**תיעוד ומידע**

YARA

במהלך העבודה כחלק ממחקר בנושא אבטחת מידע וכלים של אבטחת מידע, נחשפנו ל-YARA. YARA הוא כלי בתחום הסייבר סקיוריטי, שנועד לזיהוי ואפיון קבצים ומערכות ולאיתור איומי אבטחה. הכלי הזה שימושי מאוד לחוקרי אבטחת מידע ולמומחי סייבר בזיהוי ומניעה של איומים.

YARAמאפשרת ליצור חוקים מותאמים אישית המגדירים תבניות של נתונים או התנהגויות שקשורים לנוזקות. כשקובץ או מערכת עומדים בתנאים של חוק כזה, ניתן לזהות אותם כנוזקה או כמאוימים. באמצעות הכלי, ניתן לכתוב חוקים שמזהים מחרוזות ועל ידי כך לזהות אותם כנוזקות. יתר על כן, אפשר לשלב חוקים של YARA בסקריפטים וכלים אוטומטיים, מה שמאפשר אינטגרציה עם מערכות אבטחה קיימות.

CLAMSCAN

כלי OPEN-SOURCE המיועד לאיתור והסרה של נוזקות ווירוסים. ClamScan הוא הרכיב של ClamAV שמבצע את הסריקה עצמה.

תכונות עיקריות של ClamAV ושל ClamScan:

1. מנוע סריקה חזק: משתמש במנוע סריקה מתקדם שיכול לאתר מגוון רחב של איומים, כולל וירוסים, תולעים, סוסים טרויאניים ותוכנות זדוניות אחרות.
2. תמיכה בסקריפטים: ניתן להשתמש ב-ClamScan יחד עם סקריפטים וכלים אחרים לצורך אוטומציה וניהול מרכזי של סריקות.

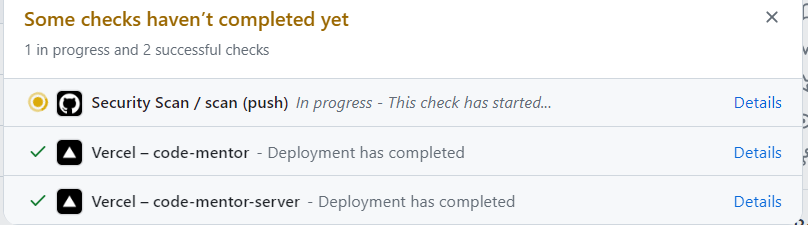
**חקרנו על שני הכלים המדוברים, ראינו את השימושים והמימושים שלהם, והחלטנו לבנות תוסף שישלב בין שני הכלים, כך שאם אחד מהכלים (לפחות) מזהה איום כלשהו, נוכל לסווג את הקובץ כולו כקובץ חשוד כזדוני.**

הרצות

במסגרת בניית התוסף וחקירת כלי ה- ClamScanניסינו להריץ את התוסף שלנו על פרוייקטי עבר שלנו שהעלנו לגיטהאב.

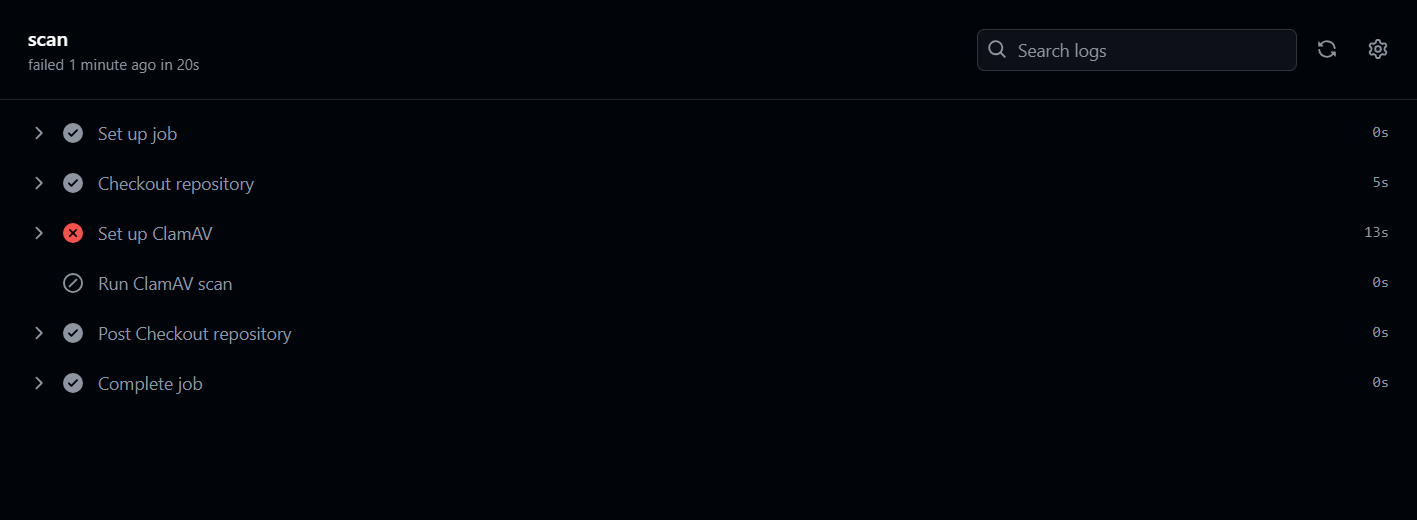
ראשית, לאחר בניית התוסף, צירפנו את הקובץ שבנינו כחלק מה-REPOSITORY, אותו רצינו לסרוק. כחלק מהגדרת התוסף, בכל בקשת PULL או PUSH, מתבצעת סריקה של התוסף לכל התיקיות בפרוייקט.

מצורף בזאת הפלט שהתקבל כחלק מהרצה (ראשונית) של התוסף על הפרוייקט שלנו. במסגרת ההרצה הצלחנו לסווג את התוסף שלנו כלא תקין (ולאחר מכן עשינו בו התאמות ושינויים):



**תמונה שמכילה טקסט, קו, גופן, צילום מסך

התיאור נוצר באופן אוטומטי**

****

לאחר שינוי ועדכון של התוסף, והרצה נוספת של אותו הפרויקט (שהוא כמובן פרוייקט תקין שלא מכיל קוד זדוני), ראינו כי התוסף אכן סיווג אותו כבטוח לשימוש:

תמונה שמכילה טקסט, גופן, מספר, צילום מסך

התיאור נוצר באופן אוטומטי

השוואת התוסף והמערכת המובנית של GitHub

על אף שאיננו מתיימרים לבנות תוסף שיוכל להתחרות ביכולות הסריקה ואיתור הוירוסים המובנית של GitHub, ישנו יתרון מובהק לבניית תוסף באופן עצמאי:

* סריקה מותאמת אישית: באמצעות בניית תוסף, נוכל לבצע סריקה מפורטת לאיתור תוכנות זדוניות, ולספק בדיקת אבטחה מותאמת אישית לצרכינו או לצרכי הלקוח.

לעומת זאת, כמובן של-GitHub יש יתרון שאיננו יכולים לספק:

* בניגוד לבניית תוסף באופן עצמאי, שדורש בניה ותחזוקה, האבטחה המובנית של GitHub מספקת חבילה מקיפה של תכונות אבטחה אוטומטיות עם הגדרה מינימלית, תוך התמקדות בפרצות תלות, סריקת קוד וזיהוי סודי.