ՏԵԽՆԻԿԱԿԱՆ ԱՌԱՋԱԴՐԱՆՔ

Տեղեկատվական անվտանգության իրադարձությունների հավաքագրման, մշակման և կառավարման համակարգին (Security information and event management) ներկայացվող պահանջներ՝

1. Համակարգի պահանջներ

1.1. Համակարգը պետք է լինի ծրագրաապարատային համալիր:

1.2. Համակարգի բոլոր բաղադրիչները պետք է լինեն արտոնագրված և ունենան համապատասխան արտադրողի կողմից տրամադրվող ուղեկցման, սպասարկման և երաշխիքային պարտավորություններ՝ առնվազն մեկ տարի ժամկետով:

1.3. Համալիրը պետք է իր մեջ ներառի հետևյալ ֆունկցիոնալ բաղադրիչները.

- իրադարձությունների հավաքագրման համակարգ (այսուհետ՝ հավաքագրման հանգույց) - 2 հատ
- իրադարձությունների մշակման և կառավարման համակարգ (այսուհետ՝ Կառավարման հանգույց) - 1 հատ
- իրադարձությունները նախնական տեսքով համակարգելու և երկարաժամկետ պահուստավորելու համակարգ (այսուհետ՝ Պահպանման հանգույց) – 1 հատ:

1.4. Հավաքագրման հանգույցը պետք է ապահովի առնվազն 6000 իրադարձությունների մշակում 1 վայրկյանում:

1.5. Կառավարման և պահպանման հանգույցներից յուրաքանչյուրը պետք է ապահովի առնվազն 40,000 իրադարձությունների մշակում 1 վայրկյանում:

1.6. Ցանկալի է, որ վերը նշված հանգույցներից որևիցե մեկը չունենա որևէ ծրագրային սահմանափակում ընդունվող տեղեկատվության հոսքի նկատմամբ: Համալիրի բաղադրիչները պետք է ապահովեն ցանցային և ապարատային հնարավորություններով սահմանված իրադարձությունների հոսքի հավաքագրում և մշակում, նույնիսկ եթե այն տևական ժամանակ գերազանցում է սահմանված իրադարձություն/վայրկյանում ցուցանիշները (ցուցանիշը գերազանցած իրադաձությունները պետք է «բուֆերիզացվեն» և շարունակեն մշակվել հնարավոր արագությամբ (միջինում նշված արագագործության առնվազն 30% -ի չափով):

1.7. Համալիրում ներառված բոլոր բաղադրիչները պետք է ունենան առնվազն 2 հատ 10 Gbps ցանցային ինտերֆեյս, իսկ Հավաքագրման հանգույցը՝ ևս 2 հատ 1 Gbps (առնվազն):

1.8. Կառավարման հանգույցը, դինամիկ մշակման և իրադարձությունների կառավարման և պահպանման համար պետք է ունենա հիմնական հիշողություն՝ առնվազն 30 TB:

1.9. Պահպանման հանգույցը պետք է ապահովի հիմնական հիշողություն՝ առնվազն 30TB:

1.10. Համալիրը պետք է հնարավորություն ունենա տեղեկատվության պահպանման համար օգտագործել նաև ցանցային տվյալների պահպանման համակարգեր հետևյալ պրոտոկոլների միջոցով՝ iSCSI, NAS:

1.11. Կառավարման և Պահպանման հանգույցներում առկա տվյալների պահոցները պետք է բաղկացած լինեն SAS կամ SATA սերվերային, բարձր հուսալիության կոշտ սկավառակներից՝ համակարգված Raid 5 (առնվազն) սկզբունքով, ինչպես նաև ցանկալի է հավելյալ SSD տիպի հիշողության առկայություն համակարգի արագագործությունը բարձրացնելու նպատակով:

1.12. Հավաքագրման հանգույցը պետք է ապահովի իրադարձությունների հավաքագրում ներքին հիշողությունում՝ ոչ պակաս, քան 2 TB ծավալով: Հավաքագրումը պետք է տեղի ունենա նաև Կառավարման հանգույցի հետ ցանցային կապուղու հասանելիության խափանման ընթացքում:

1.13. Համալիրը պետք է առնվազն ունենա/ապահովի իրադարձությունների հավաքագրման հետևյալ հնարավորությունները/պրոտոկոլները.

- WMI
- CIFS
- NFS
- SMB
- SCP
- Syslog
- FTP/SFTP
- MySQL Queries
- MSSQL Queries
- Oracle Queries
- LDAP Queries

1.14. Համալիրը պետք է լինի Gartner ռեյտինգային կազմակերպության կողմից հրապարակվող համապատասխան համակարգերի մասին տարեկան հաշվետվության, 2018 թվականին առաջադրված մասնակիցների Leaders տիրույթի մասնակից:

1.15. Համալիրը պետք է իրականացնի տարբեր սկզբնաղբյուրներից հավաքագրված իրադաձությունների համադրում, թե՛ արտադրողի կողմից առաջարկված և կարգաբերված սցենարներին համապատասխան և թե՛ հնարավորություն ընձեռի ստեղծելու սեփական պահանջներին համապատասխան համադրման կանոններ՝ հիմնված իրադարձությունների թե՛ դիսկրետ և թե՛ քանակային պարամետրերի վրա՝ առանց որևէ սահմանափակման:

1.16. Համալիրը պետք է ապահովի հետևյալ արտադրողների համակարգերից իրադարձություններ հավաքագրելու, արտապատկերելու և մշակելու հնարավորություն.

- Microsoft Windows server (2008, 2012, 2016)
- Microsoft Exchange

- Microsoft Sharepoint
- Microsoft Active directory
- Linux
- Unix
- Palo Alto
- Fortinet
- McAfee
- Kaspersky
- FireEye
- Checkpoint
- Bluecoat
- Cisco
- HP Networks
- Symantec
- CyberArk
- MySQL
- MSSQL
- Oracle

1.17. Համալիրը պետք է հնարավորություն ունենա հավաքագրելու և մշակելու ցանցային հոսքեր (Netflow):

1.18. Համալիրը պետք է իրականացնի հավաքագրված ցանցային հոսքի զննում և բացահայտի հնարավոր միջադեպերը, տեղեկացնի ռիսկային իրադարձությունների մասին՝ հիմնված արտադրողի կողմից կարգաբերված սցենարների վրա, ինչպես նաև հնարավորություն ընձեռի ստեղծել կորպորատիվ կարիքներին և կարգերին համապատասխան սցենարներ:

1.19. Համալիրը պետք է հնարավորություն տրամադրի իրական ժամանակում, ինչպես նաև հավաքագրված իրադարձությունների ցանկացած պատմական ժամանակահատվածում, դիտարկելու և համադրելու տարբեր համակարգերի իրադարձությունները/հոսքերը:

- Տվյալ իրադարձություններում/հոսքերում առկա տեղեկատվությունը պետք է հնարավոր լինի զտել, տարբերակել և համադրել հոսքերում առկա նույնականացվող տեղեկատվության հիման վրա, օրինակ՝ ըստ Համակարգի տիպի, իրադարձությունների տիպի, օգտատերերի, ցանցային և այլ չափորոշիչների:

- Տվյալ դիտարկման հնարավորությունները պետք է լինեն կարգաբերվող՝ առանց որևէ քանակային կամ ծավալային սահմանափակման:

1.20. Համալիրը պետք է ունենա ISO 27000 և PCI-DSS ստանդարտների պահանջներին համապատասխան, նախապես կարգաբերված կանոններ և ստուգման սցենարներ, ինչպես նաև՝ համապատասխան ստանդարտների պահանջների իրական ժամանակում դիտարկման հնարավորություն:

1.21. Համալիրը պետք է ունենա իրադարձությունների մասին տեղեկացնելու/ ահազանգելու հնարավորություն հետևյալ միջոցներով/պրոտոկոլներով.

- համապատասխան տեսանելի հաղորդագրություն կառավարման վահանակի պատուհանում
- ձայնային ազդանշան
- էլեկտրոնային փոստի միջոցով (SMTP)
- ցանցային հաղորդագրության միջոցով (SNMP)։

1.22. Համալիրը պետք է ունենա համապատասխան բաղադրիչ, որը թույլ կտա հավաքագրել Windows սերվերներում տեղակայված՝ տեքստային ֆայլերում պահվող հաղորդագրություններ/իրադարձություններ, անմիջապես համակարգից (Log Agent)։ Տվյալ բաղադրիչը պետք է հնարավորություն ունենա հավաքագրելու նաև MSSQL, MySQL և Oracle տիպի տվյալների պահոցների համապատասխան տիրույթներում գրանցված իրադարձություններ։

1.23. Համալիրը պետք է հնարավորություն տրամադրի ներմուծելու և մշակելու TXT, EVT, XML ֆորմատների իրադարձություններ պարունակող ֆայլեր։

1.24. Համակարգը պետք է հնարավորություն ընձեռի դասակարգելու համակարգից օգտվող օգտատերերին և կառավարիչներին, ինչպես նաև հնարավորություն ընձեռի համապատասխան սահմանափակումներ կիրառել օգտատերերի իրավասությունների և հասանելի համակարգերի ցանկի նկատմամբ։

2. Մատակարարի պահանջներ

2.1. Մատակարարը պետք է ունենա առնվազն մեկ համապատասխան արտոնագրված մասնագետ։
2.2. Մատակարարը պետք է իրականացնի առաջին աստիճանի սպասարկում։
2.3. Մատակարարը պետք է իրականացնի համակարգի տեղադրում, կարգաբերում և ինտեգրում Պատվիրատուի տարածքից, Պատվիրատուի կողմից առաջադրված պայմաններին և համակարգերին համապատասխան։
2.4. Մատակարարը պետք է ներկայացնի արտադրողի կողմից մատակարարի պաշտոնական գործընկեր լինելու և տվյալ մրցույթին մասնակցելու աջակցությունը հաստատող նամակ։