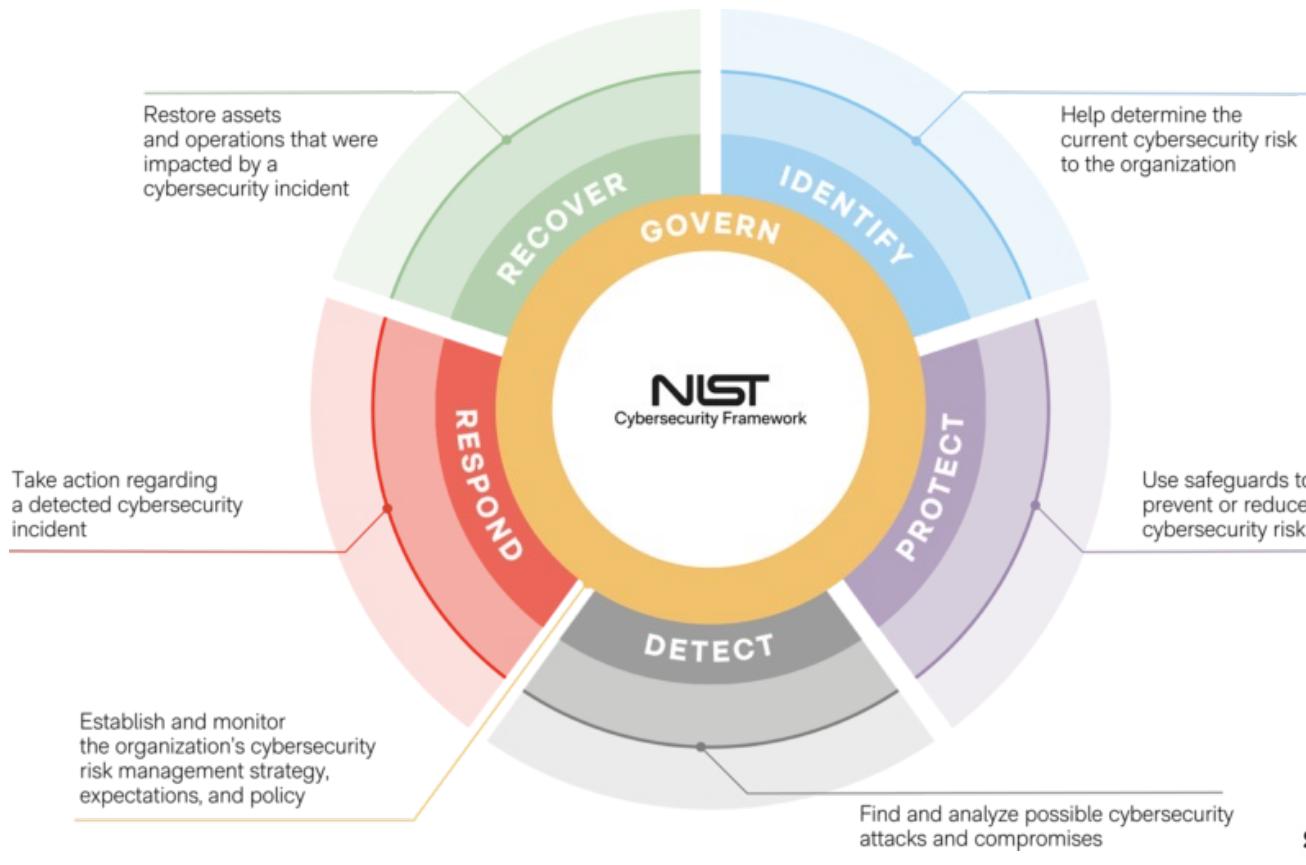


## מטרת השיעור

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



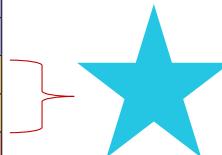
# NIST Cybersecurity Framework (2.0)



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# NIST Cybersecurity Framework (2.0): Protect

Function	Category	Category Identifier
<b>Govern (GV)</b>	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
<b>Identify (ID)</b>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<b>Protect (PR)</b>	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
<b>Detect (DE)</b>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<b>Respond (RS)</b>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<b>Recover (RC)</b>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



# הגדלה רחבה של פונקציית Protect ומדוע היא חשובה

## מהי פונקציית ה-Detect?

- ניטור רשת ושרותי לוגים, ניהול אירועים, SIEM, איתור חריגות התנהלותיות, anomalיות.
- שיטוף מידע בין המרכיבים.
- זיהוי מהיר מצמצם נזק, מאפשר תגובה יעילה, מונע פגיעה גדולה יותר (נזק כספי, תדמית).
- עמידה בתקני ציון הדורשים יכולת ניתוח ודיווח אירועים.
- לדוגמה: מעקב אחר תעבורת רשת לאיתור פעילות חשודה: יציאות או פרוטוקולים לא סטנדרטיים.  
... ניתוח לוגים לשרת Active Directory לגילוי כניסה חדשה או ניסיונות מעבר Lateral Movement



# חלקים מרכזיים של הפונקציה

## Anomalies and Events

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

## Security Continuous Monitoring

- מערכות SIEM שאווסףות לוגים מכל הסביבה (שרותים, תחנות, פירוקלים, אפליקציות), הקשורות אולי למערכות threat intelligence.
- nitore התנהגות משתמשים ושירותים לאורך זמן.



## Detection Processes

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

# חלקים מרכזיים של הפונקציה

## הקמת (Security Operations Center)

- תפקידו של SOC: סוליטור לוגים, אירועים, אירועים, אירוכוב מידע, הפעלת התראות לצוותים רלוונטיים.
- גיוס אנשי אבטחה מידע עם יכולות ניתוח ותגובה מהירה.

## שילוב עם Identify ו-Governance

- מדיניות Govern מגדרת את נחלי הניטור, ה策ות הרגולטורי, דרישות הדיווח.
- מיפוי נכסים Identify אומר ל-SOC על מה חשוב במיוחד לנטר (למשל שירותים קריטיים עם מידע רגיש).

## בחירה כלית ניטור

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

## Best Practices

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



# חלקים מרכזיים של הפונקציה

## הקמת (Security Operations Center)

- תפקידו של SOC: אבטחת לוגים, אירועים, אירוחים, מידע, הפעלת התראות לצוותים רלוונטיים.
- גיוס אנשי אבטחה מייד עם יכולות ניתוח ותגובה מהירה.

## שילוב עם Identify ו-Governance

- מדיניות Govern מגדרת את נחי הנויטור, ה策ות הרגולטורי, דרישות הדיווח.
- מיפוי נכסים Identify אומר ל-SOC על מה חשוב במיוחד לנטר (למשל שירותים קריטיים עם מידע רגיש).

## בחירה כל-INITOR

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

## Best Practices

- הפרדת רשת Network Segmentation כדי לזרז תנועות חשודות בין סגמנטים.
- ניתוח לוגים מרכזי, עם שבירת נתוני ארכיטקטורה לחקירות עתידיות.
- בדיקות תקופתיות לאפקטיביות החוקים.



# הקשרים בין הפונקציות

## Govern → Detect

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

Govern מגדירה אילו תהליכי ניטור ואייסוף לוגים הארגון נדרש להפעיל (אילו מערכות לנטר, באיזו תדירות, מי אחראי על הפעולה). Govern מבטיחה שתיהה הקצתת משאבים (תקציב, כוח אדם) לצוות SOC או כלים טכנולוגיים הנחוצים לכך איירועים. Govern מסדיר גם את מדיניות הדיווח על איירועים חריגים – למשל, חיוב בדיווח לדירקטוריון או לרגולטור בתוך פרק זמן מוגדר.

## Identify → Detect

פונקציית Identify נכסים וסיכון ממפה את הנכסים הקritisטיים, מאפיין את האיים הפוטנציאליים, וביצע הערכת סיכונים. כדי לדעת מה לנטר ואת מי להתריע, על Detect להסתמך על המידע ש-Identify סיפק: אילו מערכות הן הקritisיות ביותר, היקן הנכסים הרגישים, ואילו איים או קטורים מוגדרים כבעלי סבירות/השפעה גבוהה.



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

## הקשרים בין הפונקציות

### Protect → Detect

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

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

ניתור בקרות הגנה: מערכות הגנה עצמן מפיקות לוגים (למשל, Firewalls, EDR) וען Detect לעבודelogים אלה ולהתריע על תופעות חריגות.

התאמה לאסטרטגיית ההגנה: אם ידוע שארגון מיישם רשתות מופרדות (Network Segmentation) מ- Protect, Detect תזודא ניתור יציאות או מעברים חריגים בין הסגמנטים.



## הקשרים בין הפלוקציות

Detect  Respond

פלוקציית Respond (תגובה): מטפלת בישום תהליכי תגובה יעילים ברגע שמתגללה אירוע סיבר: איתור מקור ההתקפה, בידוד נזקים, הסלמה להנהלה או לרשויות (במידת הצורך), ונקיטת פעולות מיידיות (כיבוי שירות נגוע, שינוי סיסמאות, ועוד').

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

SHIPOR הדיק: אינטודיק התראות מ-Detect משפיעה ישירות על זמן וכיון התגובה. אם יש הצפה של התראות שווה (False Negatives), Respond או חוסר התראות (Positives), יתמודד עם קושי בזיהוי או בטריאז'.



## הקשרים בין הפלוקציות

Detect → Recover

פלוקציית Recover (התואשות): מתמקדת בשיקום שירותי, מערכות ותהליכי העבודה, אחרי מתקפה מוצלחת שהייתה לה השפעה על הארגון.

חקר האירוע: לאחר מתקפה, נדרש חקירה דיגיטלית Forensics המבוססת על נתוני הלוגים והתראות שאספבים בשלב Detect.

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

הפקת לkusים ובנית חסן: ד"ר הסיכון אחראי אירוע Post-Incident Review מעריך את תפקוד Detect. האם היה מהר מספיק? האם המערכת היו מתחזקות היטב? ומהלצות לשיפורים עתידיים בתהליכי זיהוי והתואשות גם יחד.



## הקשרים בין הפלוקציות

Detect → Recover

פלוקציית Recover (התואשות): מתמקדת בשיקום שירותי, מערכות ותהליכי עבודה, אחרי מתקפה מוצלחת שהייתה לה השפעה על הארגון.

חקר האירוע: לאחר מתקפה, נדרש חקירה דיגיטלית Forensics המבוססת על נתוני הלוגים והתראות שאספין Detect.

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

הפקת לkills ובניית חיסון: ד"ר הסיכון אחראי אירוע Post-Incident Review מעריך את תפקוד Detect. האם היה מהר מספיק? האם המערכת היו מתחזקות היטב? ומהלצות לשיפורים עתידיים בתהליכי זיהוי והתואשות גם יחד.



# יישום מעשי של פונקציית ה-Detect

The screenshot shows a detailed monitoring interface for network devices. The main area is a table listing 108 devices, each with a status icon (green, yellow, red) and performance metrics. A modal window provides a closer look at the CPU utilization of one specific device over the last hour. The left sidebar contains a tree view of monitoring categories and dashboards.

1. הגדרת צרכים ו מדיניות

2. הקמת תשתיות 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

## סיכום ושאלות



# שיעור 11

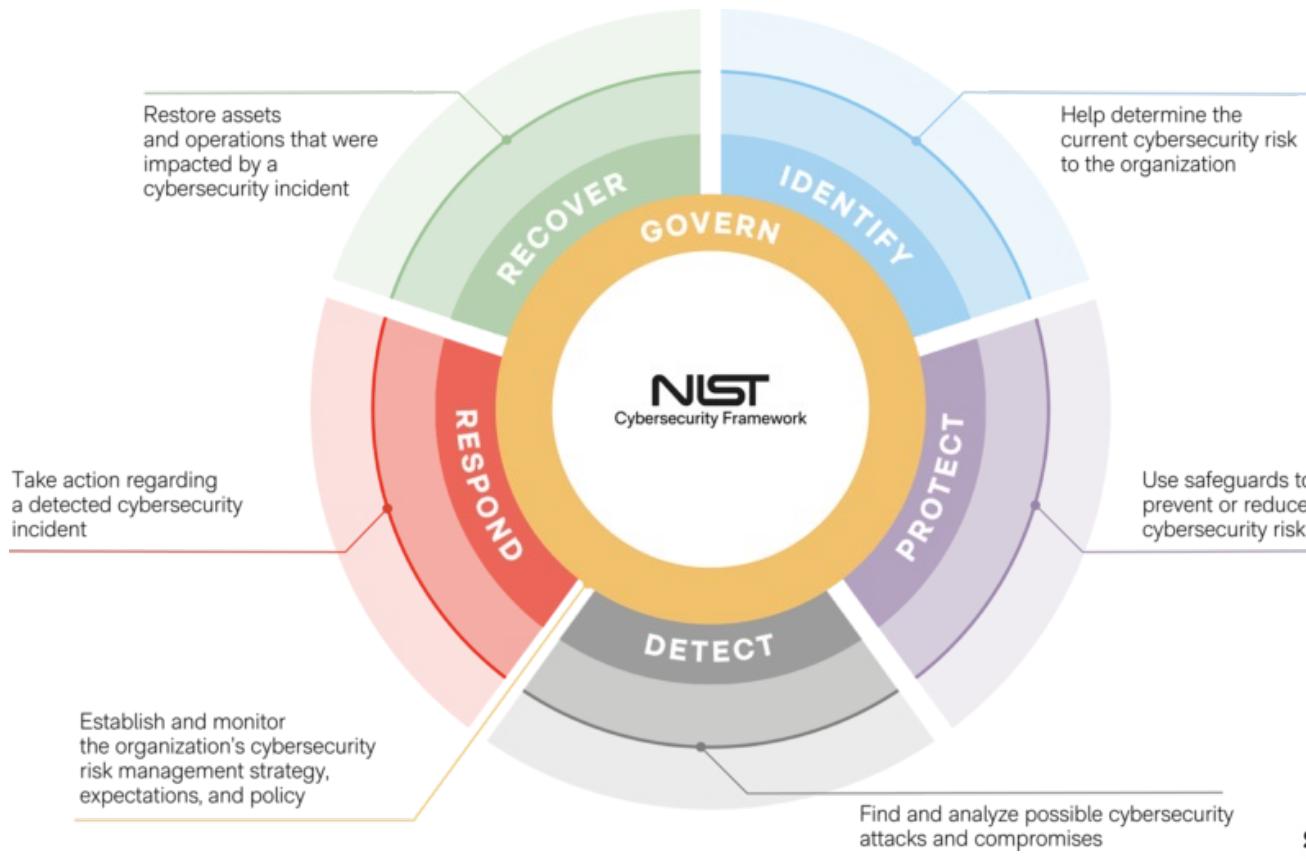
פונקציות Respond & Recover: להגיב ולהכיל תקריות סייבר ולשזר ולחזור לפעולות רגילה.

## 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 מעמיקה של פונקציות תגובה ו恢復/חזרה לפעולות.
- הבנת החיבור בין פונקציית התגובה וה恢復 לשאר הפונקציות במסגרת.

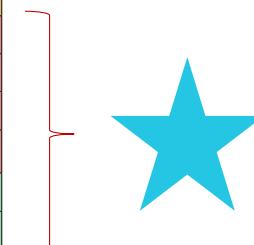


# NIST Cybersecurity Framework (2.0)



# NIST Cybersecurity Framework (2.0): Protect

Function	Category	Category Identifier
<b>Govern (GV)</b>	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
<b>Identify (ID)</b>	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
<b>Protect (PR)</b>	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
<b>Detect (DE)</b>	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
<b>Respond (RS)</b>	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
<b>Recover (RC)</b>	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



# הגדלה רחבה של פונקציית Respond ומדוע היא חשובה

## מהי פונקציית Respond?

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

## למה זה חשוב?

- גם אם בקרות ה- Protect חזקות, הארגון צריך תהיליך מבנה לטיפול באירוע כזה מתמשך בפועל.
- תגובה יעילה מפחיתה את הנזק, מקצרת את זמן השבתת המרכזות, ומאפשרת ניהול שקל מול לכוחות, ספקים ורשויות.



## חלקים מרכזיים של הפלנקציה

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



# הגדלה רחבה של פונקציית Recover ומדוע היא חשובה

## מהי פונקציית Recover?

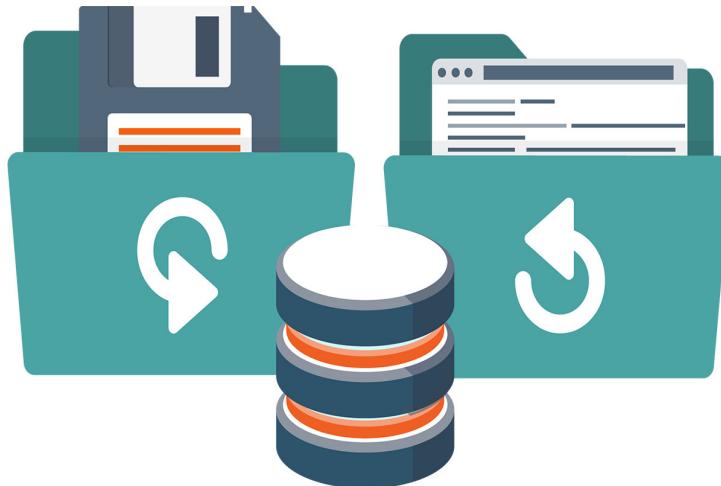
- פונקציה זו מתמקדת בשיקום מערכות הארגון, חידוש שירותי עסקים, והחזרה מהירה לפעולות לאחר מתקפה או אירוע סייבר.
- כוללת תהליכי גיבוי ו恢復, (DRP (Disaster Recovery Plan) תוכנית המשכיות עסקית (BCP ותיעוד הפקת לקוחות).

## חשיבות Recover



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

## חלקים מרכזיים של הפונקציה



- תכנון התאוששות והגדרת סדר עדיפויות
- החזרת השירותים.
- שיפור.
- תקשורת עם בעלי עניין.
- דגש על-BCI.

## הקשרים בין הפקציות

**Govern → Respond and Recover**

מגדיר את המדיניות, הנהלים והאחריות בנוגע לתגובה והתאוששות. מודא שיש תקציבים ווצאות לרגולציה.

**Identify → Respond and Recover**

מכטיב אילו מערכות מוגדרות כקריטיות וזקוקות לשחזר מהיר או לתגובה מיוחדת.



## הקשרים בין הפקציות

**Protect → Respond and Recover**

mphiat את הסיכון לאירוע חמוץ; אולם אם האירוע בכל זאת מתרחש, Respond ו-Recover נכנסים לפעולה.

**Detect → Respond and Recover**

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



## הקשרים בין הפונקציות

### Recover → Respond

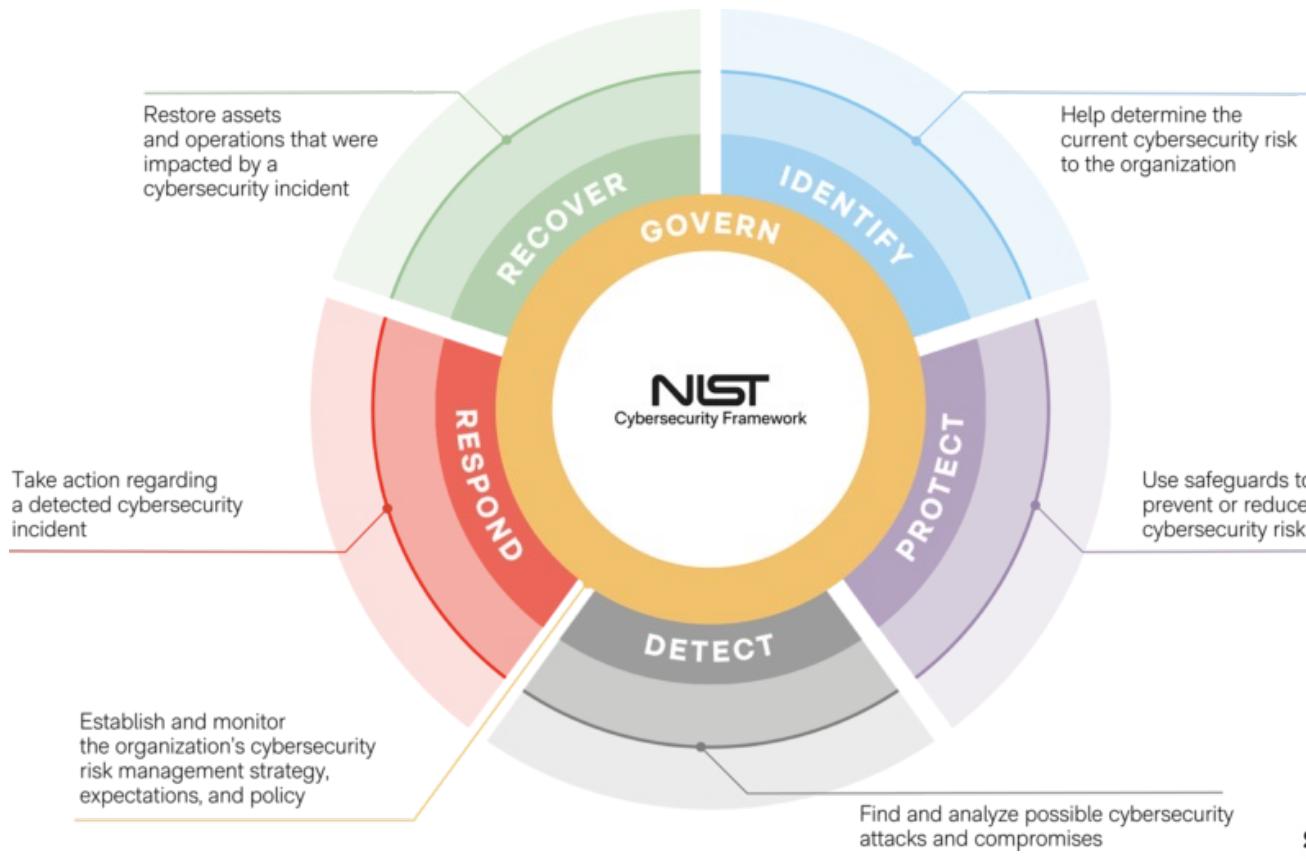
פונקציית Respond מטפלת באופן מיידי באירוע כדי לצמצם נזקים ולהחזיר שליטה, בעוד פונקציית Recover משקמת ומשיבה את הממערכות והפעולות העסקית לשגרה, וכך הן משלימות זו את זו לאורך רצף ההתמודדות עם מתקפת סייבר.



# ולסינכים...



# NIST Cybersecurity Framework (2.0)



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

## סיכום ושאלות



# שיעור 12

מדיניות בינה מלאכותית בארגונים ובסגרת ה-NIST AI RMF 1.0