Belgium Jobs Expertini®

SOC Analyst

Apply Now

Company: Cegeka

Location: Hasselt

Category: computer-and-mathematical

Beschrijving

Do you want to be a part of one of the fastest-growing and largest security operations centers in Europe? Do you have a passion for Cyber Security, especially advanced Managed Detection & Response (MDR)? Does incident response, digital forensics, threat hunting, threat intelligence and everything related to Cyber Security feel like second nature to you? Are you a Cyber Defender at heart, driven to strengthen the blue team and help organizations under attack? If you answered yes to all of these questions, then you might be the perfect fit for our CSIRT Analyst role!

You handle security alerts/incidents that have been escalated by the SOC Analysts (Tier 2)

You will handle security alerts and incidents together with your team

You do DFIR assignments, including DFIR readiness assessments

You participate in the weekly Threat Hunting duty to proactively chase threats through novel Tools, Techniques & Procedures (TTPs)

You will perform compromise assessments to identify potential compromises and their scope

You collect Threat Intelligence (IOCs and TTPs)

You will contribute to the Detection Engineering in SIEM, xDR, …

Together with the Red Team you will do Purple Teaming exercises to test and improve the defense

You contribute to the creation of a scenario in SOAR

You will co-write processes and procedures related to DFIR, Threat Intell, Threat Hunting,

…

You will be part of our incident response on call service.

Domein

IT

Ervaringsniveau

3-5 jaar

Locatie

Deze job kan op afstand uitgevoerd worden (bv. Thuiswerk,…)

Vaardigheden

You have at least 3-5 years of experience in a similar position

You have a bachelor or master degree or equivalent through experience

You have a hands-on and proactive mindset with a ‘can do’ mentality

You have experience and/or interest in working with the following MDR tools: EDR (CrowdStrike Falcon, MS Defender for Endpoint, Sentinel One, …), NDR (Vectra, Darktrace, …), xDR (CrowdStrike Identity Protection, MS Defender for Office/Clouds Apps/Identity/…)

As an analyst or engineer, you already have a good knowledge of Security Monitoring with SIEM technologies

You are passionate about the following security capabilities: Security Monitoring, Digital Forensics, Incident Response, Threat Intelligence, Threat Hunting, …

You speak fluently Dutch and English.

Ons aanbod

At Cegeka, you’ll be part of a certified Top Employer with over 150 Security professionals. To stay ahead in the ever-evolving Cyber Security world, you can participate in our Security Academy: 13 role-based learning paths, including certifications from technology providers such as Fortinet, CrowdStrike, Vectra, Cisco, Microsoft, CyberArk, Splunk, Tenable, and topics like Security Consultancy, Security Operations, and Identity & Access Management.

Cegeka consistently proves its reliability and leadership in IT services, ranking first for Security/Hosting and an impressive second place for digital transformation in the Whitelane Research year after year.

We ask a lot from you, but in return, you’ll receive a lot! Competencies and character are essential to us, alongside experience and ambitions. Cegeka continually invests in talent management to help every employee realize their potential.

You'll receive a competitive salary complemented with extra-legal benefits. Choose between an electric car with a charging pass or a mobility budget, meal vouchers, eco vouchers, a compelling group and hospitalization insurance, a mobile phone subscription, a fixed expense allowance, a powerful laptop, and the opportunity to personalize your salary package with our Flex Reward Plan.

Enjoy flexible work hours and a healthy work/life balance

Be a part of a top team where new fresh ideas and initiatives are always welcome! Team events, monthly happy hours, and an always memorable company party are part of the experience.

Apply Now

Cross References and Citations:

1. SOC AnalystChefjobsnearme Jobs HasseltChefjobsnearme ↗

2. SOC AnalystSearchlondonjobs Jobs HasseltSearchlondonjobs ↗

3. SOC AnalystDirectorjobs Jobs HasseltDirectorjobs ↗

4. SOC AnalystInteriordesignjobs Jobs HasseltInteriordesignjobs ↗

5. SOC AnalystCeojobs Jobs HasseltCeojobs ↗

6. SOC AnalystDevopsjobs Jobs HasseltDevopsjobs ↗

7. SOC AnalystUnitedkingdomjobs Jobs HasseltUnitedkingdomjobs ↗

8. SOC AnalystLegaljobs Jobs HasseltLegaljobs ↗

9. SOC AnalystSearchnzjobs Jobs HasseltSearchnzjobs ↗

10. SOC Analyst Nzjobscentral Jobs HasseltNzjobscentral ↗

11. SOC Analyst SchoolcounselorjobsJobs HasseltSchoolcounselorjobs ↗

12. SOC Analyst Developerjobs Jobs HasseltDeveloperjobs ↗

13. SOC Analyst UruguayjobsJobs HasseltUruguayjobs ↗

14. SOC Analyst Mumbaijobs Jobs HasseltMumbaijobs ↗

15. SOC Analyst Oilandgasjobs Jobs HasseltOilandgasjobs ↗

16. SOC Analyst MoscowjobsJobs HasseltMoscowjobs ↗

17. SOC Analyst Jobssearch Jobs HasseltJobssearch ↗

18. **SOC Analyst Austinjobs Jobs Hasselt Austinjobs ↗**
19. **Soc analyst Jobs Hasselt ↗**
20. **AMP Version of Soc analyst ↗**
21. **Soc analyst Hasselt Jobs ↗**
22. **Soc analyst Jobs Hasselt ↗**
23. **Soc analyst Job Search ↗**
24. **Soc analyst Search ↗**
25. **Soc analyst Find Jobs ↗**