Cyber Ireland Operational Technology Security (OTSec) Special Interest Group (SIG)

Date: 22/3/2024
Version: 1.0

The Opportunity:

The importance of digitalisation for key sectors such as manufacturing, food and drink, healthcare, utilities, among others, has grown rapidly with the Industrial Internet of Things (IIoT) and Industry 4.0. This increasing connectedness of the operational technology (OT) environment, including to customers and suppliers, brings new, inherent cyber security risks for companies and their supply chain, in both IT and OT systems.

Key sectors of Ireland's economy depend on securing the OT environment. Ireland is an international leader with clusters of world class manufacturing operations in sectors such as biopharmaceuticals, electronics, medical device technology, and food production.

Ireland has also become a global hub for cyber security, many of the top cyber security MNCs have operations here, there's over 60 Irish cybersecurity companies exporting internationally, as well as a growing number of internal cyber security functions across diversified companies in technology, financial services, health and manufacturing.

The opportunity exists to connect the OT and cyber security communities to build expertise and international leadership in OT security.

Challenges:

From discussions with OT security professionals the most significant challenges identified are:

- Organisations not having a clear OT strategy;
- Managing the differences between IT / OT and integration;
- Skills and experience needed to manage OT through continuous change;
- Software vulnerability management with OT assets that may remain in service for 10+ years;
- Impact of regulations (e.g. NIS 2.0) on OT cyber security and implementation of standards such as IEC 62443
- Demonstrating the business case for OT Security & building an OT Security Culture across the organization.

OTSec SIG Goals:

Cyber Ireland's Operational Technology Cybersecurity (OTSec) Special Interest Group (SIG) provides a forum for industry end-users, integrators and vendors to share information, best practices and support capability building in operational technology security across organisations and sectors.

To discuss and address the practicalities, opportunities and challenges, the OTSec SIG, will:

- Provide a forum for industry and professionals in the OTSec space to discuss their needs and challenges, sharing information and best practices.

- Identify the OT cyber security training needs of companies and work with education and training providers to ensure industry skill demands are met.
- Engage with relevant standards and regulations to support implementation in the sector.
- Bring solutions from Irish-based companies to meet the challenges of OT cyber security professionals and organisations.

Committee:

The OTSec SIG will be led by a committee whose responsibility will be:

- Set the strategy, goals and activities of the SIG, in line with member needs.
- Engage with OT and cyber security professionals to build the OTSec SIG community
- Organise a schedule of regular events, online and in-person, for the OTSec SIG members to meet.

A chair and vice-chair should be appointed and responsible for leading the activities of the SIG as well and representing the SIG to the Cyber Ireland Cluster Advisory Board.

Members:

Membership of the OTSec SIG is open to OT and cyber security professionals. It is not a requirement to be a Cyber Ireland member (see membership list & membership application here).

The OTSec SIG aims to connect professionals from across industry, end-users, integrators and solution providers, Education, Training and Research Providers, government agencies and other networks and associations.

To become a member, an application the form must be completed, which will be reviewed by the OTSec Committee. OTSec SIG Application Form.

Meetings:

SIGs may set their own meeting schedules. It is encouraged that SIGs organise two online meetings and two in-person meetings per year. SIG events can be organised with other Cyber Ireland events such as the National Conference.

Meetings will be communicated to SIG members through Cyber Ireland by email.

Cyber Ireland Resources:

Cyber Ireland shall provide:

- a staff member to support the running of the SIG and organisation of activities and events.
- communications to members and manage the mailing list.
- a website for the OTSec SIG to promote it’s activities - https://cyberireland.ie/otsec/

- funding for activities and events, on receipt of an annual budget. Sponsorship of events and activities will managed through Cyber Ireland.
- Communications channels such as Slack, Signal, or others, if required.

Principles & Rules:

OTSec SIG exists to work in the interest of all members of the community. The SIG shall strive to ensure that all participants are treated equally and fairly.

Efforts shall be focused on the common interests of the OTSec SIG and not the interests of individual members or group of members.

The general spirit shall be one of co-operation. Differences and rivalries between private companies, public institutions or professional organisations that may impair the effectiveness of the SIG shall, when possible, be resolved by consensus.

OTSec SIG members must not, directly or indirectly, use, disclose, reproduce or make available in any form any confidential information considered sensitive under Competition Law[1] and/or subject to Confidentiality Requirements.

There is a strict "no sales" rule applied to within the OTSec SIG. Solution providers should not pitch their solutions, unless explicitly invited to do so. OTSec SIG members should not be individually contacted or messaged for sales.

A list of OTSec SIG members will be shared within the group including, name and organisation. Contact information such as email address will not be shared unless explicitly asked for permission.

As a general information sharing rule, Traffic Light Protocol (TLP)[2] should be applied in the official CISO Community discussions. TLP labels will be applied based on the sensitivity of discussions. Conversation facilitators should indicate to the Community Members which label is applied during the information exchange. The latest version of the TLP defines 4 sharing labels:

- TLP RED
- TLP AMBER (TLP AMBER+STRICT restricts sharing to within organisations only)
- TLP GREEN
- TLP CLEAR

All OTSec SIG members are responsible and accountable for ensuring that the Principles & Rules are respected and followed.

Any issues or concerns with fairness should be raised immediately with the OTSec SIG Chair and Cyber Ireland staff.

Should non-compliance with the principles, rules & confidential result in misconduct, Cyber Ireland will ensure that all such allegations or reports of any other irresponsible or unprofessional behaviour

[1] Information and/or data sensitive under Competition Law are for example: individual company prices, market shared, cost factors, business strategy, future plans, business plan, conditions of proposals to be submitted in order to participate to tenders on the market.

[2] Traffic Light Protocol (TLP) Definitions and Usage - https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

are acknowledged and receive an appropriate and proportional response. In the event of confirmed cases of misconduct, appropriate action will be taken, having been fairly and evenly considered with regard to all the stakes involved.