

عنوان مقاله:

تاثیر پیاده سازی مرکز عملیات امنیت در سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز

محل انتشار:

کنفرانس دانشجویان مهندسی کامپیوتر، فناوری اطلاعات و ارتباطات (سال: 1401)

تعداد صفحات اصل مقاله: 9

نویسندگان:

پرهام ویسی - کارشناس ارشد فناوری اطلاعات سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز

زهرا طاهری راد - کارشناس ارشد امر ریاض سازمان فناوری اطلاعات و ارتباطات شهرداری شیراز

خلاصه مقاله:

راه اندازی مرکز SOC با مدلسازی تهدید آغاز می شود. طی این فرآیند، مدیران شبکه و امنیت IT گرد هم می آیند تا تهدیدات سایبری کلیدی را تشخیص دهند و آنها را اولویت بندی کنند. سپس شکل فرضی آنها در داده های ماشینی را به صورت مدل درآوردند و در نهایت تعیین می کنند که چطور میتوان آنها را شناسایی و اصلاح کرد. یکی از بخش های مهم و اساسی در راه اندازی SOC فرآیند واکنش به هشدارها و حوادث است و بیشتر SOC ها از یک رویکرد Multitier یا چندلایه استفاده می کنند. هشدارها از راه های مختلفی چون SIEM ها و راهکارهای مشابه SIEM ایجاد می شوند و جهت بررسی اولیه به اولین Tier فرآیندهای آنالیز می روند. اگر Tier اول نتواند حادثه را رفع کند، تا Tier بعدی توسعه می یابد، که این Tier دارای پرسنلی با دانش بیشتر و ابزار واکنش به حادثه ی پیشرفته تری 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.

کلمات کلیدی:

امنیت، فناوری اطلاعات، مرکز عملیات امنیت، SOC، فرآیند، طراحی، لاگ، تهدیدات امنیتی، رخدادهای امنیتی، پیش، فازبندی اجرای طرح، نیروی انسانی

لینک ثابت مقاله در پایگاه سیویلیکا:

<https://civilica.com/doc/1567089>

