|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NFR** | **FR** | **דרישות ותיאור** | **מספר מזהה** | **קטגוריה / מודול** |
|  | **V** | המערכת תאפשר רישום ראשוני עם אימות כתובת מייל | 1.1 | רישום וכניסה למערכת |
|  | **V** | בעת כניסה למערכת, המשתמש יצטרך להזין שם משתמש וסיסמה | 1.2 |  |
|  | **V** | למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש | 1.3 |  |
|  | **V** | המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים | 2.1 | ניטור חבילות רשת |
|  | **V** | המערכת תשלח התראה מיידית במקרה של מתקפוות כמו DDOS או PHISHING | 2.2 |  |
|  | **V** | למערכת תהיה אפשרות לייצא דוחות מפורטים על פעילות רשת | 2.3 |  |
|  | **V** | המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג | 3.1 | ניטור משאבי חומרה |
|  | **V** | ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן | 3.2 |  |
|  | **V** | המערכת תשלח התראות ברורות במקרה של זיהוי דפוסים חשודים או איומים | 4.1 | התראות בזמן אמת |
|  | **V** | ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה | 4.2 |  |
| **V** |  | המערכת תכלול ממשק משתמש ברור ואינטואיטיבי, שיתאים למשתמשים לא טכניים | 5.1 | ממשק משתמש |
| **V** |  | התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה | 5.2 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NFR** | **FR** | **דרישות ותיאור** | **מספר מזהה** | **קטגוריה / מודול** |
|  | **V** | המערכת תאפשר רישום ראשוני עם אימות כתובת מייל (נבדק) | 1.1 | רישום וכניסה למערכת |
|  | **V** | בעת כניסה למערכת, המשתמש יצטרך להזין שם משתמש וסיסמה | 1.2 | )את הקטגוריות יש להעביר לשורות ולא לעמודות – קשה לנהל את הטבלה ככה) |
|  | **V** | למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש נבדק | 1.3 |  |
|  | **V** | המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים כמו דפוסי TCP/SYC במספר גדול שמציגים סיכוי למתקפת DDOS (יש להגדיר מה הוא דפוס חריג) | 2.1 | ניטור חבילות רשת |
|  | **V** | המערכת תשלח התראה מיידית במקרה של מתקפוות כמו DDOS או PHISHING נבדק | 2.2 |  |
|  | **V** | למערכת תהיה אפשרות לייצא דוחות מפורטים על פעילות רשת (יש לפתוח מודול של דוחות / קטגורית דוחות ולפרט מה הדוחות שיהיו שם) | 2.3 |  |
|  | **V** | המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג נבדק | 3.1 | ניטור משאבי חומרה |
|  | **V** | ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן (קטגורית דוחות / גרפים) | 3.2 |  |
|  | **V** | המערכת תשלח התראות ברורות במקרה של זיהוי דפוסים חשודים שממחישים על מתקפות אינטרנטיות או איומים מיקומיים כמו וירוס שמתחזה כקובץ רגיל (יש להגדיר מה הוא דפוס חשוד / איום) | 4.1 | התראות בזמן אמת |
|  | **V** | ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה נבדק | 4.2 |  |
| **V** |  | המערכת תכלול ממשק משתמש ברור ואינטואיטיבי, שיתאים למשתמשים לא טכניים (מיותר) | 5.1 | ממשק משתמש |
| **V** |  | התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה. ניתוני הרשת יוצגו ע"י תיבות טקסט המכילות את סוג הפקטה, זמן הגעתה, צבע התיבה יראה את רמת סיכון פקטה (אדום, צהוב, ירוק) (דורש יותר פרוט) | 5.2 |  |
| **V** |  | שימוש משאבי מחשב יוצג ע"י מעגל לא סגור כך אשר בו מוצג אחוז שימוש במשאב מחשב ומסביב המעגל יהיה בצבע מתאים לרמת השימוש (נמוך:ירוק וכו..) | 5.3 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **מספר מזהה** | **דרישה ותיאור** | | **FR** | **NFR** |
| 1 | רישום וכניסה למערכת | |  |  |
| 1.1 | המערכת תאפשר רישום ראשוני עם אימות כתובת מייל (נבדק) | | V |  |
| 1.2 | למערכת תהיה אפשרות לאיפוס סיסמה דרך כתובת המייל של המשתמש נבדק | | V |  |
| 2 | ניטור חבילות רשת |  | |  |
| 2.1 | המערכת תבצע ניטור בזמן אמת של תעבורות רשת ותזהה דפוסים חריגים כמו דפוסי TCP/SYC במספר גדול שמציגים סיכוי למתקפת DDOS (יש להגדיר מה הוא דפוס חריג) | | V |  |
| 2.2 | המערכת תשלח התראה מיידית במקרה של מתקפוות כמו DDOS או PHISHING נבדק | | V |  |
| 3 | ניטור משאבי חומרה |  | |  |
| 3.1 | המערכת תעקוב אחרי ניצול CPU, RAM ודיסק קשיח ותתריע על שימוש חריג נבדק | | V |  |
| 4 | התראות בזמן אמת |  | |  |
| 4.1 | המערכת תשלח התראות ברורות במקרה של זיהוי דפוסים חשודים שממחישים על מתקפות אינטרנטיות או איומים מיקומיים כמו וירוס שמתחזה כקובץ רגיל (יש להגדיר מה הוא דפוס חשוד / איום)חוץ מווינדוז כגון איבחון וזיהוי שימוש יתר בחומרה | | V |  |
| 4.2 | ההתראות יכללו מידע על סוג האיום, מקורו, והמלצות לפעולה נבדק | | V |  |
| 5 | ממשק משתמש | |  |  |
| 5.1 | התצוגה תציג נתוני רשת ומשאבים בצורה גרפית וברורה. ניתוני הרשת יוצגו ע"י תיבות טקסט המכילות את סוג הפקטה, זמן הגעתה, צבע התיבה יראה את רמת סיכון פקטה (אדום, צהוב, ירוק) (דורש יותר פרוט) | | V |  |
| 5.2 | ניצול משאבי המחשב יוצג באמצעות תרשים מעגלי פתוח, בו יוצגו אחוזי השימוש במשאבים השונים. צבע המעגל יתאים לרמת השימוש, לדוגמה: ירוק לניצול נמוך, צהוב לניצול בינוני, ואדום לניצול גבוה. | | V |  |
| 6 | דוחות וגרפים | |  |  |
| 6.1 | המערכת תייצא דוחות מפורטים הכוללים:   * פעילות רשת: תעבורת רשת לפי IP, סוג פרוטוקול (TCP/UDP), וזיהוי איומים. * משאבי חומרה: ניצול RAM, CPU, ודיסק קשיח לאורך זמן. | | V |  |
| 6.2 | המערכת תשלח מיילים לשם התראת המשתמש על דפוסים מסוכנים במידה שהמשתמש היה רחוק מהמחשב. מיילים אלו יכללו תיאור קצר על פקטה מסוכנת ואיך בדרך כלל גורמים זדוניים  (יש לפתוח מודול של דוחות / קטגורית דוחות ולפרט מה הדוחות שיהיו שם) | |  | V |
| 6.3 | המשתמש יכול לסנן את התצוגה בממשק כך שתציג את כל סוגי הפקטות או פקטות מסוג מסוים בלבד, בהתאם להעדפתו | |  | V |
| 6.4 | ניתן יהיה להציג גרפים על שימוש במשאבי חומרה לאורך זמן (קטגורית דוחות / גרפים) | |  | V |