

## Security - Endpoint Protection

- Legacy OS support
  - Windows, Linux, Mac, Android, iOS, etc.
- AI driven engine
- Lightweight agent
- Best in class detection
- Application Whitening
- No Internet required
- Easy to manage, across a hardware estate
- Can be deployed on-prem inside the airgap
- Requires fewer updates to remain a proactive advantage over signatures... in reality this is vital
- Runs with other AV for true Defence in Depth
- Full Endpoint Detection and Response (with OPTICS)
- No reboot after installation, ideal for OT systems
- Often costs less than your traditional well known AV vendors



# CYBER SecureOT

2023

## Industrial Cyber Security Made Simple



21 June 2023



Leicester Marriott

Hosted by

**solutionspt**  
Industrial IT Solutions

**AVEVA**  
SELECT

UK & IRELAND

# Industrial Cyber Security Made Simple



Join us to explore how to keep your industrial operation secure from cyber threats in a world of evolving threats.

Get the right advice, best solutions and correct understanding of how a robust cyber security framework can keep your OT environment secure.

This one-day conference gives you an opportunity to learn how the world of cyber security is changing and how robust threat detection can simplify your security strategy.

We'll look at best in class solutions tailored specifically to the needs of the industrial enterprise to demonstrate a multi-layered defence approach to reduce risk and improve outcomes.

In addition to presentations from many of the leading names in OT cyber security, you'll get hands-on experience in our technical lab sessions.



# Reasons to attend

## We'll show how

- Our simple approach helps you identify the best cyber-strategy for your company & deliver your unique roadmap to cyber security peace of mind
- Our NCSC accredited training gives your team the practical knowledge & confidence to develop & manage your SecureOT
- Our experience of the regulatory & standards environment (such as OG86 and IEC62443) & NIST guidelines makes compliance simple & keeps insurance premiums down
- With help from SolutionsPT & our partners, Britvic has transformed its SecureOT

## You'll learn how

- Our Cyber Security Framework keeps you ahead of threats
- AI is changing the cyber-security world
- Cyber resilience requires data visibility
- Robust threat detection and risk management can help simplify your cyber security strategy
- A multi-layered defence in depth approach reduces risk & improves outcomes
- Business Continuity and Disaster Recovery plans are vital to your security posture



# A plenary session programme featuring many of the leading names in SecureOT

<p><b>Keynote: Implementing an industrial cyber security framework to keep you ahead of the ever-changing threat landscape</b></p> <p>A planned, strategized approach with a sound framework in place is key to mitigate modern industrial cyber security risks. Do you have the right governance in place and how can the latest NIST framework help you on your journey?</p>	<p>Lee Carter Industrial Cyber Security Product Manager, SolutionsPT</p>
<p><b>Keynote: An industrial cyber security journey, a customer experience</b></p> <p>Challenges faced, successes and a personal journey of discovery implementing a cyber security strategy.</p>	<p>TBA</p>
<p><b>Plan B comes first – Disaster resilience and recovery</b></p> <p>Disaster resilience and recovery is often the last stage of implementing a cyber security strategy, but the OT environment is different as availability of systems like PLC's and SCADA are key in any production environment. Find out why Plan B should be your first defence to make sure you can recover from incidents quickly.</p>	<p>Chris Whitehead Business Continuity Product Manager, SolutionsPT</p>
<p><b>Work smarter to detect threats and manage risks in your Industrial network</b></p> <p>Data driven analytics help create a baseline of how your OT network should behave. A secure system should automatically be identifying when it does not behave in an expected way and alert you to take action. Learn how to automate your threat detection to enable better protection of your network.</p>	<p>Claroty</p>
<p><b>Selecting the right end point protection (Anti Virus) for OT</b></p> <p>Discover how AI provides the right solution for end point protection in the OT environment. Be better prepared to handle cyber security incidents as they happen on the plant floor – enabling rapid response to minimise the risk of spreading to other parts of your network.</p>	<p>Blackberry</p>
<p><b>Seven steps to security – creating a modern security stack for industrial networks</b></p> <p>Threats in industrial networks are wide ranging – targeted threats from external and internal actors, collateral damage from actions between third parties, to mistakes by tired operators. Protecting your assets is the name of the game, but to do this effectively your security layers should be able to leverage the most important source of data – your asset database. This talk discusses seven key interlocked functions that deliver the best 'bang for your buck' in delivering comprehensive industrial security.</p>	<p>Dom Storey Principal Security Architect OT Tenable</p>



# A full programme of participatory technical sessions led by SecureOT experts

## PLC backup and version control

- 🔒 Octoplant might be a new name, but the technology is proven and robust. It offers an elegant and simple way to protect critical applications that are running on your PLC's and SCADA systems.
- 🔒 Version control becomes effortless with Octoplant, with a host of tools and features to track every change made by everybody, all the time. Octoplant ensures your applications are protected and available quickly should an incident occur, it can be recovered quickly, which will reduce costly downtime and helps to protect the bottom line

## Protecting your process control network

- 🔒 Tenable.ot Operational Technology is our solution for managing threats and vulnerabilities in your process control network.
- 🔒 Tenable.ot automates the discovery of assets, manages their security history, monitors their integrity and the threats against them.
- 🔒 Most importantly, Tenable.ot gives you deep context making your security monitoring decisions simpler and more reliable, helps you prioritise your cyber maintenance workstreams and minimises your cyber maintenance workloads.

## Hardening your AVEVA System

- 🔒 We all know that we have to secure our SCADA and Historian. In this session we will look at the best practises for securing your AVEVA SCADA and Historian system.
- 🔒 You will learn how to set up your firewall ports for web clients so that you can securely deploy web browsers to access plant level information.
- 🔒 We will also show you how to effectively use Historian tiering to securely move process data from your OT to IT environment

# A full programme of participatory technical sessions led by SecureOT experts

## Spend less time securing IT assets and get back to OT

- OT owners and administrators adopting Industry 4.0, IIoT, and other transformational initiatives rapidly increase the threat vector for Denial of Service, Man-in-the-middle and Trust and password exploitation vulnerabilities. Thin client architectures can dramatically reduce cost of ownership while enhancing security and availability of information and production visualization.
- Learn how ThinManager® secures your digital infrastructure by reducing the attack surface, centralizing access control, and simplifying lifecycle support.

## Cyber-Attack Recovery for ICS & OT- In 30 Seconds!

- With cyber-attack rate increasing exponentially, @Salvador Technologies sets a new standard in operational continuity and cyber-attack recovery: a complete recovery in 30 seconds for SCADA/HMI systems.
- The patented air-gap technology is designed to enhance resilience and minimize downtime in converged ICS & OT systems.
- @Salvador Technologies' offers Plug & Play on-prem solutions, through an entirely automated recovery process, enabling your operation a complete and instant recovery in a one-click action.
- Optimal for meeting RTO requirements and enterprise policy compliance

## Hiding in Plain Sight: The Threat Posed by USBs

- End users, contractors, & system integrators continue to plug USBs into the industrial network. It only takes 1 USB to infect your environment with a worm or virus.
- With the KUB Cleaner we're able to scan your USBs & guarantee they're safe to use, block unscanned USBs from connecting to your network, & eliminate the threat that USBs pose to your OT environment

# An expo of market-leading SecureOT products & partners

