

# Agenda

## Breakfast Club | OT-Security

08:15 - 09:10 Uhr	<b>Gemeinsames Frühstück und Austausch mit den anderen Teilnehmenden</b>
09:10 - 09:15 Uhr	<b>Begrüßung</b>
09:15 - 09:45 Uhr	<p><b>Einführung in das Thema OT-Security</b></p> <ul style="list-style-type: none"> <li>• Aktuelle Bedrohungslage bei produzierenden Unternehmen. Praxisbeispiele und wie man Bedrohungen hätte vermeiden können.</li> <li>• Ziele und Konsequenzen für alle Unternehmen aus den neuen EU-Gesetzen (NIS2).</li> <li>• Wie gut sind Unternehmen gegen Cyber Security Angriffe aufgestellt und wo steht Dein Unternehmen im Vergleich? Erfahrungen aus den letzten OT-Security Checks.</li> </ul>
09:45 - 10:00 Uhr	<p><b>Der OT-Security Check - Mit wenig Aufwand zu schnellen Ergebnissen.</b></p> <ul style="list-style-type: none"> <li>• Vorgehensmodell auf Basis des Standards IEC 62443 im Überblick.</li> <li>• Vorgehen und Ergebnisse am Beispiel eines konkreten Kundenprojektes.</li> </ul>
10:00 - 10:30 Uhr	<p><b>TXOne: Schutz der Produktion mit ganzheitlichen, OT-nativen Lösungen.</b></p> <ul style="list-style-type: none"> <li>• Herausforderung: Der Schutz von Assets in der Produktion.</li> <li>• Plug &amp; Play - mehr Sicherheit für Anlagen in wenigen Sekunden.</li> <li>• Schutz von Assets über den gesamten Lebenszyklus.</li> </ul>
10:30 - 11:00 Uhr	<b>Kommunikations- und Biopause</b>
11:00 - 11:45 Uhr	<p><b>Fortinet: Strategie- und Lösungsportfolio für OT/ IT-Infrastrukturen</b></p> <ul style="list-style-type: none"> <li>• Cyber-Gefahren in OT-Infrastrukturen.</li> <li>• Use Cases für Netzwerksegmentierung, Visibilität und Fernwartung.</li> <li>• OT-Hack am Beispiel einer Modbus-Umgebung.</li> </ul>
11:45 - 12:15 Uhr	<p><b>Schreckensszenario Cyberangriff. Vorbereiten auf den Ernstfall mit Business Continuity Management.</b></p> <p>Von der Erkennung über das Notfallkonzept bis zum Wiederanlauf.</p> <ul style="list-style-type: none"> <li>• Detektion, Alarmierung und Eskalation beim Cybervorfall.</li> <li>• Notfallbewältigung und Auswirkungen in der OT.</li> <li>• Disaster Recovery und Notbetrieb.</li> </ul>
12:15 - 12:45 Uhr	<p><b>Sicherer Betrieb von OT-Infrastrukturen. Wer kann das alles noch leisten?</b></p> <ul style="list-style-type: none"> <li>• Lösungsansätze für den sicheren Betrieb von OT/IT-Infrastrukturen (24x7).</li> <li>• pco Security Operation Center (SOC) und pco Incident Response Team (IRT).</li> <li>• Kundenreferenz.</li> </ul>
12:45 - 13:00 Uhr	<b>Fragen, Antworten und Abschluss</b>