Microsoft Security

3 סיבות לעבור להגנה משולבת מפני איומים

תכנים

מבוא

הארגון הממוצע משתמש כיום ביותר מ- 30 כלי אבטחה שונים, לעתים קרובות מפורקים ו'מובראגים'.

האבטחה נמצאת בנקודת מפנה. מתקפות סייבר הופכות מתוחכמות יותר ככל שארגונים ממשיכים להתמודד עם אתגרים החל ממחסור בכישרונות ואיזון עלויות וכלה בניווט בלחצים של עבודה היברידית.

בינתיים, שוק האבטחה מפוצל ומורכב מתמיד. הארגון הממוצע משתמש כיום ביותר מ- 30 כלי אבטחה שונים, לעתים קרובות מפורקים ו'מובראגים', המספקים נראות מוגבלת ותובנות לא מספקות למרכזי תפעול אבטחה (SOCs).

מובילי אבטחה ותאימות רוצים הבנה טובה יותר של הסיכונים והאיומים האחרונים, אך הם גם צריכים לדעת מה עובד, מה לא והיכן יש להם פערים.

היקף אתגרי האבטחה כיום עשוי להוציא את הרוח מהמפרשים, אבל למנהלי אבטחת מידע שמעוניינים לשפר את היעילות והאפקטיביות של פעולות האבטחה יש סיבה לאופטימיות. התשובה נעוצה בגישה משולבת להגנה מפני איומי סייבר מקצה לקצה שתסייע לארגונים:

סיבה 1: להשיג יותר עם פחות.

איחוד פתרונות נקודתיים והפחתת תקורת פעילות האבטחה SecOps.

סיבה 2: לאפשר ל- SecOps להתמקד במשימות בעלות ערך גבוה

השתמשו בכלים שמגבירים פרודוקטיביות ומעניקים אפילו לאנליסטים זוטרים יכולות גבוהות ביותר.

סיבה 3: להגדיל את פרודוקטיביות העובדים

הגן על הארגון שלך באופן שמאפשר לעובדים שלך להיות חסרי פחד כשהם יוצרים ומחדשים.

גישה זו מתאפשרת על-ידי שילוב פתרון זיהוי ותגובה מורחב (XDR) עם מערכת ניהול מידע ואירועים (SIEM) מקורית בענן המשתמשת ביכולות בינה מלאכותית (AI) ואוטומציה. הפתרון המשולב יכול לעזור ל- SOC שלך לחזות יותר התקפות ברחבי הארגון, להיות יותר פרואקטיבי בתחום זה ולהגביר את המניעה שלהן.

סיבה 1

להשיג יותר עם פחות

באמצעות איחוד כלים עם הפתרון המשולב של Microsoft, תוכל גם לחסוך בכך שתשלם עבור מה שאתה משתמש בו בלבד.

ארגונים רבים ניגשו לכלי אבטחה תוך התמקדות בפתרונות הנקודתיים הטובים מסוגם. למרבה הצער, ייתכן שגישה זו דווקא מקשה על מומחי אבטחה לזהות איומים ולהגיב להם במהירות. זה יכול גם בסופו של דבר להשפיע לרעה על הוצאות ה- IT ועל הפרודוקטיביות של משתמשי הקצה.

מכיוון שארגונים מחפשים לעשות יותר עם פחות, גישה משולבת כגון SIEM ו- XDR של Microsoft יכולה לעזור. היא יכולה להפחית את המורכבות על-ידי איחוד כלים בודדים - ומכיוון שהיא מקורית בענן, פתרון משולב יכול גם לשפר את הביצועים ואת קנה המידה.

באמצעות איחוד כלים עם הפתרון המשולב של Microsoft, תוכל גם לחסוך בכך שתשלם עבור מה שאתה משתמש בו בלבד. ניתן גם להפחית את תקורת ה- SecOps הנדרשת לניהול פתרונות באמצעות הגברת האוטומציה והאינטגרציה.

> התחלת התהליך של אימוץ כלי אבטחה חדשים היא קלה מכיוון שאתה מצפה שהפערים יהיו רחבים. כשתתקדמו מהנקודה הזו, תבינו במהרה שכלים של ספקים שונים יכולים לחפוף באופן פוטנציאלי בתחום האחריות שלהם. חפיפה כזו עשויה להיות רצויה לאיזונים ובלמים, **אך עלולה להיות לה גם עלות כספית כבדה".**
>
> **ג'ונתן קאסר**
> סמנכ"ל טכנולוגיות, MITA

1.6 מיליון USD

חיסכון מדי שנה מאיחוד ספקים

Microsoft הזמינה את Forrester Consulting לבצע מחקר מסדרה Total Economic Impact™ (TEI) ('ההשפעה הכלכלית הכוללת') ולבדוק את החזר ההשקעה (ROI) הפוטנציאלי שממנו ארגונים יכולים ליהנות לאחר פריסה של Microsoft SIEM ו- XDR. אלה היו כמה מהממצאים המרכזיים עבור ארגון מורכב היפותטי עם 8,000 עובדים בסך הכל ו- 10 מומחי אבטחה:

- **חיסכון של כמעט 1.6 מיליון USD בשנה מאיחוד ספקים**. ההשקעה ב- Microsoft SIEM וב- XDR מאפשרת לארגון המורכב להפחית את העלות של ה- SIEM הקודם שלו (USD 560,000), את התשתית המקומית המשויכת (מעל USD 360,000), פתרונות שלושת הנקודות של XDR (USD 192,000) ואת עלות העבודה השוטפת לניהול זה (USD 480,000).

- **הפחתת הסיכון להפרה מהותית ב- 60%.** עם זרימות עבודה יעילות יותר של חקירת אבטחה ותגובה, אוטומציה משופרת של תגובת אבטחה והיכולת המוגברת להגן על כל סביבות המחשוב, כולל הגנה מרובת עננים, הארגון המורכב מפחית את הסיכון לפריצות עם חיסכון שנתי של 1.6 מיליון USD.

- **יצירת החזר השקעה (ROI) של 207%.** הראיונות המייצגים והניתוח הפיננסי מצאו כי ארגון מורכב חווה הטבות של USD 17.68 מיליון USD על פני שלוש שנים לעומת עלויות של USD 5.76 מיליון USD, מה שמסתכם בערך נוכחי נקי (NPV) של USD 11.92 מיליון USD.

סיבה 2

לאפשר ל- SecOps להתמקד במשימות בעלות ערך גבוה

לכן חשוב ליצור אינטגרציה בין SIEM ו- XDR כדי לתאם התראות, לתעדף את האיומים הגדולים ביותר ולתאם פעולות ברחבי הארגון.

צוותי SecOps מוצפים בכמות האותות שעליהם לנתח, כולל אותות רבים בנאמנות נמוכה שקשה, אם לא בלתי אפשרי, לזהות באופן ידני ולטפל בהם. ככל שהאיומים גדלים, קשה ל- SOC עמוס לעמוד בקצב, במיוחד כאשר מנסים לנתח נתונים מפתרונות נקודתיים מרובים. הקצאת משאבים נוספים למילוי הפערים אינה התשובה, שכן קשה מאד למצוא מספיק אנשי מקצוע מיומנים.

לכן חשוב לשלב SIEM ו- XDR כדי לתאם התראות, לתעדף את האיומים הגדולים ביותר ולתאם פעולה ברחבי הארגון, עם בינה מלאכותית ואוטומציה מתקדמות כדי לזהות ולתקן איומים באופן יזום.

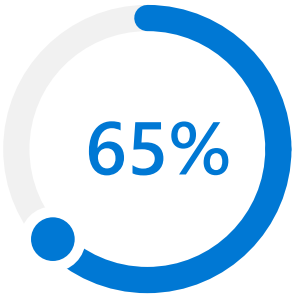
לדוגמה, אות יחיד ברמה נמוכה לא יקבל תשומת לב רבה מ- SIEM מסורתי. אבל בעזרת בינה מלאכותית, SIEM מקורי בענן יכול להשוות את האות באופן אוטומטי לאותות ממקורות אחרים ברחבי הארגון, תוך התאמה בין ערכות נתונים מרובות כדי לאתר התקפות ברמות שונות.

SIEM ו- XDR משולבים מפנים משאבי SecOps תוך העצמת אפילו אנליסטים זוטרים עם יותר יכולות וביטחון.

לאחר מכן המערכת מנרמלת מנתחת ומתאימה את הנתונים, תוך מתן הקשר לאופן שבו מתקפת הסייבר נכנסה לתשתית, יחד עם ציר הזמן של האופן שבו היא התפשטה. זה מאפשר לצוותי מרכז פעולות להציג את הפריצה – מקונסולה אחת – ולטפל בה ביעילות.

> הרבה מנהלי אבטחת מידע לא מבינים **את התקורה שהם מטילים על הצוותים שלהם עם 20 זגוגיות שונות או** פתרונות נקודתיים, ואת העלויות השנתיות הנלוות... ביטלנו הרבה עייפות של כלים עם ספק יחיד".
>
> **טרנס ג'קסון**
> מנהל אבטחת מידע ופרטיות ראשי, Thycotic

ארגון לא צריך להזדקק למומחיות עמוקה כדי לממש את הערך של פתרון אבטחה. SIEM ו- XDR משולבים מפנים משאבי SecOps תוך העצמת אפילו אנליסטים זוטרים עם יותר יכולות וביטחון.



הגישה המשולבת של Microsoft SIEM ו- XDR הפחיתה את הזמן לחקירת איומים ב- 65%.

™Forrester Total Economic Impact (TEI) שהוזמן על ידי Microsoft הראה סוג זה של יעילות SecOps בארגון המורכב שלה:

- **צמצום הזמן לחקירת איומים ב- 65% וקיצור הזמן להגיב לאיומים ב- 88%.** הגישה המשולבת של Microsoft SIEM ו- XDR לחקירה ולתגובה של איומי אבטחה הופכת זרימות עבודה אלה ליעילות יותר עבור מומחי האבטחה של הארגון המורכב. הם כבר לא צריכים לעבור בין כלים מרובים כדי לזהות איומים, בעוד שתכונות אוטומציית אבטחה משפרות עוד יותר את זרימות העבודה של התגובה.

- **צמצום הזמן ליצירת חוברת עבודה חדשה ב- 90% והזמן לקליטת מומחי אבטחה חדשים ב- 91%.** הגישה המשולבת של Microsoft SIEM ו- XDR הופכת זרימות עבודה נוספות של מומחי אבטחה ליעילות יותר. מכיוון שיומני SIEM משולבים בכל חבילת הפתרונות, יצירת חוברות עבודה היא כמעט אוטומטית, בעוד שכניסה יחידה מאפשרת למומחי אבטחה חדשים להצטרף כמעט 16 שבועות מהר יותר.

סיבה 3

שיפור פרודוקטיביות העובדים

פתרון SIEM ו- XDR משולב יכול לעזור לארגון שלכם לשפר את הפרודוקטיביות עבור משתמשי הקצה.

בנוסף לעשיית יותר עם פחות והיעילות SecOps, פתרון SIEM ו - XDR משולב יכול לעזור לארגון שלך לשפר את הפרודוקטיביות עבור משתמשי הקצה.

כפי שצוותי SecOps יודעים, כשאתה מקשה על האבטחה, אנשים עוקפים את זה. לכן, כשמשתמש קצה נתקל בבעיה, הוא עשוי לנסות להימנע מפגיעה בפרודוקטיביות של העובדים ולחשוף את ארגון לסיכוני אבטחה רבים יותר ולעלויות גבוהות יותר. סיסמאות חלשות או אבודות, גישה לא מאובטחת באמצעות מכשירים אישיים או שיתוף בלתי מוגבל של נתונים רגישים הם רק חלק מהאתגרים.

> [בעבר] היינו משתמשים בכלים גסים כשמישהו חשד בבעיה. היינו סוגרים דברים וסוגרים את הגישה, דבר שהשפיע לרעה על העסק שלנו. וזה היה מאוד ברור לכולם כי הדברים יפסיקו לעבוד באופן זמני. ב- Microsoft Sentinel יש לנו "אזמל" שבאמצעותו אנו יכולים להגיב בצורה כירורגית למה שקורה. **העסק בדרך כלל אפילו לא יודע מתי אנחנו מגיבים לאיום**, וזה מדד חשוב מאוד להצלחה שלנו".
>
> **ריק גרינגר**
> מנהל מערכות מידע ראשי, Wedgewood

כמעט

68,000

Microsoft SIEM ו- XDR שיפרו את הפרודוקטיביות של עובדים אחרים בכמעט 68,000 שעות בסך הכל מדי שנה.

הגישה המשולבת של SIEM ו- XDR עוזרת לכם לספק חוויות משתמשים חלקות שמבטיחות את הפרודוקטיביות והאבטחה הנאותה שלהם בכל ההיבטים הגלומים בחוויות העבודה היומיומיות שלהם. זה יכול להפחית את ההשפעות השליליות על הפרודוקטיביות, כגון הצורך לכבות שירותים או לבודד ולאחר מכן לדמיין מחדש מחשבים. עם זאת, SIEM ו- XDR משולבים יכולים גם ליצור הזדמנויות חדשות לרווחי פרודוקטיביות של משתמשי הקצה, כגון עם תמיכה רבה יותר באבטחה בשירות עצמי, דאשבורדים ודיווח טובים יותר, ותגובתיות רבה יותר וזמני אתחול מהירים יותר מהפעלת פחות סוכני אבטחה.

במחקר Forrester Total Economic Impact™ (TEI) שהוזמן על-ידי Microsoft, הארגון המורכב ההיפותטי עם 8,000 עובדים בסך הכל הראה עלייה בפרודוקטיביות העובדים על-ידי פריסת Microsoft SIEM ו- XDR:

- **שיפור הפרודוקטיביות של עובדים אחרים בכמעט 68,000 שעות בסך הכל מדי שנה.** Microsoft SIEM ו- XDR מונעים השפעות שליליות על עובדים אחרים מתהליכי אבטחה לא יעילים. לדוגמה, הקומפוזיט חוסך 4,000 שעות בשנה הודות ליכולת החדשה של מומחי IT לשרת בעצמם בנוגע לעדכוני אבטחה והמלצות. היא גם מאפשרת פתרון בעיות מרחוק מבוסס אבטחה במחשבים של עובדים ומפחיתה את מספר סוכני האבטחה הפועלים עליהן, ובכך חוסכת כמעט 64,000 שעות בשנה בפרודוקטיביות של משתמשי הקצה.

האבטחה הפכה לגורם חיוני להצלחה טכנולוגית. זו הסיבה שארגונים זקוקים לאמצעי אבטחה שבונים עמידות רבה ככל האפשר מפני התקפות מודרניות – כדי להגן על הפרודוקטיביות והחדשנות שמניעות צמיחה ולאפשר אותן.

קבלו הגנה משולבת מפני איומי סייבר עם SIEM ו- XDR

אינטגרציה זאת של מוצרים מובילים בתעשייה מספק מניעה, זיהוי ותגובה של איומי סייבר בפתרון מקיף אחד.

Microsoft מציעה את פתרון SIEM ו- XDR המשולב הראשון והיחיד, המספק ניראות מקצה לקצה בכל העננים והפלטפורמות. אינטגרציה זאת של מוצרים מובילים בתעשייה מספק מניעה, זיהוי ותגובה של איומי סייבר בפתרון מקיף אחד.

Microsoft SIEM ו- XDR מנצלים את העוצמה של בינה מלאכותית ואוטומציה, כמו גם השקעות עמוקות ומתמשכות בזיהוי וניתוח איומי סייבר – עם תובנות של מומחים וניראות לגבי 43 טריליון אותות מדי יום. עם אינטגרציה בין מוצרים אלה, צוותי SOC חמושים בהקשר רב יותר מאי פעם כדי לצוד ולפתור איומי סייבר קריטיים מהר יותר:

Microsoft Sentinel

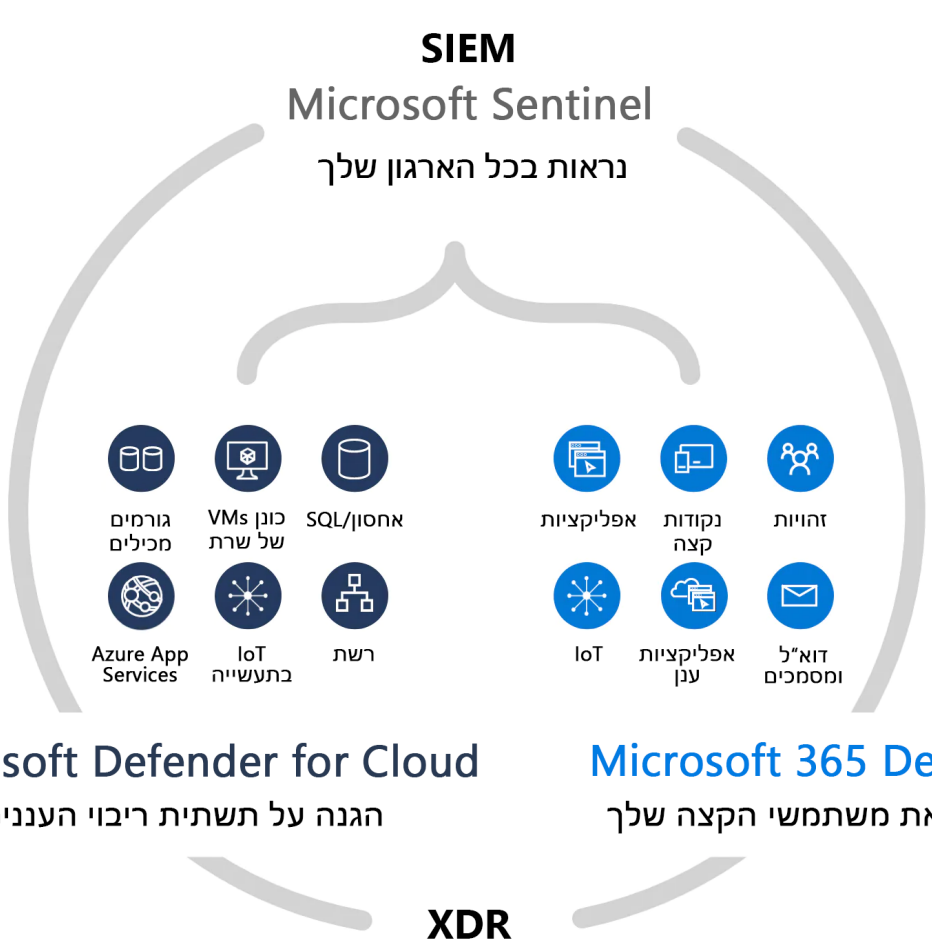
קבלו מבט ממעוף הציפור ברחבי הארגון באמצעות SIEM מקורי בענן של Microsoft. צברו נתוני אבטחה כמעט מכל מקור ויישמו בינה מלאכותית כדי להפריד בין רעש לאירועים לגיטימיים, לתאם התראות בין שרשראות מתקפת סייבר מורכבות

Microsoft Defender XDR

מנעו וזהו מתקפות סייבר בכל הזהויות, נקודות הקצה, האפליקציות, הדואר האלקטרוני, הנתונים ויישומי הענן שלכם באמצעות יכולות XDR. חקרו מתקפות סייבר והגיבו להן באמצעות הגנה מוכנה לשימוש הטובה מסוגה. חפשו איומים ותאמו בקלות את התגובה שלכם מדאשבורד יחיד.

Microsoft Defender for Cloud

הגנו על עומסי העבודה של ענן מרובה וענן היברידי באמצעות יכולות XDR מובנות. אבטח את השרתים, האחסון, מסדי הנתונים, הגורמים המכילים ועוד. התמקד בדברים החשובים ביותר באמצעות התראות מתועדפות.



אל תטפל באבטחה בנפרד. הפוך אותה לחלק אינטגרלי מהמערכת.

שימו את הכלים והאינטליגנציה הנכונים בידי האנשים הנכונים. התגוננו מפני מתקפות מודרניות באמצעות פתרון משולב מקצה לקצה, מקורי בענן.

מידע נוסף על הגנה מפני איומי סייבר של פתרונות SIEM ו- XDR של Microsoft >

Microsoft Security