Turkey Jobs Expertini®

Cyber Defence Expert - Incident Response

Apply Now

Company: Vodafone

Location: Istanbul

Category: other-general

What you'll do

• Having a strong security analyst mindset and using best practice knowledge from an attackers point of view to detect, identify and respond to cyber events, known and unknown threats, security risks and vulnerabilities with effective management of response plans, across the security platform lifecycle in line with cyber security policies and procedures,

• Continuous log review for several types of assets and actions (active directory, database, applications, network, OS, user behavior etc.) in accordance with requirements defined by the governance team and required standards / regulations like PCI-DSS, ISO27001, KVKK, GDPR, SOX etc.

• Strong hands on experience and technical knowledge on at least one of these tools / activities; EDR, NDR, SOAR, UEBA, SIEM, sandboxes, malware / forensic analysis, threat hunting and vulnerability scanning,

• Becoming an active contributor to SIEM and SOAR systems' content development, security orchestration and playbook implementation processes to improve overall cyber defence center detection and incident response capability,

• Strong understanding skills & technical abilities regarding MITRE attack framework ATT&CK,

• Integration of threat intelligence sources with SIEM and evaluation of alerts,

• Continuous attack simulation studies and defining new rules /correlations related with the output,

• Attending internal and external audits and preparing evidence when required,

• Effective reporting of log review and incident management activities on both executive and

technical level.

• Having at least one of these certifications will be a plus; Security+, ECIH, GCDA, GDAT, CCNA, CCNP, CISSP.

Who you are

• BSc. in Computer / Industrial / Electrical & Electronics Engineering is desired,

• Master's degree (preferably in Computer Science & Cyber Security) or equivalent information security experience is desired,

• At least 4 years hands on experience in information security, network administration,

• Experience working in complex operational ICT environments,

• Solid knowledge of security principles and practices,

• Proven experience in the following topics are desired:

Firewall and intrusion detection/prevention protocols,

DLP, anti-virus, anti-malware EDR solutions,

Sandboxing and Malware analysis

DFIR concepts

TCP/IP, computer networking, routing and switching,

Windows, UNIX and Linux operating systems,

Network protocols and packet analysis,

Python, Go, Bash or any other programming/scripting language knowledge

Cloud computing,

SaaS models,

Security Information and Event Management (SIEM)

• Excellent problem-solving and analytical skills

• Critical thinking with strong attention to details and follow up

• Technically competent to contribute towards the preparation and implementation of control processes, procedures and guidelines

• Advanced in English

Apply Now

Cross References and Citations:

1. Cyber Defence Expert - Incident ResponseKarachijobs Jobs Istanbul Karachijobs ↗
2. Cyber Defence Expert - Incident ResponseFresherjobs Jobs Istanbul Fresherjobs ↗
3. Cyber Defence Expert - Incident ResponseLuxuryjobs Jobs Istanbul Luxuryjobs ↗
4. Cyber Defence Expert - Incident ResponseMechanicaljobs Jobs Istanbul Mechanicaljobs ↗
5. Cyber Defence Expert - Incident ResponseTradingjobs Jobs Istanbul Tradingjobs ↗
6. Cyber Defence Expert - Incident ResponseFree-hiringJobs Istanbul Free-hiring↗
7. Cyber Defence Expert - Incident ResponseKazakhstanjobs Jobs Istanbul Kazakhstanjobs ↗
8. Cyber Defence Expert - Incident ResponseTherapistjobs Jobs Istanbul Therapistjobs ↗
9. Cyber Defence Expert - Incident ResponseJobsinsaudiarabia Jobs Istanbul Jobsinsaudiarabia ↗
10. Cyber Defence Expert - Incident Response Jobsinindia Jobs Istanbul Jobsinindia ↗
11. Cyber Defence Expert - Incident Response Searchnzjobs Jobs Istanbul Searchnzjobs
12. Cyber Defence Expert - Incident Response StartupjobsnearmeJobs Istanbul Startupjobsnearme↗
13. Cyber Defence Expert - Incident Response Washingtondcjobs Jobs Istanbul Washingtondcjobs↗
14. Cyber Defence Expert - Incident Response Spainjobs Jobs Istanbul Spainjobs ↗
15. Cyber Defence Expert - Incident Response MathematicsjobsJobs Istanbul Mathematicsjobs↗
16. Cyber Defence Expert - Incident Response AgilejobsnearmeJobs Istanbul Agilejobsnearme↗
17. Cyber Defence Expert - Incident Response Europejoblistings Jobs Istanbul Europejoblistings ↗
18. Cyber Defence Expert - Incident Response Phoenixjobs Jobs Istanbul Phoenixjobs↗
19. Cyber defence expert - incident response Jobs Istanbul ↗

20. **AMP Version of Cyber defence expert - incident response ↗**
21. **Cyber defence expert - incident response Istanbul Jobs ↗**
22. **Cyber defence expert - incident response Jobs Istanbul ↗**
23. **Cyber defence expert - incident response Job Search ↗**
24. **Cyber defence expert - incident response Search ↗**
25. **Cyber defence expert - incident response Find Jobs ↗**