CYBER CONTROL

Creating Safe Business Value

פתרונות ושירותים מנוהלים להגנת
הסייבר ואבטחת המידע בארגונים

www.cybercontrol.co.il

054-5977779

info@cybercontrol.co.il

אנו יודעים כי לא לכל דבר אפשר להיערך מראש,
אבל להתקפת הסייבר הבאה- בהחלט אפשר וצריך!

מתוך תפישה זו, אנו ב- Cyber Control התאמנו ללקוחותינו -מארגוני סטארט אפ ועד ארגוני ענק, מגוון פתרונות וחבילות שירות המאפשרות גמישות ומודולריות מרבית:

החל מייעוץ ושירותי ליווי של מנהלי אבטחת מידע, דרך אימון וסימולציות להנהלות לטובת מוכנות ארגונית, ועד ביצוע תהליכי זיהוי, חקירות מתקדמות ותהליכי תגובה מלאים כחלק מהשירותים המנוהלים שלנו.

חבילות שירות ופתרונות אלו, מותאמים לצורכי הארגון המשתנים – תשתיות קיימות, רגולציות ותקנים, סיכונים והלימה לצרכים העסקיים.

הודות לתפישה מתקדמת זו של פתרונות ושירותים מנוהלים, אתם תוכלו להתמקד בפיתוח ליבת העסקים הארגונית, ואנו נדאג להגנה על נכסי הארגון שלכם, על פי צורך ודרישה.

CISO as a Services

Chief information security officer - CISO
הוא לרוב הסמכות הבכירה בארגון בכל הקשור להיבטי אבטחת מידע והגנת הסייבר.

CISO כשירות ניתן על פי צורכי ודרישות הארגון. השירות כולל הובלת מדיניות, כתיבת נהלים, ליווי, תקנים ורגולציות, ייעוץ טכנולוגי ועוד.

צוות ה-" CISO כשירות" שלנו בעל ניסיון רב בניהול אבטחת מידע במגוון ארגונים, החל מגופי Unicorn, startup ועד לחברות Enterprise בארץ ובעולם.

השירות כולל:

- הפעלת צוות תגובת וניהול משברים
- התאוששות מאסון וניהול המשכיות עסקית
- ניהול זהויות וגישה
- פרטיות מידע
- תאימות רגולטורית (למשל, PCI DSS אמריקאי, GLBA, FISMA, GDPR, PIPEDA, HIPAA)
- ניהול סיכוני מידע
- אבטחת מידע בהיבטי טכנולוגיה
- מעקב יישום בקרות טכנולוגיות מידע למערכות פיננסיות ואחרות
- הפעלה וניהול חקירות בהיבטי פורנזיקה (ניתוח ראיות דיגיטלי)
- נהלים ומדיניות ארגונית
- סימולציות הנהלות ומודעות עובדים
- ועוד

MDR

Managed Detection & Response - MDR
הם שירותי ניטור, ניתוח, חקירה ותגובה לאירועי סייבר 24/7 הכוללים צוות SOC אשר מנטר ומגיב באופן מהיר לאירועי סייבר שמתרחשים אצל הלקוח.

MDR כולל מספר רמות שירות החל מ SIEM/SOC ועד MDR מלא הכולל ביצוע חקירות מודיעין ותגובה מלאה בסביבת הלקוח.

שירותי ה- MDR שלנו משלבים הגנה עבור נקודות קצה, בתוספת ניתוח תעבורת רשת חשודה, יכולות בינה מלאכותית וזאת באמצעות מומחיות של צוות SOC המאויש על ידי אנליסטים מהטובים בישראל.

השירותים כוללים:

SOC (חמ"ל סייבר)

- ניטור 24/7
- זיהוי וסיווג אירועים
- תגובה – חקירות ראשוניות וחקירות מתקדמות
- בידוד והכלה
- אספקת דוח המלצות חודשי
- ביצוע "ציד" איומים בצורה פרואקטיבית
- שילוב מידע מודיעיני במערכות

IR – Incident response (תגובה לאירועי משבר)

- ביצוע זיהוי היקף הפגיעה
- חקירות מודיעין מתקדמות
- ביצוע חקירות פורנזיקה (ניתוח ראיות דיגיטליות)
- ביצוע הערכת מצב ואספקת תמונת מצב להנהלה
- בידוד והכלת האירוע
- דוח מסקנות והמלצות

SIEM/SOC

SIEM -זוהי מערכת לאיסוף לוגים ויצירת חוקיות עליהם, למעשה זה ה"מוח" בחמ"ל הסייבר שהוא ה-SOC (Security Operation Center).

ה-SOC מספק שירותי ניטור, ניתוח וחקירה לאירועי סייבר 24/7 הכוללים צוות SOC אשר מנטר ומספק המלצות באופן מהיר לאירועי סייבר.

שירותי ה- SIEM/SOC שלנו משלבים יכולות ניטור גבוהות באמצעות הטכנולוגיות הטובות בעולם, שיטות עבודה מתקדמות וכל זאת עם מומחיות של צוות SOC המאויש על ידי אנליסטים מהטובים בישראל.

השירותים כוללים:

SOC (חמ"ל סייבר)

- ניטור 24/7
- טיוב ויצירת חוקה
- זיהוי וסיווג אירועים
- חקירות ראשוניות
- אספקת דוח המלצות חודשי
- ביצוע "ציד" איומים בצורה פרואקטיבית
- שילוב מידע מודיעיני במערכות

TTX - Cyber Simulation

Table Top Excessive - TTX
הינו שירות והתמחות של סימולציות סייבר ייחודיות להנהלות ארגונים, המכינות את הארגון לאירוע סייבר בקנה מידה גדול, לפגיעה מהותית בתהליכים העסקיים והתפעוליים בארגון ועוד.
הסימולציות מועברות הן להנהלות והן לצוותים המקצועיים בארגון.

סימולציה באורך של 3 עד 5 שעות אשר מהווה כלי יעיל להעלאת רמת הכישורים והמוכנות של הגורמים המשתתפים לאירוע סייבר מורכב. מטרת הסימולציה היא לדמות תרחיש/ים של אירוע סייבר בארגון, להבין מהם ההשלכות העלולות להיגרם במקרה של אירוע סייבר משמעותי בדגש על קבלת ההחלטות הנדרשות ברמת ההנהלה הבכירה.
הסימולציה ממחישה את האתגרים איתם נדרש להתמודד על בסיס אירועים בהם חברתנו טיפלה בשנים האחרונות ואירועים עדכניים בעולם בכלל, ובישראל בפרט.

סימולציה באורך של 3 עד 5 שעות אשר מהווה כלי יעיל להעלאת רמת הסימולציה מדגישה את דרכי התגובה שאירועים שניתן לצפות ולתכנן ואף לאלו שלא ניתן לצפות ובכל זאת נדרש להיות מוכנים אליהם ככל שניתן. בנוסף, הסימולציות מחדדות את חלוקת האחריות בין הגורמים השונים בארגון ומחוצה לו הנדרשים בעת אירוע ומציפה פערים ארגוניים על בסיס 3 אבני היסוד שנדרשים להתמודד עם עולם הסייבר- אנשים, טכנולוגיות ותהליכים בדגש על משמעויות עסקיות.

IR - Incident Response

Incident Response – IR
תגובה לאירועי סייבר

לרוב שמדברים על שירותי IR מדובר על תגובה לאירועים חמורים כמו הצפנה וכופר, דלף מידע ובכלל אירועים שגורמים לארגון נזק משמעותי.

שירות ה-IR מספק יכולות חקירה מאוד מתקדמות בהיבטי ראיות דיגיטליות, מודיעין, הבנה מעמיקה בקוד **ועוד.**
כמו כן- ליווי משפטי, תקשורתי, ניהול משא ומתן וכד'.

מומחי Ness Cyber Control בעלי ניסיון בטיפול באירועי IR לארגונים רבים בישראל ובעולם בעשור האחרון, החל מארגונים ביטחוניים, דרך ארגונים פיננסיים וביטוחיים ועד חברות סטארט-אפ ויוניקורנים מובילים.

השירותים כוללים:
- מיפוי מצב קיים
- שיפור מוכנות ארגונית
- ליווי הנהלות
- תמיכה רגולטורית
- חקירות פורנזיקה
- חקירות מודיעין
- ליווי משפטי
- ביטוח סייבר

Crisis Management

Crisis Management - ניהול משברים

ארגונים אשר נמצאים תחת מתקפת סייבר למעשה נמצאים במשבר משמעותי בגלל שלא רק הטכנולוגיה נפגעת אלא גם המוניטין, ולעיתים הפגיעה היא אקוטית ברמה פיננסית. כל אלו משפיעים על נדבכים רבים בארגון ועל המשכיות עסקית תקינה.

שירותי ה- MDR שלנו משלבים הגנה עבור נקודות קצה, בתוספת ניתוח תעבורת רשת חשודה, יכולות בינה מלאכותית וזאת באמצעות מומחיות של צוות SOC המאויש על ידי אנליסטים מהטובים בישראל.

השירותים כוללים:

- בניית תמונת מצב להנהלה/דירקטוריון
- הפעלת צוותי חקירות
- ניהול משא ומתן עם תוקפים
- ליווי תקשורת ודוברות
- ליווי משפטי
- ליווי עסקי ואסטרטגי

GRC

Governance, risk management and compliance - GRC
כולל ביצוע סקרים, פרויקטים ותהליכים המספקים מענה לנושא עמידה בתקינה נדרשת, רגולציות ותאימות לסטנדרטים נדרשים.

דוגמאות לתקנים וסטנדרטים מובילים:
ISO, NIST , CMMC, CCPA, GDPR, PCI ,DSS ועוד.

ל-Ness cyber control ניסיון רב בליווי, תמיכה ויישום תקנים וסטנדרטים בישראל ובעולם לטובת עמידה ברגולציות נדרשות.
החל מתקני ISO השונים, דרך תקני SOC ועד תקנים אמריקאים הנדרשים לחברות ביטחוניות שעובדות עם ארה"ב כמו CMMC ו NIST-171 או NIST 800-53 ותקנים רבים נוספים.

עיקרי השירותים:

- סקרי בגרות
- סקרי סיכונים
- סקרים לבחינת עמידה בחוזר סייבר של שוק ההון, ביטחון וחיסכון
- מבדקי חדירות בכל הרמות
- הכנה לסטנדרטים מובילים
- ביצוע Audit
- ועוד

Penetration Tests

Penetration Tests - PT
מבדקי חדירות
בדיקת חדירות היא מתקפה מתוכננת ומבוקרת על מערכת ממוחשבת שנעשית על ידי בודק ("האקר") במטרה למצוא חולשות אבטחה, פוטנציאל גישה לחולשות אלו, והבנת השימושיות שניתן להפיק מהגישה אליהן ואל המידע שהן מאחסנות.

Ness Cyber Control מבצעת שירותי PT (מבדקי חדירות) ללקוחותיה מכל המגזרים והסוגים וזאת באמצעות צוותים מומחים על פי עולמות התוכן השונים: IT, OT, IOT, MOBILE ועוד.

אנו מציעים מבדקי חדירות אפליקטיביים ותשתיתיים בתצורת BLACK/GREY/WHITE BOX וזאת בהיצמדות למתודולוגיות וסטנדרטים מובילים כמו NIST ו OWASP.

SOP's

Standard Operating Procedure - SOP'S
כתיבת נהלים ומסמכי מדיניות

מומחי הגנת הסייבר ואבטחת המידע שלנו, מתמחים בין היתר בכתיבת נהלים ומסמכי מדיניות -

- נהלי BCP / DRP (המשכיות עסקית)
- נהלי תגובה לאירועי סייבר
- מסמכי מדיניות ואסטרטגיה
- ועוד

BCP, DRP, מדיניות אבטחת מידע, נהלי טיפול באירוע כל אלו ועוד הם הבסיס שאיתו אנו עובדים ביום יום ומספקים ללקוחותנו במגוון מגזרים ותעשיות בהתאם צרכים ולדרישות שעולים מעת לעת.

המתודולוגיות על בסיסן האפיון והכתיבה מתבצעים הם על פי סטנדרטים מובילים כמו NIST, MITRE, SANS ועוד מצד אחד, ובהתאמה לדרישות הלקוח מצד שני.

מומלץ לבצע סקירה ועדכון למסמכים הנדרשים בתחום אבטחת המידע לטובת עמידה ברגולציות ותקנים נדרשים וכמובן בכדי לוודא מוכנות מרבית לעת משבר וזאת באמצעות הנגשתם המלאה.

הדרכות ו-OJT

מובילי Ness Cyber Control הם מהמדריכים והמנטורים המובילים והמוכרים בישראל בתחום הסייבר. ההדרכות מועברות באמצעות קורסים עיוניים או מעשיים, הרצאות ואימון בסביבות ייעודיות.

Ness Cyber Control הכשירה בשנים האחרונות מאות אנליסטים באמצעות הדרכות עיוניות ומעשיות, וממשיכה לבצע זאת בכל הקשור ליכולות ניטור, זיהוי, חקירה ותגובה לאירועי סייבר.

הדרכות אלו מועברות לצוותים הטכניים במטרה למקצע את יכולות החקירה או הזיהוי של אירועי סייבר בקרב צוותים אלו, זאת בכדי לשפר את היכולות הפנים ארגוניות בעולמות אבטחת המידע.

AWARENESS

Awareness -שירותי מודעות

שירות זה בא להעניק מענה למה שמוגדר על פי רוב כחוליה החלשה ביותר בארגון – העובד.
המטרה היא לעלות את מודעות העובדים לסיכוני אבטחת המידע בארגון וזאת באמצעות הדרכות, הרצאות, קמפיינים שונים להטמעת מודעות לעולם אבטחת המידע והגנת הפרטיות.

השירותים כוללים:

- הרצאות ממוקדות
- סמינרים וימי עיון
- לומדות דיגיטליות
- משחוק
- מיתוג פנים ארגוני בנושאי הסייבר
- הפקת תוכן ומסרים באמצעים שונים
- ביצוע קמפיינים בנושאי פישינג
- סימולציות סייבר ייעודיות
- ועוד

INSURANCE

Cyber Insurance – ביטוח סייבר

היום חברות רבות נדרשות לביטוח סייבר ממגוון סיבות- החל מרגולציה ועד הבנה אמיתית שיש צורך בכך כחלק ממוכנות ארגונית לאירועי סייבר וניהול סיכוני הארגון תוך שמירה על נכסיו ולקוחותיו.

ל- Ness Cyber Control שיתוף פעולה ייחודי עם חברת Howden אשר מובילה את עולם ביטוחי הסייבר בעולם, במטרה לספק נדבך נוסף כהגנה ביטוחית ומעטפת משלימה.

כמו בביטוח חיים גם כאן השימוש בביטוח נועד רק למקרה קצה.
רק שבשונה מביטוחי חיים למשל, עולם תקיפות הסייבר גדול משמעותית בשנים האחרונות והסיכוי שנזדקק לביטוח סייבר גדל בהתאמה.

שירותי הסייבר שלנו מצרפים אליהם גם יכולת לספק ליווי משפטי, ביצוע חקירות מתקדמות ועוד.

מוצרים וטכנולוגיות

Cyber Control מתמחה בבחירת המוצרים והטכנולוגיות המתקדמות והמתאימות ביותר לכלל עולמות התוכן הנדרשים היום לארגונים בהגנה מפני התקפות סייבר ואבטחת המידע של כלל הנכסים הארגוניים.

השילוב של פתרונות התוכנה הטובים ביותר, עם מומחיות יישומית כחלק מחבילות ידע ושירות עבור עשרות לקוחות בארץ ובעולם, מעמידה את Cyber Control כגוף המוביל בישראל לעולם ייצוג והפצת מוצרי סייבר ואבטחת מידע.

צוותי המומחה שלנו, אשר נמצאים "צעד אחד לפני כולם" עם הבנה והיכרות של כלל תרחישי עולם הסייבר, עומל כל העת על הרחבת היצע הטכנולוגיות והפתרונות המוצעים ללקוחותינו.

אנו מטפחים מערכות יחסים ארוכות טווח עם שותפים עסקיים אסטרטגיים על מנת להבטיח ללקוחותינו אספקת מוצרים וטכנולוגיות אופטימאליים, בעלי מוניטין ובחזית הטכנולוגיה.

BITSIGHT
SentinelOne
Radar
Microsoft
SIEMPLIFY THREATNEXUS
ARGON 18
Daon
cyber OBSERVER
RISKIQ
WhiteSource
KnowBe4 Human error. Conquered.
reflectiz Web Technologies Control