PROACTIVE OT CYBERSECURITY SOLUTION

Securing the New Cyber-Physical World

ST Engineering

OT Threat Landscape

Operational Technology (OT) refers to computing systems that manage industrial operations, as opposed to administrative operations. OT is common in Industrial Control Systems (ICS), such as Supervisory Control and Data Acquisition (SCADA) systems.

Cyber-attacks have expanded beyond the digital realm of IT into the physical world of OT. Attacks on independent and distinct supply chains could affect OT systems. With the exponential increase in vulnerabilities and risk, it calls for business leaders to adopt a holistic and proactive approach to secure the critical sectors.

Recent OT Cyber-Attacks

SEP 2023

National Power Grid Attack

The hackers used ShadowPad Trojan to target an undisclosed Asian country's national power grid.

Bank Info Security

JUL 2023

Logistics Port Attack

A ransomware attack disrupted communication systems and prevented import and export operations.

Dragos, Inc

NOV 2022

Train Network Attack

A compromise in an IT subcontractor's software testing environment caused the train to standstill for several hours.

Reuters

NOV 2022

Ransomware Attack

A ransomware attack halted outpatient care and non-emergency surgeries at a major Japanese hospital for a second day.

Bank Info Security

AUG 2022

Power and Airport System Attacks

4.9 million cyberattacks within a single day, and Taiwan's Taoyuan International Airport was allegedly attacked by hackers as it took longer than usual to open the site.

Taipei Times

Challenges Faced by Organisations

Lack of Visibility

Inexperienced OT Personnel

Rapid Pace of Change

Network Complexity

Key Factors Driving Towards a Coordinated OT/IT Security Strategy

Since 2020, there have been several high-profile cyber-attack incidents in the OT environment. According to the survey report from 'The Critical Convergence of IT and OT Security in a Global Crisis', over half (51%) of U.S.-based respondents say their organisation is now more of a target for cyber criminals compared to before COVID-19, with a striking 67% having seen cyber criminals use new tactics to target their organisation. Many factors drive this:

- Increased IT-OT Convergence
- Move towards Smart Nations Notion and Digital Acceleration of Industrial Organisations
- Growing Sophisticated and Advanced Threat Actors
- Rise in Critical OT Vulnerabilities Discovered
- Ransomware Actors Targeting OT Assets

Cyber Secure and Future Proof

ST Engineering is a leading provider of trusted and innovative cybersecurity solutions, with over two decades of deep experience and a proven track record in securing and defending critical infrastructures.

We deliver trusted, future-ready cybersecurity solutions backed by:

- ✓ **Cybersecurity capabilities**
- ✓ **Deep expertise**
- ✓ **Broad experience across all domains**

Our significant investments in research and development, strategic partnership with leading research institutes, academic partners, and industry in capability development propels us to create future-ready cybersecurity solutions to secure the dynamic digital world.

The Critical Infomation Infrastructures (CII) We Serve

Government

Media

Healthcare

Info-communications

Security & Emergency

Land Transport

Banking & Finance

Energy

Water

Aviation

Maritime

While organisations have to cover the full extent of their computer networks and secure every endpoint, attackers, only need to pinpoint the weakest link.

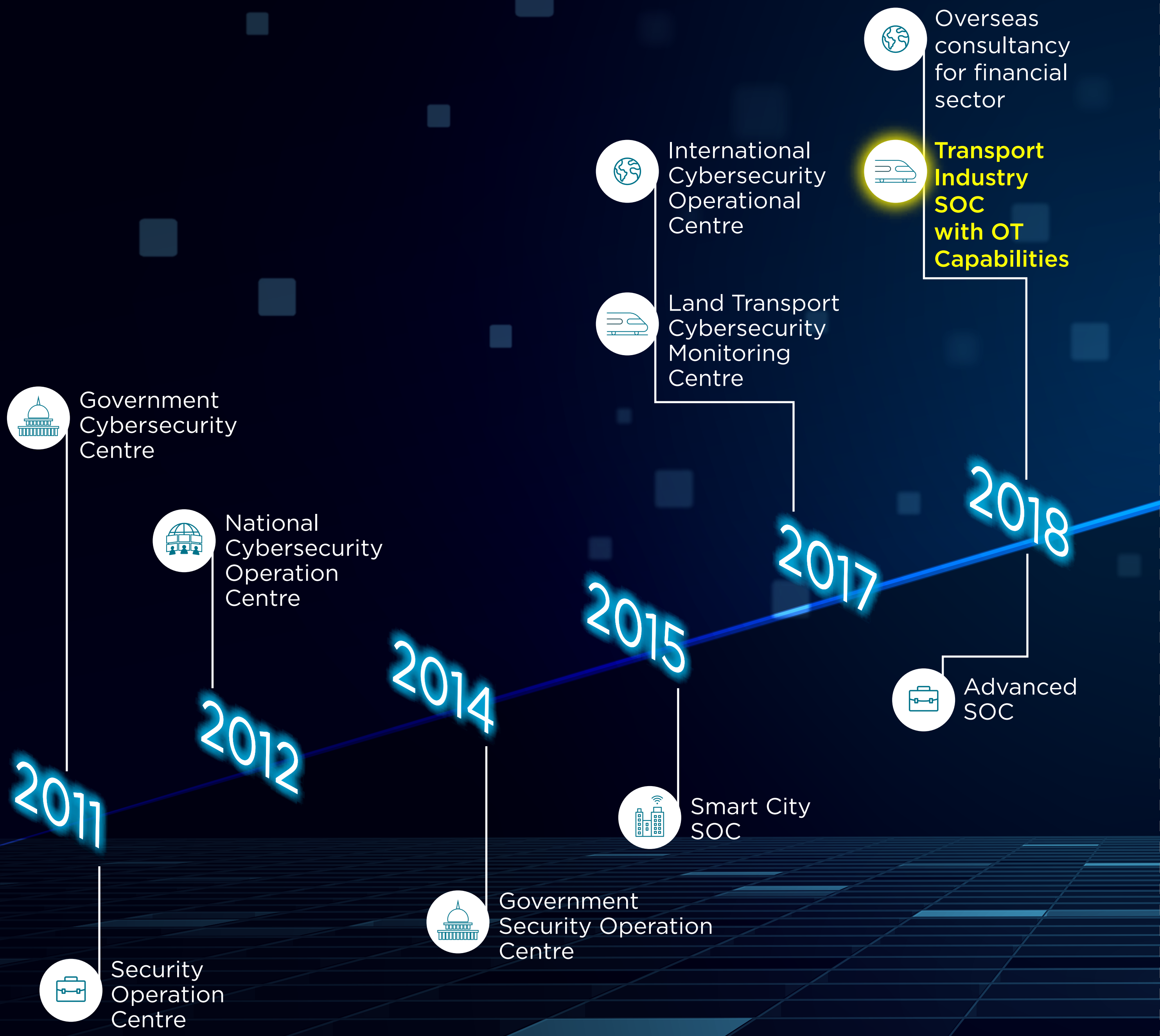
Cyber-defenders must get it right every time, while threat actors only need to get it right once.

By providing our customers with robust cybersecurity architecture, solutions, and best practices, we enable a resilient OT environment for critical sectors.

Deep Expertise in OT Cybersecurity Solutions

Beyond IT to OT

Empowering Solutions, Understanding your Goals



2011

Government Cybersecurity Centre

Security Operation Centre

2012

National Cybersecurity Operation Centre

2014

Government Security Operation Centre

2015

Smart City SOC

2017

International Cybersecurity Operational Centre

Land Transport Cybersecurity Monitoring Centre

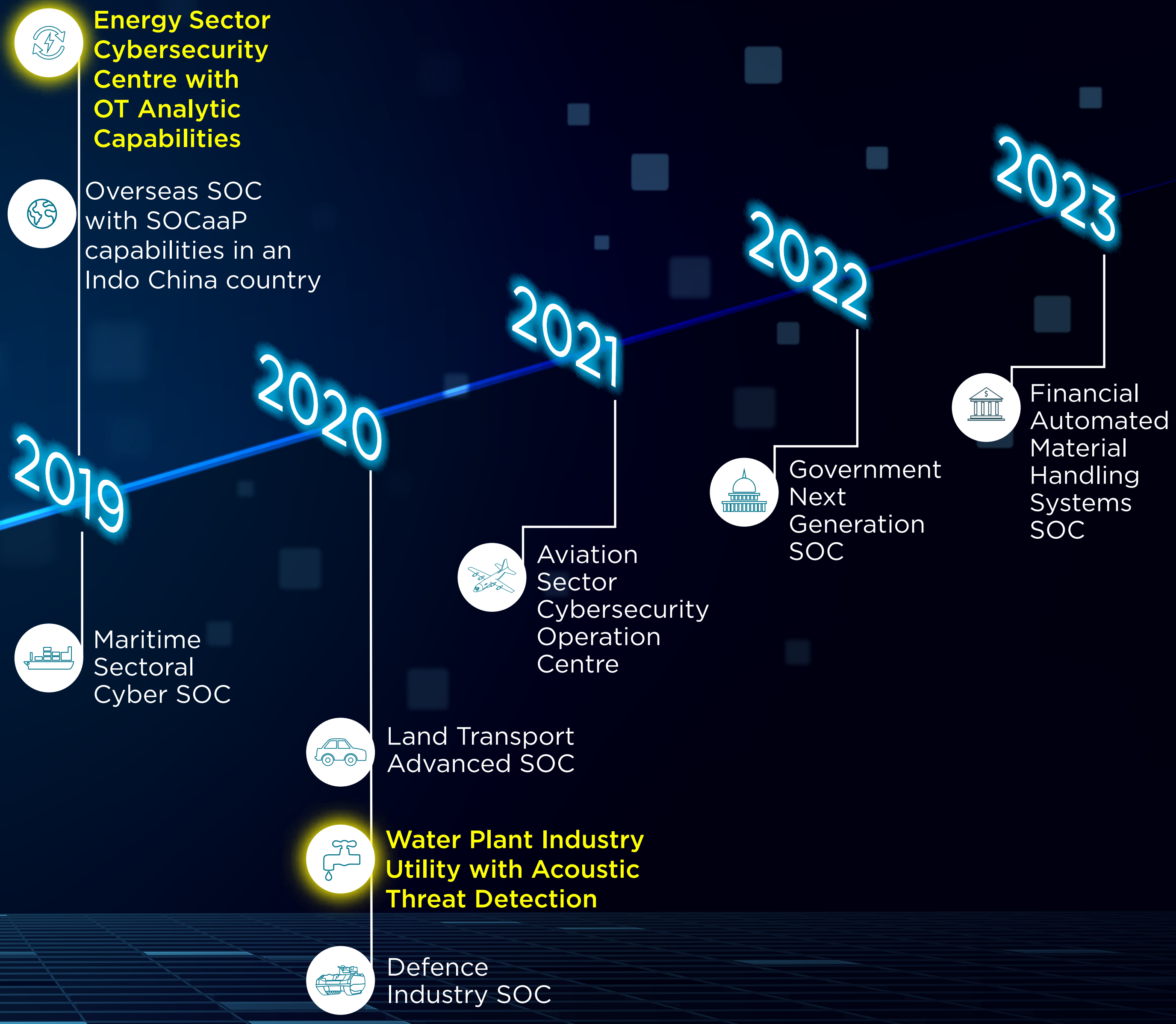
2018

Overseas consultancy for financial sector

Transport Industry SOC with OT Capabilities

Advanced SOC

Since 2011, ST Engineering has designed and built over 22 SOCs for national, defense, and government agencies across IT and OT sectors globally.



2019

Energy Sector Cybersecurity Centre with OT Analytic Capabilities

Overseas SOC with SOCaaP capabilities in an Indo China country

Maritime Sectoral Cyber SOC

2020

Land Transport Advanced SOC

Water Plant Industry Utility with Acoustic Threat Detection

Defence Industry SOC

2021

Aviation Sector Cybersecurity Operation Centre

2022

Government Next Generation SOC

2023

Financial Automated Material Handling Systems SOC

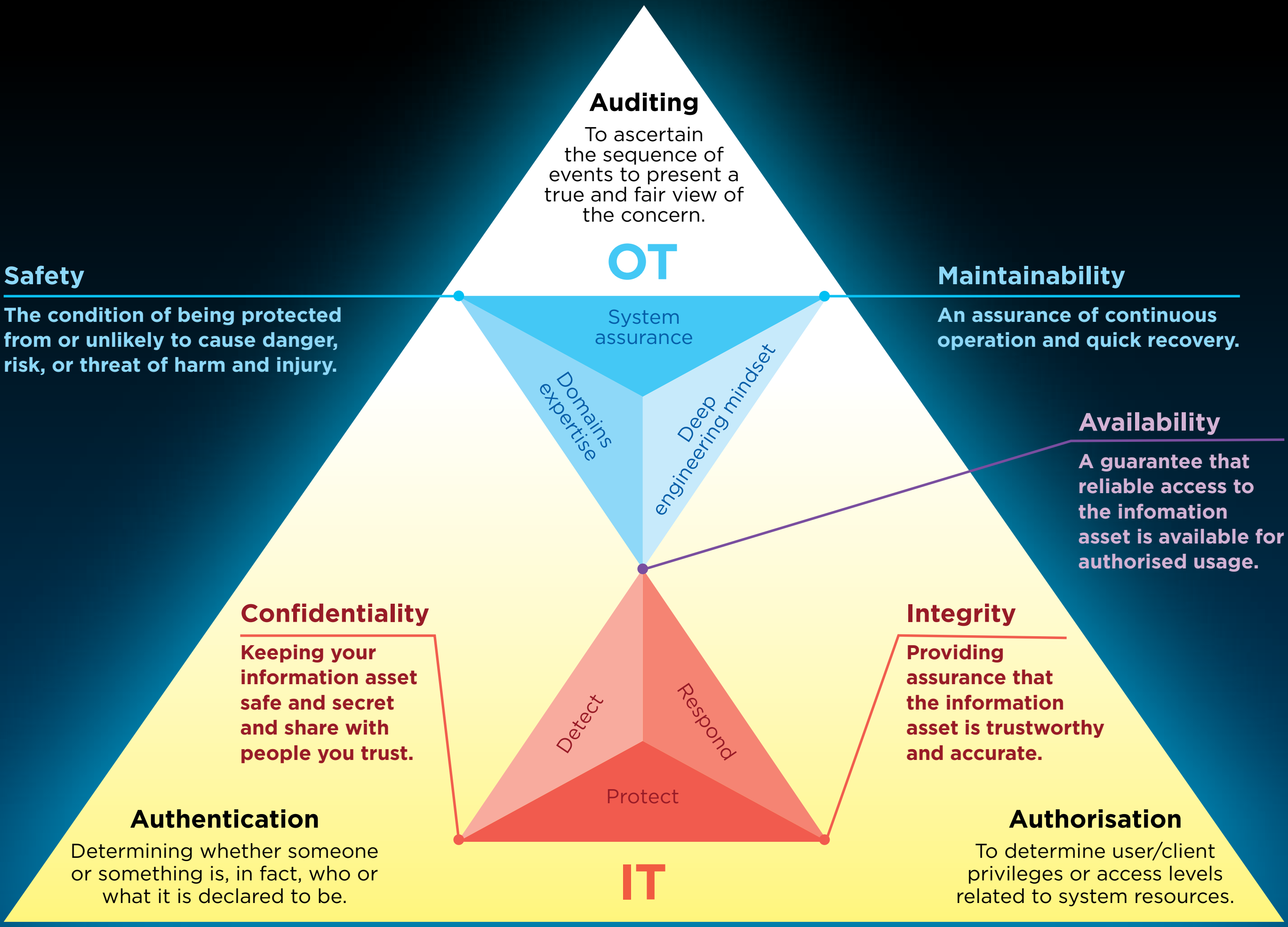
Legend ○ SOC ● **OT SOC**

An Integrated Framework

We are also aligned with global standards - Our integrated framework is aligned with the NIST Cybersecurity Framework, IEC 62443 standards and CCoP2.0 of Singapore.

To address the challenges, our approach to OT cybersecurity is adopting a multidisciplinary mindset and skillset with an integrated framework to meet the objectives of securing IT and OT networks:

AAA-SAM-CIA Pyramid



Auditing
To ascertain the sequence of events to present a true and fair view of the concern.
OT
Safety
The condition of being protected from or unlikely to cause danger, risk, or threat of harm and injury.
Maintainability
An assurance of continuous operation and quick recovery.
System assurance
Domains expertise
Deep engineering mindset
Availability
A guarantee that reliable access to the infomation asset is available for authorised usage.
Confidentiality
Keeping your information asset safe and secret and share with people you trust.
Integrity
Providing assurance that the information asset is trustworthy and accurate.
Detect
Respond
Protect
Authentication
Determining whether someone or something is, in fact, who or what it is declared to be.
Authorisation
To determine user/client privileges or access levels related to system resources.
IT

5 Cybersecurity ICS Pillars

We utilise the 5 Cybersecurity controls to create an efficient and effective Industrial Control System (ICS) or Operational Technology (OT) security programme, which enables organisations to adapt the controls to fit their environmental risks.

ICS Incident Response

Holistic operations-informed IR plan and tailored exercises to recover quickly in the event of an attack.

Defensible Architecture

Architecture to smoothly support OT systems and processes.

ICS Network Visibility Monitoring

Continuous monitoring to inform operators of potential risks.

Secure Remote Access

Remote access points to control and monitor points within secure segments.

Risk-Based Vulnerability Management

Awareness of digital controls and operating conditions to aid in risk-based vulnerability management decisions.

Source: SANS™ Institute, The Five ICS Cybersecurity Critical Controls. Published in Nov 7, 2022

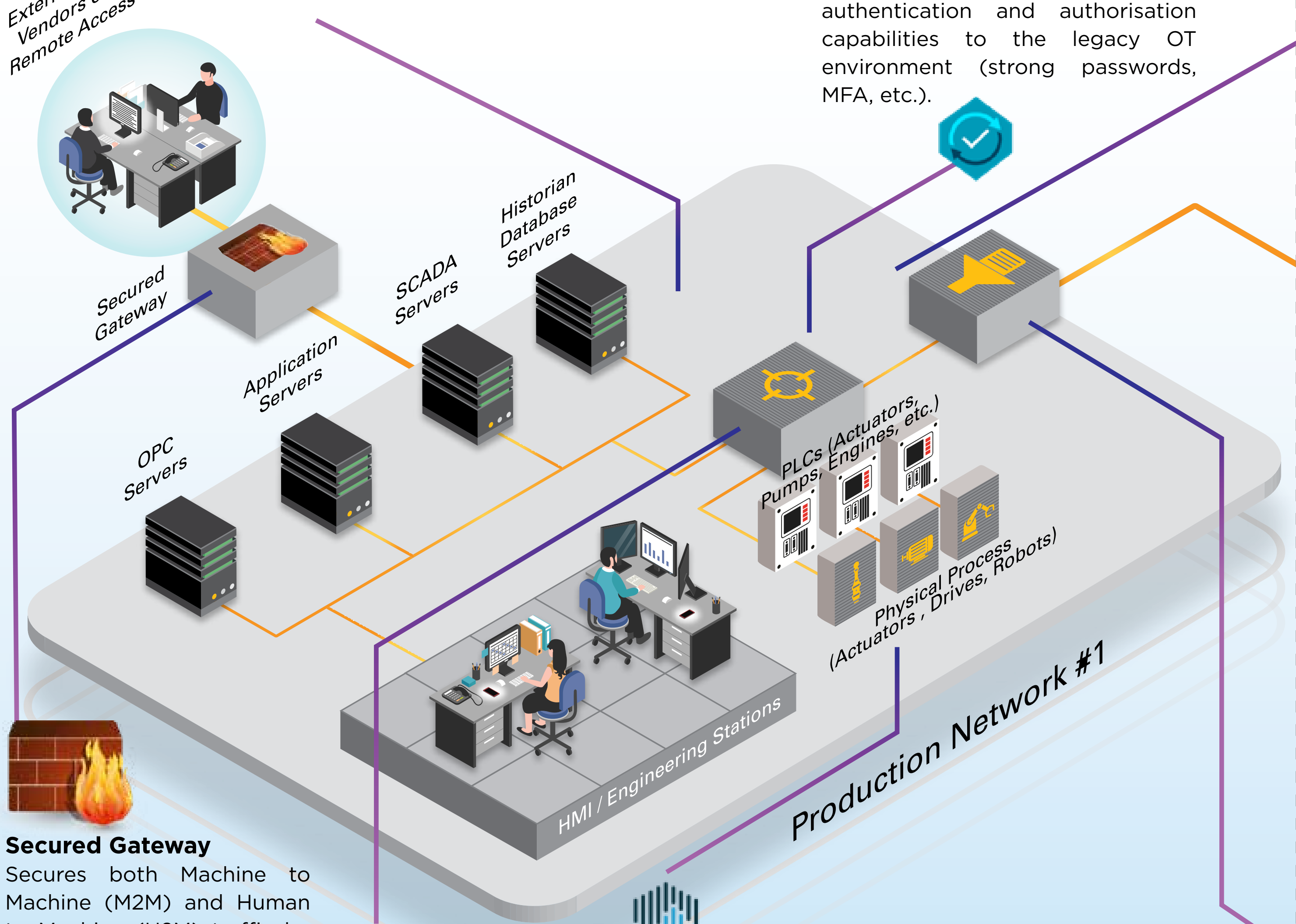
Our Holistic Solution for OT & IT Networks

OT Anomaly Detection Monitoring System (ADMS)

With 85% OT anomaly detection rate and augmented with Level 0 monitoring capability real-time alerts on behaviour anomalies without disrupting normal operation. It uses multiple security engines in parallel, each offering a unique capability to detect suspicious network traffic and activities.

Zero Trust Access Management

The Xage Fabric simplifies access management by providing a single system to manage and enforce access security policies. The Xage Security Fabric strengthens an organization's security posture by providing state of the art authentication and authorisation capabilities to the legacy OT environment (strong passwords, MFA, etc.).


External IoT Vendors on Remote Access
Secured Gateway
Historian Database Servers
SCADA Servers
Application Servers
OPC Servers
PLCs (Actuators, Pumps, Engines, etc.)
Physical Process (Actuators , Drives, Robots)
HMI / Engineering Stations
Production Network #1

Secured Gateway

Secures both Machine to Machine (M2M) and Human to Machine (H2M) traffic by incorporating Deep-Packet Inspection (DPI) capability for analysing SCADA network traffic. Upon detecting an anomaly, it automatically generates alerts, blocks the abnormal activity and isolates any affected sub-networks.

Xage Enforcement Point (XEP)

Working with the Xage Security Fabric, XEP provides access-policy enforcement to industrial systems.

SigaGuard

SigaGuard safeguards industrial assets by monitoring raw electrical signals (Level 0 real-time monitoring). By activating Machine Learning on rich and unfiltered electrical signals at Level 0, SigaGuard delivers an autonomous cyber inspection & analytics solution, offering bullet-proof detection of any cyber-attack, while delivering inaccessible insights, and operational resilience of industrial processes and automated machinery. Electrical signals at Level 0 are the most reliable source of data for OT environments.

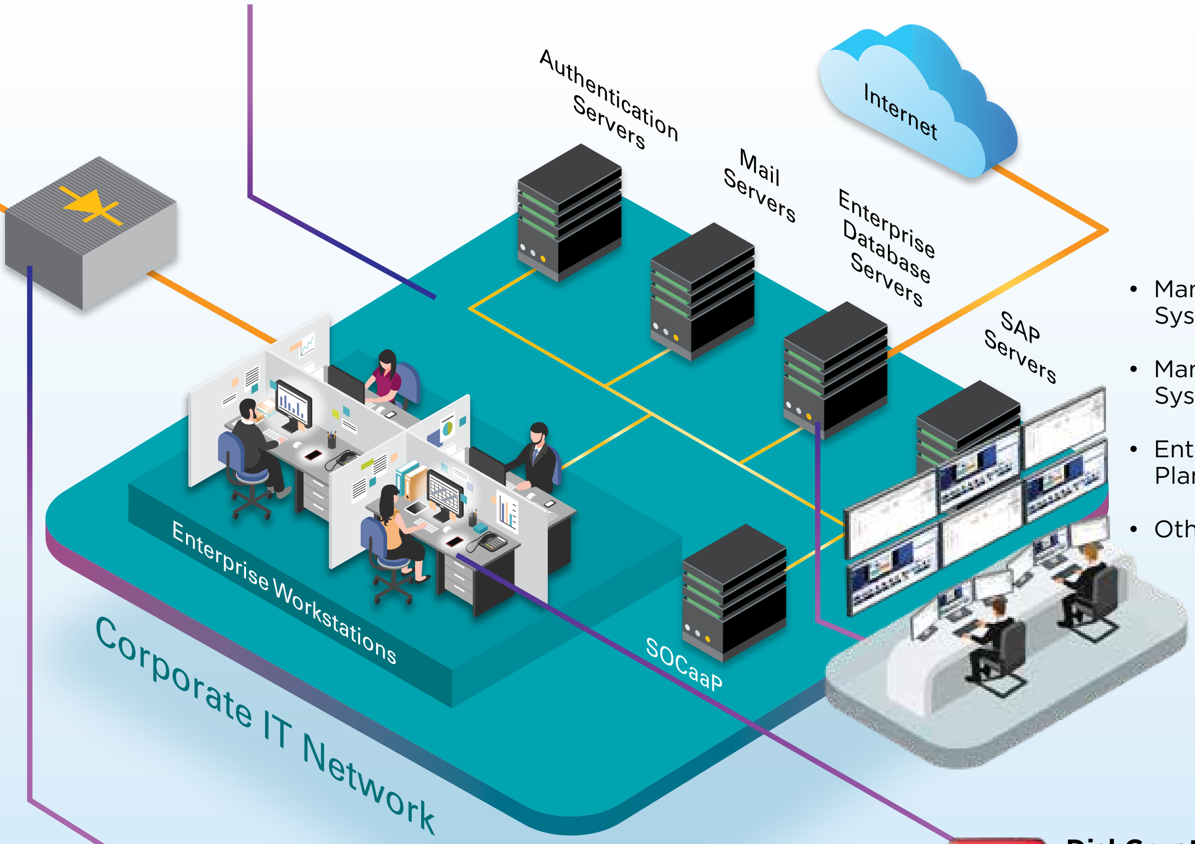
Our solutions are designed for CII, which includes Building Management System, ensuring the cybersecurity of ICS and SCADA systems. Our end-to-end solution suite involves the main deployment of OT Anomaly Detection Monitoring System (ADMS), COntinuous Risk & Vulnerability Assessment (CORVA), Data Collector (DC) and Secured Gateway (SG), alongside with proprietary products such as Data Diode and Diskcrypt M10.

Continuous Risk & Vulnerability Assessment (CORVA)

CORVA is a suite of technology solutions for assessment automation, continuous cloud monitoring, and managing supply chain cybersecurity risk. Enabled by Cyber Threat Intelligence, it also allows partners and vendors to secure and respond to threats on their networks proactively.

Operational Technology Risk Assessment (CIARA)

CIARA as part of the CORVA suite tailor made for industrial risk assessment, provides a management platform that provides risk mitigation measures while optimising cybersecurity expenditure. It also provides compliance workflow with reports and a dashboard that simplifies status reporting.



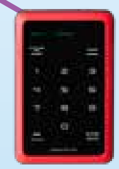
- Manufacturing Execution System (MES)
- Management Information System (MIS)
- Enterprise Resource Planning System (ERP)
- Other Enterprise Systems

ST Engineering Data Diode

Enables secure data transfer across physically separated networks, preventing data leakage, enabling network segregation and eliminating cyber-threats by enforcing one-way data transfer.

Data Collector

Sends all data traffic from remote sites to a central ADMS without overloading the network, by receiving all LAN traffic from the local switch (using port mirroring) via a secure tunnel.



DiskCrypt M10

Enables users to store information securely in an ultra-slim, credit-card size encrypted data storage with two-factor authentication smartcard protection, featuring real-time hardware encryption for data protection and smartcard technology for authentication.

www.stengg.com
cybersecurity@stengg.com

DOP 1023

www.stengg.com/cybersecurity