

שיעור 7

תורת ההגנה/NIST וששת הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover

מטרת השיעור

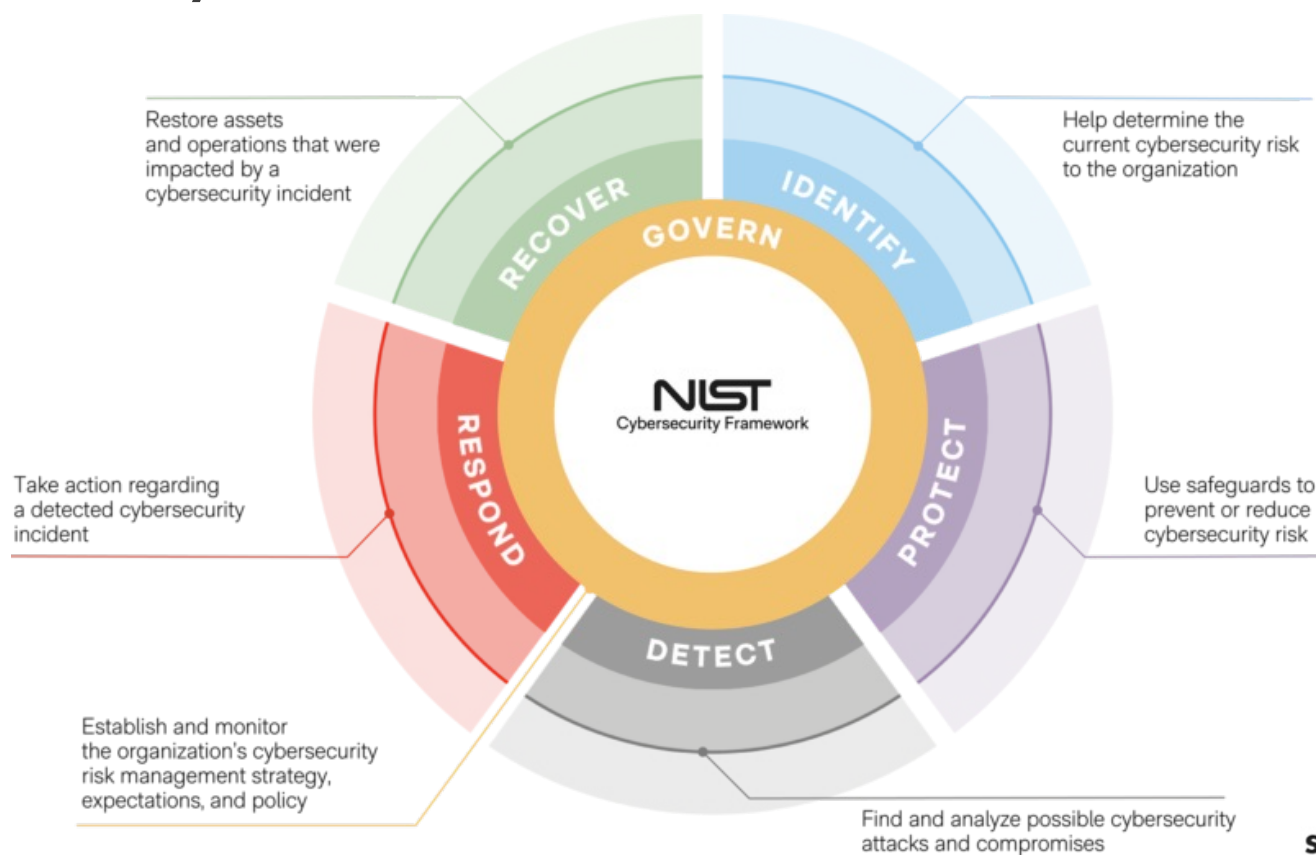
- הבנת המסגרת: הכרת מבנה מסגרת NIST 2.0 מטרותיה, ותפקידה בניהול סיכוני סייבר בארגון.



- היכרות עם הפונקציות: הבנת שש הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover

- הבנה מעמיקה על משילות הסייבר בארגון.

NIST Cybersecurity Framework (2.0)



פונקציות, קטגוריות, תת-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



עיונים במסמך ה-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>

עיונים במסמך ה-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>

הסבר קצר



<https://www.youtube.com/watch?v=yzl2bS7oPf8>

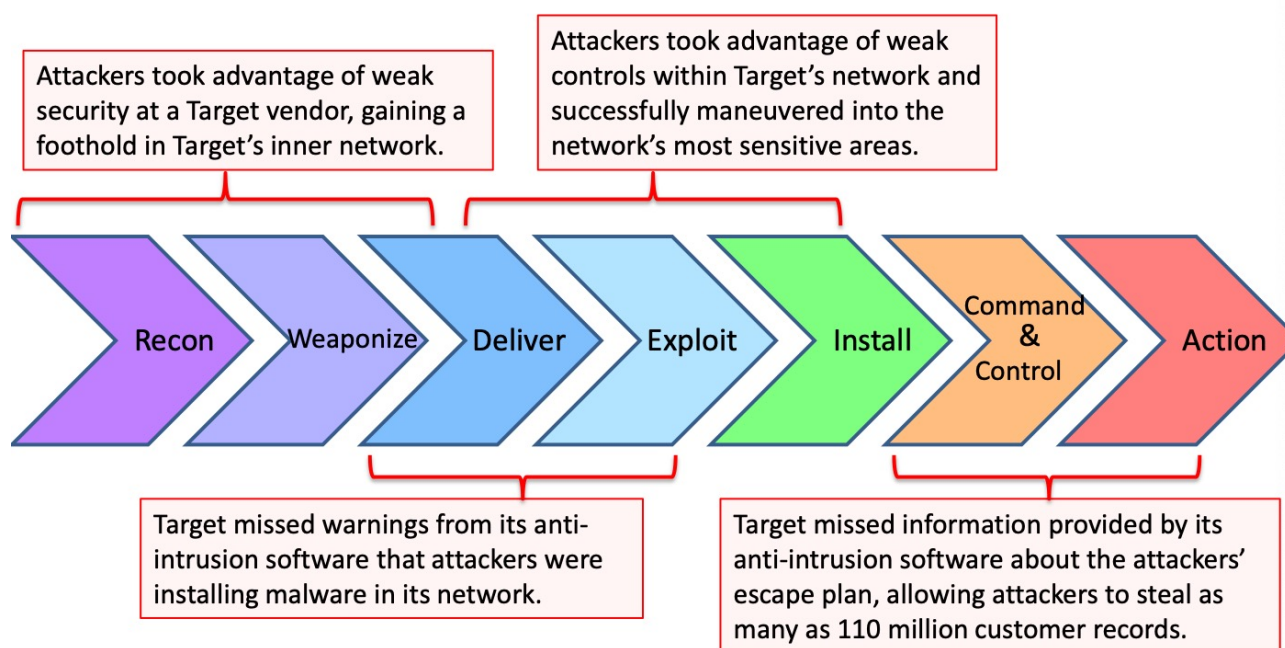
דוגמא לכישלון משילות: מתקפת הסייבר על רשת טארגט ב-2013



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

דוגמא לכישלון משילות: מתקפת הסייבר על רשת טארגט ב-2013

Target's Possible Missed Opportunities



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

עבודת הגשה: הסבר

מה עושים במטלת הביניים?

- בוחרים מסגרת או מספר מסגרות ומיישמים אותן על ארגון אמיתי או דמיוני וכותבים מסמך מדיניות ונהלים ליישום מדיניות סייבר בארגון.
- נדרשים כ-3-5 עמודי תוכן לניתוח המקרה ומצגת מסכמת, ז"א כ-2500 מילים).
- ההמלצה היא להתחיל לעבוד על הצגת מטלת הביניים באמצע הקורס לפי החומר הנלמד ולחדד את הדברים לקראת השיעורים האחרונים.

מתי מגישים ומה?

הצגה בכיתה: בשיעור האחרון!
שליחת עבודה במייל למרצה: עד חודש מהשיעור האחרון של הסמסטר.

ניקוד

- 50% תוכן ודיוק בפרטים
- 20% מבנה
- 20% כתיבה וביבליוגרפיה
- 10% הצגה בכיתה



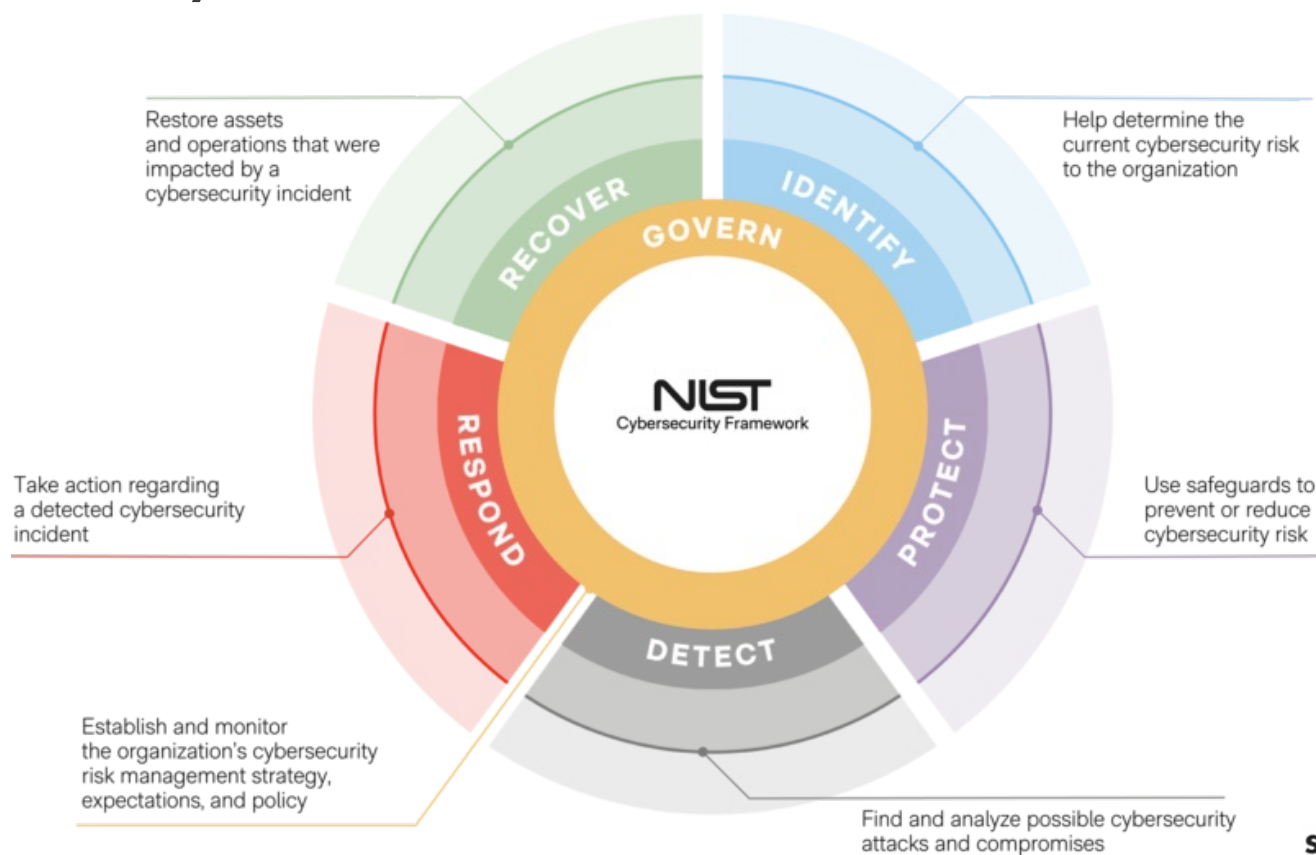
שיעור 8

פונקציית Identify: זיהוי נכסים וסיכונים.

מטרת השיעור

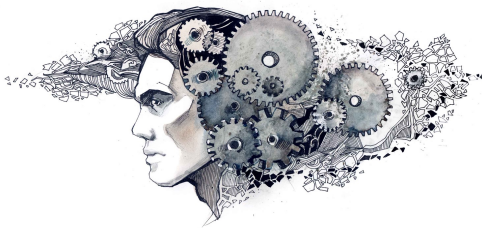
- הבנת המסגרת: הכרת מבנה מסגרת NIST 2.0 מטרותיה, ותפקידה בניהול סיכוני סייבר בארגון.
- היכרות עם הפונקציות: הבנת שש הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover
- **הבנה מעמיקה על זיהוי נכסים ארגוניים וסיכונים.**

NIST Cybersecurity Framework (2.0)



מטרת השיעור

- הבנת המסגרת: הכרת מבנה מסגרת NIST 2.0 מטרותיה, ותפקידה בניהול סיכוני סייבר בארגון.
- היכרות עם הפונקציות: הבנת שש הפונקציות: Govern, Identify, Protect, Detect, Respond, Recover
- הבנה מעמיקה על זיהוי נכסים ארגוניים וסיכונים.
- הבנת החיבור בין פונקציית הזיהוי לפונקציות האחרות.



הגדרה רחבה של פונקציית Identify | מדוע היא חשובה

ניהול נכסים Asset Management

- חשיבות מיפוי כלל הנכסים הדיגיטליים (שרתים, רשתות, אפליקציות, מסדי נתונים, התקני קצה, שירותי ענן וכו').
- קישור בין נכס לבין בעלים/גורם אחראי בארגון.
- עדכון ותחזוקה מתמשכת של רשימות הנכסים, כולל גרסאות ומיקומים פיזיים או לוגיים.

הערכת סיכונים Risk Assessment

- זיהוי הסיכונים והאיומים שעלולים להשפיע על הנכסים הקריטיים.
- הערכת ההסתברות וההשפעה Probability & Impact של כל סיכון.
- שימוש בכלי ניהול סיכונים (כמו FAIR, OCTAVE או מתודולוגיות אחרות) כדי לכמת סיכונים.



הגדרה רחבה של פונקציית Identify מדוע היא חשובה

הבנת הסביבה העסקית Business Environment

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

שילוב ממשל וציות Govern & Compliance בתוך Identify

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

ניהול סיכוני שרשרת אספקה Supply Chain Risk Management

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



הקשר בין Identify לשאר הפונקציות

Identify ↔ Protect

על בסיס מיפוי הנכסים והסיכונים, בוחרים ומיישמים בקורות הגנה Protect רלוונטיות. דוגמה: אם זוהה נכס בעל סיכון גבוה (למשל שרת בסיסי נתונים עם מידע רגיש), נדרשת בקרת גישה מחמירה, הצפנה, גיבויים תכופים וכו'.

Identify ↔ Detect

ניהול נכסים מדויק עוזר להגדיר ולכייל מערכות ניטור ובקרת חדירות, מערכות SIEM, מערכות IDS/IPS וכו' כדי לפקח על הנכסים החשובים ביותר.

דוגמה: אם ידוע על שרתים ספציפיים הנחשבים קריטיים, ניתן למקד בהם חוקים והתראות יעודיות לגילוי חריגות.



הקשר בין Identify לשאר הפונקציות

Identify ↔ Respond

תכנון נכון של Identify מתעד גם גורמים אחראיים Owners על כל נכס, וכן מידע נחוץ לתגובה מהירה בעת אירוע.

דוגמה: אם מתגלה אירוע בשרת קריטי, ידוע מיידית למי לפנות וכיצד להפעיל את תוכנית התגובה.

Identify ↔ Recover

כדי להתאושש ביעילות מאירוע, יש צורך ברשימת נכסים ובהגדרת סדרי עדיפויות, כולל תכנית גיבוי ושחזור כמו RTO/RPO.

דוגמה: אם ארגון יודע מהם הנכסים הקריטיים ביותר, הוא יתעדף את שיקומם בהקדם לאחר אירוע סייבר.



יישום מעשי של פונקציית הזיהוי

הקמת צוות Identify

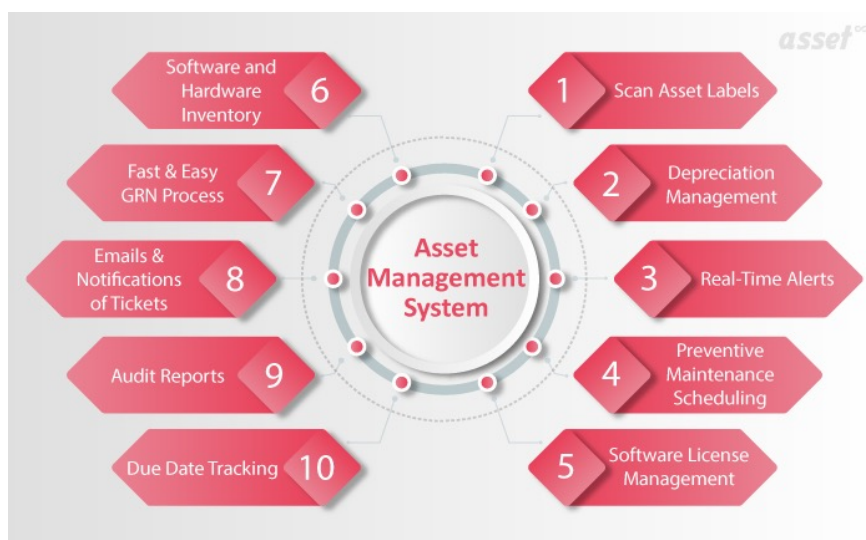
- שילוב גורמי IT, אבטחת מידע, הנהלה, ניהול סיכונים וספקים במידת הצורך.
- הגדרת בעל תפקיד מוביל (לעיתים זה ה- CISO בשיתוף עם מנהל התשתיות).

כלים וטכנולוגיות

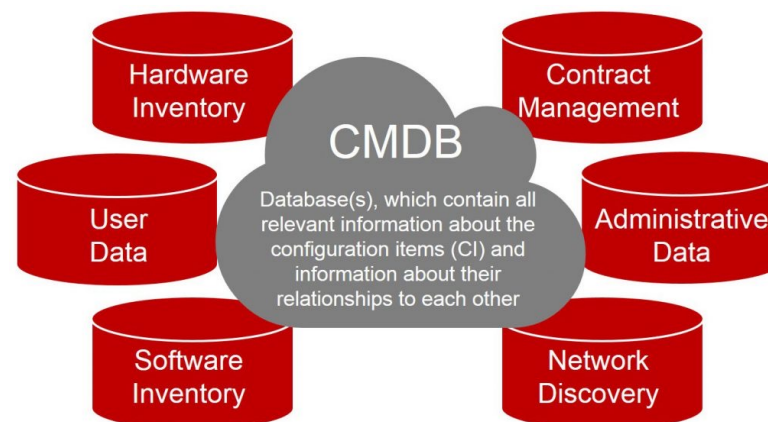
- תוכנות לניהול מלאי נכסים Asset Management Software המאפשרות גילוי אוטומטי של רכיבי רשת (סריקות, סוכנים).
- מערכות סריקת פגיעויות Vulnerability Scanners כדי לזהות חולשות בכל נכס.
- מסדי נתונים ריכוזיים CMDB – Configuration Management Database לתיעוד רשימת התצורות (גרסאות תוכנה, מערכות הפעלה וכו').



יישום מעשי של פונקציית הזיהוי



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



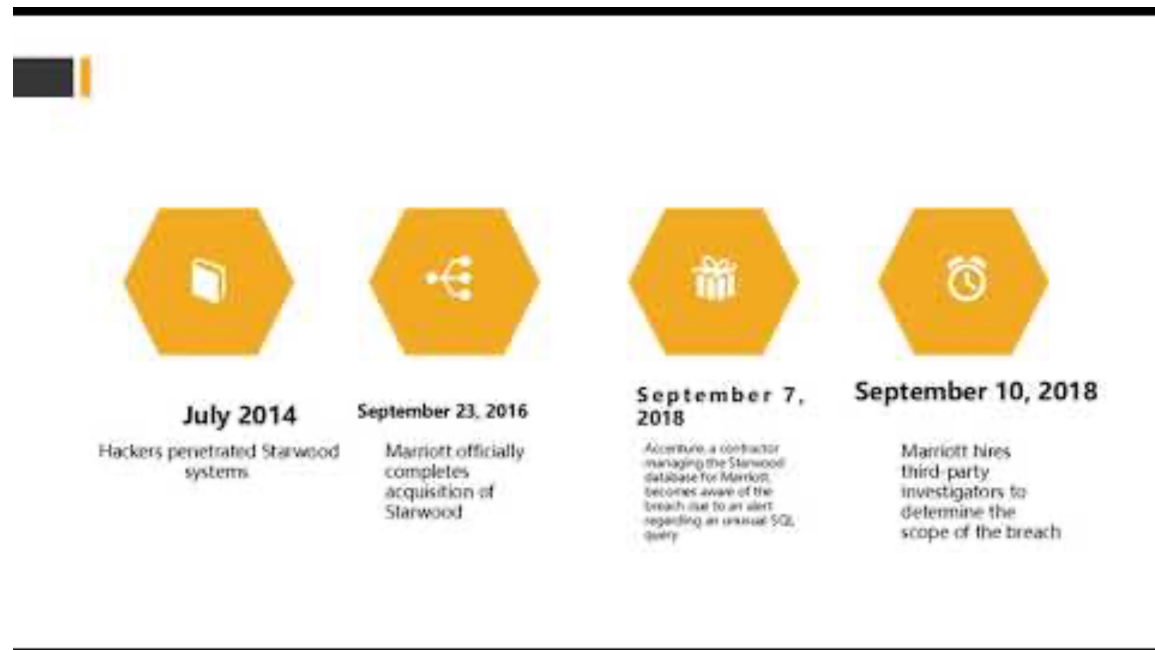
<https://pinkacademy.nl/kennisbank/configuration-management-database-cmdb/>

יישום מעשי של פונקציית הזיהוי: שלבים



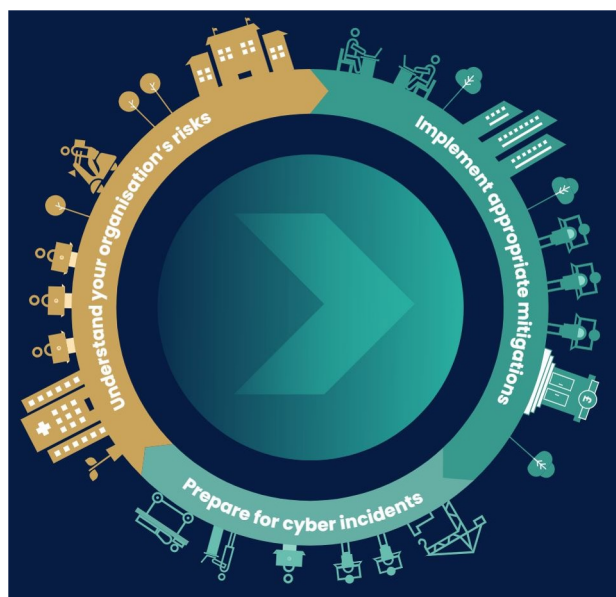
- שלב התחלתי: סריקת רשת ראשונית, בניית רשימת נכסים גולמית, מיפוי חיבורים ועבודה מול המחלקות השונות.
- שלב מתקדם: הערכת סיכונים מפורטת, תיעדוף, ניתוח איומים וסיווג רמת קריטיות.
- שלב מתמשך: עדכון ושיפור שוטף של הרשימות, ביצוע סקרים וסקירות חצי-שנתיות או שנתיות, הטמעת שינויים עקב התפתחות העסק והטכנולוגיה.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

מקרה בוחן: רשת מלונות מריוט Marriot



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

דיון/תרגיל



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

