

31-5-2024

Versie: 1.0

Functioneel Ontwerp

Projectgroep

ICTAISc3

Docent

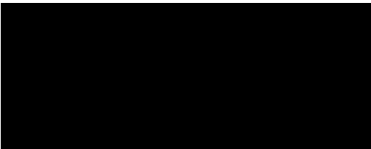


School en Opleiding

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	30-4-2024	Opzet	Eerste opzet gedaan
0.8	8-5-2024	Actoren en user stories	Actoren beschreven en een paar user stories gemaakt
1.0	28-5-2024	Afronding	De laatste user stories afgemaakt

Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
	Stakeholder	1.0	30-5-2024	Oplevering

Inhoudsopgave

1. Inleiding	3
2. Actoren	4
2.1. Analist – tier 1	4
2.2. Incident responder - tier 2	4
2.3. Threat hunter – tier 3	4
2.4. SOC-manager	4
2.5. Malware analyst	4
2.6. Forensisch specialist	4
2.7. Vulnerability manager	5
2.8. Security architect	5
2.9. Securityconsultant	5
3. Use Case Diagram	6
4. User Stories	7
5. Requirements	12
5.1. Functionele requirements	12
5.2. Niet functionele requirements	12
6. Bibliografie	13

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 geeft inzicht in de verschillende actoren die spelen binnen het SOC-team en gebruik maken van de SIEM-omgeving. De user stories zijn opgebouwd uit job stories die de taken van de verschillende actoren vertellen en hier een stroom uit kunnen maken. Het functioneel ontwerp zorgt hiermee voor meer duidelijkheid van de taken binnen de SIEM/SOC omgeving van Winfra Vital.

2. Actoren

Voor de SIEM/SOC omgeving zijn verschillende actoren betrokken die in aanmerking komen met deze omgeving. De actoren worden nader toegelicht voor verduidelijking van de use-cases, dit betreft de taken die door de verschillende rollen worden uitgevoerd en bijgehouden. Hierbij gaat het om de actoren: Analist, Incident responder, Threat hunter, SOC manager, Malware analist, Forensisch specialist, Vulnerability manager, Security architect & Security consultant.

2.1. Analist – tier 1

De analist is voornamelijk verantwoordelijk voor het bekijken van ruwe data en reviewen van alarmen en waarschuwingen die door de SIEM worden aangegeven. De analist moet identificeren of het gaat om een 'valse' melding of dat het een daadwerkelijke dreiging is. De hogere prioriteit alarmen en waarschuwingen worden doorgestuurd naar tier 2.

2.2. Incident responder - tier 2

De incident responder analyseert de hogere prioriteit incidenten. Er wordt een diepere analyse uitgevoerd door gebruik te maken van threat intelligence. De incident responder moet de grootte van de aanval begrijpen en bewust zijn van de verschillende systemen die aangetast zijn. Verder is de incident responder verantwoordelijk voor het ontwerpen en implementeren van strategieën om een incident te containen en te herstellen. Wanneer er grotere problemen optreden met het identificeren of mitigeren van de aanval wordt het incident geëscaleerd naar tier 3.

2.3. Threat hunter – tier 3

De threat hunters zijn de meest ervaren werknemers van de SOC. Deze behandelen de grootste incidenten die zijn geëscaleerd vanuit de incident responders. Verder houden de threat hunters toezicht op de kwetsbaarheden onderzoek en penetratietest of voeren deze uit. De threat hunters zoeken proactief naar mogelijke dreigingen, security gaps, en onbekende kwetsbaarheden.

2.4. SOC-manager

De SOC-manager houdt toezicht over het gehele SOC-team. De SOC-manager moet in staat zijn om technische begeleiding te bieden. Verder is moet de SOC-manager de teamleden evalueren, processen maken, incident reports beoordelen en het creëren en implementeren van crisis communicatieplannen.

2.5. Malware analist

De malware analist onderzoekt doordachte dreigingen door gebruik te maken van reverse engineering om zo hulp te bieden tijdens incident onderzoeken, het geven van threat intelligence aan de SOC, en het verbeteren van toekomstige detectie en response mogelijkheden.

2.6. Forensisch specialist

De forensisch specialist onderzoekt cyber events of incidenten die betrekking hebben tot informatietechnologie systemen, netwerken en digitale bewijsmaterialen.

2.7. Vulnerability manager

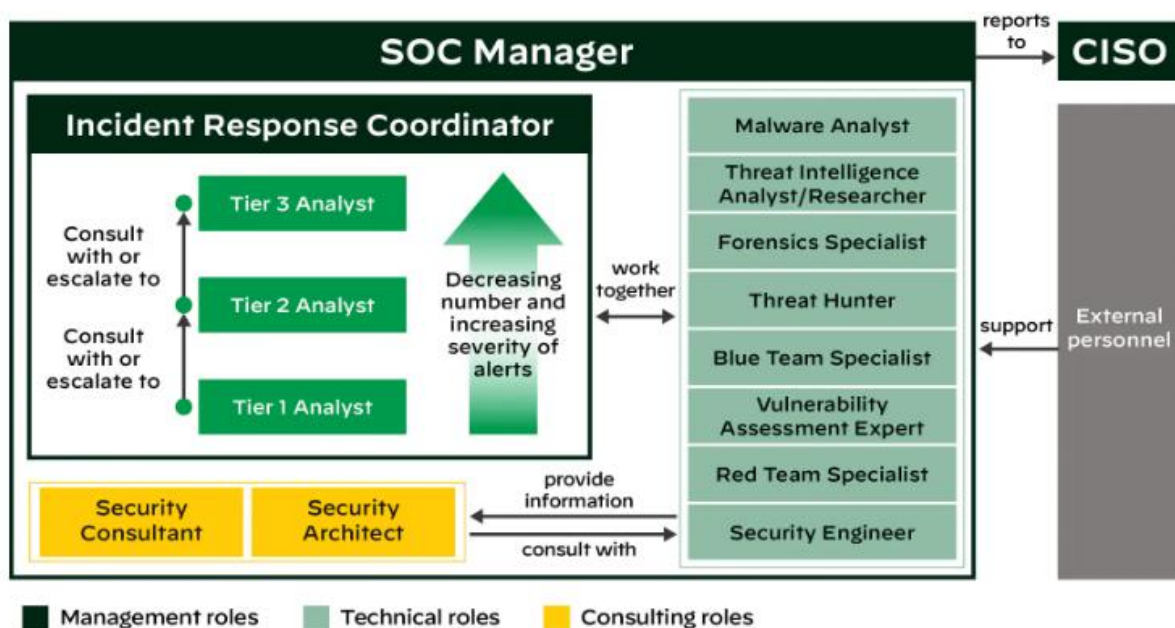
De vulnerability manager is verantwoordelijk voor het continu identificeren, beoordelen, rapporteren, managen en herstellen van kwetsbaarheden van endpoints, workloads en systemen.

2.8. Security architect

De security architect plant, onderzoekt en ontwerpt een robuust beveiligingsinfrastructuur. Verder leidt de security architect reguliere systeem en kwetsbaarheden testen, en implementeert of houdt toezicht over de implementatie van verbeteringen.

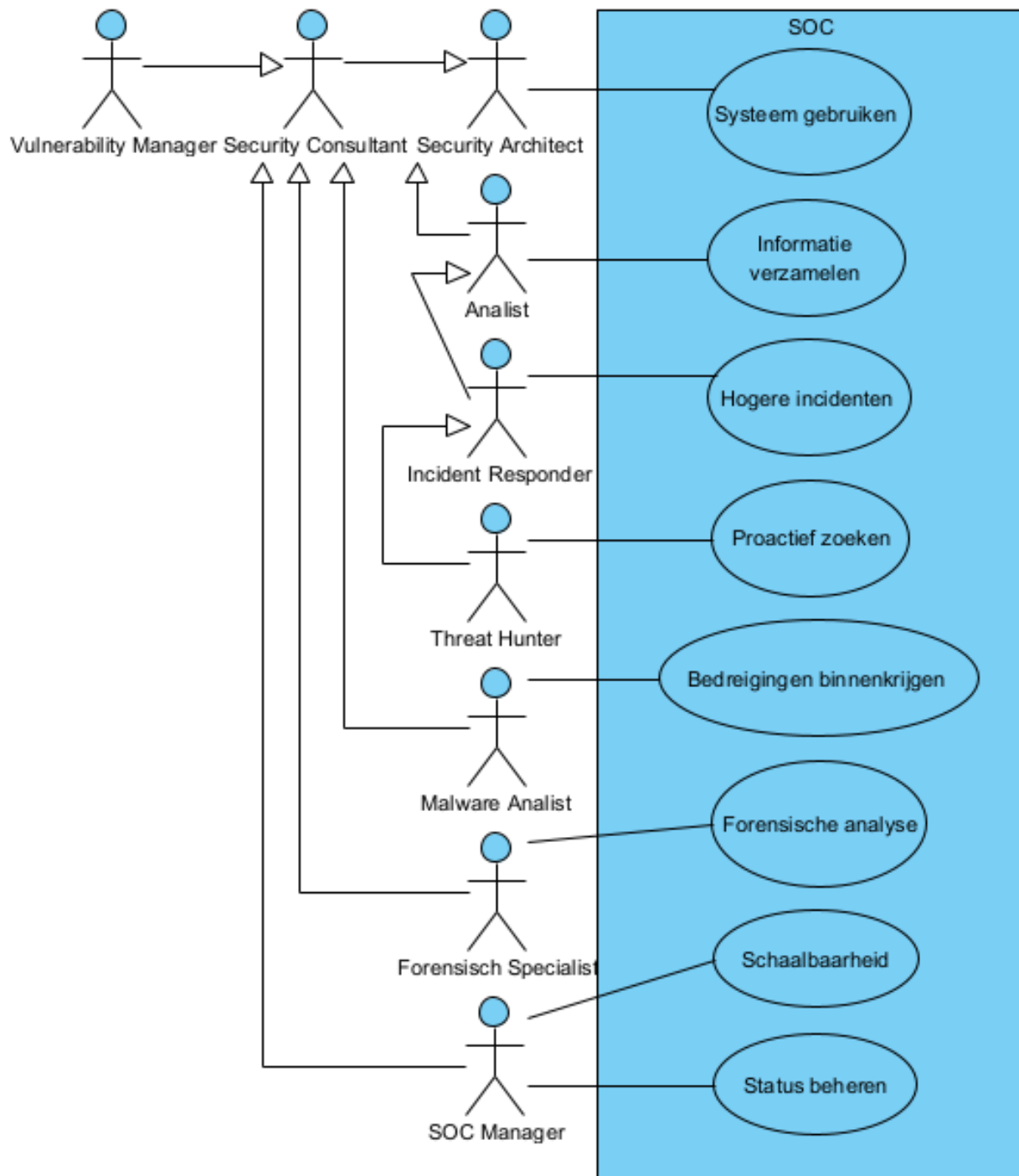
2.9. Securityconsultant

De securityconsultant onderzoekt beveiligingsstandaarden, best practices en beveiligingssystemen. Verder kan de securityconsultant een industrie overview leveren voor een organisatie en de huidige SoC mogelijkheden vergelijken met de competitie. Ook kunnen ze helpen met het plannen, onderzoeken en het ontwerpen van een robuust beveiligingsinfrastructuur.



Figuur 1, SOC werking binnen het team (paloaltonetworks, 2024).

3. Use Case Diagram



4. User Stories

1. Als een medewerker van het SOC wil ik het systeem kunnen gebruiken, zodat ik geïnformeerd kan blijven op de stand van zaken.
 - Een medewerker moet kunnen inloggen op het systeem.
 - Een medewerker kan gebruik maken van het dashboard.

Naam User story	Systeem gebruiken
Actoren	Alle actoren
Preconditie	Er is een systeem met een dashboard.
Basisstroom	1. Druk ok 'log in' 2. Vul inloggegevens in
Postconditie	Het systeem kan gebruikt worden
Alternatieve stromen	2a foute inloggegevens -> het systeem geeft een foutmelding

2. Als een security analist wil ik de mogelijkheid hebben om real-time bedreigingsinformatie te verzamelen en te analyseren, zodat ik snel kan reageren op potentiële beveiligingsincidenten.
 - Het loggingssysteem zorgt voor een overzicht van bedreigingsinformatie.
 - De verzamelde bedreigingsinformatie moet worden gepresenteerd aan de security analist via een gebruikersinterface die gemakkelijk te begrijpen en te navigeren is.
 - De gebruikersinterface moet de mogelijkheid bieden om bedreigingsinformatie te filteren, te sorteren en te doorzoeken op relevante kenmerken, zoals ernst, type dreiging, betrokken assets, enzovoort.
 - De software moet waarschuwingen en meldingen genereren voor potentiële beveiligingsincidenten op basis van de verzamelde bedreigingsinformatie, inclusief details over de dreiging, de betrokken assets en mogelijke gevolgen.
 - De verzamelde bedreigingsinformatie moet worden gevisualiseerd in overzichtelijke rapporten en dashboards, die belangrijke statistieken, trends en grafieken tonen om de security analist te helpen bij het nemen van weloverwogen beslissingen.

Naam User story	Informatie verzamelen
Actoren	Analist, incident responder, threat hunter
Preconditie	Er is een loggingssysteem
Basisstroom	1. Kijk of er een melding is van iets belangrijks 2. Filter en sorteer naar informatie om te controleren 3. Bekijk naar de grafieken en statistieken van de informatie
Postconditie	De gebruiker heeft genoeg informatie om een beslissing te maken.
Alternatieve stromen	1a belangrijke melding -> escaleer melding naar incident responder

3. Als een incident responder wil ik de hogere prioriteit incidenten binnen krijgen en analyseren, zodat ik door gebruik van threat intelligence het incident kan containen en herstellen.
 - De software moet in staat zijn om incidenten te classificeren op basis van prioriteit, waarbij hogere prioriteit wordt toegekend aan incidenten die een directe bedreiging vormen voor de beveiliging van het systeem of de organisatie.

- Incidenten met hogere prioriteit moeten automatisch worden gemarkeerd en op een duidelijke manier worden gepresenteerd aan de incident responder, zodat deze snel kan worden geïdentificeerd en geanalyseerd.
- De software moet integratie met threat intelligence feeds bieden om relevante context en informatie over de gedetecteerde incidenten te leveren, waardoor de incident responder in staat wordt gesteld om de aard en ernst van het incident beter te begrijpen.
- Incidenten moeten worden voorzien van gedetailleerde informatie, inclusief de betrokken assets, de impact op het systeem of de organisatie, en de mogelijke oorzaak of bron van de dreiging.
- Incident responders moeten de mogelijkheid hebben om geautomatiseerde acties uit te voeren om incidenten te containen en te herstellen, zoals het isoleren van besmette systemen, het blokkeren van schadelijke verkeersbronnen of het terugdraaien van schadelijke wijzigingen.
- De software moet dashboards en logs leveren die inzicht geven in de status van de incidentresponse, inclusief het aantal behandelde incidenten, de gemiddelde responstijd en de effectiviteit van de genomen maatregelen.
- De prestaties van de software moeten worden gevalideerd onder real-world omstandigheden, om ervoor te zorgen dat het systeem responsief blijft, zelfs tijdens piekbelastingen van incidentresponsactiviteiten.

Naam User story	Hogere incidenten
Actoren	Incident responder, threat hunter
Preconditie	Er is een logging systeem die filtert op prioriteit
Basisstroom	<ol style="list-style-type: none"> 1. Kijk of er een melding is geëscaleerd 2. Filter en sorteer naar informatie om te controleren 3. Zet threat intelligence in om de aard en ernst van het incident beter te begrijpen 4. Bekijk naar de grafieken en statistieken van de informatie 5. Voer acties uit om incidenten te containen 6. Voer acties uit om het incident te herstellen
Postconditie	De incident responder heeft het incident kunnen containen en herstellen.
Alternatieve stromen	3a hoogste prioriteit -> escaleer incident naar threat hunter

4. Als een threat hunter wil ik proactief zoeken naar dreigingen, security gaps, en onbekende kwetsbaarheden, zodat ik de mogelijke incidenten kan minimaliseren.
 - Het SOC-systeem biedt toegang tot gedetailleerde logbestanden, netwerkverkeerdata, en endpoint-gegevens voor diepgaande analyse.
 - Threat hunters hebben toegang tot geavanceerde zoek- en querytools om specifieke patronen en anomalieën te identificeren in grote datasets.
 - Threat hunters kunnen aangepaste detectieregels en scripts maken en toepassen om specifieke bedreigingsscenario's te identificeren.
 - Het SOC-systeem biedt visualisatietools om netwerk- en gebruikersgedrag te analyseren en afwijkingen te identificeren.
 - Het systeem ondersteunt integratie met kwetsbaarheidsbeheertools om bekende kwetsbaarheden te identificeren en te correleren met actieve bedreigingen.

- Threat hunters kunnen periodieke scans uitvoeren om onbekende kwetsbaarheden en misconfiguraties in het netwerk te detecteren.
- Het SOC-systeem biedt functionaliteiten voor het uitvoeren van aanvalssimulaties en penetratietests om security gaps en kwetsbaarheden te identificeren.
- Threat hunters kunnen hun bevindingen documenteren en gedetailleerde rapporten genereren die de geïdentificeerde dreigingen, security gaps, en aanbevelingen voor mitigatie beschrijven.
- Het SOC-systeem biedt real-time monitoring en alerting om threat hunters te waarschuwen voor verdachte activiteiten die mogelijk wijzen op nieuwe bedreigingen of kwetsbaarheden.
- Threat hunters hebben toegang tot historische data om trends en patronen te analyseren die kunnen wijzen op latente bedreigingen of opkomende kwetsbaarheden.

Naam User story	Proactief zoeken
Actoren	Threat hunter
Preconditie	Er is een netwerk waar de threat hunters kunnen zoeken naar dreigingen.
Basisstroom	<ol style="list-style-type: none"> 1. Kijk in de logbestanden naar hoge prioriteit incidenten geëscaleerd door incident response 2. Monitor het verkeer dat heeft gepasseerd binnen het netwerk 3. Gebruik zoek- en querytools in grote datasets 4. Voer periodiek scans uit om kwetsbaarheden en misconfiguraties op te sporen 5. Voer aanvalssimulaties en penetratietests uit voor verdere security gaps en kwetsbaarheden te identificeren 6. Rapporteer de bevindingen van de geïdentificeerde dreigingen en security gaps
Postconditie	Er zijn nieuwe kwetsbaarheden en security gaps in kaart gebracht, die gebruikt kunnen worden voor threat intelligence.
Alternatieve stromen	n.v.t

5. Als een SOC-manager wil ik een centraal dashboard hebben waar ik de status van alle beveiligingsgebeurtenissen en incidenten kan bekijken, zodat ik een compleet overzicht heb van de beveiligingsstatus van het netwerk.
 - Het dashboard toont een overzicht van alle beveiligingsgebeurtenissen en incidenten in real-time.
 - Een SOC-manager kan filters toepassen om specifieke gebeurtenissen te bekijken op basis van tijd, ernst, bron, enz.
 - Het dashboard biedt grafische visualisaties en rapporten om trends en patronen te identificeren.

Naam User story	Status beheren
Actoren	SOC-manager
Preconditie	Er is een centraal dashboard dat de status weergeeft van beveiligingsgebeurtenissen en incidenten
Basisstroom	<ol style="list-style-type: none"> 1. Bekijk de huidige status van alle beveiligingsgebeurtenissen en incidenten 2. Filter voor een specifieke gebeurtenis/incident 3. Bekijk grafische visualisatie/ rapport 4. Identificeer patronen en trends

Postconditie	De SOC-manager heeft beveiligingsgebeurtenissen en incidenten kunnen inzien en beheren
Alternatieve stromen	4a kritieke bevinding -> escaleer incident naar incident responder

6. Als een malware analist wil ik bedreigingen binnenkrijgen, zodat ik reverse engineering kan uitvoeren op ernstige incidenten.
- Het systeem kan bedreigingen classificeren op basis van ernstniveaus en relevantie voor de organisatie, waarbij prioriteit wordt gegeven aan ernstige incidenten die onmiddellijke aandacht vereisen.
 - Een malware analist heeft toegang tot een dashboard of interface waar ze de lijst met ontvangen bedreigingen kunnen bekijken en filteren op verschillende criteria, zoals datum, bron en ernst.
 - Het SOC-systeem biedt de mogelijkheid om gedetailleerde rapporten te genereren voor elke ontvangen bedreiging, inclusief metadata en contextuele informatie die nodig is voor reverse engineering.
 - Malware analisten kunnen bedreigingen markeren als "in onderzoek" of "behandeld", en kunnen notities toevoegen over de voortgang van hun analyse en de genomen maatregelen.
 - Het systeem ondersteunt integratie met tools en platforms die worden gebruikt voor malware-analyse en reverse engineering.
 - Het SOC-systeem bewaart een archief van ontvangen bedreigingen en bijbehorende analyses voor toekomstige referentie, auditdoeleinden en trendanalyse.

Naam User story	Bedreigingen binnenkrijgen
Actoren	Malware analist
Preconditie	Er is een bedreiging
Basisstroom	<ol style="list-style-type: none"> 1. De malware analist krijgt een bedreiging binnen 2. De malware analist kijkt naar de bedreiging 3. De malware analist probeert de bedreiging te reverse engineeren 4. De malware analist geeft zijn resultaten door
Postconditie	Het is duidelijk hoe de bedreiging in elkaar zit
Alternatieve stromen	3a lukt niet -> melden aan SOC-manager

7. Als een forensisch specialist wil ik de mogelijkheid hebben om forensische analyses uit te voeren op verdachte gebeurtenissen, zodat ik de oorsprong en impact van een beveiligingsincident kan begrijpen en geschikte maatregelen kan nemen.
- Forensisch specialisten kunnen verdachte gebeurtenissen identificeren en markeren voor verdere analyse.
 - Het systeem ondersteunt tijdlijnanalyse, waarbij forensisch specialisten de volgorde van gebeurtenissen kunnen reconstrueren om de voortgang van een beveiligingsincident te begrijpen.
 - Het systeem kan artefacten van verdachte gebeurtenissen verzamelen en opslaan, zoals malware samples, verdachte bestanden, en systeemimages, voor gedetailleerde analyse.
 - Het SOC-systeem biedt functionaliteiten voor het vergelijken van huidige gebeurtenissen met historische data om patronen en anomalieën te identificeren.

- Forensisch specialisten kunnen gedetailleerde rapporten genereren die de bevindingen van hun analyses documenteren, inclusief de vermoedelijke oorzaak, impact, en aanbevolen mitigatiemaatregelen.
- Het systeem ondersteunt samenwerking en notities, zodat meerdere specialisten hun bevindingen en inzichten kunnen delen tijdens een forensisch onderzoek.
- Forensisch specialisten kunnen de integriteit en vertrouwelijkheid van verzamelde data waarborgen door gebruik te maken van versleuteling en toegangscontrole binnen het SOC-systeem.

Naam User story	Forensische analyse
Actoren	Forensisch specialist
Preconditie	Er heeft een beveiligingsincident plaatsgevonden
Basisstroom	<ol style="list-style-type: none"> 1. De forensische specialist krijgt een melding 2. De forensische specialist onderzoekt het incident 3. De forensische specialist waarborgt alles wat met het incident tet maken heeft 4. De forensische specialist rapporteert zijn bevindingen
Postconditie	Het incident is afgesloten
Alternatieve stromen	n.v.t.

8. Als een SOC-manager wil ik dat het SOC schaalbaar is en kan omgaan met het groeiende volume van beveiligingsgebeurtenissen, zodat we onze beveiligingsactiviteiten kunnen uitbreiden naarmate onze organisatie groeit.
- Een SOC-manager moet kunnen zien hoe dicht bij de limiet dat het systeem aan kan zit.
 - Een SOC-manager moet het systeem kunnen uitbreiden.
 - Het systeem breidt het uit.

Naam User story	Schaalbaarheid
Actoren	SOC-manager
Preconditie	Er is een SOC
Basisstroom	<ol style="list-style-type: none"> 1. Meer gebeurtenissen 2. SOC-manager ziet dat het aan de limiet komt 3. SOC-manager schaaft het omhoog
Postconditie	Het is uitgebreid zonder problemen
Alternatieve stromen	n.v.t.

5. Requirements

5.1. Functionele requirements

Deze staan als acceptatiecriteria bij de user stories.

5.2. Niet functionele requirements

- Het loggingssysteem moet in staat zijn om loggegevens in real-time te verwerken en op te slaan met een latentie van minder dan 100 milliseconden.
- Het systeem moet minimaal 10.000 logberichten per seconde kunnen verwerken zonder prestatieverlies.
- Het loggingssysteem moet horizontaal schaalbaar zijn, zodat het kan uitbreiden om hogere volumes aan loggegevens te verwerken naarmate de organisatie groeit.
- Het systeem moet een uptime van 99.9% garanderen, inclusief geplande onderhoudsperioden.
- Loggegevens moeten zowel in rust als tijdens transport worden versleuteld om de vertrouwelijkheid en integriteit te waarborgen.

6. Bibliografie

paloaltonetworks. (2024, April 25). *Security Operations Center (SOC) Roles and Responsibilities*. Opgehaald van paloaltonetworks.com:
<https://www.paloaltonetworks.com/cyberpedia/soc-roles-and-responsibilities>