

Understand the Cyber Attacker Mindset

Build a Strategic Security Programme to Counteract Threats

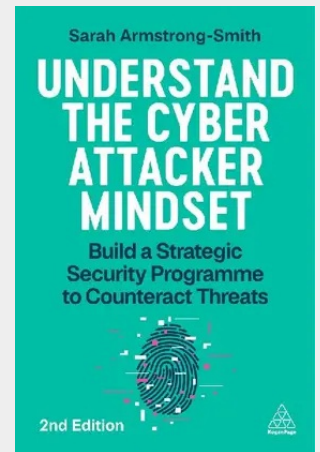
Strengthen your cybersecurity strategy by thinking like an attacker and anticipating threats before they strike. *Understand the Cyber Attacker Mindset* by Sarah Armstrong-Smith is a strategic guide for leaders who need to defend organizations against increasingly sophisticated cyber threats. By exploring the psychology, motivations and behaviours of modern attackers, this book equips leaders to make informed and proactive security decisions. This fully updated second edition reflects the latest threat landscape, with a new chapter covering how AI is accelerating attack capabilities, and details evolving risks such as cybercrime-as-a-service, insider threats and nation-state activity. Supported by real-world examples including Scattered Spider, Lapsus\$ and Sandworm, it delivers actionable insight for strengthening organizational resilience. You will learn how to: - Anticipate attacker behaviour and identify emerging threat patterns - Strengthen cybersecurity strategy using human-centric security approaches - Address insider threats and human risk at leadership level - Navigate AI-driven attacks and evolving cybercrime models - Build security cultures aligned with governance and risk priorities With expert insight and strategic frameworks, this book provides the tools CISOs, senior security leaders, risk executives and anyone who wants to defend their business can use to enhance decision-making, reduce exposure and protect enterprise value. **Themes include:** cybersecurity strategy, attacker mindset, cyber threat intelligence, AI in cybersecurity, insider threat management, cyber risk governance

Strengthen your cybersecurity strategy by thinking like an attacker and anticipating threats before they strike.

Understand the Cyber Attacker Mindset by Sarah Armstrong-Smith is a strategic guide for leaders who need to defend organizations against increasingly sophisticated cyber threats. By exploring the psychology, motivations and behaviours of modern attackers, this book equips leaders to make informed and proactive security decisions. This fully updated second edition reflects the latest threat landscape, with a new chapter covering how AI is accelerating attack capabilities, and details evolving risks such as cybercrime-as-a-service, insider threats and nation-state activity. Supported by real-world examples including Scattered Spider, Lapsus\$ and Sandworm, it delivers actionable insight for strengthening organizational resilience. You will learn how to:

- Anticipate attacker behaviour and identify emerging threat patterns
- Strengthen cybersecurity strategy using human-centric security approaches
- Address insider threats and human risk at leadership level
- Navigate AI-driven attacks and evolving cybercrime models

>With expert insight and strategic frameworks, this book provides the tools CISOs, senior security leaders, risk executives and anyone who wants to defend their business can use to enhance decision-making, reduce exposure and protect enterprise value. Themes include: cybersecurity strategy, attacker mindset, cyber threat intelligence, AI in cybersecurity, insider threat management, cyber risk governance



42,00 €

42,00 € (zzgl. MwSt.)

vorbestellbar, Erscheinungstermin ca. März 2027

Artikelnummer: 9781398630178

Medium: Buch

ISBN: 978-1-3986-3017-8

Verlag: Kogan Page Ltd

Erscheinungstermin: 03.03.2027

Sprache(n): Englisch

Auflage: 2. Revised Auflage 2027

Produktform: Kartoniert

Seiten: 296

Format (B x H): 156 x 234 mm

