Տեղեկատվական անվտանգության իրադարձությունների մոնիթորինգի և միջադեպերի արձագանքման բաժնի գլխավոր մասնագետ

Աշխատանքի նկարագրություն

Տեղեկատվական անվտանգության միջադեպերի հայտնաբերման և վերլուծության ապահովում:

Աշխատանքային պարտականություններ

- Արձանագրված տվյալների հիման վրա միջադեպերի հնարավոր աղբյուրների ուսումնասիրություն
- SIEM-ի հետ ինտեգրման պահանջների նախապատրաստում
- Տեղեկատվական անվտանգության միջադեպերի հայտնաբերման կանոնների/գործողությունների ձեռնարկների (playbook) մշակում, ճշգրտում
- SIEM–ում տեղեկատվական անվտանգության միջադեպերի վերլուծություն
- Միջադեպերին արձագանքման՝ կրկնվող, մեծ քանակությամբ նմանատիպ, ամենօրյա գործողությունների ավտոմատացում
- Տեղեկատվության պաշտպանության հետ կապված արտակարգ իրավիճակներում և ճգնաժամերի դեպքում մասնակցություն ճգնաժամի կառավարման գործընթացին
- Արդյունավետ մոնիթորինգի կազմակերպման նպատակով պաշտպանվող օբյեկտի ենթակառուցվածքում իրադարձությունների աղբյուրների և անհրաժեշտ ֆիլտրերի կարգաբերումների որոշում
- Տեղեկատվական անվտանգության կառավարման համակարգի աուդիտն իրականացրած կազմակերպության հաշվետվությունների ուսումնասիրություն և արձանագրված թերությունների վերացմանն ուղղված միջոցառումների իրականացում

Անհրաժեշտ պահանջներ

- Բարձրագույն տեխնիկական կրթություն (մագիստրոսի կամ բակալավի աստիճան)՝ տեղեկատվական տեխնոլոգիաներ (նախընտրելի է ցանցային անվտանգություն,

համակարգչային ցանցեր), կիրառական մաթեմատիկա, մաթեմատիկա, ռադիոֆիզիկա, ֆիզիկա

- Առնվազն 5 տարվա աշխատանքային փորձ տեղեկատվական համակարգերի և ցանցերի անվտանգության ոլորտում
- SIEM-ի հետ աշխատելու փորձ (Splunk, Micro Focus (HP) ArcSight, IBM QRadar, McAfee ESM, MaxPatrol և այլն)
- Linux Server/Windows Server-ների հետ աշխատանքի փորձ
- Տվյալների կառավարման հենքերի (СУБД) հետ աշխատելու փորձ (MS SQL/ORACLE/ PostgreSQL)
- Անվտանգության սկաներների (nmap, nessus և այլն) օգտագործման փորձ
- Հարձակումների հայտնաբերման համակարգերի (IDS\IPS, HIDS\HIPS) հետ աշխատանքի փորձ
- ՏԱ մոնիթորինգի կամ ՏԱ իրադարձությունների հետաքննության աշխատանքային փորձ
- Ենթակառուցվածքային սերվիսների (DNS/DHCP/AD/NTP/SMTP, հիպերվիզորներ, մոնիթորինգի և պահուստավորման համակարգեր, պահուստային կրկնօրինակման համակարգեր, CMDB և այլն) իմացություն
- Հաճախորդ-սերվեր համակարգերի աշխատանքային գործընթացների իմացություն
- Բիզնես պահանջների հիման վրա տեխնիկական առաջադրանք կազմելու հմտություններ
- Իրադարձությունների հավաքագրման մեխանիզմները (SQL (PL), API (RestFull API), XML, Syslog, SNMP, OPSEC, JSON, SCP (SSH), FTP)) ցանկալի է
- SIEM-ի հետ ինտեգրման փորձը ցանկալի է
- Ռուսերեն և անգլերեն լեզուների տիրապետում

Դիմելու ընթացակարգը

Ներկայացված պահանջներին համապատասխանող թեկնածուները կարող են ուղարկել իրենց ինքնակենսագրականը hr@armbusinessbank.am հասցեին:

Վերջնաժամկետ՝ 16.06.2023թ.:

Խնդրում ենք նամակի թեմա (subject) դաշտը լրացնել նշելով պաշտոնը և Ձեր անուն, ազգանունը հետևյալ կերպ՝ "Chief specialist of Information Security - Name, Surname":