

# stc cybersecurity

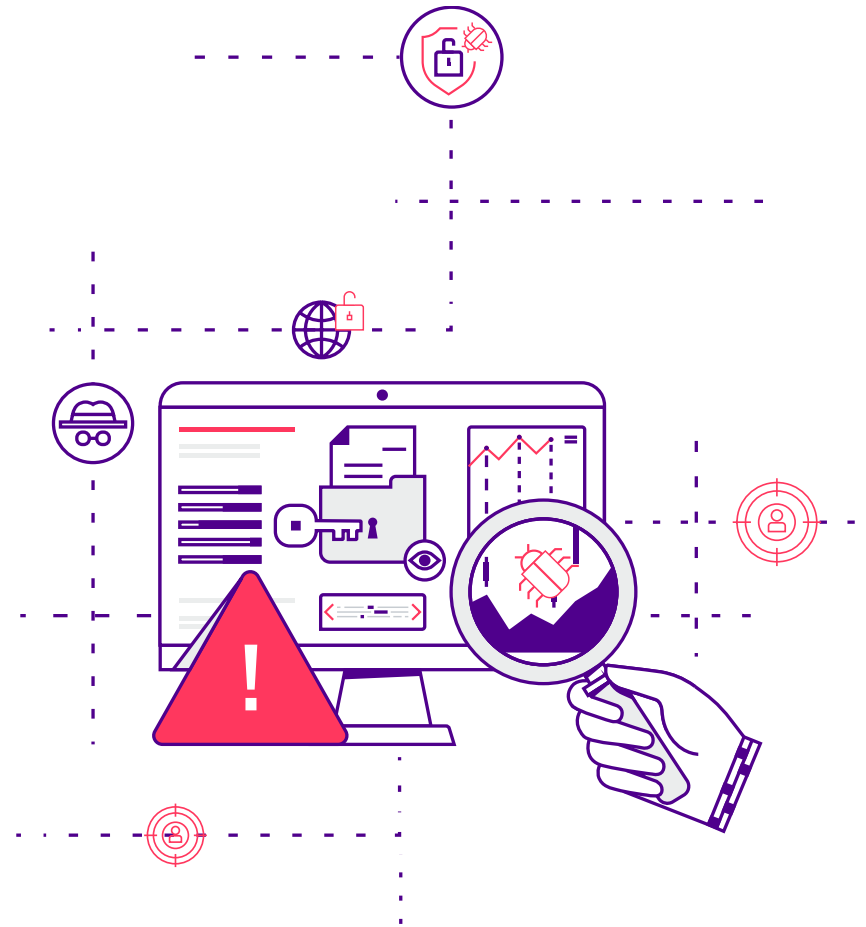
protecting your business as it grows





# stay ahead of evolving cyber risks with **stc business**

proactive and multi-layered cybersecurity solutions from stc business protect your organization from the most dangerous cyber risks. from advanced persistent threats to ransomware, we equip you with the right strategies to defend your business.



# 2

## cybersecurity myths debunked

### cybersecurity is too expensive

some view cybersecurity as costly, but with data breach costs averaging **\$4.35 million** in 2023, strong security investments lead to savings.

### small businesses are safe from cyberattacks

many believe small businesses are immune to cyber threats, but **43%** of attacks target them. tailored security solutions are essential for defense.

### a firewall is sufficient for protection

a firewall is useful, but it's not a complete solution. a multi-layered strategy is essential to address today's diverse threats.

### antivirus software provides complete protection

antivirus software is important, but it can't cover all threats. a layered security approach is needed to address all gaps.

3

# top cybersecurity challenges

01.

## complexity of threats

the constantly evolving threat landscape expands as business networks grow, requiring organizations to continually adapt defenses to manage emerging risks.

## regulatory compliance

keeping up with shifting regulations is challenging, but proactive compliance ensures data integrity and avoids the diversion of resources from core security efforts.

## incident response

organizations must be prepared to act swiftly during a cyber incident to minimize damage, maintain business continuity, and protect their reputation.

## security visibility

comprehensive security visibility is essential, starting from business problems and extending outward to evaluate the broader impact on all stakeholders.

3

# top cybersecurity challenges

02.

## **risk assessment**

a clear understanding of threats and critical assets is key to developing a robust security strategy by applying the right controls.

## **supply chain risks**

while outsourcing can improve efficiency, it often introduces vulnerabilities, necessitating a strong risk management program to mitigate vendor-related breaches.

## **protecting critical assets**

identifying and safeguarding the critical data, systems, and software that fuel business growth is crucial, particularly as part of the wider IT ecosystem.

## **employee awareness**

human error is a leading cause of breaches, underscoring the importance of training employees to recognize and prevent cyberattacks, fostering a security-conscious culture.



# our cybersecurity solutions

## 01.



### SOC as a service + SOAR

around-the-clock monitoring and threat detection and response to proactively safeguard your organization against evolving cyber risks.

#### key features:

- comprehensive security monitoring 24/7
- local SOC and integrated SOAR
- SOC made cost-effective
- automation and incident response
- SLA driven
- simplifies cybersecurity compliance program
- access to highly skilled global security experts & experienced analysts

#### solution packages:

##### security operation center as a service

add-on 1: manage cyber threat intelligence

add-on 2: SOAR - response automation

add-on 3: DFIR (digital forensics and incident response)



### managed cyber threat intelligence

empower organizations to stay ahead of the evolving security risks through continuous monitoring, analysis, and actionable insights. gain a decisive advantage against cyber adversaries with a cyber threat intelligence service.

#### key features:

- visibility over full external attack surface
- ML-powered noise cancellation
- prioritization of the most critical exposures
- actionability for swift & streamlined remediation
- SIEM, SOAR and TIP integrations
- comprehensive reports

#### solution packages:

##### managed cyber threat intelligence service

add-on 1: asset discovery & monitoring

add-on 2: data breach prevention

add-on 3: account takeover prevention

add-on 4: brand protection

add-on 5: dark web monitoring



### digital forensics and incident response

provides rapid containment, analysis, and remediation of cyber incidents to minimize the impact and prevent future attacks.

#### key features:

- rapid incident triage
- in-depth forensic analysis
- proactive threat hunting
- seamless remediation
- robust incident reporting
- SLA driven involvement
- prove due diligence to relevant stakeholders (e.g., regulators and customers)

#### solution packages:

digital forensics & incident response - remote

digital forensics & incident response - onsite



# our cybersecurity solutions

## 02.



### cyber defense services with AI security platform

AI security platform correlates threats across the entire organization, delivering proactive cyber resilience with real-time detection and autonomous response to known and novel threats.

#### key features:

- data agnostic
- real-time threat detection
- smart automation & rapid response
- comprehensive protection across your enterprise
- AI-powered autonomous defense

#### solution packages:

- package 1: cloud security
- package 2: email security
- package 3: network security (NDR)
- package 4: OT security
- package 5: identity security
- package 6: endpoint security
- package 7: proactive exposure management
- package 8: attack surface management
- package 9: incident readiness and recovery



### endpoint detection & response and MDR

identify, investigate, and automatically contain threats with endpoint protection and eradicate threats across the entire attack surface with the industry leader in managed detection and response (MDR).

#### key features:

- 24x7 monitoring and investigation of alerts
- rapid response and surgical remediation in minutes
- expert threat identification and hunting
- rapid protection and response at the endpoint, cloud workload and identity layers
- proactive threat hunting for evolving zero-day threats
- detailed root cause analysis

#### solution packages:

- package 1: managed end points detection and response
- package 2: managed XDR service
- package 3: managed detection and response service



### offensive penetration testing as a service (PTaaS)

alternative approach to traditional penetration testing service. move in to offensive and continuous penetration testing. agilely launch and manage your security tests from end to end with our vulnerability management platform and our elite cybersecurity experts.

#### key features

- streamlined and controlled testing environment
- secure local hosting of the platform
- work only with top-performing security researchers
- agilely launch multiple tests all year long
- find critical vulnerabilities and get remediation guidance
- real-time risk visibility
- real-time communication with researchers
- custom reports including regulatory compliances

#### solution packages:

- package 1: on demand PTaaS
- package 2: continuous PTaaS
- package 3: bug bounty program
- package 4: vulnerability disclosure program



# our cybersecurity solutions

## 03.



### email security as a service

advanced, multi-layered protection against the full range of email threats, including spam, phishing, spoofing, malware, and business email compromise, with a simplified deployment.

#### key features:

- visibility and control
- top-rated protection
- industry-leading security efficacy
- cost-effective cloud-based pricing
- zero-day threat prevention

#### solution packages:

- package 1: email security as a service
- package 2: business email compromise protection service

add-on 1: DMARC, SPF & DKIM protection  
add-on 2: email security remediation  
add-on 3: dedicated email security assistant



### secure access service edge (SASE)

cloud-based network architecture that converges networking and security services into a unified, scalable platform. This solution protects your branches, applications, users, workloads and OT/IoT assets regardless of their location or device.

#### key features:

- SD-WAN
- zero trust network access (ZTNA)
- secure web gateway (SWG)
- firewall as a service (FWaaS)
- cloud access security broker (CASB)
- data loss protection (DLP)
- identity driven security
- business analytics

#### solution packages:

- package 1: secure access service edge
- package 2: secure service edge



### cyber advisory services service

professional consulting services help organizations assess, improve, and maintain their security posture by offering expert guidance on identifying risks, implementing protective measures, and ensuring regulatory compliance.

#### key features:

- security assessments
- tailored recommendations
- compliance guidance
- transformation roadmap
- ongoing support

#### solution packages:

- package 1: policy & frameworks development
- package 2: cybersecurity and IT standards implementation
- package 3: GRC assessments
- package 4: architecture review
- package 5: privacy program design & rollout
- package 6: BCM/DRP program design & rollout





# our cybersecurity solutions

## 04.



### DDoS protection as a service

real-time, AI-powered DDoS mitigation that leverages global infrastructure and expert oversight to swiftly detect and neutralize even the most sophisticated attacks.

#### key features:

- automated mitigation
- comprehensive monitoring
- unlimited and unmetered mitigations
- brand protection
- subscription-based pricing

#### solution packages:

stc DDoS protection for dedicated internet access  
stc DDoS protection for advance internet service



### firewall as a service

a cloud-based solution that delivers comprehensive managed firewall protection with 24/7 expert support and the agility to adapt to evolving security needs.

#### key features:

- locally hosted
- uninterrupted protection
- robust security
- seamless deployment
- subscription-based pricing

#### solution packages:

firewall as a service – premium package (dedicated firewall)  
firewall as a service – advanced package (dedicated firewall)  
secure internet (shared firewall)



### web protect

cloud-based security solution provides the first line of defense by blocking requests to malicious destinations before a connection is established without any software installed.

#### key features:

- effortless activation
- extensive defense
- cost-effective security
- hassle-free cybersecurity
- adaptive protection
- integrated security and connectivity

#### solution packages:

web protect – business voice  
web protect – mobile broadband  
web protect – fiber broadband



# stc business your trusted cybersecurity partner

we deliver innovative, customized cybersecurity solutions designed to strengthen your security posture. as your trusted partner, we're here to safeguard your business from evolving threats.

## why choose us for cybersecurity?



**24/7** local support and rapid incident response.



tailored solutions to fit your business's unique needs.



industry-certified cybersecurity experts.

# stc

[www.business.stc.com.bh](http://www.business.stc.com.bh)

follow us on:

