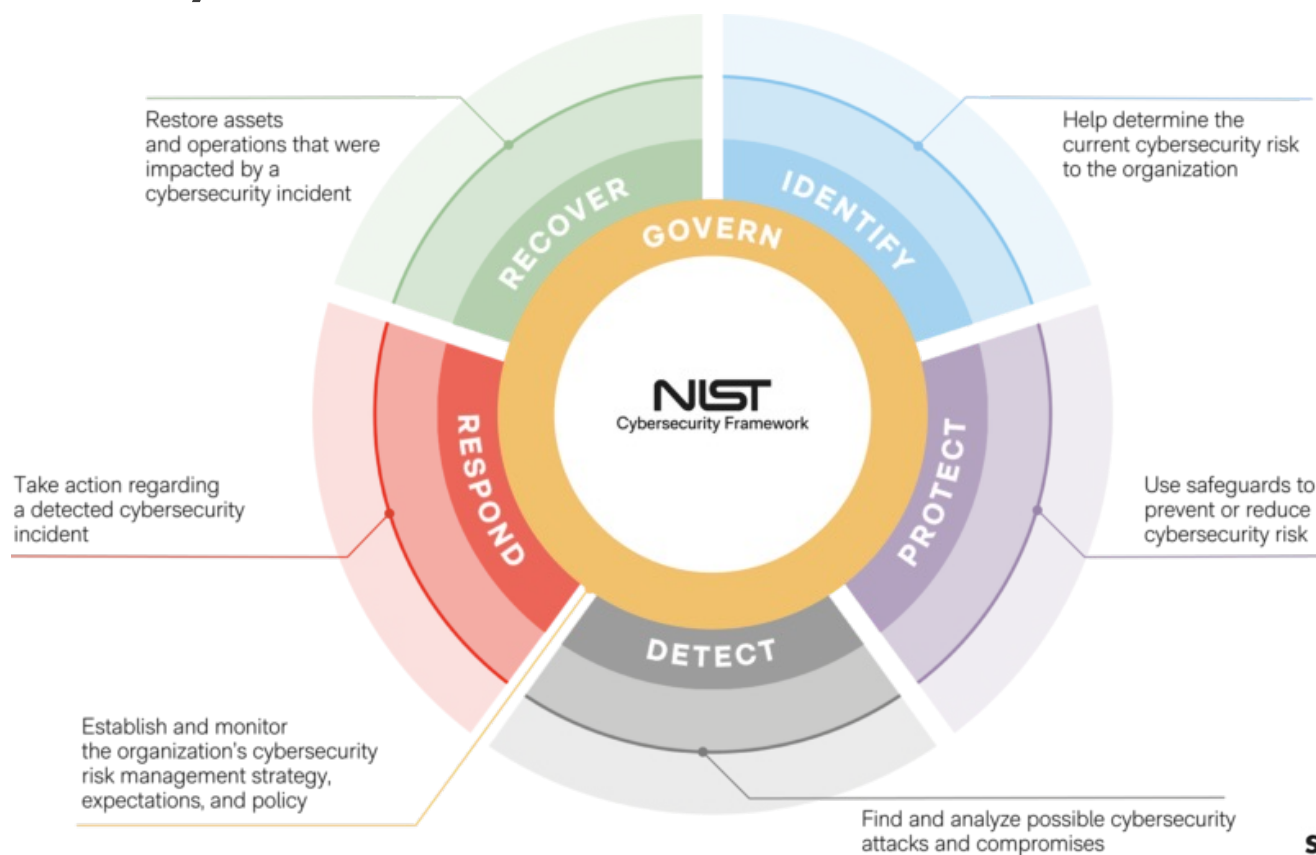


מטרת השיעור

- 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 של ניטור וגילוי.
- הבנת החיבור בין פונקציית הניטור והגילוי לפונקציות האחרות.

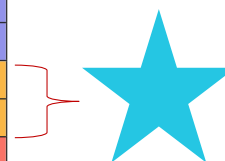


NIST Cybersecurity Framework (2.0)



NIST Cybersecurity Framework (2.0): Protect

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



הגדרה רחבה של פונקציית Protect ומדוע היא חשובה

מהי פונקציית ה-Detect?

- ניטור רשת ושרתי לוגים, ניהול אירועים, SIEM, איתור חריגות התנהגותיות, ואנומליות.
- שיתוף מידע בין המערכות.
- זיהוי מהיר מצמצם נזק, מאפשר תגובה יעילה, מונע פגיעה גדולה יותר (נזק כספי, תדמיתי).
- עמידה בתקני ציות הדורשים יכולת ניתוח ודיווח אירועים.
- לדוגמא: מעקב אחר תעבורת רשת לאיתור פעילות חשודה: יציאות או פרוטוקולים לא סטנדרטיים.
- ניתוח לוגים לשרתי Active Directory לגילוי כניסות חשודות או ניסיונות מעבר Lateral Movement...



חלקים מרכזיים של הפונקציה

Anomalies and Events

- הגדרת אנומליות (פעולה החורגת מפרופיל "נורמלי").
- שימוש בשיטות Machine Learning, חתימות, חוקים ועוד.

Security Continuous Monitoring

- מערכות SIEM שאוספות לוגים מכל הסביבה (שרתים, תחנות, פיירוולים, אפליקציות), מקושרות אולי למערכות threat intelligence.
- ניטור התנהגות משתמשים ושירותים לאורך זמן.

Detection Processes

- "תהליכי גילוי" רשמיים: מי מקבל התראות, איך מסווגים אירוע, מהי שרשרת הדיווח לצוותי ה-IR.
- בדיקת False Positives ו-False Negatives.
- איזון בין רגישות המערכות (להימנע מהצפת התראות שגויות) לבין סיכון לפספס אירוע של ממש.
- עדכון החוקים והתהליך באופן שוטף כדי להתאים לתרחישי מתקפה חדשים.



חלקים מרכזיים של הפונקציה

הקמת SOC (Security Operations Center)

- תפקידי ה-SOC: ניטור לוגים, אירועים, אירכוב מידע, הפצת התראות לצוותים רלוונטיים.
- גיוס אנשי אבטחת מידע עם יכולות ניתוח ותגובה מהירה.

שילוב עם Identify ו-Governance

- מדיניות Govern מגדירה את נהלי הניטור, הציות הרגולטורי, דרישות הדיווח.
- מיפוי נכסים Identify אומר ל-SOC על מה חשוב במיוחד לנטר (למשל שרתים קריטיים עם מידע רגיש).

בחירת כלי ניטור

- SIEM Splunk, QRadar, ArcSight וכד' לאיסוף מידע מרכזי.
- EDR (Endpoint Detection & Response) לתחנות הקצה.
- UEBA (User and Entity Behavior Analytics) לזיהוי שינויים התנהגותיים.

Best Practices

- הפרדת רשת Network Segmentation כדי לזהות תנועות חשודות בין סגמנטים.
- ניתוח לוגים מרכזי, עם שמירת נתונים ארוכת טווח לחקירות עתידיות.
- בדיקות תקופתיות לאפקטיביות החוקים.



חלקים מרכזיים של הפונקציה

הקמת SOC (Security Operations Center)

- תפקידי ה-SOC: ניטור לוגים, אירועים, אירכוב מידע, הפצת התראות לצוותים רלוונטיים.
- גיוס אנשי אבטחת מידע עם יכולות ניתוח ותגובה מהירה.

שילוב עם Identify ו-Governance

- מדיניות Govern מגדירה את נהלי הניטור, הציות הרגולטורי, דרישות הדיווח.
- מיפוי נכסים Identify אומר ל-SOC על מה חשוב במיוחד לנטר (למשל שרתים קריטיים עם מידע רגיש).

בחירת כלי ניטור

- SIEM Splunk, QRadar, ArcSight וכד' לאיסוף מידע מרכזי.
- EDR (Endpoint Detection & Response) לתחנות הקצה.
- UEBA (User and Entity Behavior Analytics) לזיהוי שינויים התנהגותיים.

Best Practices

- הפרדת רשת Network Segmentation כדי לזהות תנועות חשודות בין סגמנטים.
- ניתוח לוגים מרכזי, עם שמירת נתונים ארוכת טווח לחקירות עתידיות.
- בדיקות תקופתיות לאפקטיביות החוקים.



הקשרים בין הפונקציות

Govern → Detect

פונקציית Govern (משילות): קובעת את המדיניות הארגונית, הדרישות הרגולטוריות, התקנים המחייבים (סטנדרטים), והאחריות לניהול סיכונים סייבר.

Govern מגדירה אילו תהליכי ניטור ואיסוף לוגים הארגון נדרש להפעיל (אילו מערכות לנטר, באיזו תדירות, מי אחראי על הפעולה).

Govern מבטיחה שתהיה הקצאת משאבים (תקציב, כוח אדם) לצוות SOC או כלים טכנולוגיים הנחוצים לזיהוי אירועים.

Govern מסדיר גם את מדיניות הדיווח על אירועים חריגים – למשל, חיוב בדיווח לדירקטוריון או לרגולטור בתוך פרק זמן מוגדר.

Identify → Detect

פונקציית Identify זיהוי נכסים וסיכונים ממפה את הנכסים הקריטיים, מאפיין את האיומים הפוטנציאליים, ומבצע הערכת סיכונים.

כדי לדעת מה לנטר ואת מי להתריע, על Detect להסתמך על המידע ש-Identify סיפק: אילו מערכות הן הקריטיות ביותר, היכן הנכסים הרגישים, ואילו איומים או וקטורים מוגדרים כבעלי סבירות/השפעה גבוהה.

משתמשים במפות סיכונים מ-Identify כדי לעצב Use Cases ספציפיים ב-SIEM למשל: "ניטור כניסות חשודות לשרתים בעלי מידע רגיש".



הקשרים בין הפונקציות

Protect ↔ Detect

פונקציית Protect (הגנה): נועדה למנוע או לצמצם את הסיכוי להצלחה של מתקפת סייבר, באמצעות בקורות טכניות (הצפנה, בקרת גישה) ונהלים ארגוניים (מדיניות סיסמאות, הדרכות עובדים וכו').

חלוקת גבולות ואחריות: Protect משמשת כחומת ההגנה הראשונית, אך כאשר מתרחש אירוע בכל זאת, Detect אמור לאתר אותו מיד.

ניטור בקורות הגנה: מערכות הגנה עצמן מפיקות לוגים (למשל, Firewalls, מערכות EDR, Detect לעבד לוגים אלה ולהתריע על תופעות חריגות.

התאמה לאסטרטגיית ההגנה: אם ידוע שארגון מיישם רשתות מופרדות (Network Segmentation כחלק מ- Protect, פונקציית Detect תוודא ניטור יציאות או מעברים חריגים בין הסגמנטים.



הקשרים בין הפונקציות

Detect ↔ Respond

פונקציית Respond (תגובה): מטפלת ביישום תהליכי תגובה יעילים ברגע שמתגלה אירוע סייבר: איתור מקור ההתקפה, בידוד נזקים, הסלמה להנהלה או לרשויות (במידת הצורך), ונקיטת פעולות מיידיות (כיבוי שרת נגוע, שינוי סיסמאות, וכד').

הפעלת התגובה: Detect מספק את האיתות הראשוני לצוותי התגובה – ברגע שמתגלים סימנים של פעילות חשודה, Respond נכנס לפעולה.

שיפור הדיוק: איכות ודיוק ההתראות מ-Detect משפיעה ישירות על זמן וכיוון התגובה. אם יש הצפה של התראות שווא (False Positives), או חוסר התראות (False Negatives), Respond יתמודד עם קושי בזיהוי או **בטריאז'**.

בקרה וסגירת מעגל: לעיתים, כשיוצאים לפעולת תגובה, נדרשות יכולות ניטור נוספות (Detect כדי לוודא היכן התוקף נמצא והאם הפעילות הזדונית עדיין נמשכת).



הקשרים בין הפונקציות

Detect ↔ Recover

פונקציית Recover (התאוששות): מתמקדת בשיקום שירותים, מערכות ותהליכי עבודה, אחרי מתקפה מוצלחת שהייתה לה השפעה על הארגון.

חקר האירוע: לאחר מתקפה, נדרשת חקירה דיגיטלית Forensics המבוססת על נתוני הלוגים וההתראות שאוספים בשלב Detect.

מניעת מתקפות חוזרות: מידע על נקודות הכניסה וההתפשטות של התוקף שמתגלה בשלב הזהוי Detect מסייע לשפר את תוכניות Recover ולעיתים גם Protect, כדי למנוע הישנות של אותו תרחיש או לשפר זמני שחזור.

הפקת לקחים ובניית חוסן: דו"ח הסיכום אחרי אירוע Post-Incident Review מעריך את תפקוד Detect. האם היה מהר מספיק? האם המערכות היו מתוחזקות היטב? והמלצות לשיפורים עתידיים בתהליכי זיהוי והתאוששות גם יחד.



הקשרים בין הפונקציות

Detect ↔ Recover

פונקציית Recover (התאוששות): מתמקדת בשיקום שירותים, מערכות ותהליכי עבודה, אחרי מתקפה מוצלחת שהייתה לה השפעה על הארגון.

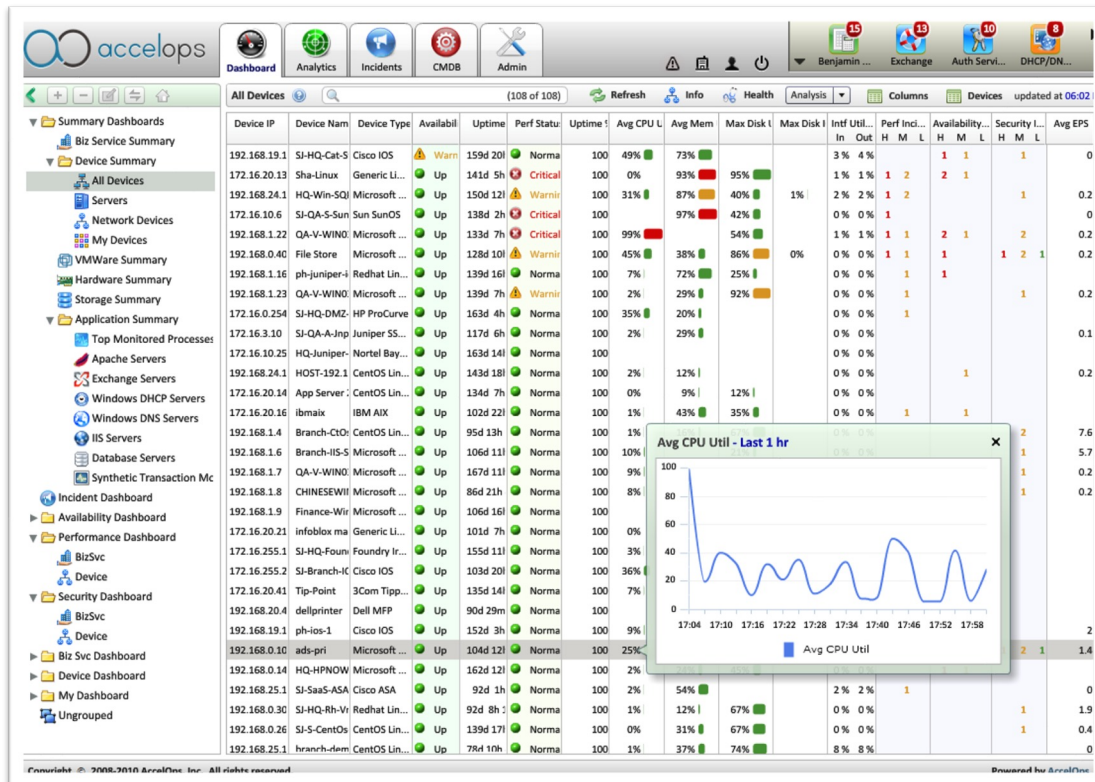
חקר האירוע: לאחר מתקפה, נדרשת חקירה דיגיטלית Forensics המבוססת על נתוני הלוגים וההתראות שאוספים בשלב Detect.

מניעת מתקפות חוזרות: מידע על נקודות הכניסה וההתפשטות של התוקף שמתגלה בשלב הזהוי Detect מסייע לשפר את תוכניות Recover ולעיתים גם Protect, כדי למנוע הישנות של אותו תרחיש או לשפר זמני שחזור.

הפקת לקחים ובניית חוסן: דו"ח הסיכום אחרי אירוע Post-Incident Review מעריך את תפקוד Detect. האם היה מהר מספיק? האם המערכות היו מתוחזקות היטב? והמלצות לשיפורים עתידיים בתהליכי זיהוי והתאוששות גם יחד.



יישום מעשי של פונקציית ה-Detect



1. הגדרת צרכים ומדיניות
2. הקמת תשתית איסוף לוגים
3. פיתוח כללי גילוי
4. הקמת צוות ניטור
5. תפעול שוטף ובקרה
6. מדידה ושיפור

Quizuzz!



<https://quizizz.com/join?gc=14419152>

Joinmyquiz.com

Join code: 723802



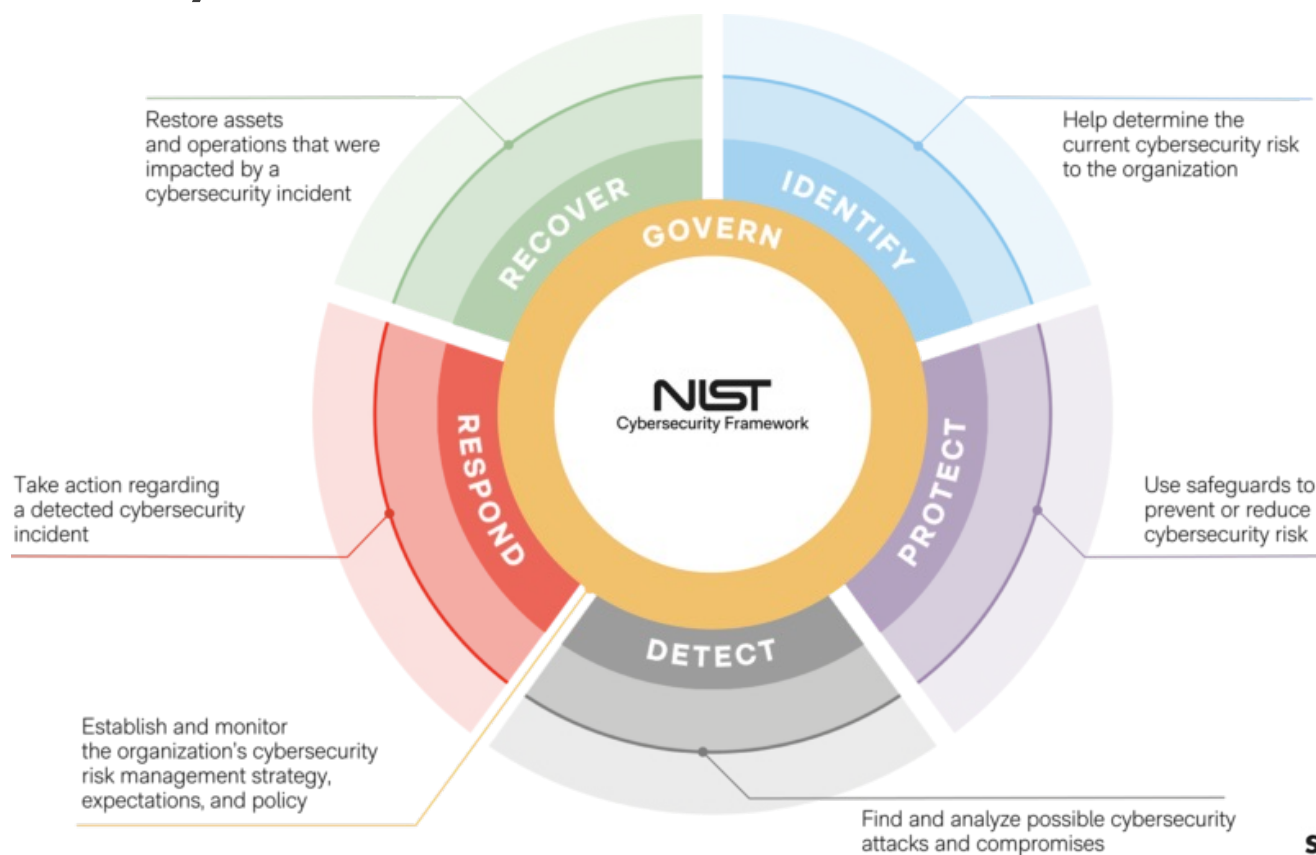
שיעור 11

פונקציות Respond & Recover: להגיב ולהכיל תקריות סייבר ולשחזר ולחזור לפעילות רגילה.

- 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 של פונקציות תגובה ושחזור/חזרה לפעילות.
- הבנת החיבור בין פונקציית התגובה והשחזור לשאר הפונקציות במסגרת.

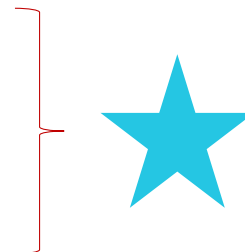


NIST Cybersecurity Framework (2.0)



NIST Cybersecurity Framework (2.0): Protect

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



הגדרה רחבה של פונקציית Respond ומדוע היא חשובה

מהי פונקציית Respond?

- פונקציה זו עוסקת בכל פעולות התגובה בעת זיהוי אירוע סייבר, החל מאיסוף המידע הראשוני ועד להקטנת הנזקים והחזרת השליטה לידיים הארגון.
- כוללת נהלי תגובה לאירועים (Incident Response Plan), מדיניות הסלמה ודיווח, הקצאת משאבים ועוד.

למה זה חשוב?

- גם אם בקורות ה- Protect חזקות, הארגון צריך תהליך מובנה לטיפול באירוע כשזה מתרחש בפועל.
- תגובה יעילה מפחיתה את הנזק, מקצרת את זמן השבתת המערכות, ומאפשרת ניהול שקול מול לקוחות, ספקים ורשויות.



חלקים מרכזיים של הפונקציה

- תכנון תגובה מוקדם (יצירת תכנית IR).
- תקשורת בעת האירוע: פנימית, חיצונית, עם בעלי עניין וכו'.
- ניתוח האירוע ומהלכים ראשוניים.
- הכלה וצמצום נזקים.
- סילוק הגורם המאיים, זיכוי המכשירים/חדרים/אנשים/חשבונות/...
- התחלת סגירת הפערים למניעה עתידית.
- *תרגילי סימולציה חשובים מאד במקרה הזה: War Games, Table Tops, etc.



הגדרה רחבה של פונקציית Recover ומדוע היא חשובה

מהי פונקציית Recover?

- פונקציה זו מתמקדת בשיקום מערכות הארגון, חידוש שירותים עסקיים, והחזרה מהירה לפעילות לאחר מתקפה או אירוע סייבר.
- כוללת תהליכי גיבוי ושחזור, (DRP (Disaster Recovery Plan, תוכנית המשכיות עסקית (BCP) ותיעוד הפקת לקחים.

חשיבות Recover

- גם אם ההגנה והתגובה בוצעו כראוי, עלול להיגרם נזק זמני. השבת מערכות במהירות מסייעת לצמצם הפסדים כספיים ונזק למוניטין.
- מכינה את הארגון טוב יותר למתקפה עתידית.
- **המטרה החשובה ביותר: Business Continuity**



חלקים מרכזיים של הפונקציה

- תכנון ההתאוששות והגדרת סדר עדיפויות.
- החזרת השירותים.
- שיפור.
- תקשורת עם בעלי עניין.
- דגש על-BC!



הקשרים בין הפונקציות

Govern → Respond and Recover

מגדיר את המדיניות, הנהלים והאחריות בנוגע לתגובה והתאוששות. מוודא שיש תקציבים וציות לרגולציה.

Identify → Respond and Recover

מכתיב אילו מערכות מוגדרות כקריטיות וזקוקות לשחזור מהיר או לתגובה מיוחדת.



הקשרים בין הפונקציות

Protect → Respond and Recover

מפחית את הסיכוי לאירוע חמור; אולם אם האירוע בכל זאת מתרחש, Respond ו-Recover נכנסים לפעולה.

Detect → Respond and Recover

משגר את ההתרעה ל-Respond ומזהה את היקף הפגיעה והמערכות הלכודות כדי לעזור בתכנון ההתאוששות (Recover).



הקשרים בין הפונקציות

Recover → Respond

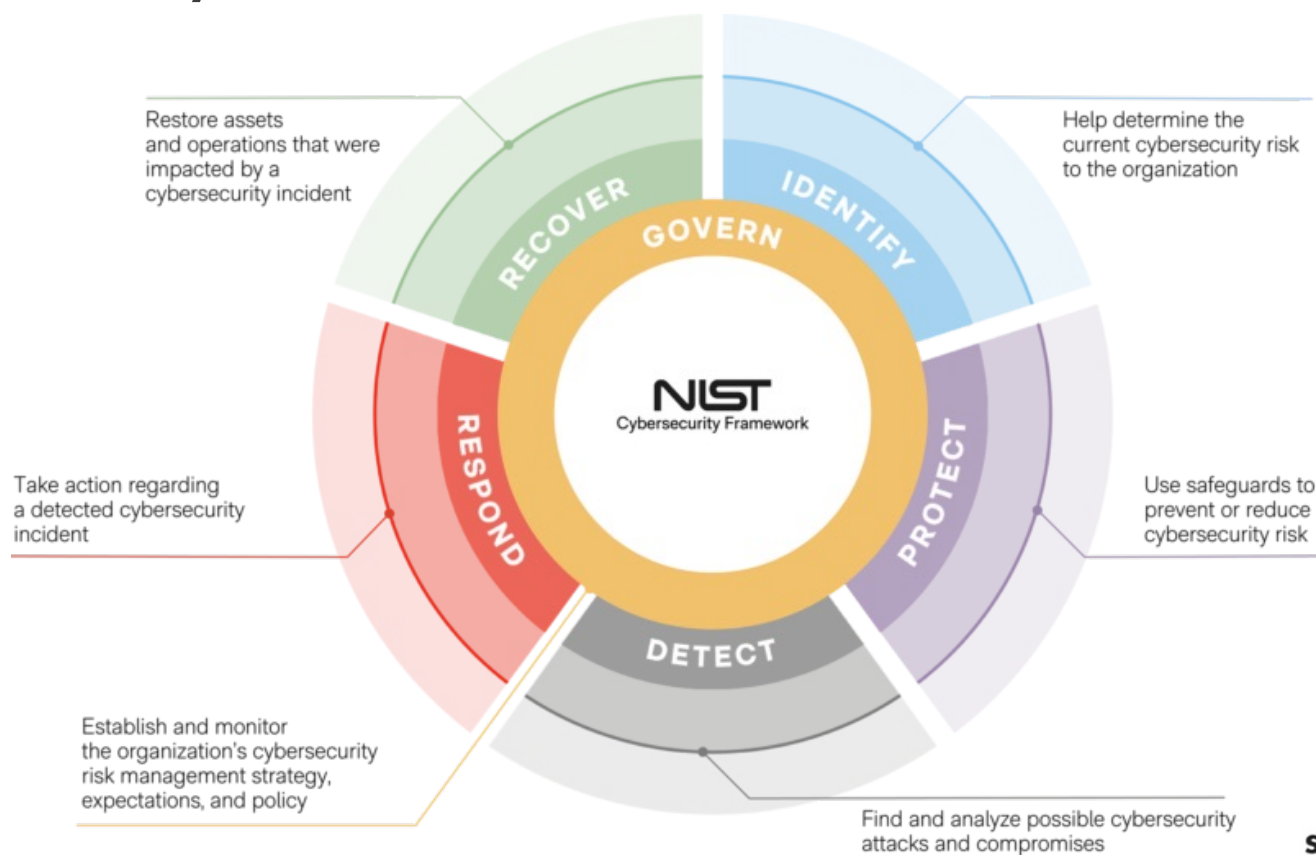
פונקציית Respond מטפלת באופן מיידי באירוע כדי לצמצם נזקים ולהחזיר שליטה, בעוד פונקציית Recover משקמת ומשיבה את המערכות והפעילות העסקית לשגרה, וכך הן משלימות זו את זו לאורך רצף ההתמודדות עם מתקפת סייבר.



ולסיכום...



NIST Cybersecurity Framework (2.0)





שיעור 12

מדיניות בינה מלאכותית בארגונים ומסגרת ה-NIST AI RMF 1.0