Erik Johansson

Cybersäkerhetsanalytiker

Stockholm, Sverige
erik.johansson@gmail.com
+46 73 789 01 23
linkedin.com/in/erikjohansson

Profil

Certifierad cybersäkerhetsanalytiker med sju års erfarenhet av säkerhetsövervakning, incidentrespons och hotanalys i kritisk infrastruktur och finanssektorn. Arbetar dagligen i SOC-miljö med analys av SIEM-larm, threat hunting och forensisk utredning av säkerhetshändelser. Dokumenterat bidrag till att reducera mean time to detect (MTTD) och mean time to respond (MTTR) med konkreta tekniska åtgärder. Söker en senior analytiker- eller teamledarroll med fokus på strategisk säkerhetsarkitektur.

Erfarenhet

Senior Security Analyst – SOC, Ericsson, Global Security Operations Center, Stockholm *Sep 2020 – Nuvarande*

Tier 3-analytiker i Ericssons globala SOC med ansvar för avancerade hot, forensik och incidentledning.

- Hanterat **över 120 säkerhetsincidenter** på Tier 3-nivå, varav 14 klassificerade som kritiska
- Reducerade MTTD med **38 %** genom att bygga och implementera nya SIEM-detektionsregler i Splunk Enterprise Security
- Ledde forensisk utredning av ett avancerat phishing-angrepp mot Ericssons leverantörsnätverk – **ansvarig för slutrapporten** presenterad för CISO och säkerhetsstyrelse
- Genomfört **40+ proaktiva threat hunting-kampanjer** per år med hjälp av MITRE ATT&CK-ramverket
- Mentor för två juniora analytiker i avancerad SIEM-analys och incidentrespons

Security Analyst – SOC, Handelsbanken, IT-säkerhet, Stockholm *Jan 2017 – Aug 2020*

Tier 2-analytiker i Handelsbankens interna SOC med ansvar för säkerhetsövervakning och initial incidentrespons.

- Övervakade och analyserade **ca 15 000 SIEM-händelser per dygn** med triagering, eskalering och dokumentation
- Bidrog till implementeringen av Microsoft Sentinel som primärt SIEM – minskade falsk positivrate med **52 %**
- Genomförde sårbarhetsscanningar med Qualys och Tenable och levererade åtgärdsrapporter till IT-förvaltning

Utbildning

MSc Informationssäkerhet i Nätverkssäkerhet och kryptografi, KTH (Kungliga Tekniska högskolan), Stockholm *Aug 2015 – Jun 2017*

Tvåårigt masterprogram med specialisering mot nätverkssäkerhet, intrångsdetektion och kryptografiska protokoll. **Exjobb betygsatt till A** om detektering av C2-trafik i krypterade nätverksflöden.

BSc Datateknik i Datateknik, KTH (Kungliga Tekniska högskolan), Stockholm *Aug 2012 – Jun 2015*

Kompetenser

SIEM, Splunk Enterprise Security och Microsoft Sentinel, Incidentrespons och forensisk analys, Threat hunting (MITRE ATT&CK), Nätverksanalys, Wireshark, Zeek, Sårbarhetsskanning, Qualys, Tenable, EDR, CrowdStrike Falcon, Phishing-analys och e-postforensik, Malware-analys (statisk och dynamisk), Python-skript för säkerhetsautomation, ISO 27001 och NIS-direktivet

Certifieringar

CISSP, Certified Information Systems Security Professional, ISC² *Jun 2022 – Jun 2022*

GIAC Certified Enterprise Defender (GCED), GIAC *Mar 2021 – Mar 2021*

Splunk Core Certified Power User, Splunk *Nov 2020 – Nov 2020*

Språk

Svenska (modersmål), Engelska (flytande)

Projekt

Utvecklade och implementerade **85 nya detektionsregler** i Splunk Enterprise Security baserade på MITRE ATT&CK. Projektet reducerade MTTD med 38 % för avancerade hotaktörer.

Referenser

Stefan Karlsson, Head of Security Operations, Ericsson, stefan.karlsson@ericsson.com, +46 73 789 01 23

Fritidsaktivitet

CTF-tävlare, Hack the Box och SANS Holiday Hack Challenge *Jan 2018*

Regelbunden deltagare i capture-the-flag-tävlingar, med placering i **topp 5 % av globalt deltagarfält** i SANS Holiday Hack 2023.