1. מהם שלושת הנושאים המטופלים על ידי אבטחת מידע ואבטחת סייבר ?

1.איומי אבטחת מידע חשאיות

דלף מידע

גניבת זהות

פגיעה בפרטיות

השגת מידע עבור תקיפה אחרת

2. איומי אבטחת מידע אמינות

שינוי מידע קיים

הוספת מידע

אבדן האמון במידע

3. אימוי אבטחת מידע זמנית

גניבת מצעי מידע

מחיקת מידע

השבתה

מניעת שירות

2.מנה/י 3 גורמי איום (נקראים גם מקורות איום) והסבר/י בקצרה (משפט שניים) מה מאפיין כל גורם

האקד בודד :

פעילות אופיינית

האקינג

הנדסה חברתית

פריצה פיזית פריצה למערכות מחשב גישה בלתי מורשה למערכת

ימוקים לתקיפה

•מחיקת מידע

•דלף מידע

•רווח כלכלי

–מכירת המידע לצד ג'

–כופרה Ransomware

•שינויים במי

ארגוני טרור

נימוקים לתקיפה סחיטה גרימת נזק ניצול נקמה

רווח פוליטית כיסוי תקשורת

פעילות אופיינית

פעילות טרור פיזית

לוחמת מידע

תקיפת מערכות

חדירה למערכות

חבלה במע

ממשלות

נימוקים לתקיפה יתרון מודיעיני

תמיכה בתעשייה מקומית

פגיעה באינטרסים של מדינה עוינת ערעור מערכות שלטון

גיוס סוכנים

סחיטה

לוחמת מידע

מבצעי השפעה

תעמולה

תקיפת מערכות

חדירה למערכות

חבלה במערכות

3. מנה/י את 5 השלבים ביישום מסגרת אבטחת  סייבר של NIST והסבר/י בקצרה (משפט שניים) מה יש לבצע בכל שלב ?

חמשת השלבים של מודל האבטחה

זיהוי ומיפוי – IDENTIFY (ID)

הגנה – Protect (PR)

איתור תקיפה – DETECT (DE)

תגובה – RESPOND (RS)

התאוששות( – RECOVER (RC

IDENTIFY

מיפוי נכסים

מיפוי סביבה עסקית

ממשל תאגידי

הערכת סיכונים

ניהול סיכונים

Protect

הגנה על מידע והגנה על תהלכים וניהולים

DETECT

אנומליות ואירועים חריגים

ניטור שוטף של היבטי אבטחה

תהליכי ניטור

RESPOND

תגובה

תכנון התגובה

תקשורת פנימית וחיצונית

ניתוח

הקטנת ובקרת נזקים

הפקת לקחים ושיפור

שחזור RECOVER (RC)

תכנון התאוששות והמשכיות עסקית

הפקת לקחים ושיפור

תקשורת פנימית וחיצונית