השתלמות לדירקטוריון החברה לפיתוח דרום הר חברות

19/06/2017

מי אנחנו?

שרון חי-מתן

- נשוי + 2
- חיי את עולם המחשוב כבר למעלה מ 20 שנה
- ניהל פרויקטי מחשוב בינלאומיים בחברות שונות

סלו פומרנץ

- נשוי + 3
- חי את עולם האינטרנט והסייבר כבר למעלה מ 18 שנה
- ניהל פרויקטים בינלאומיים בארץ ובמקסיקו

CYBER SECURITY – THE GAME
! RULES CHANGED

קצת היסטוריה

- מלחמת סייבר
- אופי המתקפות והסגנון שלהם השתנה במהלך השנים
- ההתקפות הראשונות בוצעו בתחילת שנות ה 60
- משנות ה- 60 ועד שנות ה 2000 רוב התוקפים היו "זאבים בודדים"
  - חיפשו הכרה חברתית
  - רצו להרגיש מוערכים על ידי ההשגים שלהם
  - כל פריצה למערכת היתה בשבילם הישג
- החל משנות ה 2000 העולם הפך להיות חברתי
- התוקפים התחילו להיפגש אחד עם השני
  - נוצרו קבוצות וירטואליות ופיזיות
  - נוצרו ארגונים
- ... וזו ההתחלה של מלחמת הסייבר

פשעי סייבר - CYBERCRIME

- בשנים הראשונות של פשעי סייבר, וונדליזם והרס היוו מוטיבציה
- מערכות טכנולוגיה, מחשבים ורשתות היו היעד
- הם היו עושים את על המאמצים להשבית מערכות מחשב ואת הרשת כדי להפוך אותם לא פונקציונליים.
- לשם כך הם שילבו את היכולות של כל חבר בקבוצה או בארגון לטובת ההתקפות.

- אז הם הבינו שהם יכולים לגנוב נתונים, וכי לנתונים יש ערך,
- זהו המניע השני שהביא למטרה השנייה "נוספה למשחק". MONEY
- עכשיו שהם הצליחו לגנוב נתונים, הם גם יכלו להשתמש / לסחור מידע ולמכור אותו בשוק
- ואז פשע מחשב הפך לעסק.

מה המניע להתקפות CYBER

גורמים

- מדינות – STUXNET, סנודן, WIKILEAKS
- פשע מאורגן – שם נמצא הכסף
- חברות עסקיות
- HACKTIVIST – אנונימוס, ארגוני טרור
- SCRIPT KIDDIES – אנשים שמנסים (רק תזכרו שגם ילדים אחראים משפטית)

סיבות

- פגיעה באויב, חשיפת סודות (מדיניים, צבאים, כלכליים)
- ריגול עסקי
- גניבת זהויות
- גניבת מידע
- סחיטה
- גניבת כרטיסי אשראי
- השחתת אתר
- מניעת שירות/זמינות

פשעי מחשב CYBERCRIME הם פשעים לכל דבר

- האקרים גונבים מידע מאנשים, חברות עסקיות, מוסדות פיננסיים וממשלה
- המידע שנגנב הוא בעל ערך ולכן ניתן לסחור בו
- עם הזמן ההתקפות נהפכו למסובכות, ההגנות בארגונים השתכללו וגם האקרים השתכללו.
- האקרים היו צריכים לחשוב מחוץ לקופסא, הם היו צריכים לאסוף מודיעין ולשלב מיומנויות חברתיות על מנת להגיע לאנשים בארגונים
- מכאן באה להם ההבנה שהידע שלהם לא צריך להיות המחשב, המערכת הארגונית אלא החברה, העסק והעובדים בו. דרכם ניתן יהיה לפרוץ לארגון
- רשתות מחשבים וטכנולוגיה עדכנית (כדוגמת IOT) הפכו להיות הנשק ולא המטרה של התקיפה

TECHNOLOGY AS A CRIME PLATFORM

- האקרים משתמשים, נעזרים בטכנולוגיה כדי להתקרב למטרה שלהם
- המניעים שלהם יכולים להיות שונים
  - וונדליזם והרס
  - לגנוב מידע
  - הונאות
  - כחלק מפשע מסורתי
- רשתות חברתיות נהפכו למקום בו מתקשרים בין האנשים
- קבוצות האקרים נהפכו לגלובליות
- התקשרות בין האנשים באמצעות ה DarkNet מאפשרת לשתף מידע על התקפות, ליצור קשרים ולהעזר אחד בשני לטובת תקיפות
- מאפשר שמירה על אלמוניות
- Pinpoint attacks ! – התקפות על מדינות, ארגונים, ממשלות ואנשים

סוגי התקפות

- **Old School Hackers** – התקפות מסורתיות, הם לא מסחריות, זה לא מעניין את האקר, אותו מעניין הטכנולוגיה והיכולת לפרוץ
- **Cyber Punks** - פרחחי סייבר, המטרה שלהם לתקוף, לזרוע הרס, להשחית ולשבש את הארגון אותו תוקפים. המטרה שלהם להתרברב ביכולות שלהם
- **מקצוענים** – המטרה שלהם לגנוב מידע על מנת לסחור בו, להשתמש במערכות כפלטפורמה לפשעים אחרים כמו סחיטה Ransomware איסוף מידע ועוד.
- **CODERS** – כותבי קוד ויוצרים כלי פריצה להאקרים אחרים
- **גורמים פנימיים בארגון** – עובדי הארגון המבצעים התקפה פנימית, גניבת מידע או הונאה מראש, בכוונה או בטעות
- **האקטיוויסטים** - הם מפריעים על מנת להציג השקפה חברתית או פוליטית.
- **הממשלה** - איסוף מודיעין.

מהלך תקיפה

איסוף מידע
פיתוי
הפניה
ניצול פירצה
החדרת פוגען
התקשרות למרכז שליטה
הפשע
CALL HOME

דצמבר 2014 - האלבום החדש של מדונה נגנב

ספטמבר 2014 - נגנבו ליותר
מ-100 נשים מפורסמות תמונות אישיות

ההתקפה על חברת SONY הביאה לחשיפת מידע רגיש

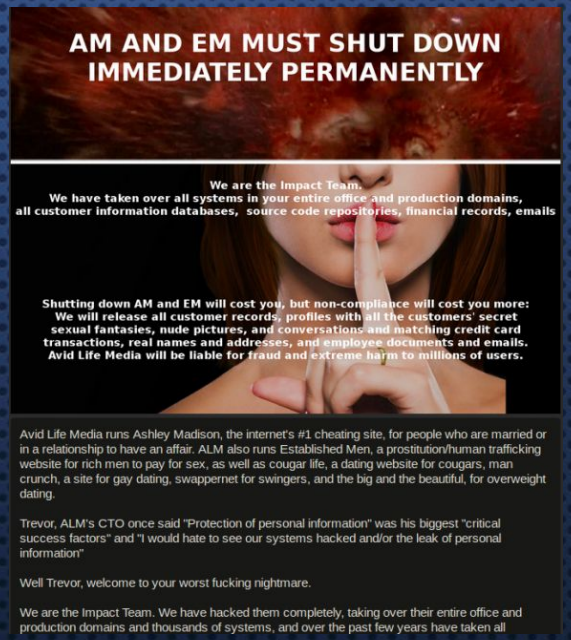
- דצמבר 2014
- 12Tb של מידע
- 25Gb של מידע רגיש על 10 אלף עובדים
- פרטים על עובדים
- פרטים על שחקנים

התאוששות מהתקפת סייבר היא ארוכה וכואבת

כשהפרטי מתחבר לציבורי

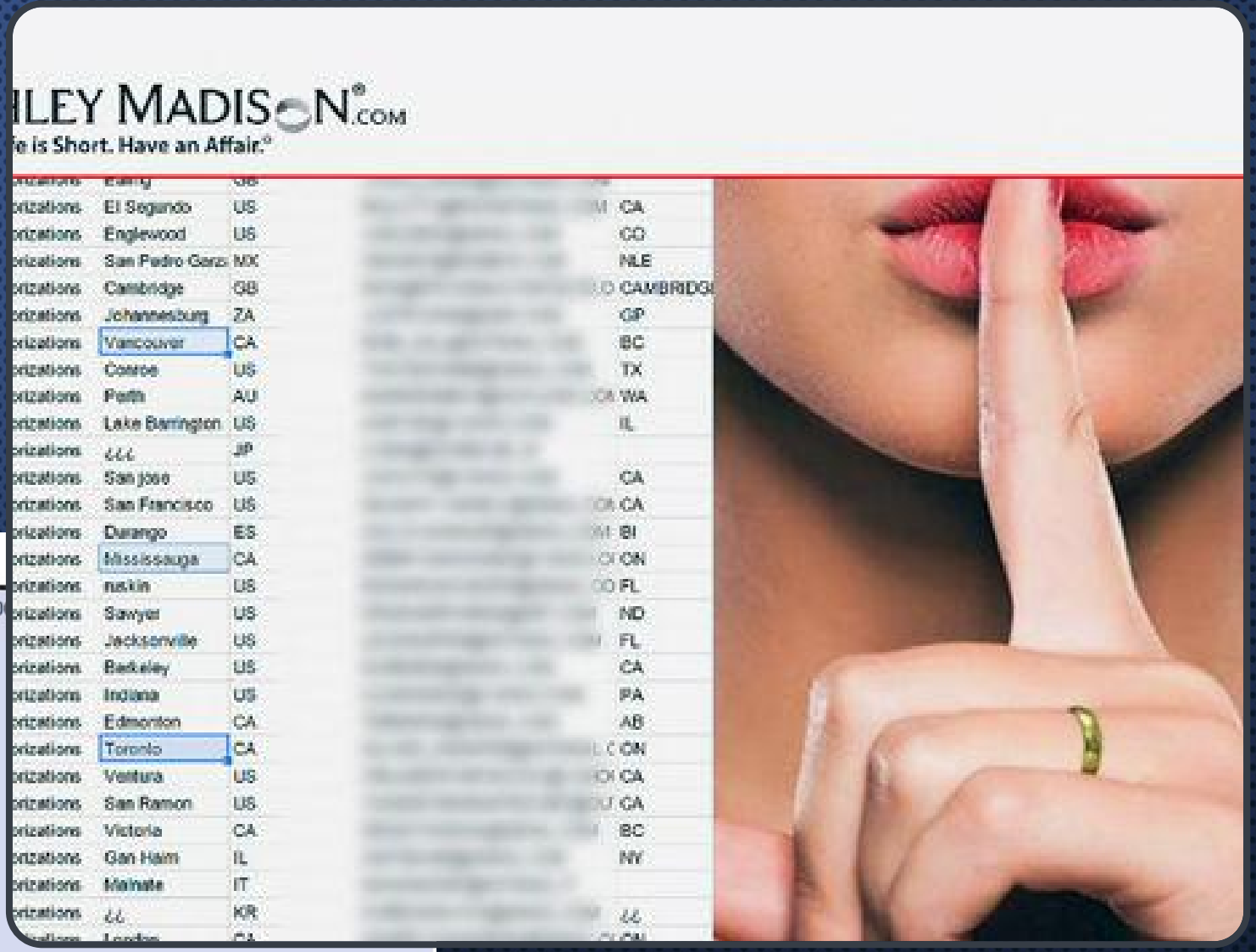
אתר הבגידות אשלי מדיסון

- יולי 2015
- 37M משתמשים רשומים
- פרטי הנישואים שלהם
- ההעדפות המיניות
- פרטי האשראי
- 3 התאבדויות



ואם ידלוף מי קונה היכן?

- דרך אגב 90% מהפרופילים של גברים
- רוב הפרופילים של נשים מזייפים
- 37,000 רשומים מישראל
- לסקרנים אפשר להוריד את הרשימה מ TORRENT



>>2978058
>gov.uk

gov.uk

a.burridge@agma.gov.uk
adam.oconnell@hants.gov.uk
adam.wrightham@northlincs.gov.uk
adele.casey@lbhf.gov.uk
alison.moten@qcda.gov.uk
Andrew.moth@hantsfire.gov.uk
andrew_rust@sandwell.gov.uk
Anthony.doyle@northumberland.gov.uk
Anthony.Doyle@Northumberland.gov.uk
barry.wright@london-fire.gov.uk
Benedict.moore@london-fire.gov.uk
Berndard.wilde@salford.gov.uk
Bob.house@hantsfire.gov.uk
Brenda.webster@merton.gov.uk
brian.allen1@nissa.gsi.gov.uk
brian.lawley@thepensionservice.gsi.gov.uk
brian.mcgeary@doeni.gov.uk
Bryn.green@kirklees.gov.uk
christoper.willard@westsussex.gov.uk
colin.dale@coi.gsi.gov.uk
connor.haughey@newryandmourne.gov.uk
csbradley@dstl.gov.uk
Darren.clark@leeds.gov.uk
darren.clifford@lancashire.gov.uk
Dave@wirral.gov.uk
david.dougherty@nissa.gsi.gov.uk
david.fuller@towerhamlets.gov.uk
David.jones@conwy.gov.uk
David.rowe@forestry.gsi.gov.uk

Anonymous 08/18/15 (Tue) 15:11:35 ID: 00000

VATICAN STRUGGLES

sample-dump:

dave1234@alpha.va
amaznjohn@co.henry.va
evelyn.zangl-milbrand@med.va
jack.blansett@med.va
phazlewood@sympatico.va
jgarland@tax.state.va
terence.green@pps.k12.va
terence.green@pps.k12.va
rmorgan@lva.lib.va
jmoore@co.arlington.va
jcook@meck.k12.va
michael.catalano@owen.va
thelmick@city.suffolk.va
f_buddy72@yahoo.va
llabra@alexandria.lib.va
michael.catalano@owen.va
seandwyer@alum.va
John.Guerin@med.va
charles.donovan@owen2001.va
paul_smith@co.roanoke.va
wifeswetpanties2003@yahoo.va
vscjclif@vba.va
hinklema@ci.staunton.us.va
peter.veruk@owen.va

JPMORGAN

- 76M פרטי בתי אב
- 7M פרטי עסקים קטנים ובינוניים
- נפרץ ב:2011,2012,2014
- מידע נלקח ממחשב של עובד

eBay

145M פרטי משתמשים

דוא"ל, כתובת מגורים, שמות משתמשים וסיסמאות

OPM

- יולי 2015
- 21.5M רשומות עובדים
- 5.6M טביעות אצבע באיכות גבוהה כולל סוכנים חשאיים

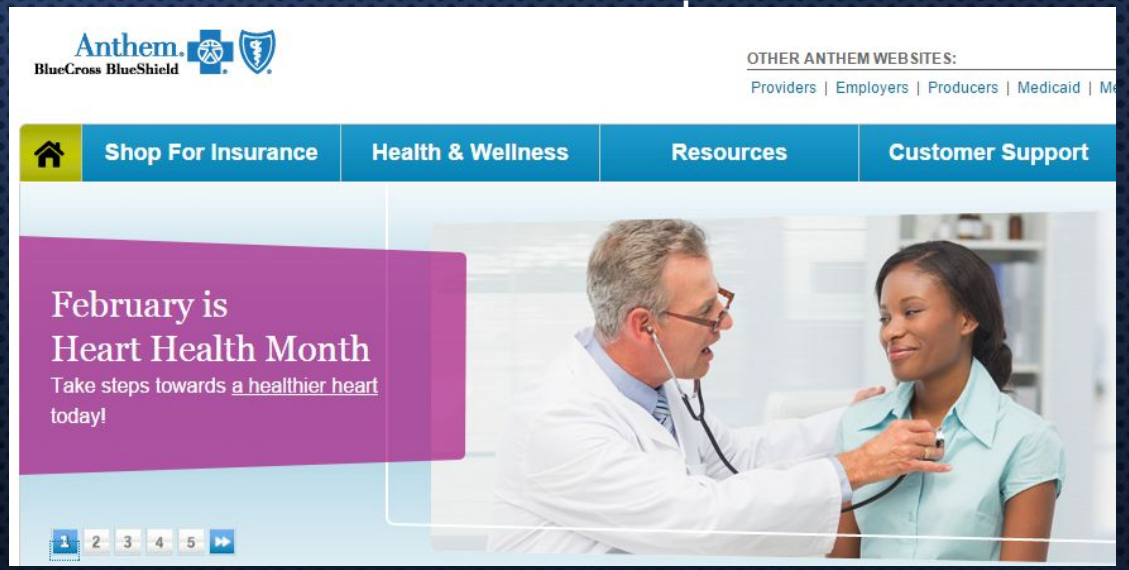
Carbanak cybergang גנבו $1B מ־100 מוסדות פיננסיים בעולם

- פברואר 2015
- עד 10M דולר בכל פשיטה
- מערכות הבנק, כספומטים וחשבונות "מילוט"

לרגל אחרי המרגל

ANTHEM פברואר 2015

- 80 מיליון פרטים של אנשים
  - תאריכי לידה
  - מספרי ביטוח לאומי
  - כתובות
  - מספרי טלפון



לאומי קארד נובמבר 2014

ניסיון סחיטה ע"ב של 2 מיליון פרטי כרטיסי אשראי של כ 1.5 מיליון לקוחות, 100 שדות נתונים על כל לקוח שנגנבו ע"י עובדי החברה

הסחיטה בלאומי קארד: המשטרה חושדת שהשתמשו בפרטי האשראי המשטרה בודקת אם החשוד המרכזי אלירן רוזנס השתמש בעשרות אלפי שקלים. המשטרה מבקשת להאריך את מעצרו, שותפיו עשויים להשתחרר

אלי סניור פורסם ב 14:19 , 20.11.14 :ynet

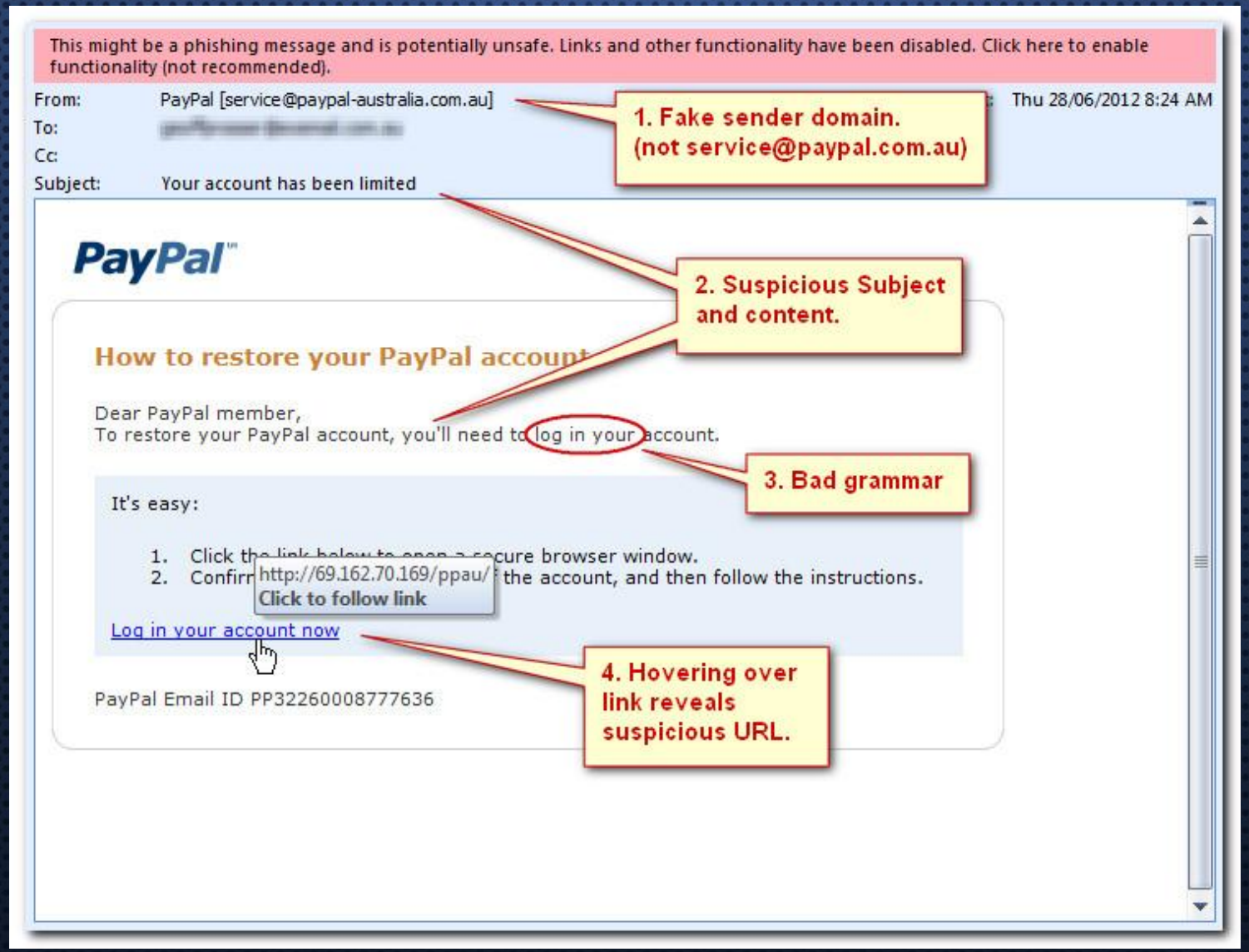
החשודים בפרשת לאומי קארד בבית המשפט (צילום: עידו ארז)

שלב הפיתוי – FISHING

"לקוח יקר
זה הבנק שלך. שכחנו את מספר ת"ז וסיסמא. למה שלא תשלח אותם חזרה אלינו כדי שנוכל להגן עליך?

יש לי תחביב חדש הוא נקרא דיוג
שלחתי דוא"ל מזויפים מהבנק למנהלים פתיים ואז אני מוצא את המידע הפיננסי שלהם ומשתמש בו כדי לגנוב כסף שהם שלא מגיע להם
לקוח יקר, זה הבנק שלך. שכחנו את מספר ת"ז וסיסמא. למה שלא תשלח אותם חזרה אלינו כדי שנוכל להגן עליך?
נראה רשמי

היו זמנים.....


This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (not recommended).
From: PayPal [service@paypal-australia.com.au]
To:
Cc:
Subject: Your account has been limited
Thu 28/06/2012 8:24 AM
1. Fake sender domain. (not service@paypal.com.au)
PayPal
2. Suspicious Subject and content.
How to restore your PayPal account
Dear PayPal member,
To restore your PayPal account, you'll need to log in your account.
3. Bad grammar
It's easy:
1. Click the link below to open a secure browser window.
2. Confirm the account, and then follow the instructions.
http://69.162.70.169/ppau/
Click to follow link
Log in your account now
4. Hovering over link reveals suspicious URL.
PayPal Email ID PP32260008777636

גם זבל משתבח עם הזמן

היי,
לפני 6 ימים הייתי שם. בפגישה עם כמה חברה

מאוד רציניים בביזנס. היו שם איזה 3 מגה
חנונים שסיפרו את סיפור הכי אישי,
ואת המאחורי הקלעים של העסק שלהם.

והאמת?
ממש הופתעתי.

אם אתה רוצה לדעת איך 3 חנונים

מקימים עסק בלתי שגרתי לכל הדעות,

מאויימים ע"י פמיניסטיות אכזריות,
מתחתנים עם דוגמניות,

ומייצרים אימפרייה ישראלית **שמדפיסה 30 מיליון שקל . . .**

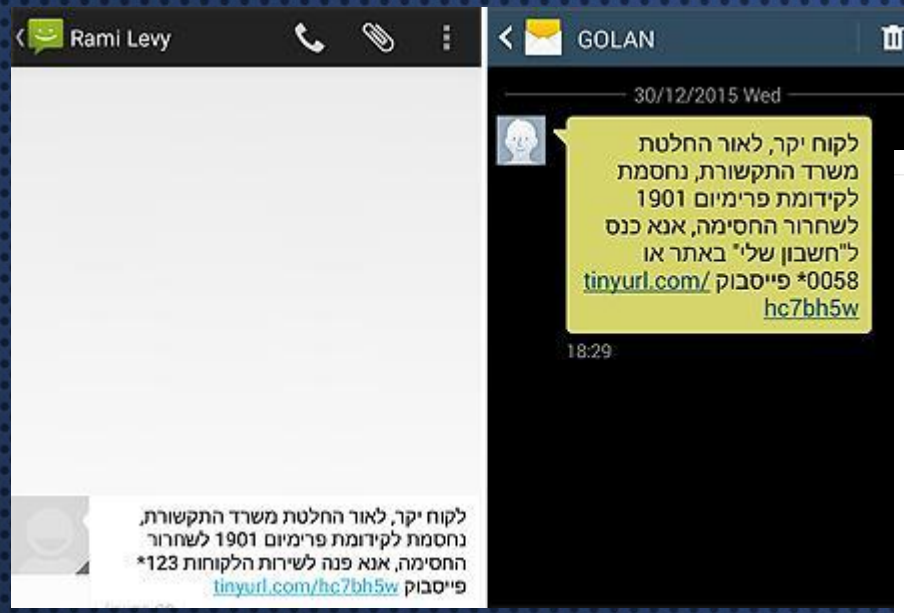
אז הסרט **הדוקומנטרי הזה**
הוא הדבר *הכי טוב* שראית אי פעם.
(הוא קצר)

עכשיו, הנה למה:
אם 3 חנונים, עם יכולות חברתיות של מטאטא שבור,
בלי הורים עשירים,
בלי רקע כלכלי,
ועם ביטחון עצמי ששואף לביטחון של בואש בשיא פעולתו הטבעית...

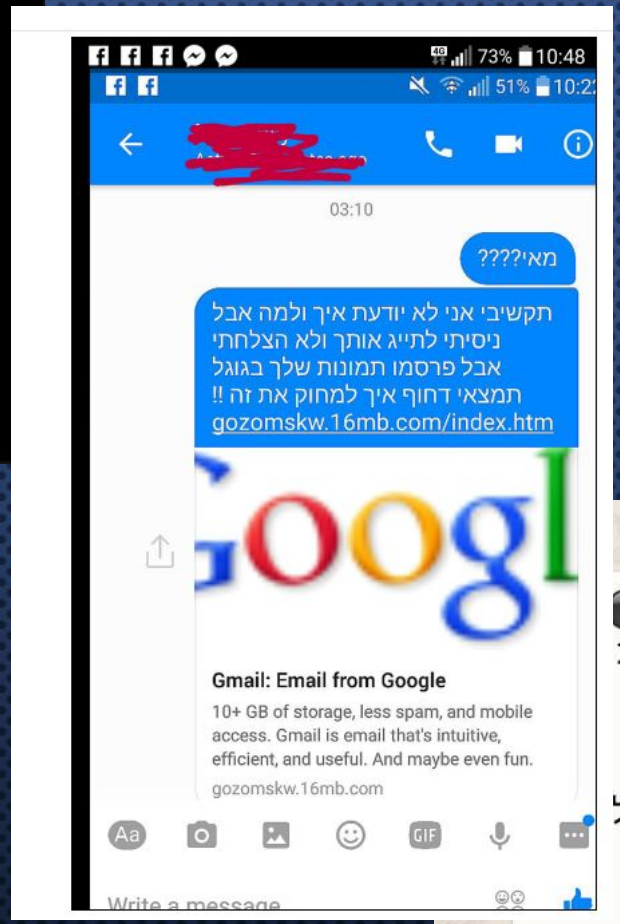
הצליחו להרים את **המעורת נחשים המפוארת הזאת**,
שמחזיקה ב"וובוס" חצי מהמדינה וזה לא רק בתחום העיסקי...
כנראה שהם יודעים לפחות דבר 1 שיעזור לך.

היום

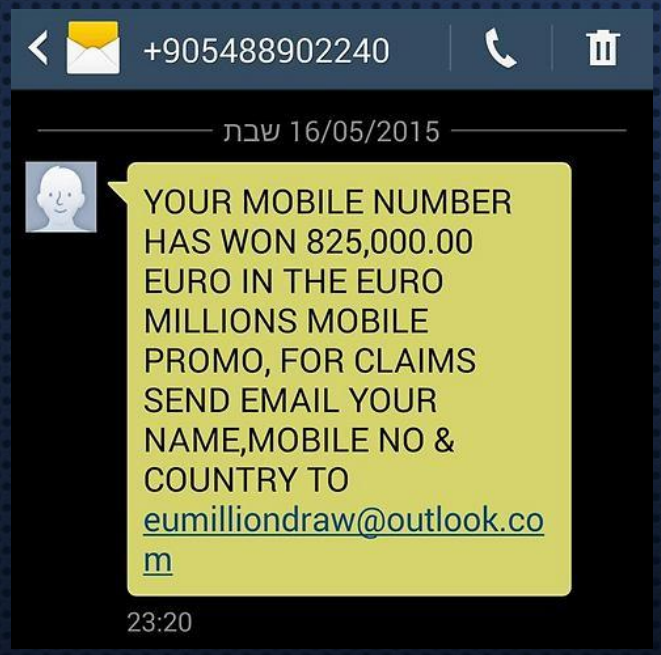
- דוא"ל, SMS, WHATSAPP
- עברית רהוטה
- מגיע מאדם מוכר לך
- שימוש במידע שנאסף עליך
- שימוש בחלקים מהאתר המקורי
- שימוש בפסיכולוגים מומחים לשיווק

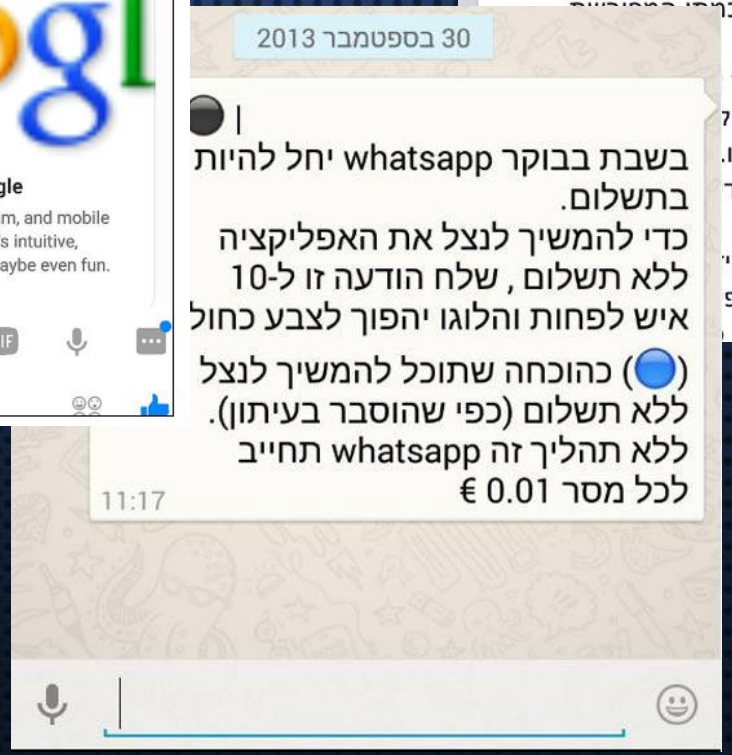

Rami Levy
לקוח יקר, לאור החלטת משרד התקשורת, נחסמת לקידומת פרימיום 1901 לשחרור החסימה, אנא פנה לשירות הלקוחות 123*
פייסבוק tinyurl.com/hc7bh5w

GOLAN
30/12/2015 Wed
לקוח יקר, לאור החלטת משרד התקשורת, נחסמת לקידומת פרימיום 1901 לשחרור החסימה, אנא כנס ל"חשבון שלי" באתר או
פייסבוק 0058* tinyurl.com/hc7bh5w
18:29

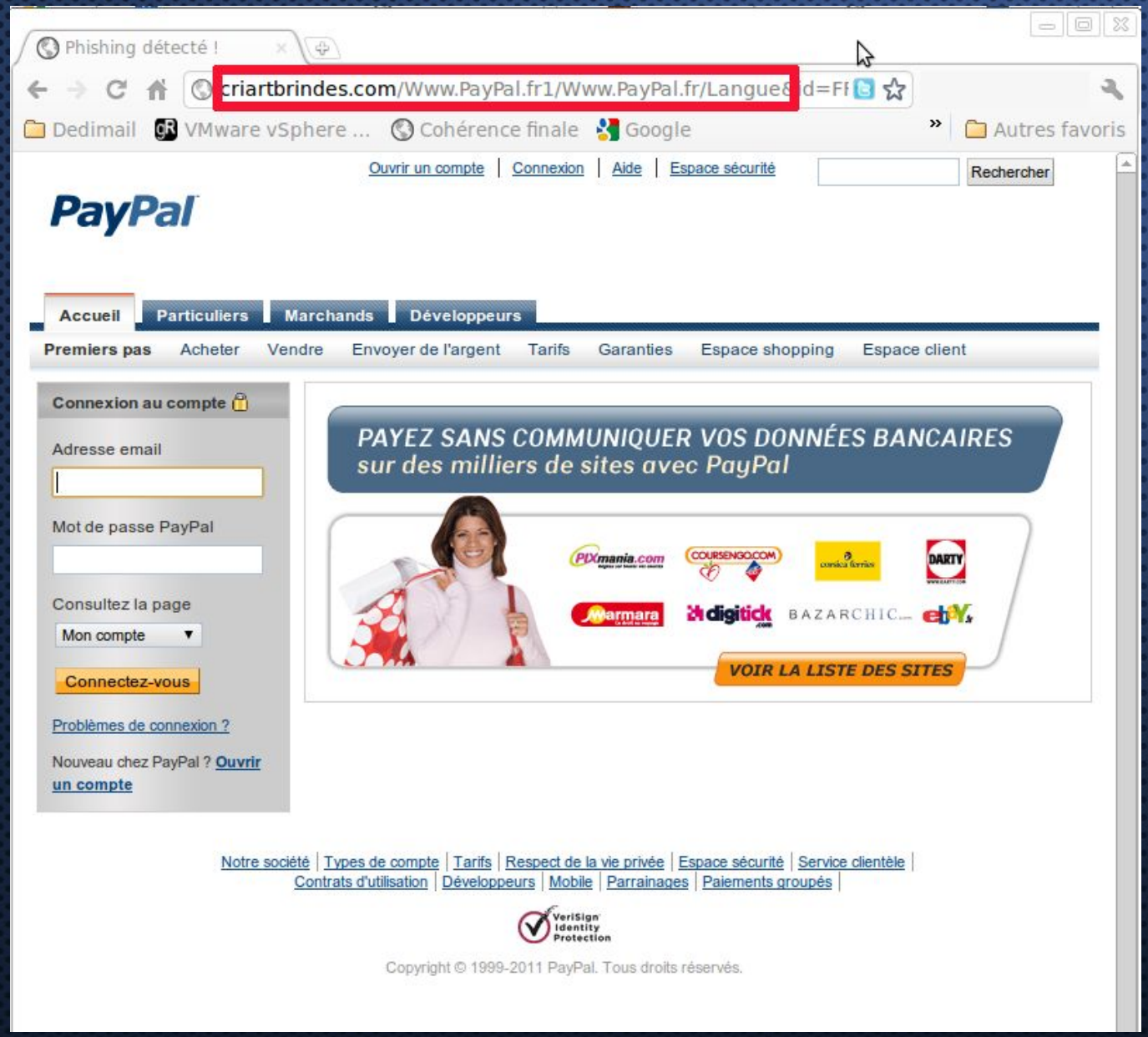

03:10
מאי????
תקשיבי אני לא יודעת איך ולמה אבל ניסיתי לתייג אותך ולא הצלחתי אבל פרסמו תמונות שלך בגוגל תמצאי דחוף איך למחוק את זה !!
gozomskw.16mb.com/index.htm
Gmail: Email from Google
10+ GB of storage, less spam, and mobile access. Gmail is email that's intuitive, efficient, and useful. And maybe even fun.
gozomskw.16mb.com
Write a message

ORANGE 3G 23:16 95%
Post
6 hours ago near Tel Aviv
בלי לפגוע בזכויות
==========
אני , בשל העובדה כי פייסבוק בחרה לערב תוכנה שתאפשר לגנוב מידע אישי שלי, מצהיר בתאריך 18 בספטמבר 2014, בתגובה למדריך החדש של פייסבוק, ובהתאם לסעיפים 112, ,L.111 113 של קוד הקניין הרוחני, כי הזכויות שלי תקפות לגבי כל הנתונים האישיים שלי, שירים, צילומים, ציורים, תמונות, קריקטורות, קומיקס, טקסטים, מוזיקה וכו' , המפורסמים בפרופיל שלי ובנספחיו.
לכל שימוש מסחרי נדרשת הסכמתי
בכתב.
על פייסבוק נאסר באיסור חמור
להפיץ, לשדר, או לנקוט כל פעול
בסיס פרופיל זה ו/או התוכן שלו.
שהוזכרו לעיל חלים גם על עובד
או אנשים בניהולו של פייסבוק.
התוכן של הפרופיל שלי מכיל מי
הפרטיות שלי תגרור עונש על-פ
1-103 1-308 1-308 ו רומא).

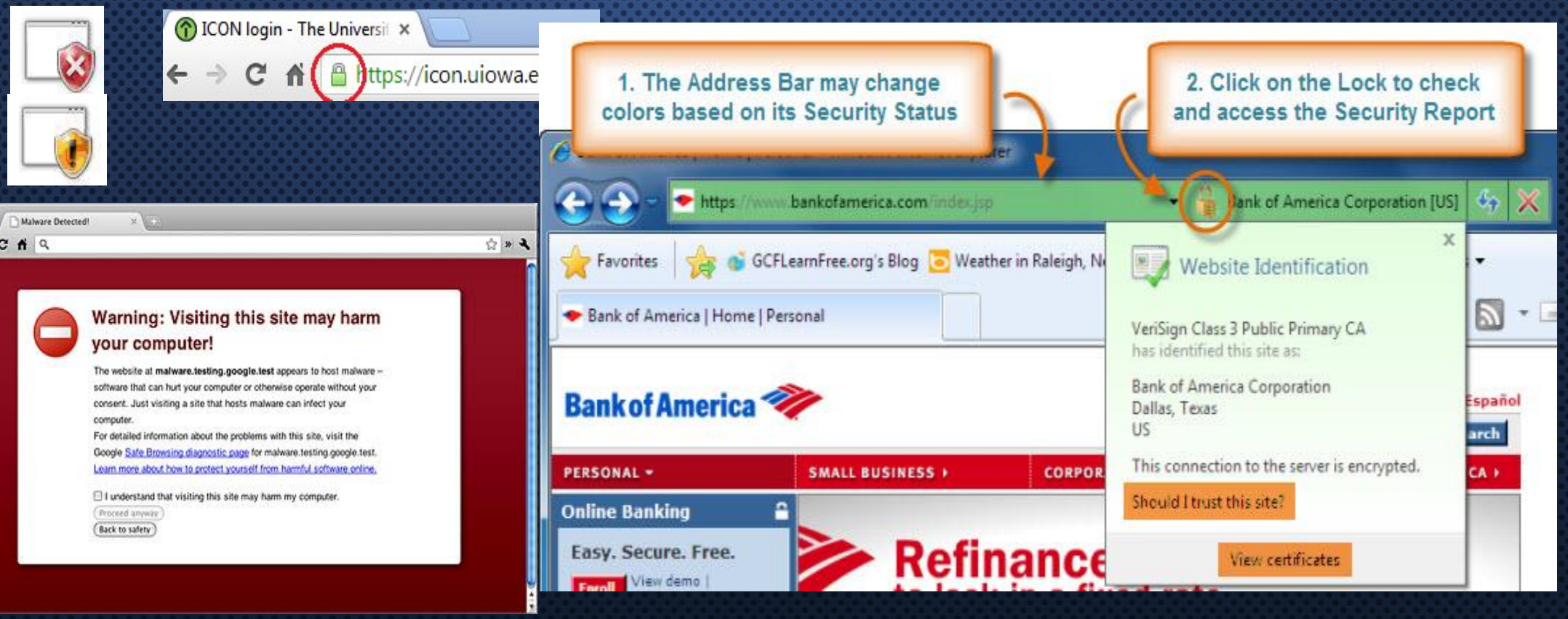

+905488902240
16/05/2015 שבת
YOUR MOBILE NUMBER HAS WON 825,000.00 EURO IN THE EURO MILLIONS MOBILE PROMO, FOR CLAIMS SEND EMAIL YOUR NAME,MOBILE NO & COUNTRY TO eumilliondraw@outlook.com
23:20


30 בספטמבר 2013
בשבת בבוקר whatsapp יחל להיות בתשלום.
כדי להמשיך לנצל את האפליקציה ללא תשלום , שלח הודעה זו ל-10 איש לפחות והלוגו יהפוך לצבע כחול
(🔵) כהוכחה שתוכל להמשיך לנצל ללא תשלום (כפי שהוסבר בעיתון).
ללא תהליך זה whatsapp תחייב לכל מסר € 0.01
11:17

הפניה לאתר FISHING



שימו לב לפרטים הקטנים



ReInquiry f514f830p417n06h5150s036r838 - Message (Plain Tex...

Message

From: Fiona G. Cabrera [redacted]

Sent: Mon 3/20/2017 1:48 PM

To: [redacted]

Cc:

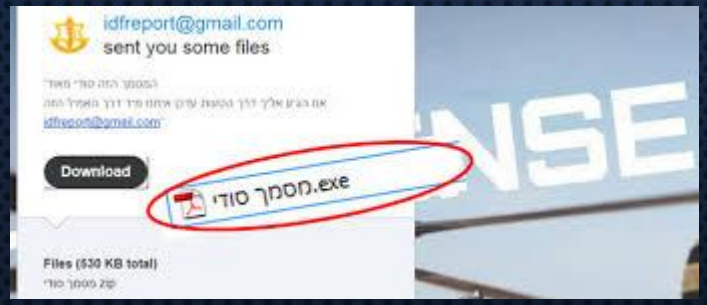
Subject: ReInquiry f514f830p417n06h5150s036r838

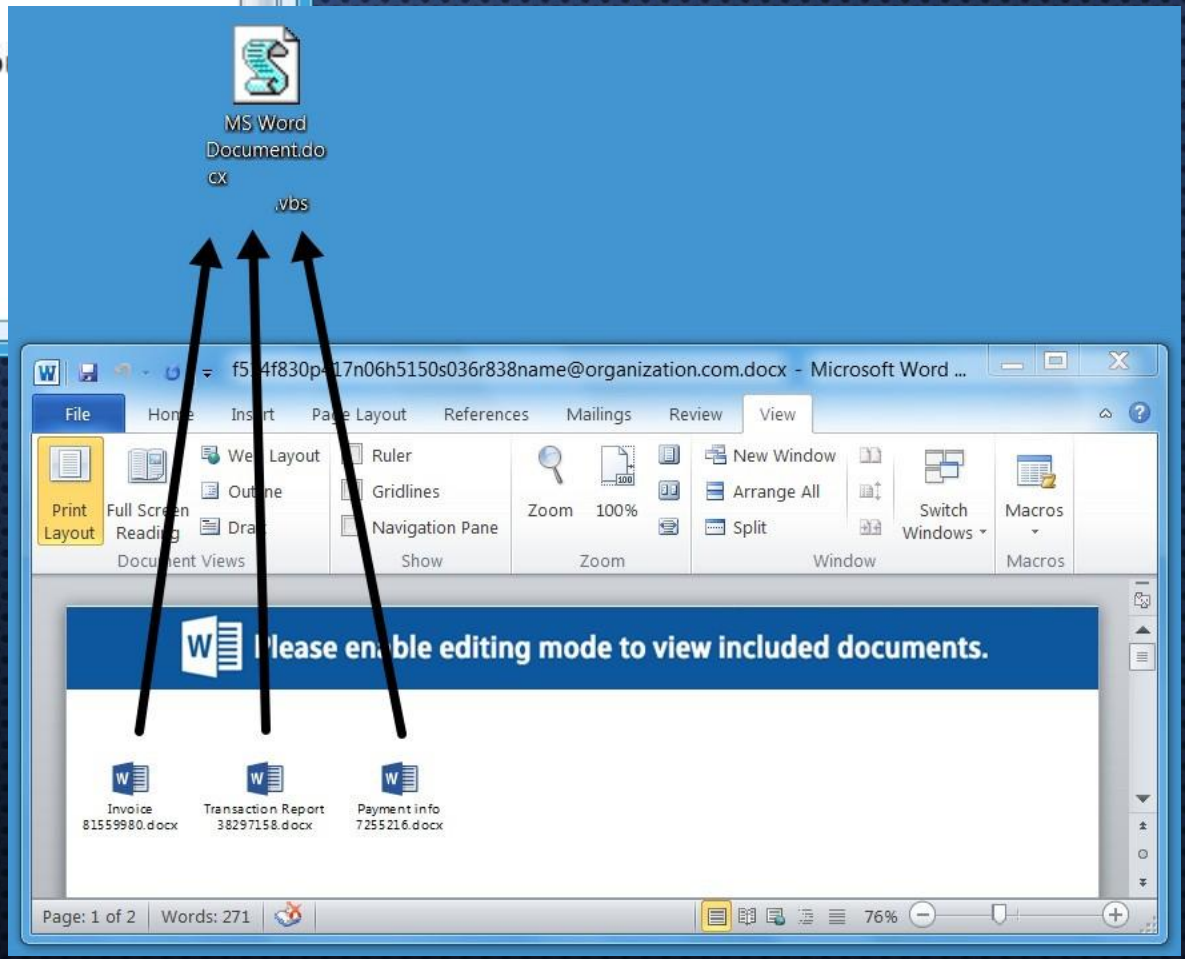
Message | f514f830p417n06h5150s036r838[redacted].docx

Check the payment report created for [redacted] as yo
ordered.

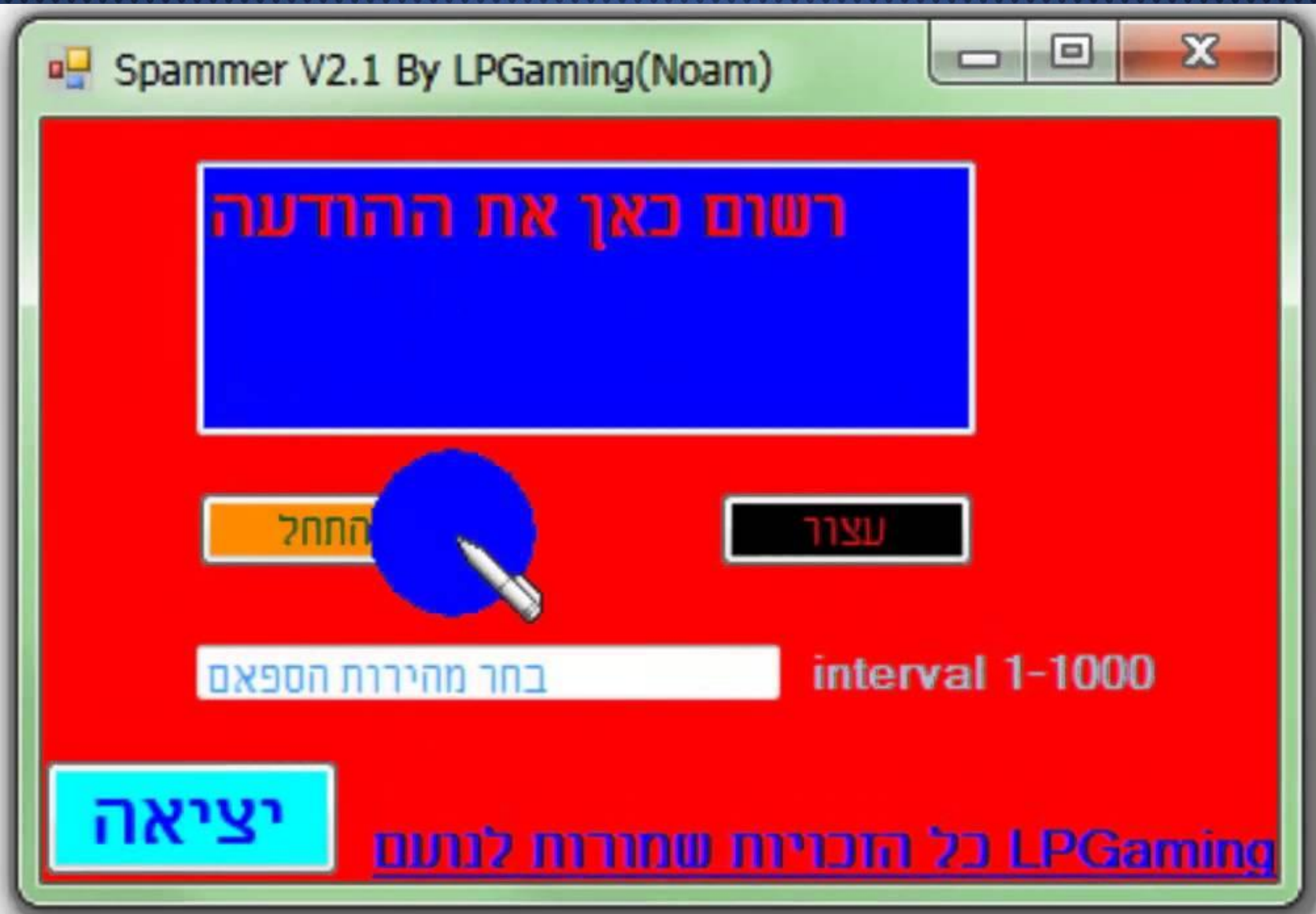
You may need Doc Passcode: EoD7FmeBW

Fiona G. Cabrera

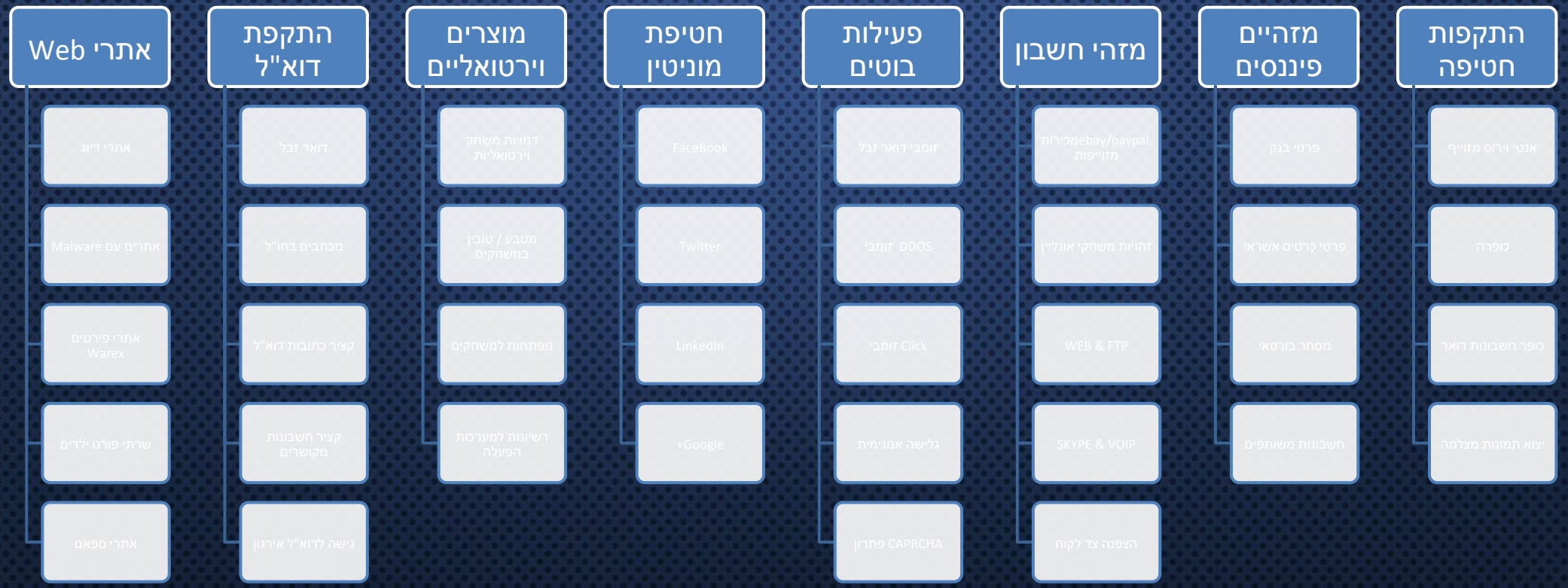




מערכת SPAM


Spammer V2.1 By LPGaming(Noam)
רשום כאן את ההודעה
התחל
עצור
בחר מהירות הספאם
interval 1-1000
יציאה
כל הזכויות שמורות לנועם LPGaming

גורמים לפריצות בארגון



סיסמאות נפוצות

ניתוח מידע מתוך מאגרים שנפרצו

- 1. 123456 (Unchanged)
- 2. password (Unchanged)
- 3. 12345 (Up 17)
- 4. 12345678 (Down 1)
- 5. qwerty (Down 1)
- 6. 123456789 (Unchanged)
- 7. 1234 (Up 9)
- 8. baseball (New)
- 9. dragon (New)
- 10. football (New)
- 11. 1234567 (Down 4)
- 12. monkey (Up 5)

13. letmein (Up 1)
14. abc123 (Down 9)
15. 111111 (Down 8)
16.mustang (New)
17. access (New)
18. shadow (Unchanged)
19. master (New)
20. michael (New)
21. superman (New)
22. 696969 (New)
23. 123123 (Down 12)
24. batman (New)
25. trustno1 (Down 1)

סוגי סיסמאות נפוצות

- שם חיית מחמד
- תאריכים: לידה (כולל ילדים ובני זוג), נישואים, סיום תיכון...
- מספר טלפון
- שמות ילדים
- מקום לידה
- חופשה אהובה
- קבוצת ספורט אהובה
- שם בשפה זרה
- רצף אותיות במקלדת

לעולם אל תמסור את הסיסמה שלך. בחר סיסמה מורכבת.

ELAL-COM.US

אל על מציעה 2 כרטיסים חינם לכל אחד! כדי לחגוג את יום השנה ה -70

Like Comment Share

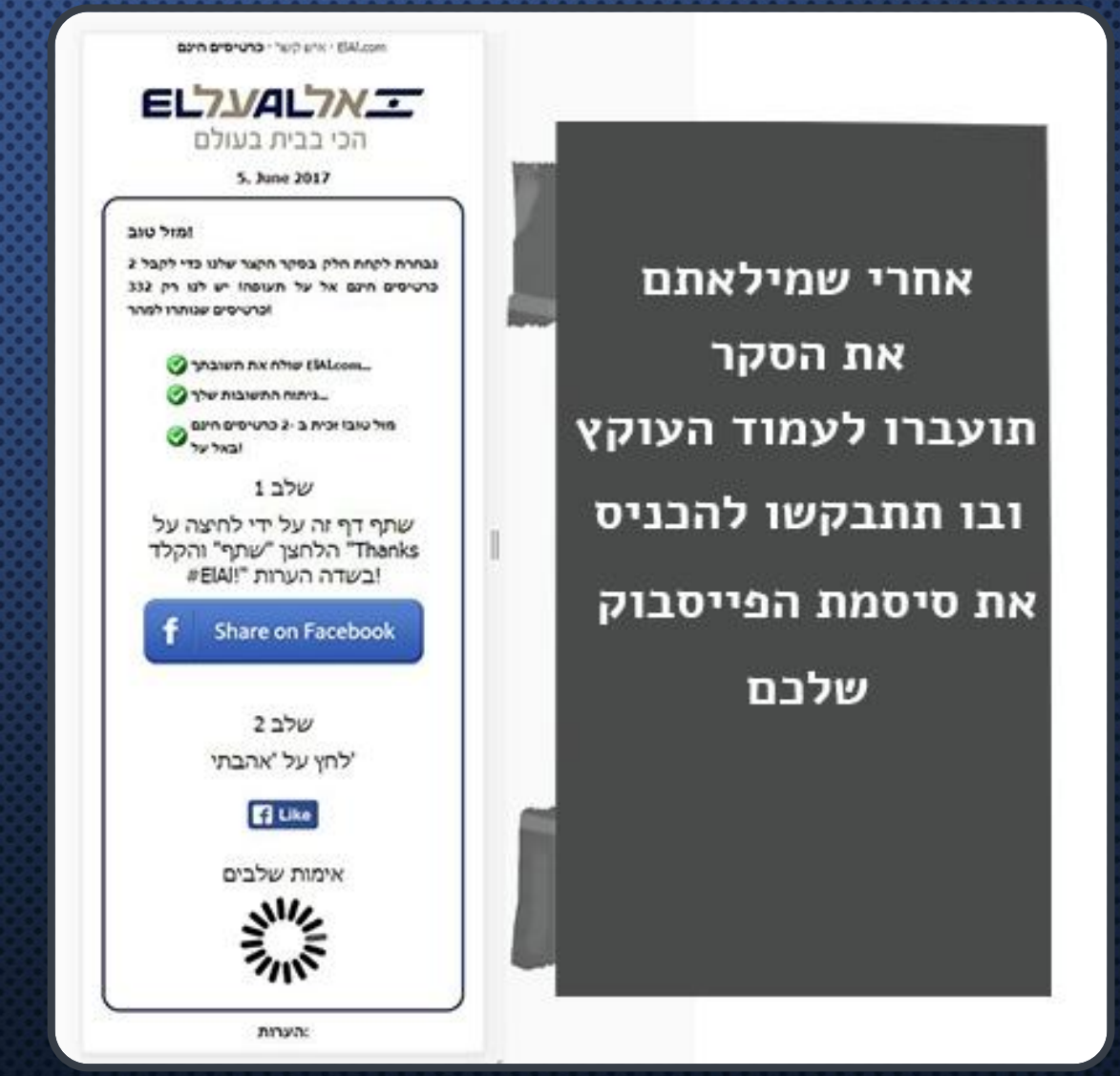
אל על מציעה 2 כרטיסים חינם לכל אחד! כדי לחגוג את יום השנה ה -70

(2 כרטיסים) לאדם

ELAL-COM.US

- הכתובת של האתר הרשמי של אל-על היא WWW.ELAL.COM
- עוד הכתובת שאתם תועברו אליה היא זו:ELAL-COM.US
- שמתם לב כבר להבדל הפשוט הזה? במידה והתפתיתם ללחוץ על הקישור שאיזה ידיד/מכרה/סבתא/אחיינית או סתם עמית לעבודה שיתפו בפיד, הרי שתגיעו לעמוד נחיתה שמתחזה לסקר שביעות רצון עילג במיוחד של אל-על:

לאחר שתסיימו לענות על הסקר בן שלוש השאלות תגיעו לעמוד העוקץ, העמוד ובו תתבקשו להכניס את פרטי ההתחברות שלכם לפייסבוק וגם לשתף את דבר ההגרלה. במידה ועשיתם את זה - הרי שהענקתם למישהו גישה לכל פרטי החשבון שלכם ומומלץ כי תשנו את הסיסמא שלכם ללא דיחוי.



אגב, בתחתית עמוד הסקר צורף גם פיד פיקטיבי של פייסבוק עם משתמשים פיקטיביים ותגובות פיקטיביות לא פחות. על פי הכתוב כאן, נראה כי מי שעמל על מתקפת הדיוג הזו אינו בקיא בעברית וכי נעשה כאן שימוש בגוגל טרנסלייט בהצלחה חלקית בלבד:

הודעת אל על .....

EL AL אל על
11 hours ago
לקוחות יקרים, ביממה האחרונה התפרסמה מודעה המבטיחה 2 כרטיסי טיסה חינם למשתתפים בסקר. באל על מבקשים להבהיר כי מדובר בהודעה שקרית (ספאם). אל על פנתה כבר אתמול לחברה שהאתר הפיקטיבי יושב בשרתיה וביקשה להסירו באופן מיידי. עד כה טרם הוסר האתר ואל על בוחנת את המשך צעדיה. במקביל פנתה אל על לפייסבוק בבקשה להסיר את הקישור.
755
454
559

מערכות הגנה קיימות – לא מספיקות מול האיומים

- התוקפים גדולים יותר במונחים של מספרים
- התוקפים מפוזרים ומאורגנים היטב ואנונימיים.
- תחומי שיפוט בינלאומיים עוזרים להם להסתתר.
- לתוקפים יש פלטפורמות תקשורת, כלים מתקדמים וידע טכני טוב יותר
- דוגמא :
  - מערכות אבטחה נוכחיות - מערכות מניעת חדירות מסחריות - יכולות לזהות ולחסום עד 40,000 סוגי התקפות.
  - כלים מסחריים - יכולים לנצל 80,000 סוגי התקפות.
  - כלי פריצה קוד פתוח - יכולים להגיע 50,000 סוגי התקפות
  - שילוב של האקר מנוסה עם כלים מסחריים וקוד פתוח, סקריפטים בעבודה ידנית יכול להגיע 100,000 סוגי התקפות.

המצב הנוכחי ואיך להגיב אליו

- אנחנו לא 100% מוגנים , כל ארגון משקיע המון כסף ואנרגיה במערכות אבטחת מידע
- ניסיונות להתקפות בארגון משאירות עקבות
- אנו בטוחים שכל ארגון מיועד להתקפה ובסופו של דבר גם ייפרץ
- מערכות אבטחת מידע כותבות לוגים על כל מה שקורה במערכת
- מידע, מחקרים ונתונים על התקפות מתעדכנים כל יום ואפילו כמה פעמים ביום
- ישנן חברות המספקות מודיעין סייבר בצורה מסחרית
- ארגונים הדוגמת ה CERT משתפים מידע על ארועים והתקפות

תגובת מנע!

- המפתח להגנה הוא ידיעה וגילוי מוקדם של התקפות
- אנחנו צריכים לקחת את המידע העצום שנוצר על ידי מערכות אבטחה, לצבור אותו, לנתח אותו ולהעשיר אותו עם מידעים חיצוניים כמו מודיעין, INTELLIGENCE, מידע מ-CERT וכן הלאה.
- ניתוח המידע הנאסף במערכת ובדיקתו מול מידע פנימי ומידעים חיצוניים
- אנליסטים אבטחת מידע - אנשי מקצוע בעלי הכשרה גבוהה, היודעים כיצד לקרוא ולהגיב על ניתוח המידע.
- צוותי תגובה המוכנים לפעול בזמן!

THE WORK FLOW

Firewalls

Window Server

Linux Server

I.P.S

Switches

Router

1

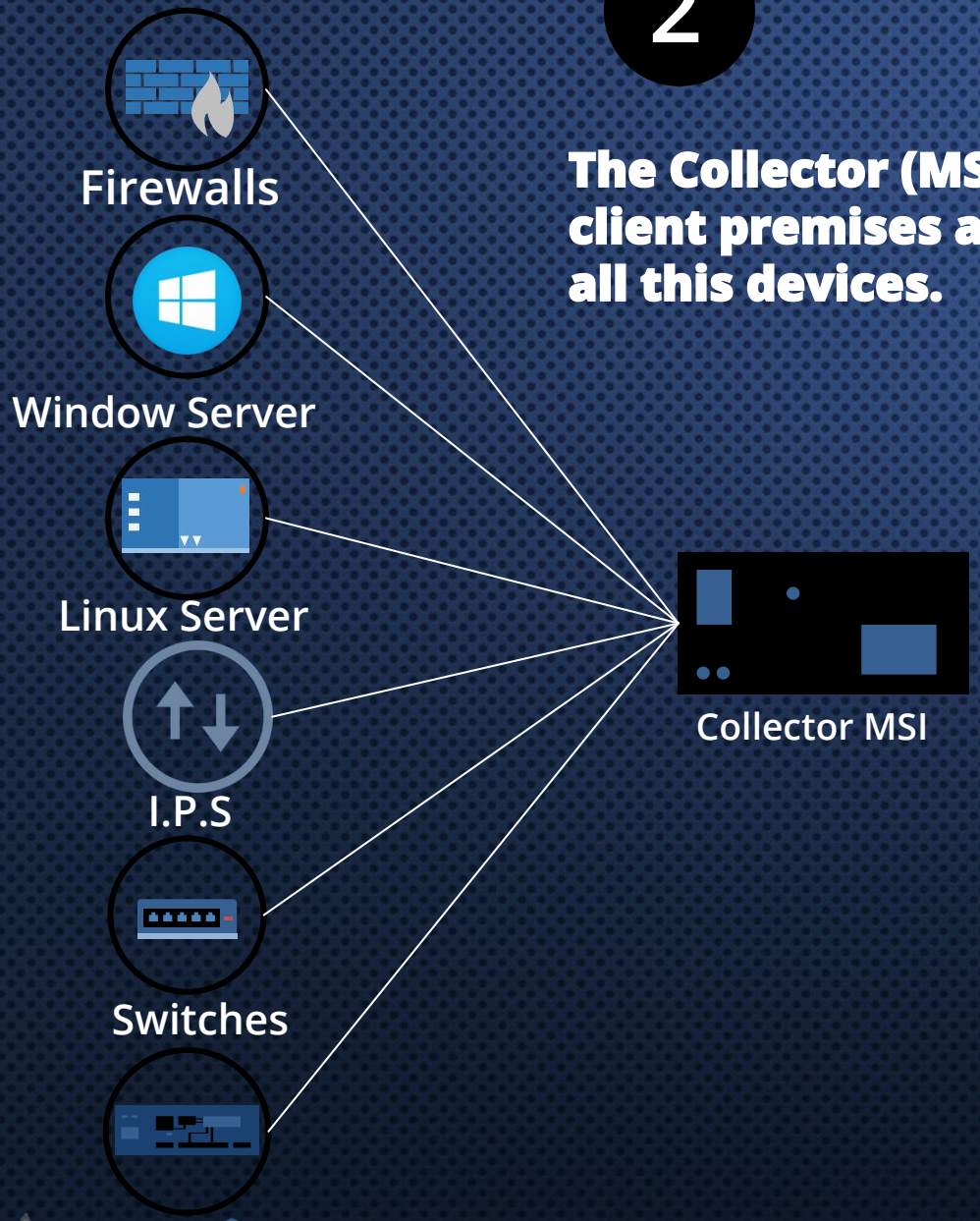
The company has different IT and Information Security Devices, such as Firewalls, IPS, Switches, routers, proxies, Anti Spam, Antivirus , Windows Servers, Linux Servers and others. Each Device Creates Its Own Security Log With Security Information On It.

Integrity
Consulting & Risk Management

CYBERSHARK
BLACKSTRATUS

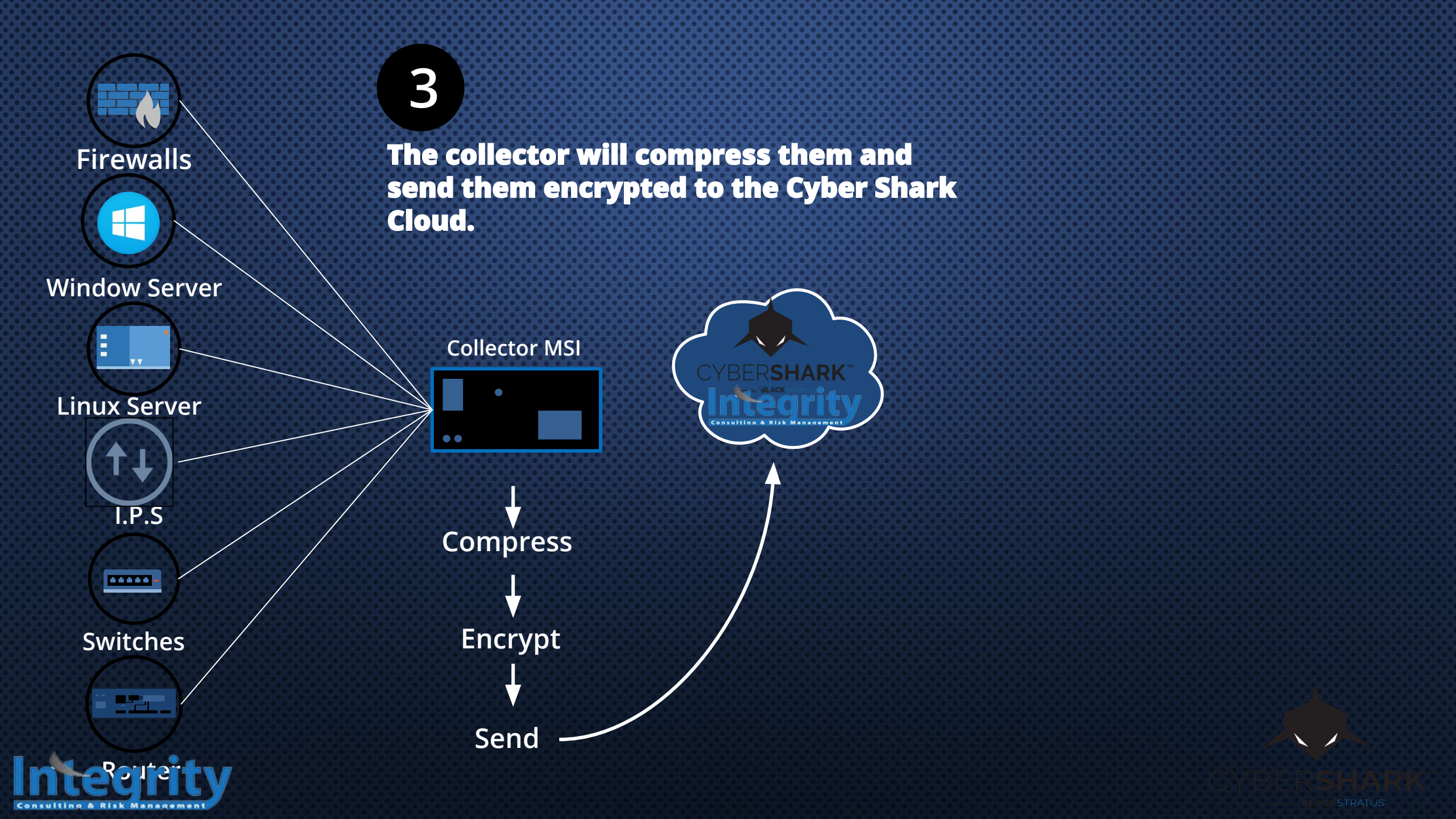
2

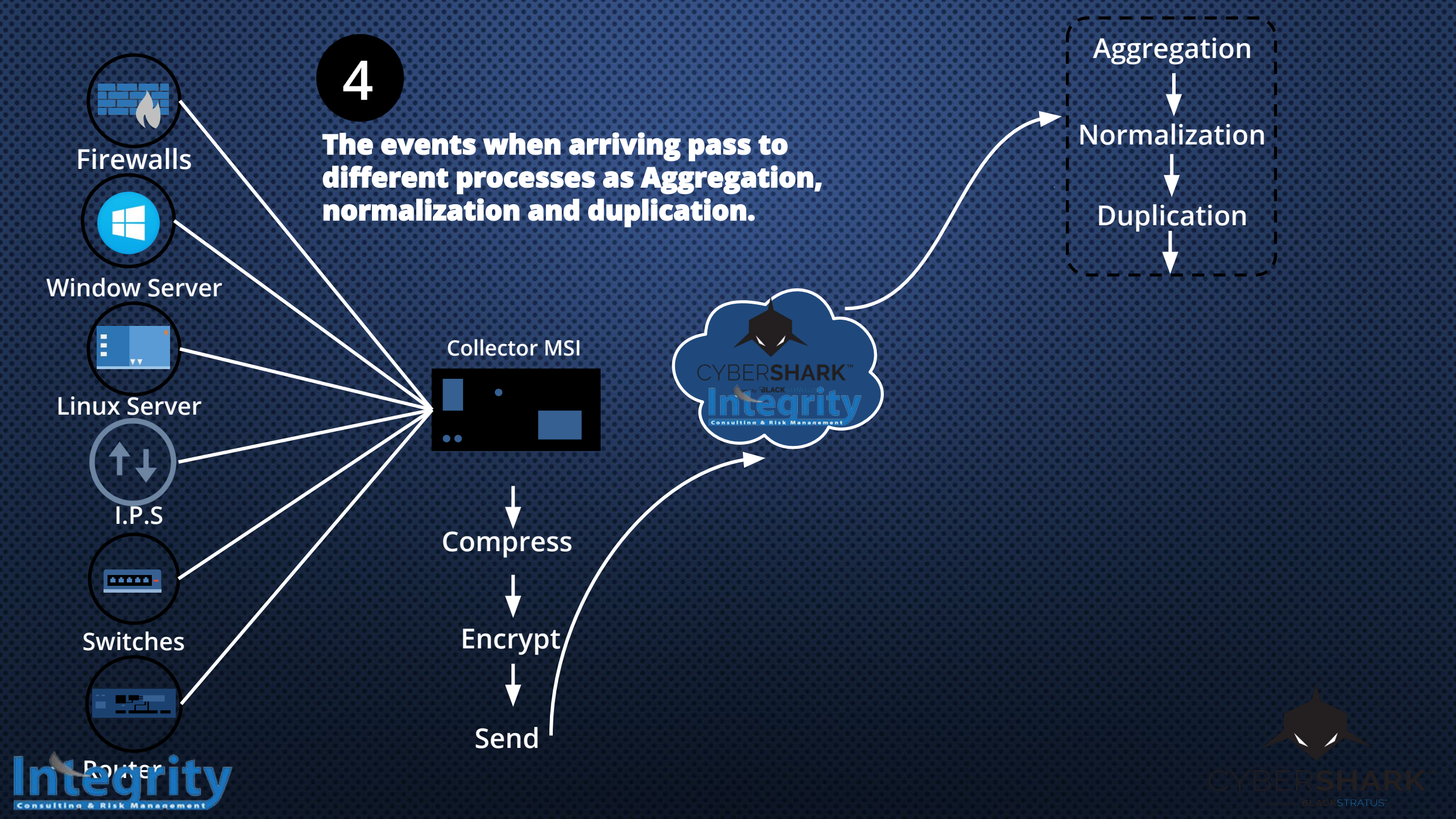
The Collector (MSI) will be installed on the client premises and will take the logs from all this devices.

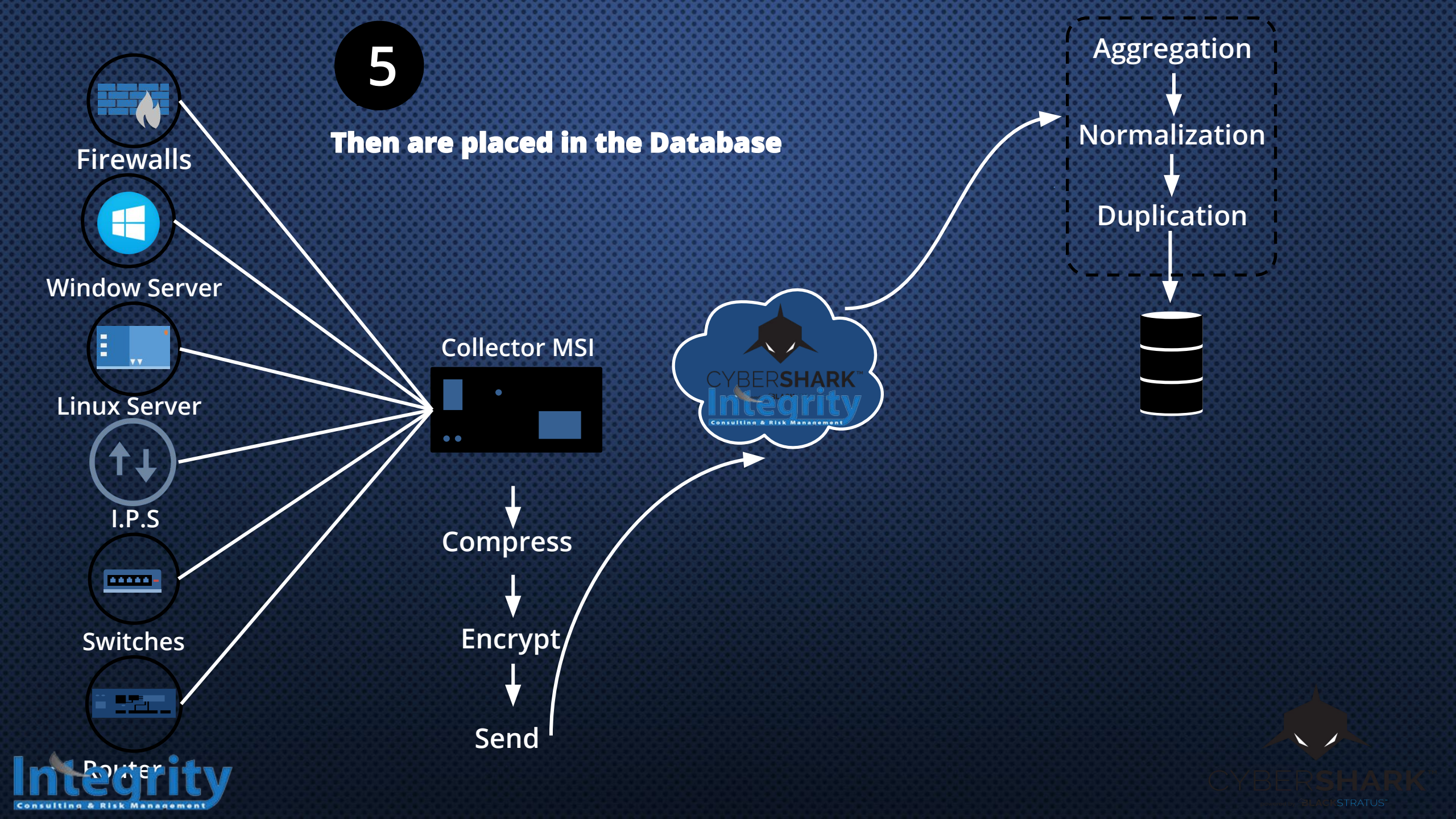


Integrity
Consulting & Risk Management

CYBERSHARK
BLACKSTRATUS


3
The collector will compress them and send them encrypted to the Cyber Shark Cloud.
Firewalls
Window Server
Linux Server
I.P.S
Switches
Router
Collector MSI
Compress
Encrypt
Send
CYBERSHARK
Integrity
Consulting & Risk Management
BLACKSTRATUS


4
The events when arriving pass to different processes as Aggregation, normalization and duplication.
Firewalls
Window Server
Linux Server
I.P.S
Switches
Router
Collector MSI
Compress
Encrypt
Send
CYBERSHARK
Integrity
Consulting & Risk Management
Aggregation
Normalization
Duplication
Integrity
Consulting & Risk Management
CYBERSHARK
BLACKSTRATUS

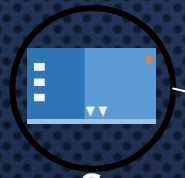

5
Then are placed in the Database
Firewalls
Window Server
Linux Server
I.P.S
Switches
Router
Collector MSI
Compress
Encrypt
Send
CYBERSHARK
Integrity
Consulting & Risk Management
Aggregation
Normalization
Duplication
Integrity
Consulting & Risk Management
CYBERSHARK
BLACKSTRATUS

6

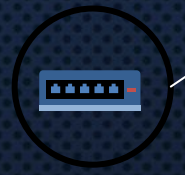
The Data on database is enriched by external sources as Blacklists and others. IT is passed through a complex set of correlation rules.

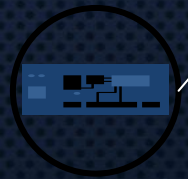
Firewalls

Window Server


Linux Server

I.P.S


Switches


Router

Collector MSI

Compress

Encrypt

Send

Aggregation

Normalization

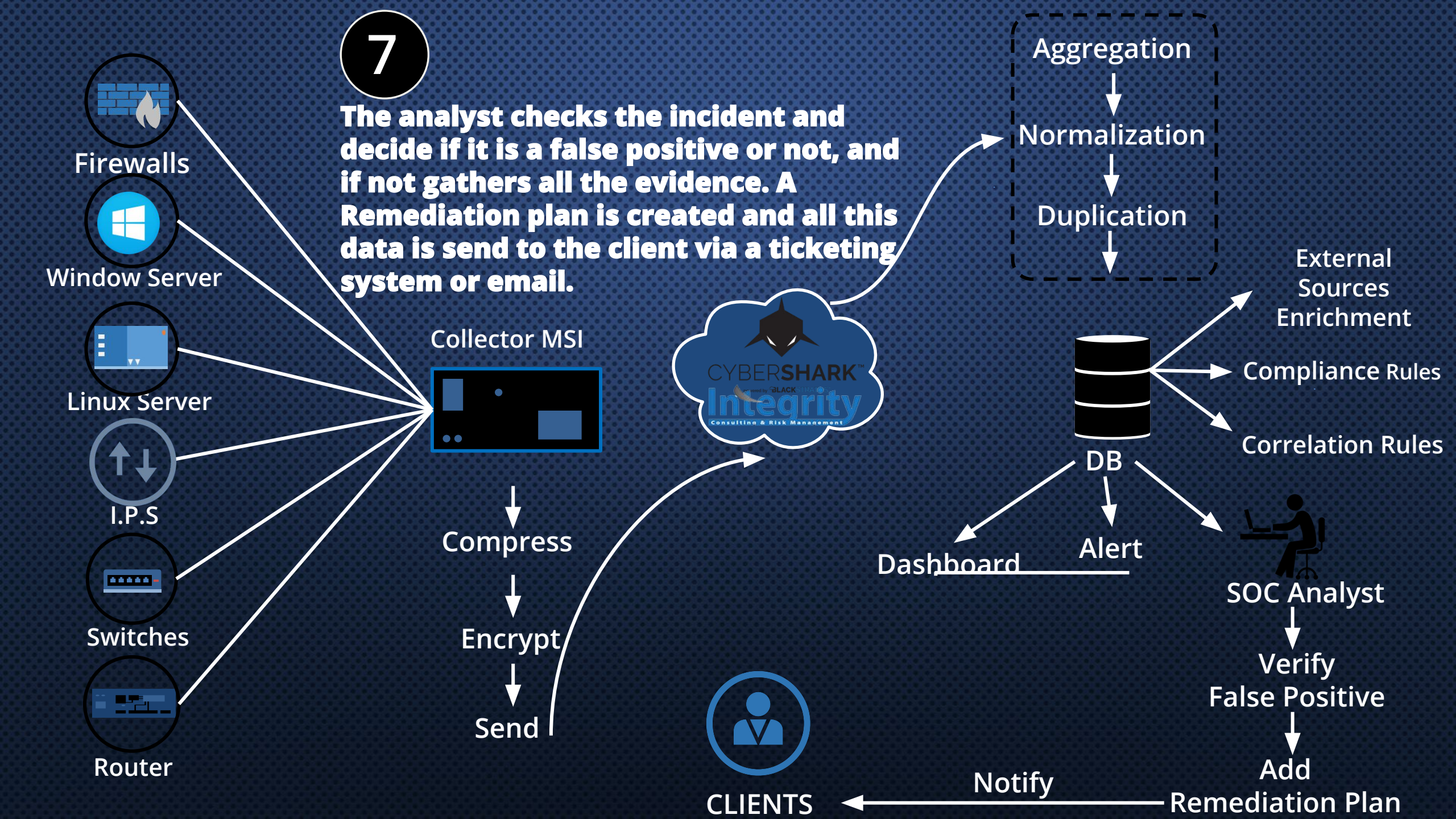
Duplication

DB

External Sources Enrichment

Compliance Rules

Correlation Rules

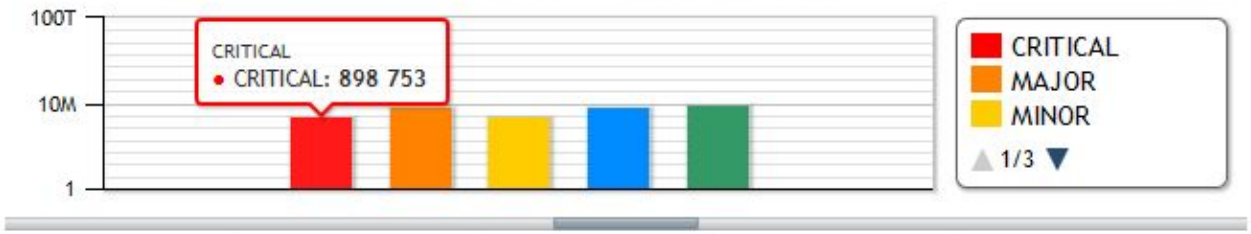

7
The analyst checks the incident and decide if it is a false positive or not, and if not gathers all the evidence. A Remediation plan is created and all this data is send to the client via a ticketing system or email.
Firewalls
Window Server
Linux Server
I.P.S
Switches
Router
Collector MSI
Compress
Encrypt
Send
CYBERSHARK
Integrity
Aggregation
Normalization
Duplication
External Sources Enrichment
Compliance Rules
Correlation Rules
DB
Dashboard
Alert
SOC Analyst
Verify False Positive
Add Remediation Plan
Notify
CLIENTS

מסך ניהול האיומים בארגון

Integrity
Consulting & Risk Management

Monitor | Detect | Inspect | Compliance | Event Search | Tools | Customers

Event by Severity (Last 90 Days - Chart maximum: 20 items) for DemoShark



CRITICAL	MAJOR	MINOR	WARNING	INFORMATIONAL
898753	6208857	1063078	6705198	9648864

Events and Aggregated Events (Current Month - Chart maximum: 20 items) for DemoShark

PERIOD	EVENT COUNT	AGGREGATED EVENTS
2016-12-31	7316	2871
2017-01-01	61815	31815
2017-01-02	52541	28047
TOTAL	322602	143863

Executive Summary (Current Month - Chart maximum: 20 items) for DemoShark

AFTER AGGREGATION	BEFORE AGGREGATION	THREATS	TOTAL CASES	OPEN CASES	CLOSED CASES	OTHER CA
143863	322602	0	4	1	2	1

Distribution of Events by Category (Current Month - Chart maximum: 20 items) for DemoShark

CATEGORY	EVENT COUNT
System Status / Configuration	121335
Authentication / Access / Authorization	201280
TOTAL	322615

Regulations

- Full compliance for:
  - HIPAA
  - PCI
  - Sarbanes/Oxley
  - FISMA
  - And other regulations
- that your business must adhere to, as well as log collection & retention with full legal chain of custody

Integrity
Consulting & Risk Management

CYBERSHARK
BLACKSTRATUS

Case Details Summary

Case Id: 19797

Name: Communication with CnC after DriveBy or FakeAV-(Source:10.0.0.2)

Status: Closed - Confirmed

Priority: Critical

Complexity: Low

Impact: Undefined

Description: Communication with CnC after DriveBy or FakeAV-(Source:10.0.0.2)

Internal device 10.0.0.2 connected to blacklisted fake anti-virus/command and control IP address 52.204.129.22, then connected to command and control IP address 54.85.127.70. Recommend scanning internal device for malware.

Summary of Tasks (additional info - https://cybersoc.atlassian.net/wiki/display/CKB/Incident+Response+-+Communication+with+CnC+after+DriveBy+or+FakeAV)

1. Detection/Identification - CYBERShark has created an incident (communication with a CnC after communication with a DriveBy or FakeAV). Please assume that device has been

מקרה אירוע

- מקרה מלפני שבוע, שבת, המערכת זיהתה התנהגות חשודה. תקשורת בין מחשבים לאינטרנט
- המערכת התריעה על הבעיה
- הציגה דרכי פתרון מידיים לסגירת הפרצה
- צוות תגובה נכנס לפעולה וסגר את הפרצה
- ביום ראשון הארגון ביצע בדיקה מעמיקה לתחקור ופעילויות שונות

THANK YOU

שרון – 054-5680114
Sharon@corporateintegrity.co.il

סלו – 052-3653227
Salo@corporateintegrity.co.il