عنوان مقاله:
ارائه چارچوب مبتنی بر هستان شناسی برای ادغام داده های سخت و نرم در تحلیل امنیت سایبری

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 7, شماره 4 (سال: 1398)

تعداد صفحات اصل مقاله: 11

نویسندگان:
علی جبار رشیدی - *صنعتی مالک اشتر*

سعداله سبحانی - *دانشگاه مالک اشتر*

سیدمجتبی حسینی

خلاصه مقاله:
در تحلیل امنیت سایبری، علاوه بر داده ها و اطلاعاتی که از حسگرهای ماشینی مانند سامانه های تشخیص نفوذ، دیواره های آتش و پویشگرهای آسیب پذیری به دست می آید (داده های سخت)، مشاهدات و برداشت های انسانی شامل گزارش های کاربران و مدیران شبکه از کارکرد عادی یا غیرعادی اجزای شبکه و تشخیص های صورت گرفته توسط تحلیلگرهای امنیتی از وضعیت امنیتی شبکه (داده های نرم) می تواند نقش مهمی در رسیدن به تخمین و تصمیم دقیق تر و مطمئن تر داشته باشد. ادغام داده های سخت و نرم در تحلیل امنیت سایبری دارای چالش هایی از قبیل طراحی چارچوب مدل سازی مسئله و نمایش انواع مختلف عدم قطعیت است. در این مقاله مدل جدیدی مبتنی بر هستان شناسی جهت ادغام داده های سخت و نرم به منظور به کارگیری در تحلیل امنیت سایبری ارائه می شود. در ابتدا مفاهیم و متغیرهای مسئله مدل می شوند و سپس با استفاده از مجموعه قواعد، استنتاج وضعیت امنیتی دارایی ها صورت می گیرد. همچنین مدل باور انتقال پذیر و قاعده ترکیب دمپستر-شفر برای مدل سازی یکپارچه عدم قطعیت و ادغام داده ها به کار گرفته شده است. نتایج به کارگیری مدل پیشنهادی در یک سناریوی نمونه از تحلیل امنیت سایبری، عملیاتی بودن آن را در ادغام داده های سخت و نرم سایبری نشان می دهد. انعطاف پذیری بالا و پویایی مدل با توجه به قابلیت توسعه هستان شناسی و پایگاه دانش، از ویژگی های مدل پیشنهادی است.

کلمات کلیدی:
ادغام داده های سخت و نرم, مدل سازی عدم قطعیت, تحلیل امنیت سایبری, هستان شناسی