Incident Response

> *Ido Naor*

-) careers

B.sc Computer Science
BugSec
Cisco- McAfee/Intel
Security Joes-freelans
Virusbay- website for Virus-research

1) Cybersecurity Research Achievement

platforms to find Bug Bounty

- hacker one
- bugcroud

כשאתה רוצה להתחיל מחקר אתה צריך להתמקד בתחום שלא התמקדו בו קודם.
הוא התמקד בIOT ופרץ לתחנת דלק מרחוק
המלצה פשוט לדבר עם AI ולתחקר אותו על המערכת שלו, ללמוד על החומרה ומערכת ההפעלה

2) Who Is a Cyber Incident Responder

למטה נמצא ה*SOC*- הם הראשונים שרואים את ההתראות, מהלוגים או מהענן, שרתים, מחשבים
כל חתיכת מידע שנחשבת כחתיכה של אבטחת מידע, היא מדיעה לSOC והם צריכים לעות אסקלציה (לתת את המשימה למישהו חכם יותר שיודע איך לחקור את זה)
אחר כך יש את ה*MDR*- נקרא ככה בגלל שהאנטי וירוס השתנה להיות EDR (נקודת קצה) זה הצוות שמנהלים את הEDR
אחר כך יש את ה*IR*- הם מביאים את התגובה בפועל
ואז יש את *Crisis Manager* (ביחד עם GRC) מנהל בעולמות הIR שעוזר לעולמות האלה להתחבר לביטוח ולקבל את הביטוח סייבר ולהגן
ואז יש את *CISO* הם חוטפים את הכל :)

3) - What Is a Cyber Incident Response

אירוע לדוגמא:

תוך כדי המלחמה חמאס משתמשים בנוזקה בשם BiBi (לקבוצה קראו KARMA) כשהמטרה היא WIPER
תהליך תקיפה:

איסוף מידע מהקורבן: שרתי הלינוקס לא עובדים
היפותזה- אחרי שאוספים את המידע מהלוקח צריך לייצר איזה היפותזה, (אם זה נניח שיש לו גישה לחומרה, גישה לרשת) צריך להבין מה התוקף עשה ומאיפה הוא הגיע
חקירה פורנזית- הבנת המודוס האופרנדי (מה התוקף בא לעשות, מה יהיה הצעד הבא שלו):
חקירת זיכרון נדיף- נותנת את המצב האחרון שהמחשב היה בו (אם רצו כל מיני תהליכים שרצים רק בזיכרון נדיף) כלי בשם **volatility**
ניסיון למצוא כלי תקיפה
צירוף של TTPs- (טכניקות, טקטיקות ותהליכים) הדרכים שבהם התוקף משתמש כדי לפרוץ
גיבוש YARA וחיפוש כלים- yara זה שפת תכנות פשוטה (YaraGen) להכניס את זה לקובץ, עם סיומת *yar.* והקוד הזה ימצא תבניות בתוך הקובץ השני ששמתי
ארטיביוטים דומים- רוצים למצוא דמיון בין מה שהתוקף עשה לבין דברים דומים שי באינטרנט
הבנת ההדבקה- בתוף הקובץ הבינרי יש OpCode (סימילריטיס) הם צרבו את השם בתוך הוירוס ברגע שהבינו ת האינדיקטורים אז הם שורפים את היכולות של התוקף עם לשרוף את הורוסם ברשת.
תזוזה ברשת- leteral Movement היה חיבור SSH בין plask לבין iDRAC
איסוף מודיעין עושים OSINT ומגלים שדיברו הרבה נגד ביבי. הה להם צילומסך הוא היה מתוך התחברות של SSH

Secutiry research

yonatan Elkabas

מה יעבוד בלינקאדין:

חוקר טוב זה למצוא תבניות, לראות איך דברים נראים לאורך זמן, מה עובד מה לא עובד, יש פה איזה דפוס כדי להבין איך דברים עובדים. פשוט להיות שם, לראות מה עובד מה לא עובד....
אז להעלות משהו שהוא קצת שובר את הכללים...
המילה היא **להיות מיוחדים**
סקרנות זה הכלי, זה הפתח זה הכל.

מה זה סקרנות?

הסיפור עם GALANVS וגם דה וינצ'י. עם הרפואה...
העניין הוא להבין כל דבר איך הוא עובד, קוראים לזה the folse mirror
בכל דבר שאני עושה אומרים דבר ראשון- זה לא נכון, להטיל ספק. ואז ללכת לבדוק אם זה נכון.
לבדוק איך דברים עובדם בכל מצב על כל דבר

סקרנות בתור תכונה בסייבר

לעקוב אחרי תבניות, לבדוק מה עובד ומה לא , לא לשבור דברים בצורה רנדומלית, כל הזמן לבדוק מה זה הכלים שאנחנו עושים.
סקרנות בריאה זה סקרנות טבעית, סלקטיבית ומאד מאד לא כיפית
תמיד כשלומדים משהו חדש, תמיד יש בהתחלה פחד, ואז התרגשות ואז סקרנות.
סקרנות בלי משמעת עצמית ובלי נחישות- זה גורר הפרעות.

נחישות בתור תכונה בסייבר

בהתחלה כלום לא עובד, יש מלא חוסר וודאות, מלא עבודה לבד.
להיות חוקר זה לשבת לבד מול המחשב כדי להבין את מה שהוא עושה.

איך מפתחים משמעת עצמית

יש לנו איזור במוח ACC, הוא מרבה קשרים כשאנחנו עושים דברים שאנחנו לא אוהבים לעשות אותם. כל פעם שאנחנו עושים דברים שאנחנו לא רוצים- זה מגדיל את השריר הזה ומאפשר לנו לעשות דברים לאורך זמן.

נושאי מטריה רחבים בתחום הסייבר

1. קבוצה כחולה- הגנה
2. קבוצה אדומה- התקפה
3. מחקר חולשות
4. מחקר OSINT

1) קבוצה כחולה

1. יDetection Enjineering (soc /siem)
   היא הולכת לרשת, ואוספת קולטקורים, היא משקפת לנו ניראות על פני הסביבה שלנו (על פי לוגים ומידע שהיא אוספת)
2. יEndpoint detection (AV, EDR sensors, os internals)
   הליבה- איך ווינדוס עובד באמת
3. יNetworking Detection (NSM)
   להבין את התעבורת רשת, פרוטוקולים
4. יIdentity Detection
   זהויות
5. יDFIR research
   מידע פורנזי, להבין מה קרה שם
6. יMalware research
   בדיקה לאחור, התנהגות אנליטית
7. יplatform & domain-specific Research
   יש מלא דברים שצריכים מחקר משלהם אבל ין להם קטגוריה משמעותית.

קבוצה אדומה

1. יExploit research (userland)
   תהליכים שרצים במחשב, תהליכים שרצים בחומרה
2. יtradecraft research (OPSEC, evasion, LOLBins)
   לשמור על אנונימיות ברשת
3. יRed team research (attack simulation, tooling)

חולשות (Vulnerability)

1. יapplication security
2. יprotocol and Network secrity research
3. יidentify research
4. היה עוד כמה

מודיעין

1. יactor and campainegn
2. יinfrastucture and OSINT research
3. יintel-to detection
4. היה עוד כמה

מסקנה: **הידע שלי בתחום הזה הוא גם הזהות שלי**

אז איך ללמוד בעצם?

-> לא להתחיל ממושגים תלושים
-> להתחיל ממנגנונים (מנגון אימות, מנגנון אבטחה, בתחום מסויים על רכיב מסויים)
-> להבין מושגים שהם טיפה מעבר לבסיס Operational Abstractions
-> איך נראה בפועל תקיפה, איך מוציאים מידע מארגון

מנגנונים וכלים שמומלץ ללמוד

- EDR
- XDR
- AV
- IDS
- IPS
- SIEM
- SIGMA RULS
- YARA RULES
- FW
- VPN
- TLS/SSL
- WIERSHARK
- IdP
- REST API
- ANTIVIRUS
- MIMIKATS
- BURP
- JWT
- encreption

אנטי-גראביטי

IOC

---

*מסקנות מהמיטאפ:
לעבור על buzzwords, להירשם לdigital wisper, ללמוד כדי להבין דבירם באמת, ולא שמות של

מושגים.
חשוב להבין את הבסיס