AKTIVITETI 10
DHOMA E LUFTËS SË SHKELJES SË TË DHËNAVE

Simulim: Reagimi ndaj Incidenteve te Sigurise

Workshop: AI dhe Dokumentet Biometrike - DITA 2

Dita 2 Pasdite | Aktiviteti 10 nga 12 | Kohezgjatja: 90 minuta

Objektivat e te Nxenit

1. Praktikoni reagimin ndaj shkeljeve te te dhenave ne kohe reale
2. Mesoni 5 fazat e pergjigjes ndaj incidenteve
3. Njihni kerkesat rregullatore per njoftim (72 ore)
4. Perdorni AI per analizen e shpejte te incidentit
5. Punoni ne ekip me role te percaktuara

Simulim: 5 skenare | 262,000 rekorde ne rrezik

Pse Pergatitja eshte Kritike?

FAKT: Koha mesatare per te zbuluar nje shkelje: 277 dite (IBM 2023)

Pasoja	Impakti per Institucione Qeveritare
Financiare	Gjoba deri 20M EUR ose 4% e buxhetit (GDPR)
Reputacioni	Humbja e besimit te qytetareve
Operacionale	Nderprerje e sherbimeve kritike
Ligjore	Padi, hetim, pergjegjesi penale
Personale	Demtim i qytetareve te prekur

5 Fazat e Pergjigjes

Faza	Emri	Koha	Fokusi Kryesor
1	IDENTIFIKIMI	0-2 ore	Konfirmoni, vleresoni, aktivizoni ekipin
2	IZOLIMI	2-6 ore	Ndaloni perhapjen, ruani provat
3	ELIMINIMI	6-24 ore	Hiqni kercenimin, mbyllni vulnerabilitetin
4	RIKUPERIMI	24-72 ore	Rivendosni, testoni, riaktivizoni
5	MESIMET	1-4 jave	Analizoni, dokumentoni, permiresoni

Kerkesat e Njoftimit

Kush Njoftohet	Afati	Kur
AKCESK	72 ore	Cdo shkelje qe prek te dhena personale
Komisioneri MDHP	72 ore	Kur preken te drejtat e subjekteve
Qytetaret e Prekur	Pa vonese	Kur rreziku eshte i larte
Policia/Prokuroria	Menjehere	Kur dyshohet veper penale

KUJDES: Mosnjoftimi brenda 72 oreve mund te rezultoje ne gjoba shtese!

Rolet ne Ekip

Roli	Pergjegjesit Kryesore
Drejtuesi i Incidentit	Koordinon, vendos, autorizon njoftimet
Analisti Teknik	Analizon log-et, identifikon sulmin, propozon zgjidhje
Koordinatori Ligjor	Perputhja rregullatore, njoftimet zyrtare
Komunikuesi	Mesazhet per publikun, media, qytetaret

Ne kete simulim, do te ndaheni ne ekipe me keto role

AI per Pergjigjen ndaj Incidenteve

Faza	Si Ndihmon AI
Identifikimi	Analizon log-et per pattern te dyshimta
Izolimi	Identifikon sistemet e lidhura qe mund te preken
Eliminimi	Kerkon vulnerabilitetin ne databazat e sigurise
Rikuperimi	Gjeneron lista kontrolli per rivendosje
Njoftimi	Harton draft-komunikime per palet e interesuara

Shablon Prompt per Analizen e Incidentit

```
Je ekspert i sigurise kibernetike dhe reagimit ndaj incidenteve.

INCIDENTI: [pershkrimi]
SISTEMET E PREKURA: [lista]
TE DHENAT NE RREZIK: [llojet]
REKORDE TE EKSPOZUARA: [numri]

Analizo dhe jep:
1. VLERESIMI I SERIOZITETIT (1-5)
2. VEPRIMET E MENJEHERSHME (5 me prioritare)
3. KERKESAT E NJOFTIMIT (kush, kur)
4. DRAFT I NJOFTIMIT per [AKCESK/Qytetaret]
5. PYETJET PER INVESTIGIM te metejshem
```

Skenaret e Simulimit

ID	Titulli	Serioziteti	Rekorde
BREACH-01	Sulm Ransomware	KRITIK	150,000
BREACH-02	Akses i Paautorizuar Brenda	I LARTE	5,000
BREACH-03	Rrjedhje nga Backup Cloud	I LARTE	80,000
BREACH-04	Sulm Phishing Administratoresh	KRITIK	25,000
BREACH-05	Humbje Laptopi me te Dhena	MESATAR	2,000

Detyra Juaj (60 Minuta)

Organizimi (5 min):

- Ndahuni ne 4-5 ekipe

- Caktoni rolet brenda ekipit

Simulimi (40 min):

- Merrni skenarin tuaj (te fsheht per te tjeret)

- Reagoni sipas 5 fazave

- Perdorni AI per ndihme ne analizen dhe komunikimin

- Dokumentoni te gjitha vendimet

Prezantimi (15 min):

- Cdo ekip paraqet rastin dhe pergjigjen (3 min/ekip)

Shablloni i Dokumentimit

Seksioni	Cfare Dokumentoni
INCIDENTI	Koha, pershkrimi, si u zbulua
IMPAKTI	Sistemet, te dhenat, numri rekordeve
KRONOLOGJIA	Cdo veprim me ore:minuta
VENDIMET	Kush vendosi cfare dhe pse
NJOFTIMET	Kush u njoftua, kur, si
STATUSI	Aktualisht ku jemi
HAPAT TJERE	Cfare mbetet per te bere

Gabimet e Zakonshme

Gabimi	Pasoja	Parandalimi
Vonesa ne izolim	Sulmi perhapet	Protokolle te paracaktuara
Mosruajtja e provave	Investigimi deshtuar	Kopjo log-et menjehere
Njoftim i vonuar	Gjoba + demtim reputacioni	Njofto brenda 72 oreve
Panik + vendime te nxituara	Demtim me i madh	Ndjek protokollin
Mungesa dokumentimi	Pamundesi auditimi	Sheno cdo hap

Komunikimi gjate Krizes

PER QYTETARET:

- Cfare ndodhi (pa detaje teknike)
- Cfare te dhenash u preken
- Cfare po bejme ne
- Cfare duhet te beni ju (ndryshoni fjalekalim, etj.)

PER AUTORITETET:

- Detaje teknike te incidentit
- Kronologji e plote
- Masat e marra
- Plani i vazhdimit

Kriteret e Vleresimit

Kriteri	Pike	Pershkrimi
Shpejtesia	20	Sa shpejt u reagua?
Metodologjia	25	A u ndoqen 5 fazat?
Dokumentimi	20	A u dokumentua gjithcka?
Komunikimi	20	A ishin mesazhet te qarta?
Puna Ekipore	15	A bashkepunoi ekipi mire?

Praktikat me te Mira

[Gatishmeri] Kini plan te paracaktuar para se te ndodhe

[Ekip] Dijeni kush ben cfare ne rast emergjence

[Shpejtesi] Koha eshte kritike - cdo ore ka rendesi

[Dokumentim] Shenoni gjithcka per auditim dhe mesime

[Komunikim] Qarte, e sakte, ne kohe te duhur

Pikat Kyce

[5 Faza] Identifikim, Izolim, Eliminim, Rikuperim, Mesime

[72 Ore] Afati maksimal per njoftimin e autoriteteve

[Ekip] Rolet e qarta dhe pergjegjesi te percaktuara

[AI Ndihmon] Per analizen, komunikimin, dokumentimin

Ne vazhdim: Aktiviteti 11 - Hartimi i Planit te Veprimit