דרכי פעולה מומלצות

צמצום סיכוני סייבר ממצלמות אבטחה

סייבר ישראל
מערך הסייבר הלאומי

סייבר ישראל
מערך הסייבר הלאומי

דרכי פעולה מומלצות

צמצום סיכוני סייבר ממצלמות אבטחה

גרסה 2.0

מרץ 2022

מסמך זה נכתב על-ידי מערך הסייבר הלאומי לצורך קידום הגנת הסייבר במשק הישראלי.
כל הזכויות שמורות למדינת ישראל - מערך הסייבר הלאומי. המסמך נכתב כשירות לציבור. העתקת המסמך או שילובו במסמכים אחרים כפוף לתנאים הבאים: מתן קרדיט למערך הסייבר הלאומי בפורמט המופיע להלן; שימוש בגרסה העדכנית של המסמך; אי הכנסת שינויים במסמך.
המסמך מכיל מידע מקצועי, אשר יישומו בארגון מצריך היכרות עם מערכות הארגון והתאמה למאפייניו בידי איש מקצוע בתחום הגנת הסייבר.
הערות והתייחסויות למסמך ניתן להעביר למייל: tora@cyber.gov.il

תוכן עניינים

צמצום סיכוני סייבר ממצלמות אבטחה

1. מבוא

1.1 רקע

השימוש במצלמות אבטחה [1]על-ידי ארגונים ויחידים במשק גובר והולך, כאשר שכיח לראות מצלמות המסייעות באיתור אירועים חריגים, דוגמת מעשי אלימות במוסדות חינוכיים ובאירועים המוניים, פריצה לבתים פרטיים ובניינים משותפים, ואירועים ביטחוניים או בטיחותיים (Safety). כמו כן, השימוש במצלמות אבטחה מהווה אבן בסיס בתפיסת "ערים חכמות" (Smart Cities), דבר המגדיל משמעותית את מספר צרכני המידע והיקף הפריסה.

מקובל להתייחס אל מצלמות האבטחה כהתקן מסוג האינטרנט של הדברים (IoT), וזאת כאשר משתמשים רבים מקשרים את התקנים אלו לרשת האינטרנט. כפועל יוצא מכך, התקנים אלו עשויים להיות נגישים מכל מקום ובכל זמן (Any Time Any Place), דבר אשר הופך אותם ליעד אטרקטיבי עבור תוקפים במרחב הסייבר.

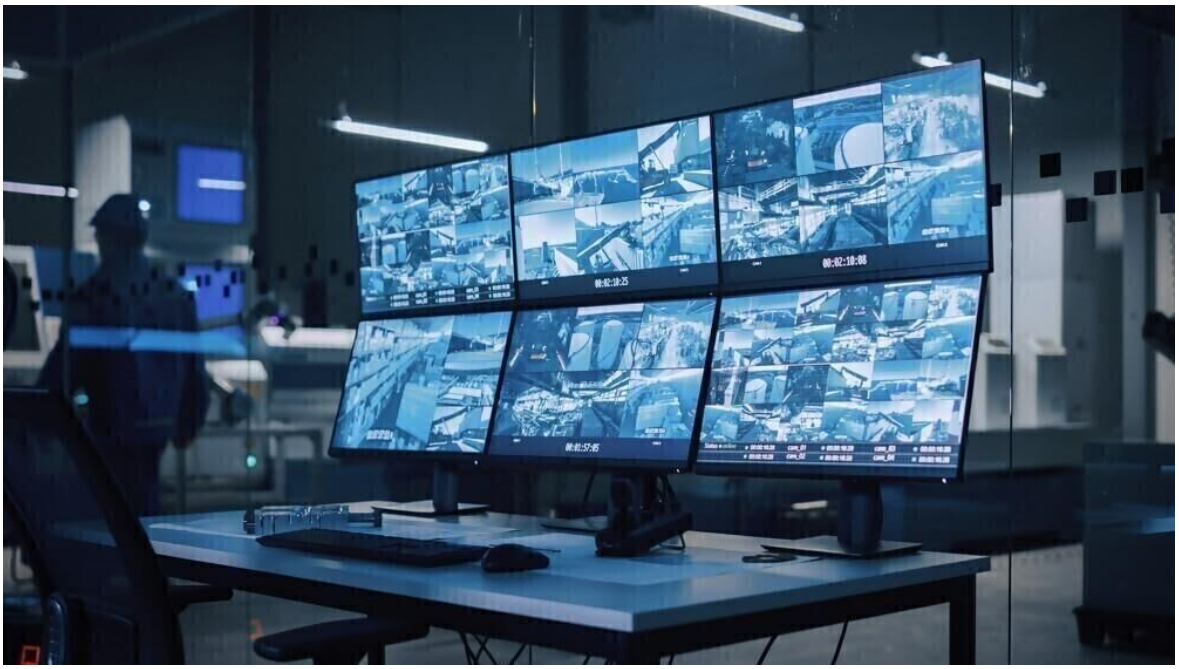
כמו כן, חלק ממצלמות האבטחה לא פותחו בהתאם לעקרונות פיתוח מאובטח מקובלים דוגמת עיצוב לאבטחה (Security by Design) ועיצוב לפרטיות (Privacy by Design), דבר אשר מגדיל משמעותית את רמת החשיפה לסיכוני סייבר.

לנוכח זאת ניתן לראות כי במרחב הסייבר הישראלי מתבצעת פעילות אויב ויריב לניצול לרעה של מצלמות האבטחה, לרבות השתלטות על מצלמות לשם הפקת מידע ערכי אודות פעילות כוחות ואנשים.

שכיח לראות ברמה העולמית כי מצלמות האבטחה מהוות תשתית פורה לאפידמית סייבר, דוגמת Mirai Botnet על גרסותיה השונות הפעילה כבר משנת 2016, ו-Mozi IoT botnet אשר פעילה משנת 2020, לערך.

בשנים האחרונות חלק מהיצרנים החלו לשלב יכולות אנליטיקה מבוססות טכנולוגית ראיה ממוחשבת (Computer Vision), וטכנולוגית אחרות, כחלק אינטגרלי ממערך מצלמות האבטחה, וזאת במטרה להציע ערך מוסף למשתמשים. ערך מוסף זה עשוי לכלול **תיאור** תמונת מצב בזמן אמת תוך תמצות וידאו, **זיהוי** אובייקטים דוגמת לוחית רישוי (LPR ו-ALPR) , פני אדם, אמצעי לחימה, או תאונת דרכים, וקיומה של יכולת **חיזוי** להתרחשות אירועים חריגים דוגמת התפרעות אלימה במסגרת אירוע המוני. ראוי לציין כי יכולות מתקדמות אלו מחייבות התייחסות פרטנית לנושא הגנה על פרטיות (Privacy), דבר המחייב שילוב של היועץ המשפטי לארגון כבר בשלב הייזום של פרויקט המצלמות.

[1] שם חלופי - טלוויזיה במעגל סגור (טמ"ס) (CCTV)

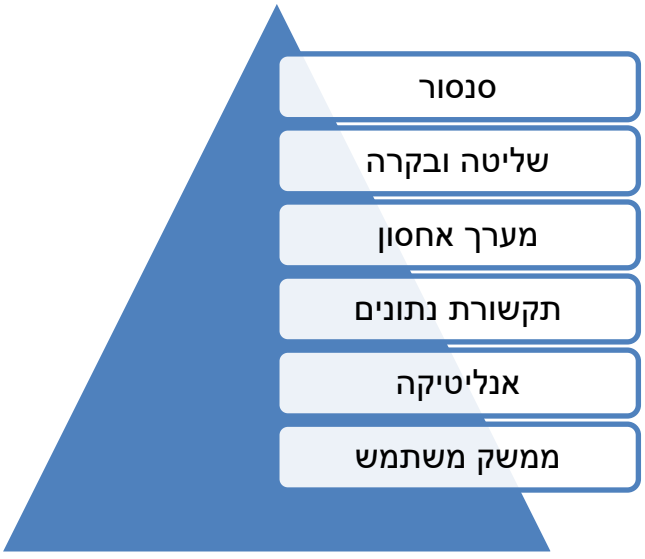


תמונה 1: צילום חדר בקרה.

לגבי השימוש בזיהוי פנים במרחב הציבורי, על כל היבטיו, מומלץ לפנות למסמך המדיניות שפרסמה היחידה להזדהות ויישומים ביומטריים במערך הסייבר הלאומי: https://www.gov.il/he/departments/general/face_recognition
(להלן:" מסמך זיהוי פנים במרחב הציבורי").

1.2ארכיטקטורה טיפוסית של מערך מצלמות האבטחה

התרשים הבא סוקר את אבני הליבה של ארכיטקטורה טיפוסית של מערך מצלמות אבטחה:



תרשים 1: ארכיטקטורה טיפוסית של מצלמות אבטחה.

הטבלה הבאה סוקרת סוגי סנסורים שכיחים במצלמות אבטחה:

מס'	סוג הסנסור
.1	מצלמה אופטית תומכת אור יום
.2	מצלמה אופטית הכוללת הגברה של אור כוכבים
.3	מצלמה אינפרה אדום (IR) פסיבית
.4	מצלמה אינפרה אדום (IR) אקטיבית (כוללת מנורת IR, לרבות שימוש בטכנולוגיית ראיית הלילה ZLID)
.5	לידאר (LiDAR) - טכנולוגיה למדידת מרחק על ידי הארת המטרה בקרן לייזר, ומדידת הזמן שלוקח לקרן האור לחזור למקלט.
.6	מגלה כיוון ומרחק (מכ"מ) על בסיס שימוש בתדרי רדיו (RF)
.7	איתור מיקום פיזי (איכון) דוגמת GPS
.8	האזנת נפח / מיקרופון
.9	סביבון (גירוסקופ) - מודד מהירות זוויתית ומספק את זווית הסיבוב
.10	מד תאוצה - מודד תאוצה קווית ומספק את מהירות ומרחק התנועה
.11	מד לחץ
.12	איתור עשן

טבלה 1: סוגי סנסורים שכיחים במצלמות אבטחה.

הטבלה הבאה סוקרת סוגי התקנים/שירותים מקובלים לשליטה, בקרה ואחסון של מצלמות אבטחה:

מס'	סוג ההתקן
.1	DVR (Digital Video Recorder)
.2	NVR (Network Video Recorder)
.3	VMS (Video Management Software)
.4	VSaaS (Video Surveillance as a Service)

טבלה 2: סוגי התקנים/שירותים מקובלים לשליטה, בקרה ואחסון של מצלמות אבטחה.

השימוש במצלמות אבטחה במרחב הציבורי והפרטי רווח בארץ ובעולם, כאשר מצלמות האבטחה מהוות יעד מועדף לתוקפים במרחב הסייבר.

מצלמות אבטחה עשויות לתעד מידע ערכי, אשר עשוי להוות מאגר מידע בהתאם לחוק הגנת הפרטיות.

הטבלה הבאה סוקרת פרוטוקולי תקשורת נתונים שכיחים אשר עשויים להיתמך על-ידי מערך מצלמות האבטחה:

Protocol	Optimized for Extended Battery Life	Nominal Range Limit	Typical Data Rate	Spectrum
NFC	✓	Personal (<10m)	2Mbps	ISM 2.4GHz unlicensed
Bluetooth	✓	Contact (<4cm)	100Kbps	ISM 13.56MHz unlicensed
WiFi	✗	Local (<100m)	> 100Mbps	ISM 2.4GHz/5GHz unlicensed
LoRaWAN	✓	Metro (>10km)	< 50Kbps	ISM 900MHz, 868MHz, 433MHz unlicensed
NB-IoT	✓	Metro (>10km)	200Kbps	Licensed cellular
2G 3G	✗	Metro (>30km)	< 2Mbps	Licensed cellular
4G LTE	✗	Metro (>30km)	> 100Mbps	Licensed cellular
5G	✗	Metro (>30km)	> 10Gbps	Licensed cellular

טבלה 3: פרוטוקולי תקשורת נתונים שכיחים אשר עשויים להיתמך על-ידי מערך מצלמות האבטחה.

יש לתת את הדעת כי חלק ממצלמות האבטחה עדיין משתמש בתשתית כבילה מסוג כבילה קואקסיאלית (תשתית אנלוגית).

להלן דוגמא ליכולות אנליטיקה אשר מערך מצלמות האבטחה יכול לספק לארגון:

א. איתור חוזי או שמע לפי תאריך, מיקום מצלמה, וכד'.

ב. חיפוש ישויות בהתאם למילות מפתח (דוגמת רכב מסוג X או רכב בעל מספר Y או רכב בעל צבע Z)

ג. זיהוי ביומטרי של אדם, כדוגמת "זיהוי פנים"

ד. איתור נוכחות של חפצים מסוכנים דוגמת נשק קר או חם

ה. איתור חריגה מקו בסיס (Baseline) או קיומה של אנומליה. לדוגמא:

- דוגמת תזוזת חפץ ממקום קבוע
- תנועה חריגה של מספר הולכי-רגל בזמן נתון
- פעילות בשעות חריגות (VMD)

ו. ביצוע קורלציה (Correlation) מול נתונים ממערכות משיקות דוגמת פלט מערכת נוכחות או מערכת בקרת גישה פיזית (PACS)

הטבלה הבאה סוקרת סוגי ממשקי משתמש שכיחים אשר עשויים לשרת את מערך מצלמות האבטחה:

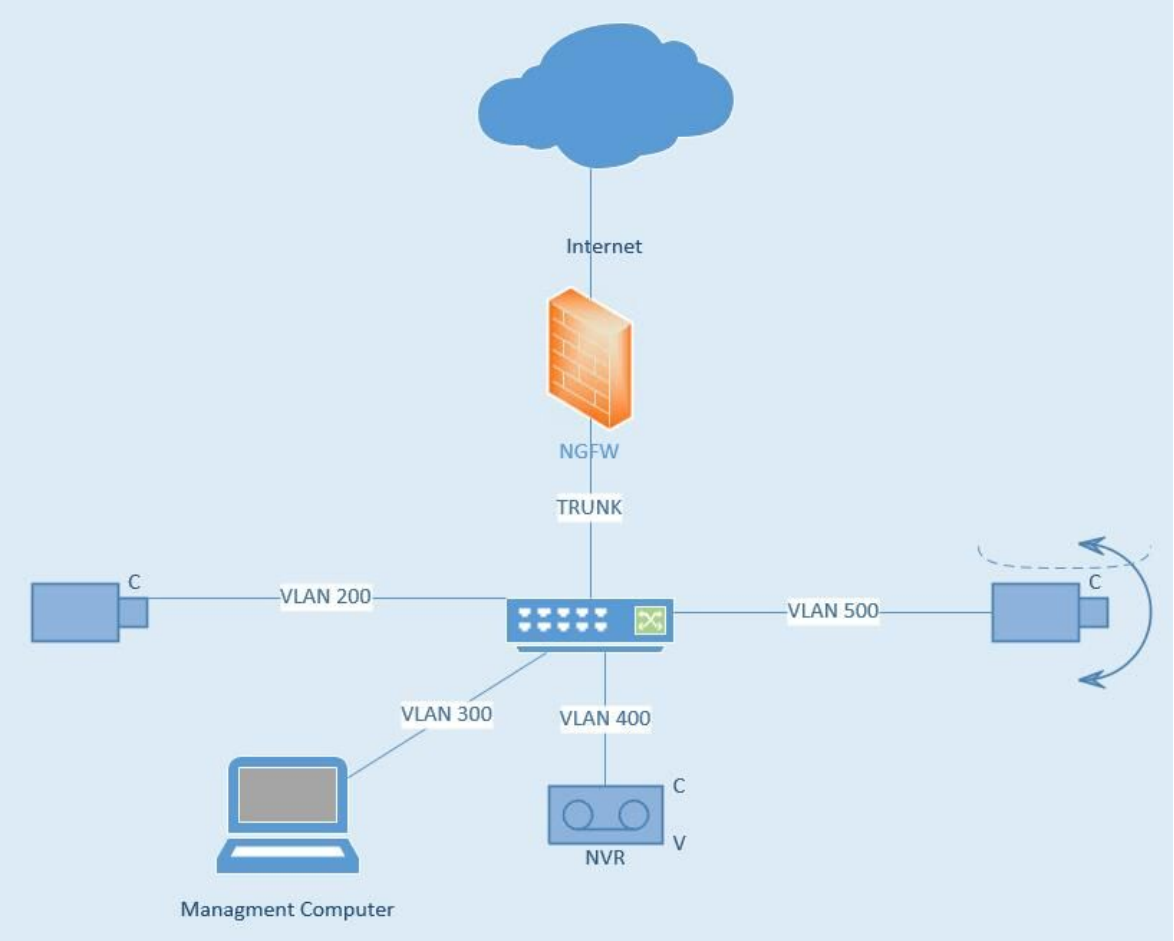
מס'	סוג הממשק
1.	אפליקציה / דפדפן במחשב
2.	אפליקציית טלפון נייד
3.	מסך / צג
4.	רמקולים / אוזניות
5.	משקפיים תומכות מְצִיאוּת רְבוּדָה (Augmented Reality)
6.	משקפיים תומכות מציאות מדומה (Virtual Reality)

.7	אביזר מחשוב לביש (Wearable Computing)
.8	ממשק מוח-מחשב (Brain Computer Interface)

טבלה 4: סוגי ממשקי משתמש שכיחים אשר עשויים לשרת מערך מצלמות אבטחה.

1.3ארכיטקטורה טיפוסית של סביבת רשת תומכת מערך מצלמות האבטחה

התרשים הבא סוקר את אבני הליבה של ארכיטקטורה טיפוסית של סביבת רשת תומכת מערך מצלמות האבטחה:



תרשים 2: ארכיטקטורה טיפוסית של סביבת רשת תומכת מערך מצלמות האבטחה.

בהתאם לתרשים לעיל ניתן ללמוד כי ממשק הניהול של מערך המצלמות עשוי להיות בהתקן ה-DVR, וכן במצלמות האבטחה.

לנוכח העובדה כי ממשקי ניהול המצלמות מהווים יעד תקיפה מועדף במרחב הסייבר, וכי רמת ההגנה המובנית במצלמות האבטחה עשויה להיות מגוונת, ישנה חשיבות גבוהה לווידוא כי ממשקים אלו אינם חשופים ישירות לאינטרנט.

2. מטרות ויעדים

מסמך זה מציג דרכי פעולה מומלצות לצמצום סיכוני סייבר ממצלמות אבטחה.

3. קהל היעד

מסמך זה נכתב עבור מנהל הגנת הסייבר בארגון (CISO), מוסמך מתודולוגיות הגנת סייבר, מוסמך מיישם הגנת סייבר, מוסמך טכנולוגיות הגנת סייבר (ארכיטקט הגנה בסייבר), ממונה ביטחון (מנב"ט), ואנשי תקשורת נתונים/תקשוב/SYSTEM IT. גורמים נוספים אשר עשויים להפיק תועלת ממסמך זה הם יועצים משפטיים וגורמים עסקיים הנדרשים לאשר את הערכת הסיכונים של נכס הסייבר/התהליך העסקי.

4. תיחום המסמך

מסמך זה מתמקד בדרכי פעולה מומלצות לצמצום סיכוני סייבר ממצלמות אבטחה. ראוי לציין כי המסמך אינו מרחיב בנושאים שלגביהם מערך הסייבר הלאומי כתב ופרסם מסמכים ייעודיים. דוגמה לנושא מסוג זה הינה הגנה פרטנית על מערכת ותשתית, דבר הזוכה למענה במסגרת מסמך *תורת ההגנה בסייבר לארגון* אשר נכתב ופורסם על-ידי מערך הסייבר הלאומי.
כמו כן, אין מסמך זה מספק כיסוי מלא לסוגיות הנובעות משילוב מצלמות אבטחה בתהליכים מורכבים דוגמת הגנה על תשתית כימית, ביולוגית, רדיולוגית או גרעינית (CERN).

5. איומים הנגזרים מתקיפות כנגד מצלמות אבטחה

פרק זה סוקר את האיומים העיקריים הנגזרים מתקיפות כנגד מצלמות אבטחה, כמפורט להלן:

	שם האיום	תיאור
1.	השתלטות על ממשק ניהול	קיומה של פגיעות (Vulnerability) או הגדרת תצורה לקויה (Misconfiguration) עשויה לאפשר לתוקף להשתלט על ממשק הניהול. להלן סיבות שכיחות המאפשרות ניצול לרעה: א. קיומה של סיסמת ברירת מחדל (Default Password) פעילה. ב. מדיניות סיסמאות חלשה (Weak Password Policy). ג. שימוש בסיסמאות זהות באתרים/שירותים מרובים מעלה את הסבירות לחשיפה גבוהה עקב דליפת סיסמאות. ד. העדר נעילה זמנית חשבון במקרה של תקיפה דוגמת תקיפת סייבר כוחנית ומתמשכת (Brute Force Attack). ה. חשיפה ישירה של ממשק ניהול לאינטרנט (לרבות HTTP, HTTPS, SSH), דבר אשר הופך את המצלמה ליעד זמין לתקיפה. ו. העדר מימוש MFA. ז. קיומה של פגיעות ללא זמינות עדכון אבטחה (פאץ') או אי הטמעת עדכון אבטחה קיים. ח. שימוש בפרוטוקולים עם פגיעות ידועה דוגמת HTTP או Telnet. ט. עבודה עם דפדפנים ישנים לא מעודכנים ללא יכולת שדרוג לגרסה עדכנית עקב אי תאימות טכנולוגית.
2.	חטיפת פעילות משתמש (Session Hijacking)	תוקף עשוי לחטוף פעילות משתמש (User Session), ובכך לקבל גישה למערך המצלמות. להלן מספר דוגמאות למימוש התקיפה:

		א. החדרת נוזקה למחשב המשתמש (לרבות פלאגין לדפדפן), דבר אשר בתורו יאפשר גניבת פרטי הזדהות אשר המשתמש מקליד או שליחת בקשות מסוג SSRF. ב. שימוש בפגיעות מסוג CSRF\XSS לשם שליחת תעבורת המשתמש ליעד הנמצא בשליטת תוקף.
3.	התערבות בתווך (MiTM)	התערבות בתווך לצורך צפייה לא מורשית בנתונים - יכולת התחברות למערכת, השתלטות או האזנה בתווך וצפייה בחומרים או בתוצרי הצילום.
4.	שימוש במצלמה כשער גשר לחדירה לארגון	קיומה של פגיעות (Vulnerability) או הגדרת תצורה לקויה (Misconfiguration) במצלמה עשויה לאפשר חדירה לארגון, וביצוע תקיפות המשך.
5.	שימוש במצלמה כשער גשר לחדירה לטלפון נייד אשר מותקנת בו אפליקציית ניהול	קיומה של פגיעות (Vulnerability) או הגדרת תצורה לקויה (Misconfiguration) במצלמה עשויה לאפשר חדירה לטלפון נייד אשר מותקנת בו אפליקציית ניהול, וביצוע תקיפות המשך.
6.	שימוש בתחנת הצפייה כשער גשר בין רשתות בעלות רמות אמון שונות	משתמש עשוי לחבר את תחנת הצפייה לרשתות בעלות רמות שונות, דבר אשר עשוי ליצור פער אבטחתי והזדמנות לתוקף.
7.	ניצול לרעה של רכיבי אפליקציה צד-לקוח	ניצול לרעה של רכיבי אפליקציה צד-לקוח. להלן סקירה של דרכי פעולה שכיחות: א. ביצוע איסוף מודיעיני באמצעות יכולות מובנות באפליקציה.

		ב. ניצול הרשאות יתר של האפליקציה לשם פגיעה בסודיות, זמינות או מהימנות ושלמות המידע.
.8	פרסום לא לגיטימי של אפליקציית מובייל ל"ניהול מצלמות"	תוקף עשוי לבצע פרסום לא לגיטימי של אפליקציית מובייל ל"ניהול מצלמות", וזאת במטרה לשטות במשתמשים להתקין תוכנה זדונית.
.9	הזלגת מידע (Data Leakage)	א. תוקף אשר קיבל גישה למצלמות או מערך האחסון עשוי לקבל יכולת להדליף מידע רגיש/חסוי באמצעות רשת התקשוב או חיבור התקן נייד, לדוגמא. ב. תוקף אשר קיבל גישה למצלמות עשוי להשתמש בסנסור (דוגמת מנורת IR או צמצם מצלמה) לשם הזלגת מידע. ג. התקנה במיקום לא נכון או העדר כיוון מספק של סנסור עשויה לגרום לתיעוד של מידע רגיש/חסוי.
.10	קבלת פקודות מרחוק באמצעות הסנסור	תוקף אשר השיג אחיזה מקדימה במערך המצלמות עשוי להשתמש במערך הקלט של הסנסור לשם קבלה מרחוק של פקודות הפעלה לנוזקה שהותקנה על-ידו.
.11	שיבוש או מחיקת הקלטות	א. שיבוש או מחיקת הקלטות על-ידי גישה בלתי מורשית, ביצוע שינויים בתמונות, שינוי ערך שעון כך שמערכת ההקלטה תשכתב מידע היסטורי וכדומה. דבר זה עשוי לפגוע בתורו בראיות משפטיות אשר עשויות לשרת את הארגון או גורם רלוונטי אחר. ב. ראוי לציין כי חלק ניכר מהתקני ה-DVR\NDR אינם כוללים יכולות גיבוי מתקדמות דוגמת "גיבוי קר" מחוץ להתקן. לפיכך ההסתמכות היא על יכולות שרידות ברמת RAID אינה מבטיחה יכולת שחזור של המידע במקרה הצורך.
.12	פגיעה בפרטיות	א. שימוש במצלמות האבטחה לשם מעקב אחר אדם פלוני שלא כדין.

		ב. איתור דפוסי התנהגות משותפים של מספר אנשים. ג. סחיטה באמצעות איום בהפצת מידע רגיש/חסוי אשר נאסף קודם לכן באמצעות מצלמות האבטחה. ד. התקנה במיקום לא נכון או העדר כיוון מספק של סנסור עשויה לפגוע בפרטיות אדם פלוני, דוגמת צילום כניסה לחדר נוחות. ה. ניצול לרעה של יכולות ניהול מובנות במצלמות PTZ לשם הגדלת תמונה או שינוי כיוון הצילום. ו. הפעלת סנסור ללא ידיעה ו/או אישור גורם מוסמך (Camfecting).
13.	הפעלה לא תקינה שמביאה לשגיאות מערכת, אשר עלולות להביא לפגיעה בזכויות אדם, או שגיאת מערכת שעלולה להביא להעדר ראיות/תוצאות הנדרשות להליך משפטי	א. העדר יכולת לקביעת אינדיקציה מדויקת לזמן קרות אירוע, דבר אשר עשוי לנבוע מתהליך סנכרון זמן לקוי. ראוי לציין כי סוגיה זו עשויה להיות בעלת השפעה קבילות ומשקל ראייתי במסגרת הליכים משפטיים. ב. "הטרדת תמימים" למול "פספוס חשודים".
14.	גניבה פיזית	גניבה פיזית של מצלמה או יחידת האחסון המכילה מידע רגיש/חסוי דוגמת הקלטה.
15.	פגישה פיזית / חבלה	פגיעה בעדשת המצלמה, הסטה פיזית של המצלמה מגזרת הצפייה שלה, ריסוס פני העדשה בצבע או ביצוע חבלה אחרת.
16.	התקפות מקוונות לצורך השבתה או	השתלטות עוינת ופריצה לצורך השבתת פעילות מצלמות האבטחה. באירועים רבים, ביצע התוקף השתלטות על מצלמות, השבית

	מניעת גישה למערכת	פעילות ושינה את סיסמאות הגישה אליהן. במקרים אחרים אף בוצעו התקפות כופר על המצלמה וכדומה.
17.	סיכון ביטחוני למדינת ישראל במיקוד לביטחון כוחותינו	תוקף אשר קיבל גישה למצלמה או ההקלטה עשוי להשתמש בהם לשם סיכון ביטחוני למדינת ישראל במיקוד ביטחון כוחותינו, דוגמת איתור מיקום כוחות בזמן אמת או מיפוי שגרות ביטחון.
18.	ניצול תשתיות של מצלמות לטובת תקיפה של צד-שלישי / אפידמיה סייבר	תוקף עשוי לנצל פגיעות לשם הפיכת המצלמה לבוט (Bot) הניתן להפעלה לטובת תקיפת סייבר של צד-שלישי, דוגמת תקיפת מניעת שירות מבוזרת (DDoS) / אפידמיה סייבר.
19.	אי עמידה בדרישות חוק ורגולציה	א. פלט מצלמות האבטחה עשוי להוות "מאגר מידע" בהתאם לחוק. אי נקיטה בפעולות אבטחה בהתאם לנדרש עשוי להוות הפרה חוקית/רגולטורית. ב. שיבוש או מחיקה של הקלטה עשוי להוות הפרה חוקית/רגולטורית, דוגמת מחיקה של ראיה משפטית. ג. אחסון פלט מידע ממצלמות האבטחה בשירות ענן הנמצא במדינה זרה, וזאת בניגוד לדרישות החוק והרגולציה. ד. שמירת מידע רגיש/חסוי ללא צורך ממשי. ה. ביצוע האזנת סתר. ו. מתן גישה למערך המצלמות לגורמים לא מורשים. להרחבה בנושא זה, ראו את עמדת הרשות להגנת הפרטיות בלינק: https://www.gov.il/he/departments/general/surveillance_cameras_info
20.	הטמעת מידע כוזב בהקלטה	תוקף עשוי להטמיע מידע כוזב במאגר צילום/הקלטה במטרה להפליל אדם או לטובת מטרה אחרת.

.21	ניצול לרעה של פגיעות במנגנוני עדכון תוכנה	תוקף עשוי לנצל לרעה פגיעות במנגנון עדכון תוכנה. להלן סקירה של דרכי פעולה שכיחות: א. טעינה מקומית של קושחה (Firmware) זדונית ב. טעינה מרחוק של קושחה זדונית ג. ניצול פגיעות בפרוטוקול FOTA\SOTA
.22	מניפולציה על תעבורת נתונים	ביצוע מניפולציה על תעבורת נתונים וזאת לשם קבלת הישג עבור התוקף. להלן סקירה של דרכי פעולה שכיחות: א. הקלטה, ושידור מחדש של תעבורת נתונים היסטורית. ב. הזרקת פקודות/קוד זדוני/נוזקה במסגרת פעילות (Session) קיימת או חדשה. ג. שינוי ניתוב רשת לשם העברת תעבורה דרך נכס סייבר הנמצא בשליטת תוקף. ד. ביצוע מניפולציה לתעבורה וזאת במטרה לגורם למנגנון עדכון התוכנה הקיים במערך המצלמות למשוך עדכון זדוני מאתר הנמצא בשליטת תוקף.
.23	הטמנה חומרתית או תוכנתית (Implant)	תוקף (לרבות היצרן) עשוי לבצע הטמנה חומרתית או תוכנתית, ובכך לשלב דלת אחורית (Backdoor), כפתור אדום (Red Button) או פצצה לוגית (Logic Bomb).
.24	מניפולציה על אלגוריתמים (דוגמת AI) של מערך האנליטיקה	תוקף עשוי לבצע מניפולציה על אלגוריתמים (דוגמת AI) של מערך האנליטיקה. להלן סקירה של דרכי פעולה שכיחות: א. מצג שווא (Presentation Attack) - הצגה של תמונה מודפסת או מוטבעת או מוקרנת של ישות דוגמת אדם או לוחית רכב.

		ב. שידור חוזר (Replay Attack) של סרטון המכיל תיעוד ישות דוגמת אדם. ג. שימוש במסכה תלת-ממדית (3D Mask Attack) לשם שחזור תכונות של פני-אדם או לשם הימנעות מזיהוי. ד. הלבשת "רעש" (לרבות רעש פיזי) המשבש את עבודת האלגוריתם או מערכת הצילום. ה. "זיוף עמוק" (Deepfake) - שימוש בתוכנת מחשב המסוגלת ליצור סרטון או תמונה סינתטיים, המייצגים אדם באופן מציאותי, וזאת לשם יצירת מצג שווא כי מדובר בסרטון לגיטימי. ו. ניצול פגיעות באלגוריתם לשם הסתרת פעילות זדונית או יצירה של אירוע כוזב. ז. שיבוש חוקי האנליטיקה. כגון הסטת גזרת הצפייה של המצלמה, שינוי/מחיקה של חוק האנליטיקה להרחבה בנושא ראו מסמכי עזר[2].
25.	ציתות (Eavesdropping)	תוקף עשוי ליירט מידע העובר על גבי רשת ציבורית (דוגמת האינטרנט), ולאחר מכן לבצע פעולות שונות במטרה לפענחו.

טבלה 5: איומים עיקריים הנגזרים מתקיפות כנגד מצלמות אבטחה.

ראוי לציין כי הרשימה לעיל אינה סוקרת את כל האיומים הנגזרים משימוש בשירותי ענן. לנוכח זאת לטובת מיפוי כלל האיומים. מומלץ לעיין בספרות מקצועיות ומתודולוגיות מקובלות MITRE ATT&CK Cloud Matrix[3] ומסמכי ארגון Cloud Security Alliance (CSA)[4].

[2] MITRE | ATLAS
https://atlas.mitre.org/
Securing Machine Learning Algorithms, ENISA, December 14, 2021
https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms
[3] MITRE ATT&CK Cloud Matrix
https://attack.mitre.org/matrices/enterprise/cloud/
[4] Top Threats
https://cloudsecurityalliance.org/research/working-groups/top-threats/

6. דרכי פעולה מומלצות - צמצום סיכוני סייבר ממצלמות אבטחה

פרק זה מציג רשימה של דרכי פעולה מומלצות, שמימוש נכון שלהן יסייע בצמצום סיכוני סייבר ממצלמות אבטחה, כמפורט להלן:

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	אבטחה פיזית	
1.	מומלץ כי הארגון ינקוט בפעולות מקובלות למניעת גישה פיזית למערך המצלמות. להלן דוגמאות ליישום: א. התקנה של המצלמה בגובה, כך שאדם לא יוכל לגשת אליה ללא עזר ב. התקנה של המצלמה בארון חסין חבלה (Tamper Resistance), תוך מימוש מנגנון לחשיפת חבלה (Tamper-Evident) דוגמת העברת התראה באמצעות מערכת אזעקה. ג. הסלקת מכשיר ההקלטה באופן שיקשה על איתורו וגניבתו. ד. התקנת נקודות רשת וכבילה באופן מוסלק באזורים חיצוניים או באזורים בעלי נגישות ציבור. ה. שימוש במדבקות אינדיקציה על פתחים/חיבורים/הברגות, תוך ביצוע ביקורות תקופתיות לאיתור ניסיונות גישה לא מורשים. ו. ניתוק פיזי של כבילה שאינה חיונית מנקודות הרשת של מתג התקשורת (Switch). ז. שימוש במצלמות דמה לשם שיפור רמת הנראות של מערך המצלמות.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ח. וידוא כי ישנה חפיפה בין אזורי הצילום של המצלמות, כך שניתן יהיה לגלות ולזהות בזמן אמת ניסיונות גישה לא מורשים למצלמה.	
2.	מומלץ כי הארגון יוודא כי המצלמה כוללת יכולות מובנות לחסימת חבלה, וחשיפת חבלה.	
3.	מומלץ כי הארגון ינקוט בפעולות מקובלות כך שגם אם תוקף קיבל שליטה על מצלמה או הקלטה, היכולת שלו להפיק מידע ערכי אודות שגרות ביטחון תהיה נמוכה ככל הניתן. דוגמאות ליישום: א. ביצוע סיורי גדר שלא בהתאם למתווה הניתן לחיזוי. ב. ביצוע פעולות ליצירת נראות. ג. כיוון המצלמה לאזורים אשר אינם מתעדים שגרות ביטחון רגישות. ד. שימוש באמצעי הסוואה (Cloaking Devices) פסיביים או אקטיביים.	
4.	מומלץ כי הארגון יוודא מתן גישה למערך המצלמות למשתמשים וזאת רק לאחר השלמת בדיקות רקע הנדרשות בהתאם לחוק. דוגמא ליישום: ביצוע בדיקות רקע בהתאם לדרישות חוק למניעת העסקה של עברייני מין במוסדות מסוימים, תשס"א-2001.	
5.	מומלץ כי הארגון יוודא יישום של הגנה פיזית וזאת בהתאם לעקרונות CPTED (Crime Prevention Through Environmental Design). בכלל זה, מומלץ כי המנב"ט ישולב בתהליך זה.	
6.	מומלץ כי הארגון יבצע סיור עתי לווידוא שלמות מבנית של מצלמות האבטחה.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.7	מומלץ כי הארגון יוודא כי מצלמות האבטחה מותקנות כך שתהיה חפיפה בין אזורי הצילום, כך שניסיון גישה לא מורשה למצלמה פלונית יתועד ויאותר על-ידי מצלמה אלמונית.	
.8	מומלץ כי הארגון ישקול שימוש במצלמות אבטחה מוסוות לשם הורדת רמת החשיפה.	
.9	מומלץ כי הארגון יבטיח עמידה של מצלמות האבטחה בתנאים האופייניים לסביבת הפעולה ותנאי קיצון דוגמת חוסן בפני אלימות פיזית. להרחבה מומלץ לעיין בתקנים הבאים: A. IEC 60529 - DEGREES OF PROTECTION PROVIDED BY ENCLOSURES (IP CODE) B. IEC 62262:2002 - Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code) C. IEC 60068-2-75:1997 - Environmental testing - Part 2-75: Tests - Test Eh: Hammer tests D. U.S. EMI MIL-STD-461E E. U.S. MIL-STD-810	
	בקרת גישה לוגית	
.10	מומלץ כי הארגון יוודא כי מערך המצלמות (מצלמה, DVR וכדומה) אינו חשוף לאינטרנט. בהינתן כי נדרשת גישה מרחוק מומלץ לנקוט בצעדים הבאים: א. מתן גישה בהתאם ל-Allowlist פרטני של כתובות מורשות. ב. מתן גישה באמצעות שימוש ב-VPN או SDP.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	ג. אירוח דף המצלמה כ-Iframe, וחשיפתו כדף אתר אינטרנט המוגן באמצעות WAF ו-IPS.	
11.	מומלץ כי הארגון יוודא כי הגישה למערך המצלמות מוקנית בהתאם לעקרון מתן רמת גישה נמוכה (Least Privilege Access), וזאת החלת בקרת גישה הן ברמת ה-FW הארגוני, והן ברמת ההתקן עצמו (מצלמה, DVR וכדומה).	
12.	מומלץ כי הארגון יוודא באופן עתי כי כתובת המצלמה אינה רשומה בשירותי מודיעין סייבר (CI).	
13.	מומלץ כי הארגון יוודא כי מערך המצלמות מוטמע בסגמנט או VLAN ייעודי שאינו מקושר לנכסי הסייבר האחרים של הארגון. בארגון בעל רמת סיכון בינונית ומעלה מומלץ לכל הפחות לממש Microsegmentation.	
14.	מומלץ כי הארגון יוודא באופן רציף כי לא ניתן לחבר לרשת המצלמות נכסי סייבר לא מורשים, וזאת על-ידי שימוש באלמנט זיהוי חד-ערכי של נכס הסייבר, אשר לא ניתן בקלות לזייפו או לשכפלו. דוגמא ליישום: מימוש פרוטוקול 802.x במערך תקשורת הנתונים תוך שימוש במערכת NAC, ותהליך אימות מבוסס פרוטוקול EAP-TLS.	
15.	מומלץ כי הארגון לא יעשה שימוש ברשת אלחוטית לשם קישור בין רכיבי מצלמות האבטחה.	
16.	מומלץ כי הארגון יוודא כי גישה לממשק הניהול תתבצע מתוך הארגון וזאת באמצעות רשת OOB.	
17.	מומלץ כי הארגון יוודא תעבורת מצלמות האבטחה הזוכה לתעדוף, כך שבמקרה של אירוע סייבר או עומס חריג, ניתן יהיה לגשת לממשק הניהול.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	דוגמא ליישום: שימוש במנגנון QoS.	
18.	מומלץ כי הארגון יוודא כי נקודות רשת שאינן פעילות יוגדרו במתג התקשורת ב"מצב קר" (Shutdown).	
19.	מומלץ כי הארגון יוודא כי בעת שימוש ברשת סלולרית לשם ניהול מערך המצלמות נעשה שימוש בתשתית APN, שאינה בעלת גישה לאינטרנט. להרחבה ראו: אבטחת תשתית APN - המלצות ליישום. מערך הסייבר הלאומי (ספטמבר 2020) https://www.gov.il/he/departments/general/apn	
	הקשחת מערכת	
20.	מומלץ כי הארגון יוודא כי במסגרת פיתוח המוצר היצרן מימש עקרונות מקובלים לעיצוב מאובטח, ולעיצוב לפרטיות.	
21.	מומלץ כי הארגון יחסום אפשרות לעבודה עם פרוטוקולים פגיעים. להלן דוגמא לפרוטוקולים פגיעים: א. HTTP ב. Telnet ג. TFTP ד. FTP ה. SSL ו. TLS v1.0 ז. TLS v1.1	

מס'		ההמלצה	סטאטוס (בוצע/לא בוצע)
	ח. SNMP v2 ט. UPnP		
22.	מומלץ כי הארגון יחליף את התעודה הדיגיטלית שמגיעה באופן מובנה (ברירת מחדל) בתעודה ייעודית למטרה זו.		
23.	מומלץ כי הארגון יוודא עיקור או חסימה של ממשקים פיזיים שאינם נדרשים לעבודה שוטפת דוגמת ממשק USB, ממשק RS-232 וממשק RS-485. דוגמא ליישום: שימוש בחסם פיזי למניעת חיבור לא מורשה לממשק USB		
24.	מומלץ כי הארגון יוודא קיומה של תמיכה פעילה בתהליך אתחול המוודאת את מקוריות ומהימנות רכיבי התוכנה, וזאת החל משלב ההפעלה ועד להשלמת טעינת מערכת ההפעלה (Secure Boot).		
25.	מומלץ כי הארגון יוודא כי פעולות קריפטוגרפיות מתבצעות ברמת מעבד (Chip) ההתקן, ולא ברמת מערכת ההפעלה/האפליקציה. דוגמא ליישום: שימוש ב-TPM.		
26.	מומלץ כי הארגון יוודא כי אחסון מפתחות קריפטוגרפיים נעשה בהתקן חומרה ייעודי מוקשח, אשר מונע אפשרות לייצוא המפתח. דוגמא ליישום: שימוש ב-TPM.		
27.	מומלץ כי הארגון יבצע בדיקה עיתית רציפה לאיתור חריגות בהגדרות תצורה וקבצים. דוגמא ליישום: מימוש FIM.		

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.28	מומלץ כי הארגון יוודא סנכרון של שעון רכיבי מערך המצלמות מול שעון זמן מהימן פנים ארגוני.	
.29	מומלץ כי הארגון יוודא כי המשתמש אינו יכול לשמור את פרטי ההזדהות בצד-לקוח (דוגמת שם משתמש וסיסמה בדפדפן), וזאת במטרה למנוע אפשרות לביצוע Login אוטומטי.	
	חשבונות משתמשים ופעילות (Session)	
.30	מומלץ כי הארגון יוודא כי לא נעשה שימוש בסיסמאות ברירת מחדל (Default Password), סיסמאות זהות באתרים/שירותים שונים או סיסמאות קלות לניחוש. כבקרה מונעת מוצע לרכוש מצלמות שכוללות מנגנון מובנה של שינוי סיסמת ברירת מחדל.	
.31	מומלץ כי הארגון יחיל מדיניות סיסמאות בהתאם לצרכיו.	
.32	מומלץ כי הארגון יוודא כי הסיסמאות אינן מאוחסנות באופן גלוי (Cleartext) בהתקן. דוגמא ליישום: וידוא כי היצרן מימש מנגנון לאחסון סיסמאות הכולל מימוש ב-Hash + Dynamic Salt.	
.33	מומלץ כי הארגון יעשה שימוש ב-MFA, בהינתן כי הדבר ישים.	
.34	מומלץ כי הארגון יוודא החלת נעילת חשבון משתמש (Account Lockout) לאחר 5 ניסיונות הזדהות לא מוצלחים, וזאת למשך 60 דקות לפחות.	
.35	מומלץ כי הארגון יוודא ניתוק מצד שרת של חשבון משתמש שאינו פעיל מעל 5 דקות.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.36	מומלץ כי הארגון יוודא הגבלה של מספר הפעילויות אשר חשבון משתמש מסוגל לעשות בהן שימוש בזמן נתון (Session Throttling).	
.37	מומלץ לוודא החלת עקרון מתן הרשאות נמוכות (Least Privilege) ומתן גישה בהתאם לעקרון הצורך לדעת (Need to Know). בכלל זה התייחסות להרשאת צפייה בזמן אמת (Live), עיון בהקלטה, שידור חוזר (Playback), הוצאת סרטון, ארכיון, שימוש ביכולות המצלמה, וכדומה. בכלל זה מומלץ לבצע הפרדה בין בעלי תפקיד שונים על-ידי שימוש ב-RBAC או מודל אחר.	
	הגנה על מידע	
.38	מומלץ כי הארגון יוודא הצפנה של מידע רגיש/חסוי במנוחה (At Rest). ראוי לציין כי חלק מיצרני הפתרונות מממשים דרישה זאת כחלק מתהליך הקידוד (Encoding) של ההקלטה.	
.39	מומלץ כי הארגון יוודא כי הגישה לממשקי הניהול ושינוע המידע בתווך (In Transit) מתאפשרים בכפוף להחלת הצפנה עדכנית וסטנדרטית. דוגמא ליישום: שימוש בפרוטוקול TLS v1.3 ואלגוריתם AES 256 Bit לטובת הצפנה סימטרית.	
.40	מומלץ כי הארגון יוודא כי סיסמת המשתמש אינה נשלחת As is על התווך. דוגמא ליישום: שימוש ב-Digest Authentication	
.41	מומלץ כי הארגון יוודא כי בזמן אמת ההקלטה נחתמת דיגיטלית ו/או מתווסף לה חתימת מים (Watermark) ייעודי לכל חַלוֹנִית (Frame), וזאת במטרה לוודא וידוא מקוריות, מהימנות ושלמות של ההקלטות.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
42.	מומלץ כי הארגון יוודא כי שמירת המידע שנקלט במצלמה ועיבודו עומד בהוראות החוק הרלוונטיות, ובכלל זה חוק הגנת הפרטיות והתקנות מכוחו.	
43.	מומלץ כי הארגון יוודא את מיקום ואופן אחסון המידע שנקלט במצלמה ומעובד על ידה.	
44.	מומלץ כי הארגון יוודא עם הספק/יצרן אם יש לו נגישות למידע שמוקלט ומעובד על ידי המצלמה. אם כן, ואם אין ברירה להשתמש במצלמה כאמור, מוצע לוודא מה השימושים שהוא יכול לבצע במידע ומי יכול לבצע את השימוש.	
45.	מומלץ כי הארגון יבצע באופן עתי בדיקה לאיתור ניסיונות להדלפת מידע רגיש/חסוי באמצעות הסנסורים הקיימים במצלמה.	
	תפעול שוטף	
46.	מומלץ כי הארגון יוודא מחיקה עתית של מידע שאינו נדרש לעבודה שוטפת (Data Minimization) או העברה של המידע למערך אחסון בעל רמת אבטחה גבוהה יותר.	
47.	מומלץ כי הארגון יוודא כי לא ניתן למחוק או לשנות הקלטות ומידע רלוונטי במשך תקופה מוגדרת (Data Retention). במקרה של העדר תמיכה מובנית על-ידי מערך המצלמות ניתן לממש המלצה זאת על-ידי יכולות אבטחה הקיימות במערכי אחסון מקובלים.	
48.	מומלץ כי הארגון יטמיע עדכוני אבטחה (פאצ'ים) בהתאם לתדירות המומלצת על-ידי היצרן. בכלל זה, מומלץ לוודא כי מנגנון התקנת עדכוני האבטחה מבצע בדיקה של מקוריות (Authentic) ומהימנות רכיב התוכנה לפני ההטמעה בפועל. בכלל זה, מומלץ לקבל פרטי קשר של נציג הספק/היצרן של המצלמה לבירורים ועדכוני אבטחה.	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
49.	מומלץ לוודא כי היצרן מספק עדכוני אבטחה, ומומלץ לוודא את מועד הפסקת עדכוני אבטחה מטעם היצרן (EOL). אם היצרן לא מספק עדכוני אבטחה אז מומלץ להימנע מרכישת המוצר.	
50.	מומלץ כי הארגון יוודא גיבוי עיתי של נתוני מערך המצלמות, לרבות הקלטות והגדרות תצורה מחוץ למערך הארגון.	
51.	מומלץ כי הארגון יעביר את הלוגים למערך המצלמות למערכת ה-SIEM הארגונית, תוך הגדרת התראות רלוונטיות. דוגמאות ליישום: א. שימוש בפרוטוקול Syslog ב. שליחת התראה במקרה של חיבור התקן לא מורשה לרשת מערך המצלמות. ג. שליחת התראה בגין אירוע סייבר רלוונטי.	
52.	מומלץ כי הארגון יגדיר באמצעות חוקי האנליטיקה התרעה על הסטת מצלמה, הסרת מצלמה, הפסקת פעולה של מצלמה, פגיעה באיכות הצילום ואירועים חריגים רלוונטיים אחרים.	
53.	מומלץ כי הארגון יבצע הדרכות מודעות שוטפות למשתמשים תוך סקירה של דרכי פעולה אפשרויות של תוקף, ודרכי התמודדות מקובלות. בכלל זה יש לוודא כי המשתמשים מודעים למשמעויות של צילום מתחם העבודה דוגמת האפשרות כי עדשת המצלמה תקלוט מידע רגיש/חסוי.	
54.	מומלץ כי הארגון יוודא גריטה של מצעי אחסון מידע, דוגמת דיסק קשיח, בהתאם לדרישות תקן ISO/IEC 21964, רמה 4.	
	אבטחת מכרזים והתקשרויות / אבטחת שרשרת אספקה	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
.55	מומלץ כי הארגון יוודא כי במסגרת מכרזים והתקשרויות הוא מעגן משפטית את עמידת הספקים בדרישות מתודת הגנה על שרשרת אספקה מטעם מערך הסייבר הלאומי. להרחבה בנושא ראו: מדריך שאלון ספקים לחיזוק שרשרת אספקה https://www.gov.il/he/departments/guides/supply_chain_guide	
.56	מומלץ כי הארגון יעגן במסגרת הסכם ההתקשרות כי מצעי אחסון מידע, דוגמת דיסק קשיח, לא יוחזרו לספק/ליצרן.	
.57	מומלץ כי הארגון יגדיר בנוהל עבודה תהליך סדור ומידי של החלפת סיסמאות בתום פעילות גורם חיצוני. דוגמא ליישום: בסיום טיפול בתקלה יתבצע הליך מידי להחלפת כל הסיסמאות של כלל החשבונות אשר גורם התמיכה החיצוני נחשף אליהן.	
	דרכי פעולה מומלצות - מתקדם	
.58	מומלץ כי הארגון יוודא כי מערך המצלמות בעל הסמכות הבאות: א. FIPS-140-2 ב. ISO 15408 EAL 2 (Common Criteria) ומעלה	
.59	מומלץ כי הארגון יוודא כי מנגנוני האנליטיקה חסינים מפני תקיפות מקובלות כנגד אלגוריתמים מסוג בינה מלאכותית.	
.60	מומלץ כי הארגון יוודא כי בתהליכים רגישים (דוגמת זיהוי פנים) מערך המצלמות עושה שימוש בשיטות פסיביות ואקטיביות לאיתור "חיות" (Liveness Detection). דוגמאות ליישום:	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	א. שימוש בו-זמני בשתי מצלמות בלתי תלויות ו/או מנגנון פוקוס לשם הבחנה בין תמונה תלת ממדית של אדם, לתמונת אדם דו-ממדית (מוקרנת או מודפסת). ב. שילוב סנסור IR במצלמה, וזאת לשם בחינת השוני בין רמת ההחזר הצפויה מעור אדם, לבין רמת ההחזר הצפויה מחומר סינטטי. ג. שימוש בו-זמני במצלמה אופטית ומצלמת IR אקטיבית, תוך בדיקת התאמה ביומטרית ורמת השוני בטמפרטורה בנקודות יחוס אקראיות בגוף האדם.	
61.	מומלץ כי הארגון יוודא כי מנגנוני האנליטיקה המשמשים לטובת תהליכי זיהוי אדם עומדים בתקנים מקובלים לבחינת חסינות בפני ניסיונות התחזות/זיוף. להרחבה ראו: ISO/IEC 19795 - תקן כללי לבחינה של מערכות ביומטריה ISO/IEC 30107 - תקן לבחינה של המנגנון לגילוי זיופים במערכות ביומטריה	
62.	מומלץ כי הארגון יקצה מתגי תקשורת תומכי POE ייעודים למערך המצלמות.	
63.	מומלץ כי הארגון יוודא כי גישה ל-API של מערך המלצות מתבצעת דרך רכיב אבטחה מתווך האוכף Positive Security. דוגמא ליישום: שימוש ב-API GW.	
64.	מומלץ כי הארגון יוודא כי התעבורה של מערך המצלמות עושה שימוש בשתי שכבות הצפנה בלתי תלויות. ראוי לציין כי המלצה זו מהותית ביחוד כאשר הכבילה עוברת באזורים פומביים ו"באזורי גדר".	

מס'	ההמלצה	סטאטוס (בוצע/לא בוצע)
	דוגמאות ליישום: א. שימוש בפרוטוקול IPsec ו-TLS v1.3. ב. שימוש בפרוטוקול MACsec (IEEE 802.1AE) ו-TLS v1.3.	
65.	מומלץ כי הארגון יבצע בקרה רציפה ומתמשכת (Continuous Monitoring) לטלמטריה של מערך המצלמות. במקרה הצורך ניתן להיעזר בספק שירות חיצוני לטובת הנושא.	
66.	מומלץ כי הארגון יוודא חסינות של מערך המצלמות ומתחמי העבודה רגישים כנגד תקיפת דופק אלקטרומגנטי (EMP). להרחבה ראו: Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment v2.2, National Cybersecurity and Communications Integration Center. (February 2019). https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf	

טבלה 6: דרכי פעולה מומלצות - צמצום סיכוני סייבר ממצלמות אבטחה.

מומלץ כי תהליך הרכישה והטמעת מערך המצלמות יזכה לליווי צמוד מצד היועץ המשפטי של הארגון, וזאת לנוכח ההשלכות האפשרויות על פרטיות המשתמשים והציבור הרחב.

לנוכח העובדה כי שכיח לראות בארגונים שמערך מצלמות האבטחה משיק למערכת בקרת מבנה (BMS), מומלץ כי הארגון יכלול התייחסות לנושא זה בבניית מעטפת האבטחה.
להרחבה ראו:
צמצום סיכוני סייבר במערכות בקרת מבנים. (אוקטובר 2020).
https://www.gov.il/he/departments/general/buildingmng

מומלץ כי ארגונים השוקלים שילוב יכולות ביומטריה במערך המצלמות יפנו להתייעצות מקדימה עם היחידה להזדהות וליישומים ביומטריים במערך הסייבר הלאומי.
פרטי הקשר של היחידה להזדהות וליישומים ביומטריים זמינים ב:
https://www.gov.il/he/departments/news/bio_contact

נספח 1 - צמצום סיכוני סייבר ממצלמות אבטחה

מטרת הנספח

לשקף לקורא את אופן פיתוח המסמך ולציין את הגורמים המעורבים בתהליך כתיבתו, ובהעברת משוב על התכנים שלו לצורך הבטחת שקיפות התהליך וגילוי נאות של הגורמים המעורבים בביצועו.

א. כיצד גובש המסמך - סקר שוק/סילבוס/השוואה בעולם

1) בחינה של תיעוד/תקינה מהעולם כגון NIST ו-ISO (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
2) בחינה של פרסומים מקובלים בתחום (דוגמאות עיקריות מוצגות במסמך בפרק "מסמכים ישימים").
3) קבלת משוב מהציבור לטיוטות המסמך אשר פורסמו:
   א. מר טוביה כפיר
   ב. מר גדי בר און, מנכ"ל מגזין securiTech
   ג. בינת יישום מערכות בע"מ
   ד. לדיקו מערכות בטיחות וביטחון - לדיקו בע"מ

7. קיצורי שמות וראשי תיבות

הפרק מציג את קיצורי השמות וראשי התיבות בהם נעשה שימוש במסמך זה.

שם המונח	ביאור
AES	Advanced Encryption Standard
ALPR	Automatic License plate Recognition
API	Application Programming Interface
APN	Access Point Name
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
BMS	Building Management System
CCTV	Closed-Circuit Television
CERN	Chemical, Biological, Radiological and Nuclear
CI	Cyber Intelligence
CPTED	Crime Prevention Through Environmental Design
CSA	Cloud Security Alliance
CSRF	Cross-Site Request Forgery

שם המונח	ביאור
CTO	Chief Technology Officer
DVR	Digital Video Recorder
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EOL	End of Life
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
FOTA	Firmware Over-The-Air
FTP	File Transfer Protocol
FW	Firewall
GPS	Global Positioning System
GW	Gateway
HTTP	Hypertext Transfer Protocol
IEC	Inclusive Engineering Consortium
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IPS	Intrusion Prevention System
IR	Infra-Red
KMS	Key Management Server
LPR	License Plate Recognition
MACsec	Media Access Control security
MIL	Military Standard
MiTM	Man-in-the-Middle Attack
NAC	Network Access Control
NIST	(US) National Institute of Standards and Technology
NVR	Network Video Recorder
OOB	Out-of-Band (Management)
PACS	Physical Access Control System
POE	Power over Ethernet
PTZ	Pan-Tilt-Zoom

שם המונח	ביאור
QoS	Quality of Services
R&D	Research and Development
RAID	Redundant Array of Independent Disks
RBAC	Role-Based Access Control
RF	Radio Frequency
RS	Recommended Standard
SDP	Software-Defined Perimeter
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOD	Segregation of Duties
SOTA	Software Over-The-Air
SSH	Secure Shell \ Secure Point-to-Point
SSL	Secure Sockets Layer
SSRF	Server-Side Request Forgery
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VMD	Video Motion Detection
VMS	Video Management Software
VPN	Virtual Private Network
VSaaS	Video Surveillance as a Service
XSS	Cross-Site Request Forgery
ZLID	Zoom Laser IR Diode
טמ"ס	טלוויזיה במעגל סגור
מכ"מ	מגלה כיוון ומרחק
מנב"ט	ממונה ביטחון

טבלה 7: קיצורי השמות וראשי התיבות בהם נעשה שימוש במסמך זה

8. מסמכים ישימים

פרק זה מכיל את מקורות המידע עליהם הסתמכו הכותבים בעת כתיבת המסמך.

מקורות מידע בעברית:

כללי

גולדשמידט, רועי. "השימוש בטכנולוגיות זיהוי וניטור במרחב הציבורי". *מרכז המידע, כנסת ישראל* (דצמבר 2020)
https://fs.knesset.gov.il/globaldocs/MMM/2503c32b-2f94-ea11-8104-00155d0aee38/2_2503c32b-2f94-ea11-8104-00155d0aee38_11_17635.pdf

כביר, עומר. "מצלמות רחוב חייבות לאזן בין בטיחות הציבור ובין פרטיות". *כלכליסט* (פברואר 2021)
https://www.calcalist.co.il/internet/articles/0,7340,L-3894350,00.html

צורי, מתן. "נתקו מצלמות מהרשת: חשש למתקפת סייבר על יישובי העוטף" (מאי 2021)
https://m.ynet.co.il/Articles/59309910

קאהאן, רפאל. "מתקפת סייבר על קבוצת גולד-בונד השביתה את פעילותה" (ינואר 2022)https://m.calcalist.co.il/Article.aspx?guid=by1m18s0t

"מאסדת הגז עד לרחוב החרדי: האקרים איראניים טוענים כי פרצו למצלמות" (ינואר 2022)https://www.jdn.co.il/flashes/2444/

זמן אמת | עונה 5 - פרק 14 - תחת מעקב
https://www.kan.org.il/Item/ampify.aspx?u=https://www.kan.org.il/item/default.aspx?itemid%3D108065

"הפתרון לשיבושים ולתקלות GPS: מערכת ניווט אינרציאלית"
https://www.geektime.co.il/israel-navigation-independence/

מערך הסייבר הלאומי

"זיהוי פנים במרחב הציבורי - קריאה לאסדרה". *מערך הסייבר הלאומי* (יולי 2021)
https://www.gov.il/he/departments/general/face_recognition

"תורת ההגנה בסייבר 2.0". *מערך הסייבר הלאומי* (יולי 2021)
https://www.gov.il/he/departments/general/cyber_security_methodology_2

"צמצום סיכוני סייבר במערכות בקרת מבנים". *מערך הסייבר הלאומי* (אוקטובר 2020)
https://www.gov.il/he/departments/general/buildingmng

"אבטחת תשתית APN - המלצות ליישום". *מערך הסייבר הלאומי* (ספטמבר 2020)
https://www.gov.il/he/departments/general/apn

"חיזוק זיהוי משתמשים במערכות ותשתיות של ארגונים על-ידי שימוש באימות רב-גורמי (MFA)". *מערך הסייבר הלאומי* (מאי 2020)
https://www.gov.il/he/departments/general/mfa

"תורת ההגנה בסייבר לארגון". *מערך הסייבר הלאומי* (אפריל 2018)
https://www.gov.il/he/departments/policies/cyber_security_methodology_for_organizations

"תפיסה לאומית בסייבר להיערכות ולניהול מצבי משבר". *מערך הסייבר הלאומי* (נובמבר 2018)
https://www.gov.il/he/Departments/news/cybercrisispreparedness

"שאלון ספקים לחיזוק שרשרת האספקה". *מערך הסייבר הלאומי* (מאי 2020)
https://www.gov.il/he/departments/news/querysupply

"מדיניות לאומית להזדהות בטוחה". *מערך הסייבר הלאומי* (מאי 2018)
https://www.gov.il/he/departments/news/bio_safeidpolicy

רשות הגנת הפרטיות

"מדריך הגנת הפרטיות לעיר החכמה". *הרשות להגנת הפרטיות*. (ינואר 2021)
https://www.gov.il/he/Departments/General/smart_city_guide

"היבטי פרטיות הנובעים מחוק התקנת מצלמות לשם הגנה על פעוטות במעונות יום". *הרשות להגנת הפרטיות*. (אוקטובר 2020)
https://www.gov.il/he/departments/news/cameras_daycare_guide

"שימוש במצלמות אבטחה ומעקב ובמאגרי התמונות הנקלטות בהן, הנחיה 4/2012". *הרשות להגנת הפרטיות*. (אפריל 2012)
https://www.gov.il/he/Departments/policies/surveillance_cameras_guidelines

"מצלמות מעקב ומצלמות אבטחה, פסיקה". *הרשות להגנת הפרטיות*. (יולי 2017)
https://www.gov.il/he/Departments/General/verdict8

משרד מבקר המדינה

ההיערכות הממשלתית ליישום טכנולוגיות מתקדמות ברשויות המקומיות - מיזם ערים חכמות, דוח שנתי 70ב, משרד מבקר המדינה (מאי 2020)
https://www.mevaker.gov.il/(X(1)S(rh2cyeb2q5q4phqun2vj2spi))/sites/DigitalLibrary/Pages/Reports/3285-5.aspx?AspxAutoDetectCookieSupport=1

הקמת מערך המצלמות האלקטרוניות ואכיפת חוקי תעבורה, דו"ח מיוחד, משרד מבקר המדינה (פברואר 2016)

https://www.mevaker.gov.il/he/Reports/Pages/495.aspx

חקיקה

חוק התקנת מצלמות לשם הגנה על פעוטות במעונות יום לפעוטות, תשע"ט-2018

תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017

חוק חתימה אלקטרונית תשס"א-2001

תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), תשס"א-2001

חוק למניעת העסקה של עברייני מין במוסדות מסוימים, תשס"א-2001

חוק הגנת הפרטיות, תשמ"א-1981

חוק הארכיונים, תשט"ו-1955

General Data Protection Regulation (GDPR)

PCI Standard

מקורות מידע באנגלית:

General

Atch, David, Gil Regev, and Ross Bevington. "How to proactively defend against Mozi IoT botnet". (August 2021). https://www.microsoft.com/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/

D-Link. "Best Practices in IP surveillance" https://s3-us-west-2.amazonaws.com/itworldcanada/archive/WhitePaperLibrary/PdfDownloads/ITW226_Best%20practices%20in%20IP%20surveillance%20-%20white%20paper%20-%20D-Link.pdf

Guri, Mordechai, Boris Zadov, and Yuval Elovici. "LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED". https://arxiv.org/abs/1702.06715

Guri, Mordechai, Dima Bykhovsky, and Yuval Elovici. "aIR-Jumper: Covert Air-Gap Exfiltration/Infiltration via Security Cameras & Infrared (IR)" https://cris.bgu.ac.il/en/publications/air-jumper-covert-air-gap-exfiltrationinfiltration-via-security-c-3

Guri, Mordechai, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. "xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs" https://arxiv.org/abs/1706.01140

IEC. "60839-11-31 - Video surveillance systems for use in security applications - Part 2-32: Recording control and replay based on web services"

Ilascu, Ionut. "Researchers Hack Surveillance Systems to Show Fake Video Feed". (July 2019). https://www.bleepingcomputer.com/news/security/researchers-hack-surveillance-systems-to-show-fake-video-feed/

Krebs, B. "Hacked Cameras, DVRs Powered Todays Massive Internet Outage". (October 2016). https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

Ronen, Eyal, Colin O'Flynny, Adi Shamir, and Achi-Or Weingarten. IoT Goes Nuclear: Creating a ZigBee Chain Reaction, Weizmann Institute of Science, Rehovot, Israel https://ieeexplore.ieee.org/document/7958578

Moses Staff. "Hacker group released thousands of CCTV & Rafael Defense cameras Israel" https://m.youtube.com/watch?v=oAHoMvN54ik

MITRE | ATLAS https://atlas.mitre.org/

U.S. MIL-STD-810

"Military-Grade Long-Range MWIR/LWIR Thermal & Visible PTZ Surveillance Camera" https://www.infinitioptics.com/cameras/vega

"Recommended standards for the surveillance camera industry". *Biometrics and Surveillance Camera Commissioner.* (October 2018). https://www.gov.uk/guidance/recommended-standards-for-the-cctv-industry

"Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment" v2.2, National Cybersecurity and Communications Integration Center. (February 2019)

https://www.cisa.gov/sites/default/files/publications/19_0307_CISA_EMP-Protection-Resilience-Guidelines.pdf

Bosch

"Secure by design requires a systematic approach". (August 2021).
https://www.boschsecurity.com/xc/en/news/trends-and-technologies/secure-by-design/

"Bosch IP video and data security guidebook v2.0". (April 2021).
https://resources-boschsecurity-cdn.azureedge.net/public/documents/Data_Security_Guideb_Special_enUS_9007221590612491.pdf

"Network Authentication - 802.1x Secure the Edge of the Network". (February 2022).
https://resources-boschsecurity-cdn.azureedge.net/public/documents/WP_802.1x_WhitePaper_enUS_9007221590608267.pdf

Cisco Systems

"SASE breakdown: Using DNS-layer security to block unwanted or malicious content"
https://umbrella.cisco.com/blog/sase-breakdown-dns-layer-security

ENISA

"Beware of Digital ID attacks: your face can be spoofed!, ENISA". (January 2022).
https://www.enisa.europa.eu/news/enisa-news/beware-of-digital-id-attacks-your-face-can-be-spoofed

"Remote Identity Proofing - Attacks & Countermeasures, ENISA". (January 2022).
https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures

"Securing Machine Learning Algorithms, ENISA". (December 2021).
https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms

FLIR

Teledyne. "How Does FLIR Ensure My Security System is Cybersecure?". (March 2021).
https://www.flir.eu/discover/security/thermal/how-flir-cameras-enhance-cyber-protection-and-ndaa-compliance/

FLIR . "FLIR Adds New Advanced Features to United VMS with 9.0.1 Update". (December 2020).
https://www.flir.eu/news-center/security/flir-adds-new-advanced-features-to-united-vms-with-9.0.1-update/

FLIR. "FLIR Announces Thermal Security Camera with Built-In Human and Vehicle Recognition Analytics". (December 2017).
https://www.flir.eu/news-center/security/flir-announces-thermal-security-camera-with-built-in-human-and-vehicle-recognition-analytics/

Hikvision

Hikvision. "Cybersecurity"
https://www.hikvision.com/en/support/cybersecurity/

Hikvision. "Securing a New Digital World with Zero Trust". (June 2021).
https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. "Product Security White Paper". (July 2019).
https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. "Cybersecurity White Paper 2019" December. (July 2019).
https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. "Product Security Long-term Support Policy". (December 2018).
https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. "Hikvision's White Paper on GDPR". (June 2018).
https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. “Hikvision Focuses on GDPR Compliance”. (May 2018). https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. “Hikvision’s White Paper on Cybersecurity”. (January 2018). https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

Hikvision. “Establishing Cybersecurity Assurance System for Video Surveillance Products”. (January 2017). https://www.hikvision.com/en/support/cybersecurity/cybersecurity-white-paper/

IEC

IEC 60529 - DEGREES OF PROTECTION PROVIDED BY ENCLOSURES (IP CODE)

IEC 62262:2002 - Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)

IEC 60068-2-75:1997 - Environmental testing - Part 2-75: Tests - Test Eh: Hammer tests

Industry IoT Consortium

“Placing a High Priority on Trustworthy and Secure IIoT Platforms” https://www.iiconsortium.org/wc-security.htm

Carielli, Sandy, Matt Eble, Frederick Hirsch, Ekaterina Rudina, and Ron Zahavi. “Security Maturity Model v1.2”. (May 2020). https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_V1.2.pdf

ISO

ISO/IEC 24745:2022 - ”Information security, cybersecurity and privacy protection – Biometric information protection” https://www.iso.org/standard/75302.html

ISO/IEC 19795-1:2021 - Biometric performance testing and reporting – Part 1: Principles and framework https://www.iso.org/standard/73515.html

ISO/IEC 30107-1:2016 - Biometric presentation attack detection – Part 1: Framework
https://www.iso.org/standard/53227.html

ISO 22311:2012 - "Societal security – Video-surveillance – Export interoperability'
https://www.iso.org/standard/53467.html

NIST

NIST SP 800-27 - "Zero Trust Architecture". (August 2020).
https://csrc.nist.gov/publications/detail/sp/800-207/final

NIST Interagency/Internal Report (NISTIR) - 8172 - "Assessment of Closed Circuit Television Digital Video Recording and Export Technologies". (March 2017).
https://www.nist.gov/publications/assessment-closed-circuit-television-digital-video-recording-and-export-technologies

***** סוף מסמך *****