דרוש/ה מומחה/ית Splunk להשתלבות
בפרויקטים מאתגרים ומעניינים בארה"ב
(העבודה תתבצע מישראל)

כחלק מצוות לניהול והתמודדות עם איומי סייבר נדרש/ת מומחה/ית
Splunk, לסיוע ללקוחות EY לנהל ולהתמודד עם מגוון איומי סייבר על
בסיס פיתוח בסביבת Splunk.

דרישות התפקיד:

- פסיון בפיתוח בסביבת Splunk
- אנגלית ברמה גבוהה
- יחסי אנוש מעולים, יכולת עבודה עצמאית ובצוות
- פסיון בניהול והתמודדות עם איומי סייבר (יתרון)
- הבנה בפרוטוקולי תקשורת, מערכות הפעלה, טכנולוגיות אבטחת מידע (יתרון)
- פסיון בפיתוח וכתיבת קוד ב-Java, Python, JavaScript, Perl, Shell C (יתרון)
- פסיון ב-SQL (יתרון)

לשליחת קו"ח: noy.dar@iLey.com

* המשרה מיועדת לנשים ולגברים כאחד.
* המשרה מתאימה גם לעובדים/ות עם מוגבלות.

Splunk Expert

In a rapidly changing IT environment, clients from all industries (USA) look to us for trusted solutions for their increasingly complex risks and vulnerabilities. As a member of our Cyber Threat Management team you'll be right at the heart of that goal, helping clients gain insight and context to their cyber threats and assessing, improving, and building security operations in order to mitigate these threats.

The opportunity
Cyber threats, social media, massive data storage, privacy requirements and continuity of the business as usual require heavy information security measures. As an information security specialist, you will lead the implementation of security solutions for our clients in the USA and support the clients in their desire to protect the business. You will belong to an international connected team of specialists helping our clients with their most complex information security needs and contributing toward their business resilience. You will be working with our Advanced Security Centers to access the most sophisticated tools available to fight against cybercrime. Our professionals work together in planning, pursuing, delivering and managing engagements to assess, improve, build, and in some cases operate integrated security operations for our clients.

To qualify for the role you must have

- A related work experience with information security systems with hands-on Splunk technical infrastructure and implementation experience (Splunk certification is a plus).

- Knowledge of general security concepts and methods such as vulnerability assessments, privacy assessments, intrusion detection, incident response, security policy creation, enterprise security strategies, architectures, and governance.
- Proficiency in English.
- Excellent interpersonal skills, ability to work independently and in a team.

Ideally, you'll also have

- Understanding of networking (TCP/IP, OSI model), operating system fundamentals (Windows, UNIX, mainframe), security technologies (firewalls, IDS/IPS, etc.) and application programming/scripting languages (C, Java, Perl, Shell).
- Experience in process definition, workflow design and process mapping.
- Familiarity with other SIEM products (QRadar, LogRhythm).

Join us in building a better working world. Apply today- Noy.dar@il.ey.com