CompTIA®

Cybersecurity strategies in the manufacturing of medical devices – importance of systematic learning and skills definition

Global certifications are requirements for CSIRT operations, laying the foundation for incident response teams around network infrastructure and the cloud environment

sysmex

TARGET	Incident Response Teams (Sysmex-CSIRT) Outsourcing contractors (SOC Tier1)

Background of Efforts

Since its establishment in 1968, Sysmex has been providing customers around the world with the solutions that enable in vitro testing of blood and urine samples. In addition to the fields of hematology, immunochemistry and hemostasis, the company has expanded business to include the life science domain, and is now an integrated manufacturer, developing and manufacturing the instruments, reagents and software that are needed for in vitro diagnostics and providing sales and support service, supporting human health in more than 190 countries and regions around the world.

As a healthcare company, quality ICT infrastructure as well as security in products and services provided are extremely important. With the establishment of CSIRT, Sysmex strives to continuously protect important information from cyber threats, including customers' data and assets indispensable to the business.

Having CSIRT teams composed of employees and outsourcing contractors with different experience, it was challenging in how to improve incident handling performance and business maturity. The company first redefined operations in CSIRT and SOC, clarifying execution criteria and tier of each role. They defined SOC as a reactive function based on SLA. Utilization of globally recognized CompTIA certifications was convincing when anticipating to deal with overseas sales companies.

CompTIA CySA+ and CompTIA PenTest+ for Tier1 requirements:
Monitoring teams to mandate security analytics skills, and diagnostic teams to mandate penetration testing skills.

CompTIA CySA+ | CompTIA CySA+ evaluates the knowledge and skills required to understand threat detection tools and identify organizational vulnerabilities, threats and risks.
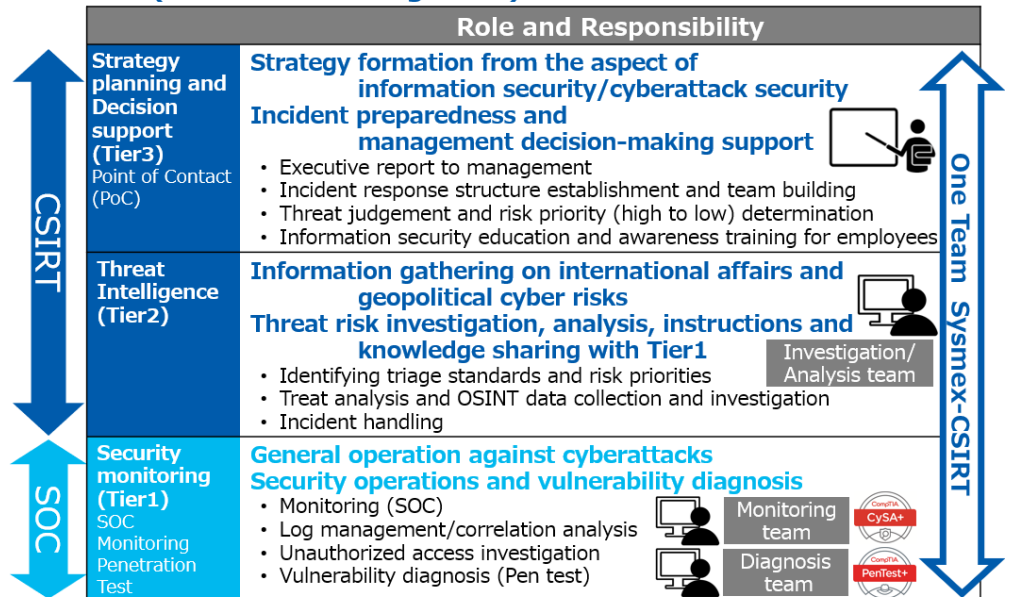
CompTIA PenTest+ | CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

ACTION

Skills definition and Teams training

CSIRT (Incident handling team) :Proactive function

Role and Responsibility		
Strategy planning and Decision support (Tier3) Point of Contact (PoC)	**Strategy formation from the aspect of information security/cyberattack security** **Incident preparedness and management decision-making support** • Executive report to management • Incident response structure establishment and team building • Threat judgement and risk priority (high to low) determination • Information security education and awareness training for employees	
Threat Intelligence (Tier2)	**Information gathering on international affairs and geopolitical cyber risks** **Threat risk investigation, analysis, instructions and knowledge sharing with Tier1** • Identifying triage standards and risk priorities • Treat analysis and OSINT data collection and investigation • Incident handling	Investigation/Analysis team
Security monitoring (Tier1) SOC Monitoring Penetration Test	**General operation against cyberattacks** **Security operations and vulnerability diagnosis** • Monitoring (SOC) • Log management/correlation analysis • Unauthorized access investigation • Vulnerability diagnosis (Pen test)	Monitoring team (CySA+) Diagnosis team (PenTest+)

SOC (Security monitoring team) :Reactive function based on SLA

Sysmex Corporation

1-5-1 Wakinohama-Kaigandori,
Chuo-ku, Kobe
www.sysmex.co.jp/en/

"Currently, we are focusing on redefining the service level of outsourced companies, acquiring specialized knowledge on cyber security, and master the skills and related technologies necessary for incident response operations.
We would like to improve the security level of the Group by acquiring the globally accepted CompTIA certification."

Sysmex-CSIRT
Mr. Shigekazu Tanimoto
(DX strategy Development)

Certification in USE
- CompTIA CySA+
- CompTIA PenTest+

Ver.1