



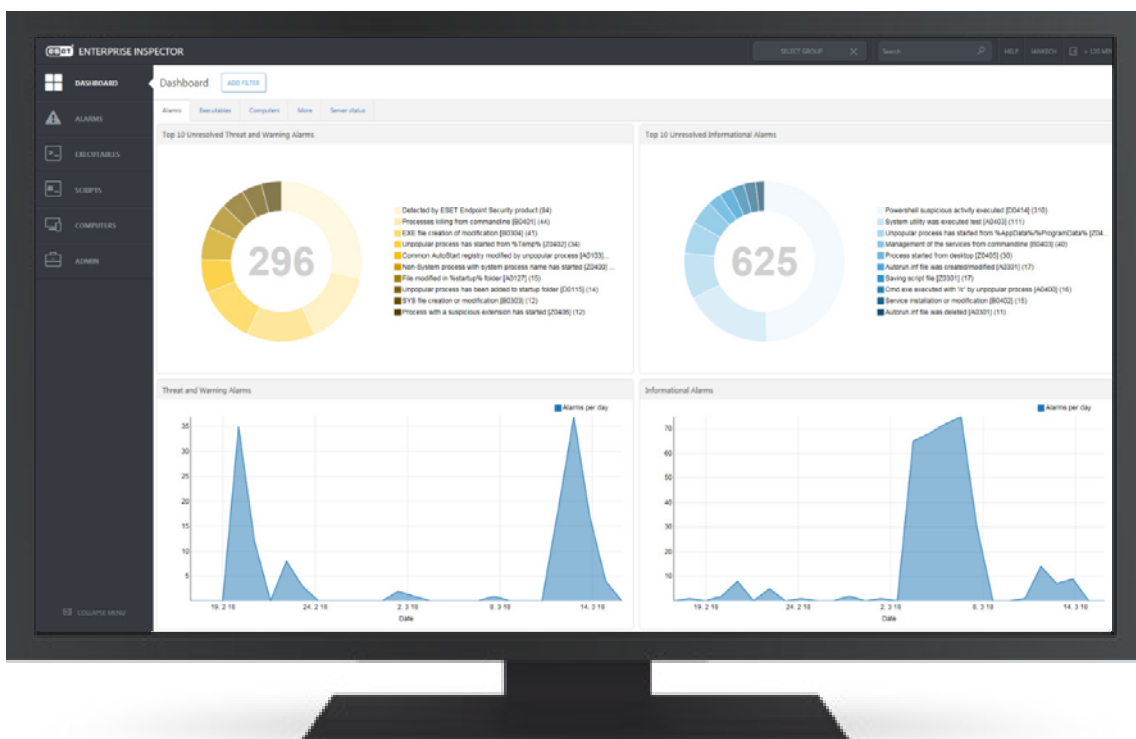
ENTERPRISE INSPECTOR

הבטיחו נראות מלאה וטיפול באירועי אבטחה
בזמן אמת באמצעות ה-EDR של ESET

CYBERSECURITY
EXPERTS ON YOUR SIDE

מהו פתרון זיהוי ותגובה לתחנות קצה (EDR)?

ESET Enterprise Inspector הוא כלי EDR מתוחכם המשמש לזיהוי התנהגויות חריגות ופריצות, הערכת סיכונים, תגובה לאירועים, תחקור וטיפול לאחר אירועי אבטחה. הוא מנטר ומעריך את כל הפעילויות שקורות ברשת (כמו שינויים החלים במשתמשים, קבצים, תהליכים, ערכי Registry, זיכרון ורשת) בזמן אמת ומאפשר לכם לנקוט בפעולה מידית בזמן אמת במידת הצורך.



מדוע יש צורך בפתרון זיהוי ותגובה לתחנות קצה?

נראות ושליטה מלאה על רשת הארגון

איומים פנימיים ומתקפות פשינג הן כאב ראש גדול לעסקים גדולים. מתקפות פשינג מופנות בעיקר לעסקים גדולים בשל מספר העובדים הגדול שיכולים לשמש כמטרות למתקפה. ישנו סיכוי טוב שאחד העובדים יבלע את הפיתיון ויסכן את הארגון כולו. מתקפות פנימיות הן איום נוסף שמאיים על עסקים גדולים, שכן מספר העובדים הגדול מגדיל את הסיכוי לכך שאחד מהם פועל בניגוד לאינטרסים של הארגון.

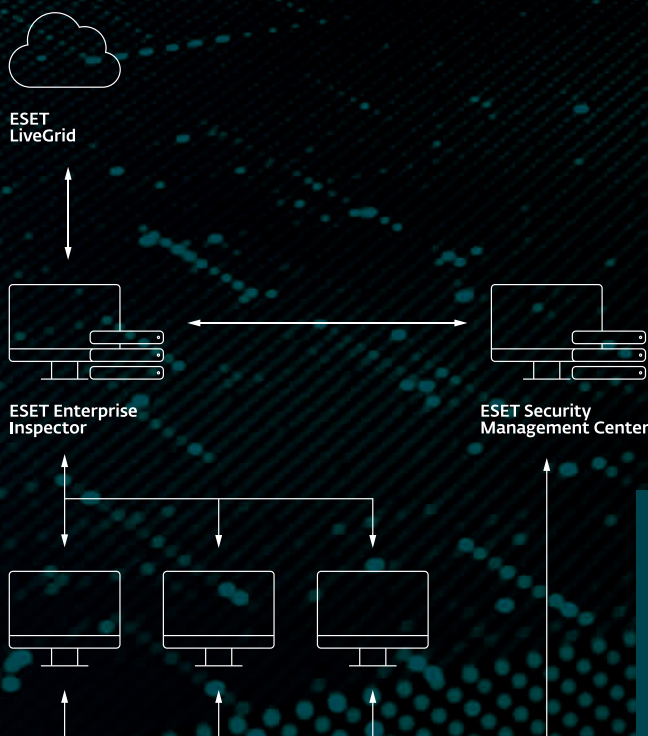
מערכות EDR מספקות את תוספת הניטור הנחוצה לארגונים כך שיוכלו לראות, להבין, לחסום ולטפל באירועי אבטחה בכל המכשירים המקושרים אליהם בזמן אמת. ESET Enterprise Inspector יכול, למשל, לזהות ולעצור במהירות סקריפטס זדוניים שמסווים את עצמם כחלק ממסמך בלתי מזיק, כמו קובץ Word.

דליפות מידע

חברות לא יכולות להסתפק רק בזיהוי של דליפת מידע - הן חייבות להכיל את אירוע האבטחה ולטפל בנזקים שגרם. את כל אלו יש לעשות בדיוק המירבי ומבלי לגרום להפרעה להמשכיות העסקית. רוב העסקים אינם ערוכים לביצוע תחקור, ובמקום זאת הם שוכרים את שירותיו של ספק חיצוני שסייע בכך. כיום ארגונים זקוקים לנראות מלאה של רשת המחשבים שברשותם כדי להבטיח שאיומים חדשים, התנהגות בעייתית של עובדים ותוכנות לא רצויות לא יסכנו את רווחי החברה והמוניטין שלה. התעשיות העיקריות שסובלות מדליפות מידע הן חברות שמחזיקות במידע יקר ערך, כמו חברות פיננסיות, סטונאות, ספקי שירותי בריאות וחברות במגזר הציבורי. זה לא אומר שיתר ענפי התעשייה בטוחים - זה רק אומר שבדרך כלל האקרים בוחנים את יחס העלות-תועלת של תקיפותיהם.

מאמץ תקיפה מתמיד (APT) ומתקפות ממוקדות

מערכות EDR משמשות בדרך כלל למטרות הבאות: זיהוי איומי APT (מאמץ תקיפה מתמיד) או מתקפות ממוקדות באמצעות ניטור איומים; הפחתת זמן התגובה לתקרית; מניעה פרואקטיבית של מתקפות עתידיות. חשיפת איומי מאמץ תקיפה מתמיד היא חשובה במיוחד לעסקים גדולים, שכן רוב העסקים כיום אינם חשים מוכנים מול המתקפות החדשות ביותר, שיכולות להימשך ברשת במשך ימים ואף חודשים מבלי שיזוהו.



מספק זיהוי ייחודי מבוסס התנהגות ומוניטין, נראות וניטור מלא לצוותי אבטחת המידע, המאפשר להם תגובה בזמן אמת על פי נתונים הנאספים מלמעלה מ-100 מיליון תחנות קצה המוגנות ע"י LiveGrid של ESET.

פתרון כולל המשלב מניעה, זיהוי ותגובה המאפשר ניתוח, בקרה וטיפול מהירים בכל בעיית אבטחה ברשת.

=

ESET Endpoint Protection

הגנה רב שכבתית לתחנות הקצה, בה כל שכבה שולחת נתונים ל-ESET Enterprise Inspector

+

ESET Enterprise Inspector

מערכת EDR מתוחכמת המנתחת כמויות עצומות של נתונים בזמן אמת כך שכל האיומים יזוהו.

כיום, ארגונים זקוקים לנראות וניטור של המחשבים ברשותם על מנת לוודא שאיומים חדשים, התנהגויות בעייתיות של עובדים ותוכנות לא-רצויות אינן מסכנות את הרווחים והמוניטין של החברה.

למה ESET Enterprise Inspector?

סנכרון מלא

ESET Enterprise Inspector, יושב על בסיס הגנת תחנות הקצה של ESET, יוצרת מערכת גומלין עקבית שמאפשרת חיבור בין כל הפריטים הרלוונטיים וטיפול מסונכרן של נזקי אירועי האבטחה. צוות האבטחה יכול לעצור תהליכים הרצים במערכות, להוריד את הקובץ שגרם לזיהוי, או פשוט להפעיל מחדש מחשבים, לכבות אותם, לסרוק אותם או לבודד אותם מהרשת, כל זה ישירות מממשק הניהול.

ארכיטקטורה פתוחה

ESET Enterprise Inspector מספקת זיהוי ייחודי מבוסס התנהגות ומוניטין, בנראות מלאה לצוותי האבטחה. כל הכללים נכתבים בפורמט XML הנפוץ, וניתן ליצור ולשנות אותם בקלות כך שיתאימו לצרכים הספציפיים של סביבות העבודה הארגוניות, ביניהם אינטגרציות SIEM.

גישה מרחוק

ESET Enterprise Inspector כולל יכולת להפעלת פקודות PowerShell מרחוק, שמאפשרת למנהלי האבטחה לבחון ולהגדיר מרחוק את המחשבים שבארגון שלהם, כך שיהיה ניתן לתת תגובה מתוככמת למתקפה מבלי להפריע לרצף העבודה של המשתמשים.

תאימות לסביבות מרובות פלטפורמות

ESET Enterprise Inspector תומכת במערכות הפעלה Windows ו-MacOS, מה שהופך אותה לבחירה המושלמת לסביבות עבודה מרובות פלטפורמות.

API ציבורי

ESET Enterprise Inspector כוללת API שמאפשר גישה לזיהויים וייצוא שלהם, יחד עם טיפול בזיהויים, מה שמאפשר אינטגרציה אפקטיבית עם SIEM, SOAR, כלי ניהול קריאות וכלים אחרים רבים.

שליטה והתאמה לרגישות הזיהויים

התאם את הזיהויים בקלות באמצעות התאמה אישית של רגישות החוקים לקבוצות משתמשים שונות או למשתמשים שונים. שלבו בין קריטריונים כמו שם הקובץ, מיקומו, מחרוזת Hash, שורת פקודה וחותרם כדי להתאים באופן מושלם את התנאים להפעלת הכללים.

MITRE ATT&CK™

ESET Enterprise Inspector יוצרת התאמה בין הזיהויים שלה ובין המסגרת של MITRE ATT&CK™, שמספקת לכם את מידע מקיף על כל האיומים, גם המורכבים ביותר, בלחיצת כפתור.

מערכת ניהול מוניטין

הסינון המקיף של ESET מאפשר למנהלי אבטחת המידע לסנן את כל התוכנות הידועות כבטוחות באמצעות שימוש במערכת המוניטין החזקה של ESET. מערכת המוניטין שלנו כוללת בסיס נתונים של מאות מיליוני קבצים הידועים כבטוחים, כך שצוותי האבטחה יקדישו את זמנם לזיהויים הלא מוכרים שעשויים להיות זדוניים במקום לכלות את זמנם על התראות שווא.

מקרים לשימוש זיהוי איום לעומק – כופרה

מקרה לדוגמה

עסק מעוניין בכלים נוספים לזיהוי פרואקטיבי של כופרות, ובנוסף מעוניין לקבל התראות אם נצפתה התנהגות הדומה להתנהגות של כופרה ברשת.

פתרון

✓ הגדרת כללים לזיהוי תוכנות הרצות מתיקיות זמניות

✓ הגדרת כללים לזיהוי קבצי אופיס (Word, Excel, PowerPoint) כאשר הם מפעילים סקריפטים או קבצים ברי-הרצה נוספים.

✓ הגדירו התראה למקרה בו אחת מהסיומות הנפוצות של קושחות נראית באחד המכשירים.

✓ צפו בהתראות של Ransomware Shield מפתרונות האבטחה לתחנות קצה של ESET באותו ממשק הניהול.

כיום, כופרות מנסות לפעול ברשת מבלי להתגלות ולהפיץ את עצמן לכמה שיותר תחנות קצה ברשת. הן חודרות לגיבויי המכשירים כדי להבטיח שאפילו שחזור הגיבויים הקודמים לא ימנע את ההפעלה המוצלחת של הכופרה.

ESET Enterprise Inspector מגדיל את הפונקציונליות של פתרונות ESET לאבטחת תחנות קצה ומאפשר לזהות באופן פרואקטיבי כופרות שאולי כבר קיימות ברשת הארגון. בתרחיש כופרה רגיל, משתמש מקבל הודעת דוא"ל שאליה מצורף מסמך. המשתמש פותח את מסמך ה-Word ומתבקש להריץ סקריפט מאקרו. לאחר שהמשתמש מריץ את סקריפט המאקרו, קובץ הרצה (EXE) מורד למערכת ומתחיל להצפין כל מה שהוא יכול, כולל כוננים ממופים.

ESET Enterprise Inspector מאפשר לצוות האבטחה שלכם לקבל התראות להתנהגות כמו זו, ולאחר כמה לחיצות תוכלו לדעת מה הושפע מהכופרה, מתי ואיפה הופעלו קבצי הרצה (EXE), סקריפטים או פעולה זדונית אחרת, ולבצע תחקור וניתוח מעמיק.

The screenshot displays the ESET Enterprise Inspector interface. On the left, the 'Alarm details' panel shows an alarm for 'Filecoder behaviour (20601)' with a yellow warning icon. Below this, there are sections for 'CSET LiveGold' and 'findpep-128'. The main area shows a process tree for 'winlogon.exe (800)' with several child processes listed, including 'explorer.exe (2128)', 'outlook.exe (2200)', 'winword.exe (2850)', 'msiexec.exe (2870)', 'powershell.exe (2908)', and 'cmd.exe (2490)'. A dark blue box on the right contains the text: 'פירוט התהליך ומידע על התנהגות Filecoder'.

זיהוי עובדים שמפרים כללי אבטחת מידע

מקרה לדוגמה

ברשת שלך ישנם משתמשים שעוברים שוב ושוב על החוקים הנוגעים לנוזקות. אותם המשתמשים נדבקים בנוזקות פעם אחר פעם. האם זה נובע מהתנהגות בעייתית, או שהם מותקפים יותר ממשתמשים אחרים?

פתרון

✓ צפייה בקלות במשתמשים ומכשירים בעייתיים.

✓ השלמת ניתוח מקורות וסיבות במהירות כדי למצוא את מקור ההדבקות.

✓ טיפול בשיטות התקיפה שנמצאו, כגון דוא"ל, רשת האינטרנט או התקני USB.

מקרה לדוגמה

מערכת ההתראה המוקדמת שלכם או מרכז פעילויות האבטחה שלכם (SOC) משגר אזהרה על איום חדש. מהם הצעדים הבאים שלכם?

פתרון

✓ ניצול מערכת ההתראה המתקדמת על מנת לאסוף נתונים על איומים קרובים או חדשים.

✓ איתור האיום החדש והאם קיים בכל המחשבים בארגון.

✓ חיפוש סימנים לפריצה (IoC) בכל המחשבים בכדי לגלות באילו מחשבים האיום היה קיים לפני כן.

✓ חסימת יכולתו של האיום לחדור לרשת העסק שלכם או לפעול בה.

במקרים רבים, החוליה החלשה ביותר במערכי אבטחה היא העובדים שיושבים ליד מקלדת, גם אם אין להם אף כוונה רעה.

ESET Enterprise Inspector מזהה בקלות את החוליות החלשות האלה באמצעות דירוג המחשבים על פי מספר ההתראות הייחודיות שכל מחשב יצר. אם משתמש מעורר מספר התראות, זהו סימן ברור לכך שיש לבדוק את הפעילות שהתרחשה במחשבו.

איתור וחסמת איומים

היתרון המשמעותי של ESET Enterprise Inspector הוא זיהוי איומים באמצעות טקטיקה של "מציאת מחט בערימת שחת".

באמצעות הפעלת מסננים על הנתונים, שממיינים קבצים על פי הפופולריות או המוניטין שלהם, החתימה הדיגיטלית שלהם, המידע ההקשרי וההתנהגותי שלהם, ניתן לזהות ולחקור כל פעילות זדונית בקלות. הגדרת מספר רב של מסננים מאפשרת להפעיל משימות לזיהוי איומים באופן אוטומטי ולהתאים את סף הזיהוי על פי הסביבה של אותו הארגון.

ניתן לזהות ולחקור כל פעילות זדונית בקלות

נראות מלאה של הרשת

מקרה לדוגמה

חלק מהארגונים מודאגים מהתוכנות שהמשתמשים מריצים על מערכות החברה. ואלו לא רק התוכנות שמותקנות באופן מסורתי שמדאיגות אתכם, אלא גם תוכנות שאינן מותקנות במחשבים עצמם. כיצד תוכלו להמשיך ולשלוט עליהם?

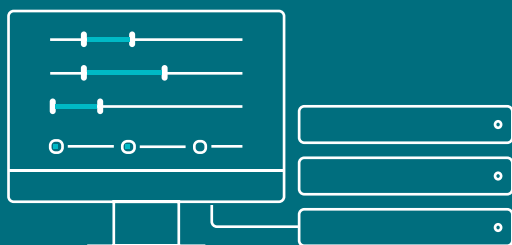
פתרון

- ✓ צפייה בכל התוכנות המותקנות על כל המכשירים וסינון שלהן בקלות.
- ✓ צפייה בכל הסקריפטים בכל המכשירים ואפשרויות סינון.
- ✓ חסימה של הרצת סקריפטים או תוכנות לא רצויים בקלות.
- ✓ טיפול באירוע באמצעות שיגור התראה למשתמשים אודות אפליקציות לא מורשות והסרה שלהן באופן אוטומטי.

ESET Enterprise Inspector הוא פתרון ארכיטקטורה פתוחה, מה שאומר שצוות האבטחה יכול להתאים את כללי הזיהוי כנגד טכניקות ההתקפה השונות לסביבה הספציפית של הארגון.

בנוסף, הארכיטקטורה הפתוחה מאפשרת גמישות רבה וכך ניתן להגדיר את ESET Enterprise Inspector לזיהוי הפרות של נהלי החברה הנוגעים לשימוש בתוכנות ספציפיות כמו תוכנות טורנט, תוכנות לאחסון בענן, תוכנות לגלישה ב-Tor, הקמת שרתים על מחשבי החברה ותוכנות לא רצויות נוספות.

אלו לא רק התוכנות שמותקנות באופן מסורתי שמדאיגות אתכם, אלא גם תוכנות שאינן מותקנות במחשבים עצמם. כיצד תוכלו להמשיך ולשלוט עליהם?



צוותי האבטחה יכולים להתאים את כללי הזיהוי כנגד טכניקות ההתקפה השונות לסביבה הספציפית של הארגון.

תחקור וטיפול באירועים על פי הקשר

הפעילות ה"זדונית" של תהליכים מסוימים תלויה בהקשר שלה.

הפעולות שמבוצעות במחשביהם של מנהלי הרשת שונות מאוד מאלו המבוצעות למשל במחלקת הכספים. באמצעות חלוקה נכונה של מחשבים לקבוצות משתמשים, צוותי האבטחה יכולים לזהות במהירות האם המשתמש רשאי לבצע פעולה ספציפית במחשב שלו. הסנכרון בין קבוצות תחנות הקצה של ESET Security Management Center ובין הכללים שמוגדרים ב-ESET Enterprise Inspector מביאים לתוצאות חסרות תקדים מבחינת מידע הקשרי.

התקנה קלה ותגובה מהירה – אין צורך בצוות אבטחה

גם אם לחברה יש צוותי אבטחה ייעודיים, לעיתים קרובות קשה לקבוע סדר עדיפויות ולהחליט על הצעדים הבאים באופן מהיר בזמן שהתראות האבטחה ממשיכות להופיע.

לכן, עבור כל התראה ניתן ליצור תוכנית פעולה מוצעת לטיפול באירועים. כש-ESET Enterprise Inspector מזהה איום, היא מספקת אפשרות לתגובה מהירה. ניתן לחסום קבצים ספציפיים על פי מחרוזת ה-Hash שלהם ולבודד מחשבים מהרשת או לכבות אותם מרחוק.

מקרה לדוגמה

הנתונים לא שווים כלום ללא ההקשר העומד מאחוריהם. כדי לקבל החלטות באופן נכון, עליך לדעת מהן ההתראות, על אלו מחשבים הן מופיעות ומיהם המשתמשים שגורמים להפעלתן.

פתרון

- ✓ יהיו ומיון המחשבים על פי Active Directory, חלוקה אוטומטית לקבוצות או חלוקה ידנית.
- ✓ חסימת הפעלתם של תוכנות וסקריפטים או מתן הרשאות לשימוש בהן בכל אחת מקבוצות המחשבים השונות.
- ✓ חסימת הפעלתם של תוכנות וסקריפטים או אפשר אותן לכל אחד מהמשתמשים השונים.
- ✓ קבלת התראות רק עבור קבוצות מסוימות. והסרה שלהן באופן אוטומטי.

מקרה לדוגמה

לא לכל העסקים יש צוותי אבטחה ייעודיים, וכך הזנת והטמעת כללי זיהוי מתקדמים עשויה להפוך למשימה קשה מאוד.

פתרון

- ✓ מעל ל-800 כללים מובנים שהוגדרו מראש.
- ✓ תגובה בקלות באמצעות חסימת אפליקציות, הפסקת פעולתן או הכנסת מחשב להסגר בלחיצת כפתור אחת.
- ✓ תוכניות פעולה מוצעות הן חלק מובנה מההתראות. מההתראות.
- ✓ יתן לערוך את הכללים בשפת XML וכך לאפשר כוונן עדין של הכללים הקיימים או יצירת כללים חדשים.

יכולות הפתרון

זיהוי איומים

ניתן לסנן נתונים כדי למיין אותם על פי הפופולריות של הקובץ, המוניטין שלו, החתימה הדיגיטלית שלו והמידע ההתנהגותי או ההקשר שלו. הגדרה של סננים מרובים מאפשרת זיהוי איומים קל, הכולל גם איומי מאמץ תקיפה מתמיד (APT) ומתקפות ממוקדות, באופן המותאם לסביבה של הארגון. באמצעות התאמת כללי ההתנהגות, ניתן להתאים אישית את ESET Enterprise Inspector כך שיבצע גם זיהוי איומים היסטורי ו"יסרוק מחדש" את כל בסיס הנתונים של האירועים.

איתור תקריות

(ניתוח מעמיק לשורש הבעיה)

ניתן לצפות בכל אירועי האבטחה בקלות ובמהירות באיזור הזיהויים. לאחר כמה לחיצות על העכבר, צוותי האבטחה יוכלו לראות ניתוח מעמיק, שבו ניתן לראות מה הושפע מהאירוע וכן מתי ואיפה הופעלו קבצים, סקריפטים או פעולות שונות.

תחקור וטיפול באירועים

שימוש במערך כללים מובנה ויצירת כללים מותאמים לארגון כדי להגיב לתקריות שזוהו. לכל זיהוי שהופעל ניתן ליצור תוכנית פעולה מוצעת שתבצע אוטומטית טיפול באירוע. אפשרות תגובה מהירה מאפשרת לחסום קבצים מסוימים על פי מחרוזת ה-Hash שלהם, לעצור תהליכים ולהכניס אותם להסגר, לבודד מחשבים או לכבות אותם מרחוק. אפשרות התגובה המהירה הזו עוזרת להבטיח שאף אירוע אבטחה לא ייפול בין הכיסאות.

בידוד בלחיצה אחת

הגדרת מדיניות גישה לרשת כדי לעצור במהירות התפשטות של נזקה. ניתן לבודד מכשיר מודבק מהרשת בלחיצה אחת בלבד מהממשק של ESET Enterprise Inspector. בנוסף, ניתן להוציא את המכשירים בקלות ממצב ההסגר לאחר מכן.

ניקוד

הגדירו סדר עדיפויות למידת החומרה של ההתראות באמצעות מערכת ניקוד שמשייכת ערכי חומרה לתקריות ומאפשרת למנהל הרשת לזהות בקלות מחשבים שבהם הסיכון להיווצרות אירוע אבטחה הוא גבוה יותר.

תיוג

הוספת והסרת תגים לסינון מהיר של עצמים ESET Enterprise Inspector כמו מחשבים, התראות, כללי החרגה, משימות, קבצים ברי-הרצה, תהליכים וסקריפטים. ניתן לשתף את התיוגים בין המשתמשים, ולאחר שתיוג נוצר ניתן לשייך אותו לעצם בשניות ספורות.

איסוף נתונים

צפייה במידע מפורט אודות תהליך חדש שהופעל, כולל זמן ההרצה, זהות המשתמש שהפעיל אותו, זמן השייה וההתקנים שהושפעו ממנו.

כניסה בטוחה

אימות דו-שלבי - שכבת הגנה נוספת - לחשבון המנהל שלכם כדי למנוע מאדם בעל כוונות זדוניות להיכנס למשתמש, גם אם יש לו את הסיסמה לחשבון.

זיהוי סימנים לפריצה

צפייה במודולים וחסומים שלהם על בסיס למעלה מ-30 סימנים שונים, הכוללים מחרוזת Hash, שינויים ב-Registry, שינויים בקבצים והתחברויות ברשת.

זיהוי אנומליות והתנהגות

בדיקת פעולות שבוצעו ע"י קובץ בר הרצה והשתמשו במערכת המוניטין LiveGrid כדי להעריך במהירות אם התהליכים שהופעלו הם בטוחים או חשודים. ניתן לנטר אירועים חריגים הקשורים למשתמשים מסוימים באמצעות כללים ספציפיים המוגדרים לפעול לפי התנהגות מסוימות, ולא רק על פי זיהוי בסיסי של נזקה או חתימה זדונית. חלוקת המחשבים לקבוצות על פי משתמשים או מחלקות מאפשרת לצוותי האבטחה לזהות האם המשתמש מורשה לבצע פעולה מסוימת או לא.

זיהוי הפרה של נהלי החברה

מניעה ממודולים זדוניים לפעול ברשת הארגון. ניתן לזהות הפרות של נהלי החברה הנוגעים לשימוש בתוכנות ספציפיות כמו תוכנות טורנט, תוכנות לאחסון בענן, תוכנות לגלישה ב-Tor, הקמת שרתים על מחשבי החברה ותוכנות לא רצויות נוספות.

קצת על ESET

מבלי לעצור ותוך מינימום צריכת משאבים. בין לקוחותינו בישראל ניתן למנות משרדי ממשלה ועיריות, מוסדות חינוך ובריאות, חברות היי-טק ועסקים במגוון תחומים רחב.

www.eset.com.il

ESET היא חברת תוכנה בינלאומית ויצרנית אבטחת המידע מס' 1 באיחוד האירופי. עם ניסיון של 30 שנים, אנחנו מפתחים פתרונות הגנה לתחנות קצה המצטיינים במניעה, זיהוי ותגובה לאירועי סייבר, ומאפשרים לארגונים להתמקד במטרותיהן

ESET במספרים

110m+
משתמשים
ברחבי העולם

400k+
לקוחות
עסקיים

200+
נציגויות
בעולם

13
מרכזי מו"פ
עולמיים

בין לקוחותינו



**MITSUBISHI
MOTORS**

Drive your Ambition

מוגנת ע"י ESET מאז 2017;
מעל 14,000 תחנות קצה

Canon

Canon Marketing Japan Group

מוגנת ע"י ESET מאז 2016;
מעל 9,000 תחנות קצה

Allianz 
Suisse

מוגנת ע"י ESET מאז 2016;
מעל 4,000 תיבות דוא"ל



פק שירותי אינטרנט, שותף אבטחה
מאז 2008; למעלה מ-2 מיליון לקוחות



ESET עומדת בתקן ISO/IEC 27001:2013, תקן בעל הכרה בינלאומית הנחשב כתקן בטיחות ישים להטמעת וניהול הגנה על מידע. האישור ניתן ע"י גוף התקינה החיצוני SGS, שהוא גוף תקינה בעל מוניטין רב, מה שמראה על העמידה של ESET בתקנים החדשניים ביותר של התעשייה באופן מלא.

ESET היא אחת התורמות הגדולות ל-ESET. Mitre ATT&CK מוכיחה את עמידתה בהבטחה – לספק הגנה מיטבית לקהילה וללקוחותינו – באמצעות היותה אחת מספקיות שירותי האבטחה שתרמו נתונים בהיקף הגדול ביותר ל-Mitre ATT&CK.



פרסי ESET



הכרה מתעשיית אבטחת המידע



חברת ESET היא היחידה שזכתה לתואר Challenger במבדק Gartner Magic Quadrant for Endpoint Protection Platforms של שנת 2019, וזו השנה השנייה ברציפות.



חברת ESET זכתה לתואר "Strong Performer" בדוח של Forrester Wave™ לרבעון השלישי של 2019, המדרג ערכת אבטחה למוצרי קצה.



חברת ESET דורגה כ-"Top Player" בשנת 2019 בדוח שוק אבטחת נקודות הקצה של Radicati על פי שני קריטריונים עיקריים: פונקציונליות וחזון אסטרטגי.