte praktijken beschikbaar.	<u>4</u>

Eindproducten

Hier een overzicht van de te leveren producten en hun corresponderende bestandstypen.

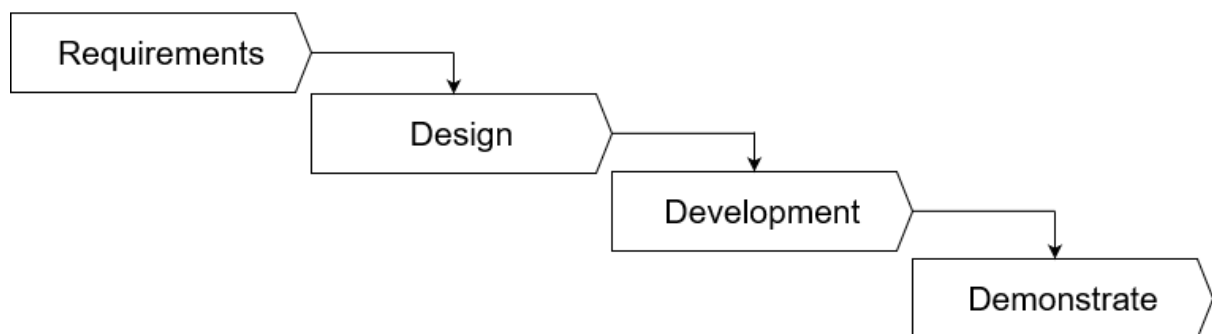
Te Leveren	Inhoud	Type
Projectplan	Een gedetailleerd plan voor de uitvoering van het project.	.PDF
Onderzoeksdocument	Een onderzoeksdocument gebaseerd op de DOT-methode voor het analyseren van problemen.	.PDF
Proof of Concept	Om een van de mogelijke oplossingen in de praktijk te testen en te evalueren.	.PDF
Adviesrapport	Een uitgebreid rapport met aanbevelingen gebaseerd op de onderzoeksresultaten.	.PDF
Presentatie	Een presentatie van de belangrijkste bevindingen en conclusies.	.PPTX

Project-aanpak en planning

Aanpak

Voor dit project wordt de **Waterval-methode** gevolgd. Deze gestructureerde aanpak helpt bij het systematisch doorlopen van het project in opeenvolgende fasen, van probleemdefinitie tot evaluatie, zonder onderhoudsfases.

Waterval-methode



Fase 1: Requirements (Analyse)

- Onderzoek doen naar het huidige systeem en vereisten voor de implementatie van Netdata, Wazuh en Suricata binnen een Kubernetes-cluster.

Fase 2: Design (Ontwerp)

- Zoeken naar en evalueren van mogelijke architecturen voor de integratie van Netdata, Wazuh en Suricata.

Fase 3: Development (Implementatie)

- Ontwikkeling en testen van een Proof of Concept.

Fase 4: Demonstrate (Presenteren)

- Presenteer het project aan belanghebbenden, verzamel feedback.

Waarom waterval-methode?

Voor dit project is de Waterval-methode gekozen omdat deze goed past bij de verwachte opleveringen en een duidelijke opbouw heeft. De methode werkt stap voor stap, waarbij elke stap helemaal wordt afgerond voordat de volgende begint. Dit zorgt voor een goed overzicht van de voortgang en maakt het makkelijker om de planning aan te houden.

Bij het kiezen van een aanpak is ook gekeken naar andere manieren van werken, zoals Scrum en Kanban. Deze methodes zijn flexibeler en werken met tussentijdse aanpassingen, maar dat is voor dit project minder handig. De resultaten die opgeleverd moeten worden, liggen namelijk vooraf vast en hoeven niet steeds aangepast te worden. Daarnaast vraagt een flexibele aanpak om veel overleggen en veranderingen, wat minder goed past bij de gestructureerde en technische inhoud van dit project. Daarom is gekozen voor de Waterval-methode, omdat deze de beste balans biedt tussen planning, duidelijkheid en uitvoering.

Planning

De planning geeft een overzicht van de verschillende fases en mijlpalen binnen het project, van de start op 02 maart 2025 tot de oplevering op 22 juni 2025. Gedurende deze periode worden belangrijke producten opgeleverd.

Fase	Taak	Startdatum	Einddatum	Duur
Initiatie	Eerste concept projectplan	02-maart-2025	02-maart-2025	1 dag
	Finaliseren van projectplan	10-maart-2025	14-maart-2025	5 dagen
Onderzoeksfase	Onderzoeksdocument opstellen	17-maart-2025	11-april-2025	4 weken
Ontwerpfase	Proof of Concept ontwikkelen	21-april-2025	01-juni-2025	6 weken
Adviesfase	Adviesrapport opstellen	02-juni-2025	06-juni-2025	1 week

Leeruitkomsten

In deze sectie worden de leeruitkomsten van het project beschreven. De leeruitkomsten geven aan welke vaardigheden, kennis en competenties tijdens het project worden ontwikkeld en aangetoond.

Leeruitkomsten	Criteria
LO1: Analytics for Enterprise Infrastructure	You can collect data from various stakeholders / interest groups in a methodical way to arrive at requirements for the design of an enterprise infrastructure.
LO2: Architecture of Enterprise Infrastructure	You can methodically translate the requirements for an enterprise infrastructure into different alternatives for an infrastructure design and justify these alternatives with clear advantages and disadvantages.
LO3: Realization of Enterprise Infrastructure	You can realize an enterprise infrastructure in a methodical way and demonstrate with an extensive test report and demos that the infrastructure meets the specifications drawn up.
LO4: Setting up management for Enterprise Infrastructure	In a methodical manner, you can proactively manage enterprise infrastructure by designing, testing, and demonstrating its capabilities through monitoring incidents and events to ensure effective handling.
LO5: Innovations and Trends	You have insight into innovations/trends for the infrastructure and/or the management of the infrastructure and you can research these innovations in a

	methodical way, report on them and indicate what the innovation/trend will mean for existing enterprise infrastructures.
LO6: Professional Standard	You conduct work in accordance with an industry supported methodological approach in terms of your project's goals, stakeholder involvement, applied research, advising, decision making and reporting. You take ethical and sustainable considerations into account.
LO7: Personal Leadership	You are aware of your strengths and pitfalls in ICT as well as your personal development. To nurture personal growth and your learning attitude you undertake actions that align with your core values.

Communicatieplan

Tijdens mijn project is het belangrijk om duidelijke en consistente communicatie te onderhouden met de verschillende belanghebbenden. Dit plan beschrijft hoe en wanneer ik met de belanghebbenden zal communiceren om ervoor te zorgen dat iedereen goed op de hoogte blijft van de voortgang en de planning.

De volgende kanalen zullen worden gebruikt voor de communicatie tijdens mijn stage:

- **Face-to-face meetings:** Tweewekelijkse bijeenkomsten waarin ik updates geef over de voortgang van het onderzoek.
- **Microsoft Teams:** Voor online vergaderingen en korte vragen of discussies gebruik ik Microsoft Teams
- **E-mail:** Voor formele communicatie zoals het vastleggen van afspraken, het indienen van voortgangsrapporten gebruik ik e-mail.

Communicatie frequentie

Om ervoor te zorgen dat de voortgang van de project goed bewaakt wordt en belanghebbenden op de hoogte blijven, zal de communicatie op de volgende momenten plaatsvinden:

- **Tweewekelijkse voortgangsupdate:** Elke twee weken vindt er een voortgangsgesprek plaats met de supervisor. Tijdens deze gesprekken wordt de huidige status van het project besproken, inclusief behaalde mijlpalen, uitdagingen en de planning voor de komende periode.
- **Ad-hoc communicatie:** Indien er tijdens de project vragen of kwesties opkomen, wordt er gebruik gemaakt van een van de beschikbare communicatiekanalen voor snelle afstemming, of e-mail voor formele vragen en verzoeken.

Go/no go momenten

Op vooraf bepaalde momenten in het project worden Go/No Go-beslissingen genomen. Hierbij wordt beoordeeld of de opgeleverde resultaten voldoen aan de gestelde eisen en verwachtingen. Bij een Go-beslissing kan het project doorgaan naar de volgende fase. Bij een No Go-beslissing worden verbeteringen of aanpassingen doorgevoerd voordat er verder kan worden gegaan.

Noodcommunicatie

In het geval van urgente vragen of onvoorziene problemen die directe aandacht vereisen, kan ik altijd contact opnemen met mijn supervisor via Microsoft Teams of face-to-face en/of e-mail.

Project risico's

In dit gedeelte worden de mogelijke risico's beschreven die het succes van het project kunnen beïnvloeden. Deze risico's worden geïdentificeerd met als doel passende maatregelen te treffen om de risico's te beheersen.

Risico's en uitwijkactiviteiten

Risico	Uitwijkactiviteiten
Technische beperkingen van de infrastructuur	Zoeken naar alternatieve oplossingen
Verlies van projectdata door technische storingen	Backup-data gebruiken om de voortgang te herstellen zonder verlies van werk.
Veranderende doelen tijdens het project	Projectplan aanpassen om nieuwe doelen te integreren.