Training System Updates

Cybersecurity

Access
Compliance
Data theft
Security
Fraud
Data integrity
Disruption of business activities

CAE offers Training System Updates to existing military customers to enhance training system capability and availability, and prolong the useful life of equipment. As a leading training expert, CAE collaborates with customers to determine the best plan of action for your needs and budget.

Overview

As more and more training devices of all types connect to networks, cybersecurity is becoming a growing concern. Increasingly resources must be deployed to fend off cyberattacks from agents looking to carry out industrial espionage for financial gain or to infiltrate military networks for strategic advantage.

Flight simulators are possible targets of such cyberattacks since they represent advanced technology containing detailed information on aircraft, engines, avionics and other aircraft systems as well as CAE's intellectual property, but also that of original equipment manufacturers (OEMs) of aircraft, engines and aircraft systems (avionics, radar, sonar, etc.). They may also represent potential points of entry into government networks.

Cybersecurity services

To protect against cyberattacks, CAE is currently working on two initiatives:

1. Define a new simulator architecture baseline, using Microsoft Windows 10, which is inherently more cybersecure than previous versions of Windows, and for which additional simulator-specific cybersecurity features are being created. This baseline will be available in 2020 for installation on new simulators.
2. Provide cybersecurity services on existing simulators and training centers which have not yet migrated to Microsoft Windows 10.

The services for existing simulators and training centers are provided in two phases:

Phase 1: *Site survey / architecture review and assessment.*

Phase 2: *Propose solutions to address the vulnerabilities found.*

These cybersecurity services conform to the five functions specified in the National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-171.

The specific tasks carried out as part of these services are also linked to the Center for Internet Security (CIS) Controls Version 7.1.

**Identify — Protect — Detect
Respond — Recover**

Your worldwide
training partner
of choice

CAE

Site survey

The site survey includes the following tasks:

Identify

Assess the integrated design, implementation and operation of security practices.

- Security architecture review
- Firewall configuration review
- Identify risks and vulnerabilities
- Propose solutions to improve site security

The result of the site survey is a report which explains the cybersecurity issues found and recommends solutions to mitigate the identified risks, better protect the simulators and maintain compliance with applicable cybersecurity standards.

Solutions

CAE's cybersecurity solutions carry out the remaining CIS functions:

Protect

Implement appropriate safeguards to ensure secure use of the simulator.

- Malware defences
- Boundary protection (e.g. next-generation firewalls)
- Security awareness and training
- Inventory (validation of all installed software / hardware)

Detect

Timely discovery of cybersecurity events.

- Logging and monitoring (e.g. account monitoring)
- External vulnerability scans
- Security validation

Respond and Recover

Timely recovery to normal operations.

- Incident response
- Single, consolidated view of cybersecurity incidents
- Centralized management of security controls and solutions

These cybersecurity solutions include provision of new hardware and services to continuously monitor a site, including regular updates of malware detection and anti-virus software, responses to cyberattacks and recovery procedures to minimize any impact on simulator training.

Program Example

As the prime contractor on the U.S. Air Force KC-135 Aircrew Training System program, CAE has performed numerous cybersecurity updates on KC-135 operational flight trainers and other KC-135 training devices. These cybersecurity updates were required so KC-135 training devices could operate on the U.S. Air Force Distributed Training Center Network (DTCN), which allows virtual distributed mission training for KC-135 aircrews, including pilots and boom operators. The U.S. Air Force Air Mobility Command considers the cybersecurity updates delivered by CAE for the KC-135 aircrew training devices to be the benchmark for addressing cybersecurity issues across all their aircrew training system contracts.

Talk to your CAE representative to determine the right approach for your needs and budget.

Canada
Tel: +1-613-247-0342
milsim@cae.com

Europe
Tel: +49-2402-106-0
info@cae-gmbh.de

India
Tel: +91-80-2625-6000
caeindiapvtltd@cae.com

United States
Tel: +1-813-885-7481
cae_usa@cae.com

Australia
Tel: +61-2-9748-4844
caeaus@cae.com.au

Middle East
Tel: +971-2-676-7676
milsim@cae.com

United Kingdom
Tel: +44 (0) 1444-247535
cae_plc@cae.co.uk

Asia
Tel: +65 6430 4390
milsim@cae.com

Corporate Headquarters
Tel: +1-514-341-6780
milsim@cae.com

milsim@cae.com
@CAE_Defence
CAE
cae.com

Your worldwide
training partner
of choice