Critical Infrastructure Defense Center (CIDC)

Cybersecurity Services Brochure

SIEMENS

Introduction

Today’s world is rapidly changing. Globalization and geopolitical tension along with the increasing digitalization of products, systems and solutions is changing the way business is conducted. Information Technology (IT) and Operations Technology (OT) is converging, and the security challenge is expanding. This reality is creating new opportunities, but also new challenges and increasing the risk of cyber threats the world progresses its digitalization.

According to Gartner Inc., ….by 2025, cyber attackers will have weaponized operational technology (OT) environments to successfully harm or kill humans.

Gartner also predicts, ….that the financial impact of cyber physical attacks resulting in fatal casualties will reach over $50 billion by 2023. Even without taking the value of human life into account, the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant. Gartner also predicts that most CEOs will be personally liable for such incidents.”

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.

Critical Infrastructure Defense Center (CIDC)

Critical infrastructure and strategic manufacturing organizations rely heavily on OT and increasingly on Digitalization. This dependency poses new cybersecurity challenges that Siemens can solve.

Siemens is uniquely positioned to leverage its deep domain knowledge and experience in Operations Technology (OT) security enabling technology agnostic best practices that have been refined for more than 10 years.

At CIDC, we have a team of world class cybersecurity researchers, coupled with the first dedicated **OT Security Operations Center (SOC) in Canada**. We aim to solve the OT cyber security challenge holistically by taking a lifecycle approach to security that starts from embedding security at the inception and taking it all the way to the delivery of any initiative or program.

The Siemens competency in OT cybersecurity is situated within the Siemens Critical Infrastructure Defense Center (CIDC) in New Brunswick, Canada. The CIDC is a first of its kind, focused on OT, offering Advisory, Managed Security, and Research & Development Services.

Our Services

We provide a wide range of cybersecurity services delivered through our Consulting Services, Professional Services, and Managed Security Services. Our services include the following:

1 Cybersecurity Assessment

Our advisory services include a variety of cybersecurity assessments to help organizations understand their cybersecurity programs relative to baselines and different frameworks

NIST CSF	Assessment and review of cybersecurity program and existing controls using the NIST Cybersecurity Framework
NIST SP800-53	Assessment and review of Enterprise/IT cybersecurity program and existing controls using the NIST Special Publications 800-53
NIST SP 800-82	Assessment and review of OT network and existing controls using the NIST Special Publications 800-82 for Industrial Control Systems
ISA/IEC 62443	Assessment and review of cybersecurity management system (CSMS) against the ISA/IEC 62443 cybersecurity standards
C2M2	Assessing the maturity of an organization's cybersecurity program using the cybersecurity capability maturity model from the United States Department of Energy (DoE)
AESCSF	Assessment and review of cybersecurity program and existing controls using the Australia Energy Sector Cybersecurity Framework
ISO/IEC	Assessment and implementation of an Information Security Management Systems (ISMS) based on ISO/IEC 27001

2 Vulnerability Assessment

We offer specialized OT vulnerability assessments, IT vulnerability assessments, and IT/OT combination vulnerability assessments through the following:

Network Vulnerability Assessment

Active or passive vulnerability assessment (including scanning services) of an OT network and infrastructure using a combination of best-in-class tools, techniques, and procedures on customer's site

Vulnerability Assessment as a Service

this includes:

- Scheduled Vulnerability Assessments (VA's)
- Reports, findings, and recommendations to mitigate security gaps and vulnerabilities and provide support to cybersecurity by interpreting scan results and recommend remediation plans
- VA summary reports of the testing and documentation of findings
- Specialized VA testing to include database and web application assessments, wireless technology testing and analysis as part of planned security assurance activities
- Ad-hoc or emergency VA scanning to support targeted incident investigation, escalation, and emergency response to security events

NERC CIP Vulnerability & Patch Notification

Vulnerability monitoring services using bulletin notification system to meet NERC CIP 007-6 R2.2 requirement through Siemens SVM or Villocify Solution

3 Program Management

Comprehensive integrated program management of security strategy and project, risk management, and security services planning guided by PM@Siemens methodology

4 Penetration Testing and Red Team Services

OT focused penetration testing exercises that is inclusive of penetration test exercises of Level 4 and 5 of the Purdue Enterprise Reference Architecture

5 Threat Analysis and Intelligence

- Detect, monitor, analyze, and mitigate targeted, highly organized, or sophisticated threats
- Perform consolidated and comprehensive information and intelligence analysis of threat data obtained from various sources to provide indication and warnings of impending attacks
- Provide reporting on technical network and host-based attack vectors, emerging cyber threats, new vulnerabilities, and current trends used by malicious actors

6

OT Security Operations Center

The cornerstone of our security services offering is our OT Security Operations Centre (SOC). The SOC is the first of its kind in North America that is purely dedicated to monitoring and protecting critical infrastructure services and strategic manufacturing

The SOC provides the much-needed visibility into detecting threats and vulnerabilities within the operational technology network

We provide automated 24 hours per day, 7 days per week, 365 days per year (“24x7”) network monitoring, security event triage, analysis, alerting, computer security incident response support, threat intelligence and reporting

Monitoring and Detection

Security Investigation

- Investigation and identification of anomalous events detected by security devices, or reported by external entities, system administrators, and general users
- Documentation of all event investigation activities, incoming request for information, or suspected incident reports as required to support the incident management process

Incident Response

- Provision of 24x7 incident response, remediation, and recovery support services
- Provision of support to perform technical analysis of potentially malicious services that have occurred or believed to have occurred through security event data from the SOC

Advanced Analytics

- Automated population and management of a database of observed OT and related IT assets in core OT environments
- Searchable asset database through customer facing dashboard, and periodic generation of reports for review

Global Customer References

Port of Antwerp, Belgium – Clear OT cybersecurity roadmap thanks to IEC 62443 Assessment

Customer profile

Port of Antwerp plays an important public role in Belgium by

Managing and maintaining the second largest port in Europe

Causing more than 1,500 direct and more than 140,000 indirect jobs

Realizing 4.8% of Belgian's Gross Domestic Product (GDP)

Customer objectives

- To have a clear overview of the cybersecurity maturity of its IT and OT environment

Siemens solution

IEC 62443 Assessment

Siemens mapped the OT systems of Port of Antwerp on the IEC 62443 standard to have a good understanding of the as-is situation

Afterwards, Siemens provided clear guidance on how to achieve a higher security level in the form of a very detailed and tangible roadmap

Customer value

Siemens provided Port of Antwerp a clear OT cybersecurity roadmap

A synergy was found between the knowledge/experience available within Port of Antwerp' internal IT/OT cybersecurity teams and Siemens' expertise in IEC 62443

"As CISO, I'm responsible for both IT and OT cybersecurity. Having a clear understanding of the challenges specific for OT is very important.

Siemens helped us by providing a clear analysis of the current situation, as well as defining a roadmap to mitigate the risks.

Yannick Herrebaut, CISO at Port of Antwerp

Süd-West Netz Wiesbaden

ISO 27001 / 27019 Assessment and Certification

- Advised for implementation of ISO 27001
- Conducted certification readiness and assisted with gaps remediation

VSB / VMB – Vallourec & Sumitomo Tubes (Steel Making)

Designed, deployed, and operated OT Security, Governance, Service Management

- IT and OT network and security controls for a large plant, designed and operated OT service desk

Stadtwerke Hockenheim

ISO 27001 / 27019 Assessment and Certification

- Advised for implementation of ISO 27001
- Conducted certification readiness and assisted with gaps remediation

VALE – second world's largest iron ore mining company

Created a company wide OT Security Program

- Assessment of IT & Network Security
- Identified and prioritized OT security controls
- Created internal standards, policies and procedures
- Designed and deployed controls in many plants

EnergieSüdwest Netz GmbH

ISO 27001 / 27019 Assessment and Certification

- Advised for implementation of ISO 27001
- Conducted certification readiness and assisted with gaps remediation

Grupo Energía Bogotá" (GEB) in Latin America

Cybersecurity consultancy services

- Develop program based on NERC CIP
- Audit of security measures, threats and risks analysis, definition of a cybersecurity policy and plans

A large utility in Europe

Secure substation Migration and Security Management Services

- 18 Substations – security design, hardening and Malware protection
- Logs and event management

Dubai Electricity and Water Authority (DEWA)

Design and implement threat OT detection/monitoring

- Designed and deployed IDS
- Integrated IDS with SIEM
- Developed use cases for IEC 61850 and IEC 104 communication

Contact Us

CIDC.ca@siemens.com

Fredericton, New Brunswick, CA

siemens.ca/cidc

Published by
Siemens Canada Limited
1577 North Service Road East
Oakville, ON L6H0H6
Canada