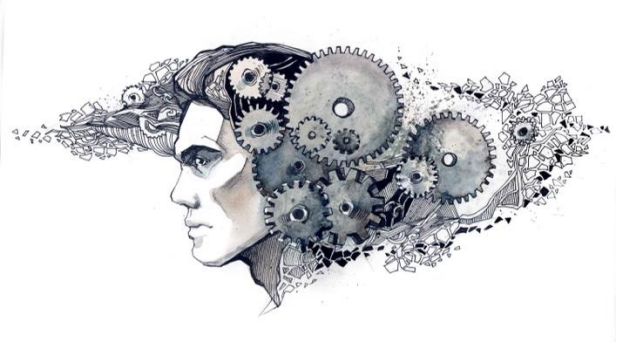
שיעור 9

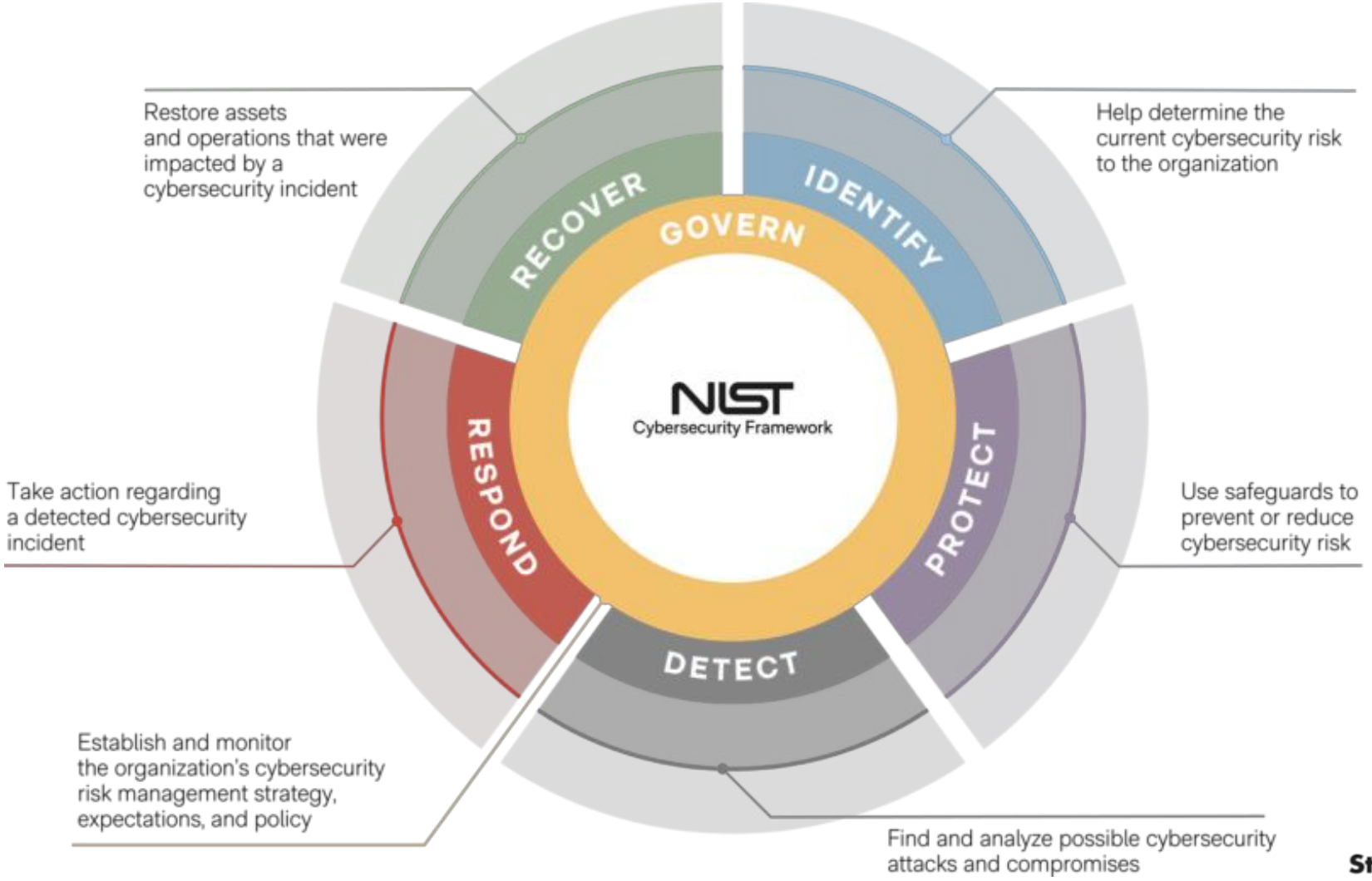
פונקציית Protect: בקרות והגנות.

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 בקרות והגנות (גנרי).**
- **הבנת החיבור בין פונקציית ההגנה 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
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

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

הגדרה רחבה של פונקציית Protect ומדוע היא חשובה

מהי פונקציית ה-Protect?

Protect מתמקדת ביישום בקרות והגנות שמצמצמות את הסיכונים שזוהו בשלב ה-Identify.

דוגמאות: בקרות גישה, ניהול זהויות, הצפנה, הדרכות עובדים, מערכות הגנה היקפיות.

Firewalls, IDS, IPS, EPP/EDR/XDR, etc., SOC, SIEM, SOAR...

WAF, CASB, NAC...

הגדרה רחבה של פונקציית Protect ומדוע היא חשובה

הפונקציה מכילה מספר קטגוריות (ראו טבלה בשקפים קודמים):

Identity Management, Authentication, and Access Control

- ניהול זהויות והרשאות גישה, הגדרת משתמשים, תפקידי גישה, אימות רב-גורמי.
- ניהול סיסמאות ומדיניות נעילה.
- בקרת גישה על סמך תפקיד, זמן, מיקום או הקשר.

Awareness and Training

- הדרכת משתמשים ועובדים לגבי אבטחת מידע, הנחיות לטיפול במידע רגיש, נהלי דיווח.
- יצירת תרבות אבטחת מידע כך שכל עובד יכיר את החובות והאחריויות שלו, כולל מבחני מודעות תקופתיים.

הגדרה רחבה של פונקציית Protect ומדוע היא חשובה

Data Security

- הצפנת מידע במנוחה ובמעבר.
- הגנה על מידע רגיש באמצעות DLP (Data Loss Prevention).
- גיבויים מאובטחים ומדיניות השמדה/גריסה של מידע שלא בשימוש.

Information Protection Processes and Procedures

- נהלי הקשחת שרתים ותחנות קצה, כללי פאטצ'ינג (עדכונים שוטפים).
- מדיניות הפעלה בטוחה, סטנדרטים לאבטחת תוכנה וסביבות ענן.
- תהליכי בדיקה תקופתיים לתקינות בקרות האבטחה.

הגדרה רחבה של פונקציית Protect ומדוע היא חשובה

Maintenance

תחזוקה שוטפת של מערכות הקריטיות לאבטחה (לדוגמה, Antivirus, מערכות גילוי פריצות).

ביצוע עדכוני תוכנה ((Patchingבאופן מתוזמן.

ניטור פעולות צד שלישי המבצע תחזוקה, והבטחת הגנת מערכות בזמן תחזוקה (Lockdown Mode).

Protective Technology

- שימוש בכלים טכנולוגיים כגון Firewalls, SIEM, IPS/IDS בצד ה- Detect אך גם הגנה היקפית וצד ג׳ (WAF, CASB, NAC). כמובן EPP, EDR, etc. וגם אנטי-וירוסים וכו׳.
- מערכות ניהול פגיעויות, מערכות לבקרה של התקני אחסון ניידים, טכנולוגיות סיווג ותיוג מידע, וכדומה.

הקשר בין Protect לשאר הפונקציות

Govern ↔ Protect

מבטיחה שהפוליסות וההנחיות מיושמות בפועל: מי אחראי להטמעת בקרות, אילו משאבים מוקצים לצורכי הגנה, וכיצד נמדדת אפקטיביות ההגנה.

Identify ↔ Protect

מיישמת בקרות בהתאם לדרגת הסיכון ולאופי הנכס: שרתים רגישים יקבלו שכבות הגנה מתוגברות, גישת מנהלים תהיה מנוטר וכו'

Protect ↔ Detect

לעתים הגבול מטושטש: הגנה עשויה לכלול גם כלי ניטור EDR אך מבחינת NIST, Detect מושם דגש על איתור אירועים וחריגות. Protect מתמקד בהצבת הגנות שמונעות מראש התקפות או מצמצמות נזק.

Protect ↔ Respond & Recover

ככל שמנגנוני ההגנה טובים יותר, כך גובר הסיכוי שתגובת הארגון תהיה מהירה וממוקדת, ושההתאוששות תהיה פשוטה יותר. לדוגמה, הצפנת נתונים וגיבוי אמין מפחיתים את השפעת מתקפות כופר.

יישום מעשי של פונקציית ה-Protect

ניתן ליישם את פונקציית ה-Protect בשלבים הבאים:

1. קביעת סדר עדיפויות הגנה: ע"ב פונקציית הזיהוי.
2. הרכבת צוות הגנה ומערכי הגנה, מרכז תפעול, שליטה ובקרה, מיישמי הגנה וכו'.
3. בחירת כלים וטכנולוגיות (ביחד עם סעיף 2), הצפנות, הגנות קצה וכו' (ראו כל האותיות מהשקופיות הקודמות).
4. נהלי הפעלה, הדרכה והטמעה: הכנת פרוצדורות, מקרים ותגובות, הדרכות עובדים.
5. מעקב ושיפור: מדדי KPIs: כמות מכונות מעודכנות Patch Compliance מספר תקריות הנובעות מהחזקת סיסמאות חלשות, אחוז עובדי שעברו הדרכת Phishing בהצלחה, ירידה במספר תחנות לא מוגנות וכו'.

בשיעור הבא: Detect

ניטור, גילוי הפרות ומתקפות בזמן אמת (או מהר ככל שניתן).

סיכום ושאלות