Cybersecurity Fundamentals — Bazat e sigurisë kibernetike

Kurs fillestar në shqip për studentë dhe profesionistë që hyjnë në IT. Mësoni të vlerësoni rreziqet, të mbroni llogaritë, pajisjet, rrjetet, aplikacionet dhe të dhënat, të analizoni regjistrat dhe të koordinoni reagimin ndaj incidenteve. Parakushtet janë përdorimi bazë i kompjuterit dhe i shfletuesit. Ushtrimet përdorin të dhëna fiktive dhe kryhen me një dokument ose tabelë llogaritëse. Koha orientuese është 18–22 orë me ushtrime, vlerësime dhe projekt.

Përmbajtja

1. Bazat dhe menaxhimi i rrezikut
2. Kërcënimet dhe mashtrimet
3. Identiteti dhe qasja
4. Mbrojtja e rrjetit
5. Siguria e aplikacioneve web
6. Mbrojtja e pajisjeve dhe të dhënave
7. Siguria në cloud
8. Zbulimi dhe përgjigjja ndaj incidenteve
9. Puna profesionale dhe projekti

1. Bazat dhe menaxhimi i rrezikut

1. Konfidencialiteti, integriteti dhe disponueshmëria

Konfidencialiteti, integriteti dhe disponueshmëria

Konfidencialiteti kufizon leximin, integriteti mbron saktësinë dhe disponueshmëria siguron qasjen kur duhet. Një kopje rezervë e palexueshme nuk e mbron disponueshmërinë vetëm pse ekziston. Për të dhëna kritike zakonisht duhen kontrolle për të tria.

Shembull i arsyetuar

Konfidencialitet: role leximi. Integritet: histori ndryshimesh dhe miratim. Disponueshmëri: objektiv rikthimi dhe kopje e provuar.

Burimi i mësimit

Detyra

Në klinikën fiktive, një listë takimesh lexohet nga persona të paautorizuar, një orar ndryshohet pa miratim dhe portali bie për 45 minuta. Klasifikoji sipas ndikimit kryesor dhe propozo nga një kontroll.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Konfidencialitet: role leximi. Integritet: histori ndryshimesh dhe miratim. Disponueshmëri: objektiv rikthimi dhe kopje e provuar.

2. Aseti, kërcënimi, dobësia dhe rreziku

Aseti, kërcënimi, dobësia dhe rreziku

Aseti ka vlerë për organizatën. Kërcënimi mund të shkaktojë dëm, ndërsa dobësia krijon një mundësi që dëmi të ndodhë. Vlerëso gjasën dhe ndikimin, cakto pronarin e rrezikut dhe dokumento rrezikun që mbetet pas kontrollit.

Shembull i arsyetuar

Për laptopin, vjedhja është kërcënimi, mungesa e enkriptimit është dobësia dhe ekspozimi i të dhënave është pasoja. Dokumento supozimet pas secilës pikë.

Detyra

Krahaso një laptop me të dhëna klientësh pa enkriptim, një printer zyre jashtë shërbimit dhe një portal me kopje rezervë të paprovuar. Shëno gjasën dhe ndikimin në shkallë 1–3 dhe shpjego renditjen.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Për laptopin, vjedhja është kërcënimi, mungesa e enkriptimit është dobësia dhe ekspozimi i të dhënave është pasoja. Dokumento supozimet pas secilës pikë.

3. Mbrojtja me disa shtresa

Mbrojtja me disa shtresa

Kontrollet parandaluese ulin gjasën e incidentit, kontrollet zbuluese nxjerrin në pah devijimin dhe kontrollet korrigjuese ndihmojnë rikthimin. Shtresat kanë vlerë kur mbulojnë mënyra të ndryshme dështimi dhe kur funksionimi i tyre mund të provohet.

Shembull i arsyetuar

MFA për hyrjen, alarm për hyrje të pazakonta dhe rikthim i provuar nga kopjet rezervë janë tri shtresa me qëllime të ndryshme.

Detyra

Vizato tre shtresa për një portal faturash. Për secilën shkruaj veprimin, pronarin dhe provën që kontrolli funksionon.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

MFA për hyrjen, alarm për hyrje të pazakonta dhe rikthim i provuar nga kopjet rezervë janë tri shtresa me qëllime të ndryshme.

Gjashtë funksionet e NIST CSF 2.0

Qeveris (Govern) cakton përgjegjësitë dhe pritshmëritë. Identifiko (Identify) njeh asetet dhe rreziqet. Mbro (Protect) vendos masa si MFA dhe kopjet rezervë. Zbulo (Detect) kërkon ndryshime dhe sinjale. Përgjigju (Respond) koordinon analizën, kufizimin dhe komunikimin. Rikupero (Recover) rikthen shërbimin dhe verifikon rezultatet. Funksionet punojnë njëkohësisht.

Ushtrim: Për portalin e klinikës cakto nga një rezultat të matshëm për secilin funksion. Shembull: “Për 100% të roleve të privilegjuara kemi një pronar të dokumentuar.” Shëno burimin e provës dhe

sa shpesh kontrollohet.

2. Kërcënimet dhe mashtrimet

4. Phishing dhe verifikimi i kërkesave

Phishing dhe verifikimi i kërkesave

Një mesazh i dyshimtë mund të përdorë urgjencë, emra të njohur ose një kanal të pazakontë. Verifiko kërkesat financiare ose të qasjes përmes një kontakti të besuar që e ke tashmë. Raporto mesazhin përmes kanalit të organizatës.

Shembull i arsyetuar

Ndalo pagesën, verifiko te numri i njohur i furnitorit dhe raporto mesazhin. Ruaj vetëm provën e nevojshme.

Detyra

Një mesazh nga një adresë e panjohur kërkon kalim pagese në një llogari të re para orës 14:00. Rendit tri shenja dhe shkruaj përgjigjen e brendshme për financën.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Ndalo pagesën, verifiko te numri i njohur i furnitorit dhe raporto mesazhin. Ruaj vetëm provën e nevojshme.

5. Llojet e programeve keqdashëse

Llojet e programeve keqdashëse

Ransomware mund të bllokojë qasjen ose të shoqërohet me vjedhje të të dhënave. Spyware synon të vëzhgojë aktivitetin. Një trojan paraqitet si program i dobishëm, ndërsa një worm përhapet vetë. Simptoma orienton hetimin, por nuk provon llojin.

Shembull i arsyetuar

Dokumentet sugjerojnë një incident të mundshëm ransomware. Shëno orën, pajisjet dhe alarmet. Eskalo te ekipi përgjegjës.

Detyra

Për tri raporte fiktive, sistemo faktet, hipotezat dhe provat që duhen kërkuar: dokumente të palexueshme, alarm për program të panjohur, aktivitet i pazakontë i ngjashëm në disa pajisje.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Dokumentet sugjerojnë një incident të mundshëm ransomware. Shëno orën, pajisjet dhe alarmet. Eskalo te ekipi përgjegjës.

6. Sinjalet e kompromet imit të llogarisë

Sinjalet e kompromet imit të llogarisë

Një njoftim MFA i pakërkuar, një pajisje e panjohur ose një rregull i ri përcjelljeje mund të kërkojë hetim. Vlerëso sinjalet së bashku me identitetin, orën dhe kontekstin. Regjistro çfarë është

konfirmuar dhe çfarë mbetet supozim.

Shembull i arsyetuar

Pyet përdoruesin për veprimet e veta përmes kanalit të besuar dhe kërko verifikimin e historikut të hyrjeve dhe ndryshimeve.

Detyra

Rendit një sekuencë me njoftim MFA të pakërkuar, hyrje të suksesshme më pas dhe ndryshim të rregullit të postës. Shkruaj dy pyetje verifikuese.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Pyet përdoruesin për veprimet e veta përmes kanalit të besuar dhe kërko verifikimin e historikut të hyrjeve dhe ndryshimeve.

Kartela e raportimit

Mbaj të ndara kohën e vëzhgimit, burimin, përshkrimin, ndikimin e mundshëm dhe veprimin e parë. Një raport i mirë mund të përdoret nga personi i radhës pa pyetur raportuesin për të dhëna që mungojnë.

Ushtrim: Krahaso dy raporte: “Email i keq” dhe “09:10 UTC, kutia e financës, kërkesë e pazakontë për ndryshim të të dhënave bankare, pagesa e pezulluar”. Plotëso raportin e parë me fakte fiktive dhe identifiko çfarë prove mungon.

3. Identiteti dhe qasja

7. Autentikimi, autorizimi dhe MFA

Autentikimi, autorizimi dhe MFA

Autentikimi verifikon identitetin, autorizimi përcakton veprimet që lejohet të kryhen. MFA përdor faktorë të kategorive të ndryshme. FIDO2 ose passkeys rezistente ndaj phishing-ut mund të ulin rrezikun e kopjimit të kredencialeve. Rikuperimi i llogarisë duhet të mbrohet po aq mirë.

Shembull i arsyetuar

Hyrja me metodë të fortë kontrollon identitetin. Roli dhe kufiri i miratimit kontrollojnë autorizimin.

Burimi i mësimit

Detyra

Përcakto si hyn një punonjës i financës dhe cilin hap e kontrollon sistemi kur ai kërkon të miratojë pagesën.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Hyrja me metodë të fortë kontrollon identitetin. Roli dhe kufiri i miratimit kontrollojnë autorizimin.

8. RBAC dhe privilegji minimal

RBAC dhe privilegji minimal

RBAC lidh lejet me rolet e punës. Privilegji minimal kufizon lejen, objektin dhe kohëzgjatjen sipas nevojës. Ndarja e detyrave shmang përqendrimin e krijimit dhe miratimit të një transaksioni te i njëjti person.

Shembull i arsyetuar

Krijuesi regjistron faturën, miratuesi vendos për pagesën, auditori lexon historikun. Përcakto kush autorizon përjashtimet.

Detyra

Ndërto një matricë për krijues faturash, miratues dhe auditor. Përcakto kush krijon, kush miraton dhe kush vetëm lexon.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Krijuesi regjistron faturën, miratuesi vendos për pagesën, auditori lexon historikun. Përcakto kush autorizon përjashtimet.

9. Cikli i llogarisë dhe SSO

Cikli i llogarisë dhe SSO

Procesi hyrje–ndryshim–largim lidh personelin me identitetet dhe qasjet. SSO centralizon hyrjen dhe ul numrin e kredencialeve, por kërkon mbrojtje dhe monitorim të ofruesit të identitetit. Inventarizo

sesionet, tokenët dhe llogaritë lokale.

Shembull i arsyetuar

Pezullo identitetin, revoko seancat sipas procedurës, kontrollo llogaritë lokale dhe transfero pronësinë e dokumenteve.

Detyra

Për një kontraktor që largohet sot, dokumento pronarin, afatin e çaktivizimit, seancat aktive dhe qasjen te skedarët e projektit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Pezullo identitetin, revoko seancat sipas procedurës, kontrollo llogaritë lokale dhe transfero pronësinë e dokumenteve.

Fjalëkalimet dhe rikuperimi

Përdor fjalëkalime unike, një menaxher të miratuar dhe metoda të forta MFA. Ruaj kodet rezervë me qasje të kontrolluar. Regjistro mënyrën e verifikimit të identitetit kur pajisja e autentikimit humbet. Për llogaritë e privilegjuara planifiko një rol urgjence me pronar të qartë, monitorim dhe rishikim periodik.

Ushtrim: Shkruaj një procedurë rikuperimi për një telefon të humbur. Përfshi kush verifikon identitetin, si regjistrohet kërkesa, çfarë revokohet dhe si konfirmohet qasja e re.

4. Mbrojtja e rrjetit

10. Firewall dhe segmentimi

Firewall dhe segmentimi

Firewall-i lejon ose kufizon rrjedhat sipas burimit, destinacionit, shërbimit dhe drejtimit. Segmentimi ul lëvizjen midis pajisjeve. Hartëzo rrjedhat e nevojshme, dokumento përjashtimet dhe verifiko efektin përpara përdorimit.

Shembull i arsyetuar

Tabela duhet të shënojë burimin, destinacionin, shërbimin, veprimin dhe arsyen e biznesit. Zona e vizitorëve nuk ka rrugë për serverët e brendshëm.

Detyra

Vizato zona për vizitorë, staf dhe serverë. Vizitorët kanë nevojë vetëm për internet, ndërsa stafi për portalin e brendshëm.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Tabela duhet të shënojë burimin, destinacionin, shërbimin, veprimin dhe arsyen e biznesit. Zona e vizitorëve nuk ka rrugë për serverët e brendshëm.

11. VPN, TLS dhe kufijtë e besimit

VPN, TLS dhe kufijtë e besimit

VPN siguron tunel midis pikave të përcaktuara, ndërsa TLS mbron komunikimin midis klientit dhe shërbimit. Prania në tunel nuk provon autorizim për çdo aplikacion. Kontrolli i identitetit, gjendjes së pajisjes dhe rolit mbetet i nevojshëm.

Shembull i arsyetuar

Portali publik kërkon HTTPS. Konsola kërkon autorizim të veçantë dhe qasje nga pajisje e miratuar. VPN zgjidhet sipas arkitekturës.

Detyra

Krahaso tre raste: punonjës në udhëtim, klient në portalin publik, administrator që përdor konsolën e brendshme. Shëno çfarë mbrohet në secilën lidhje.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Portali publik kërkon HTTPS. Konsola kërkon autorizim të veçantë dhe qasje nga pajisje e miratuar. VPN zgjidhet sipas arkitekturës.

12. IDS, IPS dhe monitorimi

IDS, IPS dhe monitorimi

IDS jep sinjale për aktivitet të dyshimtë, ndërsa IPS mund të pengojë rrjedha sipas politikës. Alarmi është pikënisje për verifikim. Kriptimi mund të kufizojë dukshmërinë e përmbajtjes, por kohët,

adresat dhe vëllimi mund të mbeten të dobishëm.

Shembull i arsyetuar

Krahaso oraret, punët e planifikuara dhe pronarin e destinacionit. Shpjego pse një ndryshim në vëllim nuk mjafton si provë.

Detyra

Analizo tre regjistra të sajuar: qasje e zakonshme, dyfishim i trafikut gjatë kopjeve rezervë dhe rritje e panjohur jashtë orarit. Shëno çfarë verifikohet fillimisht.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Krahaso oraret, punët e planifikuara dhe pronarin e destinacionit. Shpjego pse një ndryshim në vëllim nuk mjafton si provë.

Verifikimi i rregullave të rrjetit

Matrica e rrjedhave lidhet me përdorimin real të biznesit. Para miratimit, kontrollo rrjedhat e lejuara, komunikimin e ndaluar dhe regjistrat e vendimeve.

Ushtrim: Shto në hartë shërbimin e kopjeve rezervë. Dokumento drejtimin e lidhjes, sistemet e nevojshme dhe pronarin. Përgatit tre raste verifikimi të politikës me rezultate të pritshme, përfshirë një rrjedhë të ndaluar.

5. Siguria e aplikacioneve web

13. Parandalimi i SQL Injection

Parandalimi i SQL Injection

Parametrat e lidhur mbajnë hyrjet e përdoruesit të ndara nga struktura e pyetjes SQL. Përdor parametrizim për vlerat dhe listë të lejuar për zgjedhje strukturore si kolonat e renditjes. Llogaria e bazës merr vetëm privilegjet që i duhen.

Shembull i arsyetuar

Emri kalon si parametër. Opsioni i renditjes përkthehet nga një listë e miratuar. Llogaria e kërkimit ka qasje të kufizuar.

Burimi i mësimit

Detyra

Përshkruaj si një kërkim kursesh pranon një emër dhe një opsion renditjeje. Shkruaj kontrollet që duhet të kërkojë rishikuesi.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Emri kalon si parametër. Opsioni i renditjes përkthehet nga një listë e miratuar. Llogaria e kërkimit ka qasje të kufizuar.

14. Parandalimi i XSS dhe CSRF

Parandalimi i XSS dhe CSRF

Për XSS përdor kodim të daljes sipas kontekstit dhe pastrim të HTML kur formatimi lejohet. Për CSRF mbro veprimet që ndryshojnë gjendjen me token të verifikuar nga serveri dhe politika të përshtatshme të cookies. Kontrolli i qasjes mbetet detyrë e serverit.

Shembull i arsyetuar

Komenti kodohet në dalje. Formulari përdor metodë për ndryshim gjendjeje, token CSRF dhe kontroll të autorizimit në server.

Burimi i mësimit

Detyra

Bëj një rishikim në letër të një komenti publik dhe të një formulari për ndryshim emaili. Për secilin shëno kontrollin dhe vendin ku ekzekutohet.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Komenti kodohet në dalje. Formulari përdor metodë për ndryshim gjendjeje, token CSRF dhe kontroll të autorizimit në server.

15. HTTPS, seancat dhe autorizimi në server

HTTPS, seancat dhe autorizimi në server

HTTPS mbron transportin dhe ndihmon në verifikimin e shërbimit përmes certifikatës. Cookies me Secure, HttpOnly dhe SameSite të përshtatshëm ndihmojnë mbrojtjen e seancave. Çdo kërkesë për një dokument duhet të kontrollojë në server lejen mbi atë dokument.

Shembull i arsyetuar

Kontrolli i serverit kontrollon lejen mbi faturën për çdo kërkesë dhe regjistron ngjarjet përkatëse pa ruajtur përmbajtje të panevojshme.

Detyra

Rishiko një portal fature ku lidhja është HTTPS dhe butoni i shkarkimit fshihet për rolet e tjera. Shëno çfarë duhet provuar përpara publikimit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Kontrolli i serverit kontrollon lejen mbi faturën për çdo kërkesë dhe regjistron ngjarjet përkatëse pa ruajtur përmbajtje të panevojshme.

Paketa e verifikimit për publikim

Rishikuesi kërkon provë për përdorimin e parametrave në kërkimin e kurseve, kodimin e komenteve dhe autorizimin për skedarët e studentëve. Dokumento funksionin, kontrollin, rezultatin e pritshëm dhe pronarin.

Ushtrim: Shkruaj një kriter pranimi për secilin nga këto raste: emër me apostrof shfaqet saktë, komentet shfaqen si tekst dhe studenti A nuk merr faturën e studentit B.

Burimi i mësimit

6. Mbrojtja e pajisjeve dhe të dhënave

16. Përditësimet dhe konfigurimi bazë

Përditësimet dhe konfigurimi bazë

Inventarizo versionin, pronarin dhe ekspozimin. Jep përparësi sipas rëndësisë së shërbimit, përdorimit dhe ndikimit. Përditëso grupin provë, verifiko funksionet, zbato sipas valëve dhe dokumento përjashtimet me afat.

Shembull i arsyetuar

Vendos përparësinë me arsyetim, grupin provë, kriteret e suksesit dhe masë të përkohshme me afat për sistemin e vjetër.

Detyra

Përgatit një plan për laptopët, serverin publik dhe një sistem të vjetër të brendshëm që kërkon miratim të furnitorit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Vendos përparësinë me arsyetim, grupin provë, kriteret e suksesit dhe masë të përkohshme me afat për sistemin e vjetër.

17. Mbrojtja e pajisjes dhe reagimi ndaj alarmit

Mbrojtja e pajisjes dhe reagimi ndaj alarmit

Mbrojtja e pajisjes kombinohet me regjistrim, konfigurim të qëndrueshëm, enkriptim dhe kontroll të privilegjeve. Një alarm nga EDR duhet marrë në kontekst. Veprimet e izolimit duhen koordinuar me pronarin dhe procedurën e incidentit.

Shembull i arsyetuar

Ndaj faktin nga hipoteza. Regjistro se kush lejohet të izolojë pajisjen dhe kur kërkohet eskalim.

Detyra

Plotëso një kartelë për një laptop që shfaq një proces të panjohur, me emrin e pajisjes, orën UTC, burimin dhe ndikimin e mundshëm.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Ndaj faktin nga hipoteza. Regjistro se kush lejohet të izolojë pajisjen dhe kur kërkohet eskalim.

18. Kopjet rezervë, RPO dhe RTO

Kopjet rezervë, RPO dhe RTO

RPO përshkruan humbjen e pranueshme të të dhënave në kohë, ndërsa RTO kohën e synuar të rikthimit. Kopjet e izoluara dhe të mbrojtura ulin rrezikun e humbjes së përbashkët. Prova e rikthimit mat aftësinë reale për t'u kthyer në punë.

Shembull i arsyetuar

RPO nuk arrihet sepse humbja e mundshme është 7 orë. RTO arrihet sepse rikthimi zgjat 5 orë.

Detyra

Portalit i duhen RPO 4 orë dhe RTO 6 orë. Kopja e fundit është 7 orë para incidentit dhe shërbimi rikthehet pas 5 orësh. Vlerëso rezultatet.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

RPO nuk arrihet sepse humbja e mundshme është 7 orë. RTO arrihet sepse rikthimi zgjat 5 orë.

Prova e rikthimit

Zgjidh një dokument fiktiv dhe ruaj një kopje rezervë në një dosje të veçantë. Ndrysho dokumentin e punës dhe rikthe kopjen në një dosje të re. Krahaso përmbajtjen me origjinalin dhe regjistro kohën.

Dorëzim: Shëno versionin e pritshëm, kohën e nisjes dhe të mbarimit, dallimet dhe hapin e ardhshëm. Shpjego si do ta shtrije të njëjtën provë te një shërbim me bazë të dhënash.

7. Siguria në cloud

19. Përgjegjësia e përbashkët

Përgjegjësia e përbashkët

Ndarja e përgjegjësive varet nga shërbimi. Në IaaS klienti zakonisht menaxhon sistemin operativ të instancës. Në SaaS ekipi i klientit ende menaxhon identitetet, ndarjen e të dhënave dhe konfigurimet që ka në dispozicion.

Shembull i arsyetuar

Infrastruktura fizike i takon ofruesit. Klienti mban pronësi mbi rolet dhe politikat e ndarjes. Kontrollo dokumentacionin e shërbimit për kufijtë specifikë.

Detyra

Ndërto një matricë përgjegjësish për postën SaaS dhe një server IaaS, me rreshta për pajisjen fizike, rolet, konfigurimin dhe përditësimet.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Infrastruktura fizike i takon ofruesit. Klienti mban pronësi mbi rolet dhe politikat e ndarjes. Kontrollo dokumentacionin e shërbimit për kufijtë specifikë.

20. Të dhënat, çelësat dhe ndarja

Të dhënat, çelësat dhe ndarja

Klasifikimi i të dhënave udhëzon ndarjen, enkriptimin, afatin e ruajtjes dhe kontrollin e qasjes te çelësat. Enkriptimi nuk korrigjon lejet publike që shërbimi vetë i respekton. Ndarja duhet të jetë e qëllimshme dhe e kontrollueshme.

Shembull i arsyetuar

Kufizo ndarjen te grupet përkatëse dhe verifiko konfigurimin, regjistrat dhe rastet që kërkojnë eskalim.

Detyra

Një dosje fiktive me kontrata është vendosur me qasje publike ndërsa ruajtja është e enkriptuar. Shkruaj gjetjen, kontrollin dhe provën pas korrigjimit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Kufizo ndarjen te grupet përkatëse dhe verifiko konfigurimin, regjistrat dhe rastet që kërkojnë eskalim.

21. Regjistrimi dhe identitetet e shërbimit

Regjistrimi dhe identitetet e shërbimit

Regjistrat e cloud dokumentojnë ndryshime të roleve, politikave dhe resurseve. Identitetet e shërbimit duhen ndarë nga llogaritë njerëzore dhe kufizuar në funksionin përkatës. Kredencialet

afatshkurtra ulin kohën e ekspozimit.

Shembull i arsyetuar

Cakto lexim vetëm për resurset e nevojshme. Alarmo ndryshimet që shtojnë privilegje dhe cakto pronarin e shqyrtimit.

Detyra

Për një aplikacion që vetëm lexon raporte, përshkruaj rolin, sinjalet për ndryshim të lejeve dhe kujt i dërgohen alarmet.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Cakto lexim vetëm për resurset e nevojshme. Alarmo ndryshimet që shtojnë privilegje dhe cakto pronarin e shqyrtimit.

Inventari cloud

Krijo katër rreshta për identitetin qendror, ruajtjen e dokumenteve, monitorimin dhe kopjet. Për secilin shëno llojin e shërbimit, pronarin, qasjet, klasifikimin dhe një provë kontrolli.

Rast: Një ekip i brendshëm kërkon qasje leximi në një dosje për shtatë ditë. Përshkruaj miratimin, mënyrën e dhënies së qasjes, skadimin dhe verifikimin.

8. Zbulimi dhe përgjigjja ndaj incidenteve

22. Analiza e regjistrave dhe kronologjia

Analiza e regjistrave dhe kronologjia

Normalizo orën në UTC dhe dallimin midis orës së ngjarjes dhe orës së mbledhjes. Krahaso burime të pavarura. Kërko intervale që mungojnë dhe numëro ngjarjet me një metodë të dokumentuar.

Shembull i arsyetuar

Kronologjia është hyrje 10:02, ndryshim 10:04 dhe marrje alarmi 10:09 UTC. Përfundimet mbi identitetin kërkojnë verifikim.

Detyra

Regjistri A shënon hyrje 10:02 UTC. Regjistri B shënon ndryshim lejesh 11:04 CET. Regjistri C e merr alarmin në 10:09 UTC. Renditi dhe dalloi ngjarjen nga mbledhja.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Kronologjia është hyrje 10:02, ndryshim 10:04 dhe marrje alarmi 10:09 UTC. Përfundimet mbi identitetin kërkojnë verifikim.

23. Triagimi, kufizimi dhe ruajtja e provave

Triagimi, kufizimi dhe ruajtja e provave

Triagimi cakton përparësinë nga ndikimi, besueshmëria dhe shtrirja. Kufizimi synon të frenojë dëmin ndërsa ekipi mbledh prova. Ruaj origjinalet, dokumento zinxhirin e kujdestarisë dhe kufizo qasjen te personat përgjegjës.

Shembull i arsyetuar

Përcakto prioritetin, shkallën e pasigurisë, informacionin për kufizimin e seancave dhe pronarin e vendimit.

Detyra

Një llogari e privilegjuar ka një alarm me besueshmëri të lartë. Përgatit kartelën e triagimit dhe vendimin që i dërgohet përgjegjësit të incidentit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Përcakto prioritetin, shkallën e pasigurisë, informacionin për kufizimin e seancave dhe pronarin e vendimit.

24. Rikthimi dhe mësimet pas incidentit

Rikthimi dhe mësimet pas incidentit

Rikthimi kërkon kriter të verifikueshëm për shërbimin dhe kontroll të shenjave të përsëritjes. Raporti teknik përshkruan kronologjinë dhe provat. Përmbledhja për drejtuesit vendos në qendër

ndikimin, vendimet dhe veprimet me afat.

Shembull i arsyetuar

Provo funksionet kritike, konfirmo integritetin, verifiko alarmet dhe vendos pronar e afat për çdo përmirësim.

Detyra

Shërbimi është hapur përsëri pas incidentit. Listo provat për rikthimin, një shenjë monitorimi dhe dy veprime për takimin pas incidentit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Provo funksionet kritike, konfirmo integritetin, verifiko alarmet dhe vendos pronar e afat për çdo përmirësim.

Ushtrim në tryezë

Instruktori paraqet tre fakte me radhë: një sinjal hyrjeje, ndryshim i rolit dhe raport për ndërprerje të portalit. Caktoni përgjegjësin e incidentit, analistin e provave dhe kontaktin e biznesit. Për çdo fakt shënoni çfarë ndryshon vendimi dhe çfarë mbetet e panjohur.

Kriter: Regjistri i vendimeve duhet të përmbajë orën UTC, burimin, vendimin, arsyen dhe personin përgjegjës.

9. Puna profesionale dhe projekti

25. Rishikimi mbrojtës i dobësive

Rishikimi mbrojtës i dobësive

Një inventar dhe një kontroll konfigurimi ndihmojnë të identifikohen dobësitë. Vlerësimi merr parasysh ekspozimin dhe rëndësinë e asetit. Një gjetje kërkon provë të mjaftueshme, pronar, afat dhe verifikim pas masës.

Shembull i arsyetuar

Jep përparësi gjetjeve me ekspozim dhe ndikim të lartë. Shëno provën, pasojën, masën, pronarin dhe riprovën.

Detyra

Nga një raport i sajuar, krahaso sistemin publik të pambuluar nga përditësimet, një printer të izoluar dhe një dosje publike me kontrata. Përgatit tri kartela gjetjesh.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Jep përparësi gjetjeve me ekspozim dhe ndikim të lartë. Shëno provën, pasojën, masën, pronarin dhe riprovën.

26. Dokumentimi, auditimi dhe komunikimi

Dokumentimi, auditimi dhe komunikimi

Politika përshkruan çfarë kërkohet. Procedura udhëzon si kryhet puna. Prova tregon çfarë ka ndodhur. Gjetja e auditimit duhet të lidhë kërkesën, gjendjen e vëzhguar dhe ndikimin.

Shembull i arsyetuar

Shëno kriterin, periudhën dhe provat e shqyrtuara. Kërko evidencë ose cakto masë me pronar dhe afat.

Detyra

Kërkesa e brendshme parashikon rishikim tremujor të roleve. Provat për tremujorin e fundit mungojnë. Përgatit gjetjen dhe kërkesën për sqarim.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Shëno kriterin, periudhën dhe provat e shqyrtuara. Kërko evidencë ose cakto masë me pronar dhe afat.

27. Projekti final: regjistër rreziku dhe përgjigje

Projekti final: regjistër rreziku dhe përgjigje

Një analist lidh vendimet teknike me ndikimin në organizatë. Projekti përmbledh sigurinë e një biznesi me portal, identitet cloud dhe staf në distancë. Çdo përfundim duhet të jetë i gjurmueshëm te një fakt ose supozim i deklaruar.

Shembull i arsyetuar

Dokumenti emëron pronarë, masa dhe prova. Përgjigjja përcakton kufizimin e autorizuar, rikthimin me kritere dhe veprimet pas incidentit.

Detyra

Dorëzo inventar me pesë asete, pesë rreziqe të renditura, matricë me tri role, kronologji UTC, plan rikthimi me RPO/RTO dhe një përmbledhje prej 150 fjalësh për drejtuesit. Përdor skenarin e projektit.

Dorëzimi

Përgatit një shënim ose tabelë me vendimin, provën që e mbështet dhe supozimet. Për çdo veprim cakto kush e kryen dhe si verifikohet rezultati.

Vetëkontrolli

Dokumenti emëron pronarë, masa dhe prova. Përgjigjja përcakton kufizimin e autorizuar, rikthimin me kritere dhe veprimet pas incidentit.

Simulim interviste për analist fillestar

Përgjigju me strukturën situatë, veprim dhe rezultat. Për zbulim të paqartë thuaj çfarë di, çfarë do të verifikosh dhe kur do ta eskalosh.

Ushtrim: Jep një përgjigje të shkurtër për rastin “Nga cili regjistër do të nisje kur dikush raporton humbje të qasjes në portal?” Përmend identitetin, gjendjen e shërbimit dhe provat që i dallojnë dy shkaqet.

Projekti final — Rasti Liria

Liria është një kompani fiktive me 24 punonjës, portal faturash, identitet cloud, hapësirë dokumentesh dhe laptopë pune. Vizitorët përdorin Wi-Fi të veçantë. Shërbimi i faturimit ka objektiv RPO 4 orë dhe RTO 6 orë. Një kontraktor largohet sot. Disa administratorë ende nuk përdorin MFA rezistente ndaj phishing-ut. Ekipi i financës ka gjetur një lidhje publike për një dosje me kontrata.

Regjistrat e dhënë

- 08:00 UTC, kopjet rezervë: kopja e fundit e portalit përfundoi.
- 12:20 UTC, mbështetja: finance-02 raporton një njoftim MFA të pakërkuar.
- 13:22 CET, identiteti: hyrje e suksesshme e finance-02 nga pajisje e panjohur.
- 12:27 UTC, posta: u krijua një rregull përcjelljeje nga finance-02.
- 12:34 UTC, operacionet: portali i faturimit nuk i përgjigjet kontrollit.
- 16:10 UTC, operacionet: portali kaloi verifikimin e funksioneve pas rikthimit.

Dorëzimet

1. Inventar me pesë asete, pronar, klasifikim, varësi dhe ndikim.

2. Regjistër me pesë rreziqe. Shëno gjasën dhe ndikimin nga 1–3, kontrollin, pronarin, afatin dhe provën e mbylljes.

3. Matricë për krijuesin e faturës, miratuesin dhe auditorin. Shto hapat për largimin e kontraktorit.

4. Kronologji UTC. Dallo faktet nga hipotezat dhe përcakto si verifikohet lidhja e mundshme midis ngjarjeve.

5. Plan për kufizimin, provat, rikthimin dhe monitorimin. Llogarit diferencën midis kopjes dhe ndërprerjes dhe kohën deri te rikthimi.

6. Përmbledhje për drejtuesit, maksimumi 150 fjalë, me ndikimin e ditur, të panjohurat, vendimin dhe dy masa me afat.

Vlerësimi

- Inventari dhe renditja e rrezikut — 25 pikë.
- Identitetet, ndarja e detyrave dhe dokumentet — 20 pikë.
- Kronologjia dhe cilësia e provave — 20 pikë.
- Kufizimi, afatet e rikthimit dhe verifikimi — 25 pikë.
- Përmbledhja dhe cilësia e dorëzimit — 10 pikë.

Pragu i rekomanduar është 70/100. Arsyeto çdo supozim të rëndësishëm dhe përdor vetëm të dhënat e skenarit.