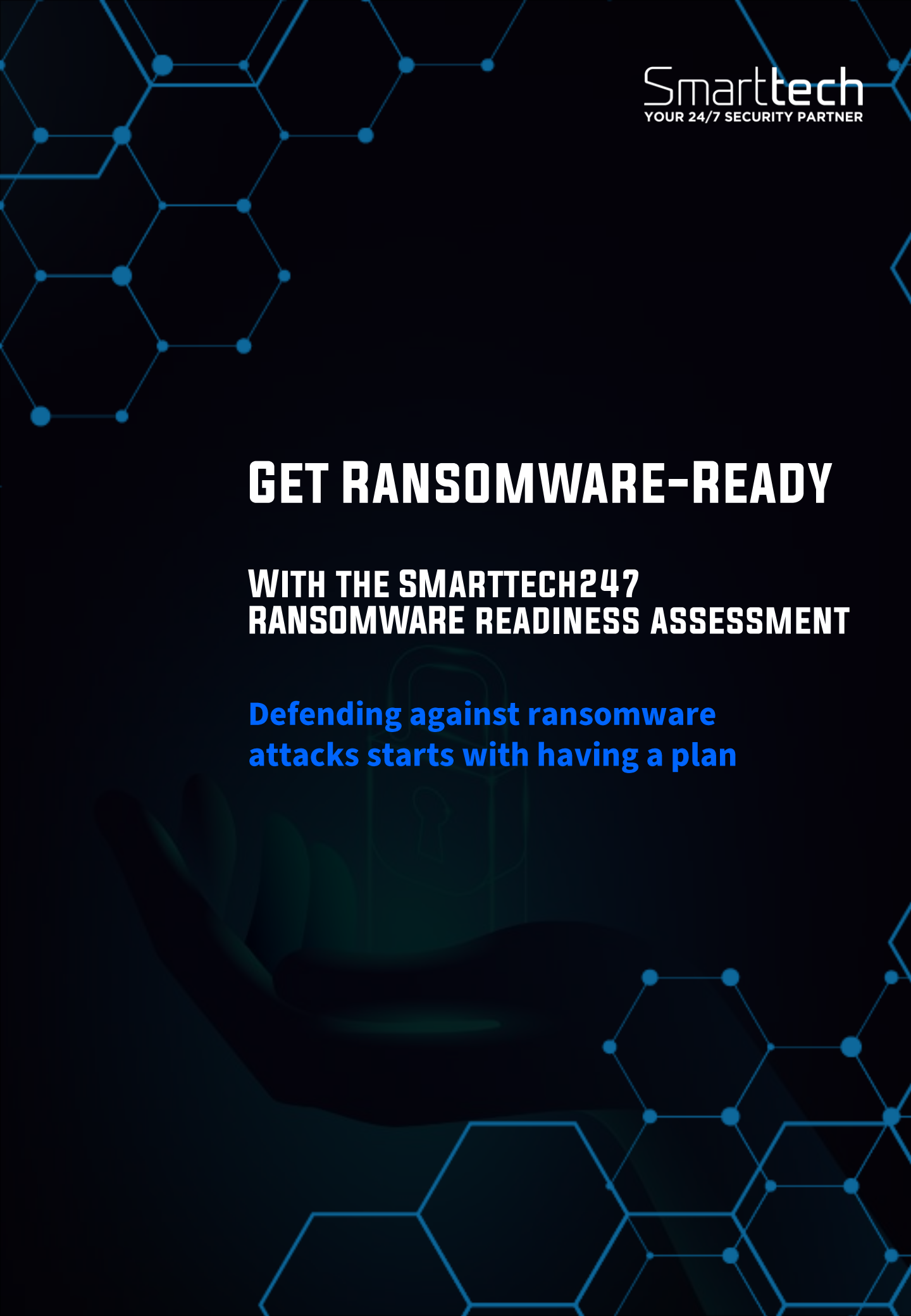
Smarttech
YOUR 24/7 SECURITY PARTNER

GET RANSOMWARE-READY

WITH THE SMARTTECH247 RANSOMWARE READINESS ASSESSMENT

Defending against ransomware attacks starts with having a plan



Smarttech
YOUR 24/7 SECURITY PARTNER

RANSOMWARE THREATS

Attackers are holding organizations hostage

Ransomware is reaching unprecedented levels. Ransomware operators are now taking a much more focused approach to targeting their victims. The Smarttech247 research shows that hackers take their time to learn about the victims and their networks, and then swiftly infect hosts. Besides encrypting data, an increasing number of adversaries now exfiltrate and threaten to publish stolen data to increase ransom payments.

Ransomware attacks can quickly disrupt the operations and cripple businesses functions by cutting off access to critical information within minutes.

The global average cost of a data breach in 2020 was $3.86 million although this average for the US increased to $8.64 million.

Since the global onset of COVID-19 last year, cybercrime heights have soared and many companies have struggled to keep up with the complexity of evolving cyber threats. Ransomware attacks are becoming more and more sophisticated and are now starting to become a daily threat to our lives. Notable ransomware attacks so far this year include Ryuk, Conti and Sodinokibi — and cyber criminals are expected to keep organisations firmly in their sights in 2021 and beyond.

95% of cybersecurity breaches are caused by human error.

Ransomware damages from cybercrime are expected to hit $6 trillion in 2021, up from $20 billion in 2020 and $11.5 billion in 2019.

37% of all breaches involve the use of stolen credentials.

SMARTTECH247 EXPERT-LED RANSOMWARE READINESS ASSESSMENT

The new breed of ransomware strains means that threat actors are utilising cobalt strike and other tools to navigate their way around your network before deploying ransomware - often by using compromised active directory privileged credentials or a zero day vulnerability.

Compromised privileged AD accounts cause a significant number of breaches. Hackers use these accounts to infiltrate the core of the network and subvert security controls. They can turn off your AV systems and other security tools. The Smarttech247 Complete Ransomware Analysis addresses this challenge with a ransomware-focused compromise assessment.

The Smarttech247 threat intelligence and advanced forensics team will work with you to fully understand your potential exposure. This is a technical engagement through the lens of a hacker. It includes scanning endpoints in your environment, reviewing forensic artefacts and collecting endpoint telemetry to uncover evidence of malicious files or suspicious activity often associated with early stages of the ransomware lifecycle.

AS PART OF THIS PACKAGE YOU RECEIVE:

- A full ransomware readiness assessment
- Analysis of internal network scan findings
- A review of your response plan and recommendations to strengthen it

THE BENEFITS OF THIS PACKAGE ARE:

- Avoid attacks with ransomware safeguards
- Recover faster with a best-practice response playbook
- Test your readiness with a ransomware tabletop exercise

REACH OUT TO US FOR PRICING

WWW.SMARTTECH247.COM
INFO@SMARTTECH247.COM
+353 212 066033

Smarttech
YOUR 24/7 SECURITY PARTNER