Israel Jobs Expertini®

Mid/Sr Security Engineer (Detection and Response)

Apply Now

Company: Incode

Location: Israel

Category: other-general

REIMAGINE TRUST Incode is the leading provider of world-class identity solutions that is reinventing the way humans authenticate and verify their identities online to power a world of digital trust. Through our revolutionary identity solutions, we are unleashing the business potential of universal industries including finance, government, retail, hospitality, gaming and more, by reducing fraud and transforming human interactions with data, products, and services. We’re in the process of rapidly scaling our diverse global team and we’re looking for entrepreneurial individuals and leaders who are curious, driven, and excited by ownership to join a Unicorn-status scale-up! The Opportunity We seek a trustworthy and proactive Mid/SR Security Engineer as a technical thought leader and driver of holistic security operations across Incode. As an early security hire at Incode, you will work across the security operations lifecycle for detection engineering and incident response, influence the security operations program development, and be the first line of defense through assessing threats, collecting and analyzing data, and responding to abnormal activities and events. In close collaboration with our security team members, the compliance team, the SRE team, and product engineering teams, we share the responsibility to identify, protect, detect, respond, and recover from cyber threats. <span

data-contrast="none">If you are a hands-on Security Engineer passionate about building high-signal detection strategies, conducting threat-hunting exercises, automating and enriching events, and leading our first line of defense across our corporate and product at Incode, we would love to chat with you. This is an exciting opportunity to shape and build security operations and influence our overall security strategy. Responsibilities <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Be the first line of defense to protect, detect, respond to, and recover from cyber-attacks in both our corporate and product environments. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Develop and run tools to gather security telemetry data from cloud production systems. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Automate workflows and improve identification and response time for security events. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Build and optimize high signal detections with enriched data and orchestration. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="

{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Define and improve
processes, procedures, and technologies used for detection and response.<span
data-ccp-props="{}"> <li data-leveltext=" " data-font="Symbol" data-
listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Develop runbooks
and incident playbooks for new and existing detections and influence our security
operations roadmap. <li data-
leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Lead threat hunting
practices, suggest product and infrastructure signals to surface attacks and incorporate
findings into security controls. <li
data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Research attacker
tactics, techniques, and procedures (TTPs) and craft detections to quickly identify and contain
potential security threats. <li
data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Respond to security
events, triage, perform investigations, incident analysis, and communicate clearly and
efficiently with partners. <li data-
leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Participate in an on-

call rotation. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697" data-aria-posinset="1" data-aria-level="1">Onboard new systems and services to SIEM and SOAR and build new detection pipelines. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697" data-aria-posinset="1" data-aria-level="1">Facilitate incident response processes and tabletop exercises. Qualifications: <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697" data-aria-posinset="1" data-aria-level="1">Experience as a security engineer, including security monitoring, detection engineering, incident response, and threat hunting in a SaaS company <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697" data-aria-posinset="1" data-aria-level="1">Practical understanding of common attacks, adversary tactics, techniques, and procedures (TTPs) and MITRE ATT&CK principles <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697" data-aria-posinset="1" data-aria-level="1">Operating systems internals and forensics experience for macOS, Windows & Linux <li data-leveltext=" " data-font="Symbol" data-

listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Domain experience
managing and working with current SIEM and SOAR platforms, DLP, email security
platforms, endpoint protection platforms, secure service edge, etc.<span data-
ccp-props="{}"> <li data-leveltext=" " data-font="Symbol" data-
listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Experience
developing tools and automation using common DevOps toolsets and programming
languages <li data-leveltext=" "
data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Understanding of
malware functionality and persistence mechanisms<span data-ccp-props="
{}"> <li data-leveltext=" " data-font="Symbol" data-listid="1" data-
list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Ability to analyze
endpoint, network, and application logs for anomalous events<span data-ccp-
props="{}"> <li data-leveltext=" " data-font="Symbol" data-listid="1"
data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Proficiency in
programming in Golang or Python
<li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697

data-aria-posinset="1" data-aria-level="1">Excellent collaborative skills <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Outstanding written and verbal communication Preferred Experience and Certification: <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">SaaS Startup experience in security focused industries, such as fintech, security software and services, healthtech, identity and access management. <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Hands-on experience with data analysis, modeling, and correlation at scale <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Familiarity in continuous integration and Infrastructure as Code <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="{"335552541":1,"335559685":720,"335559991":360,"46976[8226],"469777803":"left","469777804":" ","4697 data-aria-posinset="1" data-aria-level="1">Experience designing, and optimizing high throughput ETL pipelines<span data-ccp-props="

{}"> <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Possess a breadth of knowledge and experience across the information security domain, such as endpoint security, cloud security, application security, or automation <li data-leveltext=" " data-font="Symbol" data-listid="1" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Experience as a software engineer, infrastructure engineer, or site reliability engineer <span data-ccp-props="
{"134245417":false}"> <li data-leveltext=" " data-font="Symbol" data-listid="11" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Experience detecting or responding to threats in Kubernetes (K8s), AWS, and Linux environments
 <li data-leveltext=" " data-font="Symbol" data-listid="11" data-list-defn-props="
{"335552541":1,"335559685":720,"335559991":360,"46976
[8226],"469777803":"left","469777804":" ","4697
data-aria-posinset="1" data-aria-level="1">Certifications in Security, Incident Handling, Forensics, and/or Offensive Security (<span data-ccp-

parastyle="Body Text">eg. CERT-CSIH, GCIH, GCIA, GCFA, Security+, ECIH, GX-IH, OSCP, GPEN, CEH, CISSP etc). 8 Aspects of our Culture: Values are what we value
High performance
Freedom & responsibility
Context, not control
Highly aligned, loosely coupled
Continuous Feedback
Pay Top of Market
Promotions & Development
Learn more about Life at Incode<u>!</u> Benefits & Perks: Meaningful Equity
Flexible Working Hours & Workplace
Open Vacation Policy
Wellness Program
International Travel Opportunities
Additional benefit package according to location (401k, medical insurance, etc.)   Equal Opportunities: Incode is an equal opportunity employer, committed to creating a diverse and inclusive work environment. We take great pride in having an inclusive, diverse, and global team and are always on the lookout for talented, passionate people from all backgrounds and walks of life. Applicant Data Privacy: We will only use your personal information in connection with Incode’s application, recruitment, and hiring processes.

Apply Now

Cross References and Citations:

1. Mid/Sr Security Engineer (Detection and Response) Seouljobs Jobs Israel Seouljobs ↗

2. Mid/Sr Security Engineer (Detection and Response) Supplychainjobs Jobs Israel Supplychainjobs ↗

3. Mid/Sr Security Engineer (Detection and Response) Ecologyjobs Jobs Israel Ecologyjobs ↗

4. Mid/Sr Security Engineer (Detection and Response) Agilejobsnearme Jobs Israel Agilejobsnearme ↗

5. Mid/Sr Security Engineer (Detection and Response) Entertainmentjobsnearme Jobs Israel Entertainmentjobsnearme ↗

6. Mid/Sr Security Engineer (Detection and Response) Firefighterjobsnearme Jobs Israel Firefighterjobsnearme ↗

7. Mid/Sr Security Engineer (Detection and Response) Taiwanjobs Jobs Israel Taiwanjobs ↗

8. Mid/Sr Security Engineer (Detection and Response) Searchlondonjobs Jobs Israel Searchlondonjobs ↗

9. Mid/Sr Security Engineer (Detection and Response) Fitnessjobs Jobs Israel Fitnessjobs ↗

10. Mid/Sr Security Engineer (Detection and Response) Techgiantcareers Jobs Israel Techgiantcareers ↗

11. Mid/Sr Security Engineer (Detection and Response) Govcareer Jobs Israel Govcareer ↗

12. Mid/Sr Security Engineer (Detection and Response) Videoplatformjoblistings Jobs Israel Videoplatformjoblistings ↗

13. Mid/Sr Security Engineer (Detection and Response) Psychiatristjobsnearme Jobs Israel Psychiatristjobsnearme ↗

14. Mid/Sr Security Engineer (Detection and Response) Findpythonjobs Jobs Israel Findpythonjobs ↗

15. Mid/Sr Security Engineer (Detection and Response) Devopsjobs Jobs Israel Devopsjobs ↗

16. Mid/Sr Security Engineer (Detection and Response) Presidentjobs Jobs Israel Presidentjobs ↗

17. Mid/Sr Security Engineer (Detection and Response) Jeddahjobs Jobs Israel Jeddahjobs ↗

18. Mid/Sr Security Engineer (Detection and Response) Professionalnetworkjobs Jobs Israel Professionalnetworkjobs ↗

19. Mid/sr security engineer (detection and response) Jobs Israel ↗

20. AMP Version of Mid/sr security engineer (detection and response) ↗

21. **Mid/sr security engineer (detection and response) Israel Jobs ↗**
22. **Mid/sr security engineer (detection and response) Jobs Israel ↗**
23. **Mid/sr security engineer (detection and response) Job Search ↗**
24. **Mid/sr security engineer (detection and response) Search ↗**
25. **Mid/sr security engineer (detection and response) Find Jobs ↗**