**Webtechnologie intro**

2023-2024

A logo with a triangle and a triangle

Description automatically generated

**Langlopende taak**

**Projectopdracht-1+2**

Al-Karawi Mustafa

Website zal over network security zijn

# Thema

Homepage: Welkom bij UnityNet

Verbinden versterken door geavanceerde netwerktechnologie

## Overzichtsonderwerpen Pagina

### Cybersecurity Awareness

Welkom bij ons Cybersecurity Awareness Hub!

In het digitale tijdperk van vandaag is veilig online blijven niet slechts een aanbeveling; het is een noodzaak. Met cyberdreigingen die zich in een ongekend tempo ontwikkelen, is het cruciaal dat zowel individuen als organisaties uitgerust zijn met de kennis en hulpmiddelen om hun digitale activa te beschermen. Onze missie is om u te voorzien van de laatste inzichten, beste praktijken en proactieve maatregelen om uw online veiligheid te waarborgen.

Het Begrijpen van Cyberdreigingen

Cyberdreigingen komen in verschillende vormen voor, waaronder virussen, malware, phishing-aanvallen, ransomware en meer. Deze dreigingen zijn ontworpen om persoonlijke informatie te stelen, operaties te verstoren en de integriteit van gegevens in gevaar te brengen. Door de aard van deze dreigingen te begrijpen, kunt u uw risico om slachtoffer te worden aanzienlijk verminderen.

Beste Praktijken voor Online Veiligheid

Sterke Wachtwoorden: Gebruik complexe en unieke wachtwoorden voor al uw accounts. Overweeg het gebruik van een wachtwoordbeheerder om ze bij te houden.

Regelmatige Updates: Houd uw software en apparaten up-to-date om te beschermen tegen de nieuwste kwetsbaarheden.

Bewustzijn van Phishing: Wees voorzichtig met e-mails of berichten die onmiddellijke actie vereisen, gevoelige informatie aanvragen of verdachte links bevatten.

Veilige Verbindingen: Gebruik veilige, gecodeerde verbindingen bij het online browsen. Zoek naar "HTTPS" in de URL en overweeg het gebruik van een VPN voor extra privacy.

Back-up Uw Gegevens: Maak regelmatig een back-up van belangrijke gegevens naar een externe schijf of cloudopslag om verlies in geval van een cyberaanval te voorkomen.

Iedereen Empoweren

Cybersecurity is een gedeelde verantwoordelijkheid. Of u nu thuis surft, op afstand werkt of een organisatie beheert, uw acties kunnen een verschil maken. We moedigen u aan deze informatie te delen met vrienden, familie en collega's om een veiligere online gemeenschap te creëren.

Blijf Geïnformeerd

Het landschap van cybersecurity verandert voortdurend. Blijf vooroplopen door geïnformeerd te blijven over de nieuwste dreigingen en veiligheidstips. Abonneer u op onze nieuwsbrief, volg onze blog en neem deel aan onze communityforums om in contact te komen met cybersecurity-experts en liefhebbers.

### Threat Intelligence Services:

Verhoog Uw Cybersecurity Positie

In een constant evoluerend digitaal landschap is voorkennis macht—vooral als het gaat om cybersecurity. Onze Threat Intelligence Services zijn ontworpen om bedrijven een voorsprong te geven tegen cyberdreigingen. Door het benutten van geavanceerde technologie en diepgaande cybersecurity expertise, bieden we bruikbare inzichten die uw digitale activa beschermen voordat dreigingen materialiseren.

Wat Zijn Threat Intelligence Services?

Threat Intelligence houdt het verzamelen, analyseren en verfijnen van gegevens over potentiële of huidige aanvallen die de veiligheid van de digitale omgeving van uw organisatie bedreigen in. Het gaat niet alleen om monitoring; het gaat om het begrijpen van de risico's en weten hoe deze te voorkomen. Onze diensten bieden een uitgebreid overzicht van het landschap van cyberdreigingen, en leveren op maat gemaakte intelligentie die relevant is voor uw specifieke bedrijfsbehoeften en beveiligingspositie.

Waarom Kiezen Voor Onze Threat Intelligence Services?

Proactieve Bescherming: Blijf cybercriminelen een stap voor met inzichten die u in staat stellen om dreigingen te anticiperen en te mitigeren voordat ze uw bedrijf beïnvloeden.

Aangepaste Intelligentie: Ontvang informatie die het meest relevant is voor uw organisatie, zodat u niet alleen op de hoogte bent van het algemene dreigingslandschap, maar ook geïnformeerd bent over specifieke dreigingen die uw sector richten.

Strategische Beveiligingsbeslissingen: Maak met onze bruikbare intelligentie geïnformeerde beslissingen over uw beveiligingsstrategieën en middelenverdeling, en verbeter zo uw algehele beveiligingskader.

Naleving en Risicobeheer: Navigeer met gemak door de complexe wereld van regelgevende vereisten, aangezien onze diensten u helpen uw cybersecurityrisico's effectief te begrijpen en te beheren.

Ons Threat Intelligence Proces

Verzameling: We verzamelen inlichtingen uit een breed scala van bronnen, inclusief monitoring van het diepe en donkere web, om een uitgebreide zichtbaarheid van dreigingen te garanderen.

Analyse: Onze experts analyseren de verzamelde gegevens, identificeren trends, tactieken, technieken en procedures die door cyber tegenstanders worden gebruikt.

Verfijning: We destilleren de geanalyseerde gegevens tot bruikbare intelligentie, zodat u relevante en tijdige informatie ontvangt.

Levering: Onze bevindingen worden geleverd via intuïtieve platforms, rapporten en waarschuwingen, waardoor u snel actie kunt ondernemen.

Empower Uw Organisatie

Of u nu gevoelige gegevens wilt beschermen, bedrijfscontinuïteit wilt waarborgen, of uw bestaande beveiligingsmaatregelen wilt verbeteren, onze Threat Intelligence Services zijn uw poort naar een veiligere toekomst. Wij bieden niet alleen de intelligentie die u nodig heeft om uw operaties te beschermen, maar ook de ondersteuning om effectieve verdedigingsstrategieën te implementeren.

Klaar om Uw Beveiligingsstrategie Te Transformeren?

Neem vandaag nog contact met ons op om meer te leren over hoe onze Threat Intelligence Services uw cybersecurity verdediging kunnen versterken. Samen kunnen we een veerkrachtige en proactieve beveiligingspositie creëren die uw bedrijf vooruit helpt in een veilig digitaal ecosysteem.

### Netwerkbeveiliging:

Netwerkbeveiliging omvat de beleidslijnen, praktijken en hulpmiddelen die zijn ontworpen om de integriteit, vertrouwelijkheid en toegankelijkheid van computernetwerken en gegevens te beschermen met behulp van zowel hardware- als softwaretechnologieën. Het doel is om ongeautoriseerde toegang, misbruik, storing, wijziging, vernietiging of ongepaste openbaarmaking te voorkomen, waardoor wordt gegarandeerd dat het netwerk zijn kritieke functies correct uitvoert. Belangrijke elementen zijn onder meer firewalls, antivirussoftware, inbraakdetectie- en preventiesystemen, encryptie en veilige toegangscontroles.

Netwerkbeveiligingspagina

Netwerken versterken tegen bedreigingen

Ontdek het nieuwste op het gebied van netwerkbeveiligingspraktijken, van firewalls en encryptie tot inbraakdetectiesystemen en VPN's. Leer hoe u uw netwerk kunt beschermen tegen ongeautoriseerde toegang, gegevensinbreuken en andere cyberdreigingen.

### Schaalbaarheid:

Schaalbaarheid verwijst naar het vermogen van het netwerk om te groeien en een toegenomen vraag te beheren zonder de prestaties of beveiliging in gevaar te brengen. Een schaalbaar netwerk kan efficiënt meer gebruikers, apparaten of gegevensdoorvoer accommoderen indien nodig. Ontwerpen voor schaalbaarheid omvat het overwegen van toekomstige groei in netwerkplanning en -implementatie, zodat het netwerk kan uitbreiden in termen van grootte, bandbreedte of verwerkingscapaciteit.

Schaalbaarheidspagina

Groeien zonder grenzen

Ontdek strategieën voor het efficiënt schalen van uw netwerk, inclusief overwegingen voor hardware, software en architectuur. Leer over de uitdagingen van het opschalen naar boven of naar buiten en hoe u tijdens de groei prestaties en beveiliging kunt handhaven.

### Prestatieoptimalisatie:

Prestatieoptimalisatie in netwerken omvat technieken en strategieën om de snelheid en efficiëntie van gegevensoverdracht te verbeteren, latency te verminderen, doorvoer te verhogen en een hoge beschikbaarheid van netwerkdiensten te garanderen. Dit kan het optimaliseren van routeringsprotocollen, bandbreedteallocatie, load balancing en het minimaliseren van congestie omvatten om ervoor te zorgen dat netwerkbronnen zo efficiënt mogelijk worden gebruikt.

Prestatieoptimalisatiepagina

Efficiëntie en snelheid maximaliseren

Duik in technieken en hulpmiddelen voor het optimaliseren van netwerkprestaties, inclusief QoS, bandbreedtebeheer en congestiecontrole. Begrijp hoe u netwerkprestaties kunt beoordelen en verbeteringen kunt implementeren.

### Beheer en monitoring:

Netwerkbeheer en -monitoring omvat het gebruik van tools en praktijken om toezicht te houden op de werking van een computernetwerk en ervoor te zorgen dat het optimaal en veilig werkt. Beheerstaken omvatten het configureren van netwerkapparaten, het beheren van gebruikerstoegang en het installeren van updates. Monitoring houdt in dat de prestaties van het netwerk continu worden gecontroleerd, dat bedreigingen van de beveiliging worden gedetecteerd en hierop wordt gereageerd en dat problemen worden geïdentificeerd en opgelost wanneer ze zich voordoen. Effectief beheer en monitoring kunnen downtime helpen voorkomen, de beveiliging verbeteren en de prestaties optimaliseren.

Pagina Beheer en monitoring

Netwerken optimaal laten presteren

Ontdek de essentiële tools en praktijken voor netwerkbeheer en -monitoring. Begrijp hoe u de gezondheid, prestaties en beveiliging van het netwerk kunt volgen en hoe u proactief op problemen kunt reageren met de juiste tools en technieken.

### Fouttolerantie en Redundantie:

Fouttolerantie en redundantie zijn strategieën die worden gebruikt om ervoor te zorgen dat een netwerk operationeel blijft, zelfs wanneer een of meer van zijn componenten falen. Fouttolerantie houdt in dat het netwerk zo wordt ontworpen dat het correct kan blijven functioneren, zelfs als een component faalt. Redundantie voegt dubbele componenten toe, zoals servers

Kan later gebruikt worden op de inlogpagina

Word lid van de UnityNet Community

Word onderdeel van UnityNet en sluit je aan bij een groeiende gemeenschap van netwerkprofessionals en liefhebbers. Deel je kennis, leer van anderen en blijf vooroplopen in de netwerktechnologie.

# Inspiratie

1. <https://www.site24x7.com/network-monitoring.html>

Ik vond Navbar leuk

En ook onderstaand

A screenshot of a computer

Description automatically generated

1. <https://cybermap.kaspersky.com/>

Ik vind de kaart leuk en kan misschien wel iets gebruiken

1. Maps <https://www.digitalattackmap.com/>

<https://threatmap.checkpoint.com/>

<https://threatmap.fortiguard.com/>

1. Ik vind de afbeelding mooi hoe ze ze mirageren

<https://www.akamai.com/es/why-akamai?tab%3Dattacks%26theme%3Ddark&rel=nofollow,noopener,noreferrer&target=_blank>

1. Dashbord https://grafana.com/

# kleurenpalet

#11DA80

#2E6749

#121615

Logo

A logo with a shield and a sword

Description automatically generated

Home - Desktop

A screenshot of a computer

Description automatically generated

Overzichtspagina – Desktop

A screenshot of a computer

Description automatically generated

Dashboard– Desktop

**A screenshot of a computer

Description automatically generated**

Contact – Desktop

A screenshot of a computer

Description automatically generated

Home – mobile devices

A screenshot of a cellphone

Description automatically generated

Overzichtspagina - mobile devices

A screenshot of a cell phone

Description automatically generated

Dashboard - mobile devices

A black rectangular object with white text

Description automatically generated

Contact - mobile devices

**A black and white screen

Description automatically generated**