

Տեղեկատվական անվտանգության իրադարձությունների մոնիթորինգի և միջադեպերի արձագանքման բաժնի առաջատար մասնագետ

Աշխատանքի նկարագրություն

Տեղեկատվական անվտանգության իրադարձությունների վերլուծություն:

Աշխատանքային պարտականություններ

- Պաշտպանվող օբյեկտի ենթակառուցվածքում իրադարձությունների աղբյուրներից ստացված տվյալների վերլուծություն, շեղումների ՏԱ հնարավոր միջադեպերի հայտնաբերում
- ՏԱ միջադեպերի ըստ առաջնահերթության, կարևորության և վնասակարության դասակարգում
- Իրադարձությունների մոնիթորինգի և կորելացիայի համակարգերի համար կանոնների մշակում, առկա կանոնների լրամշակում և կատարելագործում
- Պաշտպանվող օբյեկտի ենթակառուցվածքի և համակարգերում առկա գործընթացների վերլուծություն և կոնկրետ ենթակառուցվածքին համապատասխան՝ ճշգրիտ կարգաբերում
- Արդյունավետ մոնիթորինգի կազմակերպման նպատակով պաշտպանվող օբյեկտի ենթակառուցվածքում իրադարձությունների աղբյուրների ֆիլտրերի կարգաբերում
- Միջադեպերի կառավարման գործընթացների կատարելագործում (համակարգի պատասխանատուներին տեղեկացում, արձագանքման մեխանիզմների գործարկում)

Անհրաժեշտ պահանջներ

- Բարձրագույն տեխնիկական կրթություն (մագիստրոսի կամ բակալավրի աստիճան)՝ տեղեկատվական տեխնոլոգիաներ (նախընտրելի է ցանցային անվտանգություն, համակարգչային ցանցեր), կիրառական մաթեմատիկա, ռադիոֆիզիկա, ֆիզիկա, մաթեմատիկա
- Առնվազն 3 տարվա աշխատանքային փորձ տեղեկատվական համակարգերի և ցանցերի անվտանգության ոլորտում
- Աշխատանքային փորձ՝ ՏԱ նշված ոլորտներից որևէ մեկում

- Տեղեկատվական անվտանգության մոնիթորինգ
- Ցանցային թրաֆիկի և տարբեր աղբյուրների իրադարձությունների մատյանների վերլուծություն
- ՏԱ մոնիթորինգի կառուցում և կատարելագործում
- ՏԱ իրադարձությունների հետաքննություն
- Ցանցային արձանագրությունների իմացություն
- Օպերացիոն համակարգերի հիմնական տիպերի ճարտարապետության իմացություն
- ՏԱ իրադարձություններին արձագանքման մեթոդների, գործիքների և գործընթացների իմացություն
- Սկրիպտային լեզուների օգտագործմամբ (bash/python/powershell) խնդիրների ավտոմատացման հմտությունների իմացություն
- Windows/Linux օպերացիոն համակարգերի ադմինիստրավորման փորձը ցանկալի է
- Ցանցային սքաներների (nmap, nessus և այլն) օգտագործման փորձը ցանկալի է
- Ցանցում հարձակումների հայտնաբերման համակարգերի (IDS\IPS, HIDS\HIPS) հետ աշխատանքի փորձը ցանկալի է
- ՏԱ մոնիթորինգի կամ ՏԱ իրադարձությունների հետաքննության աշխատանքային 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՝ "Leading Specialist of Information Security - Name, Surname":