

TRUSTED INDUSTRIAL CYBERSECURITY SOLUTION

Securing the New Cyber-Physical World



OVERVIEW OF OT THREATS

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.

Recent OT Cyber-Attacks

Cyber-attacks have expanded beyond the digital realm of IT into the physical world of OT and through second level breaches. Attacks on independent and distinct supply chains could affect OT systems. With new vulnerabilities and risks, stakes are escalating. Security and risk management leaders are forced to adopt a paradigm shift in their cybersecurity approach. The breach of a personal computer may cause data loss and private distress, but a cyber-attack on infrastructures can disrupt or destroy essential services, and ultimately affect lives.

APR 2022

SOPHISTICATED RUSSIAN CYBER-ATTACK

Ukraine thwarted this attack on its power grids that could have halted power to 2 million, raising fears in people.

AUG 2022

GREECE GAS OPERATOR ATTACK

There was a network intrusion. Data were accessed and leaked.

JUL 2023

PORT OF NAGOYA, JAPAN, ATTACK

Operations came to a halt due to a ransomware attack. It disrupted communication systems and prevented import and export operations.

AUG 2022

UK WATER SUPPLIER ATTACK

South Staffordshire Water, which has about 1.6 million customers, was targeted.

NOV 2022

DANISH TRAIN NETWORK ATTACK

Trains came to a standstill for several hours, due to a compromise in an IT subcontractor's software testing environment.

Sources:

Apr 2022 - The New York Times

Aug 2022 - CPO Magazine

Aug 2022 - Bleeping Computer® LLC


Nov 2022 - Reuters®

Jul 2023 - Dragos, Inc.



Key Factors Driving Towards a Coordinated OT / IT Security Strategy

Since 2020, there were 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. This is driven by many factors:

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

Source: CSA, Singapore Cyber Landscape 2020, Published in 2021

Challenges Faced by Organisations



Lack of Visibility



Inexperienced OT Personnel



Rapid Pace of Change



Network Complexity

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.

CYBERSECURITY CAPABILITIES



DEEP EXPERTISE



**BROAD EXPERIENCE
ACROSS ALL DOMAINS**



Our significant investments in research and development, coupled with our active engagements with leading research institutes, academic partners and industry leaders in capability development, enable us to create future-ready cybersecurity solutions and stay ahead of cyber-attacks.



Government



Info-communications



Media



Banking & Finance



Healthcare



Security & Emergency



Land Transport



Energy



Water



Aviation



Maritime

Critical Information Infrastructures (CII)

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 have to get it right every time, while threat actors only need to get it right once.

By providing our customers with the suitable cybersecurity architecture, future-ready solutions and best practices, we help them to maintain a vigilant and resilient digital space, securing their OT environment to ensure the proper and uninterrupted functioning of the digital economy.

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



DEEP EXPERTISE OT CYBERSECURITY SOLUTIONS

Beyond IT to OT | Empowering Solutions, Understanding your Goals



Established in 2011, ST Engineering has designed and built over 22 SOC's for national and government agencies and defense purposes.

We have expanded into OT cybersecurity and are now leaders in OT monitoring and deployment tools utilised by numerous local and international companies.

The Key is Our People

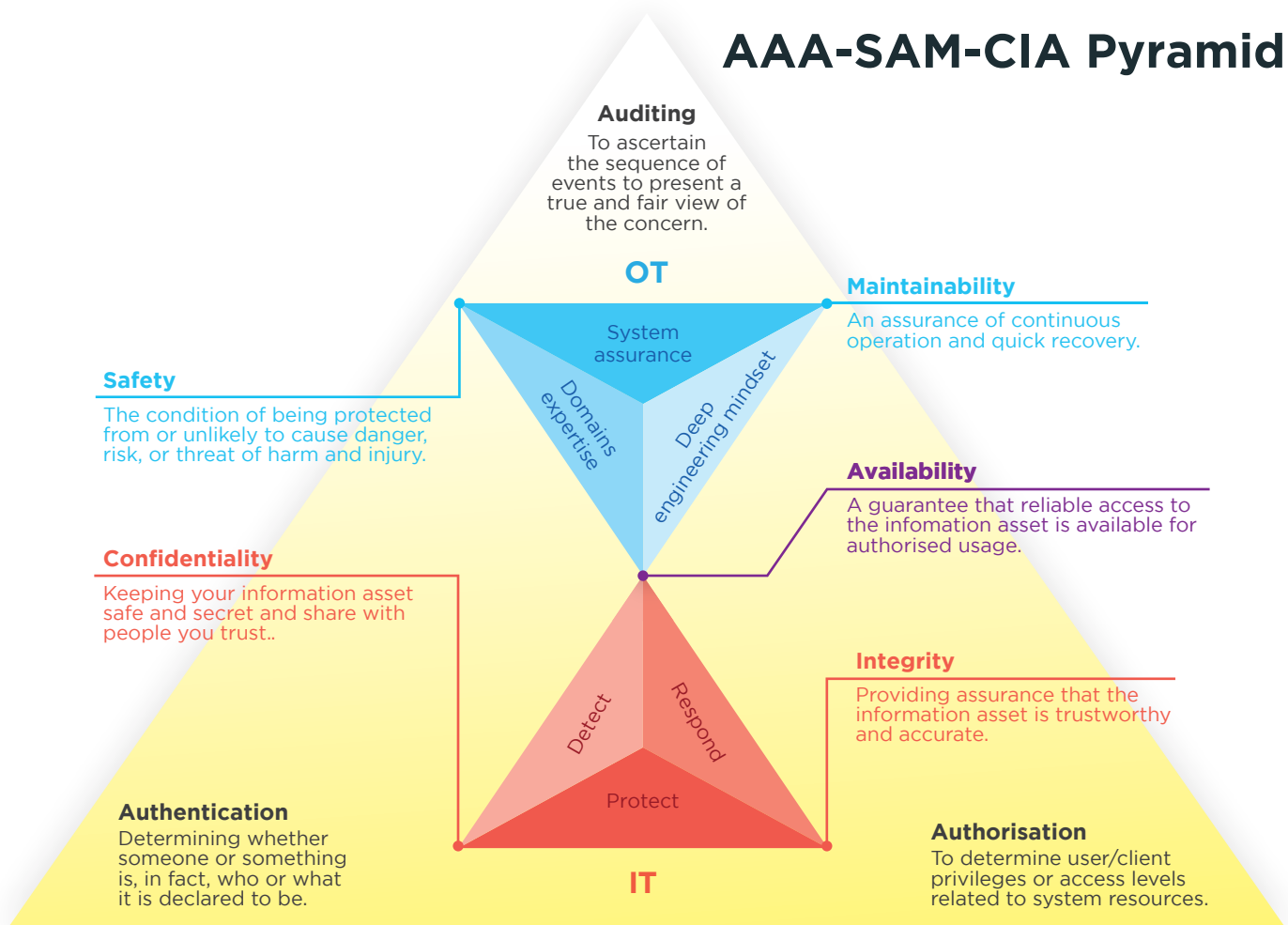
At the Heart of Our Success: Our People and a Holistic Approach to Pragmatic Solutions is key to Secure What Matters.

From consultation to implementation, we pride ourselves on our dedicated team. With decades of experience designing and building world-class SOC for esteemed local and international clients, our specialised cybersecurity professionals possess an unparalleled understanding of information security, cutting-edge technologies, and operational implementation. We are committed to developing and delivering secure critical infrastructures through this expertise, fortifying the cyber ecosystem globally.

AN INTEGRATED FRAMEWORK

To address the challenges, our approach to OT cybersecurity is engineering-oriented rather than solely IT-centric. Leveraging this multidisciplinary mindset and skillset, we adopt an integrated framework to encompass all the objectives of IT and OT networks:

AAA-SAM-CIA Pyramid



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.

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.

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

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

Application Servers

SCADA Servers

Historian Database Servers

OPC Servers

PLCs (Actuators, Engines, etc.)
Pumps

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

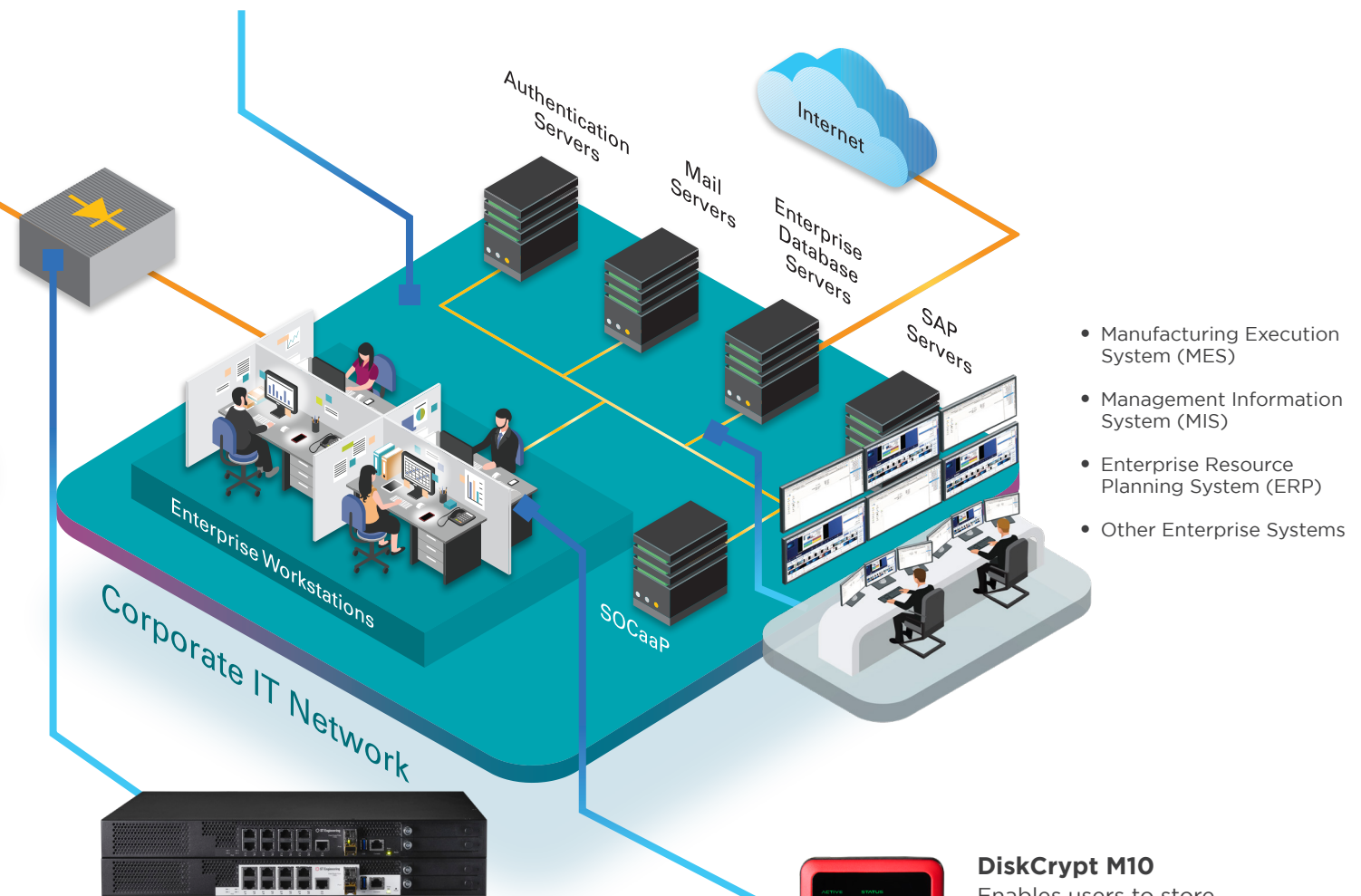
SigaGuard safeguards industrial assets by monitoring raw electrical signals (Level 0 real-time monitoring). By activating Machine Learning on rich and unfiltered electrical signals at Level 0, SigaGuard delivers an autonomous cyber inspection & analytics solution, offering bullet-proof detection of any 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 holistic cybersecurity solution for Production OT networks and Enterprise IT is designed for CII, which includes Building Management System, ensuring the cybersecurity of ICS and SCADA systems.

Embracing security by design, 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)

An advanced cybersecurity assessment to validate cybersecurity posture of an enterprise. Protect key digital assets by simulating realistic techniques of attack vectors used by malicious actors, identifying vulnerabilities in the computing and network environment, and then providing prioritised remediation guidance.



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

© 2023 ST Engineering Info-Security Pte. Ltd. All rights reserved.

DOP 0823



www.stengg.com/cybersecurity