DUTCH EXPAT

CV

CAGRI

NETWERK BEVEILIGINGSINGENIEUR, SOC-ANALIST, SIEM , CYBERVEILIGHEID, KALI LINUX, SPLUNK, CISCO PRIME, FIREWALL, IBM SECURITY QRADAR, IDS/IPS

Dit CV wordt u aangeboden door Dutch Expat N.V.

Al onze CV's behoren tot hooggekwalificeerde kandidaten die woonachtig zijn in Turkije. Wilt u één van onze kandidaten in dienst nemen, dan zorgen wij door middel van de kennismigratieprocedure dat alle benodigde juridische en organisatorische stappen worden gezet om de betreffende kandidaat bij uw bedrijf aan het werk te krijgen. Dit geeft u toegang tot toptalenten van de Turkse arbeidsmarkt.

CAGRI

Woonplaats **Ankara**
Nationaliteit **Turkse**
Geboortedatum **17.04.1988**
Burgerlijke Staat **Ongehuwd**
Beroep/Functie **Cyber Security Specialist**
Web

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

NETWERK BEVEILIGINGSINGENIEUR, SOC-ANALIST, SIEM , CYBERVEILIGHEID, KALI LINUX, **SPLUNK,** CISCO PRIME, **FIREWALL,** IBM SECURITY QRADAR, IDS/IPS,

PERSOONLIJK PROFIEL

Graag maak ik mijn interesse kenbaar voor de functie van Cyberbeveiligingsanalist, zoals recentelijk door uw bedrijf geadverteerd. Met een solide achtergrond in het verbeteren van bedrijfsbeveiliging door middel van uitgebreide audits, proactief kwetsbaarheidsbeheer, diepgaande netwerkanalyse en het strategisch aanpassen van firewall-instellingen, ben ik ervan overtuigd een waardevolle bijdrage aan uw team te kunnen leveren.

In mijn laatste rol heb ik significante verbeteringen aangebracht in de systeembeveiliging door het implementeren van geavanceerde strategieën voor het beheer van kwetsbaarheden, wat leidde tot een substantiële vermindering van de risico's op beveiligingsincidenten. Mijn deskundigheid omvat ook het efficiënt beheren van SIEM-tools, waarmee ik een waakzame en proactieve benadering van bedreigingsdetectie en -respons garandeer.

Verder heb ik ruime ervaring in het leiden van de implementatie van robuuste VPN-oplossingen, inclusief IPSEC en SSL-VPN, wat mijn toewijding benadrukt om continu op de voorgrond te blijven binnen de technologische evolutie. Mijn ambitie om internationale ervaring op te doen en de culturele diversiteit te omarmen wordt versterkt door mijn wens om in Nederland te werken, waar ik de dynamiek van het zakelijke klimaat en de rijke culturele omgeving hoop te ervaren.

Ik kijk uit naar de mogelijkheid om mijn bijdrage en toewijding verder te bespreken tijdens een persoonlijk gesprek.

WERKERVARING

Netwerk Beveiligings Engineer

Luchtverkeersleidingscentrum Turkije (Ankara)

05-2023 / Heden

- VPN-configuratie en -beheer: 58 site-to-site IPsec VPN-tunnels opzetten tussen Cisco-routers van bijkantoren en gecentraliseerde FortiGate firewalls. SSL-VPN clients inschakelen om verbindingen op afstand mogelijk te maken.
- Netwerkbeveiliging en probleemoplossing: Nauwgezet analyseren van debug logs om problemen op te lossen zoals Anti-Replay fouten of crypto incompatibiliteiten, en snel bijwerken van configuraties aan beide uiteinden als dat nodig is. Fijn afstellen van object definities en policies op FortiGate 100D en 200F firewalls.
- Monitoring en diagnose: Het configureren van 'monitor capture' functionaliteit op Cisco 4400 series routers om pcap-bestanden te genereren en deze naadloos door te sturen naar een FTP-server voor gestroomlijnde procedures voor probleemoplossing. Verbeter de mogelijkheden voor logboekbeheer en onderzoek naar overtredingen, gebeurtenissen en stromen met IBM Security QRadar SIEM. Creëer de bijbehorende regels en controleer de dagelijkse alarmen.
- Beveiligingsaudits en compliance: Verhoog de systeembeveiliging door grondige ISO 27001 audits uit te voeren en de resultaten te rapporteren aan de burgerluchtvaart en overheidsinstanties.
- Vulnerability Management: Uitvoeren van kwetsbaarheidsscans met nmap en Nessus op de servers die naar het internet gaan om het aanvalsoppervlak te verkleinen.
- Samenwerking met overheidsinstanties: Samenwerken met het National CIRT om beter beschermd te zijn tegen tegenstanders door middel van door hen verzamelde informatie over bedreigingen.

SOC-analist

Siemens Energie (Karlsruhe)

03-2022 / 05-2023

- Logbeheer en monitoring: Implementeren van geavanceerde log collector setups voor onderdelen van energiecentrales, optimaliseren van gegevensoverdracht naar het AWS-platform. Proactief bewaken en onderzoeken van logboekwaarschuwingen van externe locaties, uitvoeren van uitgebreide logboek- en gebeurtenisanalyses van meerdere ICS-componenten. Uitgebreide loganalyse uitvoeren met behulp van geavanceerde tools zoals Elastic Stack (ELK).
- Communicatie en incidentbeheer: Beveiligingstickets genereren via Footprints en bevindingen meedelen aan klanten via Teams calls of e-mail.
- Netwerkbeveiliging: IPSEC-tunnels en RDP-verbindingen opzetten om beveiligingsproblemen van klanten snel op te lossen. Versterkte de beveiliging door ICS-firewalls te configureren, zoals de Scalance S-serie, ICS-netwerkcomponenten zoals RUGGEDCOM en SCALENCE-routers en -switches, om een meerlaagse verdediging te garanderen.
- Beveiligingsbeheer en automatisering: Beheerde en implementeerde beveiligingsconfiguraties bij Foreman en distribueerde deze naar componenten met Puppet. Application Whitelisting via McAfee ePolicy Orchestrator (ePO) binnen het netwerk van de klant geïmplementeerd.
- Vulnerability Management en antivirusoptimalisatie: Voerde grondige kwetsbaarheidsbeoordelingen uit met Tenable OT en SIESTA, waarbij gebruik werd gemaakt van Nessus voor uitgebreide inzichten. Optimaliseerde de TrendMicro en McAfee AV-configuraties van de klant om ervoor te zorgen dat deze up-to-date zijn via de nieuwste handtekeningupdates.

Netwerk Ingenieur

Algemeen Directoraat van de Staatsluchthavenautoriteit, DHMI (Ankara)

01-2015 / 03-2022

- Netwerkinstallatie en configuratie: Installeren van nieuwe VPLS, MPLS of TDM lijnen samen met de ISP. Inzet van voornamelijk Cisco-routers en -switches voor verschillende luchtvaartsystemen. Optimaliseren van IP-connectiviteit tussen meer dan 50 radar- en spraakstations in het hele land en het hubcentrum door GRE-tunnels te installeren. Configureerde verschillende netwerktechnologieën zoals HSRP, VRRP, toegangslijsten, VLAN's, STP op Cisco-apparaten.
- Netwerkmonitoring en probleemoplossing: Leidde uitgebreide monitoring van LAN- en WAN-verbindingen via SolarWinds en Cisco Prime. Luisterde en analyseerde het netwerk met Wireshark en tcpdump om de problemen op te lossen. Verzamelde pcap-bestanden voor verdere analyse.
- Operationeel netwerkbeheer: Werkte in dag-/nachtploegen om een naadloze werking van het netwerk te garanderen.
- Prestaties en verbeteringen: Oplossing voor een van de grootste netwerkproblemen in de burgerluchtvaart. De backbone routers vielen herhaaldelijk uit door hoog CPU-gebruik waardoor alle vluchtgegevens verloren gingen tijdens het luchtverkeersbeheer. Het probleem geïdentificeerd en aangeboden om OSPF hello timers vrij te geven naar een handiger niveau en dit heeft het probleem opgelost.

Professionele training

/ Heden

- Certified SOC Analyst (CSA) - EC-Council (22 oefenlabs).
- Gecertificeerd blauw team niveau 1 (BLT1) - Blauw team beveiliging.
- CompTIA Cyber Security Analyst - CySA+ (CS0-003) Complete cursus & oefenexamen.
- Fortinet Certified Associate - FortiGate 7.4 Operator Zelfstudie.
- ISO:IEC 27001:2022 Information Security System Management (ISMS) - Lead Auditor.
- Crowdstrike: Zero to Falcon Admin - Hailie Shaw.
- Splunk Core Certified Power User - Examenvoorbereiding - Hailie Shaw.
- Security Server (SeS3000) & drApS3000 Admin Training - Power Academy (Siemens Energy).
- SPPA-T3000 systeembasis - Power Academy (Siemens Energy).
- Certified Ethical Hacker (CEH)v10 - EC Council.
- Cyberincident Response Team - Barikat Academy.
- Offensieve beveiliging - Barikat Akademy.
- Cisco Certified Network Associate (CCNA R&S).
- Cisco Certified Network Professional (CCNP R&S).
- Certified AWS Solutions Architect - Associate - A Cloud Guru.
- Certified Incident Handler (ECIH) – EC Council (22 Practice Labs)

Technische vaardigheden

/ Heden

- Vaardigheden: Skills ISO/IEC 27001:2022; IEC 62443; MITRE ATT&CK Framework; NIST Cybersecurity Framework; Ethical Hacking; Vulnerability Analysis; Threat Intelligence; Digital Forensics; Phishing Analysis; Incident Response; Application Whitelisting; Endpoint Detection and Response (EDR); Security Information and Event Management (SIEM); Event log analysis; Malware analysis; Routing & Switching; Log Management; Network Analysis; Firewall Management; AWS Cloud Computing.
- Gereedschap: Splunk, Elastic Stack (ELK), IBM Security QRadar; Nessus, Nmap, Python, Tenable; NIDS, Snort; Crowdstrike Falcon EDR; Cortex XSOAR; Wireshark, tcpdump, Nagios, SolarWinds, Cisco Prime; Metasploit, Security Onion; FTK, KAPE, CyberChef, Autopsy, Volatility; Microsoft Defender 365, McAfee, TrendMicro; IDA Pro, OllyDebug; Confluence, Footprints, Jira.
- Protocollen: TCP/IP, SSH, telnet, RDP, FTP, IPSEC, SNMP, Syslog, Netflow, OSPF, HSRP, VRRP, EIGRP, MSTP, Siemens S7, PCS7, PROFINET.
- Firewall management: Fortigate 100D&200F, Sophos UTM, Cisco ASA, Scalance S series, RuggedCom (ROX II)

OPLEIDINGEN

2019 - 2021
Master - Wetenschap in cyberveiligheid
Technische Universiteit Midden-Oosten (Ankara)
Diploma: Ja

2006 - 2012
Bachelor - Ingenieur Elektronica en Communicatie
Suleyman Demirel Universiteit (Isparta)
Diploma: Ja

Cursussen

04/2024 -
Certified Incident Handler (ECIH) – EC Council
Certificaat :Ja

04/2024 -
IBM Professional Certified Plus – SOC Analyst
Certificaat :Ja

04/2024 -
IBM Certified Analyst –Security QRadar SIEM V7.5
Certificaat :Ja

03/2024 -
Certified SOC analyst (CSA)- EC-Council
Certificaat :Ja

02/2024 -
Splunk Core certified user (SPLK-1002)
Certificaat :Ja

01/2024 -
Certified Cybersecurity Analyst CompTIA (CySA+)
Certificaat :Ja

12/2023 -
Fortinet Certified Associate in Cybersecurity (FCA)
Certificaat :Ja

10/2023 -
Certified ISO/IEC 27001: 2022 Lead Auditor
Certificaat :Ja

11/2023 -
Crowdstrike Certified Falcon Administrator (CCFA-200)
Certificaat :Ja

10/2021 -
Certified Ethical Hacker (CEH)v10 - EC Council
Certificaat :Ja

08/2019 -
AWS Certified Solutions Architect - Associate (SAA)
Certificaat :Ja

-
Certified Blue Team Level 1 – Security Blue Team (24 hour Incident Response exam)
Certificaat :Ja

Computervaardigheden

AWS

Kali Linux

Python

Cisco ASA

SIEM

Talen

Engels (Vloeiend)

Turks (Moedertaal)

Hobby’s en interesses

Boeken lezen en het leven van auteurs bestuderen

Drummen

Tennis