عنوان مقاله:
رویکردی دفاعی برای مقابله با شناسایی تجهیزات فعال شبکه های کامپیوتری

محل انتشار:
پنجمین کنفرانس ملی پژوهش های کاربردی در علوم برق ،کامپیوتر و مهندسی پزشکی (سال: 1399)

تعداد صفحات اصل مقاله: 14

نویسندگان:
ایمان رجبی زاده - *دانشجوی کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی واحد تهران شمال*

ناصر مدیری - *استادیار دکتری تخصصی کامپیوتر دانشگاه آزاد اسلامی واحد زنجان*

خلاصه مقاله:
به واسطه رشد علم و تکنولوژی به تبع آن فناوری اطلاعات و ارتباطات وایجاد فضای سایبری و نفوذ هرچه بیشتر آن در جوامع و ملت ها، مسائلمربوط به این حوزه از اهمیت بالایی برخوردار گردیده است به گونه ای که امروزه مقابله به تهدیدات سایبری یکی از جدی ترین چالش های امنیت ملی واقتصادی برای دولت ها و سازمان ها محسوب می شود تهدیدات سایبری با اثرگذاری بر روی زیر ساخت های حیاتی هزینه های زیاد و گاه غیر قابل جبرانی را به سازمانی ها، جوامع و کشورها تحمیل می کند اقدام اصلی در مواجهه با این موارد شناسایی تهدیدات فوق است تشخیص و پیشگیری از حملات در زنجیره کشت سایبری امری بیار ضروری می باشد و سازمان ها به منظور جلوگیری ازتهدیدات باید دارای فناوری تشخیص نفوذ باشند تا در صورت نقض قوانین از تهدیدات حاصل از ان مطلع گردند. با توجه به این مهم که عموم راهکارهای تشخیص حملات و تهدیدات مبتی بر شناسایی رفتار و یا نشانه ها و امضای تهدیدات هستند که عموما شناخته شده هستند، لذا بسیاری از تهیدیدات از دید سامانه های تشخیص و شناسایی تهدیدات به دور می باشند راهکار شکار تهدیدات سازمان ها را برای شناسایی این موارد یاری می نماید. تمرکز این مقاله تا حد زیادی بر روی زنجیره کشت سایبری و چگونگی اجرای کنترل و فن آوری های پیشگیرانه برای محافظت از سازمان ها می باشد بنابراین محورهای روش پیشنهادی در این مقاله روی سه موضوع جمع آوری اطلاعات و رویدادها، تجزیه و تحلیل اطلاعات بدست آمده در نهایت کنترل داده ها متمرکز شده است.

کلمات کلیدی:
زنجیره کشت سایبری، تهدیدات سایبری، کنترل های امنیتی SIEM،