ANNEX B

Trusted, Future-Ready Cyber Security Capabilities on Showcase at GovWare 2017

Cyber Innovations

Cyber Security Command and Control Centre (new)

Designed to monitor critical network and systems around the clock, the new Cyber Security Command and Control Centre is designed to detect abnormalities and flag potential attacks. It is equipped with cognitive capabilities driven by Threat Intelligence as well as Artificial Intelligence to enhance cyber threat detection, data analytics and capabilities to respond to threats across endpoints, networks and users with speed and accuracy.

Key features

- Leverages advanced data analytics and visualisation, as well as automation tools to deliver comprehensive situational awareness, enabling effective control on a cyber-threat situation through the applications of orchestration and predictive incident response tools.

- Equipped with deep learning and machine learning analytics to perform adaptive or active learning models such as User Entity Behavior Analytics, Network Threat Analytics, and Endpoint Threat Analytics. Enables clients to identify and protect against cyber incident overtime based on a collection of data or abnormal behaviours in real time.

- Capacity to detect early abnormalities, uncover and remove unknown and advanced threats for proactive defense - better resource planning, utilisation and assets management.

- Modular and scalable architecture; ability to be easily integrated into entire system architecture without impacting individual functions within the architecture.

Black Computer L100 (new)

The world's unique laptop version of Black Computer L100 is being introduced in Singapore for the first time, sparking a revolutionary change in the way critical infrastructures are being protected against cyber-attacks today. The Black Computer L100 is a powerful all-in-one security solution that provides comprehensive protection coverage for organisations.

A unique computer designed to provide robust security and convenience, it has two securely segregated workspaces, allowing users to work in both a trusted (Intranet) and untrusted (Internet) environment at the same time. Unlike standard protection which starts at the software platform, the Black Computer offers protection at the hardware level, with the ability to enforce network isolation to guard against any cyber exploitations. This dual system with built-in advanced malware protection technology eliminates the hassle of requiring two separate computers for different work needs, while offering enterprises an effective end-point protection.

Key features

- Performs Network Isolation – Dual operating system that allows users to surf both the internet and work on intranet sites securely through its hardware-defined segregation technology.

- Clean Operating System after every reboot - Reset-on-Boot feature that enables open system to get back to clean state.

- Security Layered Approach - Security embedded at Secure-BIOS level, with each layer guarding against a specific threat while enhancing its defence mechanism against different threats.

- Remote Management and Forensics - Manage and push down policies from the backend such as dynamic white listing of USBs and performing remote forensic from the command centre immediately upon detection of threats.

Single Box Data Diode (new)

The first made-in-Singapore data diode is a unidirectional communication and data transfer gateway that enables organisations to transfer data across physically separated networks. The new version is compact and cost effective, integrating seamlessly with backend systems. Equipped with enhanced security features, the new Data Diode prevents data leakage and eliminates cyber threats through one way data transfer. It complements ST Electronics' suite of cyber security solutions that enhances the security and resilience of Information Technology and Operation Technology infrastructures against targeted cyber-attacks.

Key Features

- Enhanced Network Security – Enables transfer of data from physically isolated networks securely

- Ease of Integration and Compact Design – A compact, cost-effective and user-friendly management portal which eases system configuration.

- High Performance – Configured to meet High Availability requirements, with a high throughput and assurance.

- Hardware Design – Silent design with heat-sink technology.

NetCrypt 1000

NetCrypt 1000 is a high performance Internet Protocol (IP) encryptor that enables users to leverage public Ethernet or IP infrastructure to connect to multiple sites in a secure manner. The Netcrypt 1000 offers a robust security feature such as Elliptic curve Diffie–Hellman (ECDH) of up to P521bits and implements a unique, additional layer of protection over the internet key exchange protocol to protect against denial-of-service attack.

In addition, it comes with a Path Redundancy feature for high availability reliability that allows the encryptor to connect to the next alternate available path should its primary link fails, thus ensuring operational continuity.

With the flexibility to use industry standard Simple Network Management Protocol (SNMP) network management system, NetCrypt 1000 allows local and remote monitoring of devices, as well as firmware field-upgrading to support the introduction of new features, algorithm updates and maintenance.

NetCrypt 1000 offers organisations a reliable and cost effective solution to counter the rising cost of operations and increasing cyber threats.

Key features

- High-assurance IP encryptor with Firewall capabilities
- 1Gbps aggregate throughput
- Internet Protocol Security (IPsec) standards-based encryption, authentication, digital certificates and key management
- Supports Advanced Encryption Standard (AES) algorithms for data confidentiality
- Supports 800 concurrent IPSec tunnels
- Easy deployment in existing network environment

EtherCrypt 10G

EtherCrypt 10G is a layer-2 link encryptor that protects sensitive data transmission over Ethernet and Metro-Ethernet networks. It offers full duplex confidentiality, integrity and replay protections using AES-256 Galois Counter Mode (GCM) encryption algorithm, and is suitable for point-to-point, point-to-multipoint and fully-meshed Ethernet networks.

It can be easily deployed into existing networks without any change to the network configuration, and also supports unicast, multicast and broadcast Ethernet frames. Designed with the strictest security standards, EtherCrypt 10G includes a tamper-resistant chassis, emergency erasure and active zeroisation of the encryption key. It also incorporates a Federal Information Processing Standard (FIPS) 140- 2 Level 3 certified platform module for secure key storage and cryptographic processing, a US government computer security standard used to approve cryptographic modules. In addition, it comes with in-built temperature detection to prevent the data centre from overheating.

Key features

- High-assurance encryptor
- 9Gbps throughput
- Supports AES-GCM (Galois/Counter Mode) algorithm for data confidentiality, integrity and anti-replay
- Redundant Power Supplies
- Over Temperature Detection
- Emergency Erasure Button

Cyber Security Trainer

The Cyber Security Trainer is a versatile simulation and evaluation platform that integrates live systems, virtualised platforms and modelled software virtual entities within a safe synthetic environment. The system can be used for individual or team training involving Red-Blue wargaming.

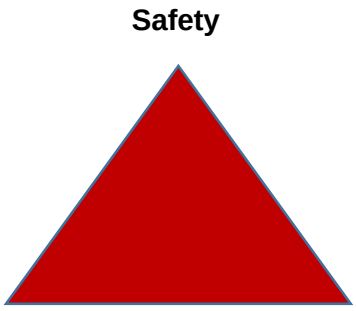
Key features

- Full spectrum capabilities encompassing Network Modelling (wired and wireless), Test & Evaluation and Operational Training
- Realistic training in a high fidelity and safe synthetic environment
- Networked capability offers team-based training experience
- All-In-The-Rack solution that allows for rapid start-up, ease of transportation and storage

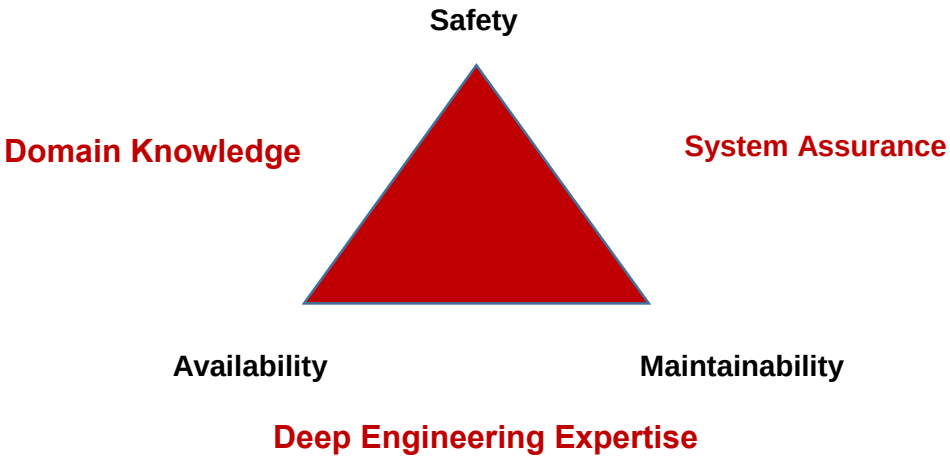
Cyber Security for Critical Information Infrastructures

Governments need to protect the vast array of essential infrastructures that operate over networks, including Water, Energy and Transport among the 11 sectors of Critical Information Infrastructure (CII).

Introducing SAM™ for Metro, Water or Power (New Cyber Security Model)



Industrial Control Systems that drive Critical Information Infrastructure (CII) require a high level of SAM (Safety, Availability and Maintainability) for their operations. The balance between these variables of Safety, Availability and Maintainability requires intricate understanding and expert handling. Any variable created from Cyber induced attacks that impacts on this fine balance will compromise the safety integrity of the System and its users, creating a domino effect that affects the normal operations of our critical information infrastructures such as water and power plants, as well as metro operations.



Leveraging ST Electronics' industry domain knowledge (such as land transport), deep engineering expertise and safety & system assurance capabilities, it is the trusted partner of choice for its full spectrum of next-generation solutions that secure critical infrastructures.

These solutions and technologies, which include the use of deep learning capabilities, equip governments with intelligent intrusion systems that help systems detect anomalies in almost real time, learning important patterns to prevent cyber-attacks, and ensure the continued operations of critical infrastructures.

Securing the weakest and most sophisticated links, ST Electronics' suite of cyber products such as encryption solutions, the Authentication Server, Black Computer and Data Diode can also be integrated into part of any enterprise or government's cyber security infrastructure, enhancing the cyber resilience of any Critical Information Infrastructure.