Қайырлы күн, құрметті студенттер! Барлығыңызды көргеніме қуаныштымын. Біз, міне, 4-модульге де келіп жеттік, және бүгін бұлттағы қауіпсіздік, яғни AWS Cloud Security туралы сөйлесеміз.

Сондай-ақ, AWS қауіпсіздікпен байланысты бірқатар сервистерді талқылаймыз. Кейбір сервистерді толығымен, ал кейбіреулері жайлы азырақ айтатын боламыз, дәлірек айтқанда, біз онша танымал емес сервистердің ең негізгі тармақтары мен анықтамаларына тоқталамыз. Дегенмен, бұл сервистер нақты AWS емтиханында кездесуі мүмкін, сондықтан біздің дәрістерімізде алатын білім мен ақпарат нақты AWS емтиханындағы сұрақтарға сәтті жауап беру үшін жеткілікті болады.

Әр бөлімге қысқаша шолу жасайық. Біріншісі – AWS shared responsibility model. Біз оның не екенін және оның бізге қалай көмектесетіні туралы айтатын боламыз. Әрі қарай біз AWS IAM сервисімен танысамыз. Осыдан кейін біз жаңа AWS аккаунтын қауіпсіздендіруге көмектесетін қадамдарды анықтаймыз. Және қауіпсіздікке қатысты кейбір AWS сервистерін қарастырамыз. Сондай-ақ, бұлттағы деректерді қалай қорғауға болатындығы туралы сөйлесеміз.

Біз бірінші бөлімді бастаймыз, атап айтқанда AWS shared responsibility model. Бұлттағы қауіпсіздікті екіге бөліп қарастырамыз: біріншісі – бұлтты пайдаланушылар, яғни біз, ал екіншісі – бұлтты провайдер. Соған сәйкес логикалық тұрғыдан жауапкершілікті де екі бөлікке бөлеміз. Бұлтты провайдер security of the cloud, яғни бұлттың қауіпсіздігіне, жауап береді. Бұлтты пайдаланушылар, яғни біз туралы айтатын болсақ, біз security in the cloud, бұл дегеніміз бұлттағы қауіпсіздікке біз жауап беретінімізді білдіреді.

Біз AWS бұлтты провайдері бұлттың қауіпсіздігіне жауапты екенін айттық. Ал бұл нені білдіреді? Бұл тәулік бойы, яғни 24/7 дата-центрінің физикалық қауіпсіздігін және бөгде адамдардың осы дата-центрге кіруіне жол бермеу үшін қажетті күзетпен қамтамасыз етеді деген сөз. Келесі – hardware and software infrastructure қауіпсіздігі, бұл барлық аппараттық құрал, яғни біздің серверлер, қатты дискілер және AWS-ке тиесілі кез келген басқа жабдықтардың қауіпсіздігін білдіреді. Содан кейін software infrastructure, бұған операциялық жүйелердің, барлық қосымшалар мен виртуалдандыру қосымшаларын қауіпсіздікпен қамтамасыз ету және үнемі жаңартып отыруы кіреді. Әрі физикалық не виртуалды тұрғыдан бұлтты провайдердің шекарасына бөтен адам кіре алмайтындай әртүрлі қауіпсіздік жаңартулары орнатылады.

Әрі қарай, біз желілік инфрақұрылымның қауіпсіздігі және виртуалдандыру туралы, яғни біздің роутерлар, свитч, load balancer, firewall, кабельдер және т.б. жайлы сөйлесеміз.

Өкінішке орай, біз кез-келген дата-центрді барып көре де, тексере де алмаймыз, өйткені бұл рұқсат етілмейді, бірақ бұл инфрақұрылымның қауіпсіз және стандарттарға сәйкес келетінін тексеріп, тиісті есептерді шығару үшін, AWS арнайы аудиторларды үнемі шақырып отырады. Әрі қажет болған жағдайда мезгіл-мезгіл шығатын барлық есептерді тегін жүктеуге мүмкіндік береді.

Енді пайдаланушының, яғни біз неге жауапты екенімізді және бұлттағы қауіпсіздікті қалай қамтамасыз ету керектігін мұқият қарастырайық. Егер біз Amazon EC2-ді қолданатын болсақ, жаңартылған және қауіпсіздік мәселелері жоқ операциялық жүйені таңдау біздің міндетіміз, бірақ қандай да бір мәселелер туындаса, біз қауіпсіздік патчтарының бәрін орнатуымыз керек. Содан кейін осалдығы жоқ қосымшаларды таңдау да біздің міндетіміз, немесе егер болса, тиісті қауіпсіздік патчтарды қолдануымыз керек. Инфрақұрылым туралы айтқан кезде, желілерді орнатқан кезде біз security топтарын дұрыс баптауымыз керек және қауіпсіздік саңылаулары болмауы үшін бүкіл желі дұрыс бапталынуы керек. Сондай-ақ, сіз командаңызбен Account management өткізуді, қауіпсіздік кілттерін, логиндерді, парольдерді және т.б. қалай дұрыс сақтау жайлы сөйлесуіңіз керек. Ал ең бастысы – біздің деректеріміздің қауіпсіздігі, біз деректерді тасымалдаған кезде, яғни in transit кезінде деректер шифрланған болуы керек және біздің деректеріміздің қауіпсіздігі at rest, яғни оларды сақтау кезінде де шифрлану керек. Бұл ықтимал шабуылдарды болдырмау, деректердің жоғалуы, инфрақұрылым мен барлық жұмыс процесінің бұзылуының алдын алуын қамтамасыз етеді.

Енді мен сервисті жеткізу үлгісі тұрғысынан қауіпсіздік мәселелерін қарастырғым келеді. Естеріңізде болса, бізде сервисті жеткізу үлгісінің үш түрі бар: IaaS, PaaS және SaaS. Мұндағы басты идея – IaaS-тан SaaS-қа дейін ІТ-ресурстарын басқару деңгейі азайып, біздің басқару міндетіміз азайған бөлікті бұлтты провайдерге өткіземіз, енді бұл бөліктің қауіпсіздігін бұлтты провайдер қамтамасыз етуі керек болады.

Мысалы, IaaS жағдайында біз Amazon EC2 туралы айтып отырмыз, ал қауіпсіздік біздің жағымызда қала береді. Amazon RDS туралы айтсақ, бұл PaaS шешімі, біз енді операциялық жүйеге де, оның қауіпсіздігіне де жауап бермейміз. Өйткені біз оны бұлтты провайдерге өткіздік. Software as a Service жайлы айтқан кезде, мысалы, электрондық пошта немесе Amazon Chime сервисі, бұл Zoom аналогы, олар дайын қосымша ретінде беріледі, ал іс жүзінде бізде басқару деңгейі аз немесе оны өзгерту үшін басқару деңгейі мүлде жоқ. Осылайша, бізге байланысты емес барлық операциялар бұлтты провайдердің көмегімен қауіпсіздендірілуі керек.

Мен өткен материалды бекіту үшін сіздермен біраз жаттығу жасағым келеді. Мен сұрақтар қоямын, ал сіз дұрыс жауап беруіңіз керек: бұған AWS жауапты және ол security of the cloud болып саналады немесе security in the cloud болып есептеліп, қауіпсіздікке бұлт пайдаланушылары, яғни біз жауаптымыз.

Енді мен инфрақұрылым жайлы тез айтып өтейін. Бізде AWS аккаунты бар делік. Біз Amazon S3 сервисін қолданамыз, содан кейін VPC сервисін қолданамыз, онда бізде Amazon EC2 инстанстары, сондай-ақ Oracle дерекқорының инстанстары бар. Енді сұрақтарды қарап шығайық. Сіз видеоны тоқтатып, ойланып дұрыс жауап беруіңіз керек.

Бірінші сұрақ. Amazon EC2 инстансында операциялық жүйенің қауіпсіздік патчтарын жаңарту және орнату. Видеоны тоқтатып, ойланып көріңіз. Дұрыс жауабы: the customer, яғни пайдаланушылар бұл үшін жауапты.

Келесі сұрақ. Дата-центрдің физикалық қауіпсіздігі? Дұрыс жауабы: AWS.

Үшінші сұрақ. Виртуалдандыру кезінде инфрақұрылым қауіпсіздігіне кім жауап береді? Дұрыс жауабы: AWS.

Келесі сұрақ. Amazon EC2 инстансында security group-ты дұрыс бапталуына кім жауап береді? Дұрыс жауап: the customer, яғни біз.

Бесінші сұрақ. Amazon EC2-де жұмыс істейтін қосымшалар баптаулары, яғни конфигурациялардың қауіпсіздігіне кім жауап береді? Дұрыс жауабы: the customer, яғни біз бұл үшін жауаптымыз.

Келесі сұрақ. Amazon RDS инстансы ретінде іске қосылатын Oracle инстансы үшін қауіпсіздік патч жаңартуларын орнатуға кім жауап береді? Дұрыс жауабы: AWS. Біз опреациялық жүйені баптамаймыз немесе қауіпсіздікті жаңартпаймыз, өйткені ол PaaS шешімі ретінде беріледі және AWS бұл үшін жауапты болғандықтан, ол осы бөліктің қауіпсіздігіне де жауап береді. Біз жай ғана дайын дерекқорды сервис ретінде аламыз.

Келесі сұрақ. Amazon EC2 инстансында іске қосылған Oracle дерекқорының қауіпсіздік патчтары мен жаңартуларына кім жауап береді? Дұрыс жауабы – the customer, Oracle дерекқорын орналастырудың осы түріне біз жауаптымыз. Amazon EC2 инстанстарында жұмыс істейтін барлық операцияларға, Amazon EC2 инстансының қауіпсіздігіне, виртуалды қауіпсіздікке пайдаланушы жауапты.

Және соңғы сұрақ. Amazon S3 bucket қауіпсіздігіне қол жеткізуді дұрыс баптауға кім жауап береді? Дұрыс жауабы: the customer, демек біз бұл үшін жауаптымыз. AWS бізге осы мүмкіндіктерді bucket-ке баптауға рұқсат береді, ал біз оларды дұрыс орнатуға жауаптымыз.

Енді басқа архитектураны қарастырайық. Жаттығудың логикасы өзгеріссіз қалады. Мен сұрақ қоямын, сіз видеоны тоқататып, дұрыс жауап беруге тырысасыз, бұл үшін AWS жауап береді немесе пайдаланушы, яғни біз деп дұрыс жауабын табуыңыз керек. Ал, ендеше, кеттік.

Біздің инфрақұрылымымызда бапталған VPC бар, ал оның ішінде Amazon EC2 инстансында орнатылған веб-сервері бар бапталған subnet бар. Бұл инстанс Amazon S3 bucket-імен өзара әрекеттеседі, сонымен қатар біздің VPC-ге қосылған internet-gateway бар, оның көмегімен AWS Management Console арқылы немесе SSH кілттерін енгізу арқылы командалық жолына, яғни AWS CLI көмегімен веб-серверімізге қосыламыз.

Сонымен, бірінші сұрақ. Хакерлер AWS Management Console-ін бұза алмайтындай етіп қауіпсіздігін қамтамамсыз ету. Бұл үшін AWS жауап береді.

Әрі қарай, subnet-тердің дұрыс бапталынуы? Дұрыс жауабы: customer, яғни AWS бізге subnet-терді конфигурациялауға арналған құралдарды ұсынады, ал оларды дұрыс әрі қауіпсіз конфигурациялау біздің міндетімізге жатады.

Келесі сұрақ, VPC-дің дұрыс қауіпсіз конфигурациясы? Бұл үшін де біз жауаптымыз. Идея subnet-тегімен бірдей. Әрі қарай жүрейік.

AWS аймақтарында желінің істен шығуын қорғау? Дұрыс жауабы: AWS, яғни аймақтар арасындағы желі AWS жаһандық инфрақұрылымының бөлігі болып табылады, сондықтан AWS бұл үшін жауап береді.

SSH кілттерін қорғау? Бұған біз, яғни пайдаланушылар, SSH кілттерін қорғауға жауап береміз. Әрі қарай жүрейік.

Алтыншы сұрақ. AWS пайдаланушылардың деректері арасында желілік оқшаулауды қамтамасыз ету? Бұл үшін AWS жауап береді, яғни пайдаланушылар ретінде бізде басқа пайдаланушылардың деректеріне жетуге мүмкіндік болмағандықтан, оны ешқандай жолмен баптай алмаймыз. Сондықтан, AWS бұл үшін жауап береді.

Жетінші сұрақ. Веб-сервер мен Amazon S3 bucket арасындағы кең жолақты жылдам қатынауды қамтамасыз ету? Дұрыс жауабы: AWS, себебі бұл тағы да AWS-тің жаһандық инфрақұрылымына тиесілі, себебі Amazon EC2 инстансы мен Amazon S3 bucket сол жерде орналасқан. Осы екі сервис арасында жылдам қол жетімділікті қамтамасыз ету үшін біз интернетті пайдаланбаймыз, дәлірек айтсақ, AWS интернетті емес, тезірек және қауіпсіз әрекет ету үшін өзінің жаһандық инфрақұрылымын пайдаланады. Бұл үшін AWS жауап береді.

Және соңғы сұрақ. Пайдаланушыларды авторизациялау үшін MFA қолдануды ілгерілету? Бұл үшін customer, яғни біз жауап береміз. Идеясы қандай? Идея мынада, біз IAM ішінде пайдаланушыларды құрамыз, осылайша қарапайым физикалық пайдаланушылар, біздің қызметкерлер AWS аккаунтына берілген логин, құпиясөзді қолдана отырып кіре алады. Олардың барлығы бір AWS аккаунтында жұмыс істейді және логин мен құпиясөзден басқа, сіз MFA-ді де реттей аласыз. Әдетте, виртуалды MFA бапталған қосымша орнатылады және әр 30 секунд сайын жаңа алты таңбалы код жасалады, және авторизация кезінде пайдаланушы логин мен құпиясөзді енгізіп қана қоймайды, сонымен қатар авторизацияланған құрылғыға рұқсаты бар екенін растайды да, жаңа кілтті енгізеді, содан кейін әрі қарай кіреді. Осылайша MFA опциясын жылжыту және қосу толығымен customer-ге, яғни бізге байланысты болады. Ол бастапқыда өшіріліп тұрады, бірақ AWS-тің ұсынысы бойынша оны қосуға болады, дегенмен ол компанияның өзіне байланысты болғандықтан, кейбір жағдайда ол өшірулі тұрады. Ол неғұрлым үлкен болса, соғұрлым ол осалдықтар мен ықтимал шабуылдарға аса назар аударады, сондықтан MFA арқылы біз өзімізге аккаунттың бұзылмайтындығына және зиян келтірушілер бірдеңе ұрлап немесе инфрақұрылымды бұзып, AWS бұлтына қосыла алмайтынына кепілдік береміз. Осымен біз бірінші бөлімді аяқтаймыз.

Негізгі ойларға назар аударайық. Біз shared responsibility model не екенін қарастырдық және бұлттың толық қауіпсіздігі үшін екі тарап: яғни бұлтты провайдер және пайдаланушы, яғни біздің белгілі бір жерлерде қауіпсіздікті қамтамасыз етуіміз керек екендігі туралы әңгімелестік. Бұл нақты жерлерді екі бағытқа бөлуге болады, яғни AWS security of the cloud-ты қамтамасыз етеді, яғни бұлттың өзін, ал бұлттың ішінде жұмыс істейтін customer бұлттағы қауіпсіздікті қамтамасыз етеді, яғни security in the cloud. AWS жағдайында біз дата-центрдің, аппараттық құралдардың және оның қателіктері, қауіпсіздік саңылаулары болмауы үшін қолданылатын барлық бағдарламалық жасақтаманың физикалық қауіпсіздігін айтамыз және мұның бәрі мерзімінен бұрын жаңартылады. Сustomer туралы айтатын болсақ, біз ықтимал шабуылдар үшін кейбір жерлер ашылып қалмас үшін, дұрыс management, кілттерді басқарудың тиісті қауіпсіздігі, логиндер, құпиясөздер, яғни credentials және сіздің пайдаланушыларыңыз үшін осы дұрыс management конфигурациялауды айтамыз. Сондай-ақ, біз қолданатын сервиске байланысты олар сервис жеткізу үлгісінің үш түрі бар. Бұл IaaS моделі, PaaS моделі және SaaS моделі. Және осы деңгейлерге байланысты біздің ІТ-ресурсты басқаруымыз өзгереді, сәйкесінше, белгілі бір ресурстың қай бөлігінің қауіпсіздігіне жауап беретінімізді анықталады.

IaaS туралы айтатын болсақ, бізде IT-ресурстарға көбірек бақылау бар болғандықтан, бізде қауіпсіздікті қамтамасыз ету қажет жерлер көп болады. PaaS және SaaS туралы айтқан кезде, бізде бақылау азаяды. Тиісінше, бұлтты провайдер жауап беретін бөлік үшін өзі қауіпсіздікті қамтамасыз ететін болады. Бұл енді біздің міндетіміз емес.

Біз екінші бөлімге ауысамыз, яғни AWS Identity and Access Management сервисі, яғни AWS IAM. Бұл сіздің ағымдағы AWS аккаунтыңызға және оның құрамында болуы мүмкін барлық ресурстарға қатысты кез-келген қол жетімділікті қамтамасыз ететін сервис. Осылайша, біз осы сервис арқылы кім қандай ресурстарға қол жеткізе алатындығы, қалай және қандай жағдайларда қол жеткізуге болатындығы туралы айта аламыз және ескерте кететін бір жайт, AWS IAM – бұл біз төлемейтін тегін сервис.

Енді AWS IAM сервисінің негізгі компоненттерін қарастырайық. Бұл IAM user, IAM group, IAM policy және IAM role. Әр компоненттің өз мақсаты бар. IAM user туралы айтатын болсақ, бұл өзінің жеке идентификаторы бар ұйым, сонымен қатар өзінің ARN, кіру кілттері, логині, құпиясөздері бар және біз бұл ақпаратты компаниядағы қызметкерге бере аламыз, осылайша ол біздің user-іміз арқылы бұлттағы АWS аккаунтымызға қосыла алады.

Әрі қарай, бізде IAM groups бар, енді біз өз пайдаланушыларымызды осы топтарда біріктіре аламыз. Бұл бізде ұқсас міндеттері бар бірнеше пайдаланушылар болған кезде қолданылады, немесе кем дегенде, олар бұлтта қолжетімділікке теңдей ие болуы керек, біз бұл пайдаланушыларды тиісті атаумен арнайы құрылған топқа қосып, топқа қажетті құқықтарды бере аламыз. Осылайша, онда отыратын барлық пайдаланушылар тиісті сервистер мен іс-шараларға қол жеткізе алады. Айта кету керек бір жайт, бір топта бірнеше пайдаланушы болуы мүмкін, және әр пайдаланушы бірнеше топта болуы мүмкін. Бұл да дұрыс. Мысалы, пайдаланушы белгілі бір сервистер жиынтығына бір топ арқылы қол жеткізе алады және басқа топ арқылы басқа сервистерге қол жеткізе алады. Осылайша, ұжымдық түрде ол тек бір топта отыратын басқа пайдаланушыға қарағанда көбірек сервистерге қол жеткізе алады. Сондай-ақ, AWS ішінде әр пайдаланушының кіруін нақтырақ баптауға болады.

IAM policy жайлы айтатын болсақ, бұл JSON түрінде сипатталған құжат және ол қандай ресурстарға, қандай операцияларға қол жеткізе алатынымызды сипаттайды, бірақ қандай нысан екені белгіленбейді, біз policy-ді тікелей user-ге немесе group-қа байланыстырамыз. Тұтастай алғанда, best practice – бұл топтарға сілтеме жасау policy-і. Егер бізде бір пайдаланушы болса да, сол пайдаланушы үшін топ құруға, осы топқа қосылуға, содан кейін біз жасаған барлық policy-ді пайдаланушыға емес, біз жасаған топтарға байланыстыруға кеңес береміз.

Келесі соңғы ұйым – IAM role. Оның идеясы мынада, біз бұлтта IT-инфрақұрылымын құрып жатырмыз деп айттық, ол әртүрлі компоненттерден тұрады, әр компонент белгілі бір сервис және оның ресурсы болып табылады. Олар белгілі бір бизнес тапсырманы орындау үшін бір-бірімен өзара әрекеттеседі. Сонымен, бастапқыда кез-келген сервисте қол жетімділік немесе қандай да бір құқықтар болмайды, ол тек өз сервисі аясында жұмыс істей алады. Мысалы, AWS Lambda, яғни функцияны жасаған кезде, біз сол жерде код жазамыз, ішінде қандай да бір логика болуы мүмкін, бірақ бұл код басқа AWS ресурстарына қол жеткізе алмайды, яғни файлды сол жерден шығару үшін белгілі бір Amazon S3 bucket-іне қол жеткізе алмаймыз. Мүмкін емес. Сондықтан AWS Lambda сервисі AWS Lambda-ға role-ді, одан кейін policy-ді, тиісті bucket-ке қол жеткізуге мүмкіндік беретін role-ге байланыстыру мүмкіндігіне ие. Осыдан кейін, бұл bucket-ке кодтың ішіне кіріп, біз ол жерде access denied, яғни қолжетімділік жоқ деген қателікті көрмейміз.

Role-ді қолдану кезіндегі тағы бір use case – бізде бірнеше AWS аккаунттары болған кезде және біз барлық пайдаланушыларды бір аккаунтда құрғанымызды елестетіп көрейік, бірақ біздің инфрақұрылымымыз біріншісінде де, екінші AWS аккаунтында да жұмыс істейді. Біз екінші AWS аккаунтында пайдаланушыларды құрмай, бірінші AWS аккаунтындағы пайдаланушыларға осы ресурстарға қол жеткіздіре алатын мүмкіндік беруіміз керек. Бұл келесідей жасалады: екінші AWS аккаунтында тиісті role жасалады, trust policy жазылады, яғни осы role-ді пайдалана алатын AWS аккаунттары мен пайдаланушылары тіркеледі. Осылайша, біз бірінші аккаунттағы тиісті пайдаланушыларға немесе топтарға assume мүмкіндігін береміз, яғни басқа аккаунттағы role-ді пайдалану, екі тараптан кіруге рұқсат беру мүмкіндігі. Бұл жағдайда пайдаланушы үшін, ол қосылатын аккаунттың, ол қолданатын role-дің атын біле отырып, ол өз role-ін өзгертеді және қайта қосылады. Осылайшы, ол бір AWS аккаунтынан басқа AWS аккаунтына ауысады немесе көшеді делік. Ол бұл role-дің екінші AWS аккаунтында бар барлық рұқсаттарға ие болады. Осы role-дің бір бөлігі ретінде ол өзінің екінші AWS аккаунтында жұмыс істей алады.

Енді пайдаланушының AWS аккаунтына қалай қосыла алатыны туралы сөйлесейік. Екі нұсқа бар. Біріншісі – AWS CLI немесе AWS SDK қолданған кездегі бағдарламалық жасақтама. Бұл жағдайда ол өзінің access key ID не пайдаланушыны құру кезінде пайда болатын secret access key қолдануы керек. Бұған байланысты бізде жеке Демо болады, және біз осы дәрісте айтылатын барлық тармақтарды Демода қарастырамыз.

Екінші нұсқа – пайдаланушы AWS Management Console-ге қосылған кезде. Бұл жағдайда ол осы аккаунттың 12 таңбалы account ID немесе егер ол орнатылған болса alias білуі керек. Ол сондай-ақ өзінің логинін білуі керек, яғни username және осы пайдаланушының құпиясөзін.

Үшінші нұсқа – егер MFA қосылған не қажет болған жағдайда сәтті қосылу үшін virtual MFA құрылғысында орнатылған қосымша арқылы жасалған кодты енгізуі керек.

Енді авторизация туралы сөйлесейік. Аутентификация – бұл пайдаланушы бұлтқа қосылғанда, пайдаланушы ол өзі екенін айтып жүйеге кіру мүмкіндігі. Авторизация туралы айтатын болсақ, бұл жерде мәселе біз іс-әрекеттерін анықтап берген пайдаланушылар жайлы болмақ. Бастапқыда тек пайдаланушы құрылған кезде, оның әзірге еш жерге қолжетімділігі болмайды, яғни implicit deny деген термин бар, бұл барлық ресурстарға жасырын тыйым салу, егер ол нақты берілмесе, әдетте ол әдепкі қалпы бойынша қосыла алады және кіруді қамтамасыз ету үшін біз осы пайдаланушыға немесе топқа қай жерде, қандай шарттарда, қандай нақты операцияларға кіру мүмкіндігі бар екенін көрсететін AWS policy-дің қандай да бір түрін қосамыз. Осыдан кейін, principle of least privilege атты ұғым бар екенін атап өткен жөн. Бұл тек қажетті қолжетімділікті қамтамасыз ету үшін бар күшімізді салуымыз керек дегенді білдіреді.

Мысалы, егер пайдаланушыға Amazon S3 bucket-іне оқу режиміне кіру керек болса және өз жұмысын орындау үшін файлдарды жүктей алса, оларға толық қолжетімділік берудің қажеті жоқ, яғни оған жаңа bucket-тер жасауға, басқа файлдарға және bucket-терге қол жеткізуге мүмкіндік берудің қажеті жоқ, тек өзі жұмыс істеп отырған режимнің мүмкіндіктері жеткілікті. Сондай-ақ, бір bucket ішінде егер оның міндеттері талап етілмесе, оған жаңа файлдарды жоюға немесе жүктеуге рұқсат берудің қажеті жоқ. Сізге тек қажетті қолжетімділікті беру принципін ұстану керек.

Айта кету керек, IAM сервисі жаһандық болып табылады. Осы сервисті қосып, ашқан кезде, сіз оның жоғарғы оң жақта қай аймаққа тиесілі екенін көре алмайсыз, бірақ сіз global жазуын көресіз. Бұл – құрылған пайдаланушылар барлық аймақтарда автоматты түрде қолжетімді деген сөз. Егер сізге белгілі бір аймақтарға кіруді шектеу қажет болса, сіз осы пайдаланушыға немесе топқа сілтеме жасайтын IAM policy-де жасай аласыз.

Енді IAM policy-інің не екенін және олардың қандай түрлері болуы мүмкін екенін қарастырайық. IAM policy identity-based policy және resource-based policy болып бөлінеді. Identity-based policy – бұл policy белгілі бір ұйымға байланады, яғни identity, ал біздің жағдайда ол role, пайдаланушы немесе топ болуы мүмкін. Resource-based policy жайлы айтатын болсақ, policy-ді тек оған қатысты белгілі бір сервистің ресурсымен байланыстыруға болады және ол қандай ұйымдарға қол жеткізе алатындығын немесе оны осы ресурспен нақты не істейтінін сипаттайды.

Мысал ретінде Amazon S3 bucket бола алады. Сіз оған resource-based policy-ді байланыстыра аласыз, яғни Administrators тобындағы пайдаланушылар осы bucket-тің белгілерін өзгерту мүмкіндігіне ие, ал Simple Users тобындағы пайдаланушылар осы bucket ішіндегі файлдарды жүктей алады, бірақ олар бұл файлдарды жоя немесе өзгерте алмайды дегенді білдіреді.

Іdentity-based policy туралы айтатын болсақ, оның үш түрі бар. Біріншісі – біз тағайындайтын custom policy. Ол өзімен-өзі жүретіндіктен, сіз бұл policy-ді role-ге, пайдаланушыға немесе топқа байланыстырасыз. Екіншісі – managed policy, бұл оны Amazon өзі басқарады, жаңартады және қолдайды дегенді білдіреді. Әр сервисте әртүрлі деңгейдегі бірнеше managed policy болуы мүмкін. Мысалы, біз Amazon S3 деп айтамыз, және AmazonS3 full access policy деген бар, яғни бұл policy-і бар кез-келген identity Amazon S3 сервисіне толық бақылау жасай алады.

Егер біз қарапайым policy туралы айтатын болсақ, яғни power user policy-і әкімшілік құқықтары жоқ жетілдірілген пайдаланушы, ол bucket-терді жасай алмайды немесе жоя алмайды, бірақ ол bucket-тер ішінде жұмыс істеп, файлдарды жоя алады не құра алады.

Және соңғысы – readonly policy-і, ол тек кейбір файлдарды оқуға мүмкіндік береді, бірақ құруға, жоюға және одан да көп жаңа bucket-терді жасауға немесе осы bucket-терді жоюға мүмкіндігі болмайды.

Үшінші нұсқа – inline policies. Іnline policy белгілі бір топтарда немесе белгілі бір role-дерде жасалады, бұнда біз жеке ID-і бар, жеке ARN-мен оқшаулы policy жасамаймыз. Бұл policy топқа немесе role-ге байланысты болғандықтан жеке-дара бола алмайды. Егер сіз бірегей policy жасасаңыз, оны бөлек жасаудың қажеті жоқ, сіз оны белгілі бір role немесе топ үшін арнайы жасай аласыз және ол сол жерде байланыстырылады да, сонымен қатар жұмыс істейді. Егер сізде бірнеше түрлі role-дерге немесе бірнеше түрлі топтарға сілтеме жасайтын policy болса, онда сіз әр түрлі субъектілерге байлана алатын оқшау policy жасауды қарастыруыңызға болады.

Тағы бір айта кететін маңызды мәселе – біздің policy-іміздің қалай жазылатындығы. Бұл белгілі бір құрылымы бар JSON документі, оның белгілі бір кілттері, тиісті мәндері болады, оларды келесі слайдтарда талқылаймыз. Policy туралы айтқан кезде, оның қандай ресурсқа немесе қандай ұйымға байланысты екеніне қарамастан, белгілі бір ұйымға немесе ресурсқа арналған барлық қолжетімді policy қарастырылады. Қолжетімділік болған кезде рұқсат беріледі, ал қолжетімділік болмаған кезде, implicit deny деген хабарлама жазылады, яғни жасырын тыйым салынды дегенді білдіреді. Сонымен қатар, біз policy-де анық explicit deny деп көрсетсек, яғни рұқсат етілмейді деген болсақ, содан кейін кез-келген басқа жерде рұқсат етілген деп көрсетіп, бірақ кем дегенде басқа бір жерде тыйым салынған болса, ол кез-келген рұқсаттан басым болады да, қолжетімділіктің күші жойылады.

IAM policy мысалын қарастырайық. Сіз мұнда IAM policy-інің мысалын көресіз, бұл JSON документ, оның белгілі бір нақты құрылымы бар және енді онда белгілі бір кілттер мен мәндер күтіледі. Нақтырақ қарастырайық. Біз version және statement бар екенін көріп отырмыз. Version – бұл стандартты мән, мысалға 2012-10-17, сіз оны өзгертпейсіз, ол қала береді, ал егер бірдеңе өзгерген болса, бұл ақпаратты AWS құжаттамасынан таба аласыз.

Әрі қарай жүрейік. Statement, яғни бұл массивте өтетін біздің policy. Қазіргі жағдайда бізде екі policy бар екенін көреміз, біріншісі – рұқсат беру, яғни effect тармағында allow деп тұр, ал екіншісі – deny. Екі ықтимал нұсқа allow немесе deny болып табылады. Егер біз action туралы айтатын болсақ, мұнда біз қолжетімділікті беретін немесе одан бас тартатын операциялардың тізімін көре аламыз.

Операция дегеніміз не? Бұл сервистің атауы, қос нүкте және операцияның атауы. Мысалы, S3 : get object. Бұл біз Amazon S3 сервисіне объектіні алу операциясына қолжетімділікті береміз немесе бермейміз, біз осы рұқсатқа ие болғаннан кейін файлды жүктей аламыз. Егер біз операция орнында жұлдызшаны көретін болсақ, бұл осы сервис бойынша барлық операциялар қолжетімді екенін білдіреді.

Келесі қарастыратын мәселе – resource, мұнда біз policy жасағымыз келетін ресурстардың тізімін көрсетеміз. Мұнда айта кету керек маңызды мәселе, сіз қанша allow policy-ін жасағаныңызға қарамастан, егер сізде осы ресурс немесе осы ұйым үшін, яғни identity үшін deny policy болса, онда ол бәрінен бұрын басымдыққа ие болады. Белгілі бір ресурсқа, белгілі бір сервистің белгілі бір операциясына allow де, deny policy да жоқ деп айтатын болсақ, онда бұл жағдайда қолжетімділікке нақты allow де жоқ, бұл жағдайда біз ештеңеге рұқсат бермейміз, әдепкі бойынша бізде implicit deny, яғни жасырын тыйым салу болады.

Resource-based policy қатысты бірнеше қосымша жайттар. Біз бұл белгілі бір ресурс үшін жасалған әрі сол ресурстың құжатында айтылған policy екенін талқыладық және policy құжатында кім, қандай операция ала алатынын немесе керісінше кіруге тыйым салатынын көрсетеміз.

Алдында айтқанымыздың бәрін блок-схема ретінде қарастырайық. Бізде белгілі бір policy бар делік, бұл resource-based policy ме немесе identity-based policy ма маңызды емес, біз осы пайдаланушы үшін нақты операцияның бар-жоғын тексереміз, белгілі бір ресурс үшін explicit deny бар болса, біз кіруге рұқсат бермейміз деп көрсетеміз. Егер explicit deny, яғни нақты тыйым жоқ болса, енді біз explicit allow бар ма екен іздейміз, яғни белгілі бір операцияға нақты рұқсат бар ма, жоқ па білеміз де, егер бар болса, қолжетімділік беріледі. Егер explicit deny да, не explicit allow да болмаса, онда қауіпсіздік мақсатында біз бұл әрекетке implicit deny, яғни тыйым саламыз. Бұл маңызды мәселе, сондықтан мен оны бірнеше жолмен түсіндіруге тырыстым.

Келесі негізгі ұғымға IAM groups-қа көшейік. Жалпы, біз бұл туралы айтып өткен едік, ал енді егжей-тегжейлі мәліметтерді талқылайық. Біріншіден – топта бірнеше пайдаланушы болуы мүмкін және сәйкесінше әр пайдаланушы бірнеше топта болуы мүмкін. Екінші мәселе – топ кірістірілген бола алмайды, сондықтан топты басқа топқа қосу мүмкін емес, топта тек пайдаланушылар бола алады. Үшіншіден, сіздің барлық пайдаланушыларыңыз бірден отыра алатын әдепкі топ болмайды. Егер сіз барлық пайдаланушыларды топқа қосуыңыз керек болса, оны қолмен немесе қарапайым скрипт жазуыңыз керек, бірақ мұның бәрі сіздің жағыңызда жасалады, мысалға, сіз арнайы топ құру үшін оның атауын жазасыз және барлық пайдаланушыларыңызды қосасыз

IAM-ның келесі маңызды компоненті – IAM role-дері. Көп жағдайда IAM role-дері екі жолмен қолданылады. Бірінші жағдай – бір сервистерге басқа сервистерге қол жеткізуді ұсыну. Біз алдында келтірілген бір мысалды еске түсірейік. Бізде лямбда-функциясы бар екенін елестетіп көрейік және ол Amazon S3 серверіне қосылып, файлды белгілі бір жол бойымен жүктеп, оны өзгертіп, қайта жүктеуі керек. Бұл жағдайда, lambda мұны істей алу үшін сіз осы функцияға байланысқан role-ге тиісті құқықтарды тағайындауыңыз керек. Сіз policy жазасыз, оны role-ге байланыстырасыз, бірақ біз тек осы role-де болатын inline policy-ді жасай алатынымыз есімізде, сонымен қатар Amazon өзі басқаратын, қолдайтын managed policy-ді қолдана аламыз. Role-ге арналған екінші пайдалану жағдайы – бір AWS аккаунтынан басқа AWS аккаунтының ресурстарын пайдаланушылар үшін жасалатын кросс-аккаунт. Идеясы мынада: екінші аккаунтта role жасалып, тіркеледі, ол жерде негізгі account ID-дің account ID-і көрсетіледі, ал мұнда сіздің пайдаланушылар отырған негізгі account ID assume role операцияларына рұқсат беріледі, екінші AWS аккаунтында осы ресурстың ARN-і көрсетіледі және содан кейін ғана екі жақтан рұқсат болған жағдайда ғана бұл пайдаланушының сол role-ге ауысу мүмкіндігі болады және осы role-дегі барлық рұқсатпен басқа AWS аккаунтында жұмыс істейді.

Біз бүгінгі дәрістің екінші бөлімін аяқтап, IAM сервисімен таныстық. Бұл бұлттағы барлық жобаларда, қашықтан қосылуға болатын IT-инфраструктураларда қолданылатын өте маңызды сервис, және мұның бәрін істеу үшін бізге белгілі бір құқықтар беру керек. Біз IT-инфраструктура жайлы айтсақ, бұл біздің сервистеріміз бір-бірімен әрекеттесіп жұмыс істейтін жүйе. Және бұл сервистер бір-бірімен жұмыс істеуі үшін біз тиісті құқықтар беруіміз керек.

Құқықтарды берудегі басты ереже – біз least privilege принципі бойынша беретінімізді есте сақтау керек. Біз тек осы identity немесе осы ресурс үшін дәл осы уақытта қажет құқықтарды береміз. Егер біз негізгі ұғымдарға назар аударсақ, бұл IAM policy, ол құқық береді. Және бізде үш ұйым бар: IAM user, IAM group және IAM role.

Біз үшінші бөлімге келіп жеттік, мұнда сіз жаңадан құрылған AWS аккаунтыңызды мүмкіндігінше қорғау үшін қандай қадамдар жасау керектігі туралы сөйлесеміз. Жаңа AWS аккаунтын құрған кезде, бұл аккаунтта ештеңе болмайды. Бұлтқа қосылудың жалғыз нұсқасы – root user ретінде, бәріне толық қол жеткізе алатын супер пайдаланушы болу. Best practices күнделікті тапсырмалар үшін root user пайдалануды, арнайы пароль жасауды, оған MFA құруды және оны жасыруды ұсынбайды, оны қажеттілік болған кезде ғана қолданады. AWS бұлтында root пайдаланушысын қолданатын белгілі бір әрекеттер бар, сіз бұл әрекеттерді сирек жасайсыз, өйткені бұл әдетте қайталанатын әрекеттер емес, бір реттік операциялар.

Енді егер біз best practices туралы айтатын болсақ, AWS сізге осы AWS аккаунтының иесі ретінде арнайы admin пайдаланушысын құруға және admin ретінде кіріп, күнделікті операциялардың бәрін жасауға кеңес береді. Сіздің қызметкерлеріңіз туралы айтсақ, сіздің қызметкерлеріңіздің міндеттеріне қарай олар үшін бөлек пайдаланушылар жасалып, соған қарай арнайы топ құрған жөн, содан кейін барлық role-дер, барлық policy-ді топқа байланыстырасыз.

Root аккаунтыңызда жасау керек басқа параметрлердің бірі – root аккаунтында access кілттері бар болса, оларды жою. Есімізде болса, олар CLI немесе SDK арқылы бұлтқа бағдарламалық қол жеткізу үшін қолданылады. Root пайдаланушы арқылы ештеңе болмайтындықтан, оны әдетте жеке кірген кезде ғана қолданады, ал барлық басқа жағдайларда, сіз арнайы жасалған пайдаланушыларды немесе егер ол сервис болса, role-ді пайдалануыңыз керек. Сондықтан осы access кілттерін жоясыз. Тағы бір мәселе, сіз password policy жасауыңыз керек және оны мүмкіндігінше күрделі етуіңіз міндетті, яғни бұл IAM пайдаланушылары үшін құпиясөздің қаншалықты күрделі немесе қандай таңбаларды пайдалану керектігін сипаттайтын құжат.

Бұлтты одан әрі қорғауға көмектесетін тағы бір функционал – MFA. MFA қосымша фунционалдылық, сондықтан оны арнайы іске қосып, белсендіру қажет. MFA нені білдіреді? MFA – Multi-Factor Authentication. Мұндағы идея, пайдаланушылар AWS Management Account кірген кезде бірнеше факторларды қамтамасыз етеді. Фактор дегеніміз не? Фактор, мысалы, пайдаланушы білетін ақпарат. Пайдаланушы логин мен құпиясөзді біледі. Тағы бір фактор – пайдаланушыда бар зат. Бұл зиянкелтірушіде жоқ физикалық нәрсе. Мысалы, бұл телефон, ол виртуалды MFA арқылы жүзеге асырылады. Виртуалды MFA қосымшасы смартфонға орнатылады және осы қосымшаның ішінде AWS Management Account пайдаланушысы мен сіздің аккаунтыңыз бір-бірімен байланыстырылады. Қосымшада байланыстыру орнатылғаннан кейін, сіз әр 30 секунд сайын алты таңбалы сан аласыз. Осылайша, сіз аутентификацияны өткен кезде логин мен құпиясөзді енгізесіз. Осыдан кейін сіз өзіңіздің MFA кілтіңізді енгізесіз және AWS Management Account осы алты таңбалы нөмірдің сол кезде дәл осы пайдаланушыға көрсетілгенін тексереді. Егер бәрі дұрыс болып, сандар сәйкес келсе, сіз пайдаланушы ретінде өзіңізді екі фактор бойынша анықтағаныңызды білдіреді. Осылайша бұл сіз емес, қандай да бір зиянкелтіруші екендігін анықтауға көмектесе аласыз.

Сіздің бұлтыңыздың қауіпсіздігін арттыруға көмектесетін келесі қадам – AWS CloudTrail деп аталады. Бұл – ұшақтағы қара жәшікке ұқсас сервис. Ол мүмкіндігінше жақсы қорғалып, бұлт инфраструктасындағы барлық өзгерістер мен барлық қоңырауларды AWS API-ге жазады. Және аккаунтыңыздағы барлық әрекеттеріңізді 90 күн тегін сақталады. Ал егер сізге қосымша операция орнату немесе 90 күн емес, белгілі бір құжат бойынша сақтау керек болса, әрі сіз қандай да бір қаржылық ұйым немесе үкімет болсаңыз және сіз бұл ақпаратты белгілі бір жылдар бойы сақтауыңыз керек жағдайда қосымша мүмкіндік бере алады. Бұл жағдайда сіз өзіңіздің аккаунтыңызда ұзақ уақыт бойы орын алатын барлық әрекеттерді жинайтын AWS CloudTrail-дің Trail ресурсын жасайсыз. Бұл жағдайда ақы алынуы мүмкін. Trail өзінің барлық деректерін Amazon S3 сервисінің ішінде сақтайды және логтар мәтінге негізделген ақпарат болғандықтан, AWS CloudTrail шығындары әдетте өте төмен. Бірақ бұлт ішінде мәселе туындаған кезде, бұл тергеу мақсаттары үшін маңызды ақпарат болғандықтан, оны қосып қою және әрдайым белсенді ұстау ұсынылады.

Біз сіздермен алдыңғы дәрістерде billing сервистері мен бұлттағы шығындармен, яғни Cost-пен таныстық. Best practice секілді, бюджетке ескертулерді орнатуды ұсынады, сонымен қатар барлық шығындарыңызды тез және жылдам көріп, нақты әрекеттерді орындау үшін есептерді орнату ұсынылады.

Сіз мұны AWS Cost Explorer ішінде жасай аласыз немесе сізге егжей-тегжейлі ақпарат қажет болса, AWS Cost and Usage Reports сервисін пайдалана аласыз, ол шығындарыңыз туралы деректер мен метадеректерді Amazon S3-ке жүктейді, және сіз осы деректерді бірегей кастомды есептерді құру үшін пайдалана аласыз.

AWS Cost and Usage Reports көбінесе ірі компаниялар қолданатын өте жетілдірілген нұсқа болып табылады, сондықтан сіздің жағдайыңызда, осы есептерді зерттеп-зерделеудің қажеті жоқ, AWS Cost Explorer-ге сүйенсеңіз жеткілікті, ол қажет нәрсенің бәрін, есептеріңізді де ыңғайлы түрде сақтауды көрсетіп береді.

Сонымен, біз дәрістің үшінші бөлімінің соңына жеттік және біз сіздің бұлт инфаструктасының қауіпсіздігін қамтамасыз ететін AWS бұлтындағы қолжетімді барлық негізгі қадамдар, әрекеттер, сервистер және мүмкіндіктер туралы әңгімелестік.

Ал енді біз дәрістің төртінші бөліміне көшеміз және аккаунттарымызды қорғауға көмектесетін қосымша сервистер жиынтығы туралы сөйлесеміз.

Ең алғашқы сервис – AWS Organizations. AWS Organizations – бұл бірнеше AWS аккаунттарын орталықтан басқаруға мүмкіндік беретін сервис. Ол, сондай-ақ, consolidated billing орнатуға мүмкіндік береді. Бұл жердегі идея, біз AWS аккаунттарының әрқайсысы үшін барлық шығындарды бір жерде жинаймыз және оларды бір негізгі аккаунтта ыңғайлы түрде көрсетеміз.

Қауіпсіздікті қамтамасыз етуде AWS Organizations атқаратын функционалдар бар. Ол Service control policies деп аталады. Бұндағы идея – бұл да JSON құжаты, бұл да policy, бірақ ол AWS аккаунтымен байланысты. Бәріміз білетін OU функционалдығы, яғни AWS Organizations ішіндегі organizational units бар, бұл сіздің аккаунтарыңызды өзара топтастыруға мүмкіндік береді. Осылайша, сіз өзіңіздің аккаунттарыңызды икемді және мүмкіндігінше ыңғайлы түрде топтастыра аласыз, ал Service Control Policies жеке аккаунтқа емес, бүкіл топқа, яғни organizational units-ке байланыстырылуы мүмкін. Қолжетімділікті мүмкіндігінше дұрыс күйге келтірсеңіз, мысалы, сіз әзірлеу болып жатқан аккаунттарда ресурстарға көбірек қолжетімділік пен көбірек бақылау беріңіз де, ал production аккаунттарыңызға мүмкіндігінше аз қолжетімділік беріңіз, дегенмен бәрі дұрыс жұмыс істеуі керек, әрі мүмкін бұзылуларды алдын алып,зиянкелтіруші production ортасына кірсе де көп мүмкіндікке ие бола алмайтындай, сіздің ІТ-инфраструктараларыңызға аз зиян келтіретіндей қолжетімділік болуы керек.

Келесі қызмет – AWS KMS, яғни Key Management Service. Бұл сервис бұлттағы шифрлау кілттерін басқаруға көмектеседі. Қазіргі уақытта сізге тек анықтамасын білу жеткілікті, біз бұл сервис туралы келесі сабақтарда толығырақ сөйлесеміз.

Келесі қызмет – Amazon Cognito. Біз бұл сервисті егжей-тегжейлі қарастырмаймыз, өйткені нақты емтихан мақсатында анықтамасын білу жеткілікті. Ал анықтамасы мынадай: бұл сіздің қосымшаларыңыздың пайдаланушыларын басқаруға мүмкіндік беретін сервис, яғни ол сізге кіруге, тіркеуге және басқаруға және барлық пайдаланушыларыңыз туралы ақпаратты сақтауға мүмкіндік береді.

Қауіпсіздікке байланысты келесі managed сервис – AWS Shield. Сіз тек анықтаманы білсеңіз жеткілікті: бұл сервис DDoS-шабуылдарынан қорғауға мүмкіндік береді.

Біз дәрістің бесінші бөліміне көшеміз және бұлттағы деректерімізді қалай қорғауға болатындығы туралы сөйлесеміз. Деректер сақтала алатын бірінші күй – at rest деп аталады, яғни бұл деректер қатты дискілерде сақталған күйі. Бұл жағдайда біз AES-256 шифрлауды қолдана аламыз немесе деректерді сақтау жағдайында шифрлау үшін бұрын айтылып кеткен AWS KMS қолдана аламыз.

Қорғалуы қажет деректердің басқа күйі – тасымалдау кезінде, яғни біз өз деректерімізді желі арқылы жіберген кездегі күй. Бұл жағдайда деректер ағынын қорғау үшін SSL кілттерін немесе TLS сертификаттарын жасауға мүмкіндік беретін AWS Certificate Manager сервисі бар. Бұл, сондай-ақ, веб-трафикке де қатысты, сондықтан осы AWS Certificate Manager сервисін пайдаланып, HTTPS қосылымы болып табылатын Secure HTTP орната аламыз. Осы тізімді көргеннен кейін, сіз бұл bucket-терге интернетпен кіру қажеттілігін анықтай аласыз, егер қажет болмаса, сіз оларды тізімдеп өтіп, интернеттен ортақ қол жетімділікті блокқа коя аласыз.

Сіздің компанияңыздың қандай салада жұмыс істейтініне,қандай елде екеніңізге немесе әлемнің қандай аймағында орналасқанына қарамастан сіз белгілі бір сапа немесе нормативтік стандарттар талаптарына сай болуыңыз керек. AWS өз тарапынан мерзімді негізде әртүрлі тексерулерден өтеді, белгілі бір нормативтік талаптарға сәйкес келетін сапа сертификаттары мен қорытынды құжаттарды алады.

AWS емтиханында кездесуі мүмкін, compliance бағдарламаларының бірі – AWS ISO/IEC 27001:2013 сапа сертификатын алды. Сондай-ақ, оның HIPAA заңының талаптарына сәйкес келетіні туралы растау бар. Бұл медицина саласында жұмыс істейтін компаниялар үшін қажет. Үшіншісі – GDPR, ол көбінесе Еуропада орналасқан компанияларға арналған және бұл құжатта жеке деректерді сақтау және олармен жұмыс істеу талаптары сипатталған.

Сіз осы барлық құжаттарды, сапа сертификаттарын және соңғы құжаттарды AWS Artifact сервисінен жүктей аласыз. Бірақ бұл шын мәнінде сервис емес, осы құжаттар сіздің компанияңыз үшін қажет болған жағдайда жүктей алатын беттер жиынтығы болып табылады.

Егер біз өзіміздің іс-әрекетіміз, қандай ресурстар бар екенін және осы ресурстарда қандай өзгерістер болғанын түсіну үшін AWS аккаунтының бөлігі ретінде compliance-ті айтатын болсақ, онда біз AWS Config-ті қолдана аламыз, ол барлық өзгерістерді жазады және белгілі бір жағдайларда қосымша әрекеттерді орындай алады. Бұл анықтама емтихан мақсаттары үшін жеткілікті болғандықтан, біз әрі қарай өтейік.

Бізде дәрістің соңғы бонустық бөлімі бар, және біз оны мүмкіндігінше тез өтеміз. Бұл AWS Service Catalog сервисі. Бұл сервистің идеясы – сіздің компанияңыз мақұлдаған сервистерді таңдау және сіздің қызметкерлеріңізге AWS Service Catalog арқылы осы сервистерге қол жетімділікті қамтамасыз ету.

Қалған үш қызмет – Amazon Macie, бұл жеке деректерді анықтау үшін инфраструктарыңыздағы барлық деректерді сканерлеу үшін машиналық оқытуды қолданатын сервис. Содан кейін, анықталған ақпаратпен сіз сәйкесінше әрекет ете аласыз, немесе бұл деректерді арнайы сақтау орнында сақтай аласыз немесе ол кездейсоқ мән болса, оны жойсаңыз болады.

Қалған екі сервис – Amazon Inspector мен Amazon GuardDuty бір-біріне ұқсас. Бұл сервистердің идеясы – Amazon-ның managed-сервистері болып табылады және сіз оны іске қосқаннан кейін сіздің бұлтыңыз бен ІТ-инфраструктураңыз кейбір мәселелерді анықтау үшін автоматты түрде сканерленіп, содан кейін сіздің ІТ-инфраструктураңыз қауіпсіздігін жақсарту үшін ұсыныстар тізімі жасалады.

Міне, біз дәрістің соңғы слайдтарына келдік. Дәрісті аяқтамас бұрын сізге қысқаша түйіндеме бергім келеді.

Біріншіден, біз shared responsibility model дегеніміз не екенін талқыладық.

Әрі қарай, біз AWS IAM-ді жақынырақ қарастырдық.

Содан кейін біз жаңа AWS аккаунтын құруға жасалатын және жасау үшін ұсынылатын қадамдарды қарастырдық. Содан кейін біз бұлттың қауіпсіздігімен байланысты бірқатар AWS сервистерін талдадық.

Мұнда сіз керемет жұмыс жасағаныңызды атап өткім келеді. Мен ақпараттың ауқымы үлкен, көптеген жаңа терминдер және көптеген жаңа серсис атаулары бар екенін түсініп отырмын. Ең бастысы, алаңдамаңыз. Менің ұсынысым – кейбір жерді оқып алып конспект жазыңыз, кем дегенде, сервистердің атауларын жазып алыңыз. Сіз мұны жазған кезде немесе дәрістерді қайта көргенде, сервистердің атаулары есте қалады және таныс болады.

Біз AWS нақты емтиханда жиі кездесетін кейбір сервистер туралы әлі де толығырақ сөйлесеміз. Бізде белсенділіктер, Демо болады. Мен сізге AWS Management Console әртүрлі серсистерді мысал ретінде, көзбен есте қаларлық етіп қалай көрінетінін көрсетемін. Сондай-ақ, бізде бірнеше зертханалық белсенділіктер болады, онда сіз бұлтты көре аласыз. Сіздердің кейбіреулеріңіз үшін бұл белсенділіктер бұлттың қалай көрінетінін, онымен қалай жұмыс істеу керектігін, қандай артықшылықтар барын және т.б. әрекеттері жақсырақ есте сақтауға көмектеседі деп білеміз.

Бұл слайдта осы тақырыптарға байланысты пайдалы болуы мүмкін сілтемелерді ұсынамыз, тереңірек білгім келеді десеңіз сілтеме бойынша өтсеңіз болады.

Осымен біздің дәрісіміз аяқталды. Назарларыңызға рахмет. Сәттілік! Келесі дәрісте күтемін.