عنوان مقاله:
بررسی مقایسه ای مراکز عملیات امنیت در حوزه فناوری اطلاعات و مدل های کاربردی آن

محل انتشار:
همایش ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک ایران (سال: 1395)

تعداد صفحات اصل مقاله: 12

نویسندگان:
محمد یوسفی لهمالی - *دانشجوی کارشناسی ارشد موسسه آموزش عالی روزبهان و کارمند شرکت برق منطقه ای مازندران و گلستان*

بردیا بهنیا - *عضو هیات علمی موسسه آموزش عالی روزبهان و کارمند شرکت برق منطقه ای مازندران و گلستان*

خلاصه مقاله:
ترکیب فناوری های مختلف با هدف برآورده نمودن نیازمندی های کسب و کار، سازمان ها را با چالش هایی جدید روبرو نموده است، چرا که عموما هیچ روش یا مکانیزمی با هدف جمع آوری، نرمال سازی، همبسته سازی و اولویت بندی میلیون ها رخداد گزارش شده از سوی سامانه های مختلف فناوری اطلاعات و ارتباطات وجود ندارد. استفاده از فناوری های مختلف و نامتجانس منجر به افزایش سربار فعالیت های امنیتی سازمان، ایجاد مدل های امنیتی ضعیف و عدم موفقیت فرآیندهای ممیزی می گردد. در چنین وضعیتی، همبسته سازی بلادرنگ وقایع مختلف که توسط تجهیزات و ابزارهای مختلفی تولید شده است و شناسایی یک حمله یا نفوذ مشخص، بسیار مشکل و عموما غیرممکن می باشد. علاوه براین، تحلیل های پس از وقوع حوادث نیز بسیار کند انجام خواهند شد، چرا که ترکیب اطلاعاتی که به روش های متفاوت در ابزارها و تجهیزات مختلف نگهداری می شوند، کاری بسیار زمان بر و پرهزینه است و سوالات زیر در این خصوص مطرح می گردد:...

کلمات کلیدی: