SOC Analyst

Introduction

At IBM, work is more than a job - it's a calling: To build. To design. To code. To consult. To think along with clients and sell. To make markets. To invent. To collaborate. Not just to do something better, but to attempt things you've never thought possible. Are you ready to lead in this new era of technology and solve some of the world's most challenging problems? If so, lets talk.

Your Role and Responsibilities

· Review the ServiceNow platform for security incidents escalated by Security Desk Analysts,
· Support handling of incidents in an advanced level according to Customer
· Upgrade or downgrade priority assigned by Security Desk
· Conduct secondary triage and analysis on escalated events and initial remediation for escalated incidents
· Perform containment, eradication and recovery actions as defined in the customer Playbooks and according to the assigned responsibilities and authorization
· Use Qualys Vulnerability Scanner and perimeter IDPS solutions for additional triage according to Playbooks and assigned authorization
· Raise requests to appropriate customer IT and Security administrators for actions to be taken on other customer's tools and solutions according to Playbooks
· Drive internal and external communication
· Track the progress on incidents that have been re-assigned or submitted to other teams
· Review events in the environment based on the information gathered during analysis to determine if an incident needs to be created or append to existing ticket according to customer policies and processes
· Providing service in 24/7 shifts (at night and weekends as well)

Find more about IBM Security Jobs:
http://www-03.ibm.com/employment/security/

Required Technical and Professional Expertise

Effective written communication
Process and Procedure adherence
General network knowledge, TCP/IP Troubleshooting
Ability to trace down an endpoint on the network based on ticket information
Familiarity with system log information and what it means
Understanding of common network services (web, mail, DNS, authentication)
Understanding of host based security tools such as Anti-malware, and EDR
General Desktop OS and Server OS knowledge
TCP/IP, Internet Routing, UNIX / LINUX & Windows
Strong analytical and problem solving skills

Preferred Technical and Professional Expertise

previous SOC experience

What we can offer:

Competitive salary
Health/insurance related benefits (private health insurance, pension plan contribution, life insurance)
Flexible benefit elements (SZÉP card, School Support, Local Travel Pass)
Commuting and relocation support
Special discounts with IBM card
International environment
Development and career opportunities

Location: Budapest
We are looking forward to reading your CV. Please send your application if you are interested in it:
https://ibm.biz/Bdffjs