عنوان مقاله:

Cyber Threats Intelligence Modeling

محل انتشار:

نوزدهمین کنفرانس بین المللی فناوری اطلاعات، کامپیوتر و مخابرات (سال: 1402)

تعداد صفحات اصل مقاله: 11

نویسنده:

Omid Davarzani - *Department of Computer Engineering, Hakim Sabzevari University ,Sabzevar,Iran*

خلاصه مقاله:

This article discusses the importance of the cyber threat intelligence model to address the growing threat of cyberattacks. Cybersecurity professionals are constantly protecting computer systems against different types of cyber threats. Cyberattacks hit businesses and private systems every day and the number of attacks has increased rapidly. According to former Cisco CEO John Chambers, "There are two types of companies:people who have been hacked and those who do not know they have been hacked. Overall, the cyber threat intelligence model is an essential part of any comprehensive cybersecurity strategy, and by leveraging advanced technology and trained staff, organizations can develop and deploy performance models that provide valuable insights into the threat landscape and enable them to take proactive steps to protect their assets.Cyber Threat Intelligence (CTI) is actionable data collected and used by an organization's cybersecurity systems and/or security professionals to help them better understand vulnerabilities. , .take appropriate action to prevent an attack, and protect corporate networks and endpoints from future attacks

کلمات کلیدی:

CTI, IoT, DCMS, IOC

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1712759