Ville Järvinen

Kyberturvallisuusanalyytikko

Espoo, Suomi
ville.jarvinen@gmail.com
+358 44 345 6789
linkedin.com/in/villejarvinen

Profiili

Analyyttinen kyberturvallisuusanalyytikko, jolla on kuuden vuoden kokemus tietoturvauhkien havaitsemisesta, tutkinnasta ja reagoinnista SOC-ympäristöissä. Erikoistunut haittaohjelmien analysointiin, verkkoliikenteen anomalioiden tunnistamiseen ja tapahtumien tutkintaan. Olen kehittänyt useita SIEM-sääntöjä ja automaatioskriptejä, jotka ovat parantaneet uhkien havaitsemistarkkuutta merkittävästi. Minulle on tärkeää pysyä kehityksessä mukana jatkuvasti muuttuvassa uhkaympäristössä.

Kokemus

Kyberturvallisuusanalyytikko (Taso 2), Nokia, Espoo — *Jun 2021 – Nykyhetki*

Toimin globaalin SOC-tiimin tason 2 analyytikkona vastaten monimutkaisempien tietoturvatapausten tutkinnasta ja ratkaisemisesta.

- Tutkinut **yli 400** tietoturvapoikkeamaa vuodessa, joista 32 luokiteltu kriittisiksi ja ratkaistu alle neljässä tunnissa
- Kehittänyt 18 uutta SIEM-korrelaatiosääntöä (Microsoft Sentinel), joilla havaittu aiemmin tunnistamattomia uhkaprofiileja
- Luonut Python-automaatioskriptin IOC-tietojen rikastamiseen, joka lyhensi analysointiaikaa **40 %** tapausta kohti
- Pitänyt neljä sisäistä koulutusta phishing-kampanjoiden tunnistamisesta **yli 200** työntekijälle

SOC-analyytikko (Taso 1), Tietoevry, Helsinki — *Aug 2018 – May 2021*

Vastasin ensimmäisen tason hälytysten analysoinnista ja eskalaatiosta asiakkaan hallinnoidun tietoturvapalvelun (MSSP) SOC:issa.

- Käsitellyt keskimäärin **80 hälytystä** päivässä SLA-vaatimuksella alle 15 minuutin vasteaika, saavutettiin **97 %**
- Kehittänyt runbook-kirjaston 25 yleisimmälle tietoturvapoikkeamatyypille, joka otettiin koko tiimin käyttöön
- Osallistunut kahteen red team -harjoitukseen harjoitellen IR-prosesseja käytännössä

IT-tukihenkilö, Metropolia AMK, Helsinki — *Jul 2018 – Jul 2018*

Vastasin oppilaitoksen IT-infrastruktuurin ylläpidosta ja tietoturva-asetuksista opintojen ohessa.

- Ylläpitänyt **600+** käyttäjän Active Directory -ympäristöä ilman merkittäviä käyttökatkoksia
- Toteutanut verkon segmentoinnin projektin, joka paransi oppilaitosverkon tietoturvatasoa huomattavasti
- Dokumentoinut IT-ympäristön muutokset ja ylläpitänyt sisäistä tietopankkia **yli 50 artikkelilla**

Koulutus

Insinööri (AMK), pääaine Tietotekniikka, tietoverkot ja tietoturva, Metropolia AMK, Helsinki — *Sep 2014 – May 2018*

Suuntautuminen tietoturva. Opinnäytetyö: SIEM-järjestelmän käyttöönotto ja sääntöjen optimointi pk-yrityksessä.

Taidot

SIEM (Microsoft Sentinel, Splunk), Haittaohjelmien analyysi, Verkkoliikenteen analyysi (Wireshark), Incident Response, Threat Intelligence, MITRE ATT&CK -viitekehys, Python (tietoturva-automaatio), Tunkeutumistestauksen perusteet, Active Directory -tietoturva, Tietoturvalainsäädäntö (NIS2)

Sertifikaatit

CompTIA Security+, CompTIA — *Jan 2020*

Certified SOC Analyst (CSA), EC-Council — *Jan 2022*

Microsoft SC-200: Security Operations Analyst, Microsoft — *Jan 2023*

Kielet

Suomi (äidinkieli), Englanti (sujuva), Ruotsi (toimiva)

Projektit

Uhkatiedustelun automaatioalusta (sisäinen hanke) — *Sep 2022 – Jun 2023*

Suunnittelin ja toteutin Python-pohjaisen alustan, joka kerää ja korreloi uhkatiedustelutietoja useista lähteistä automaattisesti.

- **Integroitu 6 ulkoista threat feed -lähdettä** (MISP, AlienVault OTX, AbuseIPDB) yhdeksi kokonaisuudeksi
- Lyhensi IOC-tietojen analysointiaikaa **60 %** ja otettiin käyttöön koko SOC-tiimissä

Suositukset

Petri Lahtinen, SOC Manager, Nokia, petri.lahtinen@nokia.com, +358 40 551 2378