15th International Conference on
Information Technology, Computer & Telecommunication

(پیاده سازی مرکز عملیات امنیت (SOC

در سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز)

زهرا طاهری راد
کارشناس ارشد امار ریاضی سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز

پرهام ویسی
کارشناس SOC سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز

چکیده

راه اندازی مرکز SOC با مدل‌سازی تهدید آغاز می‌شود. طی این فرآیند، مدیران شبکه و امنیت IT گرد هم می‌آیند تا تهدیدات سایبری کلیدی را تشخیص دهند و آن‌ها را اولویت‌بندی کنند. سپس شکل فرضی آن‌ها در داده‌های ماشینی را به صورت مدل درآورند و در نهایت تعیین می کنند که چطور می‌توان آن‌ها را شناسایی و اصلاح کرد.

یکی از بخش‌های مهم و اساسی در راه اندازی SOC فرآیند واکنش به هشدارها و حوادث است و بیشترSOC ها از یک رویکرد Multitier یا چندلایه استفاده می‌کنند. هشدارها از راه‌های مختلفی چون SIEM ها و راهکارهای مشابه SIEM ایجاد می‌شوند و جهت بررسی اولیه به اولین Tier فرآیندهای آنالیز می‌روند. اگر Tier اول نتواند حادثه را رفع کند، تا Tierبعدی توسعه می‌یابد، که این Tier دارای پرسنلی با دانش بیشتر و ابزار واکنش به حادثه‌ی پیشرفته‌تری است.

پس از راه اندازی مرکز عملیات امنیت شهرداری، تاثیراتی که این مرکز بر بهبود فرآیندها و ارتقای سطح امنیت سازمان خواهد داشت بررسی می شود.

واژگان کلیدی: امنیت، فناوری اطلاعات، مرکز عملیات امنیت، SOC، فرآیند، طراحی، لاگ، تهدیدات امنیتی، رخدادهای امنیتی، پایش، فازبندی اجرای طرح، نیروی انسانی