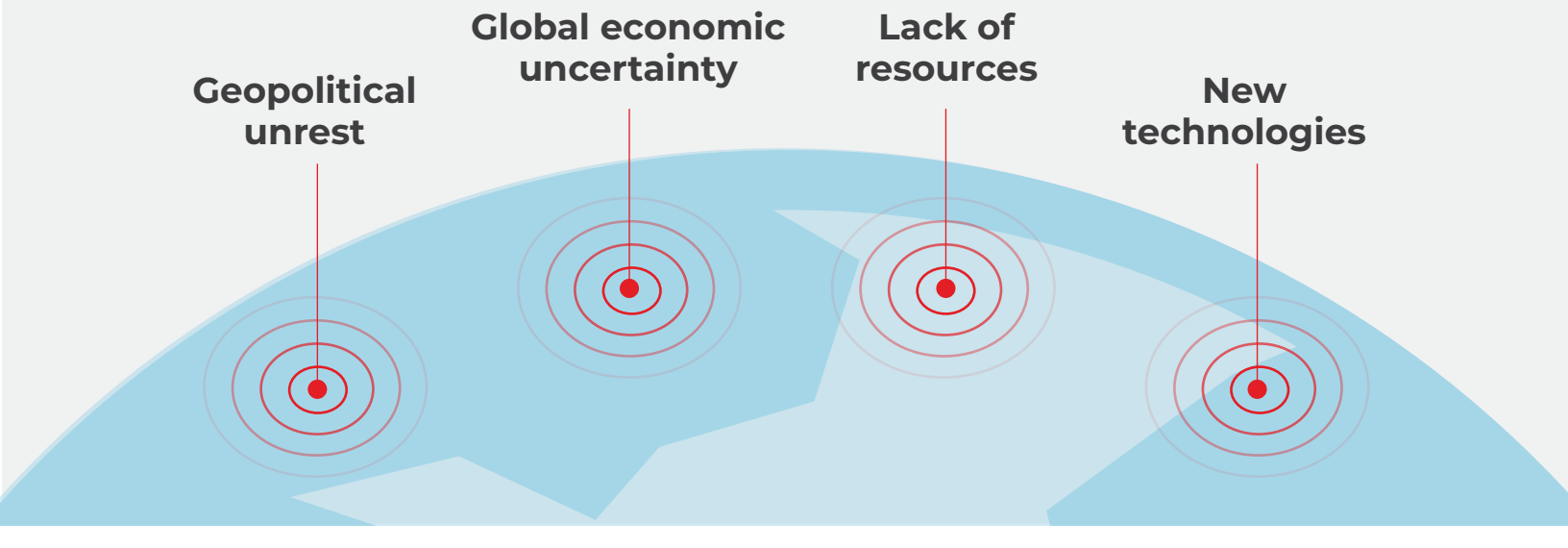
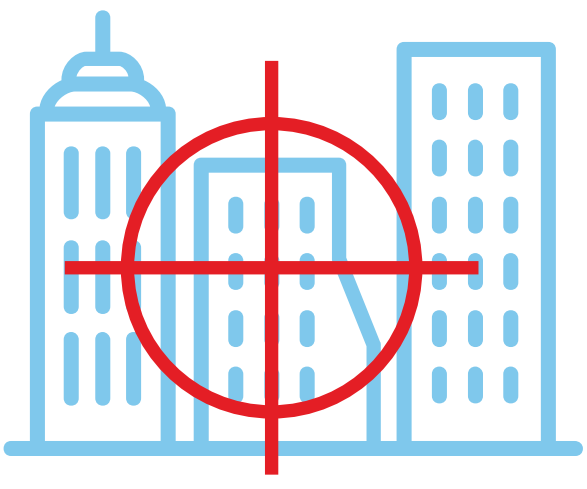
INCREASINGLY SOPHISTICATED

SUPPLY CHAIN CYBER-ATTACKS ARE ON THE RISE

DUE TO SEVERAL GLOBAL FACTORS





ENTITIES ACROSS THE CONSUMER, COMMERICIAL, INDUSTRIAL AND GOVERNMENT SECTORS ARE AT RISK

- Disrupted business continuity
- Damaged reputation
- Endangered national security
- Increased litigation costs
- Lost business opportunities

EMERGING TECHNOLOGIES INCREASE VULNERABILITY

41%

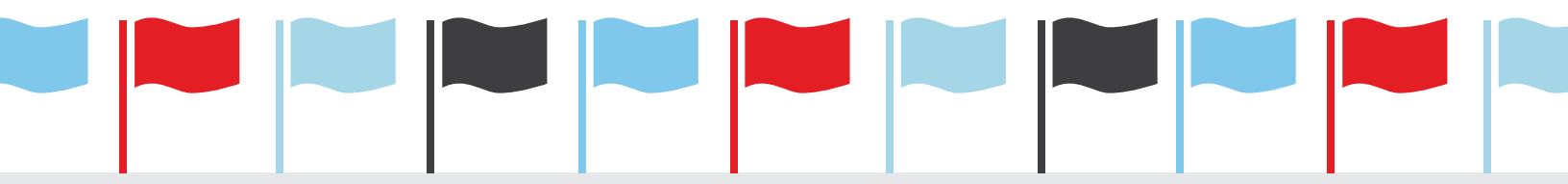
increase in the average number of weekly attacks per organization targeting IoT devices in the first two months of 2023 compared to 2022.

>80%

of analyzed open-source code in 2022 contained at least one vulnerability. **More than 50% had high-risk vulnerabilities.**

95%

growth in cloud exploitation cases in 2022. **Nearly 40% of businesses experienced a data breach in their cloud environment.**



MORE THAN 156 COUNTRIES ARE ENACTING CYBERCRIME LEGISLATION

and several others are drafting new legislation setting new requirements for cyber and supply chain security.

PROTECT YOUR ORGANIZATION WITH SCS 9001

INDUSTRY SPECIFIC FOR ICT

THE FIRST EVER CYBER AND SUPPLY CHAIN SECURITY STANDARD DEVELOPED SPECIFICALLY FOR THE ICT INDUSTRY.

- ✓ Protects business operations and revenues
- ✓ Improves critical infrastructure resiliency
- ✓ Reduces risk of litigation
- ✓ Gains a competitive advantage
- ✓ Meets global government mandates
- ✓ Protects brand reputation
- ✓ Builds credibility with end customers
- ✓ Provides common framework of measurement and rating

SCS 9001 STANDS OUT FROM OTHER STANDARDS

- + Prioritizes security for full product life cycle
- + Addresses specific needs of the ICT industry
- + Sets a comprehensive global standard
- + Is network, technology and device agnostic

SCS 9001 establishes a process-based architecture and provides a systematic framework that's repeatable in all industries

TIA®

THE TRUSTED INDUSTRY ASSOCIATION FOR THE CONNECTED WORLD.

Learn more about SCS 9001 at tiaonline.org