



## 2. Cybersecurity Symposium Nordschwarzwald



Wir begrüßen Sie herzlich zum 2. Cybersecurity Symposium Nordschwarzwald.

Zu den vier Themenschwerpunkten

- Cybercrime Trends,
- IT/OT,
- System Security und
- Anomalie- & Angriffserkennung

erwarten Sie hervorragende Fachbeiträge und begleitend eine Fachausstellung, die Ihnen zusammen Wissensvorsprung, Wissensaufbau und Wissensvertiefung ermöglichen. Wenn nicht bereits am ersten Tag in den Pausen wertvolle Kontakte geknüpft werden, dann geschieht dies spätestens beim Networking-Abend am 6.3.2024 im Digital Hub Nordschwarzwald in Horb, zu welchem Sie unser Shuttle-Service bringen bzw. später auch gerne wieder abholen und zurück zum Campus fahren wird.

Nutzen Sie die Möglichkeit mit Experten, Betroffenen und hoffentlich nie betroffenen Teilnehmenden des Symposiums ins Gespräch zu kommen.

**Wir wünschen Ihnen spannende Beiträge und einen guten Austausch!**

*Prof. Dr. Tim Jansen & Thomas Hegenauer*

DHBW / STZ Digital Workspace

Digital Hub Horb

## Tag 1 (6.3.2024) sponsored by CLOUDFLARE

Moderation: Prof. Dr. Tim Jansen, DHBW / Steinbeis-Transferzentrum Digital Workspace

8:30 Uhr **Registrierung und Eröffnung der Fachmesse**

9:30 Uhr **Eröffnung des Symposiums**

Prof.in Antje Katona, Campusleitung DHBW Stuttgart Campus Horb

Prof. Dr. Tim Jansen, Studiengangsleiter Maschinenbau Produktionstechnik

Thomas Hegenauer, Leiter Digital Hub Nordschwarzwald Horb

### Themenschwerpunkt Cybercrime Trends

9:50 Uhr Prof. Dr. habil. Martin Plümicke,  
Vizepräsident für Digitalisierung  
und Prozesse, DHBW



Dipl. Ing. (BA) Tech. Inf. Günter Aigle  
Information Security Manager,  
Leiter CC-InfoSec, DHBW



#### **Cybercrime Trends – die aktuelle Bedrohungslage unter Berücksichtigung der dynamischen Entwicklung von KI**

*KI ist in aller Munde: quasi „über Nacht“ hat der Marktprimus OpenAi mit „Chat GPT“ im November 2022 KI in alle Welt gebracht. Seitdem verzeichnen wir eine exponentielle Durchdringung von KI in praktisch allen Lebens- und Arbeitsbereichen. Leider haben auch Cyberkriminelle die Fähigkeiten und Möglichkeiten von KI sehr rasant adaptiert. So finden heutige Angriffe längst auch mit Hilfe von KI statt. Der Vortrag beleuchtet die aktuelle Bedrohungslage unter besonderer Berücksichtigung der aktuellen Möglichkeiten von KI. Hervorzuheben ist hier insbesondere auch die zunehmende Bedrohung durch sog. „Deep Fakes“. Final zeigen wir, wie den Bedrohungen z.B. mit einer guten „Cyber Hygiene“ begegnet werden kann.*

10:35 Uhr Andreas Bechter,  
Senior Solutions Engineer Strategic Cloudflare,  
Cloudflare GmbH



#### **Cyber Threat Landscape - Global & Deutschland**

*Der Vortrag gibt einen Einblick in die globale und deutsche Cyber-Bedrohungslandschaft. Es wird gezeigt, wie sich die Bedrohungen in der digitalen Welt verändern und entwickeln, technische Maßnahmen, welche Rolle AI spielt und mit welchen Angriffen Unternehmen aktuell konfrontiert sind. Sie erfahren mehr über die aktuellen Trends und die Bedrohungen, die speziell die deutsche IT Landschaft betreffen.*

11:10 Uhr

Sandra Jörg,  
CEO,  
BLACKPIN GmbH



### **Wie man sich vor Cyberattacken im Messaging-Umfeld schützen kann**

*Der Mobile Messaging Markt ist einer der 3 größten Wachstumsmärkte weltweit. Obwohl sich bereits zahlreiche Anbieter am Markt befinden, gibt es große Unterschiede bezüglich der Lösungen gerade im B2B Bereich. So bekommt das Thema Data Security und GDPR Compliance eine immer größere Rolle. Zahlreiche neue Gesetze und Sicherheitsstandards stellen Unternehmen vor neuen Herausforderungen. In dem Vortrag wird vorgestellt, welche Unterschiede es am Messangermarkt gibt und was man bei der Wahl eines Produktes beachten muss, um sicher zu sein.*

11:35 Uhr

Dipl. Betriebswirt (DH) Jörg Dreger,  
Geschäftsführender Gesellschafter,  
Dreger Group GmbH



### **Hybrid Warfare, Blackout Risiken, Radikalisierung in der Belegschaft - Wie können sich Unternehmen / Institutionen wirksam davor schützen**

*I. Hybride Kriegsführung und Blackout-Risiken – Es werden Strategien und Notfallpläne zur Minimierung von Cyberangriffen und Stromausfällen vorgestellt.*

*II. Radikalisierung in der Belegschaft – Dieser Teil beleuchtet, wie Unternehmen interne Radikalisierung erkennen und verhindern können, um ein sicheres Arbeitsumfeld zu schaffen.*

*III. Zu guter Letzt um effektive Schutzmaßnahmen – Hier wird beschrieben, wie Unternehmen sich durch Mitarbeiter-Schulungen, Sicherheitstechnologien und eine starke Sicherheitskultur schützen können*

12:00 Uhr

**Mittagspause, Networking** und  
vertiefende Gespräche mit den Ausstellern auf der **Fachmesse**

13:30 Uhr

Dr. Lucian Dold,  
Sen. General Manager Global Account Management,  
OMRON Corporation



Dipl. Wirt. Inform. (FH) Marcus Stier,  
Leiter Business Development,  
COMBACK GmbH



### **Reiter der Apokalypse oder doch was für Erdmännchen?**

*Sobald das Thema Informationssicherheit auf den Tisch kommt, verstummt die Euphorie für die SMART Factory. Gerade wurde noch über digitale Zwillinge und Künstliche Intelligenz gesprochen, bei Cybersecurity oder besser IT / OT Konvergenz verdüstern sich die Mienen und es ist wie in so mancher Beziehung: ES IST KOMPLIZIERT! Liegen (Security)-Reiter der Apokalypse richtig und sind wir alle verloren sobald wir unsere Fabriken vernetzen, oder können wir uns unbeschwert an Cloud und IoT anbinden, wie die lustigen Erdmännchen Ihr Leben leben? Antworten, die vermutlich dazwischen liegen - mit Empfehlungen aus der Praxis nehmen Sie gesichert aus diesem Vortrag mit.*

14:15 Uhr

Dr. Tim Senn,  
Mitgründer und Geschäftsführer,  
narrowin.ch / \ Network & Security



### **Von Komplexität zur Klarheit – Pragmatische Ansätze für Netzwerksicherheit in IT & OT**

*Klassische IT und Operational Technology (OT), wie z.B. industrielle Produktionssysteme, werden zunehmend vernetzt. Netzwerkunterbrüche können zu erheblichen Produktionsausfällen führen. Der sichere und zuverlässige Betrieb dieser Netzwerke ist daher geschäftskritisch. Dafür braucht es jedoch Transparenz hinsichtlich des eigenen Netzwerks sowie eine realistische Road Map, die die Organisation nicht überfordert. Anhand konkreter Beispiele wird in diesem Beitrag gezeigt, wie dieses Ziel erreicht werden kann und wie wertvoll dabei Automatisierung und die richtige Dosis Pragmatismus sind.*

14:40 Uhr

Dr. Andreas Aschenbrenner,  
Associate Vice President für Cybersecurity,  
Siemens AG – Siemens Advanta Consulting



### **IT und OT Cybersecurity – eine Liebesgeschichte?**

*Anhand von Kundenbeispielen werden die Schwierigkeiten im OT Cybersecurity Bereich erläutert, wie dies mit dem unterschiedlichen Reifegrad zur IT Cybersecurity zusammenhängt und was bei der Produktentwicklung beachtet werden muss. Weiterhin wird auch auf die NIS2 eingegangen.*

15:05 Uhr **Pause** und vertiefende Fachgespräche mit den Ausstellern auf der **Fachmesse**

15:50 Uhr Hicham Bensouda,  
System Engineer (SE) OT/IoT,  
Fortinet



### **Cyber-Sicherheits-Checks der operativen Technologie**

*Informationstechnologie (IT) und Betriebstechnologie (OT), die zwei Ökosysteme gibt es schon eine ganze Weile. Beide Systeme teilen eine Gemeinsamkeit in Bezug auf die Datenspeicherung, nur bei der Datenverarbeitungszeit verhält sich OT sehr kritisch. OT wird in einer Vielzahl von Branchen eingesetzt, darunter die Produktions- und Fertigungsindustrie, Öl- und Gasindustrie, Stromerzeugung und -verteilung, Luftfahrt, Schifffahrt, Eisenbahn und Versorgungsunternehmen.*

*Die IT/OT-Konvergenzzone ist eigentlich die Trennungsebene (Air-Gap) zwischen IT und OT. Diese Ebene wird auch als demilitarisierte Zone (DMZ) bezeichnet, die oft als Teil der OT betrachtet wird. Im Rahmen des Vortrags wird aufgezeigt, wie man die IT/OT Konvergenz mit der Einführung von Sicherheitsstandards nach IEC62443 im OT-Umfeld sicherer machen kann.*

16:15 Uhr **Podiumsdiskussion** zum Thema: **Die ruhigen Zeiten sind vorbei - Kommune, Hochschule und Unternehmen im Gespräch**  
mit

Dejan Micic, Wirtschaftsförderer Stadt Horb am Neckar  
Prof. Dr. habil. Martin Plümicke, Vizepräsident für Digitalisierung und Prozesse, DHBW  
Christoph Lauffer, Managing Director Maschinenfabrik Lauffer GmbH & Co. KG

## Networking-Abend

ab 17:00 Uhr Transfer / Shuttle-Bus

sponsored by



zum Digital Hub Nordschwarzwald Horb  
Geschwister-Scholl-Str. 10  
72160 Horb am Neckar

### **Networking-Abend**

Begrüßung: Dejan Micic, Wirtschaftsförderer Stadt Horb am Neckar

bis 23 Uhr Shuttle-Bus / Rücktransfer zum Campus Horb der DHBW

08:30 Uhr **Registrierung, Fachausstellung**

09:30 Uhr **Begrüßung**  
Dejan Micic, Wirtschaftsförderer Stadt Horb am Neckar

## Themenschwerpunkt System Security

09:40 Uhr Richard Ranftl,  
Geschäftsführer,  
SIGN8 GmbH



### **Digitale Identitäts- und Zertifikats-Infrastruktur, -Architektur und Anwendungen in Europa (eIDAS)**

*Es werden nicht nur die komplexe Ausgangslage der digitalen Identitäts- und Zertifikatsinfrastruktur in Europa beleuchtet, auch die verborgenen Angriffsvektoren, die in der digitalen Welt lauern, werden enthüllt.*

*Es wird dargestellt, wo in der komplexen Systemlandschaft, von Microsoft 365 über Outlook bis hin zur Firewall, digitale Zertifikate als entscheidende Sicherheitsinstrumente agieren können. Denn Zertifikate bilden die Grundlage für vertrauenswürdige digitale Identitäten, können in verschiedensten Bereichen angewendet werden und garantieren höchste Sicherheitsstandards.*

*Der Vortrag bietet tiefgreifende Einblicke in innovative EU-Initiativen und Architekturansätze wie die eIDAS-Verordnung oder das EU-Wallet. Diese Ansätze zeigen nicht nur, wie wir digitale Identitäten schützen können, sondern bieten auch einen inspirierenden Ausblick darauf, wie wir sie sicher und innovativ in die eine digitale Zukunft überführen können.*

10:25 Uhr Mario Ivanda,  
Regional Sales Manager,  
DataCore Software GmbH



### **NIS2 und Kritis bis zum Storage zu Ende gedacht**

*Harte Deadlines für NIS2 und Kritis und was diese für Unternehmen bedeuten. Erfahren Sie, wie Sie Security- und Datenkonzepte bis auf Storage-Ebene abbilden und Compliance-Anforderungen lösen können. Eine clevere Wahl der Storage Architektur gibt Sicherheit gegen Ransomware, Trojaner, Datenausfall und bietet Mehrwerte, um Ihre Daten auch noch wirtschaftlich nutzbar zu machen.*

11:00 Uhr Dipl. Wirt. Inform. (FH) Marcus Stier,  
Leiter Business Development,  
COMBACK GmbH



### **Warum eine Datensicherung für Cybersecurity wichtig ist**

*Das Thema Cybersecurity ist weiterhin in aller Munde und auch die große Unbekannte, wenn es um die Digitalisierung geht. Wie aber passt die Datensicherung da hinein? Die Datensicherung ist schließlich einer der traditionellsten Bereiche in der IT und... doch überall vorhanden. Wie sicher aber sind Ihre Daten in der Datensicherung? Können Sie diese nach einem Angriff überhaupt benutzen? Und wenn ja, wie? Wissen Sie was nach einem Angriff mit der Datensicherung passiert?*

11:35 Uhr Florian Handke,  
Leiter Industrial Security,  
Campus Schwarzwald



### **Larifari Industrie 4.0**

*Wie kann Vertrauen zwischen industriellen Endgeräten hergestellt werden? Digitale Identitäten sind eine Schlüsseltechnologie für sichere Kommunikation, sichere Soft- und Firmwareupdates und Geräteintegrität. Erfahren Sie, wo die Herausforderungen liegen, was digitale Identitäten ermöglichen und wie wir mit unserem Open Source Projekt Trustpoint Vertrauen in der Fabrik ermöglichen.*

12:00 Uhr **Mittagspause, Networking** und  
vertiefende Gespräche mit den Ausstellern auf der **Fachmesse**

## Themenschwerpunkt Anomalie- und Angriffserkennung

13:30 Uhr     Marvin Gerhardt,  
Technischer Produktmanager Cybersecurity,  
Vector Informatik GmbH



### Sicherheitsmechanismen für eingebettete Systeme am Beispiel der Automobilbranche

*Seit Jahren ist Cybersecurity ein fester Bestandteil der Entwicklungen in der Automobilbranche. Durch neue Regularien erfahren diese Bemühungen eine verstärkte Aufmerksamkeit. Dabei werden verschiedene Sicherheitsmechanismen implementiert, um eingebettete Systeme zu schützen und die Sicherheit von Fahrzeugflotten zu gewährleisten. Dieser Vortrag gibt Einblicke in die vielfältigen Maßnahmen zur Bewältigung dieser Herausforderungen.*

14:15 Uhr     Vertiefende Gespräche mit den Ausstellern auf der **Fachmesse**

16:30 Uhr     **ENDE** des Symposiums

Die zur Veröffentlichung freigegebenen Beiträge werden im Nachgang den Teilnehmenden per Email als Downloadlink zur Verfügung gestellt.

Wir danken allen Mitwirkenden, insbesondere unseren Sponsoren



den Ausstellern und den Referenten.

Wir freuen uns auf ein Wiedersehen am **5.-6. März 2025** zum  
**3. Cybersecurity Symposium Nordschwarzwald**