

שיעור 7

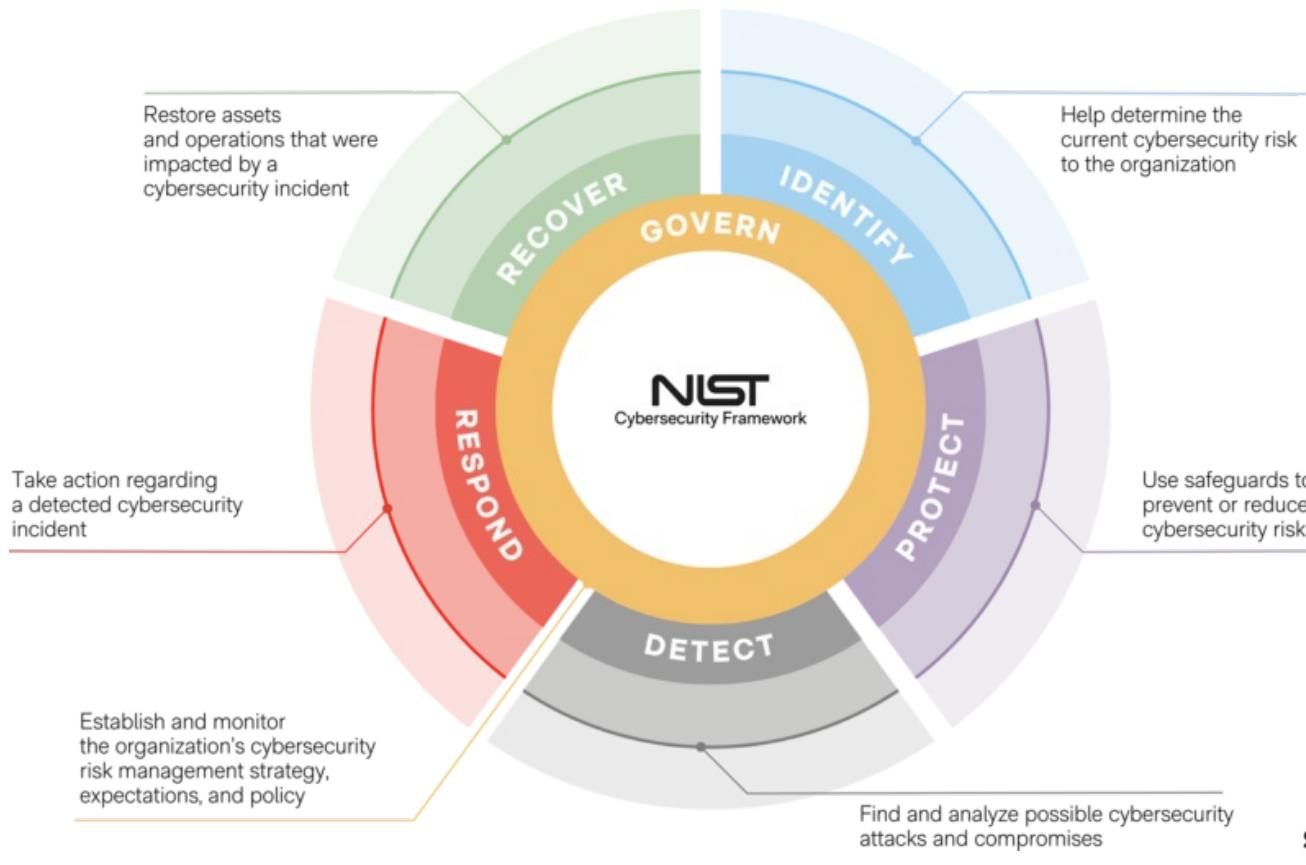
תורת ההגנה/NIST ושות הפענקציות: **Govern, Identify, Protect, Detect, Respond, Recover**

מטרת השיעור

- הבנת המסגרת: הכרת מבנה מסגרת 2.0 NIST מטרותיה, ותפקידה בניהול סיכון סייבר בארגון.
- היכרות עם הפונקציות: הבנת שש הפונקציות: Detect, Respond, Recover
- הבנה עמוקה על משלות הסייבר בארגון.



NIST Cybersecurity Framework (2.0)



פונקציות, קטגוריות, נת-קטגוריות

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



עינויים במחסום ה-5 NIST CSF 2.0

The CSF Core Functions — GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER — organize cybersecurity outcomes at their highest level.

- **GOVERN (GV)** — *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.* The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations. Governance activities are critical for incorporating cybersecurity into an organization's broader enterprise risk management (ERM) strategy. GOVERN addresses an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

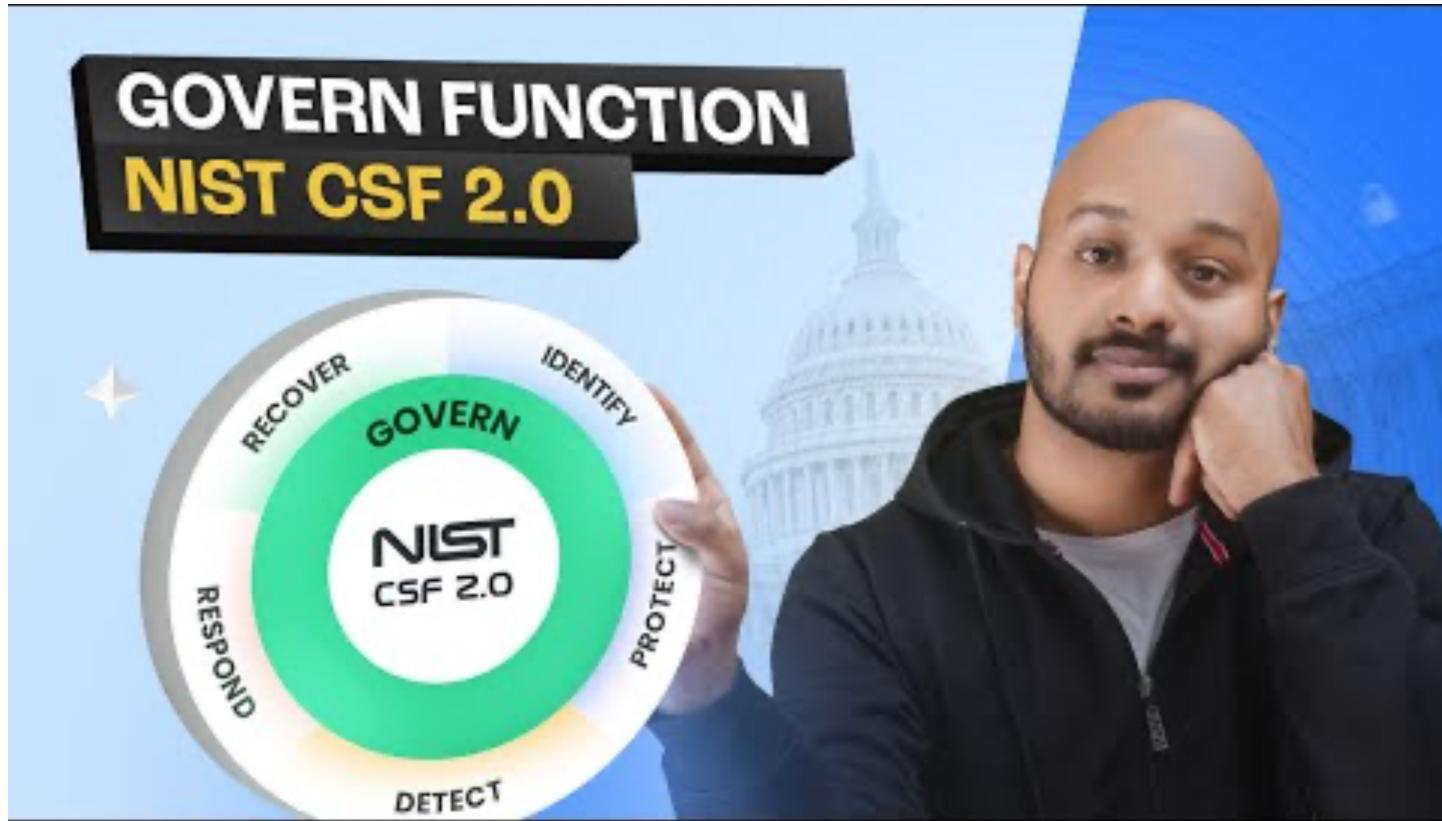


עינויים במחסום ה-5 NIST CSF 2.0

The GOVERN Function supports organizational risk communication with **executives**. Executives' discussions involve strategy, particularly how cybersecurity-related uncertainties might affect the achievement of organizational objectives. These governance discussions support dialogue and agreement about risk management strategies (including cybersecurity supply chain risk); roles, responsibilities, and authorities; policies; and oversight. As executives establish cybersecurity priorities and objectives based on those needs, they communicate expectations about risk appetite, accountability, and resources. Executives are also responsible for integrating cybersecurity risk management with ERM programs and lower-level risk management programs (see Sec. 5.2). The communications reflected in the top half of Fig. 5 can include considerations for ERM and the lower-level programs and, thus, inform managers and practitioners.

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>





<https://www.youtube.com/watch?v=yzlzbS7oPf8>

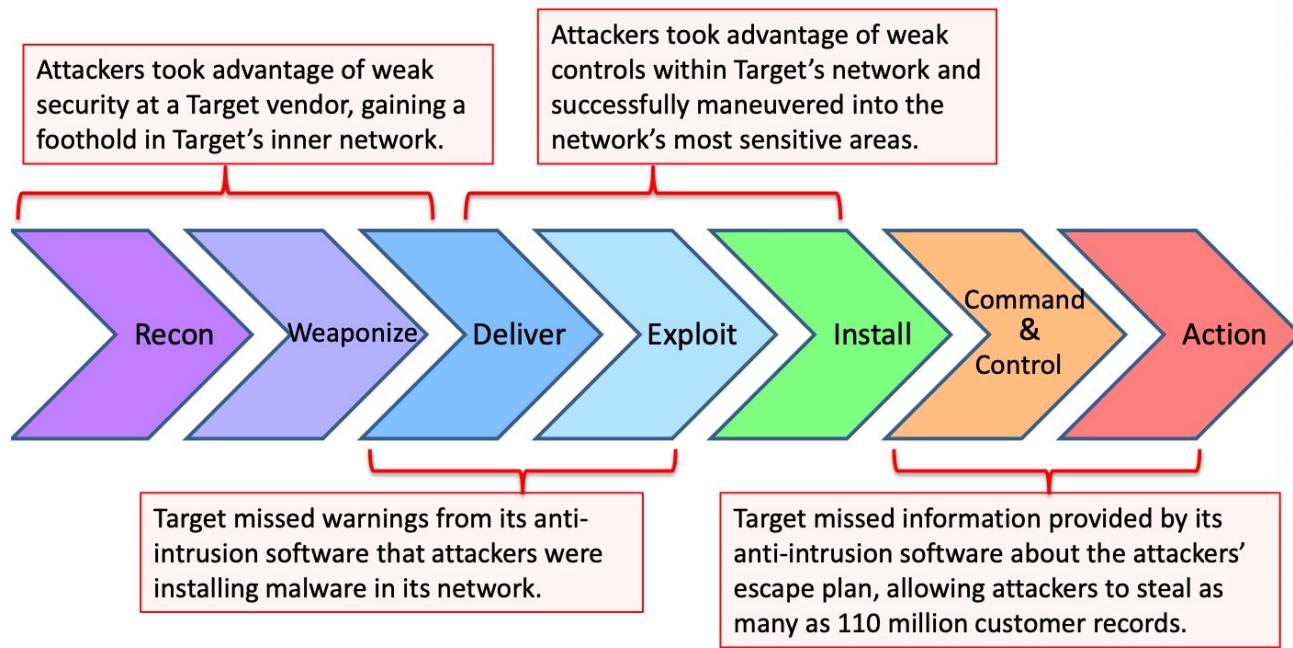
דוגמא לכישלון משלוח: מתקפת הסייבר על רשות טרגט ב-2013



<https://www.youtube.com/watch?v=v5rAW9oqTD8>

דוגמה לכישלון משלוח: מתקפת הסייבר על רשת טארגט ב-2013

Target's Possible Missed Opportunities



<https://www.commerce.senate.gov/services/files/24d3c229-4f2f-405d-b8db-a3a67f183883>

עובדת הגשה: הסבר

מה עושים במלת הביניים?

- בוחרים מסגרת או מספר מסגרות ומישמים אותן על ארגון אמיתי או דמיוני וכותבים מסמך מדיניות ונוהלים- לשימוש מדיניות סיבר בארגון.
- **נדרשים כ-5-3 עמודי תוכן לניתוח המקירה ומצגת מסכמת, ז"א כ-2500 מיליון).**
- המליצה היא להתחיל לעבוד על הצגת מטלת הביניים באמצעות הקורס לפי החומר הנלמד ולחدد את הדברים לקרהת השיעורים האחרונים.

מתי מגישים ומה?

הציג בכתיבה: בשיעור האחרון!

שליחת עבודה במיל למרצה: עד חודש מהשיעור האחרון של הסמסטר.

ניקוד

50% תוכן ודיק בפרטים

20% מבנה

20% כתיבה וביבליוגרפיה

10% הציג בכתיבה

סיכום ושאלות



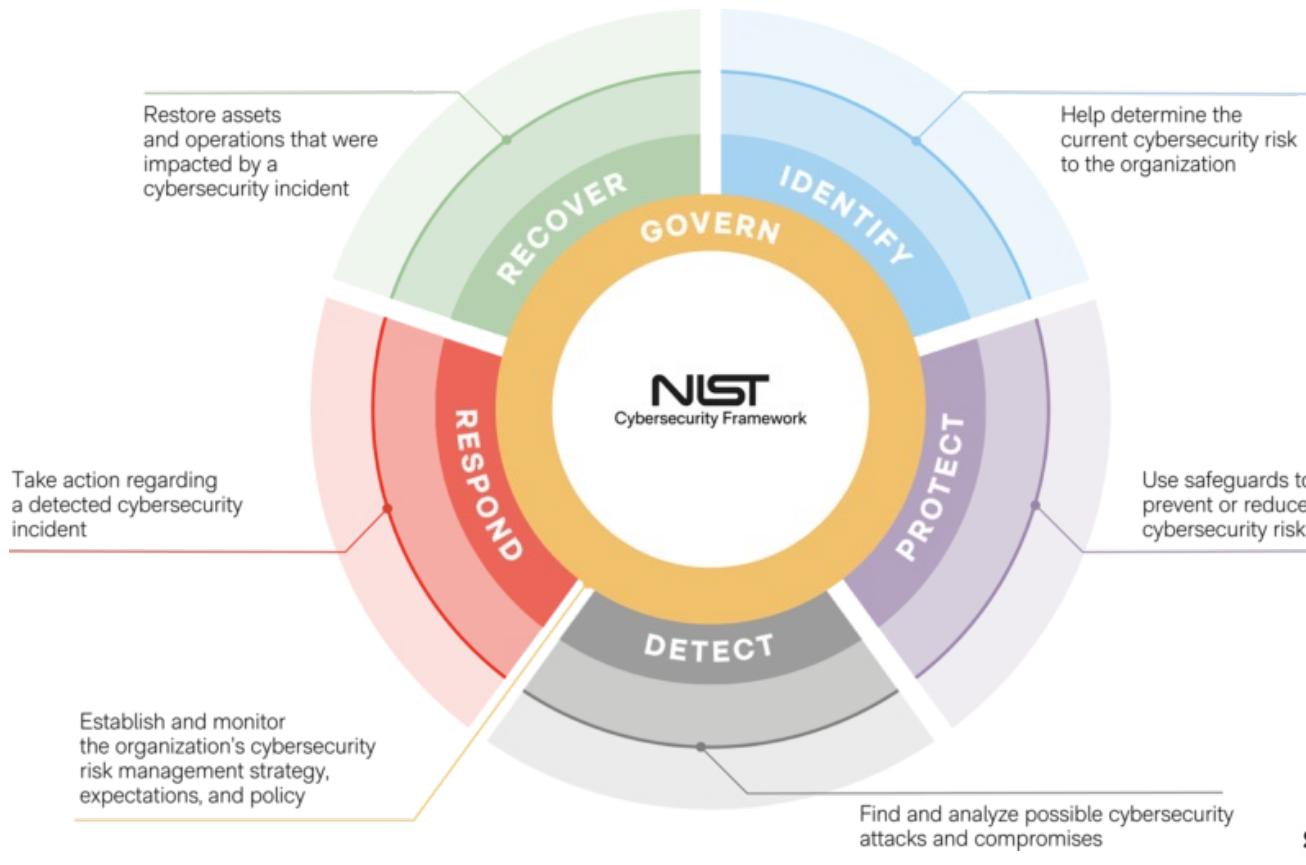
שיעור 8

פונקציית **Identify**: זיהוי נכסים וסיכוןם.

מטרת השיעור

- הבנת המסגרת: הכרת מבנה מסגרת 2.0 NIST מטרותיה, ותפקידה בניהול סיכון סייבר בארגון.
- היכרות עם הפונקציות: הבנת שש הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover
- **הבנה עמוקה על זיהוי נכסים ארגוניים וסיכוןם.**

NIST Cybersecurity Framework (2.0)



מטרת השיעור

- הבנת המסגרת: הכרת מבנה מסגרת 2.0 NIST מטרותיה, ותפקידה בניהול סיכון סייבר בארגון.
- היכרות עם הפונקציות: הבנת שש הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover
- הבנה עמוקה על זהויות נכסים ארגוניים וסיכוןים.
- הבנת החיבור בין פונקציית הזהוי לפונקציות האחרות.



הגדרה רחבה של פונקציית **Identify** מודיען היא חשובה

ניהול נכסים Asset Management

- חשיבות מיפוי כל הנכסים הדיגיטליים (שרותים, רשותות, אפליקציות, מסדי נתונים, התקני קצה, שירותי ענן וכו').
- קשרור בין נכס לבין בעליים/גורם אחראי בארגון.
- עדכון ותחזוקה מתמשכת של רשימות הנכסים, כולל גרסאות ומיקומים פיזיים או לוגיים.

הערכת סיכוןים Risk Assessment



- זיהוי הסיכוןים והאיוםים שעלולים להשפיע על הנכסים הקritisטיים.
- הערכת ההסתברות וההשפעה Probability & Impact של כל סיכון.
- שימוש בכלים ניהול סיכון (כמו FAIR, OCTAVE או מתודולוגיות אחרות) כדי לכמת סיכון.

הגדרה רחבה של פונקציית **Identify** מודיען היא חשובה

הבנת הסביבה העסקית Business Environment

- הבנת המשימות הקייטיות, התלות בין יחידות עסקיות שונות, שרשרת הערך של הארגון והספקים העיקריים.
- קביעת סדרי עדיפויות לאבטחה בהתאם לסיכון העסקי.

שילוב ממשל וציותות Identify & Govern & Compliance בtower

- התאמת תהליכי הזיהוי למסגרת הרגולציה והמדיניות שהוגדרה ב-Govern & Compliance.
- זיהוי דרישות תאימות (כגון GDPR, HIPAA, PCI-DSS וכו') בהתאם לאופי ולמיקום פעילות הארגון.

ניהול סיכון שרשרת אספקה Supply Chain Risk Management

- זיהוי ספקים וצדדים שלישיים המהווים חוליה אפשרית לפגיעה בארגון (לדוגמה: ספק ענן, קבלנים, אינטגרטורים).
- מיפוי נקודות החיבור לרשות הארגון וסקירת הסכמים (חוזי אבטחה, SLA).



הקשר בין Identify לשאר הפעולות

Identify ↔ Protect

על בסיס מיפוי הנכסים והסיכוןם, בוחרים ומישמים בקרות הגנה Protect רלוונטיות. דוגמה: אם זהה נכס בעל סיכון גבוה (למשל שרת בסיס נתונים עם מידע רגיש), נדרשת בקרת גישה מחמירה, הצפנה, גיבויים תכופים וכו'.

Identify ↔ Detect



ניהול נכסים מדויק עוזר להגדיר ולכידل מערכות ניטור ובקרת חדרות, מערכות MIES, מערכות IPS/IDS וכו' כדי לפקח על הנכסים החשובים ביותר.

דוגמה: אם ידוע על שירותי ספציפיים הנחשבים קריטיים, ניתן למקד בהם חוקים ותראות ייעודיות לגילוי חריגות.

הקשר בין Identify לשאר הפעולות

Identify → Respond

תכnon נכון של Identify מתחד גם גורמים אחראים Owners על כל נכס, וכן מידע נוחז לתגובה מהירה בעת אי-rouch.

דוגמא: אם מתגלת אי-rouch בשרת קרייטי, ידוע מידית למי לפנות וכי-יך להפעיל את תוכנית התגובה.

Identify ← Recover

כדי להתאושש ביעילות מאירוע, יש צורר ברשימה נכסים ובהגדרת סדרי עדיפות, כולל תוכנית גיבוי ו恢復 כמו RPO/RTO.



דוגמא: אם ארגון יודע מהם הנכסים הקרייטיים ביותר, הוא יתעדף את שיקומם בהקדם לאחר אי-rouch סייבר.

יישום מעשי של פונקציית היזהוי

הקמת צוות Identify

- שילוב גורמי ID, אבטחת מידע, הנהלה, ניהול סיכון וספקים במידה הצורך.
- הגדרת בעל תפקיד מוביל (לעתים זה ה- ISO 27001 בשיתוף עם ניהול התשתיות).

כליים וטכנולוגיות

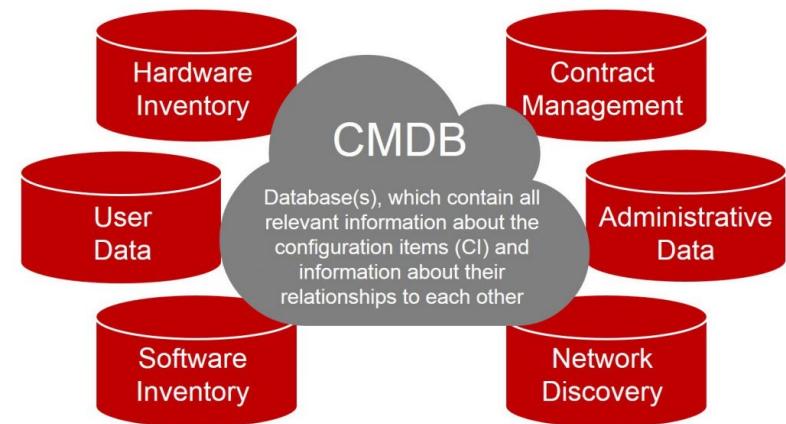
- תוכנות לניהול מלאי נכסים Asset Management Software המאפשרות גילוי אוטומטי של רכיבי רשת (סרייקות, סוכנים).
- מערכות סריקת פגיעויות Vulnerability Scanners כדי לזהות חולשות בכל נכס.
- מסדי נתונים ריכוזיים CMDB – Configuration Management Database לтиיעוד רשימת התוצרות (גרסאות תוכנה, מערכות הפעלה וכו').



ישום מעשי של פונקציית הזיהוי



<https://www.assetinfinity.com/blog/requirements-of-asset-management-system>



<https://pinkacademy.nl/kennisbank/configuration-management-database-cmdb/>

יישום מעשי של פונקציית הדיזהוי: שלבים



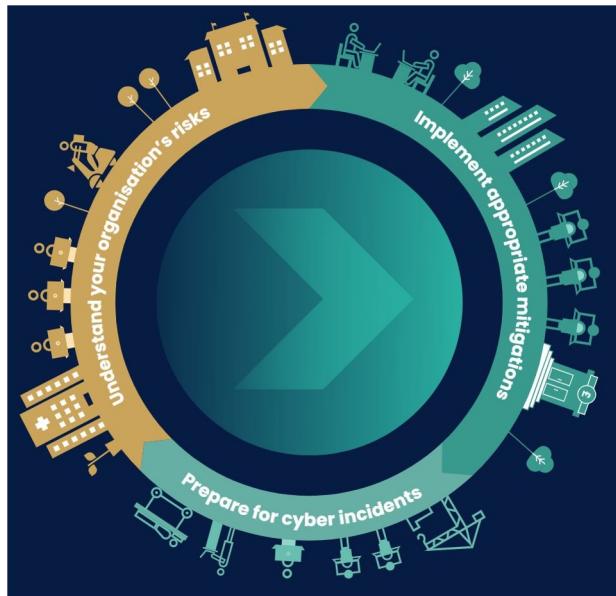
- שלב התחלתי: סריקת רשת ראשונית, בניית רשימת נכסים גולמית, מיפוי חיבורים ועבודה מול המחלקות השונות.
- שלב מתקדם: הערכת סיכונים מפורטת, תיעוד, ניתוח איזומים וויאזג רמת קritisיות.
- שלב מתמשך: עדכון ושיפור שוטף של הרשימות, ביצוע סקרים וסקירות חצי-שנתיות או שנתיות, הטמעת שינויים עקב התפתחות העסק והטכנולוגיה.
- ***שימוש בסטנדרטים ידועים כמו ISO 27001 בתחום ניהול סיכונים וניהול נכסים.

מקרה בוחן: רשת מלונות מרriott



<https://www.youtube.com/watch?v=JFRkneFoz5M&t=69s>

דיוון/תרגיל



- משילות, זיהוי, מלאי וסיכון, אחריות
- זיהוי וקשר עם שאר הfonוקציות

סיכום ושאלות

