شاخص‌های کارشناس امنیت سایبری

برخی از شاخص‌های عملکردی و کاربردی برای تیم شما

KPI چیست؟

- شاخص‌های کلیدی عملکردی یا همان Key Performance Indicators، در واقع متریک‌ها و معیارهای اندازه‌گیری هستند، که به ما در تعیین درستی انجام کارها و فعالیت‌هایمان کمک می‌کنند.

- ما با استفاده از KPIها، قرار است تا بدانیم در چه وضعیتی هستیم و با اندازه‌گیری این پارامترها، می‌توانیم بگوییم که در راه رسیدن به اهدافمان چگونه عمل می‌کنیم.

شاخص‌های اصلی

۱ زمان پاسخگویی به حوادث امنیتی
Security Incident Response Time

۲ میانگین زمان تعمیر
Mean Time to Repair (MTTR)

۳ نرخ نقض امنیت
Security Breach Rate

۴ نرخ مثبت کاذب
False Positive Rate

۵ انطباق حسابرسی امنیتی
Security Audit Compliance

۶ بهبود آگاهی امنیت کارکنان
Employee Security Awareness Improvement

۷ نرخ اصلاح آسیب‌پذیری سیستم
System Vulnerability Remediation Rate

۸ نرخ تشخیص تهدید
Threat Detection Rate

شاخص‌های اصلی

۹ تجزیه و تحلیل هزینه-منافع امنیتی
Security Cost-Benefit Analysis

۱۰ همکاری با تیم‌های فناوری اطلاعات
Collaboration with IT Teams

۱. زمان پاسخگویی به حوادث امنیتی

Security Incident Response Time

کارایی و اثربخشی متخصص امنیت سایبری را در پاسخگویی و حل و فصل حوادث امنیتی می سنجد. زمان پاسخ کمتر نشان‌دهنده قابلیت های بهتر رسیدگی به حادثه است، در صورتیکه میزان تکرار حوادث نیز در نظر گرفته شود.

زمان پاسخگویی به حوادث امنیتی = (مجموع زمان پاسخ به حادثه / تعداد حوادث)

SMART

۲. میانگین زمان تعمیر

Mean Time to Repair (MTTR)

میانگین زمان صرف شده برای بازگرداندن سیستم ها به حالت عادی پس از یک حادثه امنیتی را اندازه گیری می کند. MTTR کمتر نشان دهنده بازیابی سریعتر و کاهش زمان خرابی است.

میانگین زمان تعمیر = (کل زمان توقف / تعداد حوادث)

SMART

۳. نرخ نقض امنیت

Security Breach Rate

دفعات نقض امنیتی را در یک بازه زمانی خاص اندازه گیری می‌کند. نرخ پایین تر نشان دهنده اقدامات امنیتی موثر و شناسایی پیشگیرانه تهدید است.

نرخ نقض امنیت = (تعداد نقض امنیت / کل دوره زمانی)

SMART

۴. نرخ مثبت کاذب

False Positive Rate

دقت ابزارهای امنیتی و توانایی متخصص امنیت سایبری در تمایز بین تهدیدهای واقعی و هشدارهای نادرست را اندازه‌گیری می کند. نرخ پایین تر نشان دهنده بهبود کارایی تشخیص تهدید است.

نرخ مثبت کاذب = (تعداد مثبت کاذب / تعداد کل هشدارها) × ۱۰۰٪

SMART

۵. انطباق حسابرسی امنیتی

Security Audit Compliance

میزان اطمینان متخصص امنیت سایبری از رعایت استانداردها و مقررات امنیتی را اندازه گیری می کند. نرخ انطباق بالا نشان دهنده مدیریت موثر ریسک و رعایت مقررات است.

انطباق حسابرسی امنیتی = (تعداد استانداردهای امنیتی رعایت شده / تعداد کل استانداردهای امنیتی) × ۱۰۰٪

SMART

۶. بهبود آگاهی امنیت کارکنان

Employee Security Awareness Improvement

اثربخشی تلاش‌های متخصص امنیت سایبری در بهبود آگاهی امنیتی کارکنان را اندازه‌گیری می‌کند. می توان آن را از طریق ارزیابی های قبل و بعد از تمرین و کاهش حادثه ارزیابی کرد.

بهبود آگاهی امنیت کارکنان = (بهبود امتیازهای آگاهی امنیتی) یا (کاهش حوادث امنیتی به دلیل خطای انسانی)

SMART

۷. نرخ اصلاح آسیب‌پذیری سیستم

System Vulnerability Remediation Rate

سرعت رفع آسیب‌پذیری‌های شناسایی‌شده را اندازه‌گیری می‌کند. نرخ بالا نشان دهنده کاهش پیشگیرانه ریسک است.

نرخ اصلاح آسیب‌پذیری سیستم = (تعداد آسیب‌پذیری ثابت / تعداد کل آسیب‌پذیری‌های شناسایی شده) × ۱۰۰٪

SMART

۸. نرخ تشخیص تهدید

Threat Detection Rate

توانایی متخصص امنیت سایبری را برای شناسایی تهدیدهای بالقوه قبل از ایجاد آسیب می سنجد. نرخ بالا نشان دهنده نظارت و تحلیل موثر تهدید است.

نرخ تشخیص تهدید = (تعداد تهدیدات شناسایی شده / تعداد کل تهدیدات بالقوه) × ۱۰۰٪

SMART

۹. تجزیه و تحلیل هزینه- منافع امنیتی

Security Cost-Benefit Analysis

بازده سرمایه گذاری برای طرح های امنیتی را اندازه گیری می‌کند. هزینه اقدامات امنیتی را در مقابل ارزش تلفات جلوگیری شده ارزیابی می کند.

تجزیه و تحلیل هزینه-منافع امنیتی = (به دلیل اقدامات امنیتی از هزینه جلوگیری می‌شود / هزینه اقدامات امنیتی)

SMART

۱۰. همکاری با تیم‌های فناوری اطلاعات

Collaboration with IT Teams

اثربخشی همکاری با سایر تیم های فناوری اطلاعات را برای اطمینان از امنیت کلی سیستم اندازه گیری می کند. این نشان‌دهنده توانایی کار متقابل است.

ارزیابی بر اساس بررسی افراد هم‌رده، موفقیت پروژه و بازخورد ذی نفعان.

SMART

تهیه شده در ریرا

ممنون از توجه شما