DUTCH EXPAT

CV

EMRE

CYBERBEVEILIGINGSSPECIALIST, SOC-ANALIST, INCIDENTAFHANDELING, SIEM-SYSTEMEN, LOGBEWAKING, BEDREIGINGSANALYSE, SCRIPTING, ENDPOINTBESCHERMING, FIREWALLCONFIGURATIE, KWETSBAARHEIDSSCANS, DASHBOARDONTWIKKELING, NETWERKBEVEILIGING

EMRE

Woonplaats **Istanbul**
Nationaliteit **Turkse**
Geboortedatum **22.04.1994**
Burgerlijke Staat **Ongehuwd**
Beroep/Functie **Cyberbeveiligingsspecialist**
Web **https://www.linkedin.com/in/emre-ozkbk**

GSM **+31 621 25 33 70**
Tel **+90 312 905 01 10**
Web **www.dutch-expat.com**
E-mail **info@dutch-expat.com**

BELANGRIJKE VAARDIGHEDEN

CYBERBEVEILIGINGSSPECIALIST, SOC-ANALIST, **INCIDENTAFHANDELING,** SIEM-SYSTEMEN, LOGBEWAKING, **BEDREIGINGSANALYSE,** SCRIPTING, **ENDPOINTBESCHERMING, FIREWALLCONFIGURATIE,** KWETSBAARHEIDSSCANS, DASHBOARDONTWIKKELING, NETWERKBEVEILIGING,

PERSOONLIJK PROFIEL

Mijn naam is Emre. Als een dynamisch en innovatief persoon heb ik voortdurende zelfontwikkeling tot mijn levensfilosofie gemaakt. Met enthousiasme en toewijding blijf ik mezelf verbeteren, zowel op persoonlijk als professioneel vlak. Na het afronden van mijn bacheloropleiding Computer Engineering aan de Süleyman Demirel Universiteit, heb ik actief deelgenomen aan verschillende projecten waarin ik mijn theoretische kennis in praktijk kon brengen. De vaardigheden die ik in deze periode heb opgedaan, vormen een sterke basis voor mijn professionele loopbaan.

Ik heb mij gespecialiseerd in cybersecurity en blijf mij voortdurend verdiepen in dit snel evoluerende vakgebied. Tijdens mijn werkervaring bij toonaangevende organisaties zoals Etiya, KoçSistem en Diler Holding, heb ik gewerkt als Cyber Security Specialist, waar ik mijn vaardigheden op het gebied van teamwerk, projectmanagement en probleemoplossing verder heb ontwikkeld. Tevens heb ik waardevolle ervaring opgedaan in multiculturele omgevingen, wat mijn communicatieve vaardigheden en intercultureel bewustzijn heeft versterkt.

Als Cyber Security Specialist beschik ik over sterke analytische vermogens en een scherp oog voor risico's. Ik heb bewezen ervaring in het herkennen, analyseren en verhelpen van kwetsbaarheden, en in het implementeren van passende beveiligingsmaatregelen. Ik heb uitgebreide kennis van en ervaring met tools zoals ELK Stack, IBM QRadar, Splunk, Cortex XSOAR, CrowdStrike EDR, Xcitium, Cisco Ironport, Trellix, Forcepoint Proxy, Checkpoint, Nessus, CyberArk, DNSSense, Wazuh, Nmap, Burp Suite, Kali Linux, MITRE ATT&CK, Wireshark en Metasploit. Met deze tools kan ik effectief beveiligingslogs analyseren, verdachte activiteiten detecteren en snel reageren op incidenten.

Mijn grootste motivatie om te wonen en werken in Nederland is de innovatieve werkcultuur, de hoge levenskwaliteit en de inclusieve samenleving. Nederland is bovendien een wereldwijde koploper op het gebied van cybersecurity, met sterke nadruk op duurzaamheid, privacy en technologische innovatie — waarden die naadloos aansluiten bij mijn carrière-ambities. Ik ben ervan overtuigd dat ik in deze omgeving zowel professioneel als persoonlijk verder kan groeien, en direct waarde kan toevoegen aan uw organisatie.

Ik kijk ernaar uit om mijn motivatie en achtergrond verder toe te lichten in een persoonlijk gesprek. Met mijn hoge mate van aanpassingsvermogen en sterke motivatie ben ik volledig voorbereid om snel te integreren in uw team en direct bij te dragen aan uw doelstellingen.

WERKERVARING

Cyberbeveiligingsspecialist
Diler Holding (Istanbul)

07-2024 / Heden

- CRYPTOSIM (SIEM): Nieuwe dashboards, meldingen en geplande rapporten maken, afstemoperaties op regels uitvoeren, logactiviteiten beheren.
- Cortex XSOAR: Controle van SOAR-meldingen en acties ondernemen.
- Cortex XDR: Installatie van Cortex XDR voor gebruikers, uitsluitingen schrijven, incidentcontrole en acties ondernemen, dashboards en rapporten creëren, onderzoek uitvoeren, reageren en detecteren van regels, correlaties.
- Xcitium: RMM, DLP, patchbeheer, apparaatbeheer, procedures, endpointbescherming, endpoint zero trust (EPP+EDR+ZD), dashboards en rapporten maken, meldingen analyseren, uitsluitingen schrijven en whitelist beschrijven.
- Beamsec Email Security Products: Phishingmailscenario's creëren, activiteiten voor bewustwording van cybersecurity organiseren en trainingen voor gebruikers definiëren.
- Cisco Ironport Secure Email Gateway: E-mails vrijgeven die als spam zijn gemarkeerd, tenzij het phishingmails zijn, en toevoegen aan de whitelist. Phishingmails analyseren, toevoegen aan de bloklijst en inkomende-uitgaande e-mailbeleid creëren.
- Trellix: Meldingen analyseren, uitsluitingen schrijven, beleid definiëren en bewerken, DLP, on-access scan, on-demand scan uitvoeren.
- Forcepoint Web Security Proxy Gateway: Installatie van het gerelateerde product voor gebruikers, rapportage, uitzonderingen beschrijven, meldingen analyseren.
- Checkpoint: Geplande rapporten, regels, beleidsmaatregelen creëren. Logbestanden analyseren en monitoren.
- Nessus – Het uitvoeren van kwetsbaarhedenscans voor het bedrijf en de regio's (hoofdkantoor, fabrieken en hotels) op regelmatige basis.
- CyberArk (PAM [Privileged Access Management]).
- Roksit DNS Security (DNSSense): Beheer van beleidsmaatregelen, analyseren van verkeer, incidenten en logboeken, dashboards en rapporten creëren, DDR (Domain Detection & Response), DNS Firewall.
- Wazuh: Nieuwe dashboards, meldingen en geplande rapporten creëren, afstemoperaties op regels uitvoeren, logactiviteiten beheren.

Cyberverdedigingsingenieur
KocSistem (Istanbul)

10-2023 / 11-2023

- Beheer en Tuning van Regels in IBM QRadar: Beheer van regels en afstemoperaties binnen het IBM QRadar SIEM-platform.
- Analyse van Offenses in IBM QRadar: Uitgebreide analyse van beveiligingsincidenten (offenses) binnen IBM QRadar.
- Maandelijkse SOC-Rapporten: Opstellen en presenteren van maandelijkse rapporten voor klanten met betrekking tot beveiligingsoperaties en incidenten.
- Incidentverwerking via Cortex XSOAR: Gebruik van Cortex XSOAR voor incidentverwerking, inclusief het nemen van actie bij waarschuwingen en beveiligingsincidenten.

Senior Specialist Beveiligingsoperaties
ETIYA (Istanbul)

02-2023 / 09-2023

- Opstellen en Presenteren van Maandelijkse SOC-Rapporten: Het opstellen en presenteren van maandelijkse rapporten voor klanten, met betrekking tot beveiligingsoperaties en incidenten.
- Rapportage van Gevoelige Gegevens: Het opstellen en presenteren van rapporten met betrekking tot gevoelige gegevens voor klanten, inclusief risico-analyses.
- Periodieke Threat Hunting-Activiteiten: Uitvoeren van periodieke threat hunting-activiteiten om potentiële dreigingen en kwetsbaarheden vroegtijdig te identificeren.
- Loganalyse en Monitoring via Splunk: Gebruik van Splunk voor loganalyse en monitoring van beveiligingslogboeken en netwerkactiviteit.
- Beheer van EDR-Meldingen via CrowdStrike: Beheer en analyse van EDR-meldingen via CrowdStrike om verdachte activiteiten op eindpunten te identificeren en te reageren op incidenten.
- Beheer van IBM QRadar-regels en Meldingen: Beheer van beveiligingsregels en meldingen binnen IBM QRadar, inclusief tuning en optimalisatie.
- Incidentverwerking via SOAR-oplossingen: Gebruik van SOAR-oplossingen voor de verwerking van incidenten, inclusief de uitvoering van actieplannen en coördinatie van responsmaatregelen.
- Loganalyse en Rapportage met FortiAnalyzer: Loganalyse en rapportage van netwerk- en systeemactiviteiten via FortiAnalyzer.
- Gebruik van SOCRadar voor Dreigingsinformatie en Surface Monitoring: Gebruik van SOCRadar voor dreigingsinformatie, het monitoren van het externe netwerkoppervlak en het identificeren van potentiële kwetsbaarheden.

Beveiligingsspecialist

ETIYA (Istanbul)

12-2020 / 02-2023

- Logmonitoring en Analyse met ELK: Uitvoeren van logmonitoring en -analyse met behulp van het ELK-platform (Elasticsearch, LogStash, Kibana) om beveiligingsincidenten en verdachte activiteiten te identificeren.
- Creëren van Dashboards en Waarschuwingen in ELK: Het maken van nieuwe dashboards en waarschuwingen binnen ELK voor geavanceerde dreigingsdetectie en monitoring.
- Toepassing van Machine Learning in ELK: Gebruik van machine learning-technieken in het ELK-platform voor geavanceerde dreigingsdetectie en voorspellingen.
- Opstellen van SOC-Rapporten en Gevoelige Gegevensrapporten: Het opstellen van maandelijkse rapporten over beveiligingsoperaties en gevoelige gegevens, en deze presenteren aan klanten.
- Onderzoek en Reactie op Verdachte Activiteiten: Onderzoek en reactie op verdachte activiteiten binnen alle bedrijfsassets in een 24/7 ploegendienst.
- Feedback om Cybersecurityprocessen te Verbeteren: Het geven van terugkoppeling en aanbevelingen om de effectiviteit van cybersecurityprocessen te verbeteren.
- Monitoring en Rapportage van Wereldwijde Cybersecurity-Incidenten: Monitoring en rapportage van wereldwijde cybersecurity-incidenten en actuele dreigingen om de veiligheid van de organisatie te waarborgen.
- Loganalyse en Forensisch Onderzoek: Het uitvoeren van loganalyse en forensisch onderzoek ter ondersteuning van het beveiligingsmonitoringsproces, en het identificeren van de oorzaken van incidenten.

Cyberbeveiligingsadviseur

Zero Second Information Systems and Consulting Co. Ltd. (Istanbul)

03-2020 / 06-2020

- Uitvoeren van Systeemcontroles op Firewalls en Gateways: Uitvoeren van systeemcontroles op firewallbeheer en gateways bij klanten, inclusief controle van logcapaciteit om de operationele efficiëntie te waarborgen.
- Analyse en Interpretatie van Firewallrapporten: Analyseren en interpreteren van firewallrapporten (Application-URL Filtering, IPS, AntiBot en AntiVirus); verstrekken van statusupdates en ondernemen van noodacties na goedkeuring om de beveiliging te waarborgen.
- Schrijven van Artikelen over Cyberbeveiligingsincidenten: Het schrijven van artikelen over actuele cyberbeveiligingsincidenten en deze publiceren op de bedrijfswebsite om klanten te informeren over recente dreigingen en oplossingen.
- Onderzoek en Vertaling van Technische Onderwerpen: Onderzoeken en vertalen van technische onderwerpen, met focus op tools zoals Boldon James, BackBox en Rapid7 InsightIDR, om technische documentatie te ondersteunen en te vertalen voor een breder publiek.
- Uitvoeren van Diagnostische Tests en Firewallinstallaties: Uitvoeren van diagnostische tests en het installeren van firewalls om ervoor te zorgen dat netwerken beveiligd blijven tegen ongeautoriseerde toegang.
- Opstellen van Back-up- en Herstelrapporten: Het opstellen van back-up- en herstelrapporten, evenals gezondheidscontroles, om de integriteit van de gegevens te waarborgen.
- Deelname aan Trainingen en Webinars: Actief deelnemen aan trainingen, webinars en webcasts om up-to-date te blijven met de nieuwste ontwikkelingen in de cybersecurityindustrie.

Stagair Software en Hardware

I-Tech Robotics Automation Trade Co. Ltd. (Isparta)

09-2019 / 11-2019

- Code schrijven voor fietsslotproject: Ik heb code geschreven voor het fietsslotproject met behulp van de programmeertaal Python op een Raspberry Pi.
- Gebruik van afstandssensoren leren: Ik heb geleerd hoe ik de HC-SR04 afstandssensor en de URM37 ultrasone afstandssensor kan gebruiken op de Raspberry Pi en Arduino voor het AGV (Automated Guided Vehicle) project, en ik heb samen met mijn teamleider code geschreven.
- Voertuigbewegingen realiseren in AGV-project: Voor het AGV (Automated Guided Vehicle) project heb ik de bewegingen van het voertuig gerealiseerd door de onderdelen Hard Link en Symbolic Link in Linux te leren en de bijbehorende Linux-commando’s in te voeren.
- Onderzoek naar websitebeveiliging uitvoeren: Ik heb onderzoek gedaan naar het onderwerp "beveiliging van websites" en rapporten opgesteld voor het e-developmentproject.

OPLEIDINGEN

2014 - 2019
Bachelor - Computer Engineering (Computertechniek)
Süleyman Demirel Universiteit (Isparta)
Diploma: Ja

Cursussen

Structured Query Language (SQL) – Smartpro Teknoloji – maart 2024
Certificaat :Ja

Gecertificeerd SOC-analist (CSA) – EC-Council – december 2023
Certificaat :Ja

Certificaat van Deelname SOC-analist (CSA) – EC-Council – november 2023
Certificaat :Ja

Cambly Certificaat van Voltooiing (Engelse conversatie met native docenten) – Cambly Inc. – augustus 2023
Certificaat :Ja

Microsoft-gecertificeerde Oplossingsexpert – Smartpro Teknoloji – april 2023
Certificaat :Ja

Gecertificeerde Ethical Hacker (CEH) – EC-Council – december 2022
Certificaat :Ja

Splunk Installatie en SPL (SIEM) – Udemy – augustus 2022
Certificaat :Ja

Praktische Cyberbeveiliging en Ethical Hacking Training – Udemy – augustus 2022
Certificaat :Ja

Blauw Team: Incidentbehandelaar – Udemy – juni 2022
Certificaat :Ja

Basiscursus Beveiliging voor Cyberoperaties – Udemy – januari 2022
Certificaat :Ja

Malware-analyse Training – Bilişim Vadisi – november 2020
Certificaat :Ja

Netwerkpakket- en Protocolanalyse Training – Bilişim Vadisi – september 2020
Certificaat :Ja

5 Redenen om Detectie- en Responsoperaties uit te besteden – BrightTALK – april 2020
Certificaat :Ja

Computervaardigheden

Microsoft Office Programma's

Python

Java

Programmeertaal C

Linux

SQL

HTML5

CSS3

Arduino

Raspberry Pi

Talen

Turks (Moedertaal)

Engels (Vloeiend)

Nederlands (Beginnersniveau)

Hobby's en interesses

Een persoonlijke bibliotheek creëren

Poëzie en songteksten schrijven

Zwemmen

Hardlopen

Fitnessactiviteiten

Kickboksen

Voetbal