

# NOC הונאות

## תחומי אחריות

# מבוא

- ☐ חזון – מטרות ותהליכי עבודה חדשים
- ☐ סיכונים עיקריים
- ☐ תרחישים עיקריים
- ☐ תכנית העבודה בפועל

# מחלקת הונאות

יוני 2022

**572** לקוחות הונאה

# סיכונים עיקריים

פגיעה כלכלית

פגיעה תדמיתית

פגיעת סייבר

אי עמידה ברגולציה

# תרחישים עיקריים

התרחישים העיקריים ורמת הסיכון

התרחיש הראשון



• בינונית

רכישה ואקטוב סים  
עם פרטים בדויים

# תרזשישים עיקריים

התרזשישים העיקריים ורמת הסיכון

התרזשי הנ"ל מתבצע האופן הבא:



ביצוע יצירת שיחות פיקטיביות מסימים שונים ליעדים יקרים מתבצע באופן הבא:



# תרחישים עיקריים

התרחישים העיקריים ורמת הסיכון

התרחיש השני



גבוהה

שכפול סים של  
לקוח קיים

- ❑ ניצול פרצה המאפשרת שכפול סים של לקוח קיים
- ❑ שימוש בסיים מקביל ללקוח
- ❑ פגיעה כלכלית בלקוח ובחברה
- ❑ סיכוני רגולציה (פרטיות, תקשורת וכו')
- ❑ פגיעה תדמיתית בחברה

# תרחישים עיקריים

התרחישים העיקריים ורמת הסיכון

התרחיש השלישי



גבוהה

שרשרת אספקה  
משווקים

- ☐ ממשיך אקטוב למשווקים
- ☐ יכולת לאקטוב מחדש סים הונאתי
- ☐ גישה למערכות החברה ללא הגנת סייבר משמעותית
- ☐ תגמול שלא לצורך
- ☐ גורם לבעיות אקטוב סים עם פרטים בדויים ושכפולי סים



# תרחישים עיקריים

התרחישים העיקריים ורמת הסיכון

התרחיש הרביעי



נדידה לחו"ל

• גבוהה מאוד

- ☐ גניבת סים בחו"ל
- ☐ שימוש אינטנסיבי ויקר בסיים בחו"ל עד לחסימתו
- ☐ במקרה שהTAPים מגיעים באיחור משמעו חשיפה כלכלית משמעותית
- ☐ במקרה שישולב עם הונאות אחרות (לדוג': אקטוב סים עם פרטים בדויים, שכפול סים וכו') – עלול לגרום לחשיפה מוגברת

# תכנית העבודה בפועל



# תכנית העבודה בפועל

אוטומציה- מערכת הונאה

כחלק מההתפתחות והחזון של מחלקת ההונאה, אנו נתמקד בפיתוח ותפעול של מערכת ההונאה ופעילות שוטפת באמצעות אוטומציה

נרצה לפתח

מערכת הונאה



הוספת מוניטורים

מוניטור מנויים ברומינג

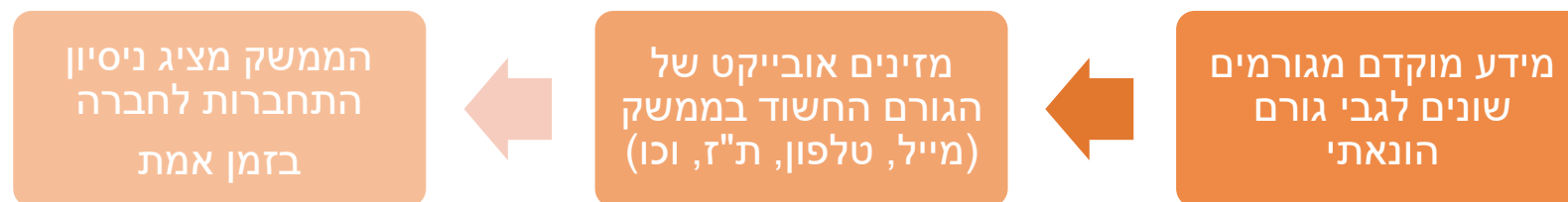
מוניטור מב"ל מנויי WE MOBILE



# תכנית העבודה בפועל

שדרוג ממשק Black List

Black list תורם למניעת הונאות באופן הבא:



נוסף לממשק:

ביטול חסימות	
חסימה בפועל	
התראות למייל בזמן אמת	

# תכנית העבודה בפועל

הכנסת עולמות נוספים- פרויקט NOC

העברת פעילות ה-NOC מ-OASIS לפעילות פנים ארגונית

מיפוי אתרים



הגדרות נהלים



פעילות הונאה •



גיוס נציגים



# תכנית העבודה בפועל

## הכנסת עולמות נוספים - Roaming

בין התרחישים עליהם דיברנו בתחילת המצגת, הינו התרחיש של נדידה לחו"ל, וכפי שציינו, זהו התרחיש ברמת הסיכון הגבוהה ביותר ובעל הפוטנציאל נזק הכספי הגדול ביותר.

קבלת קבצי ROAMING בזמן אמת\*

חסימה על פי RUL בעת זיהוי דפוס התנהגות חשוד

שליחת הודעות ללקוחות בנושא זהירות בעת נדידה

חסימת יעדים עוינים + ALERTS של מנויים בניסיונות חיוג

➤ פעילות שוטפת מול מחלקת ההונאה של פרטנר בעולם הנדידה

➤ עדכון מידי לאחראי ה-ROAMING בחברה

➤ איכון בנתב"ג להצעת חבילה ללקוח - הצעה לאלי ברומברג

\*במקרה של איחור של שלוש שעות לפחות- על מי הנזק?

# תכנית העבודה בפועל

אבטחת מידע פנימית – SOC



מוקד SOC מערך הסייבר של משרד התקשורת

## הכנסת פעילות SOC של משרד התקשורת

מוקד ניטור 24/7



שירות חינמי ✓



התראות בזמן אמת



בהצלחה לנו 😊