CONSIST
Business Information Technology

EKRAN
אי אפשר להסתיר דבר!

מערכת הקלטה, ניטור התרעה וניהול בקרת גישה להגנה מהאיום הפנימי

מערכת EKRAN הינה כלי מתקדם לביצוע ניטור מלא של פעילות משתמשים בארגון ולהגנה מפני גניבת מידע וזליגת מידע כתוצאה מפעילות של גורם הפועל עם הרשאות גישה - עובד, קבלן חיצוני, שותף עסקי וכו'. המערכת מבצעת ניטור מלא על ידי הקלטה ותיעוד ויזואלי של הפעולות, איסוף מידע Meta Data חכם ותיעוד מלא של הפעילויות ברשת ה-IT של הארגון כולל כל תחנות העבודה והשרתים.

EKRAN פועלת באמצעות דפדפן הכולל ממשק ניהול נוח וידידותי, מתריעה בזמן אמת אודות כל פעילות חריגה או חשודה, ומספקת כלים מתקדמים מבוססי AI לניהול זהויות ובקרת גישה, וכן נגן וידאו מתקדם הכולל חיפוש מהיר.

הפלטפורמה מספקת תעודת בטחון לכל ארגון המעוניין להגן על נכסיו הדיגיטאלים מפני האיום הפנימי.

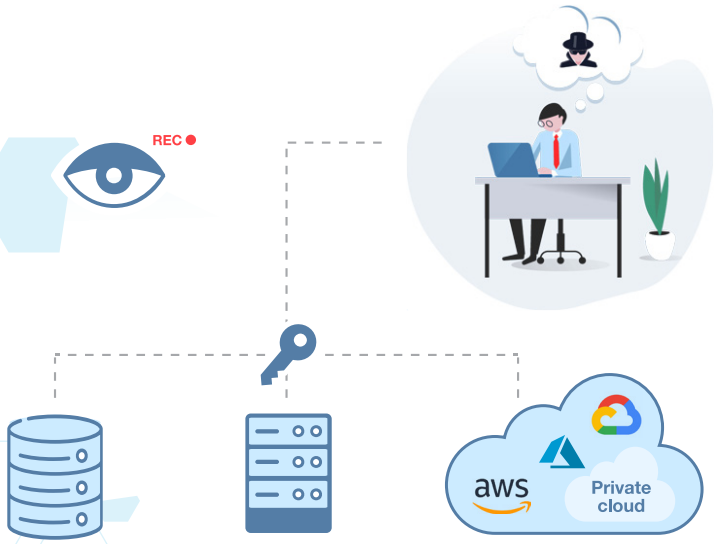
EKRAN נותנת לי שקט ... המערכת עוקבת אחרי ספקים ואם יש חשש מסוים, אני יכול לעקוב אחרי כל דבר.

אורון בירה
מנהל תשתיות ומחשוב בדפוס בארי

האיום הפנים-ארגוני הוא בעל פוטנציאל הנזק ההרסני ביותר

ארגונים משקיעים משאבים רבים בפתרונות אבטחה מתקדמים בכדי להגן על הארגון מאיומים חיצוניים, זאת בעוד שההתקפות ההרסניות ביותר מגיעות במקרים רבים דווקא מבפנים, ממשתמשים בעלי הרשאות גישה לרשת הארגון – עובדים, ספקים ושותפים עסקיים. למשתמשים אלו יש גישה חוקית לליבת היישומים העסקיים ולמידע הרגיש של הארגון, ולכן פוטנציאל הפגיעה של משתמש הפועל מתוך הארגון הוא גדול ביותר.

עם EKRAN אי אפשר להסתיר ממך דבר!



EKRAN היא מערכת לניהול ההגנה על המידע הארגוני ותשתיות ה-IT מפני איומים פנים-ארגוניים. הפתרון ש-EKRAN מספקת עונה על מלוא הצרכים של אבטחת המידע בכל הרמות – החל מתחנת העבודה ועד לשרתים ומערכות הליבה הארגוניות. הפלטפורמה משלבת פונקציות פיקוח והתרעה מקיפות עם מערך כלים מתקדם לניהול גישה ובקרת זהות, מענה ידני ואוטומטי לאירועים ויכולות דיווח מיידיות.

יכולות מתקדמות אלו הופכות את EKRAN לפיתרון משולב ואוניברסלי המאפשר לארגון ליישם את מדיניות אבטחת המידע הארגונית בהיבטים פנימיים.

כמערכת מובילה לניטור איומי פנים, EKRAN מנטרת חשבונות של משתמשים כלליים ופריבלגים, ומספקת טכניקות הגנה מתקדמות כדי להבטיח שאפילו הפעילות ברשת של אנשי ה- IT, בעלי הרשאות גישה מתקדמות, יהיו גלויות לאנשי אבטחת המידע.

EKRAN מאפשרת להגדיר את הסוכן בהתאם להגדרות האבטחה הרצויות והמתאימות לארגון, וכן לתעד פעילות מסוימת ביישום, באתר אינטרנט, לחיצות עכבר ועוד. המערכת מאפשרת גם להפעיל מצב מאובטח בכדי להגן על המידע ולמנוע ממשתמש כלשהו להפסיק את יכולות הניטור.

EKRAN מאפשרת פריסה מהירה ושקטה של סוכנים באמצעות ממשק התקנה מרוחק.

EKRAN - תכונות ויכולות

התרעות ועידכונים

ניתן להגדיר התרעות בזמן אמת עבור כל פעילות חשודה או פוגענית וכן כל הפרה בתחום אבטחת המידע

צפייה בהקלטות

כל פעילות מוקלטת זמינה לצפייה ישירה או בהקלטה, ומספקת מידע מלא אודות הפעילות

דו"חות

ניתן להפיק דו"חות המפרטים את אופן וזמן הפעילות שתועדה וכן לתזמן דוחות מותאמים אישית לכל מידע בו מעוניינים

ניתוח

EKRAN מאפשרת לחקור כל סרטון וידאו ודו"ח פעילות, לאתר במהירות קבצי וידאו ולקבל גישה לפעילות בזמן אמת

*Pushing IT **Forward!***

רח' גרניט 2 קרית אריה ת.ד 4194 פתח - תקוה, 4913000

+972-3-9204111 +972-3-9204112 www.consist.co.il Info@consist.co.il

CONSIST Business Information Technology

ניטור ובקרה מלאים על פעילות המשתמשים ברשת

» הקלטות וידאו של פעילות המשתמשים ברשת – בתחנות הקצה ובשרתים

EKRAN מאפשרת לך להקליט את כל הפעולות של כל המשתמשים ברשת בכל נקודת קצה. המערכת מספקת גם אפשרות להקליט ולסנן על-פי רשומות מבוססות כתובת IP ושם משתמש. פורמט ההקלטה העיקרי הוא הקלטות וידאו עם מספר שכבות של מטא-דאטה, החל משמות היישומים, הקלדות, התקנים מחוברים ועוד. בהתאם לסוג של נקודת הקצה, הקליינט של המערכת מסוגל להקליט משתמש אחד, מספר רב של משתמשים וכן את כל הפעילויות במקביל.

» חיפוש לפי מפתח אירוע

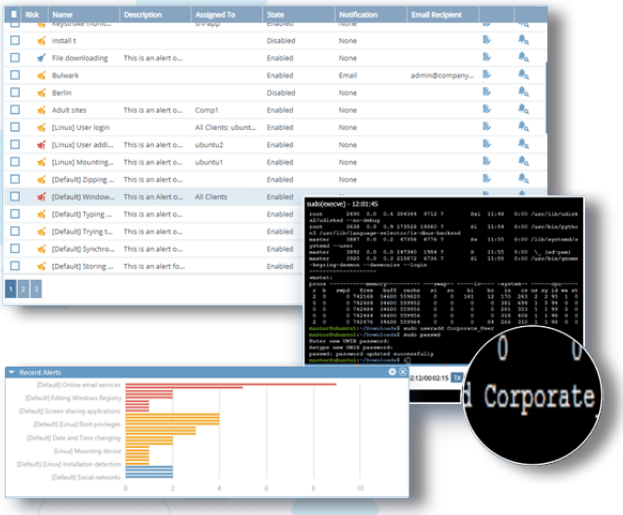
מלבד מתן פרטי החיבור של המשתמשים, המהווה אמצעי חשוב בביקורת של פעילות מרחוק, EKRAN מאפשרת ניתוח נוסף של סוגי הפעילויות השונות. החוקרים יכולים לחפש לפי פרמטרים שונים כגון שם היישום הפעיל, כתובת ה- URL ממנו הגיע הביקור, הפקודה שהוזנה וכן הקלדת טקסט בתוך ההפעלה הנוכחית ובכל ההפעלות שהוקלטו.

הגנה על הניטור

כדי להבטיח ניטור רציף של הפעילות של כל משתמש עם הרשאות גישה בכל רמה שהיא, EKRAN כוללת שילוב חכם של מנגנוני הגנה על תהליכים כדי למנוע כל אפשרות של הפסקת פעילות הניטור על-ידי המשתמש. במידה והחיבור לשרת נופל, הקלטת הפעולות נמשכת באופן מקומי.

לזהות איומים ולהגיב בזמן אמת

EKRAN מספקת מערכת התרעות המבוססות על כללים הניתנים להתאמה אישית בהתאם לנוהלי אבטחת המידע של הארגון. כללים אלו כוללים, בין השאר, אינדיקטורים התנהגותיים של איומי פנים פוטנציאליים, וכן מודול ניתוח התנהגות משתמשים המופעל על ידי AI לאיתור חריגות בפעילות של משתמשים פנים-ארגוניים ובעלי הרשאות גישה.



» התרעות מוגדרות מראש ומותאמות אישית

EKRAN מספקת יכולות מתקדמות לסימון אירועים הנושאים אופי חשוד עם מגוון רחב של תבניות התרעה המכסות את סוגי התרחישים הנפוצים ביותר בהיבט של האיום הפנים-ארגוני. ניתן לשפר כל העת את המערכת באמצעות כללי ההתרעה של הארגון ומגוון פרמטרים של פעילויות: שמות תהליכים, כתובות אינטרנט פתוחות, התקני USB מחוברים, הקלדות ופקודות שבוצעו ועוד.

» ניתוח התנהגות משתמשים ויישויות (UEBA)

מערכת ההתרעות של EKRAN כוללת מודול בינה מלאכותית אשר מודד ומשווה את התנהגות המשתמש אל מול מספר רב של משתנים במטרה לאתר ולזהות באופן המדויק ביותר כל סוג של חריגה מהפעילות הרגילה של אותו משתמש.

» תגובה אוטומטית לאירועים

EKRAN מאפשרת להגדיר סט של פעולות מנע אוטומטיות בנוסף לפעולות הרגילות של שליחת הודעה לחברי צוות אבטחת המידע בארגון. פעולות אלו כוללות שליחת הודעות אזהרה למשתמשים אודות הצורך באישור הפעילות שלהם ברשת, וכן טרמינציה של הפעילות של המשתמש ברשת וחסימה שלו באופן מיידי.

» שליטה בהתקני USB

EKRAN מזהה, עוקבת ומסוגלת להפעיל התרעות בכל פעם שמתבצע חיבור של התקני USB. המערכת גם מספקת ערכת כלים המאפשרת לחסום התקנים וסוגי התקנים ספציפיים בהתאם לרשימות לבנות ורשימות שחורות, וכן להחיל אישור ידני על תרחישים מסוימים לשימוש בהתקני USB.

EKRAN מאפשרת לך לשלוט בגישה לחשבונות המשתמשים

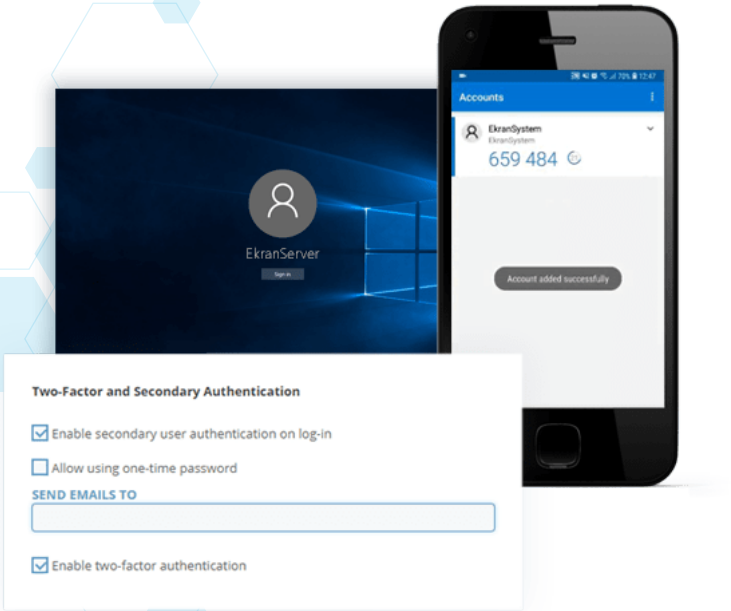
EKRAN מספקת יכולות מתקדמות לניהול הגישה לחשבונות משתמשים מיוחדים וחשבונות משתמשים כלליים, עם שליטה מלאה בניהול חשבונות, סיסמאות ותמיכה בזרימת עבודה בבקשת גישה. EKRAN גם משתלבת באופן מושלם עם מערכת ניהול הקריאות שלך ומאפשרת לאכוף את עקרון הגישה אך ורק בהתאם למטרה.

כדי לנטר ולשלוט באופן מיטבי בזיהוי זהות המשתמש, המערכת מספקת אפשרויות לאימות דו-שלבי אמין ויעיל.

ניטור ומעקב אחר פעילות ספקים ברשת

בנוסף לצורך לנטר ולעקוב אחר הפעילות של עובדי חברה ברשת הארגון, חיוני לא פחות לנטר ולעקוב אחר פעילותם של גורמים מחוץ לארגון המספקים שירותי מיקור חוץ ולכן מחזיקים בהרשאות גישה לרשת ה-IT של הארגון. גורמים אלו יכולים להיות:

- ספקי שירותים מנוהלים.
- ספקי שירותי מיקור חוץ של IT, המכונים לעתים קרובות ספקי IT.
- ספקי צד שלישי מרוחקים.
- מבקרים ומומחים עצמאיים.



גורמים אלו יכולים לנהל את מסדי הנתונים שלך, להגדיר ולתחזק את השרתים והיישומים הקריטיים שלך, לפקח על היקפי אבטחה, לבדוק את פגיעות המערכת ולבצע משימות חשובות אחרות כדי להבטיח המשכיות עסקית. בשל תפקידיהם ומשימותיהם, יש להם גישה מיוחדת לנקודות קצה קריטיות והם בקשר עם מידע רגיש.

מדוע אתה זקוק לפתרון ניטור ומעקב אחר פעילות של גורמים צד ג'?

- כדי לעמוד בדרישות נוהלי אבטחת מידע ותקנות חוק הנוגעות לפרטיות.
- כדי לשלוט בתצורות של מערכות ארגוניות קריטיות ולקבל התרעות על כל שינוי תצורה.
- כדי לאבטח את המידע הרגיש של הארגון.

כאשר ספק IT או ספק צד שלישי מבצע פעולה חריגה או כזו שהיא קריטית לתצורת מערכת כלשהי, EKRAN תתריע ותשלח הודעה מיידית לצוות שלך, עם קישור לאירוע, כדי שתוכל להגיב באופן מיידי.

מלבד התרעה בזמן אמת על כל פעולת משתמש שעלולה להיות מסוכנת, EKRAN מסוגלת גם להודיע על כל חיבור או ניסיון חיבור של משתמש חוץ ארגוני. ניתן להגדיר הודעות של משתמשים ספציפיים לפי שם משתמש או כתובת IP. מערכת ההתרעות של המערכת גם מסוגלת להפעיל פעולות תגובה אוטומטיות לאירוע, כגון סיום פעולה או חסימת משתמש.

מדוע ארגונים מובילים בעולם סומכים על EKRAN?

» **תמיכה מלאה במחשבים שולחניים ושרתים**

EKRAN מספקת תמיכה מלאה במחשבים שולחניים ובשרתים כפלטפורמת תוכנה מבוססת סוכנים. EKRAN תומכת בכל מערכות ההפעלה הפופולאריות ובסביבות וירטואליות כמו גם בארכיטקטורות רשת שונות. באמצעות מערכת EKRAN תוכלו לשלב בין תוכניות מבוססות סוכנים ופריסת שרתי קפיצה.

» **כל הפונקציונליות להגנה מפני איומים פנים-ארגוניים בפלטפורמה אחת**

EKRAN מספקת ניטור פעילות משתמשים וזיהוי אירועים יחד עם פונקציונליות של ניהול זהות ובקרת גישה באמצעות סוכן יחיד המותקן בנקודות הקצה. עם EKRAN, אין צורך בהתקנה והגדרת תצורה של מספר מודולים ותוספים. EKRAN תומכת באופן מלא בתוכנית להפחתת הסיכון שלך בפני איומים פנימיים מכיוון שהיא בנויה בהתאם ל NIST 800-53 ולרוב תקני אבטחת ה- IT.

» **הגנה מקיפה לארגונים מסחריים וממשלתיים כאחד**

EKRAN פותחה במיוחד למעקב אחר פעילות העובדים ברשת ולבקרת הפעילות של קבלני משנה ארגוניים. EKRAN מאפשרת לנטר ולהקליט עשרות אלפי נקודות קצה תוך שמירה על יציבות וביצועים יוצאי דופן. המערכת מספקת זמינות גבוהה ותמיכה בפריסה מרובת משתמשים, לוחות מחוונים למעקב אחר משאבי המערכת ובריאותה ואוטומציה מלאה של פעילויות תחזוקה שגרתיות. מערכת EKRAN מתכוננת בקלות ומתפקדת בצורה מושלמת בתשתיות IT הטרוגניות גדולות.

» **מודל תמחור גמיש המתאים לצרכים של הארגון**

מודל התמחור המיוחד של EKRAN וקונסיסט מאפשר לארגון להתאים את המערכת בהתאם לצורכי הביטחון הייחודיים שלו, החל מביצוע הטמעה בהיקף מוגבל ועד לפרוייקטים ארגוניים רחבי היקף. תכנית הרישוי המיוחדת לתחנות הקצה מאפשרת להעביר רישיונות בין נקודות קצה שונות בלחיצת כפתור, וכל תהליך מתן הרישיונות בארגון הוא אוטומטי וניתן לבצעו במהירות רבה.

אודות קונסיסט - מיישמת EKRAN בישראל

» קונסיסט היא המשווקת והמיישמת הבלעדית של מערכת EKRAN בישראל, והמערכת מותקנת אצל כמה מהארגונים המובילים במשק, כולל ארגונים ביטחוניים.

» קונסיסט מפעילה צוות של מיישמים ותומכים טכנים המספקים תמיכה ויישום ברמה הגבוהה ביותר ללקוחות EKRAN בישראל. לקונסיסט מוקד תמיכה - HELP DESK - המאוייש באנשי מקצוע מהשורה הראשונה.

» קונסיסט בישראל הנה חברת טכנולוגיית מידע בינלאומית מובילה ועתירת ניסיון, המספקת פתרונות, מוצרים ושירותים ליותר מ-700 לקוחות בישראל, ארה"ב ואירופה. בין מאות לקוחות החברה בישראל נמנים הארגונים הגדולים והמובילים במשק, כולל עשרות משרדי ממשלה, חברות אנרגיה, תקשורת, ביטוח ופיננסים, מרבית הבנקים הגדולים, רשויות ומועצות אזוריות, רשתות מזון ארציות, קמעונאים מובילים, המרכזים הרפואיים הגדולים, מוסדות אקדמים, ארגונים מסחריים מקומיים ובינלאומיים, חברות הייטק ועוד. לחברה תחומי עיסוק רבים הכוללים יישום והטמעה של מערכות מחשוב, פיתוח ואינטגרציה של מערכות ותוכנות, פיתוח ותחזוקה של תשתיות מחשוב, שירותי ענן ואבטחת מידע, מיקור חוץ של עובדי הייטק ועוד. לקונסיסט עשרות שנות ניסיון בהטמעה ותחזוקה של מערכות ופתרונות מחשוב.

» קונסיסט בישראל פועלת מזה כ-35 שנה והיא חלק מקבוצת קונסיסט הבינלאומית, שלה יותר מ-1000 עובדים ברחבי העולם ומשרדים ומרכזי פיתוח בגרמניה, ספרד, ארה"ב, ארגנטינה ובישראל. בישראל לחברה יש ארבעה משרדים ומרכזי פיתוח - בפתח-תקוה, אשדוד, לוד ויקנעם והיא מעסיקה כ-400 עובדים.

מקצת מהארגונים המשתמשים במערכת EKRAN