TrackerIQ

מערכת לזיהוי אנומליות אפליקטיביות של משתמשים

TrackerIQ הינה מערכת יחודית לזיהוי אנומליות באפליקציות ארגוניות. היחודיות של המערכת הוא יכולת הניתוח של רצפי התנהגות המשתמשים בצורה מדויקת ומהירה ללא כל צורך בהבנה מוקדמת של תוכן האפליקציה. הפתרון נרשם כפטנט ייחודי לחברה, שרמת הדיוק הגבוהה שלו ממקדת את הארגון בהתראות אמיתיות ומדרגת את הסיכון בהתאם להגדרות רגישות מותאמות לארגון. המערכת נותנת מענה לכל אפליקציה שהיא, on-prem cloud או SaaS ובכל טכנולוגיה שהיא.

האתגרים הקיימים במציאת אנומליות אפליקטיביות

תחום זיהוי פעילויות אפליקטיביות חשודות של משתמשים עבר שינויים משמעותיים בעשור האחרון, ממערכות זיהוי באמצעות אוסף חוקים, למערכות מתקדמות יותר מבוססות סטטיסטיקות ומודלים.

כשרוצים לזהות פעילות חריגה של משתמשים באפליקציות הארגוניות יש צורך בהבנת מהות הפעולה.

האתגר הגדול הוא לקחת את רצף הפעולות האפליקטיביות ולגלות את הסיפור המלא של אותה פעילות חריגה, המסכנת את הארגון ברבדים שלא ניתן לאמוד בכלי החוקים והסטטיסטיקה הקיימים כיום בשוק – המיקוד הוא ברובד המשתמש והתנהגותו האפליקטיבית - Human Layer .

יש פער ביכולת הזיהוי של פעילות אנומלית אפליקטיבית

בזיהוי פעילות עוינת של משתמשים באפליקציות הארגוניות קיים "חור שחור", מאחר והכלים הקיימים לניטור ארועים בשכבת האפליקציה, אינם כלים מתקדמים ואינם עדכניים בטיפול בבעיות מסוג זה. ניתוח פעולות עסקיות מלוגים אפליקטיביים דורש הבנה והיכרות עם האפליקציה והשונות הגדולה בין האפליקציות (הן בהיבט התוכן העסקי והן בהיבט מבנה הלוג) מהווה חסם מרכזי לאפשרויות ניטור גנריות.

המעבר לשימוש באפליקציות ענן)SaaS(העצים את הבעיה וזאת למרות שבדרך כלל קיימים לוגים אפליקטיביים למערכות אלה, אך אין לארגון יכולת לנטר את הלוגים הללו כדי לענות על השאלה, מה מהפעולות שנעשו באפלקציה מלמדות על איום לארגון? במציאות המשתנה בקצב כה מהיר, היכולת לזהות במהירות פעילות חריגה בשכבה האפליקטיבית, הופכת לצורך הכרחי בארגון, ומאפשרת למזער נזקים של פעילות חריגה שעלולה להזיק לארגון) טעות אנוש, מעילה, הונאה, השבתה, גניבת זהות וכיו"ב(.

כיום, מידי יום, נאספת כמות עצומה של נתונים)לוגים(ונשמרת ב Data Lake או בתשתית המערכות עצמן)בסיס הנתונים, שרתים(. הקושי העיקרי הוא לא איסוף הנתונים, אלא היכולת לנתח אותם באופן מהיר ופשוט ולתרגם אותם לתובנות עסקיות מועילות, יעילות ומדויקות ולנהל סיכון ותהליך קבלת החלטות מקצועי.

ניהול סיכונים הפך בשנים האחרונות לחלק אינטגרלי ממפת התפקוד של כל ארגון. בעולם הטכנולוגי ובעולם הסייבר ניהול הסיכון מהווה BaseLine בעיקר בשל המורכבות הטכנולוגית ומתאר האיומים ההולך וגדל.

RevealSecurity מאפשרת ניהול סיכון בקטגוריה של Application Detection Response אשר עד כה לא קיבלה מענה בר יישום לניטור אירועים עסקיים חריגים, אלא באמצעות כתיבת חוקים (Rule-Based) אשר מחפשים אנומליה "מתחת לפנס"- שיטה שאינה יעילה לפעולות לגיטימיות של משתמשי הארגון.

"הסתכל מסביבך - זה שאינך רואה הוא שיפילך"

TrackerIQ

שיטה חדשנית לזיהוי חריגה התנהגותית

TrackerIQ מבוססת על לימוד אוטומטי (מבוסס Machine Learning) של פרופילי הפעילות של משתמשים באפליקציות הארגוניות, אשר בעזרתם המערכת מזהה פעילות אנומלית. המערכת לומדת הן את דפוסי הפעילות האישיים של כל משתמש והן את דפוסי הפעילות של קבוצות המשתמשים בארגון. המערכת בודקת כל רצף פעילות חדש של משתמש ובמידה והרצף אינו תואם את אחד הפרופילים האישיותיים ו/או הקבוצתיים, המערכת תתריע על כך כחריגה ותאפשר תחקור מהיר ויעיל.

לימוד פרופילי הפעילות (Digital profiling) מסתמך על הפעולות אותם מבצעת הישות, סדר הפעולות, ופרקי הזמן בין הפעולות. מכיוון שדפוס הפעילות לאורך session הוא מאפיין ייחודי לכל ישות, ומכיוון שהמערכת לומדת מספר דפוסי פעילות עבור כל ישות, רמת הדיוק באיתור חריגות היא מאד גבוהה ואחוז התרעות השווא הוא נמוך ביותר (עקב האכילס של שאר מערכות הניטור ההתנהגותיות). רמת הדיוק הגבוהה נובעת מהעובדה שהמערכת מאתרת רצפים אנומליים ולא פעולות בודדות, ומתבטאת הן באחוז נמוך מאוד של התרעות שווא (False positives) והן באחוז נמוך מאוד של פעילויות עוינות ש TrackerIQ לא מזהה (False Negatives). את פרופילי ההתנהגות בונה TrackerIQ בצורה אוטומטית על סמך Log events עבור כל משתמש ומערכת שהארגון יבחר לנטר אותה.

TrackerIQ מחשבת לכל אנומליה ציון סיכון המבוסס על הפעולות שבוצעו במהלך הרצף האנומלי ומידת החריגה של הרצף האנומלי תוך שיקלול של רגישות פעולות מסויימות בהתאם להגדרת הארגון.

TrackerIQ אינה שומרת לוגים אלא רק את אלה הקשורים לאנומליות שהתגלו (לצרכי תחקור האירוע) ויודעת "לגשת" לכל לוג שהארגון רוצה לנטר, בין אם הוא מקומי (on-prem) ובין אם הוא ענני (SaaS).

TrackerIQ אינה דורשת כל התקנה על שרתי הארגון (Agentless).

היתרונות של TrackerIQ

- המערכת מזהה כל פעילות עוינת / חריגה ברמת האפליקציה.
- הפתרון מאפשר לנטר כל לוג אפליקטיבי ולא מצריך פיתוח מודלים או הגדרת חוקים
- רמת הדיוק הגבוהה של המערכת הנובעת מעובדה שהמערכת מאתרת רצפים אנומליים ולא פעולות בודדות, מתבטאת בכמות מאד נמוכה של התראות השווא (false positive)
- המערכת מחשבת לכל אנומליה ציון סיכון המבוסס על הפעולות שבוצעו במהלך הרצף האנומלי ומידת החריגה של הרצף האנומלי
- המערכת מאפשרת תיחקור מהיר של האנומליה ומייעלת את עבודת האנליסט
- למערכת קיים ממשק מובנה למקורות הלוג שונים (כגון SIEM,Datalake, בסיסי נתונים, קבצי לוג, ועוד), כאשר המידע המאוחזר ממקורות מידע אלו אינו משוכפל ב TrackerIQ אלא מעובד בלבד
- היישום הינו פשוט וקל, אשר לא מצריך כל התקנה על אחד ממוצרי הארגון

תהליך העבודה

קריאה
קריאת לוגים אפליקטיבים מכל אפליקציה באשר היא

למידה
למידת כל רצף פעילויות של כל משתמש בכל אפליקציה

יצירה
יצירת מודל גנרי עבור רצפי הפעולות האפליקטיביות של המשתמשים

יצירת פרופילי התנהגות
בנית פרופילי התנהגות לכל משתמש בכל אפליקציה

זיהוי
זיהוי וניטרול של התנהגויות חריגות של משתמשים

בקרה
בקרה וזיהוי פעילויות אנומליות באופן רציף

תעדוף
מתן ציון סיכון לכל התנהגות חריגה

התראה
התראה על סיכונים מזוהים הדורשים פעולה

תצוגה
הצגת שורש סיבות של התראות ע"י כלי ניתוח

אודות RevealSecurity

RevealSecurity הינה חברה ישראלית המציעה לארגונים גדולים פתרון אוניברסלי לזיהוי מהיר ומדויק של פעילות אנומלית ברמת האפליקציה הארגונית.
באמצעות למידה אוטומטית של דפוסי פעילות המשתמשים באפליקציות, המערכת מאתרת ומתריאה על אירועים חריגים שעלולים להיות פעילות זדונית של משתמש או פעילות שנעשתה בשוגג. חשוב להדגיש שאיתור מהיר של פעילות חריגה באפליקציות הארגוניות מקטין משמעותית את הנזק לארגון לכן יכולת ניטור של פעולות משתמשים באפליקציות הארגוניות הינה צורך קריטי לארגון.

Reveal security | www.reveal.security | info@reveal.security

TAG CYBER 2022 DISTINGUISHED VENDOR