Tema 2 Centru de Operatiuni de Securitate pentru Deutsche Bank

Deutsche Bank este una dintre cele mai mare institutii financiare la nivel global, fiind infintata in 1870.

Principalele nevoie de securitate.

Deutsche bank este supusa urmatoarelor amenintari:

1. Atacuri de tip phishing, ca banca aceasta gestioneaza un volum mare de tranzactii si date sensibilie, fiind o tinta atractiva pentru atacatori.

2. Atacuri DDoS, acestea pot perturba seriviciile bancare si pot distrage atentia in timp ce se desfasoara alte tipuri de atacuri

3. Amenintari interne, angajatii si tertii avand acces la date sensibile pot reprezenta o amenintare dificil de detectat

4. Atacuri ransomware, un astfel de atac poate cauza pierderi masive prin blocarea accesului la date

5. Brese de securitate, prin exploatarea vulnerabilitatilor in infrastructura IT

Obiectivele SOC

1. Monitorizarea infrastructurii IT si a sistemelor bancare 24/7

2. Protejarea datelor sensibile ale clientilor

3. Prevenirea si detectarea atacurilor cibernetice

4. Gestionarea eficienta a incidentelor

5. Asigurarea conformitatii cu reglementarile internationale privind protectia datelor GDPR

6. Actualizarea sistemelor critice prin cele mai recente patch-uri de securitate

Plan de actiune

1. SOC va implementa o platforma de tip SIEM si SOAR pentru colectarea datelor si actiune, prin care o echipa dedicata va gestiona incidentele de securitate

2. Se vor face teste de penetrare regulat si evaluari de securitate pentru a identifica si remedia vulnerabilitatile

3. Campanii de simulari phising pentru a creste constientizarea si educarea angajatilor

Functii si responsabilitati in cadrul SOC

1. Analist de evenimente: Monitorizeaza fluxurile de date si activitatea retelelor prin SIEM pentru a detecta, investiga si documenteaza evenimentele detectate.

2. Manager de incidente: Coordoneaza raspunsul echipei la incidente si implementeaza masuri adecvate. Coopereaza cu alte echipe de securitate pentru gestiona incidentele din diverse departamente si tocmeste rapoarte detaliate post-incident. De asemenea realizeaza exercitii periodice de simulare a incidentelor.

3. Analist de Securitate: realizeaza analize ale amenintarilor detectate si sugereaza masuri de securitate, investigheaza sistemele compromise pentru a identifica vectorii de atac, colaboreaza cu echipele de conformitate pentru a se asigura ca se respecta masurile de securitate, dezvolta strategii de protectie pentru amenintari de tip Zero Day.

4. Manager SOC: Supervizeaza activitatea zilnica SOC, coordoneaza resursele umane si tehnologice necesare echipei. Gestioneaza bugetul SOC, realizeaza rapoarte de performanta si asigura comunicarea atat interna cu echipa executiva si alte departamente, cat si cu stakeholderi. Coordoneaza traininguri de securitate.