Cybersecurity for Indusrial Networks

Student Guide

Dr Diarmuid Ó Briain

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Table of Appreviations

A&E	Accident & Emergency
AAR	After Action Report
ABAC	Attribute-based Access Control
ACL	Access Control Lists
AGO	Attorney General's Office
AGS	An Garda Síochána
AI	Attribution Threat Intelligence
ALE	Annualised Loss Expectancy
ANSI	American National Standards Institute
APT	Advanced Persistent Threats
ARO	Annualised Rate of Occurrence
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
AWS	Amazon Web Services
BCMS	Business Continuity Management System
BCP	Business Continuity Plan
BIA	Business Impact Analysis
C2	Command and Control
C3WG	CNI Cyber Coordination Working Group
CCSC	Common Cyber Security Constraints
CI	Contextual Threat Intelligence
CIA	Confidentiality, Integrity, Availability
CIM	Computer-Integrated Manufacturing
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model Integration
CMU	Carnegie Mellon University
CND	Computer Network Defence
CNI	Critical National Infrastructure
COOP	Continuity Of OPerations
COTS	Commercial Off-The-Shelf
CPS	Cyber-physical systems
CSA	Cloud Security Alliance
CSC	Critical Security Controls
CSF	NIST Cyber Security Framework
CSIRT	Computer Security Incident Response Team
CSIRT-IE	CSIRT Ireland
CSMS	Cyber Security Management System
CVD	Coordinated Vulnerability Disclosure
CyCLONe	Cyber Crisis Liaison Organisation Network
DAFM	Department of Agriculture, Food and the Marine
DC	Data Confidentiality
DCS	Distributed Control Systems
DECC	Department of the Environment, Climate and Communications
DF	Defence Forces

DFA	Department of Foreign Affairs
DHCP	Dynamic Host Configuration Protocol
DHPLG	Department of Housing, Planning and Local Government
DiD	Defence-in-Depth
DIY	Do It Yourself
DJ	Department of Justice
DNS	Domain Name System
DoD	Department of Defence
DoS	Denial-of-Service
DRP	Disaster Recovery Plan
DSP	Digital Service Providers
EAP	Extensible Authentication Protocol
EDR	Endpoint Detection and Response
EF	Exposure Factor
ENISA	European Union Agency for Cybersecurity
ePO	ePolicy Orchestrator
ERP	Business Enterprise Resource Planning
EU	European Union
EU-CyCLONe	European Cyber Crises Liaison Organisation Network
EUC	Equipment Under Control
FIM:	File Integrity Monitoring
FR	Foundational Requirements
GIS	Government Information Services
Gov-CORE	Government Coordination and Response Network
GTF	Government Task Force
HA	High Availability
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
I/O	Input/Output
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control Systems
IAM	Identity Access Management
IAS	Industrial Automation Systems
ICS	Industrial Control Systems
ICT	Information and Communications Technology
ID	Identifier
IDMZ	Industrial Demilitarized Zone
IDS	Intrusion Detection Systems
IDS/IPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IG	Implementation Group
IOC	Indicators Of Compromise
IOC	Indicators of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention Systems
IPSec	Internet Protocol Security

IS	International Standards
ISA	International Society of Automation
ISACA	Information Systems Audit and Control Association
IT	Information Technology
IXP	Internet eXchange Points
JIT	Just In Time
KVM	Kernel Virtual Machine
LGD	Lead Government Department
MES	Manufacturing Execution Systems
MISP	Malware Information Sharing Platform
ML	Maturity Levels
MOM	Manufacturing Operations Management
MSSP	Managed Security Service Provider
MTDL	Maximum Tolerable Data Loss
MTPD	Maximum Tolerable Period of Disruption
NAI	National Authorities
NAT	Network Address Translation
NCEP	National Cyber Emergency Plan
NCSC	National Cyber Security Centre
NECG	National Emergency Coordination Group
NERC	North American Electric Reliability Corporation
NI	Northern Ireland
NID	Network Intrusion Detection
NIS	Network and Information Systems
NIS2	Network Information Systems 2
NIST	National Institute of Standards and Technology
NSAC	National Security Analysis Centre
NSC	National Security Committee
OEP	Office of Emergency Planning
OES	Operators of Essential Services
OI	Operational Threat Intelligence
OS	Operating System
OSINT	Open-Source INTelligence
OT	Operational Technology
OTSec	OT Security
OTX	Open Threat Exchange
OWASP	Open Web Application Security Project
PCS	Process Control Systems
PDF	Portable Document Format
PERA	Purdue Enterprise Reference Architecture
PID	Proportional-Integral-Derivative
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
PoLP	Principle of Least Privilege
RA	Resource Availability
RAID	Redundant Array of Independent Disks

RBAC	Role-Based Access Control
RDF	Restricted Data Flow
RE	Requirement Enhancements
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAFECode	Software Assurance Forum for Excellence in Code
SAICA	Safety, Availability, Integrity, Confidentiality, Accessibility
SBU	Sensitive But Unclassified
SCA	Security Configuration Assessment
SCADA	Supervisory Control and Data Acquisition
SDL	Security Development Lifecycle
SEM-NSF	Strategic Emergency Management: National Structures and Framework
SI	Strategic Threat Intelligence
SI	System Integrity
SIEM	Security Information and Event Management
SIR	Security Incident Response
SL	Security Level
SL-A	SL – Achieved
SL-C	SL – Capability
SL-T	SL – Target
SLA	Service Level Agreements
SLE	Single Loss Expectancy
SMB	Server Message Block
SME	Small and Medium-sized Enterprises
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centres
SOM	SOC Manager
SP	Special Publication
SR	System Requirements
TI	Tactical Threat Intelligence
TLD	Top Level Domain
TLP	Traffic Light Protocol
TR	Technical Reports
TRE	Timely Response to Events
TS	Technical Specifications
TTP	Tactics, Techniques, and Procedures
UC	User Control
UK	United Kingdom of Great Britain and Northern Ireland
UPS	Uninterruptible Power Supplies
USM	Unified Security Management
VFD	Variable Frequency Drives
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
XDR	Extended Detection and Response

Module Aim

Provide learners with the ability to combine Industrial Automation and Control System (IACS) systems and protocols with Cybersecurity frameworks and tools in order to prepare the model for incident response plans to counteract the cyber attacks.

Learning Outcomes

On successful completion of this module the learner should be able to:

- Visualise IACS as they are employed in manufacturing, distribution and critical infrastructure.
- Construct a business case for Security of an IACS.
- Consider Cyber Security Architectures applicable to the security of IACS.
- Categorise physical and digital access controls as they apply to the security of an IACS.
- Appraise risk management, risk assessment and the execution of risk management tasks in the context of IACS security.

Supplementary Book Resources

Pascal Ackerman 2017, Industrial Cybersecurity, Packt Publishing Ltd [ISBN: 9781788395984]

Eric D. Knapp,Joel Langill 2014, Industrial Network Security, Syngress Press [ISBN: 0124201148]

Edward J. M. Colbert,Alexander Kott 2018, Cyber-security of SCADA and Other Industrial Control Systems, 1 Ed., 16, Springer

[ISBN: 3319812033]

Pierre Kobes, *Guideline Industrial Security: IEC 62443 is Easy*. HEYER, 2017. [Online]. Available: https://books.google.ie/books?id=uQEjtAEACAAJ

Recommended Article/Paper Resources

US National Institute of Standards and Technology (NIST) 2022, Guide to Industrial Control Systems Security Revision 2, Special Publication, NIST SP 800-82.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

US National Institute of Standards and Technology (NIST) 2015, Guide to Operational Technology (OT) Security Revision 3, Initial Public Draft, NIST SP 800-82r3 ipd.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

US National Institute of Standards and Technology (NIST) 2020, Security and Privacy Controls for Information Systems and Organizations to OT', NIST SP 800-53 Rev. 5.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

Abstract

This course explores cybersecurity on Operational Technology (OT), it will cover some of the basic OT and fundamentals of OT security by putting OT into real-world context, both from an industry standpoint and everyday life. The course will begin by considering some of the recent history of OT, how they've evolved into the types of complex industrial environments that exist today, and some examples of how some of the devices that make up control systems actually work. This will be followed by a a deeper dive into those devices as well through examples, real-world context. This will be followed lead to some of the industry-standard frameworks and standards that are commonly used when we're applying controls to OT networks such as those from the US National Institute of Standards and Technology (NIST), the Purdue Enterprise Reference Architecture (PERA), International Society of Automation (ISA) 62443, SANS Cyber Kil lChain for Industrial Control Systems (ICS) and the MITRE ATT&CK framework. The module will progress to consider convergence and its importance within the OT space, convergence meaning IT, OT, and security coming together to protect, control and secure those systems. Finally the module will work through the steps to respond to a breach, what to do when a breach occurs on the OT network.

This page is intentionally blank