OVERVIEW OF OT THREATS

Recent Attacks on OT

Cyber-attacks have expanded beyond the digital realm of IT into the physical world of OT. The stakes have escalated as it opens new vulnerabilities and risks that are pushing security and risk management leaders to adopt a paradigm shift in their cybersecurity approach. While the breach of a personal computer may cause data loss and private distress, the cyber-attack on infrastructures can disrupt or destroy essential services, and ultimately affect lives.

Oct 2016  
The Mirai botnet was used to attack internet infrastructure provider Dyn, causing many organisations across the internet to go offline. 
Source: CSO, March 2018

May 2017  
The WannaCry ransomware attacked the UK networks, before spreading to over 150 countries affecting industrial plants across Europe and Asia. 
Source: Security Intelligence, September 2017

Mar 2018  
The malware found in the US energy, nuclear, water and critical manufacturing networks are traced to Moscow. 
Source: The CyberX-Files Issue 10, May 2019

Mar 2019  
Ransomware attacked Norsk Hydro, one of the world’s largest aluminum producers, shutting down its worldwide network, and stopping or disrupting its plants. 
Source: Ars Technica, March 2019

Key Factors Driving Towards a Coordinated OT/IT Security Strategy

By 2021, 25% of asset-centric enterprises will adopt a hybrid model of traditional security controls and specialised OT security tools to secure OT environments, up from 10% in 2018. This forecast is driven by many factors:

1. New Risks Arising from OT/IT Convergence

2. Wider Range of Industries Impacted by OT/IT Convergence

3. Reduced Effectiveness of Air Gap Technique in Securing Merged Environments

4. Increasing Pressure on Regulatory Compliance

Source: Gartner OT Security Best Practices, September 2018

Challenges Faced by Organisations

- Lack of Visibility
- Lack of Personnel with overarching and in-depth knowledge on ICS/SCADA/Cybersecurity
- Rapid Pace of Change
- Network Complexity

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.

Operational Technology (OT)

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.

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

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.

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.

This is why we developed our 90%, 9% and 1% cybersecurity architecture. Technology is used to eliminate 90% of the known threats to reduce the noise threshold. Processes are then applied to counter another 9% of the sophisticated threats and malware. Finally, our deep expertise is utilised to eliminate the last 1% of sophisticated and unknown threats.

In providing our customers with the right 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 undisrupted functioning of the digital economy.

Critical Information Infrastructures (CII)

- Government
- Information & Communications
- Media
- Banking & Finance
- Healthcare
- Security & Emergency
- Land Transport
- Energy
- Water
- Aviation
- Maritime
Since 2011, the company has successfully designed, built and operated over 15 Security Operations Centres (SOC) in local and overseas for government agencies and commercial enterprises. Coupled with the broad experience and expertise in all domains, we are well positioned to provide a SOC with OT capability and not just from the IT perspective.

The key to successful delivering of our holistic and pragmatic solutions, from consulting to implementation on the ground, is our people.

With decades of proven skills in designing and building world-class SOC for local and international customers, our specialised cybersecurity professionals have the deep understanding of information security, technologies and operations implementation, to develop and deliver a secure critical infrastructure for the cyber eco-system.

To date, our ST Engineering Cybersecurity Academy has trained cybersecurity professionals in the IT and OT environment in more than 100 organisations.
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, Internet of Things (IoT) and OT networks:

**CIA-SAM-AAA Pyramids**

- **Confidentiality**: Keeping your information asset safe and secret and share with people you trust.
- **Authenticity**: Determining whether someone or something is, in fact, who or what it is declared to be.
- **Integrity**: Providing assurance that the information asset is trustworthy and accurate.
- **Availability**: A guarantee that reliable access to the information asset is available for authorised usage.
- **Maintainability**: An assurance of continuous operation and quick recovery.
- **Safety**: The condition of being protected from or unlikely to cause danger, risk, or threat of harm and injury.
- **Auditing**: To ascertain the sequence of events to present a true and fair view of the concern.
- **Authorisation**: To determine user/client privileges or access levels related to system resources.
- **Detection**: Develop and implement the appropriate activities to identify the occurrence of a cyber-attack.
- **Protection**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Response**: Develop and implement the appropriate activities to take action regarding a detected cyber-attack.
- **Recovery**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-attack.

**Aligned with US National Institute of Standards and Technology (NIST) Cybersecurity Framework**

Proven by global standards, our integrated framework is aligned with the NIST Cybersecurity Framework. The global cybersecurity guidance on how organisations can assess and improve their ability to prevent, detect and respond to cyber-attacks, covers 5 key areas:

- **Identify**: Develop the organisational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- **Detect**: Develop and implement the appropriate activities to identify the occurrence of a cyber-attack.
- **Protect**: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Respond**: Develop and implement the appropriate activities to take action regarding a detected cyber-attack.
- **Recover**: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber-attack.
OUR HOLISTIC SOLUTION FOR OT & IT NETWORKS

Radiflow iSEG Ruggedised 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.

Radiflow iSID Threat Detection System
(Augmented with Level 0 monitoring capability)
Monitors OT networks to provide situational awareness and 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 traffic and activities within the networks.

Radiflow iSAP Smart Probe
Sends all data traffic from remote sites to a central iSID Threat Detection System without overloading the network, by receiving all LAN traffic from the local switch (using port mirroring) via a secure tunnel.
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 Radiflow iSID, iSAP and iSEG, alongside proprietary products such as DigiSAFE Data Diode, Diskrypt and Black Computer.

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

DigiSAFE Data Diode
Enables secure data transfer across physically separated networks, preventing data leakage, enabling network segregation and eliminating cyber-threats by enforcing oneway data transfer.

DigiSAFE 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.

DigiSAFE Black Computer (Desktop Version)
Allows users to work securely in both trusted (Intranet) and untrusted (Internet) environments, through hardware-defined segregation that guards against cyber exploitation. If infected, it removes malware from any infected surface with a simple reboot.