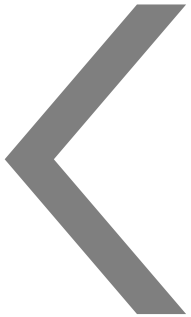
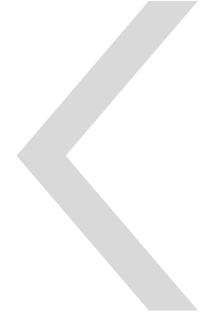


# אתגרי הגנת סייבר לדיגיטל במעבר



IIA ISRAEL 040118



**1. ההשלכות של פעילות במרחב דיגטלי על תפיסת ההגנה הקיימת**

**2. תפיסת ההגנה החדשה ומסגרת ניהול נדרשת**

**3. מתאוריה לפרקטיקה - מוקדי ביקורת רלוונטיים**



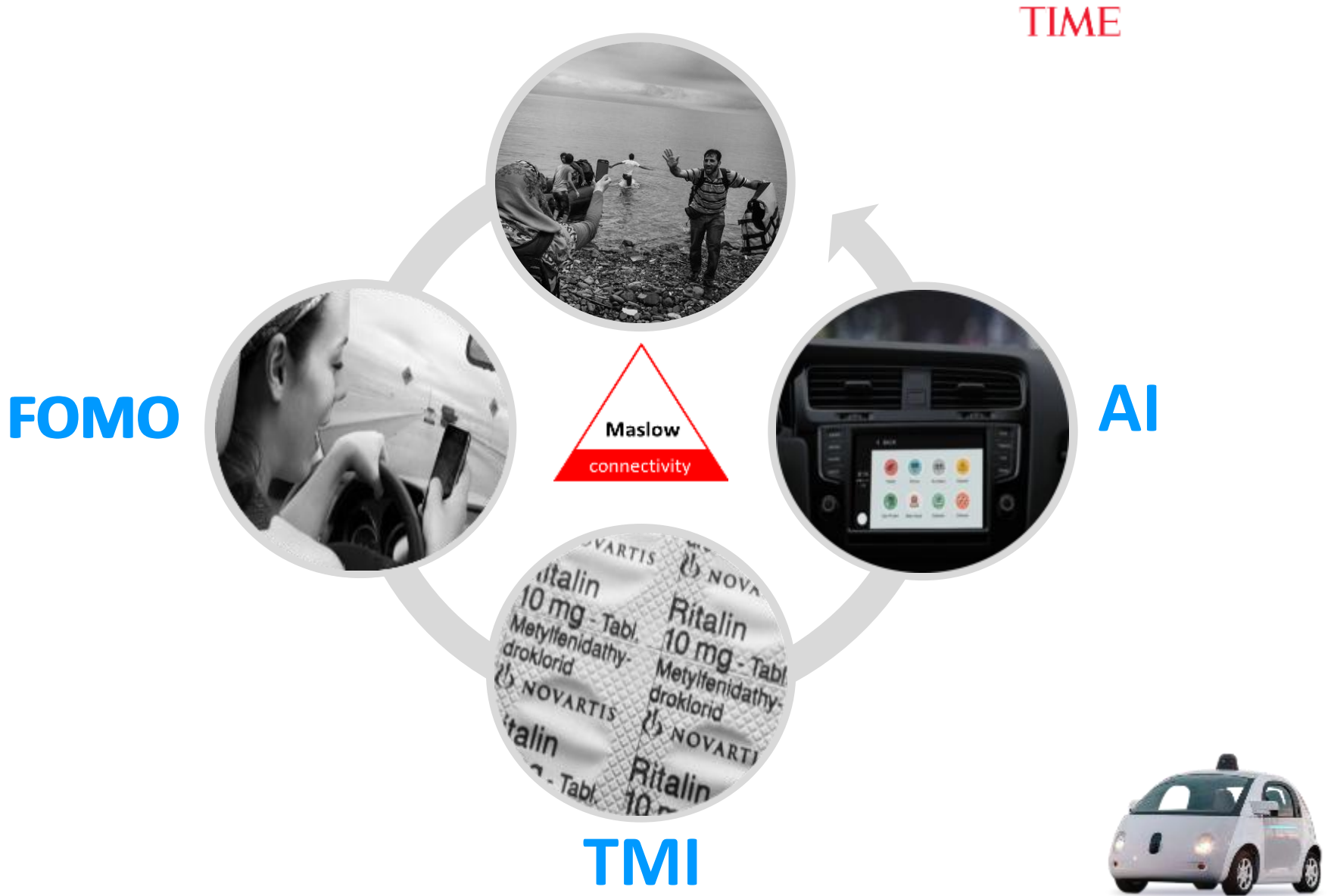
"In the next millennium, we will find that we are talking as much or more with machines than we are with humans"

**Being Digital** by Nicholas Negroponte , 1995

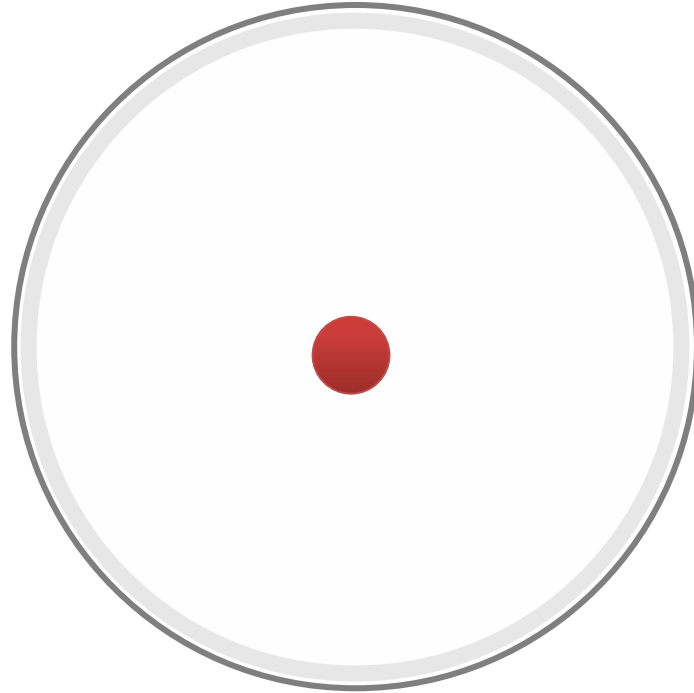


Smartphones Have Become a Lifeline for Syrian Refugees.

Google Maps is putting Europe's human-traffickers out of business

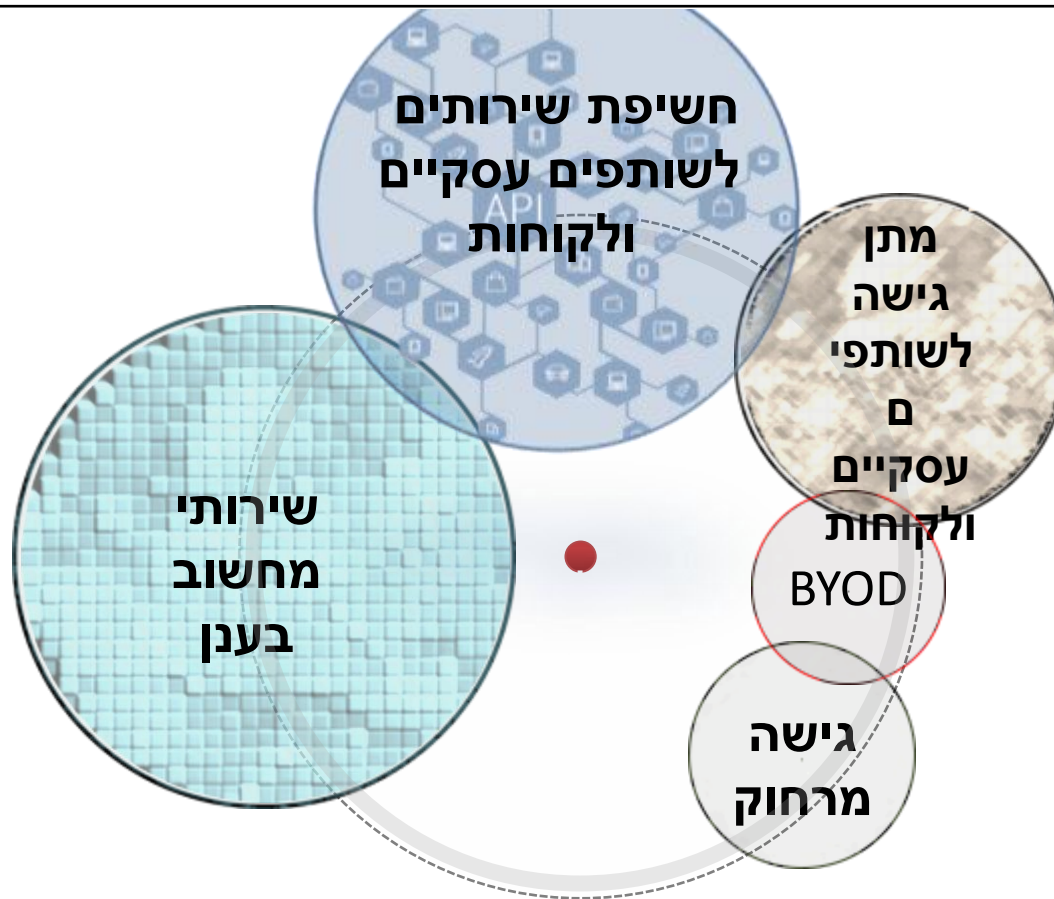






עבר

# אתגרי הגנת סייבר בדיגיטל



הווה



# אתגרי הגנת סייבר בדיגיטל

תפוצה גוברת ונגישות לכלי תקיפה ברמת  
מדינה

▪ זליגה של כלי CIA, NSA

▪ התפתחות תעשייה ענפה של Crime as a Service

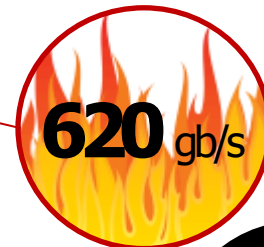


קישוריות מעבר לגבולות הארגון והחלשות אפקטיביות  
הבקרה הפריפריאלית (חומות אש).

▪ מיקרו-שירותים. ביזור ושילוב קוד ואפליקציות ממקורות חיצוניים.

▪ חשיפת מערכות מורשת.

▪ שילוב אמצעי מחשוב אישיים וסנסורים בתהליכי עבודה (BYOD, IOT).



17,000

4%

53%

קושי לתת מענה לאירועי סייבר בשל עודף  
מידע, רעש ברשת והעדר תשתית תומכת.

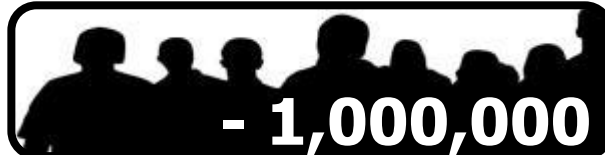
▪ מידע כשירות: מחסני נתונים, מידע ניהולי צורך בתמונת לקוח של  
360°

▪ ריבוי חיוויים מאמצעי אבטחת מידע וכלי שליטה ובקרה. (FireEye)

(2017

▪ קושי בזיהוי נכסי מידע

1 4 7



# אתגרי הגנת סייבר בדיגיטל

## הגנה מעבר לגבולות הארגון

- הפיכת ה-DATA CENTER הארגוני לתשתית מחשוב ענן, רשתות מבוססות תוכנה
- SDN/NFV ויצירת הפרדה והגנה ברמת רכיב בתוך הרשת.
- הסדרה והאחדה של אבטחת תשתיות והתמקדות באבטחת הרובד האפליקטיבי.
- הגנה על המידע ללא תלות בגבולות הארגון (blockchain?).

## הגנה מרגע הלידה

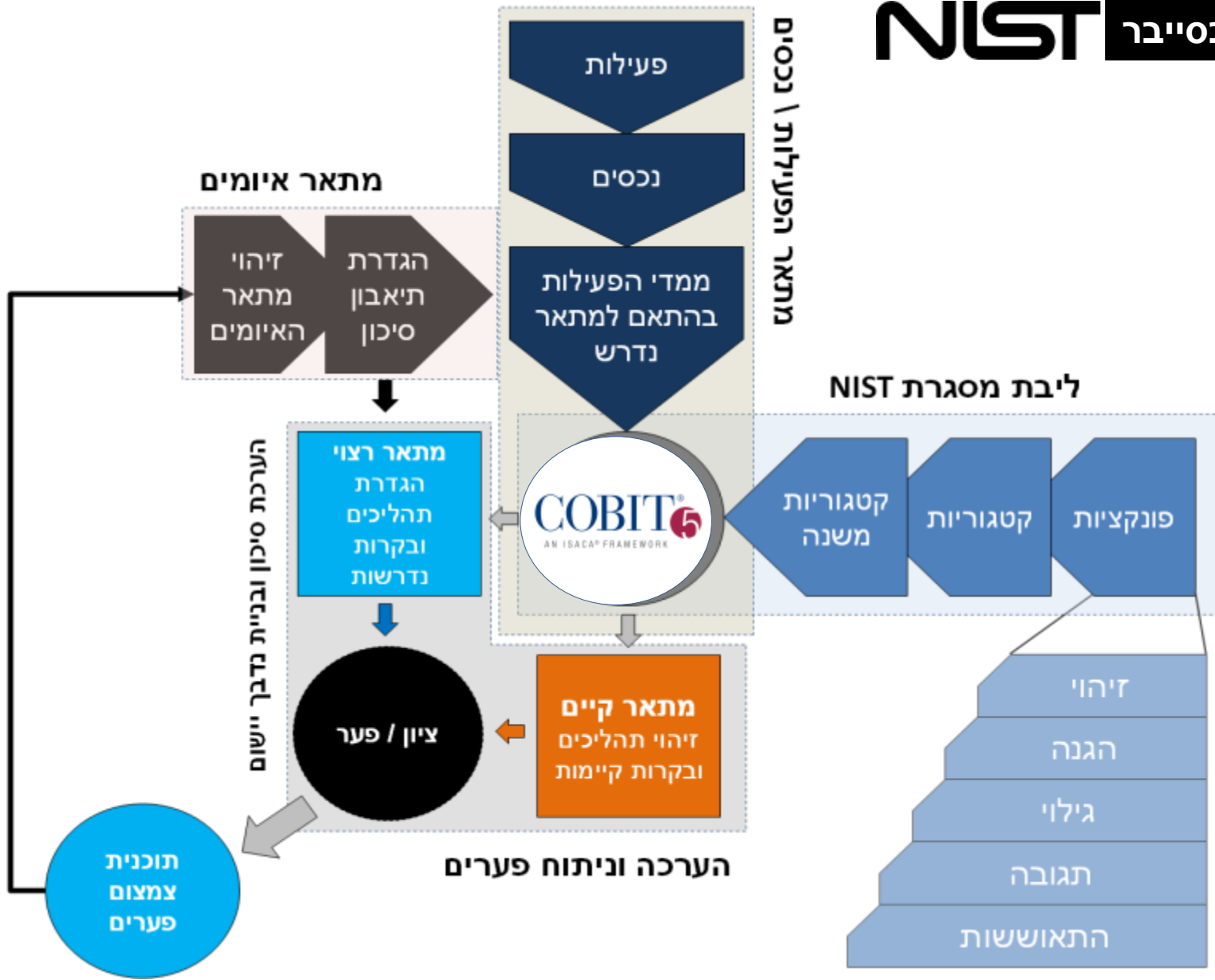


- שילוב גורמי אבטחת מידע כחלק אורגני בצוותי הפיתוח.
- מיכון ואוטומציה של תהליכי בדיקה לאורך שלבי הפיתוח – DevOps Security
- הגדרת RED TEAM

## מהגנה פאסיבית להגנה פרו-אקטיבית



- יצירת יכולת לשיתוף פעולה בין ארגונים, מטריית הגנה של המדינה ומודיעין מוקדם.
- חיזוק יכולת זיהוי התקפות באמצעות אנומליות בפעילות באמצעות תוכנות BIG DATA ו-AI.
- אימוץ מערכות לניהול אירועים הכוללות חיוויים תומכי החלטה.
- הגדרת תקן לאנליסט סייבר



פונקציות  
NIST

נכסים/רכיבים

	SME INDIVIDUAL FUNCTIONAL AREA SCORES						SCORES		RESULTS		
	POLICY	NETWORK	ENDPOINT/ DATA PROTECTION	IDENTITY	OPs	APPs	SME AVERAGE	CORE GROUP	COMBINED SCORE SME AND CORE	TIER TARGET SCORE	RISK GAP
<b>IDENTIFY</b>											
Business Environment	3	3	3	2	3	2	3	2	2	3	1
Asset Management	3	2	2	2	1	3	2	3	3	3	0
Governance	3	2	3	2	2	2	2	2	2	2	0
Risk Assessment	2	2	2	2	2	3	2	1	2	3	1
Risk Management Strategy	4	3	2	2	2	2	3	2	2	4	2
<b>PROTECT</b>											
Access Control	2	3	3	2	3	2	3	2	2	3	1
Awareness/Training	2	3	3	2	3	3	3	3	3	4	1
Data Security	2	2	2	2	2	2	2	3	3	3	0
Protective Process/Procedures	2	2	2	2	2	2	2	2	2	4	2
Maintenance	3	2	2	2	2	4	2	1	2	3	1
Protective Technologies	2	2	1	3	1	2	2	3	2	3	1
<b>DETECT</b>											
Anomalies/Events	2	3	1	2	2	4	2	2	2	4	2
Security Continuous Monitoring	2	2	1	2	1	1	1	2	2	4	2
Detection Process	2	3	2	2	3	2	2	4	3	3	0
Threat Intelligence	3	3	3	2	2	2	3	3	3	3	0

Mapping highlighted outliers and major differences

Focus areas stand out (large Δ)

פונקציה	נושא
זיהוי	מיפוי שירותים, מערכות, ספקים. מדיניות ואישור שיתוף שירותים.
הגנה	<b>ניהול הצפנה ומפתחות API, ניהול סביבות פיתוח בענן, אבטחת קוד פתוח, שילוב קוד חיצוני באפליקציות מקומיות</b>
גילוי	וקטור שותפים עסקיים
תגובה	כנ"ל



זיהוי	תשתיות פיתוח, תהליכי העברה לייצור
הגנה	<b>שילוב תהליכי בדיקה סטטיים ודינאמיים באופן ממוכן שימוש בשכבת שירותי רשת מוקשחת לתהליכים חוזרים ישום הגנה באופן ממוכן בעת מעבר לייצור (הצפנת קבצי הגדרות)</b>
גילוי	בקרת איכות - כחול ירוק
תגובה	שיתוף מידע עם אמצעי הגנה תשתיתיים



זיהוי	תשתיות אסוף, מערכת גילוי, כלי תחקור ופורנזיקה
הגנה	<b>שיתוף אירועים עם חברות, פרוטוקול לשיתוף אירועים (STIX)</b>
גילוי	<b>גילוי אירועים בשכבת שירותים - מעבר מוקטור תשתיתי לאפליקטיבי (lateral movement vs. depth movement)</b>



לדיגיטל

אתגרי הגנת סייבר  
במעבר

# תודה על ההקשבה

אלי חזן CISSP, CISA

מנהל תחום ייעוץ וביקורת סייבר

050-2076100

[elih@lionorl.co.il](mailto:elih@lionorl.co.il)