29–30 september 2026
K-märkt Science Tower Kista
insightevents.se/scada

InsightEvents sweden

SCADA & OT-SÄKERHET 2026

Ökad hotbild – det senaste inom OT- och cybersäkerhet

- Framtidssäkra din SCADA & OT-miljö: **Kunskap, nätverk och innovation**
- Deep Dive: **NIS2 & Cyber Resilience Act (CRA)** - dess stora påverkan på SCADA/OT
- För att möta verkligheten med **AI-drivna angrepp** måste försvarsstrategier utvecklas i en högre takt än hoten själva
- **Hybrida hot mot Sverige** - konkreta exempel på hur hybrida hot kan identifieras och mötas
- Vad vi faktiskt ser i OT-nät – **ett år av detektioner och insikter!**
- Hur styrsystemen anpassas – från "blanka lösenord", till att implementera moderna metoder som **Trust on First Use (TOFU) eller krypterad kommunikation**
- **Människa mot maskin:** Den farliga trenden att låta programvara fatta autonoma beslut utan att operatören har full insyn eller möjlighet att ingripa snabbt

Bland talarna:

Tomas Wallin
Försvarsmakten

Andreas Synning
IT-Centrum

Mette Svensson
Cybercampus Sverige KTH

Karl Castor
Swedavia

Mattias Nilsson
Beckhoff Automation

Moderator:

John Lindström
Luleå tekniska universitet

Övriga talare:
Anders Jonsson, AH CyberSec and European Union Agency for Cybersecurity (ENISA)
Christopher Stein, Maritime Cyber Guild
Daniel Rosenring, Grundfos
Hanne M. Hansen, Bureau Veritas
Jacob Henricson, Nørdsnipe & Cybercampus Sverige KTH
Joakim Elgh, Sectra Critical Infrastructure
Jörgen Holmlund, Försvarshögskolan
Mikael Holmgren, Advenica
Ulf Rönndahl, Veralex AB
Talare från CERT-SE

Silversponsorer:

advenica
Swedish cybersecurity at your service

BUREAU VERITAS
Shaping a World of Trust

SECTRA
Knowledge and passion

Samarbetspartners:

LULEÅ TEKNISKA UNIVERSITET

CYBERCAMPUS SVERIGE

Kista Science City

PROGRAM DAG 1 • 29 SEPTEMBER 2026

08:30 Registrering och morgonkaffe

09:00 Moderatorn inleder konferensen

John Lindström, *professor cybersäkerhet, verksamhetsledare Centrum för säkerhet i samhälle och kritiska infrastrukturer,* ***Luleå tekniska universitet***

09:10 Cyber Resilience Act (CRA) och dess stora påverkan på SCADA/OT

- Från statiskt till dynamiskt: OT-system går från att vara isolerade och stabila till att bli miljöer som kräver kontinuerliga uppdateringar
- Nya tekniska krav: Ökat fokus på regelbunden patchning, aktiv sårbarhetshantering och krav på transparens, exempelvis genom SBOM
- Kritisk leverantörskedja: Organisationer måste kunna ställa krav, följa upp och validera att leverantörer uppfyller CRA, vilket förändrar både upphandling och förvaltning
- Sektorsspecifika utmaningar: Järnväg och kollektivtrafik är tydliga exempel på sektorer där CRA får stor påverkan
- Strategisk drivkraft: Den viktigaste slutsatsen är att CRA fungerar som en motor för att skapa mer robusta, transparenta och framtidssäkra OT-miljöer, snarare än att bara vara ett passivt regelverk

Anders Jonsson, *Senior Advisor Cyber Security, NIS2, CER & CRA Expert, AH CyberSec & Member Enisa AHWG EUCS Cloud Services,* ***European Union Agency for Cybersecurity (ENISA)***

10:00 NIS2 & CRA Implementation in OT Environments: From Compliance to Operational Security

- Decode NIS2 and CRA requirements specific to OT/ICS environments
- Map regulatory obligations to existing OT architectures
- Implement compliance without operational disruption
- Build sustainable security governance frameworks
- Prepare for audits and third-party assessments

Hanne M. Hansen, *Head of OT Security,* ***Bureau Veritas***

10:20 Förmiddagskaffe, nätverkande och LiveHacking

11:00 Hur kan vi stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter?

- Agera vid inträffade it-säkerhetsincidenter genom att sprida information och stötta verksamheter i arbetet med att avhjälpa eller lindra effekter av det inträffade
- Samordna insatser vid större it-säkerhetsincidenter
- Samverka med myndigheterna inom det nationella Cybersäkerscentret (NCSC-SE)
- Vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt att utveckla samarbetet och informationsutbytet med dessa

Talare från CERT-SE - Sveriges nationella Computer Emergency Response Team

11:40 Förenklad regulatorisk efterlevnad med hjälp av datadioder

- Så säkerställer Advenicas datadioder dataöverföring genom ett enkelriktat flöde mellan två nätverk, för att skydda den känsliga infrastrukturen för olika produktionsmiljöer
- Genom kundscenarier visar vi hur organisationer på ett enkelt sätt kan möta ökande regulatoriska krav, inklusive NIS2-direktivet och standarder som IEC 62443 och samtidigt skydda sig mot avsiktliga så väl som oavsiktliga incidenter

Mikael Holmgren, *Executive Sales Representative,* ***Advenica***

12:00 Lunch och nätverkande

13:10 Vad vi faktiskt ser i OT-nät – ett år av detektioner och insikter

Joakim Elgh, *Detection Engineer,* ***Sectra Critical Infrastructure och representant från energiföretag***

13:30 How computers kill people: Computer based systems dependencies in safety critical industries and how 346 people died partly because of poor software engineering and design

- System Dependencies: How modern industries (aviation, maritime, energy) build in a total reliance on software, meaning a minor bug can lead to physical, fatal consequences
- MCAS (Maneuvering Characteristics Augmentation System): How the software system was prioritized over pilot control, and how a lack of redundancy became the direct cause of a fatal accident
- Human vs. Machine: The dangerous trend of allowing software to make autonomous decisions without the operator having full visibility or the ability to intervene quickly
- Lessons for the Maritime Industry: The transition to autonomous systems and increased digitalization means the industry must learn from aviation's mistakes to avoid "cyber-physical" accidents at sea

Christopher Stein, *Expert in Maritime Cybersecurity,* ***Maritime Cyber Guild***
Maritime Cyber Guild is a non-profit organization dedicated to advancing cybersecurity within the maritime industry.

14:20 Eftermiddagskaffe, nätverkande och LiveHacking

15:00 HETA STOLEN: INTERVJU

Vad är status för säkerheten i Sverige i en osäker omvärld? – intervju med Jörgen Holmlund, Försvarshögskolan

Uppdatera dig kring det senaste om säkerhetsläget med **Jörgen Holmlund,** årets Trygghetsambassadör och tidigare polisöverintendent samt en av Sveriges mest erfarna säkerhetsexperter. Med en gedigen bakgrund inom Polisen och omfattande erfarenhet av säkerhetsarbete, inklusive tjänstgöring inom Försvarsmakten både nationellt och internationellt, har han etablerat sig som en ledande auktoritet inom området. Dessutom var han en nyckelperson i arbetsgruppen som utvecklade FN:s handbok i militär underrättelsetjänst. Under denna intervju får du en aktuell överblick av hur Jörgen ser på statusen för säkerheten i Sverige och den allt mer osäkra omvärld som vi alla lever i.

Jörgen Holmlund, *lärare i underrättelsetjänst,* ***Försvarshögskolan***

PROGRAM DAG 1 • 29 SEPTEMBER 2026

15:30 Att navigera i ett osäkert hotlandskap: AI:s intåg och den nya verkligheten vi måste anpassa oss till i omvärldsläget

• Växande gap mellan anfallare och försvarare: Avståndet mellan de som attackerar och de som försvarar ökar ständigt, drivet av teknisk komplexitet och ett alltmer osäkert omvärldsläge

• Intåget av AI har accelererat takten och sofistikeringsgraden i cyberattacker, vilket gör det svårare att identifiera verkliga hot i ett konstant brus av larm

• För att möta verkligheten med AI-drivna angrepp måste försvarsstrategier utvecklas i en högre takt än hoten själva

• Från reaktion till proaktivitet: Slutsatsen är att organisationer behöver ställa om för att kunna filtrera bort bruset och fokusera på de mest kritiska och faktiska hoten i en föränderlig värld

• Omvärlden är i en ruskigt snabb förändring och presentationen kommer uppdateras med allt det senaste som händer inom området

Jacob Henricson, *VD, Nørdsnipe och rådgivare,* ***Cybercampus Sverige KTH***

16:10 Alla pratar om cybersäkerhet – men hur når vi dit?

Trots avancerad teknik beror över 90 % av alla cyberattacker på mänskligt beteende. Hur ser det ut för svenska företag och organisationer i Sverige?

• Etablera en hållbar cybersäkerhetskultur på jobbet:

1. Skapa rätt förutsättningar: Arbetsgivare behöver lära sig att skapa strukturer och riktlinjer

2. Skaffa rätt kompetens: Kompetensutveckling av personal förbättrar användarbeteende i organisationen

• En guide för hur arbetsgivare går tillväga för att kompetensutveckla sin personal

Mette Svensson, *Project Manager,* ***Cybercampus Sverige KTH***

16:50 Moderatorn avrundar konferensens första dag

17:00 -18:00 Nätverksmingel

18:20 GEMENSAM KONFERENSMIDDAG

Fortsätt dialogen med konferensdeltagarna och knyt nya kontakter samtidigt som du njuter av god mat och dryck.

OBS! Anmälan krävs och vi reserverar oss för att middagen kan bli fullbokad.

PROGRAM DAG 2 • 30 SEPTEMBER 2026

08:30 Morgonkaffe och nätverkande

09:00 Moderatorn inleder den andra konferensendagen

John Lindström, *professor cybersäkerhet, verksamhetsledare Centrum för säkerhet i samhälle och kritiska infrastrukturer,* ***Luleå tekniska universitet***

09:10 Vad kan vi lära oss av cyberattacken mot Svenska kyrkan?

• Mina erfarenheter som ledare under cyberattacken mot Svenska kyrkan

• Hur vi hanterade krisen, kommunicerade och nystartade verksamheten

• Vad jag lärde mig om ledarskap, kultur och samarbete när allt sattes på prov

Andreas Synning, *IT-chef,* ***IT-Centrum***

09:50 Nytt cyberförsvarsförband försvarar civil infrastruktur

Huvudsyftet med cyberförsvarsförbandet är att försvara kritisk civil infrastruktur som Försvarsmakten är beroende av för att lösa sin huvuduppgift; försvaret av Sverige och våra allierade. Under presentationen kommer överstelöjtnant Tomas Wallin, chef för 4:e cyberförsvarsförbandet att berätta mer om satsningen på denna kritiska verksamhet för vår framtid.

Vad innebär satsningen:

• Nytt förband: Försvarsmakten har inrättat ett fjärde cyberförsvarsförband

• Huvuduppdrag: Att försvara kritisk infrastruktur som myndigheten själv inte äger eller styr över

• Prioriterade sektorer: Verksamheten fokuserar inledningsvis på finans, energi och telekommunikation

• Placering: Förbandet är baserat i Mälardalsområdet

• Personal: Består huvudsakligen av civila cybersäkerhetsspecialister och officerare

Tomas Wallin, *chef för fjärde cyberförsvarsförbandet som är inriktade på cyberförsvar av kritisk infrastruktur,* ***Försvarsmakten***

10:30 Förmiddagskaffe och nätverkande

11:10 Från blanka lösenord till inbyggd säkerhet: Resan mot "Secure by Default"

• Regelverk möter verklighet: Vi reder ut kraven i CRA, NIS2 och Maskinförordningen. Vi förklarar varför "NIS2-certifierade produkter" är en myt, och hur vi istället möter kraven genom funktionell efterlevnad och inbyggda skydd i styrsystemet

• Att patcha en anläggning som körs (IT vs. OT): I IT-världen styr dataskydd (CIA) och automatisk patchning. I OT är tillgängligheten allt (AIC) och en omstart kan kosta miljoner. Vi tittar på hanteringen av uppdatering beroende på system

• Evolutionen mot "Secure by Default": Praktiska exempel på hur styrsystemen anpassas. Från att tvätta bort arvet av "blanka lösenord", till att implementera moderna metoder som Trust on First Use (TOFU) eller krypterad kommunikation

Mattias Nilsson, *Product Specialist Security, Application Support Building Automation,* ***Beckhoff Automation***

12:00 Lunch och nätverkande

13:10 Vi tar pulsen på SCADA & OT-säkerhet – liveundersökning!

13:30 How we Manage day-to-day Security Challenges across a complex technical environment

Daniel Rosenring, *Senior Specialist, Safety & Cyber Security Embedded SW,* ***Grundfos***

PROGRAM DAG 2 • 30 SEPTEMBER 2026

14:20 Extended Purdue Model to meet new requirements in Industry4.0 settings

- Benefits and limitations of the current Purdue Model in Industry4.0 settings, which is used to model the set ups of process and manufacturing industries as well as critical infrastructures
- Extension of the Purdue model with IT/OT/ET environments to achieve a cleaner security architecture with improved performance regarding production/distribution processes. ET is Enterprise Technology which comprises assets such as equipment/machines, systems and solutions that should not be in the IT nor OT environments
- Managing communications for ET assets based on a method to evaluate the need and suitability to be connected to internal and/or external networks or not at all

John Lindström, *professor cybersäkerhet, verksamhetsledare Centrum för säkerhet i samhälle och kritiska infrastrukturer,* ***Luleå tekniska universitet***

15:00 Eftermiddagskaffe och nätverkande

15:30 Cyberresiliens i kritisk infrastruktur: Hur Swedavia arbetar för att säkerställa att flygplatsverksamheten kan fortsätta även under pågående cyberattacker eller tekniska störningar

Karl Castor, *Head of Cyber Security,* ***Swedavia***

16:10 Säkerhet i den fjärde industrirevolutionen – ett turbulent och osäkert affärslandskap

- Skall vi ha regelbaserade eller riskbaserade processer i ett turbulent affärslandskap?
- Att se cybersäkerhet som skydd av intäktströmmar istället för skydd av tekniken
- Cybersäkerhet som en del av kontinuitet, reselience och motståndskraft
- Cybersäkerhet - en viktig funktion som måste vara med i organisationens strategiplanering

Ulf Rönndahl, *grundare & VD,* ***Veralex AB***

16:50 Moderatorn avslutar konferensen

SILVERSPONSORER

advenica
Swedish cybersecurity at your service

Advenicas expertis hjälper länder, myndigheter, företag och organisationer att skydda den allra viktigaste digitala informationen. Våra välbeprövade och betrodda cybersäkerhetslösningar isolerar nätverk fysiskt och kopplar samtidigt samman data på ett säkert sätt. Sedan starten 1993 designar, utvecklar och tillverkar vi alla krypto- och segmenteringsprodukter i Sverige för att garantera hög assurans. Läs om vår unika teknologi och dess EU- och nationella godkännanden på högsta säkerhetsnivå på www.advenica.com

BUREAU VERITAS
Shaping a World of Trust

Bureau Veritas är en global ledare inom testning och certifiering och erbjuder cybersäkerhetstjänster som ISO 27001/IEC 62443 certifiering, PEN testning, riskbedömningar, efterlevnadsrevisioner, utbildning och incidenthantering. Våra experter identifierar säkerhetsluckor och vidtar proaktiva åtgärder för att öka din organisations cyberresiliens.

SECTRA
Knowledge and passion

Sectra Communications är en expert och ledande leverantör inom cybersäkerhet och arbetar för ett tryggare och stabilare samhälle. Företaget utvecklar produkter och tjänster som skyddar delar av samhällets mest känsliga information och kommunikation. Erbjudandet omfattar säker röst- och datakommunikation med lösningar som är certifierade såväl nationellt som av EU och NATO, samt säkerhetsanalys och övervakning av kritiska IT/OT-system för exempelvis el- och vattendistribution. Företaget grundades 1978 och har sitt huvudkontor i Linköping. Sectra utvecklar även IT-system som hjälper sjukhus världen över att effektivisera vården. I dag har Sectra direktförsäljning i 19 länder och säljer genom samarbete med partners över hela världen.

Bli partner till SCADA-säkerhet 2026 – möt rätt beslutsfattare inom OT & cybersäkerhet

SCADA-säkerhet är en av Sveriges ledande mötesplatser för experter och beslutsfattare inom OT-, ICS- och cybersäkerhet. Här samlas aktörer från kritisk infrastruktur, industri, energi, transport och samhällsviktig verksamhet för att diskutera de mest aktuella säkerhetsutmaningarna – och lösningarna.

Som partner får du en unik möjlighet att positionera ditt företag i centrum av en bransch där efterfrågan på säkerhetslösningar växer snabbt. För ytterligare information och kostnadsförslag – välkommen att kontakta:

Roland Behrendt
+46 (0)8 587 662 77
roland.behrendt@insightevents.se

Samarbetspartners:

LULEÅ TEKNISKA UNIVERSITET

CYBERCAMPUS SVERIGE

Kista Science City

Framtidssäkra din SCADA & OT-miljö: Kunskap, nätverk och innovation

Hotet mot våra industriella styrsystem ökar i takt med att vi drar nytta av digitaliseringens möjligheter. Men med rätt strategier kan vi vända utmaning till styrka. Genom att modernisera autentisering och säkra nätverksstrukturer bygger vi en stabil grund för framtidens industri.

Vi kommer under konferensen också göra en ”Deep Dive” inom NIS2 & Cyber Resilience Act (CRA) och dess stora påverkan på SCADA & OT-Systemen. Vi reder ut vad det innebär för din vardag. Andra aktuella teman som kommer att tas upp under dagarna är Supply Chain Security och AI-Säkerhet.

På konferensen SCADA & OT-säkerhet får du koll på vad som händer inom området och du får utmärkta möjligheter att utbyta erfarenheter och nätverka med branschkollegor och experter från hela landet.

- Mötesplats för universitet, institut, myndigheter och företag för att dela idéer, knyta nya kontakter och accelerera innovation
- 2 fullspäckade dagar med know-how och best practice från hela branschen
- Välrenommerade talare och praktikfall som valts ut utifrån dagens och framtidens behov inom SCADA & OT-Säkerhet
- Träffa gamla och nya kontakter för att diskutera både utmaningar och lösningar i SCADA & OT-säkerhetsarbetet
- Fortsätt nätverkandet på kvällen den 29:e september när vi träffas för nätverksmingel och en gemensam konferensmiddag

Stefan Broman
Team Leader & Senior Projektledare
Insight Events Sweden

Priser

PRISLISTA	**Boka t.o.m 19/6**	**Boka t.o.m 4/9**	**Boka fr.o.m 5/9**
Konferens	10 990 kr	12 590 kr	13 190 kr
Middag	950 kr	950 kr	950 kr

Priserna är exklusive moms och inkluderar digital dokumentation, lunch och kaffe. Lokal bekräftas en månad innan konferensen via e-post och via vår hemsida insightevents.se/scada

Betalning erläggs mot faktura 30 dagar netto, dock senast tre arbetsdagar före konferenstillfället. Vid avbokning, som skall göras skriftligen och bekräftas via email, debiteras ingen avgift om avbokningen sker 30 dagar före första konferensdagen, 50% om avbokningen sker senast 14 dagar före och 100% om avbokningen sker senare. Om du får förhinder och inte har möjlighet att delta kan du självklart överlåta din plats till en kollega.

Tid & plats

29-30 september

K-märkt Science Tower Kista
Lokal kan ändras och bekräftas senast en månad innan konferensens start