Tema 5 - Compania Tereschbank necesita o arhitectura de securitate robusta pentru a proteja datele si a raspunde rapid la amenintari. Se poate crea o arhitectura de securitate completa folosind solutiile oferite de Microsoft. Folosirea unui singur vendor pentru toate solutiile de securitate ofera avantajul unei integrari eficiente si mai putine probleme de compatibilitate.

1. XDR – Microsoft Defender for Endpoint – este o solutia de XDR a Microsoft, care monitorizeaza si raspunde la amenintarile de securitate prin colectarea datelor din endpointuri, servere si retele. Acesta monitorieaza automat dispozitivele din retea, ofera protectie in timp real, raspunde automatizat la incidente si detecteaza comportamente suspecte.

2. Microsot Defender Antivirus – am decis sa fie utilizat programul antivirus de la acelasi vendor Microsoft. Microsoft Defender Antivirus este o solutie de tip Next-Gen Antivirus integrata cu Windows, ce foloseste machine learning si inteligenta artificiala pentru a bloca atat amenintarile cunoscute cat si cele necunoscute. Ofera protectie automata impotriva atacurilor prin semnaturi si analiza comportamentala. Acesta se integreaza cu Defender for Endpoint.

3. Microsoft DLP Purview – este solutia integrata de prevenire a scurgerilor de date oferita de Microsoft. Aceasta monitorizeaza si controleaza modul in care datele sensibile sunt utilizate si partajate in cadrul organizatiei. Monitorizeaza automat fluxurile de date prin aplicarea politicilor de securitate. Colaboreaza cu XDR si Antivirus pentru a bloca automat tentativele de exfiltrare a datelor.

4. Microsoft Sentinel – ca SIEM vom utiliza Sentinel care capabilitatea si de SOAR. Colecteaza si investigheaza datele din intreg sistemul IT, iar SOAR ne ofera capabilitatea sa si raspundem asupra incidentelor. Sentinel colecteza automat logurile si alertele din toate solutiile de securitate Microsoft si alte surse externe. Automatizeaza raspunsul la incidente prin integrarea cu Microsoft Defender for Endpoint pentru a bloca atacurile si a inita actiuni de remediere.

5. Azure Firewall – pentru a preveni atacurile de tip DDOS si spori protectia la nivel de retea vom folosi Azure firewall care este un Next-Gen Firewall. Acesta inspecteaza pachetele din retea, aplica regule de securitate si detecteaza comportamentul anormal in trafic. Este oferita o protectie automata prin monitorizarea in timp real a traficului retelei, oferind totodata capabilitati de detectarea si prevenire.

6. Threat and Vulnerability Management – ofera capabilitati de evaluare si remediere a vulnerabilitatilor intr-un sistem sau retea. Ofera o evaluare continua a punctelor slabe din infrastructura IT. Poate oferi prioritizare a vulnerabilitatilor pe baza contextului specific al organizatiei. Ofera scanare, evaluare si remediere automata a vulnerabilitatilor. De asemenea se integreaza cu Defender for Endpoint si SIEM.

O potentiala echipa de securitate care sa se ocupe de aceste solutii o constituie urmatoarea: CISO – Security Manager – echipa SOC L3,L2,L1 – Network Security Engineer – Security Analyst – Data Protection Engineer.

Aceste solutii colaboreaza perfect intre ele, Microsoft oferind conectori de integrare a solutiilor. Avand in vedere ca infrastructura IT este on premise, acestea ar acoperi partea de securitate si pot fi scalate si intr-un eventual sistem hibrid. Desi ar putea fi costisitor, in cazul utilizarii preponderente a sistemelor de operare Windows, sunt de parere ca tot Microsoft ofera cel mai bun si versatil serviciu de securitate, dat fiind si faptul ca telemetria si loguile sunt tot oferite de ei.