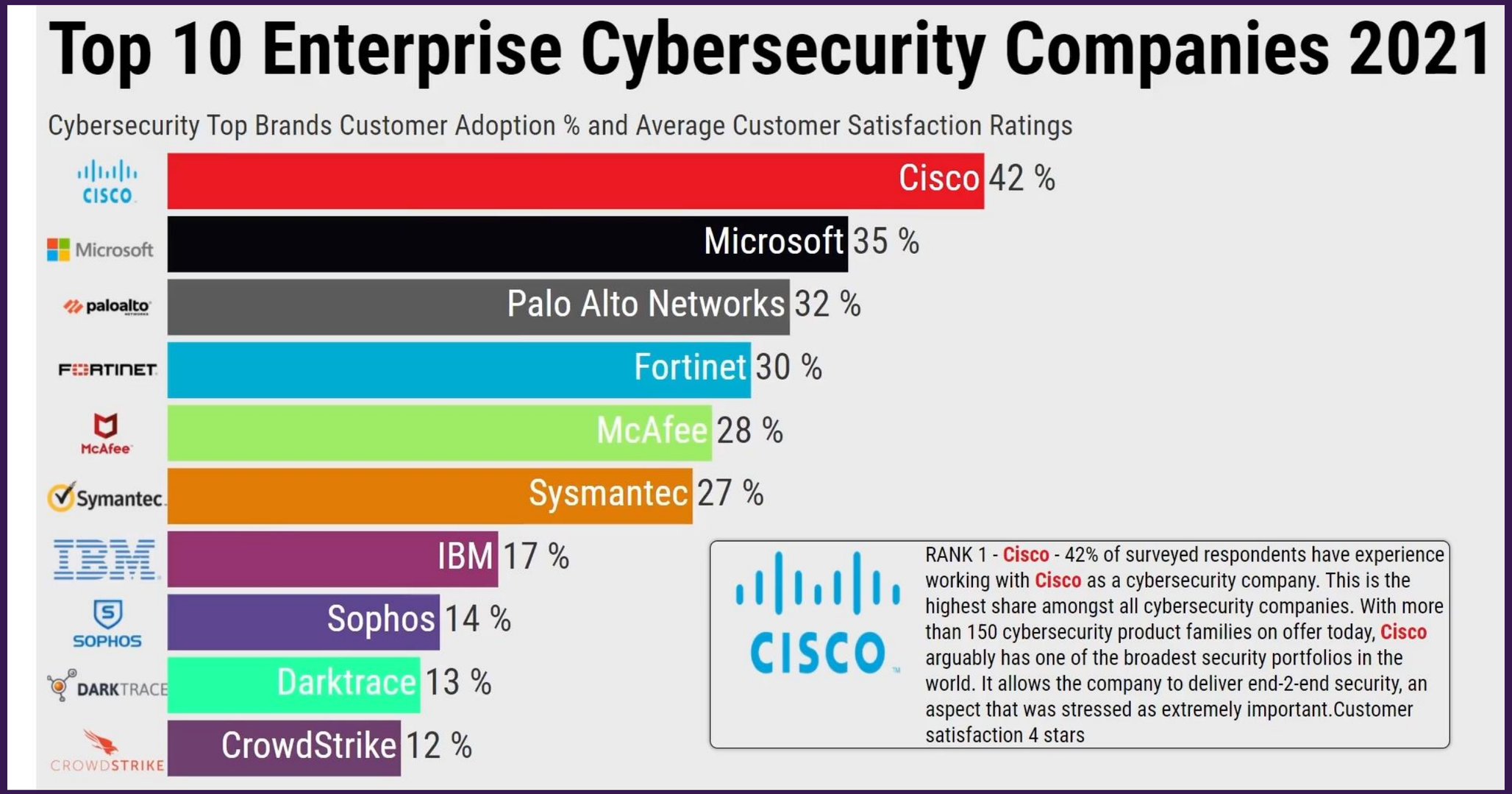
CISO וקבוצת INFOSEC בארגון

קבוצת INFOSEC ממלאת תפקיד חיוני בהגנה על נכסי המידע החיוניים של כל ארגון.

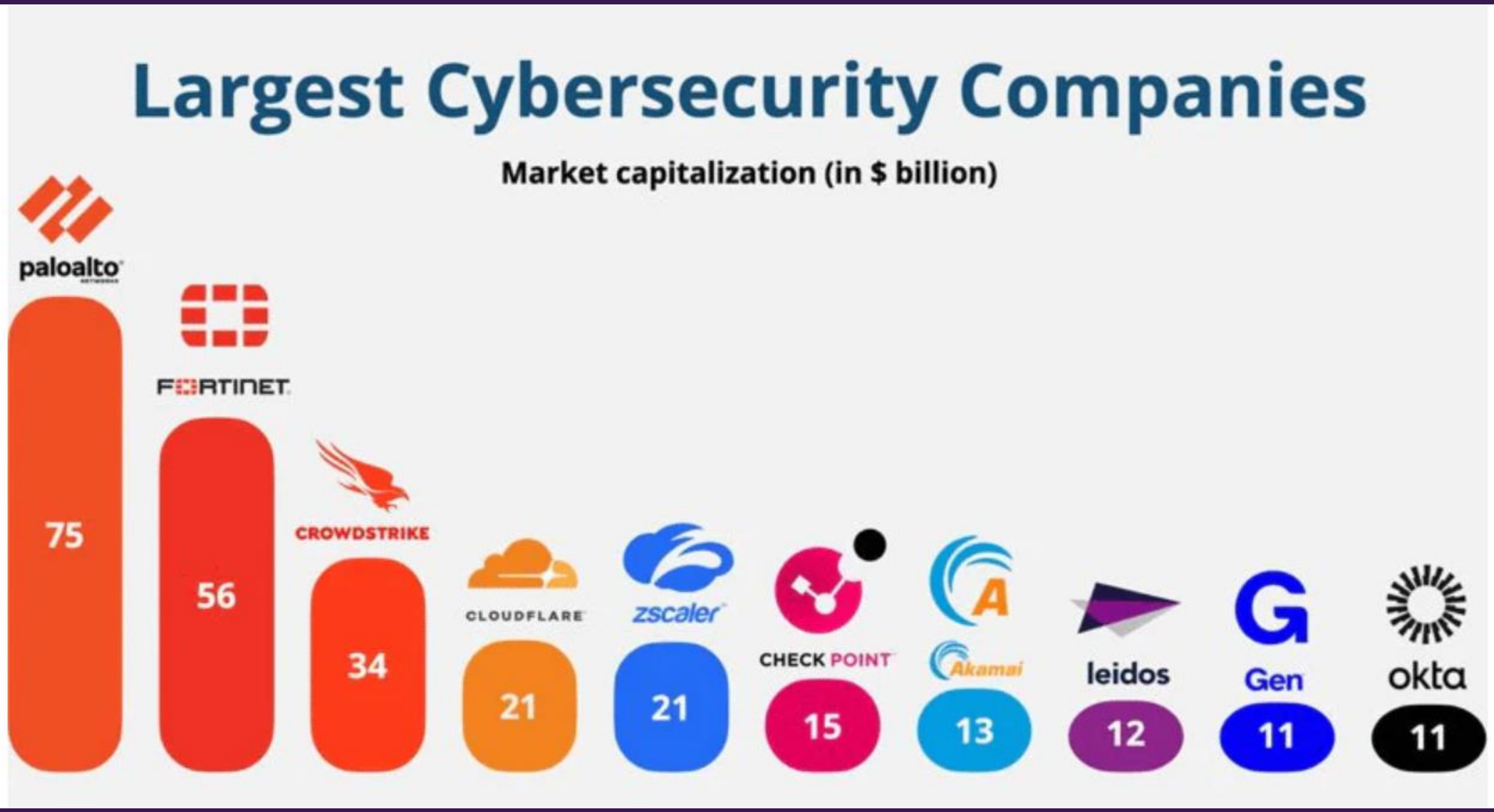
המכללה
האקדמית
רמת גן

2021



המכללה
האקדמית
רמת גן

2024


Largest Cybersecurity Companies
Market capitalization (in $ billion)
paloalto
75
FORTINET
56
CROWDSTRIKE
34
CLOUDFLARE
21
zscaler
21
CHECK POINT
15
Akamai
13
leidos
12
Gen
11
okta
11

Top 10 Cyber Security Companies in the U.S. in 2025 Making a Difference

Palo Alto Networks
Founding Year: 2005 Revenue: $8.29 Bn
Headquarter: SANTA CLARA, California

CrowdStrike
Founding Year: 2011 Revenue: $845.3 Mn
Headquarter: Toronto, Ontario (ON)

Fortinet
Founding Year: 2000 Revenue: $1.42 Bn
Headquarter: SSunnyvale, CA

Cisco Systems
Founding Year: 1984 Revenue: $53.8 Bn
Headquarter: San Jose, CA

Zscaler
Founding Year: 2008 Revenue: $628 Mn
Headquarter: San Jose, California

Check Point Software Technologies
Founding Year: 1993 Revenue: $2,565 Mn
Headquarter: Redwood City, California

Proofpoint
Founding Year: 2002 Revenue: $1.05 Bn
Headquarter: Sunnyvale, California

Okta
Founding Year: 2009 Revenue: $605 Mn
Headquarter: San Francisco, California

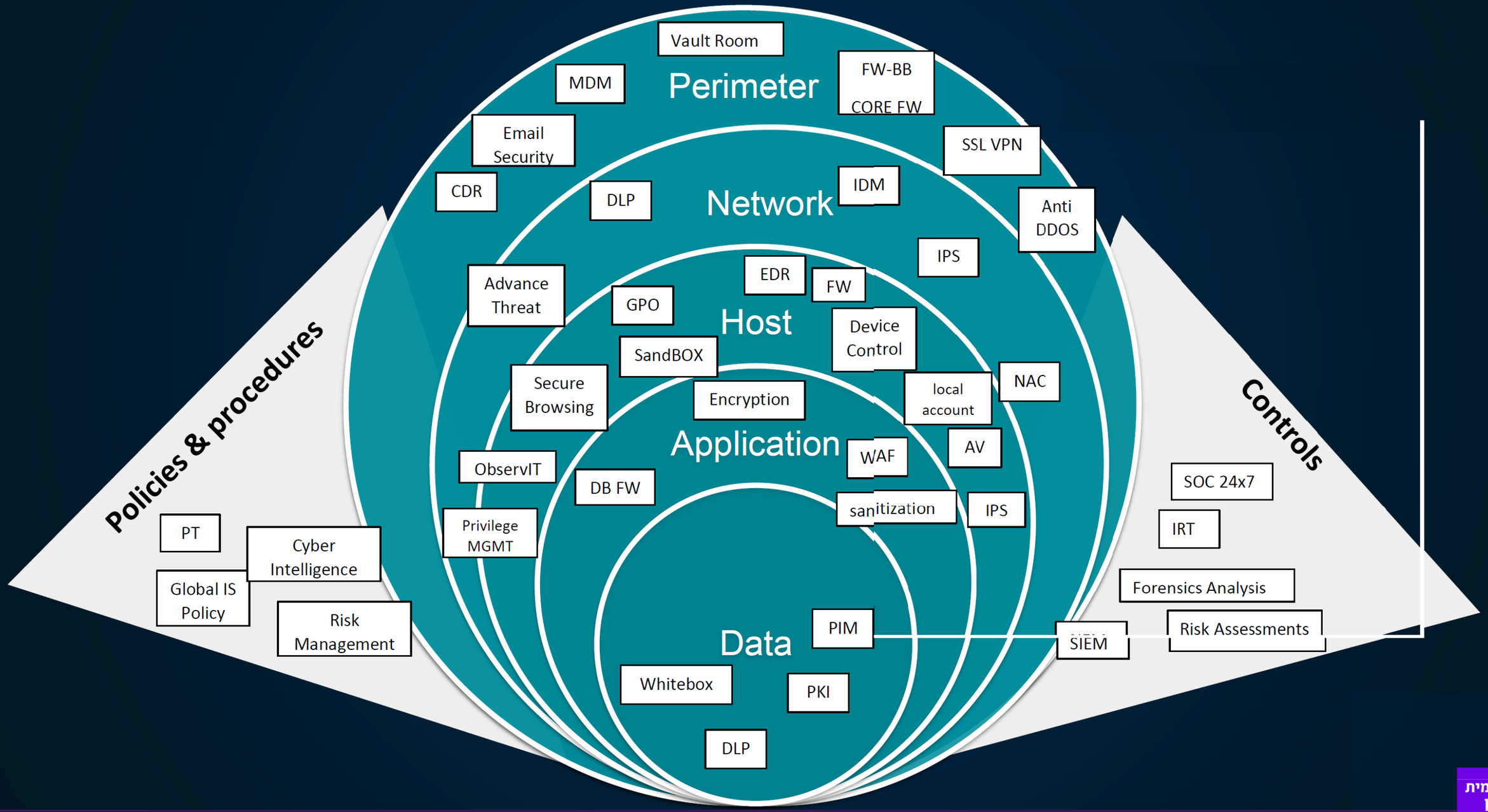
SentinelOne
Founding Year: 2013 Revenue: $210.6 Mn
Headquarter: Mountain View, California

IBM Security
Founding Year: 2015 Revenue: $62.8 Bn
Headquarter: Cambridge, Massachusetts

PERSISTENCE MARKET RESEARCH

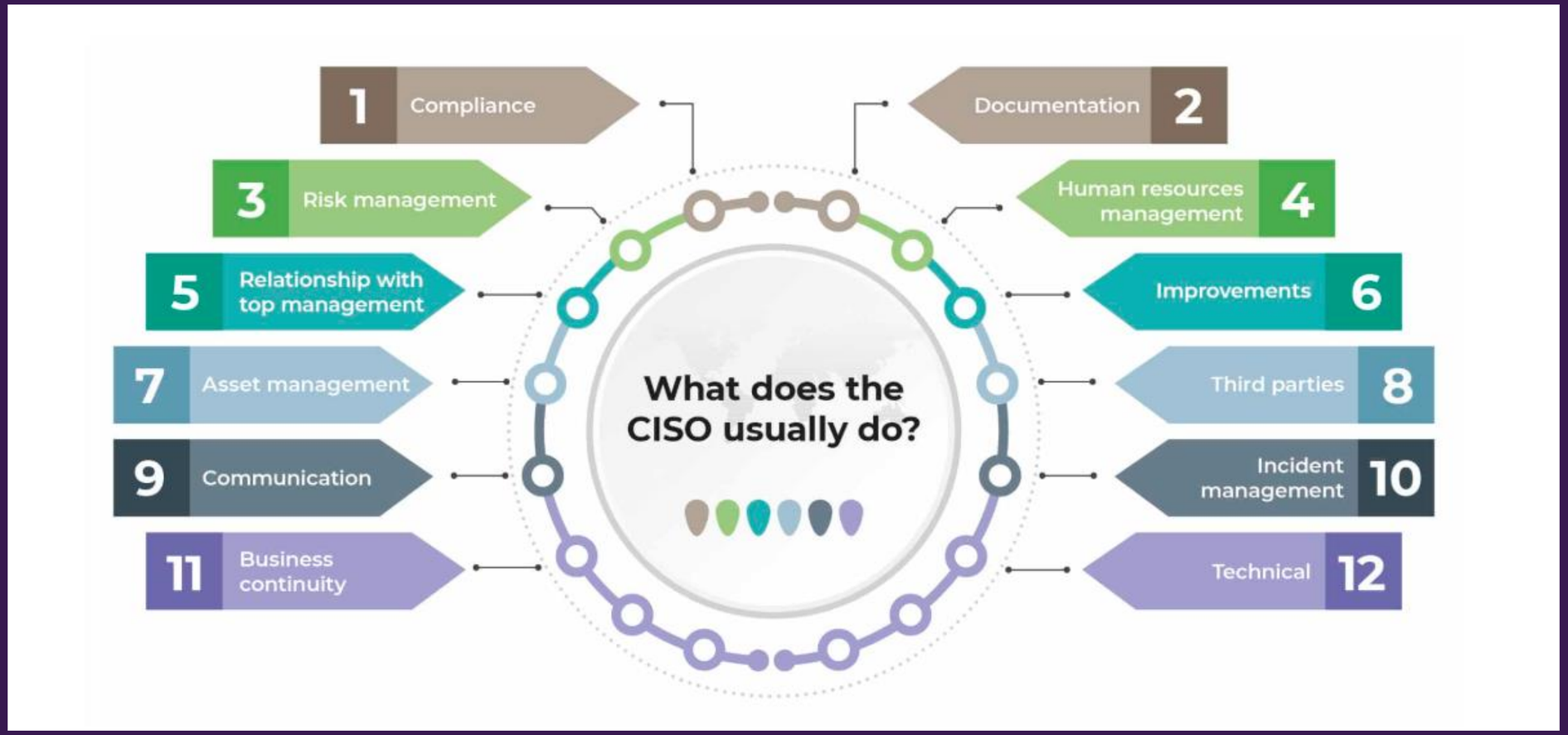
המכללה האקדמית רמת גן

תחומי הידע הנדרשים לCISO



המכללה
האקדמית
רמת גן

CISO



המכללה
האקדמית
רמת גן

הבעיה הכי גדולה – במידה ונתפסת כלא מקצוען בעיניי הארגון / עמיתים /לקוחות

- עמיתים
- אנשי IT
- מנהלים בארגון
- לקוחות
- אנשים שאת/ה מנהל

המכללה האקדמית רמת גן

מקומו הארגוני של CISO וקוים מנחים

1. מה היה בעבר ?
2. תקנות אבטחת מידע 2017
3. כפוף לסמנכ"ל לפחות (או בעצמו סמנכ"ל)
4. חבר הנהלה

המכללה האקדמית רמת גן

מה עליו לעשות כדי להצליח ?

- להכיר את כול התהליכים ונכסים
- להיות נינוח ולא דרמטי
- לשקול כול מענה, לבסס על ידע לא תחושה
- כיסוי מקצועי לכול נושא
- לשווק עד רמת אחרון העובדים
- להודעות בטעויות
- זמינות 24/7
- לענות לכול פנייה
- פגישות ותחזוקת קשרים עם עמיתים מהתעשייה
- בשום פנים לא לחצות את הגבולות המקצועיים

המכללה האקדמית רמת גן

הכרת הארגון ומערכת היחסים בארגון

מנהלים בכירים

פגוש את יו"ר הדירקטוריון, את חברי הדירקטוריון, פגישה עם חברי הדירקטוריון שמתמקדת בחזון ואסטרטגיית IT

מנהלי ביניים

פגוש את כול העמיתים, מנהלי מחלקות, מנהלי IT בארגון, יועץ משפטי, יו"ר ועד העובדים, מבקר ארגוני, אחראי עם Audit.

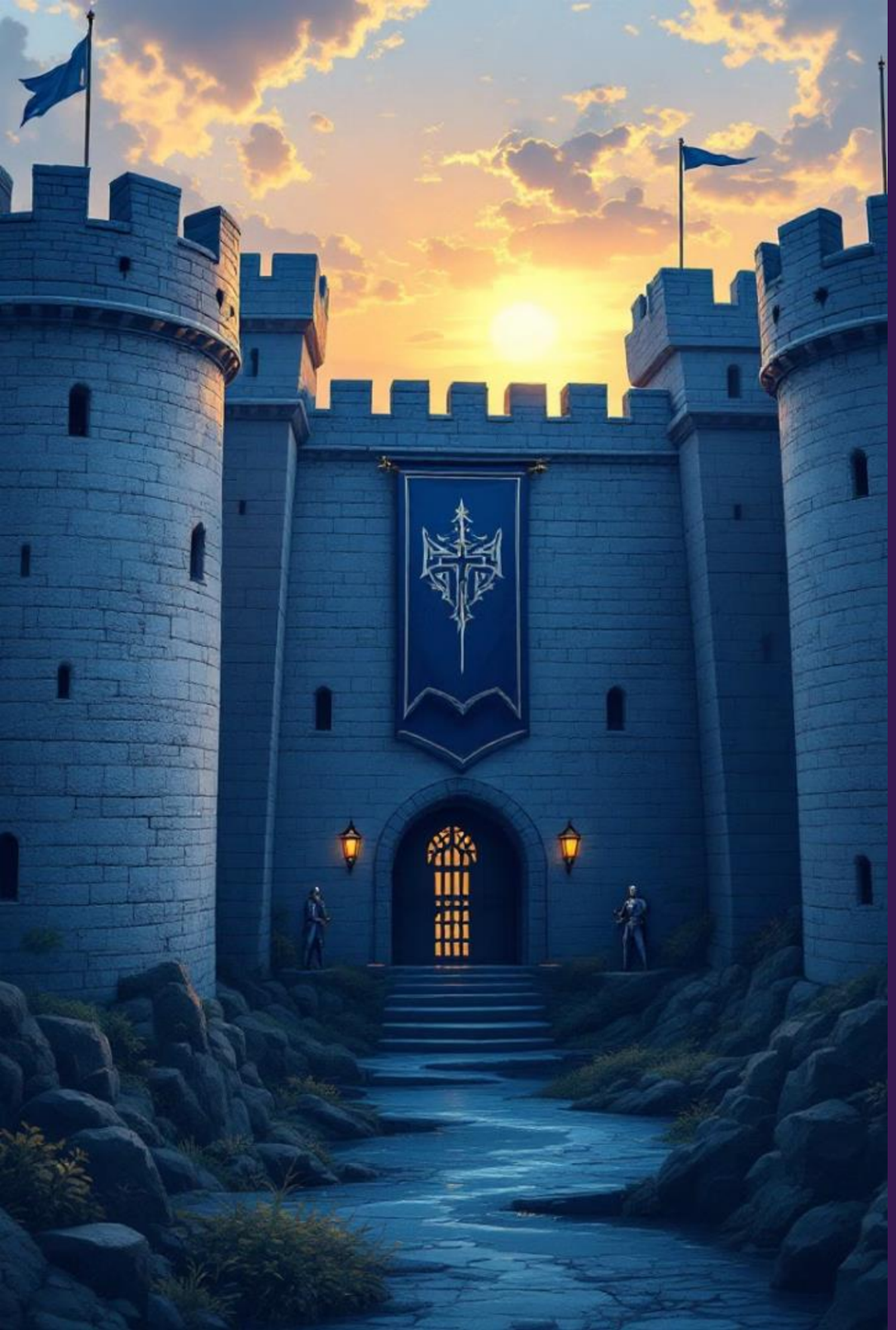
עובדים בארגון

פגוש את כול העובדים בארגון (F2F), אלא בפגישות All Hands, והסבר את משמעות אבטחת המידע וההשפעות שלה על הארגון.

המכללה האקדמית רמת גן

יש גם דוגמאות פשוטות יותר....

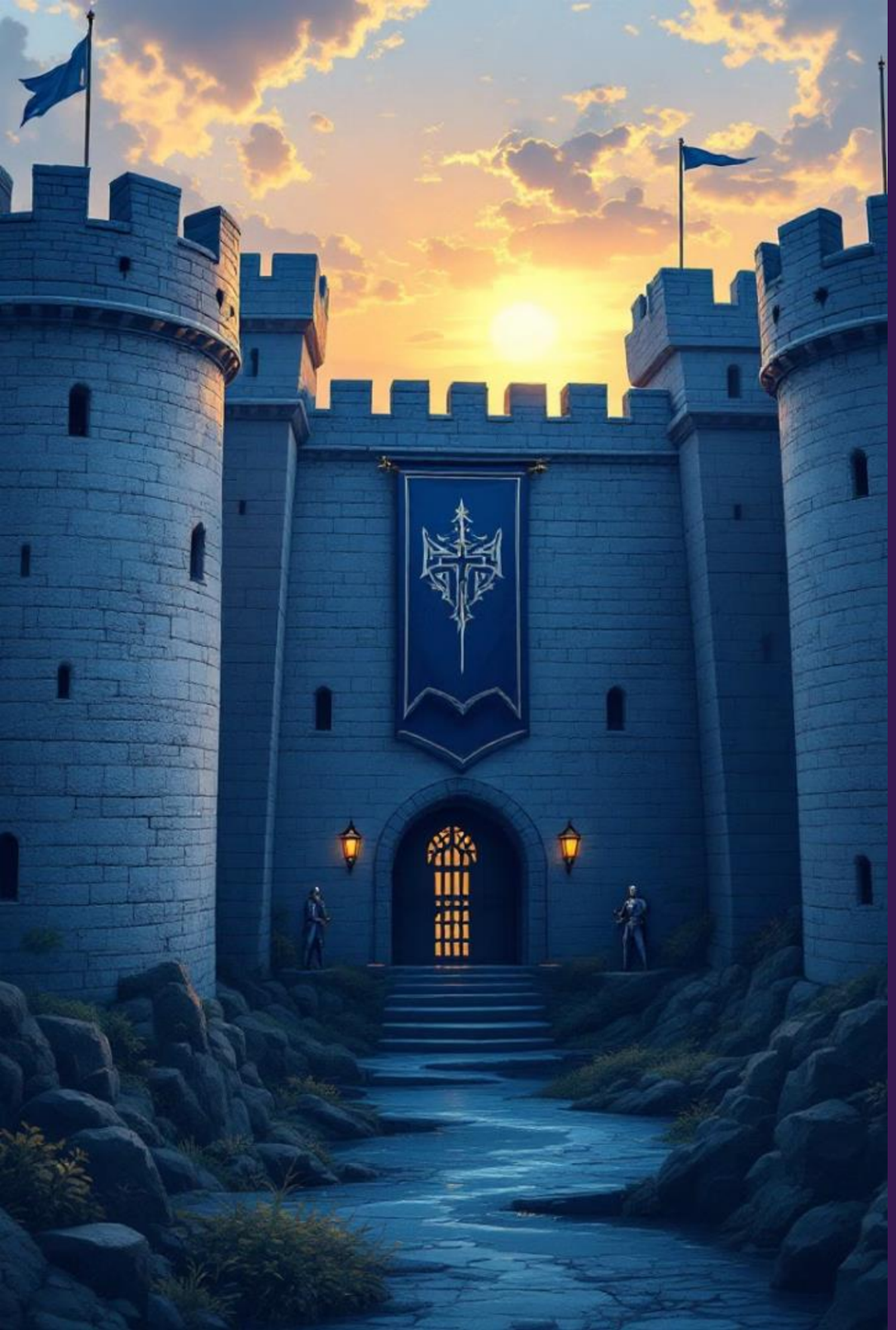
- תוך כדי שיחת WEBEX (של חברת CISCO), התחבר משתמש אנונימי
- בגלל צפיפות וכמות משתמשים לא באמת שמו לב ואישרו אותו
- דלפו מסמכי עיצוב ומסמכים טכניים של מוצרי APPLE חדשים



מחויבות לחוקים ומיניסטריון

- הכרה מעמיקה של חוקים ותקנות
- הכרה מעמיקה של חוזרי מנכ"ל המנחה המקצועי המגזרי
- לוודא סוגיות משפטיות שהיו בנושא בארגון שלך
- לוודא שהמדיניות מותאמת לדרישות החוק
- ללמוד את החוקים הרלוונטיים מהעולם
- לעבור על דוחות המבקר

המכללה
האקדמית
רמת גן

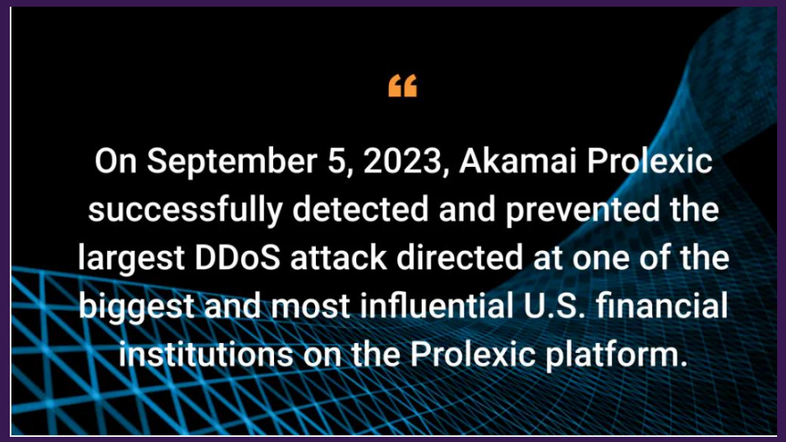


מה הכלים העומדים לרשות CISO ?

- החוק
- מדניות הגנת הסייבר הארגונית
- תקציב ייעודי
- צוות המכסה את תחומי הגנת הסייבר
- תהליכים ארגוניים המחייבים לקבל את אישורכם
- תהליכים ארגוניים שבמדיניות החוזה יש חובה בהגנת הסייבר
- מערכת בקרה וביקורת
- מבקר הארגון
- הרשות להגנת הסייבר

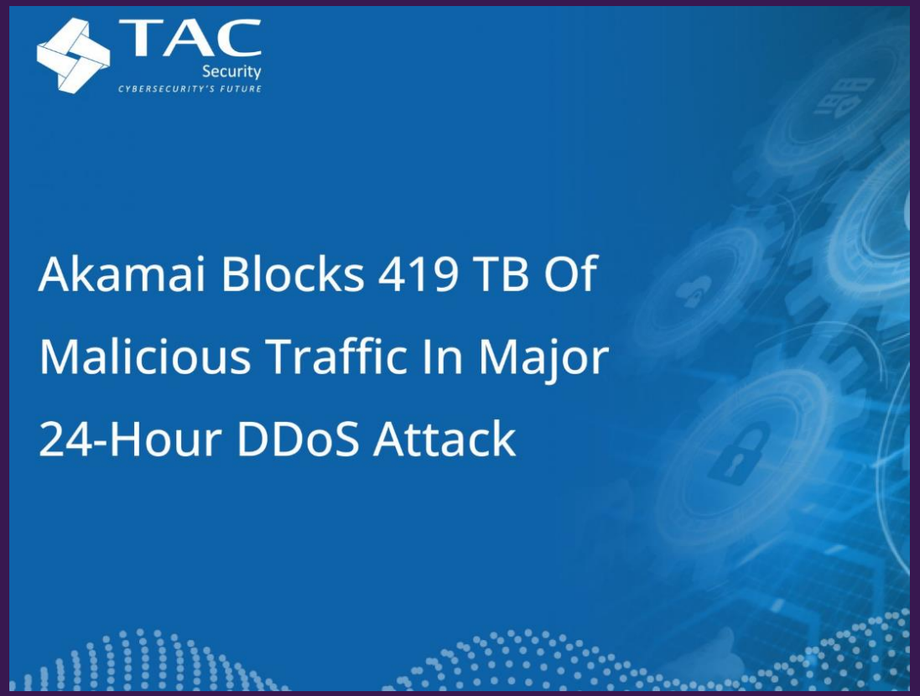
המכללה
האקדמית
רמת גן

כמה דוגמאות...



On July 15, 2024, Akamai prevented one of the largest distributed denial-of-service (DDoS) cyberattacks it has ever observed against a major financial services company in Israel.

Cybercriminals used a combination of ACK, PUSH, RESET, and SYN flood attack vectors, peaking at 633.7 gigabits per second (Gbps) and 55.1 million packets per second (Mpps)



כמה דוגמאות...

Robert Tappan Morris—The Morris Worm (1988)

Robert Tappan Morris made the first internet computer worm in history. He was a student at Cornell University. Although Mr. Morris claimed he did it to explore the size of the cyber space, it soon evolved into a virus that caused between $10 million and $100 million in damage repair costs.

Google China attack (2009)

In 2009, in an act of cyber espionage, hackers were able to get inside Google's servers and access Gmail accounts belonging to **Chinese human rights activists**. Upon further investigation, authorities discovered that many Gmail accounts of people in different countries had been penetrated.

A teenager hacks the US Defense Department and NASA (1999)

A 15-year-old named Jonathan James was able to get inside the U.S. Department of Defense's (DOD) computers and install a backdoor within its servers. He then used the backdoor to intercept internal emails, some of which had usernames and passwords inside.

James then used his access to the DOD's system to steal NASA software used to support the International Space Station.

Hacking a radio phone system to win a porsche (1995)

A man named Kevin Poulsen heard of a radio station contest where you could win a sports car. He ended up winning a Porsche 944 S2 by being the 102nd caller. He accomplished this feat by hacking the phone system, locking out other callers, ensuring his victory. He ended up getting sentenced to five years in prison.

Ukraine Power Grid Attacks

In December 2015, during the heart of winter, Russian threat actors compromised power distribution companies in western Ukraine, leading to a power outage for more than 230,000 residents.

The threat actors also reportedly flooded customer services phone lines with calls to prevent customers from reporting the incident, which lasted a number of hours.

ומה קרה בספרד ב2025 ?

- ב 28.4 היתה הפסקת חשמל בכלל ספר, פורטוגל ואיזורים שכנים

המכללה
האקדמית
רמת גן

ארגון ה INFOSEC

המכללה
האקדמית
רמת גן

תרומת קבוצת INFOSEC להצלחת הארגון הארגון

1

הגנה על נכסי המידע

הבטחת פעילות תקינה של הארגון ,מניעת אובדן נתונים.

2

שמירה על תדמית

מניעת פגיעה בתדמית הארגון ,אמון הלקוחות ,הגנה על מידע אישי.

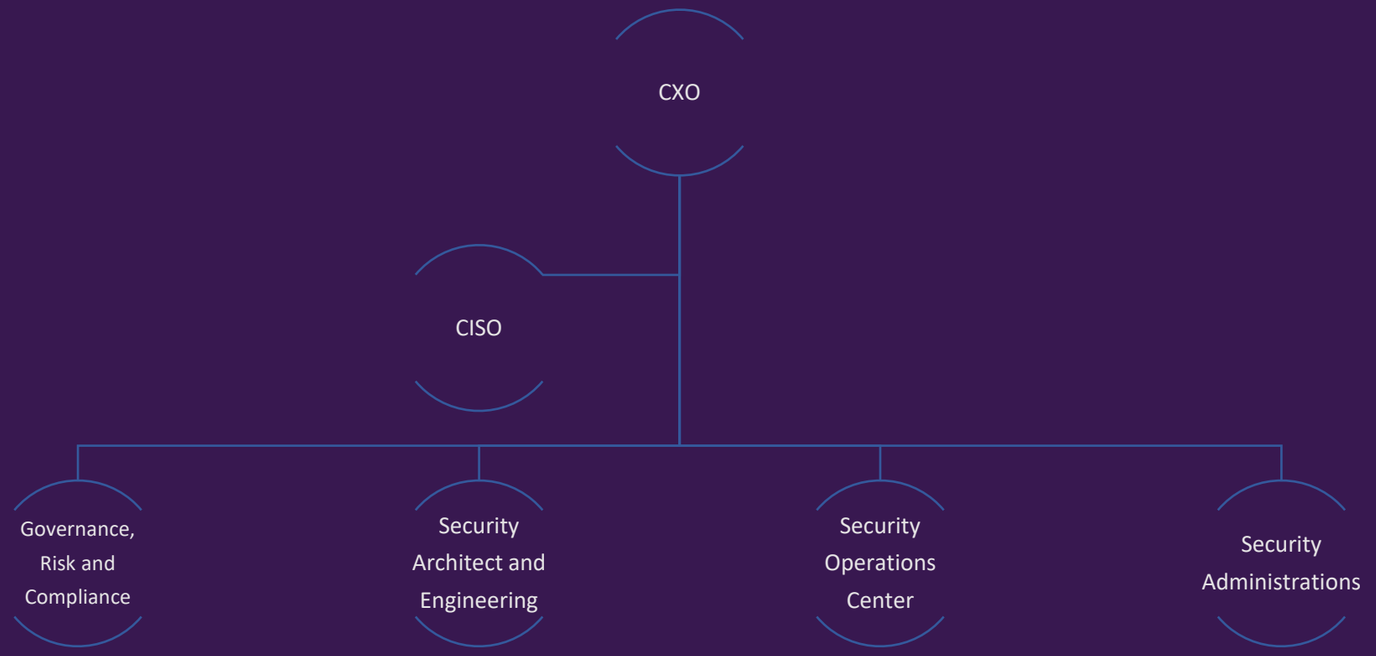
3

הבטחת צמיחה

הבטחת צמיחה עסקית ,פעילות תקינה גם במקרה של אירוע אבטחה.

המכללה האקדמית רמת גן

מבנה ארגוני



המכללה
האקדמית
רמת גן

מושגי יסוד במיגון מידע

זמינות

גישה זמינה ומהירה למידע כאשר נדרש , ללא הפרעה.

שלמות

שמירה על נכונות המידע ועל מניעת שינויים לא מורשים.

סודיות

הגנה על מידע מפני גישה לא מורשית , שמירה על סודיות המידע.

הגנת מידע כחלק אינטגרלי מהאסטרטגיה העסקית

1 הגנה על נכסי המידע

הגנה על נכסי המידע של הארגון ,כולל מידע עסקי ,נתוני לקוחות ,נתוני פיננסיים ועוד .

2 מניעת אובדן נתונים

מניעת אובדן נתונים כתוצאה ממתקפות סייבר ,תקלות טכנולוגיות או אירועי אסון.

3 שמירה על תדמית הארגון

שמירה על תדמית הארגון ועל אמון הלקוחות ,הגנה מפני פגיעה במידע אישי של

4 הבטחת המשכיות עסקית

הבטחת המשכיות עסקית , שמירה על פעילות עסקית תקינה גם במקרה של אירוע אבטחה.

בממוצע הארגונים מוציאים בין 4.4 ל 10.2 מליון דולר בשנה על הגנה על המידע שלהם

המכללה האקדמית רמת גן

האתגר הטכנולוגי :שמירה על שדרוג מתמיד

שדרוג תכוף

יישום עדכונים שוטפים למערכות ההגנה ,הבטחת רמת הגנה יעילה .

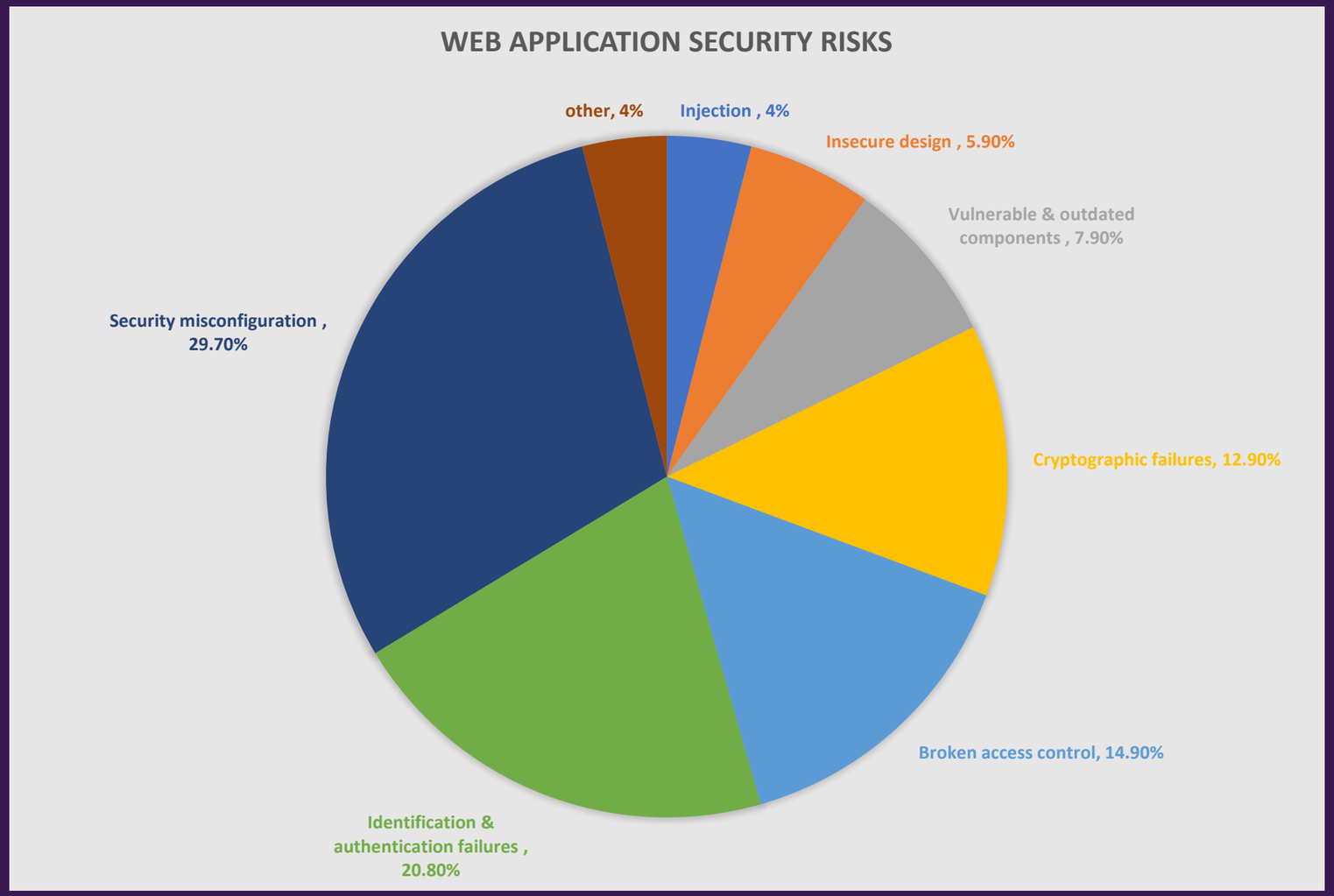
טכנולוגיות מתפתחות

הצורך להתעדכן בטכנולוגיות חדשות ומתפתחות ,להגן מפני איומים מתקדמים.

השפעות ה AI ?

המכללה
האקדמית
רמת גן

סוגי איומים פוטנציאליים על אפליקציה



המכללה
האקדמית
רמת גן

אבטחת מערכות מידע והגנה מפני איומים חיצוניים

הגנה מפני מתקפות סייבר

הטמעת טכנולוגיות אבטחה מתקדמות ,זיהוי ומניעת מתקפות סייבר.

הגנה מפני גישה לא מורשית

ניהול הרשאות גישה למידע , בקרת גישה לפי תפקידים ,הגנה מפני גישה לא מורשית.

הגנה מפני תוכנות זדוניות

הטמעת תוכנות אנטי-וירוס ,זיהוי ומניעת תוכנות זדוניות ,ניהול איומים.

המכללה האקדמית רמת גן

שאלות ?

המכללה
האקדמית
רמת גן