SECURITY OPERATION CENTRE AS-A-PLATFORM (SOCaaP)

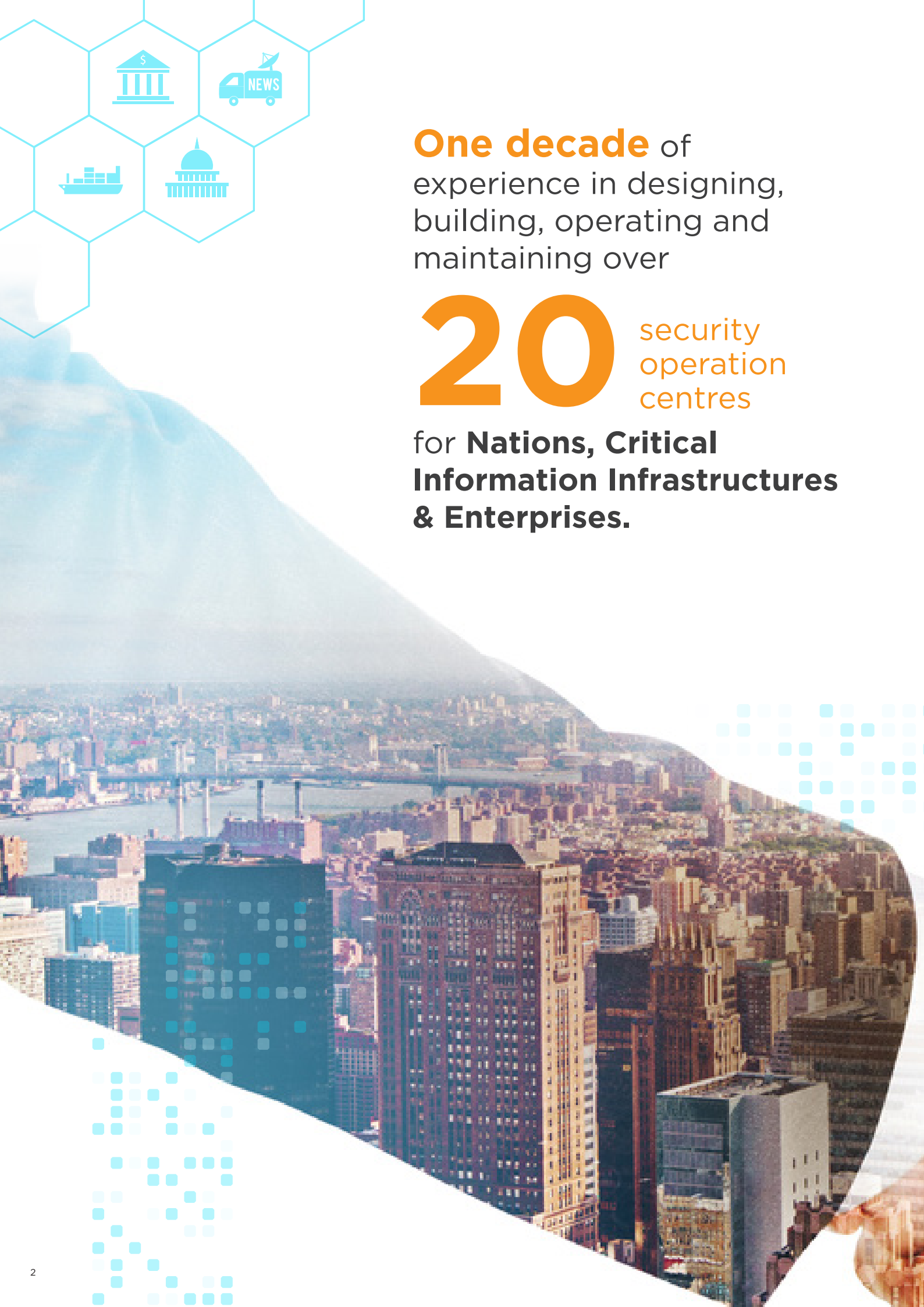
Uncover unknown threats faster than ever

ST Engineering

One decade of experience in designing, building, operating and maintaining over

20 security operation centres

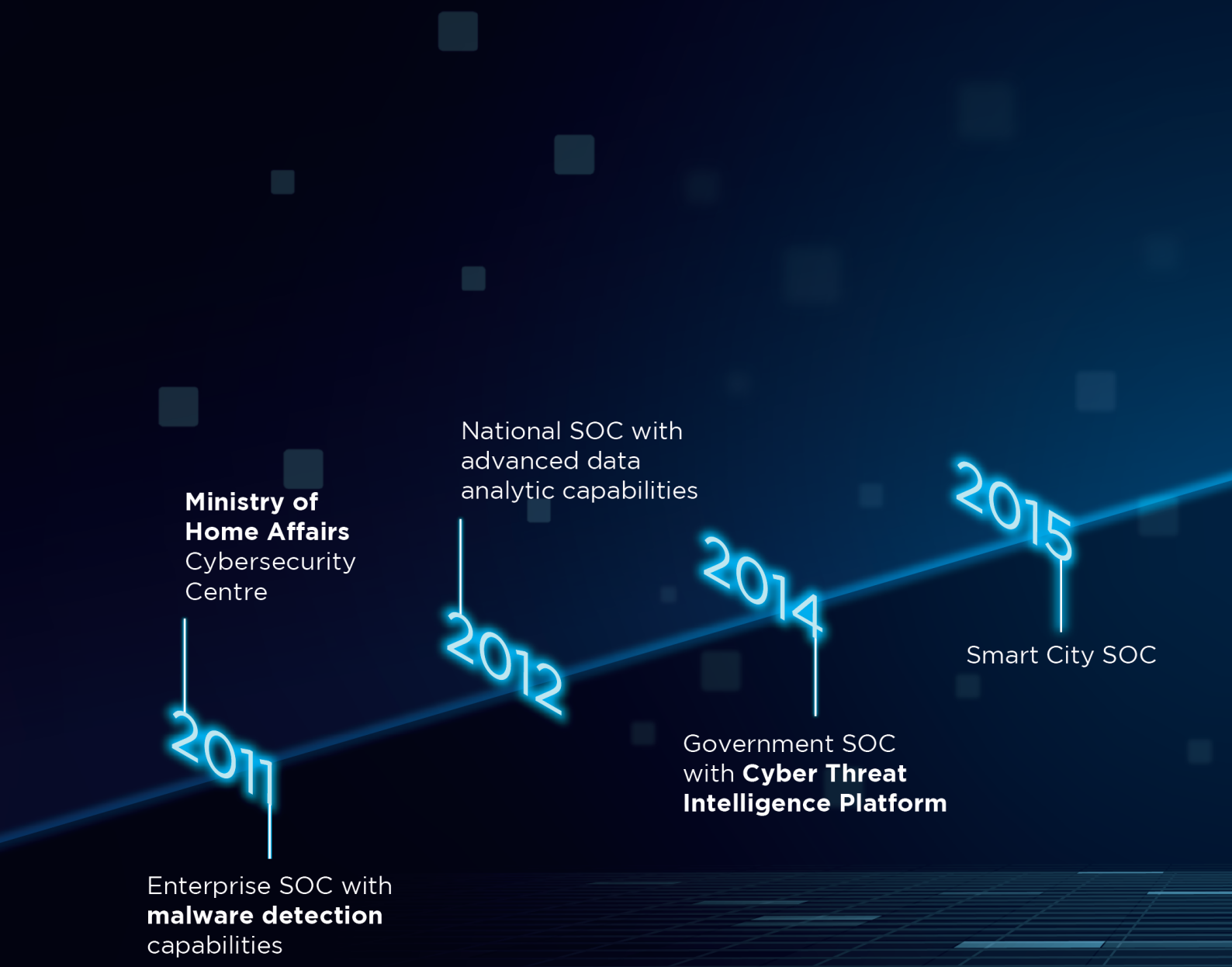
for **Nations, Critical Information Infrastructures & Enterprises.**



Who We Are

ST Engineering's cybersecurity arm is a pioneering and leading provider of cybersecurity solutions with almost two decades of comprehensive future-ready cybersecurity solutions. Backed by indigenous capabilities and deep domain expertise in cybersecurity, we offer robust cyber-secure products and services in cryptography, cybersecurity engineering, digital authentication, SCADA protection, audit and compliance. Our cybersecurity academy has also certified and trained cybersecurity professionals in more than 150 organisations.

Building SOCs for Nations, CIIs and Enterprises



DEEP EXPERTISE, VAST EXPERIENCE AND EX

SYSTEM INTEGRATION

SOC

CRITICAL INFORMATION INFRASTRUCTURES (CIIs)


Aviation


Banking & Finance


Energy


Government

Design & Build

2017

Overseas consultancy for national cybersecurity SOC (Sri Lanka)

Land transport cybersecurity monitoring centre

2018

Overseas consultancy for financial sector (Sri Lanka)

Transport SOC with operational technology capabilities

Advanced enterprise SOC with orchestration and automation capabilities

2019

Energy sector cybersecurity centre with OT analytic capability

Overseas transport SOC with SOCaaP capabilities in Myanmar

Maritime sector cyber SOC with managed security services

2020

Overseas managed security services with SOCaaP

Transport SOC with security orchestration automation response capabilities

Utility SOC with acoustic threat detection capabilities

Design, Build & Operate

XTENSIVE DOMAIN

MANAGED SERCURITY SERVICES

SOCaaP

Challenges of SOC

SUSTENANCE
OF CYBERSECURITY EXPERTISE

- Lack of cybersecurity professionals
- Inadequate skillsets
- Constantly evolving skills

EFFECTIVENESS
OF SOC OPERATIONS

- Lack of well defined processes
- Lack of targeted use cases

TECHNOLOGY
RELEVANCE & MAINTENANCE

- High cost to build and maintain
- High cost to keep up with latest technology

"Technology evolves every 6 to 18 months"

According to Prof. Issac Ben-Israel, Chairman, Israel Space Agency & Israel National Concil for R&D.

Pain Points of Organisations

"How many and what technology tools do I need to use?"

"How can I sustain the competencies of cybersecurity professionals?"

"How can I have continuous expertise to manage and monitor all the systems?"

Build Your SOC on a Resilient Foundation with Us

SOCaaP addresses these challenges and empowers organisation to do more with less, allowing security teams to focus on what really matters.

Accelerate knowledge to people

Well defined processes to optimise actions

Modular architecture to swop out obsolete technology efficiently & effectively

SOC is more than just a SIEM

Tedious to connect the dots	Alerts too many meaningless incidents. Impedes race against the attackers due to backlog of unhandled incidents.
Insufficient correlation rules	SIEM rules are insufficient to address today's needs. It needs time and technical expertise to configure extensively to the requirement.
Challenging user experience	Typically shows all network activities in a tabular format, making it difficult to decipher and pin point the cause and origin of attack at a glance.
Lack of built-in mitigation tools	Provides no actionable workflow to lead the mitigation process. SOC team needs to be notified about incidents to take remedial actions in real-time.

Power Your SOC with SOCaaP

SOCaaP is the unified solution that combines machine-based analytics, intelligence and security orchestration, automation and response (SOA through cloud to provide higher operational efficiency and ease of dep provides actionable insights, allowing security teams to uncover unkno and OT environment faster than ever.

contextualised threat
R). It is delivered
loyment. It also
wn threats in IT

PROTECT

Email

Web

End Point

DETECT

Threat Intel Driven Security Analytics

Online / Offline Log Retention

Use Cases / Correlation Rules

"**90%** of cyber threats start with email, making it the #1 threat vector."

Source: Gartner

Benefits of SOCaaP

50%

Up to 50% cost and time savings

ROI

Cost effectiveness with good ROI

Operational efficiency with well-defined processes

Adaptive decision dashboard to enable quick decision making

Key Capabilities

We are fully committed to empowering organisations to create a resilient cyber eco-system.

More than a technology, SOCaaP is a state-of-the-art cutting-edge solution that epitomises our advanced design thinking and leading competency standards. To deliver an effective SOC in the ever shifting digital landscape, the SOCaaP is designed with a full spectrum of key capabilities:

Open Architecture

Allows new solutions to be integrated without impacting individual functions.

Enables customers to evolve continuously with the cyber landscape, by being technology agnostic.

Multi-modal Analytics

Addresses unknown cyber threats through behavioural analytics from an integrated platform of analytics data models.

Contextualised Threat Intelligence

Provides intelligence-driven analysis by incorporating contextual information.

Orchestration & Automation

Automates the incident response workflow, reducing the workload and mundane tasks of analysts.

Integrated Decision Dashboard

Provides overall cyber health status and detailed operational analysis of the network, with customised dashboards for management and analysts to make informed decisions in the event of cyber-attack.

Executive Dashboard

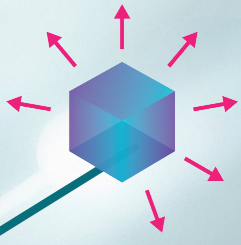
- Provides a security posture overview by displaying the log activities and alarm trends.
- Provides the foresight of attack trends, enabling the SOC manager to implement appropriate countermeasures.

Analyst Dashboard

- Enables the analyst to prioritise and react to any security incident immediately.
- Allows actions to be automated, minimising the Time to Response and Time to Resolution.

Playbook & Defined Processes

Leverages our decade-long experience in defining use cases across government agencies, critical information infrastructures and enterprises, to increase operational efficiency and consistency.



Ease of Deployment

Minimises complexity and reduces implementation lead time by covering essential SOC solutions including email protection, web isolation and endpoint device protection.

www.stengg.com
cybersecurity@stengg.com

DOP 0520

www.stengg.com/cybersecurity