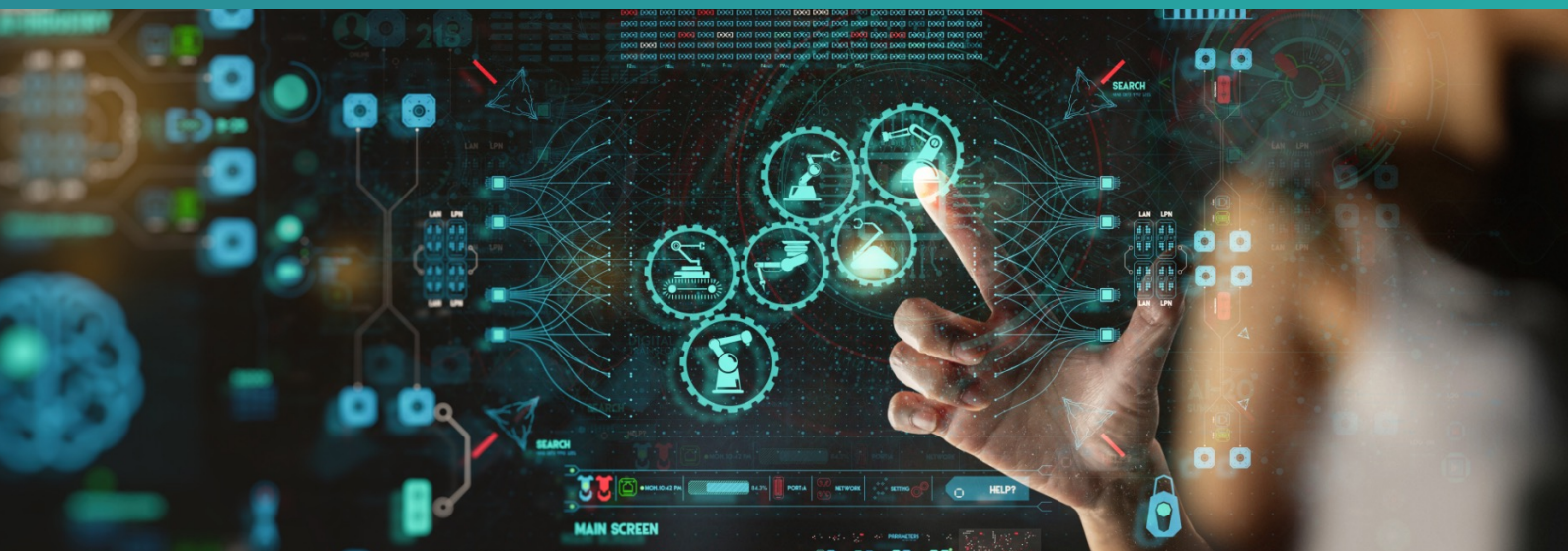
Market Sector:
CROSS SECTOR

Technology Theme:
INTELLIGENT FACTORY

DIGITAL ENGINEERING:
OPERATIONAL TECHNOLOGY CYBER SECURITY CAPABILITY



MTC CAPABILITY DEVELOPMENT IN CYBER SECURITY FOR OPERATIONAL TECHNOLOGY (OT)

The MTC has evaluated several technologies which highlight vulnerabilities or suspicious behaviour within operational technology (OT) environments, enabling the MTC to grow its Cyber Security offering within manufacturing.

> The project has given the team a large amount of insight into the capabilities of cyber security monitoring technologies. The attained knowledge and experience will soon be applied within customer projects.
>
> **Richard Rutte, Technical Specialist, Informatics Team, the MTC**

THE CHALLENGE

The lifespan of OT equipment is generally much longer compared to IT hardware, and software updates can be disruptive if at all possible. This often results in legacy equipment and unpatched software, leaving critical infrastructure open to attack.

The manufacturing industry must realise that unsecured operational environments can not only cause disruption and financial damage, but can also cause physical and environmental harm. Not to mention the reputational damage when trade secrets or sensitive data are stolen.

The MTC is looking to expand its OT Cyber Security capabilities, in partnership with a range of technology providers, retaining a vendor agnostic approach in order to support companies to become more secure in a financially viable way.

MTC'S SOLUTION

- The MTC is implementing a strategy roadmap to tackle the main challenges of Cyber Security within manufacturing.
- Leveraging valuable relationships, the MTC has acquired licences and equipment which provide network monitoring (including industrial wireless and radio frequency), specifically tailored to OT environments.
- The MTC's demonstration cells and testbeds are the perfect location for testing and analysing these technologies, with genuine OT network traffic and lower risks.

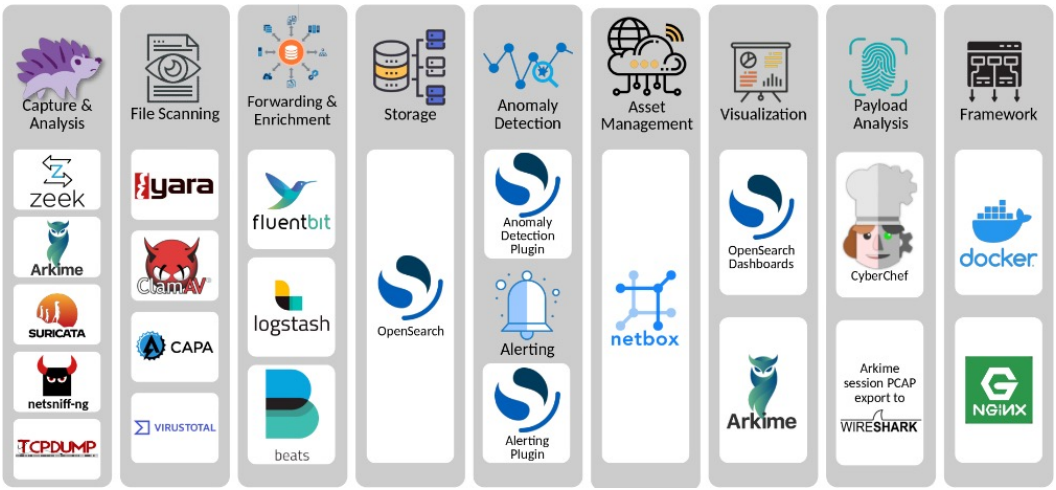
THE OUTCOME

- Increased knowledge of available OT cyber security technologies and understanding the scope of their capabilities.
- Improved technical knowledge of network monitoring architectures and how to effectively implement the necessary technologies.
- Enhanced relationships with technology providers by showcasing offerings within MTC.
- New partnerships with expert Cyber Security companies for further research and exploitation opportunities.
- Collaboration with technology providers to enhance their products and meet roadmap objectives.
- Improved view of our network vulnerabilities and current blind spots in airspace (RF) monitoring.

BENEFITS TO THE CLIENT

- Increased visibility of available technologies and their most suited applications for interested companies (e.g. SMEs, larger companies).
- Ability to evaluate the effectiveness of available monitoring technologies.
- Improved technical skillset for secure monitoring of OT assets and environments.
- Technical skillsets developed can be applied in future customer research projects.
- Capability built for setting up monitoring architectures within OT environments.
- Competence built around the configuration of network monitoring technologies.
- Understanding and identification of network vulnerabilities within OT environments.

> Cyber security in OT environments has long been avoided, instead using procedures and air gaps to protect them. With the use of networks to support data driven decisions, security must be embedded into manufacturing systems. However, this should not come at a cost to manufacturing agility and flexibility; so it is important to develop new methods to support OT development and deployment in a secure way.
>
> **Dr Stuart McLeod, Business Unit Lead, Informatics Team, the MTC**



dot™ CLAROTY Malcolm awen COLLECTIVE

solutionspt Industrial IT Solutions txOne networks LOCH TECHNOLOGIES

Manufacturing Technology Centre,
Pilot Way, Ansty Park,
Coventry, CV7 9JU

Tel: +44 (0) 2476 701 600
www.the-mtc.org

mtc Manufacturing Technology Centre