"Цифрлық үкімет" платформасының киберқауіпсіздігін қамтамасыз ету регламентін бекіту туралы

Қазақстан Республикасы Премьер-Министрінің орынбасары – Жасанды интеллект және цифрлық даму министрінің 2026 жылғы 7 тамыздағы № 462/НҚ бұйрығы

"Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-4-бабы 1-тармағының 6) тармақшасына сәйкес БҰЙЫРАМЫН:

1. Қоса беріліп отырған "Цифрлық үкімет" платформасының киберқауіпсіздігін қамтамасыз ету регламенті бекітілсін.

2. Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің Ақпараттық қауіпсіздік комитеті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) осы бұйрықты ресми жарияланғаннан кейін оны Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрлігінің интернет-ресурсында орналастыруды;

2) осы бұйрыққа қол қойылған күннен бастап күнтізбелік бес күн ішінде оның көшірмесін Қазақстан Республикасы нормативтік құқықтық актілерінің эталондық бақылау банкіне қосу үшін Қазақстан Республикасы Әділет министрлігінің "Қазақстан Республикасының Заңнама және құқықтық ақпарат институты" шаруашылық жүргізу құқығындағы республикалық мемлекеттік кәсіпорнына жіберуді қамтамасыз етсін.

3. Осы бұйрықтың орындалуын бақылау жетекшілік ететін Қазақстан Республикасының Жасанды интеллект және цифрлық даму вице-министріне жүктелсін.

4. Осы бұйрық алғашқы ресми жарияланған күнінен кейін он күнтізбелік күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасы
Премьер-Министрінің орынбасары –
Жасанды интеллект және цифрлық даму министрі *Ж. Мәдиев*

"КЕЛІСІЛДІ"
Қазақстан Республикасы
Ұлттық қауіпсіздік комитеті

Қазақстан Республикасы
Премьер-Министрінің
орынбасары – Жасанды
интеллект және цифрлық
даму министрінің
2026 жылғы 7 тамыздағы
№ 462/НҚ бұйрығымен
бекітілген

"Цифрлық үкімет" платформасының киберқауіпсіздікті қамтамасыз ету регламенті

1-тарау. Жалпы ережелер

1. Осы "Цифрлық үкімет" платформасының киберқауіпсіздігін қамтамасыз ету регламенті (бұдан әрі – Регламент) "Киберқауіпсіздік туралы" Қазақстан Республикасы Заңының 7-4-бабы 1-тармағының 6) тармақшасына сәйкес әзірленді және "Мемлекеттік техникалық қызмет" акционерлік қоғамы (бұдан әрі – "МТҚ" АҚ) "Ұлттық ақпараттық технологиялар" акционерлік қоғамымен (бұдан әрі – "ҰАТ" АҚ) бірлесіп "цифрлық үкімет" платформасының және онда орналастырылған цифрлық объектілердің киберқауіпсіздігін қамтамасыз ету жөніндегі іс-шараларды жүзеге асыру кезінде жұмыстардың реттілігін, орындалу мерзімдерін, жұмыс нәтижелерін ресімдеу тәртібін, сонымен қатар киберқауіпсіздікті қамтамасыз етуге қатысатын қызметкерлерге қойылатын ең төменгі біліктілік талаптарын айқындайды және оларды оқыту мен біліктілігін арттыру рәсімдерін сипаттайды.

2. Осы Регламентте келесі терминдер, анықтамалар және қысқартулар пайдаланылады:

1) АККҚ – ақпаратты криптографиялық қорғау құралы;

2) ККБЖ – киберқауіпсіздікті басқару жүйесі (SIEM);

3) АҚҚ – ақпаратты қорғау құралы;

4) БКТ – бастапқы кодтарды талдау;

5) БҚ – бағдарламалық қамтылым;

6) БҚЖӘ – БҚ қауіпсіз әзірлеу;

7) ВО – виртуалдау ортасы;

8) ДББЖ – деректер базасын басқару жүйесі;

9) Жарияланбаған мүмкіндіктер (бұдан әрі - ЖМ) – техникалық құжаттамада көрсетілмеген немесе сипатталғанға сәйкес келмейтін БҚ функционалдық мүмкіндіктері;

10) ИҚБШ – Интернетке қолжетімділіктің бірыңғай шлюзі;

11) КҚ – киберқауіпсіздік;

12) КҚ ТҚ – киберқауіпсіздік бойынша техникалық құжаттама;

13) ҚБҚ – қолданбалы бағдарламалық қамтылым;

14) ҚРҮҚ БТ – "Киберқауіпсіздік туралы" Қазақстан Республикасының Заңына сәйкес Қазақстан Республикасының Үкіметі бекітетін Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар;

15) НҚА – Қазақстан Республикасының нормативтік құқықтық актілер;

16) ОЖ – операциялық жүйе;

17) ТТ – техникалық тапсырма;

18) уәкілетті орган – киберқауіпсіздікті қамтамасыз ету саласындағы басшылықты және салааралық үйлестіруді жүзеге асыратын орталық атқарушы орган;

19) фреймворктар – БҚ құрылымын белгілейтін және әзірлеудің типтік тетіктерін (маршруттауды, сұрауларды өңдеуді, деректерге қол жеткізуді) қамтамасыз ететін бағдарламалық кітапханалар мен инфрақұрылымдық компоненттердің жиынтығы;

20) ЦО – цифрлық объект;

21) ЦО меншік иесі – өз қалауы бойынша өзіне тиесілі ЦО иелену, пайдалану және басқару құқығына ие субъект;

22) ЦҮ ЦО – "цифрлық үкіметтің" цифрлық объектілері;

23) "цифрлық үкімет" платформасы (бұдан әрі - QazTech платформасы) – цифрлық объектілерді әзірлеуге, дамытуға, орналастыруға, интеграциялауға арналған "цифрлық үкімет" операторының цифрлық платформасы;

24) ЭҚАЖ– электрондық құжат айналымы жүйесі;

25) Anti-DDoS – цифрлық объектінің жұмыс істеу қабілетін бұзуға бағытталған қаскүнемдердің әрекеттерінен қорғау;

26) AV – зиянды бағдарламаларды анықтау және алдын алу жүйесі;

27) Container security – жиналған Docker-бейнелердің қауіпсіздігін талдау;

28) DAST – қосымшалар қауіпсіздігінің динамикалық талдауы (Dynamic Application Security Testing);

29) DLP – қолжетімділігі шектеулі цифрлық ресурстардың таралуын болдырмауға арналған АҚҚ;

30) EDR – соңғы нүктелердегі күрделі қауіптерді анықтау және оларға ден қою жүйесі (Endpoint Detection and Response);

31) Gitlab – бастапқы кодтың репозиторийлерін сақтау және басқару жүйесі;

32) IaC security – инфрақұрылым файлдарының қауіпсіздігін талдау (Kubernetes, Terraform);

33) IPS/IDS – басып кірулерді анықтау және алдын алу жүйесі;

34) MAST – мобильді қосымшалардың қауіпсіздігін тестілеу (Mobile Application Security Testing);

35) NGFW – жаңа буындағы желіаралық экран (Next-Generation Firewall);

36) PAM – артықшылық құқығы бар пайдаланушылардың қолжетімділігін басқару жүйесі (Privileged Access Management);

37) Pentest – осалдықтарды және ықтимал шабуылдар сценарийлерін анықтау және оларды жою және алдын алу бойынша ұсыныстар беру мақсатында қаскүнемнің әрекеттерін ұқсату техникалары мен құралдарды пайдалана отырып, цифрлық объектілердің қауіпсіздігін бағалау әдісі;

38) Pipeline CI/CD – БҚ үздіксіз интеграциялау және үздіксіз жайғастыру конвейері;

39) Sandbox – күмәнді файлдардың әрекетін талдауға арналған оқшауланған виртуалды орта;

40) SAST – қосымшалар қауіпсіздігінің статикалық талдауы (Static Application Security Testing);

41) SCA – бағдарламалық қамтылым құрамын талдау (Software Composition Analysis);

42) SIEM – КҚ және КҚ оқиғаларын бақылау және басқару жүйесі;

43) Unit-тест – жүйенің жекелеген функциялары мен компоненттерінің дұрыс жұмыс істеуін тексеру;

44) WAF – веб-қосымшаларды қорғау үшін желіаралық экран (web-application firewall).

2-тарау. Бастапқы кодтың сапасын тестілеу және талдау

Бастапқы кодтың сапасын тестілеу және талдау процедуралары GitLab CI/CD конвейерінде орындалады және автоматты модульдік тестілеуді, бастапқы кодтың сапасын тексеруді және қолмен функционалды тестілеуді қамтиды.

Автоматты модульдік тестілеу (Unit Testing) - жүйенің жеке функциялары мен компоненттерін жұмыстың дұрыстығына тексеру.

Бастапқы кодтың сапасын тексеру (Code Quality check) кодтау стандарттарының бұзылуын, ықтимал қателерді және кодты қолдау проблемаларын анықтауға бағытталған.

Функционалдық тестілеу іске асырылған функционалдықтың мәлімделген талаптар мен сипаттамаларға сәйкестігін растауға бағытталған БҚ тексеру кезеңі болып табылады.

Негізгі міндеттері:

іске асырылған функциялар жұмысының дұрыстығын және бизнес-логиканы тексеру;

іске асырылған функциялардың ТТ талаптарына сәйкестігін растау;

бастапқы кодтың сапасы мен оқылуын тексеру;

қабылданған кодтау және стиль стандарттарының сақталуын бақылау;

қателіктерді ерте кезеңдерде анықтау (unit-тесттер арқылы);

табылған осалдықтарды басқару, оның ішінде оларды жіктеу және жою;

интеграциялық және қабылдау тестілеу кезеңінде қателер санын азайту;

БҚ тұрақтылығы мен сүйемелдеуін арттыру.

Автоматты модульдік тестілеу (Unit Tests) GitLab CI/CD-де құрастыру кезеңінде орындалады және код сапасын қамтамасыз ету үшін негіз болып табылады.

Кодтың сапасын тексеру Gitlab CI/CD құрастыру кезеңінде автоматты түрде жүргізіледі, ол үшін автоматтандырылған құрал қолданылады.

Функционалдық тестілер unit-тесттерден сәтті өткеннен кейін және кодтың сапасы тексерілгеннен кейін автоматты түрде орындалады. Пайдаланушы сценарийлері деңгейінде жүйенің мінез-құлқын кешенді тексеруді қамтамасыз етумен.

Тестілеу және сапаны бағалау барлық тексерулерден сәтті өткенде, белгіленген сапа көрсеткіштеріне қол жеткізгенде, сыни қателіктерді жойғанда және жауапты қатысушылардың өзгерістерді келісуі кезінде аяқталды деп саналады.

Нәтижелер бойынша объект иесі негізгі көрсеткіштерді, анықталған ескертулерді, олардың мәртебесін және жақсарту бойынша ұсыныстары бар шығарылымға дайындықты бағалауды қамтитын есеп қалыптастырылады. Есепті рәсімдеу тәртібі және мерзімдерін объект иесі дербес айқындайды.

Жұмыстарды QazTech платформасы бөлігінде "ҰАТ" АҚ және компоненттер бөлігінде ЦО иелері орындайды.

3-тарау. Қауіпсіз бағдарламалық қамтылым әзірлеу процестері

Бастапқы кодты талдау БҚ жұмыс істеу барысында оның бастапқы кодын, тәуелділіктерін, контейнерлік бейнелерін, инфрақұрылымдық қалыптарын және орындау процестерін талдайтын кіріктірілген және (немесе) интеграцияланған DevSecOps құралдарының көмегімен жүзеге асырылады.

БҚ-дағы осалдықтарды анықтау мынадай тәртіппен жүзеге асырылады:

1) pipeline іске қосылған кезде GitLab қауіпсіздікті тексеру кезеңдерін автоматты түрде бастайды;

2) талдаудың әрбір түрі SAST, SCA, DAST, MAST, Container Security және IaC Security сканерлерімен орындалады;

3) тәуекел деңгейі жоғары және орташа осалдықтар анықталған жағдайда pipeline орындау тоқтатылады;

4) "МТС" АҚ орындаушысы талдау жүргізу үшін есепті алады;

5) бағдарламалық есептерде жалған іске қосылулардың (осалдықтардың нақты бар екендігін растамайтын автоматтандырылған талдаудың қате нәтижелерінің) бар-жоғына талдау жүргізіледі;

6) БҚ-да анықталған осалдықтардың тізбесін, олардың сипаттамасын, орналасу жолын (файлға дейінгі жолын) және тәуекел деңгейін (жоғары, орташа, төмен) қамтитын есеп қалыптастырылады;

7) анықталған осалдықтарды жою жөніндегі жоспар әзірленеді және іске асырылады, оның ішінде оларды басымдыққа қарай бөлу және орындау мерзімдерін айқындау жүзеге асырылады.

ЖМ-ді анықтау мынадай тәртіппен жүзеге асырылады:

1) қауіпсіздікті тексерудің автоматтандырылған кезеңдері бар GitLab pipeline іске қосылады;

2) QazTech платформасы мен ЦО техникалық құжаттамасына, оның ішінде цифрлық объектіні жасауға (дамытуға) арналған ТТ-ға оның мақсаты, қолданылу

саласы, қолданылатын әдістері, шешілетін міндеттердің сыныбы, қолдану кезіндегі шектеулері, техникалық құралдардың ең төменгі конфигурациясы, жұмыс істеу ортасы және пайдалану тәртібі туралы мәліметтер бөлігінде талдау жүргізіледі;

3) QazTech платформасы мен ЦО бастапқы коды қолмен талдау әдісімен зерттеледі:

БҚ-ның модульдік және логикалық құрылымы, сонымен қатар функционалдық модульдері зерделеніп, олардың құрылымы техникалық құжаттамада келтірілген құрылыммен салыстырылады;

функционалдық объектілердің орындалу бағыты және өңделетін деректер тексеріледі;

кейіннен ЖМ анықтау нәтижелері туралы есепке енгізу үшін ЖМ тіркеледі;

4) ЖМ анықталған жағдайда БКТ жөніндегі қызмет мамандары жобаларды басқару жүйесінде жүргізілген талдау нәтижелері, анықталған ЖМ сипаттамасы, сондай-ақ талдау нәтижелері туралы есеп және оны жою жөніндегі ұсынымдар көрсетілетін Issue жасайды.

Осалдықтар мен ЖМ анықталмаған жағдайда орындаушы репозиторий тармағындағы өзгерістерді одан әрі ілгерілету үшін GitLab жүйесінде бекіту рәсімін жүзеге асырады.

Қауіпсіз әзірлеу процесінде қолданылатын қауіпсіздікті талдау құралдарын (SAST, SCA, DAST, MAST, Container Security, IaC Security) баптау пайдаланылатын талдау құралдарында жүзеге асырылады. Бастапқы кодты басқару жүйесімен талдау құралдарын интеграциялау, талдау бейіндерін, сындарлылық деңгейлерін, нәтижелерді өңдеу қағидаларын баптау, сонымен қатар қол жеткізу құқықтарын және пайдаланушылардың әрекеттерін журналдауды баптау жүзеге асырылады.

Талдау құралдары қолданылатын бағдарламалау тілдеріне, фреймворктерге және жобалар түрлеріне бейімделеді, талдау жүргізу аймақтары бапталады, қатысы жоқ файлдар алып тасталады және тексерулерді орындау уақыты оңтайландырылады.

Талдау құралдарының жаңа нұсқаларына тестілеу жүргізіледі және БҚ қауіпсіз әзірлеу процестерін жетілдіру жөніндегі ұсыныстар дайындалады.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ QazTech платформасының бастапқы кодын, ал ЦО меншік иесі ЦО бастапқы кодын және оған қатысты қажетті құжаттаманы ұсынады.

4-тарау. QazTech платформасының киберқауіпсіздігін қамтамасыз ету жөніндегі іс-шаралар

1. ҚРҰҚ БТ сәйкес КҚ саясатын және КҚ ТҚ әзірлеу.

"ҰАТ" АҚ КҚ ТҚ-ны әзірлеуге, оларға өзгерістер мен толықтырулар енгізуге жауапты болып табылады, бұл ретте "МТҚ" АҚ техникалық құжаттарды келісуге қатысады.

Кезеңділігі: қажеттілігіне қарай, бірақ екі жылда кемінде бір рет.

Аяқталу түрі: бекітілген КҚ ТҚ.

2. "Цифрлық үкімет" платформасында ЦО әзірлеу, дамыту, орналастыру және интеграциялау жөніндегі әдістемелік талаптарды (бұдан әрі – Әдістеме) әзірлеу (өзгерістер мен толықтырулар енгізу). Әдістеме "ҰАТ" АҚ мен "МТҚ" АҚ бірлесіп әзірлейді және оны уәкілетті орган бекітеді, кейіннен ЦО меншік иелері міндетті түрде қолданады.

Әдістемеде бастапқы кодты талдау құралдарын пайдалана отырып pipeline CI/CD ұйымдастырудың негізгі тәсілдері мен талаптары, есептердің нысандары, кодтың негізгі тармақтарындағы өзгерістерді келісу кезеңдері, жобалар мен топтардағы қол жеткізу құқықтары сипатталады. КҚ талаптарын сақтай отырып, бастапқы кодты өнімді ортаға орналастыру әдістері айқындалады.

Әдістемеде бастапқы кодты жүктеу, әзірлеу және орналастыру жөніндегі бизнес-процестердің сипаттамасы, сонымен қатар QazTech платформасының құралдарымен жұмыс істеу туралы ақпарат қамтылады.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: Әдістеме.

3. QazTech платформасының БҚ мен техникалық құралдары орналастырылған негізгі және резервтік серверлік үй-жайларға (деректерді өңдеу орталықтарына) ҚРҰҚ БТ-на сәйкестігіне тексеру жүргізу. Тексеруді "МТҚ" АҚ жүзеге асырады, бұл ретте " ҰАТ" АҚ тексеруді жүргізетін "МТҚ" АҚ жұмыскерлеріне серверлік үй-жайларға (деректерді өңдеу орталықтарына) және қажетті құжаттамаға (журналдар, шарттар және т.б.) кедергісіз қол жеткізуді қамтамасыз етеді.

Серверлік үй-жайларды (деректерді өңдеу орталықтарын) тексеру кезінде "МТҚ" АҚ жұмыскерлері ҚРҰҚ БТ-ның 8-параграфында көзделген талаптарды басшылыққа алады.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: тексеру туралы есеп.

4. QazTech платформасының серверлік жабдығын КҚ талаптарына сәйкестігіне тексеруді жүзеге асыру (ВО, әзірлеу, тестілеу және өнеркәсіптік пайдалану орталарының бөлінуі, ОЖ, ДББЖ, ҚБҚ).

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне ОЖ, ДББЖ, ҚБҚ және ВО қол жеткізуді қамтамасыз етеді, сонымен қатар қауіпсіздік саясаттарын көрсету үшін жауапты тұлғаларды (әкімшілерді) ұсынады.

QazTech платформасының серверлік жабдығын тексеру кезінде "МТҚ" АҚ жұмыскерлері Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарын басшылыққа алады.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: тексеру туралы есеп.

5. QazTech платформасының желілік жабдығын КҚ талаптарына сәйкестігіне тексеру (желіаралық экрандардың, бағдарлауыштар мен коммутаторлардың конфигурациясы, желілерді бөлу).

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне кедергісіз қол жеткізуді қамтамасыз етеді және желілік жабдықтағы қауіпсіздік саясаттарын көрсетуге және (қажет болған жағдайда) пысықтауға жауапты желілік әкімшілерді айқындайды.

QazTech платформасының желілік жабдығын тексеру кезінде "МТҚ" АҚ жұмыскерлері Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарын басшылыққа алады.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: тексеру туралы есеп.

6. Осалдықтарды анықтау мақсатында QazTech платформасына аспаптық сканерлеу жүргізу. Жаңартулардың болуына, конфигурацияларды талдауға, жалпы осалдықтар мен тәуекелдер дерекқоры бойынша белгілі осалдықтардың болуына, сонымен қатар Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарына сәйкестігіне QazTech платформасының виртуалды серверлері, желілік жабдығы және ВО сканерлеуге жатады.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне серверлер мен желілік құрылғыларға артықшылықты құқықтармен ("root" түріндегі) қашықтан желілік қол жеткізуді қамтамасыз етеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: сканерлеу туралы есеп.

7. QazTech платформасына жүктемелік тестілеу жүргізу.

QazTech платформасына жүктемелік тестілеуді қалыпты пайдалану ортасында қолжетімділіктің, тұтастықтың және құпиялылықтың сақталуын бағалау мақсатында "МТҚ" АҚ жүргізеді. Жүктемелік тестілеуді "МТҚ" АҚ жұмыскерлері автоматтандырылған сценарийлер негізінде, дербес деректер синтетикалық (жалған) деректермен алмастырылған қалыпты пайдалану ортасында мамандандырылған бағдарламалық құралды пайдалана отырып жүргізеді. Жүктемелік тестілеу пайдаланушылардың қосылу нүктелерінің саны және интеграциялық өзара іс-қимылдың қосылу нүктелерінің нұсқалары бойынша жүргізіледі. Бұл ретте "МТҚ" АҚ тестілеу сценарийін, тестілеудің уақытша және сандық сипаттамаларын айқындайды, сондай-ақ тестілеуді өткізу уақытын "ҰАТ" АҚ-мен келіседі.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлерін жұмыстарды орындау үшін QazTech платформасына қажетті қол жеткізу құқықтарымен қамтамасыз етеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: жүктемелік тестілеу туралы есеп.

8. БКТ-ны (SAST, DAST, SCA, ЖМ, Container Security, IaC Security) жүргізу.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне QazTech платформасының бастапқы кодын және қажетті құжаттаманы (журналдар, шарттар, техникалық тапсырма және т.б.) ұсынады.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: талдау туралы есеп.

9. КҚ ТҚ талаптарының сақталуына ішкі бақылауды қамтамасыз ету, оның ішінде олардың барлық мүдделі тұлғалар мен сыртқы контрагенттердің орындауын қамтамасыз ету.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: КҚ ТҚ 4-деңгейдегі бекітілген құжаттары.

10. Киберқауіпсіздік жөніндегі техникалық құжаттардың талаптарының сақталуына сыртқы бақылауды қамтамасыз ету.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне қажетті құжаттаманы ұсынады, ОЖ, ДББЖ, ҚБҚ, ВО, АҚҚ (SIEM, PAM, AV және басқалары) қол жеткізуді қамтамасыз етеді, сонымен қатар қауіпсіздік саясаттарын көрсету үшін жауапты тұлғаларды (әкімшілерді) айқындайды.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

11. Қол жеткізу құқықтары мен қолжетімділікті басқару: QazTech платформасының барлық жүйелерін/кіші жүйелерін және компоненттерін AD/LDAP жүйесіне қосу.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады, ал "МТҚ" АҚ есептік жазбаларды басқару (құру, жою, құқықтарды өзгерту) процестерін келісуге қатысады. Бұл ретте "ҰАТ" АҚ QazTech платформасының барлық компоненттерін (ОЖ , ДБ, ВО және басқаларын) AD/LDAP жүйесіне қосуды қамтамасыз етеді.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: SD жүйесіндегі өтінім.

12. Жүйелік және қолданбалы БҚ конфигурацияларын және эталондық бейнелерін басқару.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады, ал "МТҚ" АҚ жүйелік және ҚБҚ етудің конфигурацияларына және эталондық бейнелерге енгізілетін өзгерістерді келісуге қатысады, бұл ретте оларда АҚҚ алдын ала орнатылуы қамтамасыз етіледі.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

13. QazTech платформасының барлық компоненттерінің резервтік көшірмесін жасау және резервтік көшірмелерді қалпына келтіруді тестілеу.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады, ал "МТҚ" АҚ олардың орындалуын бақылауды қамтамасыз етеді. Бұл ретте резервтік көшірме жасау және резервтік көшірмелерді қалпына келтіруді тестілеу рәсімдері ҚҚ ТҚ талаптарына сәйкес орындалады.

Кезеңділігі: Платформаның ҚҚ ТҚ белгіленген мерзімдерге сәйкес.

Аяқталу түрі: резервтік көшірмелер журналы және резервтік көшірмелерді қалпына келтіруді тестілеу журналы.

14. Шифрлау кілттері мен парольдердің қауіпсіздігін қамтамасыз ету (Vault).

"ҰАТ" АҚ Vault жүйесін іске қосу, қайта іске қосу және қалпына келтіру үшін қажетті төрт seal/unseal кілтін генерациялайды. Аталған кілттер бөлініп, бір-бірден QazTech платформасының әкімшілеріне, "ҰАТ" АҚ ҚҚ бөлімшесіне және екі кілт " МТҚ" АҚ-ға беріледі. Vault жүйесін іске қосу, қайта іске қосу және қалпына келтіру рәсімдерін орындау үшін кемінде үш кілт ұсынылуы қажет.

"ҰАТ" АҚ артықшылықты пайдаланушының (root token) паролін генерациялауды және оны үш бөлікке бөлуді жүзеге асырады, кейіннен парольдің бір бөлігі QazTech платформасының әкімшілеріне, бір бөлігі "ҰАТ" АҚ ҚҚ бөлімшесіне және бір бөлігі " МТҚ" АҚ-ға беріледі.

Цифрлық объектілердің меншік иелері үшін Vault токендерін жасау, рөлдер мен қол жеткізу түрлерін айқындау "ҰАТ" АҚ мен "МТҚ" АҚ бірлесіп жүзеге асырады.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: seal/unseal кілттерінің бастапқы генерациясы актімен ресімделеді. Қалған процестер Vault оқиғалар журналында тіркеледі.

15. QazTech платформасының АҚҚ жұмысқа қабілеттілігіне мониторинг жүргізу.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады, бұл ретте "МТҚ" АҚ ҚҚ оқиғалары көздерінің жай-күйіне, олардың параметрлері мен қорғау режимдеріне бақылау жүргізуге, оның ішінде олардың жұмыс істеуіндегі кемшіліктер мен қателер туралы "ҰАТ" АҚ-ны хабардар етуге қатысады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

16. QazTech платформасының цифрлық инфрақұрылымына мониторинг жүргізу және оны басқару (серверлердің, желілік жабдықтың, ДБ, ҚБҚ және басқалардың жұмысын бақылау).

"ҰАТ" АҚ QazTech платформасының цифрлық инфрақұрылымына мониторинг жүргізуді және оны басқаруды қамтамасыз етеді, оның шеңберінде QazTech платформасының цифрлық инфрақұрылымының бағдарламалық қамтылым мен техникалық құралдарына мониторинг жүргізіледі, сондай-ақ оның әкімшілері мен пайдаланушыларының әрекеттері журналға жазылады.

"МТҚ" АҚ осы талаптың іске асырылуын бақылауды жүзеге асырады, QazTech платформасының цифрлық инфрақұрылымын мониторингтеу және басқару

жүйелерінің жұмыс істеуіне тоқсан сайын талдау жүргізеді және анықталған сәйкессіздіктерді жою жөнінде ұсынымдар береді.

Кезеңділігі: тұрақты негізде, жүйелердің жұмыс істеуіне тоқсан сайын талдау жүргізу.

Аяқталу түрі: орындалуы.

17. AV, EDR, Sandbox, DLP сыныптарындағы КҚБЖ және АҚҚ орнату және конфигурациялау.

КҚБЖ және АҚҚ орнату және конфигурациялау процестерін "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ қатысады және КҚБЖ (SIEM) бағдарламалық құралдарын және КҚ оқиғалары көздерін (AV, EDR, Sandbox, DLP) орнату, сонымен қатар КҚ оқиғалары көздерінің жұмыс істеуінің жекелеген тетіктері мен қауіпсіздік саясаттарын баптау бойынша консультациялық қолдау көрсетеді.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орнату актісі.

18. IDS/IPS/NGFW сыныптарындағы АҚҚ орнату және конфигурациялау.

"ҰАТ" АҚ IDS/IPS/NGFW техникалық құралдарын орнатуды және конфигурациялауды жүзеге асырады, ал "МТҚ" АҚ аталған жұмыстарға қатысады: IDS /IPS/NGFW сыныптарындағы АҚҚ монтаждау және баптау.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орнату актісі.

19. PAM сыныбындағы АҚҚ орнату және конфигурациялау.

"ҰАТ" АҚ (қажет болған жағдайда – "МТҚ" АҚ-мен бірлесіп) QazTech платформасының әкімшілерінің және QazTech платформасының өнімді ортасында ЦО серверлеріне сүйемелдеу көрсететін әкімшілердің әрекеттерін бақылау үшін PAM жүйесін өрістетуді және баптауды жүзеге асырады.

"МТҚ" АҚ PAM жүйесінің саясаттарын, рөлдерін, қол жеткізу құқықтарын баптау және журналдарды SIEM жүйесіне жіберу бойынша талаптарды айқындайды.

"ҰАТ" АҚ PAM жүйесінде пайдаланушыларды тіркеуді және есепке алуды жүзеге асырады, сондай-ақ "МТҚ" АҚ белгілеген талаптардың сақталуын қамтамасыз етеді.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орнату актісі.

20. Оқиғалар көздерін QazTech платформасына қосу.

Оқиғалар көздерін QazTech платформасының КҚБЖ (SIEM) қосу.

Оқиғалар көздерін QazTech платформасының цифрлық инфрақұрылымына қосу процестерін "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ қатысады және КҚБЖ (SIEM) жұмыс істеуінің жекелеген тетіктері мен қауіпсіздік саясаттарын баптау, олардың дұрыс жұмыс істеуін тексеру, сонымен қатар оқиғаларды тіркеу журналдарынан мәліметтердің КҚБЖ (SIEM) орталықтандырылған жиналуын қамтамасыз ету бойынша консультациялық қолдау көрсетеді.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орындалуы.

21. КҚ оқиғалары көздерінің жай-күйін, олардың параметрлері мен қорғау режимдерін бақылау, оның ішінде олардың жұмыс істеуіндегі қателер мен кемшіліктерді жою.

КҚ оқиғалары көздерінің жай-күйін, олардың параметрлері мен қорғау режимдерін бақылауды, оның ішінде олардың жұмыс істеуіндегі қателер мен кемшіліктерді жоюды "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ қатысады және "ҰАТ" АҚ жүгінген кезде серверлік жабдықтың, ОЖ, АҚҚ БҚ жұмысқа қабілеттілігін және QazTech платформасы мен киберқауіпсіздік оқиғалары көздері арасындағы байланыс арналарының қолжетімділігін бақылау мәселелері бойынша консультациялық қолдау көрсетеді.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орындалуы.

22. AV, EDR және Sandbox сыныптарындағы АҚҚ саясаттарын (қағидаларын) баптау.

"ҰАТ" АҚ техникалық құжаттамаға және АҚҚ өндірушінің ұсынымдарына сәйкес QazTech платформасы үшін AV, EDR және Sandbox сыныптарындағы АҚҚ конфигурация параметрлерін (саясаттарын) мерзімді түрде өзгертуді жүзеге асырады. " МТҚ" АҚ оқиғалар журналдарының негізінде АҚҚ дұрыс жұмыс істеуіне диагностика жүргізеді және қажет болған жағдайда конфигурация параметрлеріндегі (саясаттардағы) кемшіліктер туралы "ҰАТ" АҚ-ны хабардар етеді.

Конфигурация параметрлерін (саясаттарды) өзгерту, диагностика жүргізу және анықталған кемшіліктерді жою "ҰАТ" АҚ-ның өтінімдері (сұрау салуы) бойынша жүзеге асырылуы мүмкін.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: өзгертілген саясаттар.

23. КҚ бөлігінде IDS/IPS/NGFW, PAM және DLP сыныптарындағы АҚҚ саясаттарын (қағидаларын) баптау.

"МТҚ" АҚ PAM жүйесінің саясаттарын, рөлдерін және қол жеткізу құқықтарын баптауға қойылатын талаптарды айқындайды.

"ҰАТ" АҚ саясаттарды баптауды және "МТҚ" АҚ талаптарының сақталуын қамтамасыз етеді.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орындалуы.

24. Өмірлік циклдің барлық кезеңдерінде QazTech платформасының интернет-трафигінің ИҚБШ арқылы өтуін қамтамасыз ету.

"ҰАТ" АҚ қамтамасыз етеді, ал "МТҚ" АҚ интернет-трафикті ИҚБШ арқылы қосуға, ҚРҮҚ БТ сәйкес қол жеткізу саясаттарын баптауға қатысады, сонымен қатар аномалиялар мен зиянды БҚ болуына мониторинг пен трафикті талдауды жүргізеді.

"ҰАТ" АҚ байланыс арнасын қамтамасыз етеді және QazTech платформасын ИҚБШ -ға қосады.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орындалуы.

25. КҚБЖ келіп түсетін деректерді КҚ қатерлері мен оқыс-оқиғаларын анықтау қағидалары мен алгоритмдерін әзірлеу мақсатында талдау.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады. КҚ қатерлері мен оқыс-оқиғаларды анықтау қағидалары мен алгоритмдерін әзірлеу кезінде "ҰАТ" АҚ оның жұмыскерлеріне КҚБЖ артықшылықты құқықтармен (root құқықтары бар есептік жазба) қашықтан желілік қол жеткізуді қамтамасыз етеді.

QazTech платформасында AV, EDR және Sandbox сыныптарындағы АҚҚ арқылы нысаналы кибершабуылдар анықталған жағдайда "МТҚ" АҚ тиісті корреляция қағидаларын әзірлейді, оларда өзекті тактикалар, техникалар мен рәсімдер, соңғы нүктелердің артефактілері, желілік артефактілер және ымыралану индикаторлары ескеріледі.

Кезеңділігі: күн сайын.

Аяқталу түрі: КҚБЖ-дағы қағидалар.

26. КҚБЖ және ақпаратты қорғау құралдарында бұзушының іздерінің болуына оқиғалар мониторингін жүргізу (1-деңгей).

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады.

"ҰАТ" АҚ КҚ оқыс-оқиғаларын анықтау мақсатында QazTech платформасының КҚБЖ мен АҚҚ арқылы тәулік бойы мониторингті және КҚ оқыс-оқиғаларына бастапқы ден қоюды жүзеге асырады.

Кезеңділігі: тәулік бойы.

Аяқталу түрі: тәулік бойғы мониторинг, орындалуы.

27. ИҚБШ-де желілік трафикті сүзгілеу (WAF, Anti-DDoS, IPS).

"МТҚ" АҚ қамтамасыз етеді, бұл ретте "ҰАТ" АҚ (қажет болған жағдайда) қол жеткізу саясаттарын, сигнатураларды және ИҚБШ жабдығындағы қажетті АҚҚ баптауға қатысады.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: орындалуы.

28. "Қолмен" режимде енуге тестілеу (Pentest/Red Team) жүргізу.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне серверлер мен желілік құрылғыларға шектеулі құқықтармен ("user" түріндегі) қашықтан желілік қол жеткізуді қамтамасыз етеді.

"МТҚ" АҚ QazTech платформасында осалдықтардың болуына "қолмен" тестілеу режимінде Pentest жүргізеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: Pentest жүргізу нәтижелері бойынша қорытынды.

29. Осалдықтарды анықтау мақсатында QazTech платформасына аспаптық сканерлеу жүргізу.

Осалдықтарды анықтау мақсатында аспаптық сканерлеу жүргізіледі. Жаңартулардың болуына сканерлеуге және конфигурацияларды талдауға, БҚ жалпы осалдықтар мен тәуекелдер дерекқоры бойынша белгілі осалдықтарының болуына, сонымен қатар Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарына сәйкестігіне QazTech платформасының виртуалды серверлер, желілік жабдығы және ВО жатады.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ оның жұмыскерлеріне серверлер мен желілік құрылғыларға артықшылықты құқықтармен (root құқықтары бар есептік жазба) қашықтан желілік қол жеткізуді қамтамасыз етеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: сканерлеу туралы есеп.

30. КҚ мониторингі және КҚ оқыс-оқиғаларына бастапқы ден қою (1-деңгей).

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады.

"ҰАТ" АҚ КҚ оқыс-оқиғаларын анықтау мақсатында QazTech платформасының ККБЖ арқылы тәулік бойы мониторингті және КҚ оқыс-оқиғаларына бастапқы ден қоюды жүзеге асырады.

Кезеңділігі: тәулік бойы.

Аяқталу түрі: тәулік бойғы мониторинг, орындалуы.

31. КҚ оқыс-оқиғаларына ден қою (2-деңгей).

Екінші деңгейдегі ден қою шеңберінде "МТҚ" АҚ өтініш берушілерге КҚ оқыс-оқиғаларын тергеп-тексеруге, артефактілерді талдауға, қосымша ақпарат жинауға және КҚ қатерлерін/оқыс-оқиғаларын жою жөніндегі ұсынымдарды дайындауға жәрдем көрсетеді. Қажет болған жағдайда КҚ оқыс-оқиғаларына ден қоюдың үшінші/ төртінші деңгейіне эскалацияланады.

Кезеңділігі: қажеттілігіне қарай (КҚ оқыс-оқиғаларын пысықтауға жәрдем көрсетуді "МТҚ" АҚ "ҰАТ" АҚ-мен бірлесіп жұмыс күні ішінде, не демалыс және мереке күндері аса маңызды КҚ оқыс-оқиғалары кезінде екінші деңгейдің пассивті кезекшілік кестесіне сәйкес жүзеге асырады).

Аяқталу түрі: "ҰАТ" АҚ-ға есепті/ұсынымдарды ұсыну немесе ден қоюдың үшінші/ төртінші деңгейіне эскалациялау.

32. КҚ оқыс-оқиғаларына ден қою (3-деңгей).

"МТҚ" АҚ ден қоюдың үшінші деңгейінде қолдау көрсетеді, оған тергеп-тексеруге техникалық және сараптамалық қолдау көрсету, атап айтқанда КҚ оқыс-оқиғаларының туындау себептерін талдау, форензикалық зерттеу жүргізу, артефактілерді зерттеу, КҚ оқыс-оқиғасының қайталануын болдырмау жөніндегі шараларды әзірлеу және талдау нәтижелері бойынша есепті "ҰАТ" АҚ-ға ұсыну кіреді.

Кезеңділігі: екінші деңгейдегі ден қоюдан КҚ оқыс-оқиғаларының келіп түсуіне қарай (жұмыс күні ішінде не демалыс және мереке күндері аса маңызды КҚ оқыс-оқиғалары кезінде үшінші деңгейдің пассивті кезекшілік кестесіне сәйкес).

Аяқталу түрі: орындалуы, есеп дайындау немесе ден қоюдың төртінші деңгейіне беру.

33. КҚ оқыс-оқиғаларына ден қою (4-деңгей).

"МТҚ" АҚ нысаналы кибершабуылдарға ден қою мақсатында қажет болған жағдайда мынадай іс-шараларды жүзеге асырады:

негізгі статикалық және динамикалық талдау арқылы құралдар мен утилиталарды бастапқы зерттеу;

жедел жад дамптарын зерттеу, күмәнді процестер мен артефактілерді анықтау және бөліп алу;

серверлердің қатқыл дискілері дамптарын зерттеу.

"ҰАТ" АҚ зерттеу объектілерінің ұсынылуын қамтамасыз етеді. Жүргізілген зерттеу нәтижелері бойынша "МТҚ" АҚ-ның ішкі актілерінде айқындалған нысан бойынша есеп жасалады.

Аяқталу түрі: зерттеу нәтижелері бойынша есеп.

34. КҚ оқыс-оқиғаларына ден қою нәтижелері бойынша анықталған осалдықтар мен кемшіліктерді жою.

"ҰАТ" АҚ КҚ оқыс-оқиғаларына ден қою нәтижелері бойынша анықталған осалдықтар мен кемшіліктерді жою жөнінде тиісті шаралар қабылдайды, бұл ретте " МТҚ" АҚ жүргізілген жұмыстарға бақылауды жүзеге асырады.

"ҰАТ" АҚ осалдықтар мен кемшіліктерді жою шеңберінде бұрын тәжірибеде кездеспеген жаңа осалдықты жою жөніндегі іс-қимылдардың реттілігі бойынша ұсынымдары бар егжей-тегжейлі ақпаратты "МТҚ" АҚ-дан сұратуы мүмкін.

Кезеңділігі: осалдық анықталған сайын.

Аяқталу түрі: орындалуы.

35. Реактивті сервис шеңберінде (КҚ оқыс-оқиғаларына ден қою) анықталған КҚ оқыс-оқиғалары туралы ЦО меншік иелерін хабардар ету.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады. "ҰАТ" АҚ ЦО меншік иесімен бірлесіп тиісті шараларды қабылдайды.

Кезеңділігі: тұрақты негізде, КҚ оқыс-оқиғалары анықталған сайын.

Аяқталу түрі: хабарлама.

5-тарау. ЦО КҚ қамтамасыз ету жөніндегі іс-шаралар

(әзірлеу)

36. Қауіпсіз әзірлеу әдіснамасына сәйкес ЦО әзірлеу.

ЦО меншік иелері осы әдістемелік ұсынымдардың талаптарын сақтайды. Бұл ретте "ҰАТ" АҚ ЦО меншік иелеріне барлық қажетті есептеу ресурстары мен құралдарын ұсынады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

37. ЦО үшін КҚ қатерлерінің моделін әзірлеу.

Жұмыстардың негізгі орындаушысы ЦО меншік иесі болып табылады, ол КҚ қатерлерінің моделін бекітеді, ал "МТҚ" АҚ көрсетілген құжатты келіседі.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: құжат.

38. ЦО арналған ТТ келісу.

Осы жұмыстың негізгі орындаушысы Заңның 7-1-бабының 23) тармақшасына сәйкес уәкілетті орган болып табылады. Бұл ретте "МТҚ" АҚ Заңның 14-бабы 1-тармағының 3) тармақшасына сәйкес "цифрлық үкіметтің" ЦО құруға немесе дамытуға арналған ТТ киберқауіпсіздік талаптарына сәйкестігі тұрғысынан сараптама жүргізеді.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: уәкілетті органмен келісілген техникалық тапсырма.

39. ЦО меншік иелеріне QazTech порталындағы БКТ құралдарына қол жеткізуді ұйымдастыру.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады, бұл ретте "МТҚ" АҚ көрсетілген қол жеткізу құқықтарын келісуді жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

40. Unit-тестілеуді (функционалдылықты тексеруді) жүргізу және код сапасын тексеру.

Unit-тестілеуді (функционалдылықты тексеруді) жүргізуді және код сапасын тексеруді ЦО меншік иелері цифрлық объектіні ТТ қатаң сәйкестікте әзірлеу мақсатында жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

41. Әзірлеу ортасында БКТ (SAST, DAST, MAST, SCA, Container Security, IaC Security) жүргізу.

Әзірлеу ортасында БКТ-ы ЦО меншік иелері QazTech платформасында іске асырылған құралдарды (талдағыштарды) пайдалана отырып жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

42. Бастапқы кодты талдау (SAST, DAST, MAST, SCA, Container Security, IaC Security, Unit-тест).

ЦО меншік иелеріне ЦО пайдалану ортасына орналастырғанға дейін тестілеу кезеңінде бастапқы кодты талдау рәсімдерін өз бетінше жүргізу мүмкіндігі беріледі.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: бастапқы кодты талдау.

43. PROD ортасына орналастыруға өтінім беру (келісілген ТТ болған кезде).

ЦО меншік иелері ЦО-ы PROD ортасына (пайдалану ортасы) орналастырғанға дейін "ҰАТ" АҚ-ға тиісті өтінім береді. Бұл ретте "ҰАТ" АҚ өтінімді жұмысқа қабылдайды, ал "МТҚ" АҚ өтінімді келіседі не оны қабылдамау туралы шешім қабылдайды.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орналастыру немесе цифрлық объектіні PROD ортасына орналастырудан дәлелді бас тарту.

44. Осалдықтарды анықтау үшін аспаптық сканерлеу жүргізу.

Осалдықтарды анықтау мақсатында PROD ортасында аспаптық сканерлеу жүргізіледі. Жаңартулардың болуына сканерлеу, конфигурацияларды талдау, БҚ жалпы осалдықтар мен тәуекелдер дерекқоры бойынша белгілі осалдықтарының болуын тексеру, сонымен қатар КҚ қамтамасыз ету саласындағы стандарттарға сәйкестігін бағалау жүзеге асырылады. Виртуалды серверлер сканерлеуге жатады.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте ЦО меншік иелері және (немесе) "ҰАТ" АҚ оның жұмыскерлеріне серверлер мен желілік құрылғыларға артықшылықты құқықтармен (root құқықтары бар есептік жазба) қашықтан желілік қол жеткізуді қамтамасыз етеді.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: сканерлеу туралы есеп.

45. ЦО Қазақстан Республикасы заңнамасының және КҚ қамтамасыз ету саласындағы стандарттардың талаптарына сәйкестігін тексеру.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте ЦО меншік иелері көрсетілген жұмыстарды орындау үшін тиісті қол жеткізу құқықтарын қамтамасыз етеді.

Кезеңділігі: әрбір өзгеріс енгізілген кезде.

Аяқталу түрі: тексеру туралы есеп.

46. ЦО бойынша КҚ саясаты және КҚ ТҚ.

ЦО меншік иелері "ҰАТ" АҚ-ның қатысуымен пайдаланушылар басшылыққа алатын құжатталған қағидалардың, рәсімдердің, практикалық тәсілдердің немесе басшылыққа алушы қағидаттардың төрт деңгейлі жүйесі түріндегі КҚ ТҚ әзірлейді. " МТҚ" АҚ құжаттаманы әзірлеу кезінде бақылауды қамтамасыз етеді.

Кезеңділігі: ЦО енгізу кезінде және кейіннен ҚРҮҚ БТ сәйкес қайта қарау арқылы.

Аяқталу түрі: цифрлық объектінің меншік иесі бекіткен КҚ ТҚ.

47. QazTech платформасында ЦО әзірлеу және орналастыру бөлігінде Pipeline CI/CD үшін конфигурацияны әзірлеу.

ЦО меншік иесі әзірленіп жатқан ЦО шеңберінде әдістемелік ұсынымдарға сәйкес Pipeline CI/CD конфигурациясын әзірлейді.

"МТҚ" АҚ ЦО меншік иесінің Pipeline CI/CD мазмұны мен конфигурациясын зерделейді, оның құжаттамаға сәйкестігіне талдау жүргізеді, содан кейін QazTech платформасындағы жобада одан әрі пайдалану үшін Pipeline CI/CD-ны келіседі. Өнімді ортада кодты өрістету үшін пайдаланылатын Pipeline CI/CD-ға енгізілетін өзгерістер " МТҚ" АҚ-мен келісу рәсімінен өтеді.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: QazTech платформасында ЦО әзірлеу және орналастыру бөлігіндегі Pipeline CI/CD конфигурациясы.

48. КҚ қамтамасыз ету бөлігінде Pipeline CI/CD үшін конфигурацияны әзірлеу.

ЦО меншік иесі қауіпсіз әзірлеу әдістемесіне сәйкес КҚ қамтамасыз ету бөлігінде Pipeline CI/CD конфигурациясын әзірлейді.

"МТҚ" АҚ ЦО меншік иесінің Pipeline CI/CD жүйесіне талдау жүргізеді және оны QazTech платформасындағы жобада одан әрі пайдалану үшін Pipeline CI/CD форматы мен мазмұнын келіседі.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: КҚ қамтамасыз ету бөлігіндегі Pipeline CI/CD конфигурациясы.

49. Цифрлық платформаның басқа ЦО интеграциялауды келісу.

ЦО басқа ЦП ЦО-мен өзара іс-қимылын қамтамасыз ету қажет болған жағдайда ЦО меншік иелері интеграциялауға өтінім жібереді, ал "ҰАТ" АҚ "МТС" АҚ-мен келісу бойынша интеграциялауды қамтамасыз етеді.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: келісу немесе дәлелді бас тарту.

50. ЦО КҚ ТҚ талаптарының сақталуына ішкі бақылау.

"ҰАТ" АҚ ЦО-дағы КҚ ТҚ талаптарының сақталуына ішкі бақылауды қамтамасыз етеді, бұл ретте ЦО меншік иесі бақылау жөніндегі жұмыстарды орындау кезінде өзінің жауапты тұлғасының қатысуын қамтамасыз етеді.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: есеп.

51. ЦО КҚ ТҚ талаптарының сақталуына сыртқы бақылау.

"МТҚ" АҚ ЦО-дағы КҚ ТҚ талаптарының сақталуына сыртқы бақылауды қамтамасыз етеді, бұл ретте "ҰАТ" АҚ және ЦО меншік иелері жұмыстарды орындау кезінде өздерінің жауапты тұлғаларының қатысуын қамтамасыз етеді.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: есеп.

52. ОЖ, ДББЖ және ҚБҚ етудің КҚ талаптарына сәйкестігін (әзірлеу, тестілеу және өнеркәсіптік пайдалану орталарына бөлінуін қоса алғанда) чек-парақ бойынша тексеру.

"МТҚ" АҚ ОЖ, ДББЖ және ҚБҚ ету деңгейінде КҚ талаптарына сәйкестігін тексеруді жүзеге асырады, бұл ретте "ҰАТ" АҚ және ЦО меншік иелері жауапты тұлғалардың (әкімшілердің, КҚ мамандарының) қатысуымен қауіпсіздік саясаттарын көрсетуді қамтамасыз етеді.

QazTech платформасының серверлік жабдығын тексеру кезінде "МТҚ" АҚ жұмыскерлері Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарын басшылыққа алады.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: есеп.

53. Қазақстан Республикасының КҚ қамтамасыз ету саласындағы заңнамасы мен стандарттарының талаптарына сәйкестігін тексеру.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ және ЦО меншік иелері көрсетілген жұмыстарды жүргізу үшін қажетті қол жеткізу құқықтарын қамтамасыз етеді.

Кезеңділігі: жылына 1 рет.

Аяқталу түрі: есеп.

54. Осалдықтарды анықтау үшін аспаптық сканерлеу жүргізу.

Жаңартулардың болуына сканерлеуге және конфигурацияларды талдауға, БҚ жалпы осалдықтар мен тәуекелдер дерекқорындағы белгілі осалдықтарының болуына, сонымен қатар КҚ қамтамасыз ету саласындағы стандарттарға сәйкестігіне ЦО шеңберіндегі виртуалды серверлер мен желілік жабдық жатады.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ және ЦО меншік иелері оның жұмыскерлеріне серверлер мен желілік құрылғыларға артықшылықты құқықтармен (root құқықтары бар есептік жазба) қашықтан желілік қол жеткізуді қамтамасыз етеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: сканерлеу туралы есеп.

55. Жүктемелік тестілеу.

ЦО жүктемелік тестілеуі қалыпты пайдалану ортасында қолжетімділіктің, тұтастықтың және құпиялылықтың сақталуын бағалау мақсатында жүргізіледі. Жүктемелік тестілеу дербес деректер жалған деректермен алмастырылған қалыпты пайдалану ортасында автоматтандырылған сценарийлер негізінде мамандандырылған бағдарламалық құралды пайдалана отырып жүргізіледі. Жүктемелік тестілеу пайдаланушылардың қосылу нүктелерінің саны және интеграциялық өзара

іс-қимылдың қосылу нүктелерінің нұсқалары бойынша жүргізіледі. Бұл ретте тестілеу сценарийі, тестілеудің уақытша және сандық сипаттамалары айқындалады, сонымен қатар тестілеуді өткізу уақыты ЦО меншік иелерімен келісіледі.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте ЦО меншік иелері оның жұмыскерлеріне жұмыстарды орындау үшін қажетті қол жеткізу құқықтарын қамтамасыз етеді.

Кезеңділігі: жарты жылда 1 рет немесе әрбір өзгеріс енгізілген кезде.

Аяқталу түрі: жүктемелік тестілеу туралы есеп.

56. "Қолмен" режимде енуге тестілеу (Pentest/Red Team) жүргізу.

Жұмыстардың негізгі орындаушысы "МТҚ" АҚ болып табылады, бұл ретте "ҰАТ" АҚ және ЦО меншік иелері оның жұмыскерлеріне серверлер мен желілік құрылғыларға шектеулі құқықтармен ("user" түріндегі) қашықтан желілік қол жеткізуді қамтамасыз етеді.

"МТҚ" АҚ Pentest-ті "қолмен" тестілеу режимінде жүргізеді.

Кезеңділігі: жарты жылда 1 рет.

Аяқталу түрі: Pentest жүргізу нәтижелері бойынша қорытынды.

57. Жүйелік және қолданбалы бағдарламалық қамтылымның конфигурациясын және Git кодын баптау.

ЦО меншік иесі "ҰАТ" АҚ-мен бірлесіп QazTech платформасының әдістемесіне және КҚ талаптарына сәйкес жүйелік және қолданбалы БҚ конфигурациясын, сондай-ақ Git-тегі кодты баптауды жүзеге асырады.

"МТҚ" АҚ әдістемеге және КҚ талаптарына сәйкестігін тексеруді жүргізеді және жүйелік әрі қолданбалы БҚ конфигурацияларын және Git-тегі кодты қолдануды келіседі. "МТҚ" АҚ ЦО өнімді серверлеріндегі жүйелік және ҚБҚ конфигурациясына бақылауды жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

58. Резервтік көшірмелерді жасау және оларды қалпына келтіруді тестілеу.

"ҰАТ" АҚ және цифрлық объектілердің меншік иелері цифрлық объектінің барлық деңгейлерінде (ҚБҚ, ОЖ, деректер базалары) резервтік көшірмелерді жасауды және оларды қалпына келтіруді тестілеуді қамтамасыз етеді, ал "МТҚ" АҚ олардың орындалуына бақылауды қамтамасыз етеді.

Кезеңділігі: КҚ ТҚ сәйкес тұрақты негізде.

Аяқталу түрі: орындалуы.

59. Шифрлау кілттері мен парольдердің қауіпсіздігі (Vault).

ЦО меншік иесі өнімді ортада құпия деректерді (парольдер, токендер, шифрлау кілттері және т.б.) қауіпсіз сақтау және пайдалану мақсатында құпияларды басқару жүйесін (Vault) пайдаланады.

"ҰАТ" АҚ Vault жүйесінің журналдарын (оның ішінде кілттерді пайдалану оқиғаларын) SIEM жүйесіне жіберуді қамтамасыз етеді. "МТҚ" АҚ журналдардың жіберілуіне бақылауды және кілттерді пайдалану оқиғаларына мониторингті жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

60. AV, EDR, Sandbox сыныптарындағы ақпаратты қорғау құралдарын орнату және конфигурациялау.

АҚҚ орнату және конфигурациялау процестерін "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ КҚ оқиғалары көздерінің (AV, EDR, Sandbox) бағдарламалық құралдарын орнату, сонымен қатар КҚ оқиғалары көздерінің жекелеген жұмыс тетіктері мен қауіпсіздік саясаттарын баптау бойынша жүргізілген жұмыстарға бақылауды жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

61. IDS/IPS/NGFW виртуалдандыру және PAM сыныптарындағы АҚҚ орнату және конфигурациялау.

"МТҚ" АҚ PAM жүйесінің саясаттарын, рөлдерін, қол жеткізу құқықтарын баптауды келіседі және олардың қолданылуына бақылауды жүзеге асырады. "ҰАТ" АҚ QazTech платформасының артықшылықты пайдаланушыларын бақылау жүйесін орнатуды және конфигурациялауды жүзеге асырады, сонымен қатар саясаттарды баптауды қамтамасыз етеді.

"ҰАТ" АҚ IDS/IPS/NGFW сыныптарындағы ақпаратты қорғау құралдарын монтаждауды және конфигурациялауды жүзеге асырады, бұл ретте "МТҚ" АҚ IDS/IPS/NGFW сыныптарындағы АҚҚ орнату мен баптауға бақылауды жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

62. Оқиғалар көздерін QazTech платформасына қосу.

Оқиғалар көздерін QazTech платформасының цифрлық инфрақұрылымына қосу процестерін ЦО меншік иесі және "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ КҚБЖ (SIEM) жекелеген жұмыс тетіктері мен қауіпсіздік саясаттарын баптау, жұмыстың дұрыстығын тексеру, сонымен қатар КҚБЖ (SIEM) оқиғаларды тіркеу журналдарынан мәліметтерді орталықтандырылған жинауды қамтамасыз ету бойынша жүргізілген жұмыстарды келісуді және бақылауды жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

63. КҚ оқиғалары көздерінің жай-күйін, олардың параметрлері мен қорғау режимдерін бақылау, оның ішінде олардың жұмысындағы қателер мен кемшіліктерді жою.

КҚ оқиғалары көздерінің жай-күйін, олардың параметрлері мен қорғау режимдерін бақылауды, сонымен қатар олардың жұмысындағы қателер мен кемшіліктерді жоюды ЦО меншік иесі және "ҰАТ" АҚ жүзеге асырады, бұл ретте "МТҚ" АҚ серверлік жабдықтың, операциялық жүйелердің, АҚҚ БҚ жұмысқа қабілеттілігі және QazTech платформасы мен КҚ оқиғалары көздері арасындағы байланыс арналарының қолжетімділігі бөлігінде жүргізілген жұмыстарға бақылауды жүзеге асырады.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

64. AV, EDR, Sandbox сыныптарындағы АҚҚ саясаттарын баптау.

"ҰАТ" АҚ техникалық құжаттамаға және ақпаратты қорғау құралдарын өндірушінің ұсынымдарына сәйкес цифрлық объект үшін AV, EDR және Sandbox сыныптарындағы ақпаратты қорғау құралдарының конфигурация параметрлерін (саясаттарын) мерзімді түрде өзгертуді жүзеге асырады. "МТҚ" АҚ оқиғалар журналдарының негізінде ақпаратты қорғау құралдарының дұрыс жұмыс істеуіне диагностика жүргізеді және қажет болған жағдайда конфигурация параметрлеріндегі (саясаттардағы) кемшіліктер туралы "ҰАТ" АҚ-ны хабардар етеді.

Конфигурация параметрлерін (саясаттарды) өзгерту, диагностикалау және олардағы кемшіліктерді жою ЦО меншік иелерінің өтінімдері (сұрау салуы) бойынша жүзеге асырылуы мүмкін.

Кезеңділігі: қажеттілігіне қарай.

Аяқталу түрі: өзгертілген саясаттар.

65. IDS/IPS/NGFW, PAM және DLP сыныптарындағы АҚҚ саясаттарын баптау.

"ҰАТ" АҚ QazTech платформасының артықшылықты пайдаланушыларын бақылау жүйесін орнатуды және конфигурациялауды жүзеге асырады. "МТҚ" АҚ PAM жүйесінің саясаттарын қолдануды келісуді және бақылауды жүзеге асырады. "ҰАТ" АҚ IDS/IPS/NGFW сыныптарындағы АҚҚ саясаттарын баптауды жүзеге асырады, ал " МТҚ" АҚ IDS/IPS/NGFW сыныптарындағы АҚҚ саясаттарының қолданылуына бақылауды қамтамасыз етеді.

Кезеңділігі: тұрақты негізде.

Аяқталу түрі: орындалуы.

66. Қауіптер мен КҚ оқыс-оқиғаларын анықтау алгоритмдері мен корреляция қағидаларын әзірлеу мақсатында КҚБЖ келіп түсетін деректерді талдау.

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады. Қауіптер мен КҚ оқыс-оқиғаларын анықтау алгоритмдері мен корреляция қағидаларын әзірлеу кезінде " ҰАТ" АҚ "МТҚ" АҚ жұмыскерлеріне КҚБЖ артықшылықты құқықтармен ("root" құқықтары бар есептік жазбалар) қашықтан желілік қол жеткізуді қамтамасыз етеді.

ЦО-да AV, EDR және Sandbox сыныптарындағы АҚҚ арқылы нысаналы кибершабуылдар анықталған жағдайда, "МТҚ" АҚ тиісті тактикаларды, техникаларды

және рәсімдерді, соңғы нүктелердің артефактілерін, желілік артефактілерді және ымыраға келу индикаторларын ескеретін тиісті корреляция қағидаларын әзірлейді.

Кезеңділігі: күн сайын.

Аяқталу түрі: КҚБЖ корреляция қағидалары.

67. QazTech платформасының КҚБЖ арқылы киберқауіпсіздік мониторингі және КҚ оқыс-оқиғаларына бастапқы ден қою (1-деңгей).

Жұмыстардың негізгі орындаушысы "ҰАТ" АҚ болып табылады.

Кезеңділігі: тәулік бойы.

Аяқталу түрі: тәулік бойғы мониторинг, орындалуы.

68. КҚ оқыс-оқиғаларына ден қою (2-деңгей).

Екінші деңгейдегі ден қою шеңберінде "МТҚ" АҚ өтініш берушілерге КҚ оқыс-оқиғаларын тергеп-тексеруге, артефактілерді талдауға, қосымша ақпарат жинауға және КҚ қатерлерін/оқыс-оқиғаларын жою жөніндегі ұсынымдарды дайындауға жәрдем көрсетеді. Қажет болған жағдайда киберқауіпсіздік оқыс-оқиғаларына ден қоюдың үшінші/төртінші деңгейіне эскалацияланады.

Кезеңділігі: қажеттілігіне қарай ("МТҚ" АҚ КҚ оқыс-оқиғаларын пысықтау кезінде "ҰАТ" АҚ-мен бірлесіп жұмыс күні ішінде немесе демалыс және мереке күндері аса маңызды КҚ оқыс-оқиғалары кезінде екінші деңгейдің пассивті кезекшілік кестесіне сәйкес жәрдем көрсетеді).

Аяқталу түрі: "ҰАТ" АҚ-ға есепті/ұсынымдарды ұсыну немесе ден қоюдың үшінші/ төртінші деңгейіне эскалациялау.

69. КҚ оқыс-оқиғаларына ден қою (3-деңгей).

"МТҚ" АҚ ден қоюдың үшінші деңгейінде қолдау көрсетеді, оған тергеп-тексеруге техникалық және сараптамалық қолдау көрсету, атап айтқанда КҚ оқыс-оқиғаларының туындау себептерін талдау, форензикалық зерттеу жүргізу, артефактілерді зерттеу, КҚ оқыс-оқиғасының қайталануын болдырмау жөніндегі шараларды әзірлеу және талдау нәтижелері бойынша есепті "ҰАТ" АҚ-ға ұсыну кіреді.

Кезеңділігі: екінші деңгейдегі ден қоюдан КҚ оқыс-оқиғаларының келіп түсуіне қарай (жұмыс күні ішінде немесе демалыс және мереке күндері аса маңызды КҚ оқыс-оқиғалары кезінде үшінші деңгейдің пассивті кезекшілік кестесіне сәйкес).

Аяқталу түрі: орындалуы, есеп дайындау немесе ден қоюдың төртінші деңгейіне беру.

70. КҚ оқыс-оқиғаларына ден қоюды қолдау (4-деңгей).

"МТҚ" АҚ нысаналы кибершабуылдарға ден қою мақсатында қажет болған жағдайда мынадай іс-шараларды жүзеге асырады:

негізгі статикалық және динамикалық талдау арқылы құралдар мен утилиталарды бастапқы зерттеу;

жедел жад дамптарын зерттеу, күмәнді процестер мен артефактілерді анықтау және бөліп алу;

серверлердің қатқыл дискілері дамптарын зерттеу.

"ҰАТ" АҚ және ЦО меншік иесі көрсетілген зерттеу объектілерінің ұсынылуын қамтамасыз етеді.

Аяқталу түрі: жүргізілген зерттеу нәтижелері бойынша "МТҚ" АҚ-ның ішкі актілерінде айқындалған нысан бойынша есеп жасалады.

71. КҚ оқыс-оқиғаларына ден қою нәтижесінде анықталған осалдықтар мен кемшіліктерді жою.

ЦО меншік иесі КҚ оқыс-оқиғаларына ден қою нәтижесінде анықталған осалдықтар мен кемшіліктерді жою жөнінде тиісті шаралар қабылдайды, бұл ретте "МТҚ" АҚ жүргізілген жұмыстарға бақылауды жүзеге асырады.

"ҰАТ" АҚ осалдықтар мен кемшіліктерді жою шеңберінде бұрын тәжірибеде кездеспеген жаңа осалдықты жою жөніндегі іс-қимылдардың реттілігі бойынша ұсынымдары бар егжей-тегжейлі ақпаратты "МТҚ" АҚ-дан сұратуы мүмкін.

Кезеңділігі: осалдық анықталған сайын.

Аяқталу түрі: орындалуы.

72. ЦП ЦО меншік иелерін, иеленушілерін және пайдаланушыларын өздеріне қатысты бөлігінде КҚ оқыс-оқиғалары туралы хабардар ету.

ЦО меншік иесі тапсырыс берушіні/клиенттерді өздеріне қатысты бөлігінде анықталған КҚ оқыс-оқиғалары туралы хабардар етеді, бұл ретте "МТҚ" АҚ жүргізілген жұмыстарға бақылауды жүзеге асырады.

Кезеңділігі: КҚ оқыс-оқиғасы анықталған сайын.

Аяқталу түрі: хабарлама.