IT Automation

https://itautomation.com/?post_type=jobs&p=3527

User and Entity Behavior Analytics (UEBA) Analyst

Description

IT Automation LLC is seeking an experienced and highly motivated UEBA Analyst to support the development, implementation, and ongoing management of User and Entity Behavior Analytics solutions within our enterprise security environment. The ideal candidate will possess a solid background in cybersecurity and demonstrate expertise in behavioral analytics technologies to proactively detect and respond to anomalous activity, insider threats, and advanced persistent threats.

Responsibilities

- Implement and maintain UEBA platforms to monitor and analyze user and system behaviors.
- Develop and refine detection rules, baselines, and behavioral use cases aligned with evolving threat models.
- Investigate alerts generated by UEBA systems and collaborate with incident response teams to ensure timely resolution.
- Integrate UEBA solutions with other security tools, such as SIEM platforms, for enhanced threat visibility.
- Tune analytics models to minimize false positives and improve detection efficacy.
- Prepare detailed documentation, reports, and dashboards to support security operations and compliance requirements.
- Partner with cybersecurity, IT, and compliance teams to develop behavior-based detection strategies.
- Maintain knowledge of the latest threats, vulnerabilities, and technology trends in behavioral analytics and cybersecurity.

Qualifications

- Education: Bachelor’s degree in Cybersecurity, Information Technology, Computer Science, or a related field.
- Experience: Minimum 3 years of professional experience in cybersecurity; at least 1 year of direct experience with UEBA platforms.

Technical Skills:

- Proficiency with UEBA solutions such as Splunk UBA, Securonix, Exabeam, or Microsoft Sentinel.
- Strong understanding of behavioral analytics, insider threat detection, and user risk scoring.
- Experience working with SIEM tools and integrating UEBA data sources (e.g., Active Directory, VPN, endpoint logs).
- Familiarity with data analysis and scripting tools (e.g., Python, PowerShell) is an advantage.

Soft Skills:

- Strong analytical and critical thinking capabilities.
- Excellent verbal and written communication skills.
- Ability to work both independently and collaboratively in a fast-paced environment.

Hiring organization
IT Automation LLC

Employment Type
Full-time

Beginning of employment
Immediate

Duration of employment
12+ Months

Industry
Westchester County, NYS

Job Location
10551, New York, New York, USA

Working Hours
8:30 AM – 5:00 PM EST

Base Salary
$ 75,000 - $ 90,000

Date posted
March 28, 2025

Valid through
30.04.2025

Certifications (Preferred):

- CompTIA Security+, CEH, GIAC, or other recognized cybersecurity certifications.

Job Benefits

- 401(k) Retirement Plan
- Comprehensive Health, Vision, and Dental Insurance
- Annual Performance Reviews & Employee Recognition Bonuses
- Ongoing Training & Professional Development Opportunities

Contacts

- Email: info@itautomation.com
- Phone # 919-249-6373 (Work)