

כאן לשירותך

SYSEC היא שותפה לדרך של לקוחותיה ואמונה על אבטחת הארגון והבטחת עתידו עם ניסיון מצטבר של עשרות שנים באבטחת מידע וסייבר, **SYSEC** מיישמת, מתאימה ומטמיעה את פתרונות אבטחת המידע המתקדמים בתחום. תחת הסמכות בינלאומיות ושותפות עם היצרנים המובילים בעולם.

SYSEC מציעה ללקוחותיה סינרגיה מושלמת בכל היבטי אבטחת המידע לרבות הגנה על הנקודות קצה, דואר אלקטרוני, מסדי נתונים, סביבת הענן וכל פתרונות הסייבר בהתאמה ומיטוב פרטניים ומדויקים לכל ארגון ועל כל צרכיו ודרישותיו.

בנוסף לצוותי האינטגרציה וה- Professional Services מעניקה **SYSEC** ללקוחותיה שירותי SIEM-SOC ו-MDR מסביב לשעון 24/7. בין לקוחותיה של **SYSEC** משרדי ממשלה, בנקים, חברות ביטוח, תעשייה עתירת ידע, תעשייה בטחונית, אנרגיה ותשתיות.

AREAS OF EXPERTISE



CLOUD & APP
SECURITY



DATA
SECURITY



CYBER
SECURITY



SASE/SSE



SIEM-SOC
& MDR

שותפים מובילים



מערך ה- **TMSSP** מספק שירותי הגנת סייבר מנוהלים עבור ארגונים למימוש מערך ניטור, שליטה ובקרה **SOC** עבור אירועי סייבר בשילוב יכולות יישום למערכות הגנת הסייבר של הארגון.



שירות זה מספק לארגונים ניטור מרכזי לכלל אירועי הסייבר המזהים בארגון וזמינות לטיפול אקטיבי באמצעות מערכות ההגנה באופן יעיל ורציף.

שירותים מנוהלים **TMSSP MDR**

מרכז אבטחה **SOC**

מערך **SOC** המנטר את האירועים המתקבלים מהמערכות הכלולות בשירות ומספק ללקוח זיהוי, תגובה, התראה, דוחות וממצאים.

הכרות עם הארגון

לקוחות שירות ה- **TMSSP** מיועד ללקוחות פעילים ומטופלים על ידי חברת SYSEC מתוך הבנה שלא ניתן לממש פתרון מנוהל ללא הכרות אמיתית עם רשת הלקוח.

טכנולוגיות מובילות

מערך ה- **TMSSP** ממומש על ידי הטכנולוגיות המובילות בתעשייה בשיתוף פעולה עם חברות כדוגמת Palo Alto, Trellix, Symantec ועוד.

PSAAS שרות מומחה מנוהל

מערך ה- **TMSSP** מנוהל על ידי אנשים בעלי ניסיון עשיר ועתירי הצלחות במימוש פרויקטים בתחום הגנת הסייבר בהבנה מלאה של האתגרים בכל טכנולוגיה תוך התאמת הפתרון ללקוח ואשר מספקים שירותי PS ללקוחות בצורה מנוהלת.

פתרון כולל

מספקים את כלל השירותים הנדרשים עבור פתרון מוצלח - הנחיה, אופרציה וניטור התוצרים במטרה להקל על צוותי הארגון ולהורדת תקורות.

רציפות

הניסיון מראה כי עדיפה רציפות של מספר שעות ביום על פני יום עבודה אחת לשבוע. רציפות מאפשרת ניהול הפתרונות בצורה יעילה ולהשגת התוצרים הרצויים.

טיפול בהתראות

פרט לשליחת דו"חות, מתבצע מעבר על ההתראות אשר זהו עבור דיוק ושיפור השירות.

דיוק גבוה יותר - בחינה מעמיקה של ההתראות על ידי מומחים מבטיחה דיוק גבוה יותר בזיהוי איומים ומפחיתה התראות שווא.

שיפור מתמיד - תהליך מתמיד של ניתוח ושיפור אלגוריתמי הזיהוי, משפר את יעילות המערכת לאורך זמן.

הבנה מעמיקה יותר של האיומים - ניתוח ההתראות על ידי מומחים מספק הבנה מעמיקה יותר של האיומים ושל השפעתם על הארגון.

בעלות מלאה על הנתונים בסיום השירות

בעלות על המידע - הלקוח שומר על בעלות מלאה על כל הנתונים, ההגדרות והחוקים שפותחו עבורו במהלך השירות.

מעבר חלק - מעבר קל ופשוט למערכת אחרת או להפעלה עצמאית של המערכת, ללא אובדן מידע או הגדרות.

שקט נפשי - ביטחון שההשקעה במערכת לא תרד לטמיון בסיום ההתקשרות.

אסקלציה פנימית לצוות PS בחקירת אירוע

מומחיות מעמיקה - גישה למומחים בעלי ידע מעמיק במערכת ה-SIEM ובטכנולוגיות אבטחה נוספות.

תמיכה וייעוץ - תמיכה וייעוץ מקצועי בכל שלבי התהליך, החל מזיהוי האירוע ועד לתגובה וחקירה.

העברת ידע - העברת ידע וניסיון לצוות הלקוח, שיפור היכולות הפנימיות של הארגון.

פגישה דו שבועית לפיתוח המערכת

שירות מותאם אישית - התאמה מלאה של המערכת והשירות לצרכים הספציפיים של הלקוח.

שיתוף פעולה ושקיפות - שיתוף פעולה הדוק עם הלקוח ותהליך שקוף של פיתוח ושיפור המערכת.

מענה מהיר לצרכים משתנים - יכולת להגיב במהירות לשינויים בצרכים של הלקוח ולסביבת העבודה שלו.

הוספת מקורות מידע ללא הגבלה וללא תוספת מחיר

כתיבת חוקי קורלציה ללא הגבלה וללא תוספת מחיר

מערכת SIEM ייעודית לכל לקוח

ביצועים משופרים - מערכת ייעודית מבטיחה משאבים מלאים ללקוח, ללא תחרות על משאבים עם לקוחות אחרים. זה מתבטא בזמני תגובה מהירים יותר, ניתוח נתונים יעיל יותר ושיפור ביצועי המערכת.

גמישות והתאמה אישית - מערכת נפרדת מאפשרת התאמה מדויקת לדרישות הספציפיות של כל לקוח, כולל הגדרות, חוקים, דוחות ואינטגרציות.

אבטחת מידע משופרת - הפרדה מלאה בין נתוני הלקוחות מבטיחה פרטיות ואבטחה מקסימלית. מניעת חשיפה של מידע רגיש ללקוחות אחרים.

שליטה מלאה - הלקוח מקבל שליטה מלאה על המערכת שלו, כולל עדכונים, שדרוגים ותחזוקה.

מערכת SIEM בתצורת SAAS

פריסה מהירה - הטמעה מהירה וקלה של המערכת, ללא צורך בהתקנה ותחזוקה של תשתית מקומית.

נגישות מכל מקום - גישה למערכת מכל מקום ובכל זמן, באמצעות חיבור אינטרנט.

עדכונים אוטומטיים - עדכונים ושדרוגים מבוצעים באופן אוטומטי על ידי הספק, ללא הפרעה לפעילות הלקוח.

גמישות ו-scalability - ניתן להגדיל או להקטין את המשאבים לפי הצורך של הלקוח.

שירות MDR מלא + יכולת חקירה

הגנה מקיפה - שירות MDR מספק הגנה מקיפה מפני איומים מתקדמים, כולל זיהוי, חקירה ותגובה לאירועים.

מומחיות וניסיון - גישה לצוות מומחים עם ניסיון רב בתחום אבטחת המידע.

צמצום סיכונים - הפחתה משמעותית של הסיכונים הכרוכים במתקפות סייבר.

אינטגרציה עם EDR - אינטגרציה עם מערכות EDR משפרת את יכולות הזיהוי והתגובה לאיומים בנקודות הקצה.

מערכת אוטומציה עם התאמה של תרחישים

תגובה מהירה יותר לאירועים - אוטומציה של תהליכים מאפשרת זיהוי ותגובה מהירים יותר לאיומים, צמצום זמן התגובה (MTTR) ומזעור נזקים.

יעילות תפעולית - אוטומציה חוסכת זמן ומשאבים יקרים לצוות ה-SOC, ומאפשרת להם להתמקד במשימות מורכבות יותר.

עקביות ודיוק - אוטומציה מבטיחה ביצוע עקבי ומדויק של תהליכים, ללא טעויות אנוש.

התאמה אישית - אפשרות להתאים תרחישי אוטומציה ספציפיים לצרכי הלקוח ולסביבת העבודה שלו.

ELITE SOC	ADVANCED DEFENCE	BASIC SHIELD	
✓	✓	✓	מערכת SIEM ייעודית לכל לקוח
✓	✓	✓	מערכת SIEM בתצורת SAAS
✓	✓	✓	ניטור 24/7 365 ימים בשנה
אנליסטים + PS	אנליסטים + PS	אנליסטים	תמיכה
✓	✓	בתוספת תשלום	אוטומציה מותאמת אישית
✓	✓	בתוספת תשלום	הוספת מקורות מידע
✓	✓	בתוספת תשלום	כתיבת חוקי קורלציה
✓	✓	✗	בעלות מלאה על הנתונים בתום השירות
✓	✓	✗	פגישות דו שבועיות לפיתוח המערכת
✓	✗	✗	מודיעין סייבר ב-DARK NET
✓	✗	✗	הגנת CNAPP על שירותי ענן
✓	✗	✗	שירות IR בעת אירוע סייבר