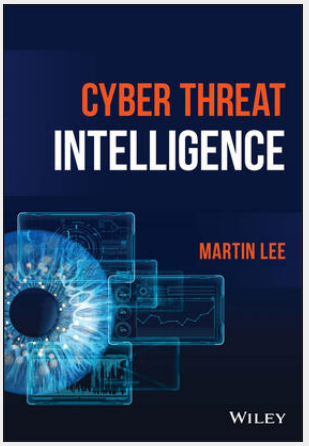
Lee

Cyber Threat Intelligence



105,50 €
98,60 € (zzgl. MwSt.)

sofort versandfertig, Lieferfrist: 1-3 Werktage

Artikelnummer: 9781119861744
Medium: Buch
ISBN: 978-1-119-86174-4
Verlag: Wiley John + Sons
Erscheinungstermin: 17.04.2023
Sprache(n): Englisch
Auflage: 1. Auflage 2023
Produktform: Gebunden
Gewicht: 598 g
Seiten: 304
Format (B x H): 157 x 235 mm

CYBER THREAT INTELLIGENCE "Martin takes a thorough and focused approach to the processes that rule threat intelligence, but he doesn't just cover gathering, processing and distributing intelligence. He explains why you should care who is trying to hack you, and what you can do about it when you know." --Simon Edwards, Security Testing Expert, CEO SE Labs Ltd., Chair AMTSO Effective introduction to cyber threat intelligence, supplemented with detailed case studies and after action reports of intelligence on real attacks Cyber Threat Intelligence introduces the history, terminology, and techniques to be applied within cyber security, offering an overview of the current state of cyberattacks and stimulating readers to consider their own issues from a threat intelligence point of view. The author takes a systematic, system-agnostic, and holistic view to generating, collecting, and applying threat intelligence. The text covers the threat environment, malicious attacks, collecting, generating, and applying intelligence and attribution, as well as legal and ethical considerations. It ensures readers know what to look out for when considering a potential cyber attack and imparts how to prevent attacks early on, explaining how threat actors can exploit a system's vulnerabilities. It also includes analysis of large scale attacks such as WannaCry, NotPetya, Solar Winds, VPNFilter, and the Target breach, looking at the real intelligence that was available before and after the attack. Topics covered in Cyber Threat Intelligence include: * The constant change of the threat environment as capabilities, intent, opportunities, and defenses change and evolve * Different business models of threat actors, and how these dictate the choice of victims and the nature of their attacks * Planning and executing a threat intelligence programme to improve an organistation's cyber security posture * Techniques for attributing attacks and holding perpetrators to account for their actions Cyber Threat Intelligence describes the intelligence techniques and models used in cyber threat intelligence. It provides a survey of ideas, views and concepts, rather than offering a hands-on practical guide. It is intended for anyone who wishes to learn more about the domain, particularly if they wish to develop a career in intelligence, and as a reference for those already working in the area.

"Martin takes a thorough and focused approach to the processes that rule threat intelligence, but he doesn't just cover gathering, processing and distributing intelligence. He explains why you should care who is trying to hack you, and what you can do about it when you know." --Simon Edwards, Security Testing Expert, CEO SE Labs Ltd., Chair AMTSO Effective introduction to cyber threat intelligence, supplemented with detailed case studies and after action reports of intelligence on real attacks Cyber Threat Intelligence introduces the history, terminology, and techniques to be applied within cyber security, offering an overview of the current state of cyberattacks and stimulating readers to consider their own issues from a threat intelligence point of view. The author takes a systematic, system-agnostic, and holistic view to generating, collecting, and applying threat intelligence. The text covers the threat environment, malicious attacks, collecting, generating, and applying intelligence and attribution, as well as legal and ethical considerations. It ensures readers know what to look out for when considering a potential cyber attack and imparts how to prevent attacks early on, explaining how threat actors can exploit a system's vulnerabilities. It also includes analysis of large scale attacks such as WannaCry, NotPetya, Solar Winds, VPNFilter, and the Target breach, looking at the real intelligence that was available before and after the attack. Topics covered in Cyber Threat Intelligence include: * The constant change of the threat environment as capabilities, intent, opportunities, and defenses change and evolve * Different business models of threat actors, and how these dictate the choice of victims and the nature of their attacks * Planning and executing a threat intelligence programme to improve an organistation's cyber security posture * Techniques for attributing attacks and holding perpetrators to account for their actions Cyber Threat Intelligence describes the intelligence techniques and models used in cyber threat intelligence. It provides a survey of ideas, views and concepts, rather than offering a hands-on practical guide. It is