BONNER IT DIALOG
by AFCEA Bonn e. V.

Programm
Standplan
Verzeichnis A–Z
Porträts Aussteller

AUSSTELLER-VERZEICHNIS

2026

» Die Resilienz Deutschlands auf dem Prüfstand

MARITIM
Hotel Bonn



Nehmen Sie Platz oder nehmen Sie Ihren Kaffee und frische Snacks einfach mit – perfekt für Ihre kleine Auszeit zwischendurch.

Täglich von 10 bis 18 Uhr geöffnet.

Café Moment | WE PROUDLY SERVE™

Maritim Hotel Bonn · Godesberger Allee · 53175 Bonn · www.maritim.de
Betriebsstätte der Maritim Hotelgesellschaft mbH · Herforder Straße 2 · 32105 Bad Salzuflen

INHALTSANGABE

Ausstellerverzeichnis **Bonner IT-Dialog 2026**

Seite

Grußwort 4
Generalmajor Armin Fleischmann, Vorsitzender AFCEA Bonn e. V.

Programm Mittwoch, 7. Oktober 2026 6
Programm Donnerstag, 8. Oktober 2026 7

Standplan Übersicht Maritim Hotel Bonn 8

Ausstellerverzeichnis nach Standnummern 10
Ausstellerverzeichnis A–Z 11

Historie AFCEA Bonn e. V. 12
Historie Bonner IT-Dialog und Koblenzer IT-Tage 14

AUSSTELLER-PORTRÄTS BONNER IT-DIALOG 2026
in alphabetischer Reihenfolge von A wie Airbus bis Z wie ZDigBw..... **Seiten 16 bis 57**

Ausblick 40. AFCEA Fachausstellung 2027 58
Mitglied werden bei AFCEA Bonn e. V. 60
AFCEA Studienpreis 2026 Vorstellung im Rahmen des Bonner IT-Dialogs 62



Die **Resilienz Deutschlands** auf dem Prüfstand

Deutschland hat die Mittel, die Fähigkeiten und die Menschen für ein funktionierendes System gesamtstaatlicher Sicherheit und Verteidigung. Zwischen Behörden, Ebenen und Systemen reißt die Handlungskette jedoch regelmäßig vor, während und nach Krisen, Schadens- und Bedrohungslagen. Allein es fehlt die Verkettung und Vernetzung.

Mit dem Bonner IT-Dialog tritt AFCEA Bonn e. V. an zwei Tagen an, für ein gesamtstaatliches Sicherheitsökosystem alle notwendigen Perspektiven zusammen zu bringen. Schirmherrin der Veranstaltung ist Mona Neubaur, Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie sowie stellvertretende Ministerpräsidentin des Landes Nordrhein-Westfalen.

Sicherheit entsteht nicht in Silos. Gesamtgesellschaftliche Resilienz setzt einen gesamtstaatlich handlungsfähigen Kern voraus. Der Staat muss verkettet sein, damit Wirtschaft und Bevölkerung überhaupt andocken können. Im Ernstfall arbeiten sechs Gruppen zusammen, die im Alltag selten an einem Tisch sitzen: Streitkräfte, Politik und Verwaltung, BOS und Zivilschutz, Kritische Infrastrukturen und Wirtschaft, Industrie und Technologie sowie die Zivilgesellschaft.

Lassen Sie sich auf dem Bonner IT-Dialog als Teil unseres gesamtstaatlichen Sicherheitsökosystems inspirieren: mit der Erstveröffentlichung der AFCEA-Studie „Gesamtstaatliches Sicherheitsökosystem 2030" — mit 30 Vorschlägen für mehr Handlungsfähigkeit, entwickelt aus 50 Interviews und dem Vergleich mit den Niederlanden, Estland, Finnland und der Ukraine. Dazu der Bericht aus einem Land, das Resilienz nicht planen konnte, sondern lernen musste.

Begegnen Sie den anderen Playern für mehr Resilienz und tauschen Sie sich aus: Die Gäste des Bonner IT-Dialogs kommen aus Bundeswehr, Behörden und Organisationen mit Sicherheitsaufgaben, Ländern, Kommunen und der Industrie. Für den Austausch steht Ihnen eine Fachausstellung mit Use Cases an beiden Tagen bereit. Wir verleihen den Studienpreis 2026 mit Vortrag des ausgezeichneten Beitrags. Testen Sie ihr Wissen in einem Resilienz-Quiz oder lassen Sie sich als „Resilience Practitioner" zertifizieren.

Gesamtstaatliche Sicherheit und Verteidigung ist keine Frage, die ein Ressort allein beantworten kann. Sicherheit ist kein Projekt. Sie ist eine dauerhafte staatliche Aufgabe, die im Alltag geübt und nicht im Ernstfall improvisiert wird. Was und wer dafür zusammenwirken muss, kommt am Bonner IT-Dialog zusammen.

Nutzen Sie den Bonner IT-Dialog. Ich wünsche Ihnen erkenntnisreiche Vorträge und viele Impulse aus Gesprächen, um die Silos gemeinsam aufzubrechen.

Generalmajor Armin Fleischmann
Vorsitzender AFCEA Bonn e. V.



„Deutschland hat die Mittel, die Fähigkeiten und die Menschen für ein funktionierendes System gesamtstaatlicher Sicherheit und Verteidigung."

Programm Mittwoch | 7. Oktober 2026

Ab **8:30 Uhr**	**Check-In** Hotel MARITIM Bonn
10.00 Uhr	**Eröffnung und Begrüßung** **Generalmajor Armin Fleischmann** (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.) Videobotschaft **Schirmfrau Mona Neubaur** (Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie des Landes NRW) **Nina Staudenrauß** (AFCEA Bonn e. V.), Vorstellung Veranstaltungsablauf
10.15 Uhr	**Scene-Setting & Key-Note: Landeskommando Rheinland-Pfalz, gesamtgesellschaftliche Resilienz aus der militärischen Perspektive** LKdo RLP: **Oberst Michael Trautermann**, Kommandeur
10.30 Uhr	**Panel: Die Rolle der Bundeswehr im Kontext gesamtgesellschaftlicher Resilienz (OpPlanDEU)** Moderation: **Major Dominik Hauschild** **Oberst Michael Trautermann** (Kommandeur LKdo RLP) **Dr. Christian Marwitz** (Geschäftsführer BWI GmbH) **Oberst i. G. Stephan Sauer** (Unterabteilungsleiter Digitalisierung Bundeswehr, Kdo CIR)
11.30 Uhr	**Preisverleihung AFCEA Bonn Studienpreis 2026** Moderation: **Dr. Michael Gerz**, (Vorstand Wissenschaft & Forschung AFCEA Bonn e. V.) Vortrag durch den 1. Preisträger AFCEA Studienpreis
12.00 Uhr	**Mittagessen**
13.00 Uhr	**Scene-Setting & Key-Note: Defence.NRW, gesamtgesellschaftliche Resilienz aus der Länderperspektive** Vortragender: **Staatssekretär Paul Frederik Höller**, NRW
13.30 Uhr	**Vortrag: Die Rolle der Industrie im Kontext gesamtgesellschaftlicher Resilienz** Vortragender: **Dr. Christian Marwitz**, Geschäftsführer BWI
14.00 Uhr	**Preisverleihung AFCEA Bonn Schulförderung 2026** Moderation: **Christopher Gaube** (Vorstand Ausbildung u. Schulförderung, AFCEA Bonn e.V.)
14.10 Uhr	**Besuch der Ausstellung/Kaffeepause**
16.00 Uhr	**Kahoot: Wer wird der nächste Quizmaster?** Moderation: **Annika Waller** (Emerging Leader AFCEA Bonn e. V.), Kahoot inklusive Preisverleihung
16.30 Uhr	**Vorstellung der Studie „Sicherheitsökosystem 2030" und Panel** Moderation: **Bernhard Steimel** (Studienleitung) **Generalmajor Armin Fleischmann** (Kdo CIR AbtLtr Planung) **Bernd König** (Geschäftsführer Google Cloud Public) **Norbert Ahrend** (Head of Public Sector Consulting, Arvato Systems)
17.30 Uhr	**Vortrag: Zivile Resilienz im Ernstfall – was die Ukraine uns lehrt** Vortragende: **Andrii Levanchuk** und **Dominik Brinkmann** über ihren zivilgesellschaftlichen Beitrag zum Krieg in der Ukraine



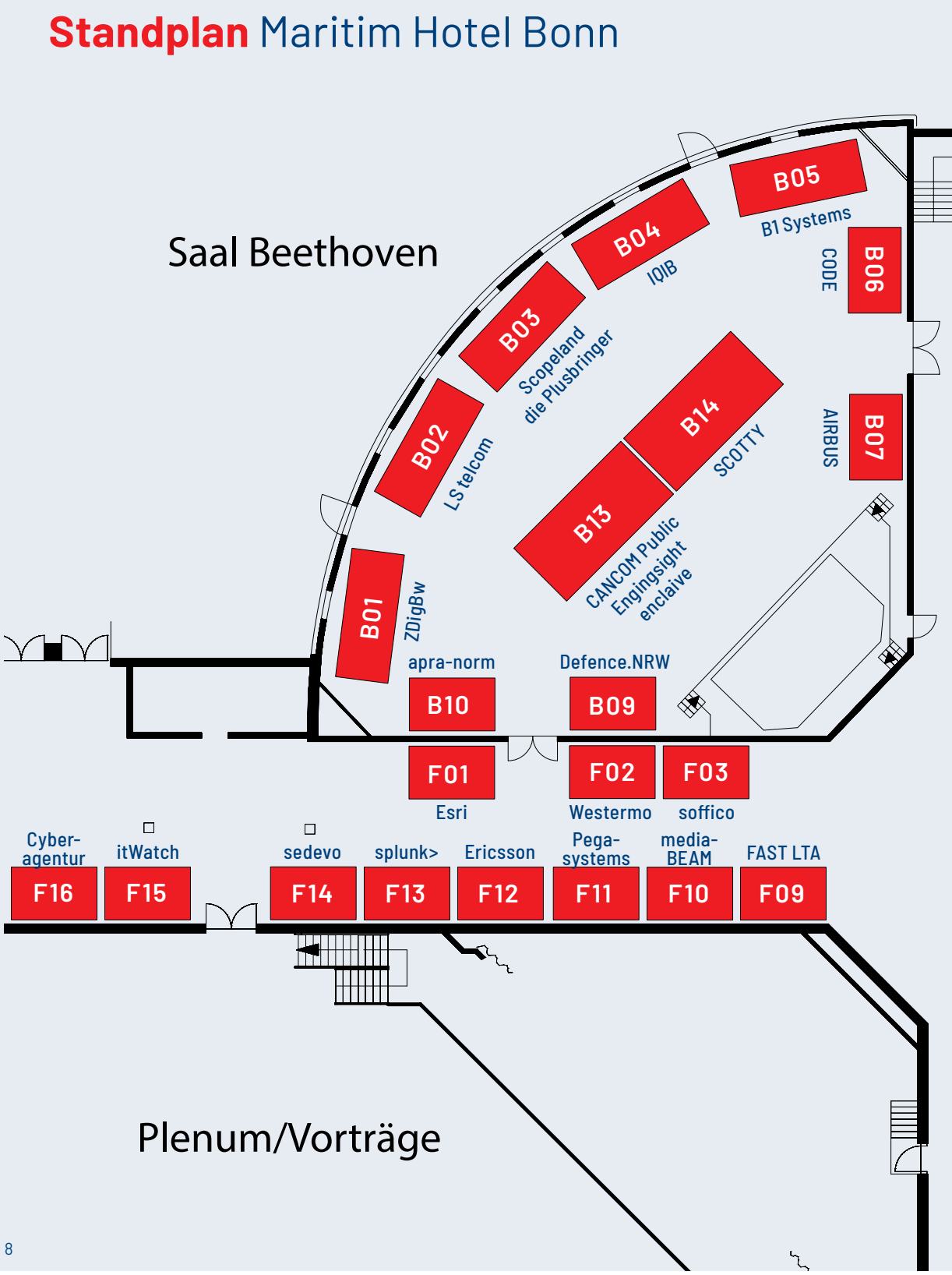
HINWEIS: Programmablauf zum Zeitpunkt der Drucklegung/Änderungen vorbehalten

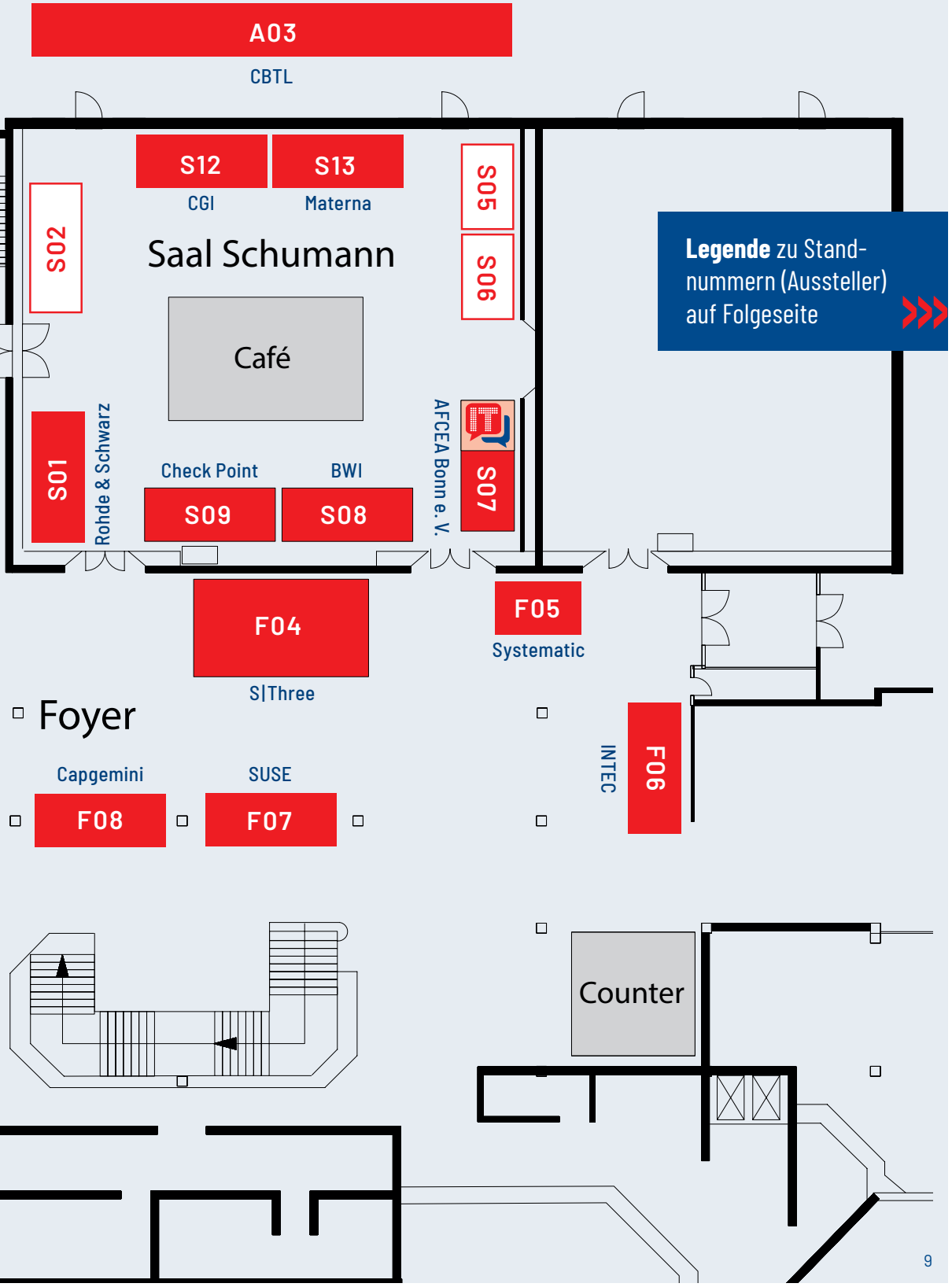
18.00 Uhr	**Tagesabschluss und Eröffnung Beer-Call** **Generalmajor Armin Fleischmann** (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.)

Programm Donnerstag | 8. Oktober 2026

9.00 Uhr	**Begrüßung Tag 2: Generalmajor Armin Fleischmann** (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.)
9:15 Uhr	**Scene-Setting & Key-Note: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, gesamtgesellschaftliche Resilienz aus der Perspektive Zivilschutz** Vortragende: **Kathrin Stolzenburg** (Referatsgruppenleiterin N.I. Vorsorgeplanung im Bevölkerungsschutz und Zivile Verteidigung)
9:45 Uhr	**Vortrag: Hybride Bedrohung und Cybersicherheit in der Chemie-Industrie** **Volker Wagner** (CISO BASF Digital Solutions GmbH)
10:00 Uhr	**Vortrag: Neuausrichtung des Bevölkerungsschutzes Rheinland-Pfalz** **René Schubert** (Präsident Koblenzer Landesamt für Brand- und Katastrophenschutz)
10:15 Uhr	**Besuch Ausstellung/Kaffeepause**
11:30 Uhr	**Vortrag: Vom Alarm zur Handlung – ein föderiertes Lagebild für hybride Angriffe auf Deutschlands KRITIS** Vortragende: **Leutnant Aaron Emde**, **Leutnant Tamino Müller** und **Leutnant Erik Zahn** Mentor: **Kapitän zur See Dr. Dr. Robert Koch**
12:00 Uhr	**Abschlusspanel** Moderation: **Anna-Lena Hohmann** (Vorstand Emerging Leaders AFCEA Bonn e. V.) **Dr. Lino Schneider-Bertenburg** (Clustermanager Defence.NRW) **Kathrin Stolzenburg** (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) **René Schubert** (Präsident Koblenzer Landesamt für Brand- und Katastrophenschutz) **Volker Wagner** (Verband der Chemie Industrie, BASF SE)
13.00 Uhr	**Verabschiedung/Ende der Veranstaltung** **Nina Staudenrauß** (AFCEA Bonn e. V.) **Generalmajor Armin Fleischmann** (Kommando Cyber- und Informationsraum, Vorstandsvorsitzender AFCEA Bonn e. V.)
13.15– 14.00 Uhr	**Mittagessen** (Besuch der Standflächen bis 14:00 Uhr möglich)

Standplan Maritim Hotel Bonn





Legende zu Standnummern (Aussteller) auf Folgeseite

Ausstellerverzeichnis nach Standnummern

STAND-NUMMER	AUSSTELLER	SEITENZAHL PORTRÄT
A03	**CBTL** Computer Based Training and Learning GmbH	23
B01	**ZDigBw** Bundeswehr	57
B02	**LS telcom**	39
B03	**Scopeland** Technology GmbH	48
B03	**die Plusbringer** GmbH	46
B04	**IQIB** - Institut für qualifizierende Innnovationsforschung u. -beratung GmbH	37
B05	**B1 Systems** GmbH	19
B06	**CODE** Forschungsinstitut - UniBw München	27
B07	**AIRBUS** SAS	17
B09	**Defence.NRW** VDI Technologiezentrum GmbH	30
B10	**apra-norm** Elektromechanik GmbH - Geschäftsbereich apraNET	18
B13	**CANCOM Public** GmbH	21
B13	**Engingsight** GmbH	32
B13	**enclaive** GmbH	31
B14	**SCOTTY** Group Austria GmbH	49
F01	**Esri** Deutschland GmbH	34
F02	**Westermo** Data Communications GmbH	56
F03	**soffico** GmbH	51
F04	**S|Three** GmbH	53
F05	**Systematic** A/S	55
F06	**INTEC** Industrie-Technik GmbH	36
F07	**SUSE** Software Solutions Germany GmbH	54
F08	**Capgemini** Deutschland GmbH	22
F09	**FAST LTA** GmbH	35
F10	**mediaBEAM** GmbH	41
F11	**Pegasystems** GmbH	42
F12	**Ericsson** GmbH	33
F13	**splunk>** a CISCO company	52
F14	**sedevo** IT Consulting GmbH	50
F15	**itWatch** GmbH	38
F16	**Cyberagentur** für Innovation in der Cybersicherheit GmbH	28
S01	**Rohde & Schwarz** GmbH & Co. KG	47
S07	**AFCEA Bonn e. V.** – Ausstellerbüro	58
S08	**BWI** GmbH	20
S09	**Check Point** Software Technologies GmbH	26
S12	**CGI** Deutschland B.V. & Co. KG	24
S13	**Materna** Information & Communications SE	40

Ausstellerverzeichnis A–Z

AUSSTELLER	STAND-NUMMER	SEITENZAHL PORTRÄT
AFCEA Bonn e. V. – Ausstellerbüro	S07	58
AIRBUS SAS	B07	17
apra-norm Elektromechanik GmbH - Geschäftsbereich apraNET	B10	18
B1 Systems GmbH	B05	19
BWI GmbH	S08	20
CANCOM Public GmbH	B13	21
Capgemini Deutschland GmbH	F08	22
CBTL Computer Based Training and Learning GmbH	A03	23
CGI Deutschland B.V. & Co. KG	S12	24
Check Point Software Technologies GmbH	S09	26
CODE Forschungsinstitut - UniBw München	B06	27
Cyberagentur für Innovation in der Cybersicherheit GmbH	F16	28
Defence.NRW VDI Technologiezentrum GmbH	B09	30
enclaive GmbH	B13	31
Engingsight GmbH	B13	32
Ericsson GmbH	F12	33
Esri Deutschland GmbH	F01	34
FAST LTA GmbH	F09	35
INTEC Industrie-Technik GmbH	F06	36
IQIB Institut für qualifizierende Innnovationsforschung u. -beratung GmbH	B04	37
itWatch GmbH	F15	38
LS telcom	B02	39
Materna Information & Communications SE	S13	40
mediaBEAM GmbH	F10	41
Pegasystems GmbH	F11	42
die Plusbringer GmbH	B03	46
Rohde & Schwarz GmbH & Co. KG	S01	47
Scopeland Technology GmbH	B03	48
SCOTTY Group Austria GmbH	B14	49
sedevo IT Consulting GmbH	F14	50
soffico GmbH	F03	51
splunk> a CISCO company	F13	52
S|Three GmbH	F04	53
SUSE Software Solutions Germany GmbH	F07	54
Systematic A/S	F05	55
Westermo Data Communications GmbH	F02	56
ZDigBw Bundeswehr	B01	57

AFCEA Bonn e. V. – seit Gründung dem Informationsaustausch verpflichtet

Im Frühjahr 1983 trafen sich in Bonn Vertreter von Bundeswehr, Öffentlichem Dienst, Forschung und Industrie, um das deutsche Chapter des Internationalen Dachverbands AFCEA zu gründen.

Der Initiator Eberhard Müller-von der Bank gehört ebenso wie Rainer Ramin, Begründer der Fachausstellung und langjähriger Fachmesseorganisator, zu den Gründungsmitgliedern, die immer noch AFCEA Bonn e. V. immer verbunden waren.



Eberhard Müller-von der Bank

Im Herbst 1983 wurde die erste Vorstandssitzung im Saal des Rathauses in Bonn-Beuel einberufen. Die Mitgliederversammlung beschloss, AFCEA Bonn als eingetragenen Verein zu führen. Ehrengast war der damalige Stellvertretende NATO-Oberbefehlshaber General Günter Kiessling, dessen Besuch in Bonn ihm seinerzeit zusätzliche Schwierigkeiten im Rahmen der „Kiessling-Affäre" bereitete.

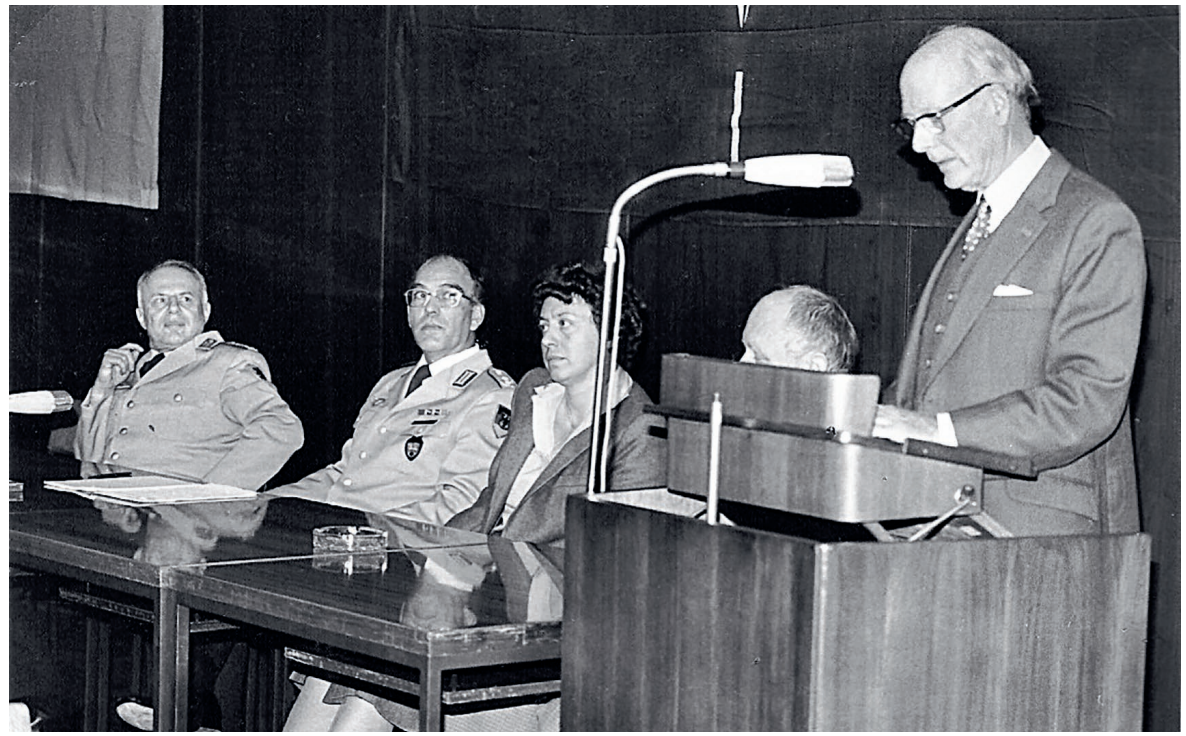
Start mit Bildschirmtext (Btx)

Ziel des Vereins war es, den Informationsaustausch zwischen Bedarfsträgern und Bedarfsdeckern, zwischen Anwendern und Herstellern zu intensivieren. Dies wurde zunächst primär über die regelmäßigen Fachveranstaltungen (in den Räumen der FGAN Wachtberg-Werthoven) realisiert.

Die erste Fachveranstaltung startete im November 1983 mit dem Thema „Bildschirmtext". Neben Fachvorträgen wurden zahlreiche Präsentationen geboten. Aus der Idee Rainer Ramins, den Informationsaustausch in einem größeren Rahmen anzubieten und neben Vorträgen auch „etwas Hardware" zu zeigen, wurde 1986 die Fachausstellung geboren. Bereits die erste Ausstellung mit dem Leitthema „Bürokommunikation" war ein voller Erfolg. Inzwischen hat sie sich zu der wichtigsten Veranstaltung von AFCEA Bonn e. V. entwickelt.

Veranstaltungsort war von 1986 bis 2017 die Stadthalle Bonn-Bad Godesberg, es folgte das Maritim Hotel in Bonn. Seit 2021 findet die Fachausstellung im World Conference Center Bonn statt.

Aus Anlass der Gründung am 26. Mai 1983 und zum 40-jährigen Bestehen hat der Verein im Jahr 2023 die Historie und seine Themen in einer interaktiven Broschüre zusammengestellt. Darin ist neben zahlreichen Beiträgen von Gründungsmitgliedern, langjährigen Wegbegleitern und engagierten Partnern auch die Geschichte und Entwicklung des Vereins in Wort, Bild und Film dargestellt. Auch zahlreiche Mitgliedsfirmen gratulieren darin. ■



Gründungsjahr 1983: Im Rathaus Bonn-Buel fanden sich die Inititatoren zur Gründung des deutsche AFCEA-Chapters zusammen.



Von der **Koblenzer Fachtagung IT** zum **Bonner IT-Dialog**

Zum 18. Mal schafft AFCEA Bonn e. V. Raum für die sicherheitspolitisch relevanten Fragestellungen zum Thema IT







Von Nina Staudenrauß, Organisation Bonner IT-Dialog

Die Koblenzer IT-Tagung hat eine lange Tradition und wurde bereits 2004, damals noch unter dem Titel „Koblenzer Fachtagung IT“, als gemeinsame Veranstaltung von AFCEA Bonn e. V. und dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) etabliert. Über viele Jahre stand die Veranstaltung für den Austausch über leistungsfähige Informations- und Kommunikationstechnik zur Unterstützung der Streitkräfte und richtete den Blick insbesondere auf die Perspektive des Bedarfsdeckers BAAINBw. Die Tagung entwickelte sich zu einem bedeutenden Forum für die IT der Bundeswehr und verband Fachvorträge und Diskussionspanels zunehmend mit interaktiven Elementen. So wurde beispielsweise 2023 erstmals ein „Innovationsraum“ geschaffen, in dem Bundeswehr, Wissenschaft, Forschung und Industrie neue Technologien und konkrete Anwendungsfälle unter anderem aus den Bereichen Künstliche Intelligenz, Cybersicherheit und Interoperabilität erlebbar machten.

2025 wurde das etablierte Format schließlich neu ausgerichtet und als Bonner IT-Dialog fortgeführt. Der Neuausrichtung diente einem Wechsel von der bisherigen Bedarfsdecker- zur Bedarfsträgerperspektive. Die Premiere des ersten Bonner IT-Dialogs fand am 1. Oktober 2025 im Maritim Hotel Bonn statt und stellte mit dem Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) die zukünftigen Planungen und Programme des Bedarfsträgers in den Mittelpunkt. Inhaltlich ging es unter dem Titel „Kriegserklärung übersehen? – Die Rolle des ZDigBw im Umgang mit hybriden Bedrohungen“ um hybride Bedrohungen, Cyberabwehr, Digitalisierung der Streitkräfte und die sicherheitspolitischen Veränderungen unserer Zeit.

Für 2026 hat AFCEA das Format nochmals deutlich weiterentwickelt: An zwei Tagen und unter Berücksichtigung von sechs Perspektiven, steht nicht mehr ausschließlich die IT der Bundeswehr, sondern IT als Enabler einer gesamtgesellschaftlichen Resilienz im Fokus. Streitkräfte, Politik, Blaulicht Organisationen, Zivilschutz, Zivilgesellschaft und Industrie stellen ihre Rolle im Sicherheitsökosystem vor und warum Verteidigung nur gemeinsam gelingen kann. ■



Koblenzer Fachtagung IT



Bonner IT-Dialog

BONNER IT DIALOG
by AFCEA Bonn e. V.
2026

AUSSTELLER-PORTRÄTS A–Z







Airbus – digitale Souveränität und Vertrauen

In Zeiten, in denen vernetzte Systeme das Rückgrat von Gesellschaften bilden, ist technologische Exzellenz die Voraussetzung für Sicherheit. Airbus steht für die Gewährleistung dieser Sicherheit. Wir vereinen entscheidende Säulen, um unsere Partner gegen die Komplexität digitaler Bedrohungen zu schützen:

Secure Connectivity

Wir bieten End-to-End-Systeme und Services, die auf maximale Einsatzfähigkeit ausgelegt sind. Als Partner übernehmen wir die gesamte Komplexität der Satellitenkommunikation. Unser Ziel ist die Entlastung Ihrer Ressourcen: Wir sichern die Verbindung, damit Sie sich ungestört auf Ihre Mission konzentrieren können.

- **Bodensegmente:** Unterstützung von strategischer Planung über den Aufbau bis hin zu Flight Operations und Full-Service-Support
- **Military & Governmental Services:** Ihr Partner für die Betreuung hochkomplexer Satcom-Projekte
- **Multi-Orbit Satcom Services:** Maximale operative Flexibilität durch Software-basierte Lösungen wie SatcomHub – ermöglicht durch unsere Meta-Operator-Kapazitäten
- **Terminals & Equipment:** Hochrobuste und zuverlässige Hardware für den Einsatz unter extremen Bedingungen – an Land, in der Luft und auf See
- **Well-Being & Connectivity:** Skalierbare Konnektivitäts- und Hardwarelösungen, die die Einsatzfähigkeit und das Wohlbefinden der Kräfte unterstützen

Cyber

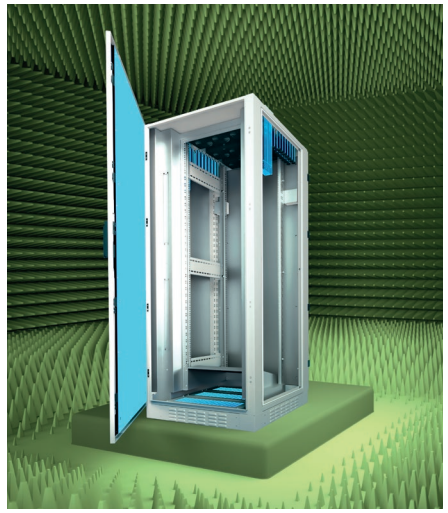
Als souveräner Partner für Cybersicherheit vereinen wir das Wissen von unseren Experten, um Kunden in den Bereichen Verteidigung, Luft- und Raumfahrt sowie Regierungen und Behörden zu schützen. Wir entwerfen, entwickeln und integrieren Cyber-Lösungen, die über den gesamten Systemlebenszyklus hinweg höchste Zuverlässigkeit garantieren. Unsere Lösungen ermöglichen es, Cyber-Operationen zu managen und stellen sicher, dass auch unter den größten Herausforderungen, die Cyber-Resilienz bewahrt werden kann. ■

AIRBUS

STAND-NUMMER B07

Defence and Space
Willy-Messerschmitt-Straße 1
82024 Taufkirchen
www.airbus.com





apra – Schutz und Integration für einsatzkritische Technologie

Wenn Zuverlässigkeit keine Option, sondern Voraussetzung ist

Ob Kommunikation, IT-Infrastruktur oder elektronische Systeme: Im Defense-Umfeld müssen Technologien zuverlässig funktionieren – auch unter anspruchsvollen Bedingungen. apra entwickelt die passende physische Infrastruktur dafür.

Wir schützen, integrieren und verbinden wertvolle Elektronik mit robusten Schrank- und Gehäusesystemen – vom bewährten Standard bis zur individuell entwickelten Lösung.

Ihre Anforderungen. Unsere Möglichkeiten.

ROBUST | Zuverlässige Schrank- und Gehäusesysteme für anspruchsvolle Anwendungen und den sicheren Schutz wertvoller Elektronik.

INDIVIDUELL | Wenn Standardlösungen nicht ausreichen, entwickeln wir Systeme, die exakt auf Ihre technischen und konstruktiven Anforderungen abgestimmt sind.

EMV-GERECHT | Für sensible Elektronik und anspruchsvolle Einsatzbereiche realisieren wir Lösungen mit abgestimmten EMV-Eigenschaften, entwickelt nach **BSI-Zonenmodells**, **Tempest NATO-Richtlinien** und **SDIP 27**.

Alles aus einer Hand – Made in Germany

Von der Entwicklung und Konstruktion über die Fertigung bis zum Aufbau vor Ort begleiten wir Ihr Projekt mit umfassendem Know-how und hoher Fertigungstiefe.

Mit unserer Erfahrung, der hohen Fertigungstiefe und breiten technologischen Möglichkeiten entwickeln wir gemeinsam mit Ihnen die passende Lösung für Ihre wertvolle und einsatzkritische Technik. ■

apra – die optimale Schale für wertvolle Elektronik

STAND-NUMMER B10

apra-norm Elektromechanik GmbH
Geschäftsbereich apraNET/Defense
Bei der untersten Mühle 5, 54552 Mehren
Telefon: +49 65 92 204-200
E-Mail: vertrieb@apranet.de
Internet: www.apra.de



B1 Systems Digitale Souveränität für Behörden und sicherheitsrelevante Organisationen

Digitale Souveränität bedeutet mehr als Open Source. Entscheidend ist, IT selbst betreiben, kontrollieren und weiterentwickeln zu können. B1 Systems unterstützt öffentliche Einrichtungen und Unternehmen dabei – mit offenen Technologien, integrierten Lösungen und dem Know-how für einen zuverlässigen Betrieb.

Das Spektrum reicht von souveränen Cloud-Infrastrukturen über zentrales Linux-Management bis hin zu webbasierten Arbeitsumgebungen und virtuellen Desktops. Dabei bleiben Daten, Systeme und Abhängigkeiten unter eigener Kontrolle.

B1 Systems konzipiert und implementiert Private-Cloud-Umgebungen auf Basis des Sovereign Cloud Stack und begleitet deren Betrieb sowie den Wissenstransfer. Mit dem B1 Linux Client Management lassen sich Linux-Systeme zentral installieren, konfigurieren, aktualisieren und absichern – inklusive Patchmanagement und CVE-Analyse.

Mit openDesk werden E-Mail, Kalender, Dateien, Dokumentbearbeitung, Chat und Videokonferenzen in einer integrierten Arbeitsumgebung gebündelt und vom lokalen Betriebssystem entkoppelt. Für Anwendungen, die weiterhin einen vollständigen Windows- oder Linux-Desktop benötigen, bietet B1 Systems eine zentrale Open-Source-VDI. Virtuelle Arbeitsplätze lassen sich so flexibel bereitstellen und zentral verwalten.

So entsteht digitale Souveränität Schritt für Schritt: Bestehende Anwendungen können weiter genutzt, neue Technologien gezielt eingeführt und Abhängigkeiten reduziert werden.

B1 Systems verbindet dafür offene Technologien mit der Fähigkeit, IT sicher und dauerhaft selbst zu betreiben – für mehr Wahlfreiheit und Kontrolle. ■

STAND-NUMMER B05

B1 Systems GmbH
Osterfeldstraße 7, 85088 Vohburg
Telefon: +49 84 57 93 10 96
E-Mail: info@b1-systems.de
Web: www.b1-systems.de



BWI GmbH – primärer Digitalisierungspartner der Bundeswehr

Die BWI GmbH ist eine 100-prozentige Bundesgesellschaft und mit rund 8.500 Mitarbeiterinnen und Mitarbeitern eines der größten IT-Service-Unternehmen in Deutschland. In Frieden, Krise und Krieg erbringt sie für die Bundeswehr stabile, sichere und effiziente IT-Services – im In- und Ausland Grundbetrieb bis in den einsatznahen Bereich. So trägt sie zur kontinuierlichen Erhöhung der Führungs- und Einsatzfähigkeit sowie der Kampfkraft der Streitkräfte bei.

2006 wurde die BWI mit dem Auftrag gegründet, die Bundeswehr-IT zu modernisieren. Im Rahmen des HERKULES-Projekts hat sie deren IT-Infrastruktur innerhalb von zehn Jahren neu aufgestellt. Das Projekt war eines der größten IT-Konsolidierungs- und Modernisierungsprojekte in Europa. Und es verschaffte der BWI das bundeswehrspezifische IT-Know-how als starkes Fundament, auf dem sie ihr Leistungsportfolio in den vergangenen Jahren enorm erweitert und ausgebaut hat.

Die BWI zeigt auf dem Bonner IT-Dialog die Softwarelösung KVInfoSysBund als Pionier in der pCloudBw: Best Practices und Erkenntnisse für eine Software Factory

KVInfoSysBund ist die erste von der BWI vollständig eigenständig entwickelte Softwarelösung, die auf der pCloudBw betrieben wird. Als ressortübergreifendes System zur Krisenvorsorge und -unterstützung trägt es wesentlich zur Sicherheit deutscher Staatsbürger im Ausland bei. Im Projekt wurden zahlreiche Herausforderungen bewältigt und wesentliche Entscheidungen getroffen – alles Faktoren für den Projekterfolg. Erfahren Sie an diesem Stand, welche Erkenntnisse gewonnen wurden, welche Ziele 2026 noch erreicht werden sollen und wie diese unmittelbar in die Entwicklung des Software Factory Service Bundeswehr einfließen. ■

BWI
IT für Deutschland

STAND-NUMMER S08

BWI GmbH
Auf dem Steinbüchel 22, 53340 Meckenheim
Web: www.bwi.de



KURZPROFIL

- ***Unternehmen:*** *CANCOM*
- ***Schwerpunkt:*** *Digitalisierung und AI-Transformation von Unternehmen, Organisationen und des öffentlichen Sektors*
- ***Kernkompetenzen:*** *Cyber Security, Datacenter & Cloud, Network & Connectivity, Modern Workplace, AI-fähige Infrastrukturen sowie Beratung, Systemintegration und IT-Betrieb*
- ***Relevanz für Defence:*** *Sichere, resiliente und souveräne IT-Lösungen für Bundeswehr, Sicherheitsbehörden und verteidigungsnahe Organisationen*
- ***Besonderheit:*** *End-to-End-Kompetenz; Betrieb eines eigenen Cyber Defense Centers mit 24/7-Sicherheitsüberwachung*

CANCOM. Digitale Souveränität, Sicherheit und Resilienz aus einer Hand

CANCOM ist ein führender Digital Business Provider und AI-Enabler und begleitet Unternehmen und öffentliche Auftraggeber in die digitale Zukunft. Im Umfeld von Bundeswehr, Verteidigung und Sicherheit unterstützt CANCOM Organisationen mit besonders hohen Anforderungen an Verfügbarkeit, Informationssicherheit, Resilienz und digitale Souveränität.

Das Leistungsspektrum reicht von Beratung und Konzeption, über Systemintegration und Beschaffung bis hin zu Managed Services und dem sicheren Betrieb komplexer IT-Infrastrukturen. Dazu zählen unter anderem sichere Netzwerk- und Kommunikationslösungen, moderne Rechenzentrums- und Cloud-Infrastrukturen, Cyber Security sowie digitale Arbeits- und Kollaborationsplattformen. Mit dem unternehmenseigenen Cyber Defense Center bietet CANCOM zudem eine 24/7-Überwachung und Reaktion auf Cyberbedrohungen.

Die internationale Kompetenz im sicherheitskritischen Umfeld unterstreicht CANCOM durch Projekte für europäische Institutionen der Außen- und Sicherheitspolitik. So unterstützt das Unternehmen unter anderem europäische Institutionen mit moderner IT-Infrastruktur für zivile Krisenbewältigungs- und Sicherheitsmissionen der Europäischen Union.

Gerade für Bundeswehr, Sicherheitsbehörden und verteidigungsnahe Organisationen verbindet CANCOM dabei technische Leistungsfähigkeit mit Sicherheit und digitaler Souveränität. Von resilienten und AI-fähigen IT-Infrastrukturen über Cyber Security bis zum sicheren Betrieb unterstützt CANCOM seine Kunden dabei, technologische Abhängigkeiten zu reduzieren, ihre digitale Handlungsfähigkeit zu stärken und IT-Infrastrukturen zukunftssicher weiterzuentwickeln. ■

CANCOM

STAND-NUMMER B13

CANCOM Public GmbH
Franklinstraße 26a
10587 Berlin
Mathias Matzner Telefon +49 151 11 80 09 20
Jörg Schüßler Telefon +49 151 10 84 15 85
www.cancom.de/branchen/branchenloesungen/bundes-und-landesverwaltung/



Capgemini gestaltet digitale Resilienz

Als globaler Partner für KI-gestützte Transformation verbinden wir Strategie, Technologie, Engineering und Operations mit fundierter Branchenexpertise und einem starken Partner-Ökosystem. Im Kontext der gesamtstaatlichen Verteidigung schaffen wir mit souveränen Datenplattformen, sicheren Informationsräumen, KI und systemübergreifender Integration Lösungen, die Resilienz, Einsatzbereitschaft und Entscheidungsfähigkeit stärken.

Live-Demo: vom Datenrauschen zum gemeinsamen Lagebild

Moderne Sensorik und offene Quellen erzeugen mehr Informationen, als sich manuell in der erforderlichen Geschwindigkeit auswerten lassen. Der Engpass liegt in der Befehls- und Auswertestrecke. Aus Tausenden Einzelmeldungen entsteht erst nach Stunden ein belastbares Lagebild. In einem Umfeld, in dem Minuten zählen, ist das zu langsam.

OmniBroker löst dieses Problem. Die Plattform führt heterogene Quellen automatisiert zusammen (Data Fusion), bewertet und verdichtet sie KI-gestützt. So entsteht in Echtzeit ein quellenbasiertes Lagebild, das nachvollziehbar, auditierbar und durch interaktiv abrufbare Evidenz belegt ist.

Wir zeigen OmniBroker live in der AWS European Sovereign Cloud. Über 40 OSINT-Quellen werden in einer gehärteten Architektur zusammengefasst: Daten und Verantwortlichkeiten konsequent getrennt, jeder Zugriff transparent. Für eine definierte Area of Interest entsteht in Sekunden ein Situational Report und verkürzt den Weg vom Sensor zur Entscheidung radikal.

Die Demo zeigt, wie souveräne Cloud-Technologien, KI und Data Fusion belastbare Lagebilder für militärische und zivile Akteure ermöglichen. Nach Zulassung und Freigaben lässt sich die Architektur perspektivisch auch in sensiblen Informationsräumen einsetzen.

Besuchen Sie uns im Foyer. ■

Capgemini

STAND-NUMMER F08

Kontakt: ***Christopher Gaube***
Head of Defense Germany
Capgemini Deutschland GmbH
E-Mail: *christopher.gaube@capgemini.com*
Web: *www.capgemini.com/de-de*



Autorensoftware für E-Learnings, die wirken

*EVOLUTION*³ ist die leistungsstarke E-Learning-Produktionsplattform von *CBTL*. Das kollaborative Autorensystem unterstützt die ressourceneffiziente Erstellung, Pflege und Versionierung anspruchsvoller Selbstlernprogramme und Tests. Als integraler Bestandteil der Virtuellen Lernumgebung der Bundeswehr (VLBw) wird *EVOLUTION*³ dazu beitragen, die Produktion multimedialer Lern- und Lehrmaterialien flächendeckend zu standardisieren.

Damit dieser Vereinheitlichungsgedanke trägt, wurden Antworten auf technische, gesetzliche und organisationsbezogene Anforderungen für die Autorenplattform in einem Framework festgelegt. Das Rahmenwerk regelt zum Beispiel die rollen- und aufgabenspezifischen Zugriffsberechtigungen und Workflows für die unterschiedlichen Benutzergruppen. Außerdem können Autoren auf eine umfangreiche Bibliothek mit bereits CI-konform gelayouteten Vorlagen zugreifen. Diese können auch Zulieferern der Bundeswehr zur Verfügung gestellt werden, wenn sie digitale Lerninhalte mit *EVOLUTION*³ produzieren.

Der kreative Freiraum für die Autoren ist auch innerhalb der Leitplanken eines Frameworks riesig: Je nach Bedarf können dies folienbasierte oder auch responsive Formate sein. Content-Entwickler haben die Möglichkeit, Kurse linear, verzweigt oder adaptiv zu gestalten. Die interaktive Einbindung von 360° Medien, 3D-Objekten und Gamification-Elementen ist ebenso möglich wie die Erstellung von Softwaresimulationen.

Organisationen mit hohem Schutzbedarf können die robuste Softwarelösung des Münchner E-Learning-Spezialisten *CBTL* souverän in der eigenen IT-Infrastruktur betreiben. ■

CBTL

STAND-NUMMER A03

CBTL Computer Based Training and Learning GmbH
Stuttgarter Straße 2, 80807 München, Deutschland
Telefon: *+49 89 358 93 46-0*
E-Mail: *kontakt@cbtl.de*
Web: *www.cbtl.de*


Foto: CGI

Defence ist Teil unserer DNA

CGI gehört zu den weltweit größten Anbietern von IT- und Geschäftsprozess-Dienstleistungen. Defence ist für uns mehr als ein Geschäftsfeld. Rund 800 Mitarbeitende arbeiten in Deutschland in Defence, Intelligence und Space – darunter zahlreiche ehemalige Soldatinnen und Soldaten. Dieses Branchenverständnis verbinden wir mit technologischer Expertise und Umsetzungserfahrung. Wir beraten, entwickeln und betreiben Lösungen in sicherheitskritischen Umgebungen. Als BSI-zertifizierter IT-Sicherheitsdienstleister kennen wir die Anforderungen aus der Praxis.

Defence-Expertise über Grenzen hinweg

Mit kanadischen Wurzeln und starker Präsenz in Deutschland verbinden wir internationale und lokale Expertise. Seit Jahrzehnten arbeiten wir mit der NATO und nationalen Streitkräften verschiedener Länder zusammen und bringen Erfahrungen über Grenzen hinweg ein. Konkrete Beispiele sind AI FELIX für KI-gestütztes Informations- und Aufgabenmanagement bei der NATO und HERMES für sichere mobile Kommunikation mit Rundum-Service. Auch mit anderen Ressorts arbeiten wir für die Stärkung der Gesamtverteidigung zusammen.

Damit diejenigen handlungsfähig bleiben, die unsere Sicherheit schützen

Wir unterstützen Streitkräfte und weitere Akteure dabei, ihren anspruchsvollen Auftrag zu erfüllen. Gemeinsam stärken wir Führungsfähigkeit und Resilienz – vom sicheren Informationsaustausch bis zum Betrieb kritischer IT. Unternehmen der Defence-Industrie befähigen wir zur sicheren Arbeit mit Verschlusssachen.

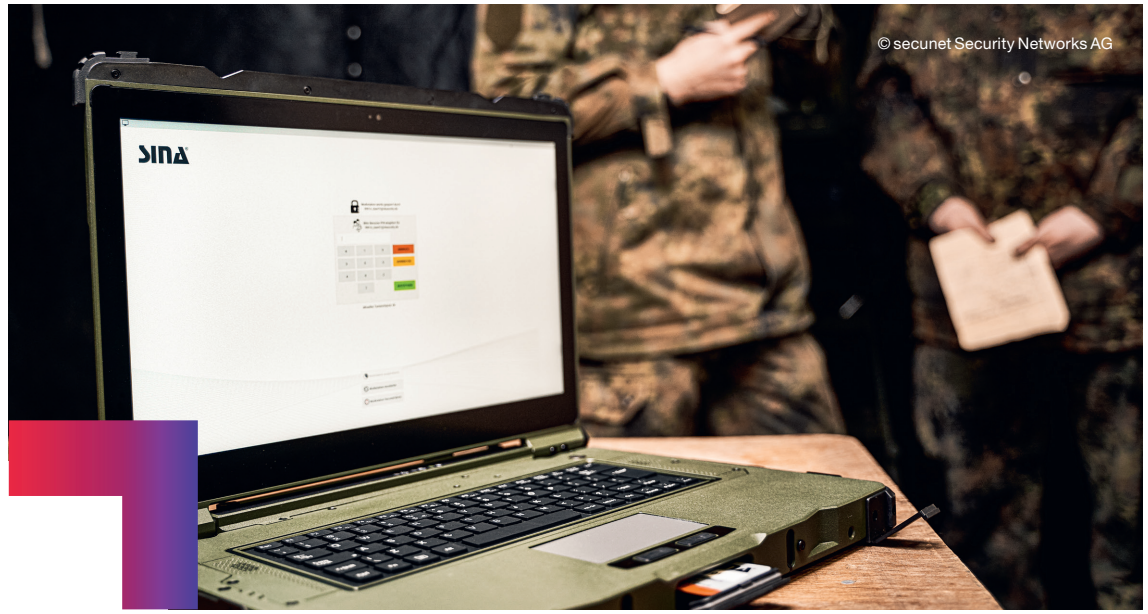
2026 feiern wir 50 Jahre CGI. Gemeinsam mit unseren Kunden entwickeln wir die Fähigkeiten von morgen – für unsere Sicherheit. Building what's next. ■

CGI

STAND-NUMMER S12

CGI Deutschland B.V. & Co. KG
Ettore-Bugatti-Straße 6–14, 51149 Köln
Ansprechpartner: Jens Elstermeier
E-Mail: jens.elstermeier@cgi.com
Telefon: +49 175 93 87 558
Web: www.cgi.com/de/defence

CGI

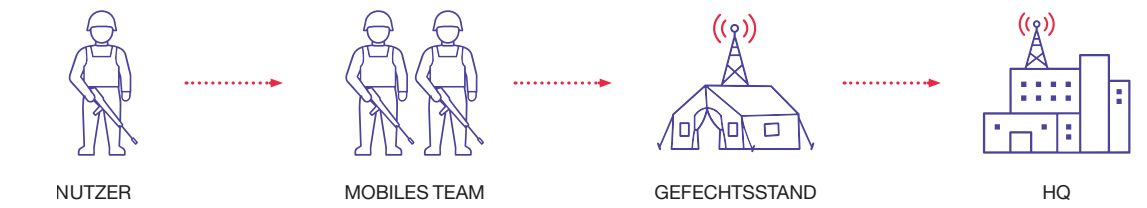


© secunet Security Networks AG

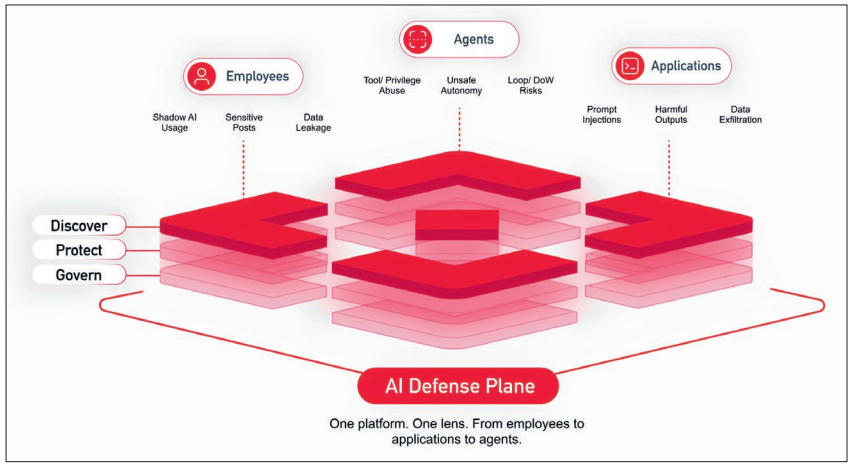
Führungsfähig, wenn's drauf ankommt

Bereits heute im Einsatz: DCIS Light ermöglicht den sicheren Zugriff auf klassifizierte Informationen – überall dort, wo sie benötigt werden.

- **In der NATO bewährt:** erfolgreich im Rahmen von NATO HERMES ausgerollt
- **Organisationsübergreifend einsetzbar:** für eine sichere Gesamtverteidigung
- **Flexibel skalierbar:** von der Einzelnutzung bis zum Einsatz im HQ



Mehr zu DCIS Light
cgi.com/dcis-light-kit





Michael Rimmele

KI verändert die Bedrohungslage schneller, als Security Teams mithalten können

Branchen, Geschäftsprozesse und Organisationen werden durch KI sukzessive verändert. Doch während Unternehmen, Behörden sowie Organisationen aus Luftfahrt, Raumfahrt und Verteidigung KI einsetzen, um Innovation und Effizienz zu steigern, nutzen Cyberkriminelle dieselbe Technologie. Sie führen Angriffe schneller, präziser und skalierbarer denn je durch. Phishing-Kampagnen entstehen in Sekunden, Schadsoftware entwickelt sich dynamisch weiter und Angriffe werden autonom ausgeführt.

Die Folge: Klassische Sicherheitskonzepte geraten an ihre Grenzen. Was früher Stunden oder Tage dauerte, geschieht heute in Minuten. Sicherheitsverantwortliche stehen vor der Herausforderung, Cyberrisiken zu kontrollieren, die sich schneller verändern, als Menschen darauf reagieren können.

Die AI Security von Check Point Software setzt genau hier an. Statt lediglich auf Angriffe zu reagieren, verfolgen wir einen präventionsorientierten Ansatz, der KI nutzt, um Bedrohungen frühzeitig zu erkennen und Risiken zu minimieren. Unser „AI Defense Plane" ist eine zentrale Sicherheitsarchitektur, die das tatsächliche Verhalten von KI-Anwendungen und KI-Agenten zur Laufzeit absichert.

HAUPTFUNKTIONEN:

Workforce AI Security: Bietet Transparenz und Echtzeit-Richtlinien für die KI-Nutzung durch Mitarbeiter (z. B. in Browsern oder Co-Piloten), um den Abfluss sensibler Daten zu verhindern.

AI Application & Agent Security: Schützt KI-Modelle, steuert Tool-Aufrufe, Dateizugriffe, das autonome Verhalten von KI-Agenten und wehrt Prompt-Angriffe ab.

AI Network Firewall: Integriert KI-Sicherheitskontrollen direkt in bestehende Firewalls, um KI-Datenverkehr im Netzwerk ohne neue Hardware sichtbar zu machen und zu steuern.

In einer Welt autonomer Angriffe reicht Reaktion nicht mehr aus. ■

CHECK POINT™

STAND-NUMMER S09

Check Point Software Technologies GmbH
Oskar-Messter-Straße 13, 85737 Ismaning
Michael Rimmele
E-Mail: michaelrim@checkpoint.com
Telefon: +49 151 440 199 00



Foto: UniBw M/Siebold

Forschung für die **Cybersicherheit**

Das Forschungsinstitut Cyber Defence und Smart Data (CODE) ist eine zentrale wissenschaftliche Einrichtung der Universität der Bundeswehr München (UniBw M). CODE erforscht Cybersicherheit in all ihren Dimensionen und bietet ein einzigartiges Forschungsumfeld. Die 20 Professuren und Fachgruppen betreiben sowohl Grundlagen- als auch anwendungsnahe Forschung und Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology zum Nutzen der Gesellschaft und der Bundeswehr.

Seit 2013 bringt CODE Expertinnen und Experten aus unterschiedlichen wissenschaftlichen Disziplinen im Bereich des Cyber- und Informationsraums zusammen. Die Zielsetzung ist die Verwirklichung innovativer technischer Neuerungen und Konzepte in der Cybersicherheit, um Daten, Software und IT-Systeme zu schützen.

Mit derzeit über 150 Mitarbeiterinnen und Mitarbeitern in rund 50 laufenden Projekten hat das Forschungsinstitut CODE eine international sehr wettbewerbsfähige Größe erreicht und ist gleichzeitig durch seine Positionierung und die enge Zusammenarbeit mit Bundeswehr und Behörden einzigartig in Deutschland.

Der direkte Zugang zu Quantencomputern ermöglicht es schon heute, Lösungen für die Herausforderungen von morgen zu finden. Auch die Cyber Range und Lehrinfrastruktur genügen den neuesten Standards und sind die Basis qualifizierter Weiterbildungsangebote für die Bundeswehr. In den Masterstudiengängen Cyber-Sicherheit und Informatik werden Studierende der UniBw M auf die IT-Herausforderungen ihres Berufslebens vorbereitet. ■

CODE FI Forschungsinstitut Cyber Defence Universität der Bundeswehr München

STAND-NUMMER B06

Forschungsinstitut CODE
Universität der Bundeswehr München
Carl-Wery-Straße 18–22, 81739 München
E-Mail: code@unibw.de
Telefon: +49 89 6004 7300
Web: www.unibw.de/code



Cyberagentur stärkt digitale Souveränität

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) initiiert, finanziert und steuert Forschungsprogramme zu zukünftigen Herausforderungen der Cybersicherheit. Als Projektträger des Bundes konzentriert sie sich auf Forschungsfragen mit hohem Disruptionspotenzial, deren technologische und sicherheitspolitische Bedeutung heute teilweise erst absehbar ist.

Die Forschungsaktivitäten gliedern sich in vier Bereiche: Sichere Gesellschaft, Cybersicherheit komplexer Systeme, Schlüsseltechnologien sowie Vertrauenswürdige technische Wertschöpfungsketten. Das Spektrum reicht von Kryptologie, Quantentechnologien und Künstlicher Intelligenz über Robotik und den Schutz kritischer Infrastrukturen bis zu vertrauenswürdigen IT-Architekturen, Kommunikation, digitalen Identitäten und Mensch-Maschine-Interaktion.

Die Programme begleiten neue technologische Ansätze grundsätzlich von der Ideenfindung bis zum funktionierenden Laborversuch und bewegen sich überwiegend in den Technologie-Reifegraden TRL 1 bis 4 nach EU-Definition. Ergänzend beobachtet das Innovationsmanagement globale Trends und identifiziert schwache Signale, um frühzeitig neue Forschungsfragen zu entwickeln.

„Wir leisten Pionierarbeit in der Cybersicherheitsforschung und stärken somit die technologische Souveränität der Bundesrepublik Deutschland von übermorgen“, sagt Prof. Dr. Christian Hummert, Forschungsdirektor der Cyberagentur. ■

cyberagentur

STAND-NUMMER F16

Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19, 06108 Halle (Saale)
Telefon: +49 345 78288032
Web: www.cyberagentur.de



Cybersicherheitsforschung
für die digitale Souveränität Deutschlands

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) ist eine führende Organisation im Bereich der Cybersicherheitsforschung in Deutschland. Die Nationale Sicherheitsstrategie hebt die aktive Rolle der Cyberagentur als Projektträger hervor. Von ihr werden zukunftsweisende Forschungsprogramme der Cybersicherheit initiiert, finanziert sowie gesteuert und sie trägt so zur technologischen Souveränität bei. Dazu ist die Cyberagentur in vier Schwerpunkte geclustert:

- **Sichere Gesellschaft**
- **Cybersicherheit komplexer Systeme**
- **Schlüsseltechnologien**
- **Vertrauenswürdige technische Wertschöpfungsketten**

Im Fokus steht die Arbeit an Programmen mit einem hohen Disruptionspotenzial. Die Forschungsprogramme begleiten Innovationen von der Ideenfindung bis zu einem funktionierenden Laborversuch (Technologie-Reifegrad TRL 1- 4 nach EU-Definition – im Einzelfall auch Vorhaben bis TRL 5 oder 6). Die Cyberagentur blickt mit ihren Programmen in die Zukunft, um langfristig den technologischen Vorsprung von übermorgen im Bereich der Cybersicherheit zu sichern und somit die Innere und Äußere Sicherheit der Bundesrepublik zu stärken.

Mission

Wir identifizieren, finanzieren und evaluieren die disruptive Forschung für übermorgen.

Vision

Als führender Projektträger gestalten wir Sicherheit und technologische Souveränität.

Strategie bis 2030

Wir werden Teil der Weltspitze in der Cybersicherheit.

Hausanschrift:
Agentur für Innovation in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)

Telefon +49 345 78288032
www.cyberagentur.de

Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) ist eine zentrale Institution der Cybersicherheitsforschung in Deutschland. Sie wurde im Juni 2020 als Inhouse-Gesellschaft des Bundes unter der gemeinsamen Federführung des Bundesministeriums der Verteidigung und des Bundesministeriums des Innern gegründet. Die Cyberagentur ist ein wesentlicher Bestandteil der Nationalen Sicherheitsstrategie, um zukünftige Herausforderungen im Bereich der Inneren und Äußeren Sicherheit zu beherrschen.

der Souveränität
von übermorgen

cyberagentur

Unsere Forschungsprogramme
www.cyberagentur.de/programme

Bundesministerium der Verteidigung
Bundesministerium des Innern



Gemeinsam stark!

Defence.NRW – Cluster für die Sicherheits- und Verteidigungsindustrie

Defence steckt in vielen Branchen.
Wir bringen sie zusammen.
Ob Biotechnologie, Photonik, Luft- und Raumfahrt, KI oder Maschinenbau – Defence.NRW vernetzt Unternehmen, Forschung, Bundeswehr und weitere Akteure aus dem Bereich Sicherheit und Verteidigung. So werden die Stärken in NRW gebündelt und Grundlagen für Innovationen im Verteidigungsbereich geschaffen.

Mehr als nur ein Netzwerk:
Beratung. Orientierung. Impulse.
Wir beraten zu Dual-Use-Produkten und Schlüsseltechnologien, geben einen Überblick über Fördermöglichkeiten, vermitteln Kontakte und schaffen mit eigenen Veranstaltungen, Matchmakings und Fachformaten Räume für Austausch und Kooperation. So werden aus Kompetenzen neue Ideen und Chancen für die SVI in NRW.

Das Cluster Defence.NRW wird betrieben durch die VDI Technologiezentrum GmbH und ist beauftragt durch das Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen. ■

DEFENCE.NRW

STAND-NUMMER B09

Beauftragt durch:

Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes Nordrhein-Westfalen

Clustermanager:
Dr. Lino Schneider-Bertenburg
E-Mail: defence.nrw@vdi.de
Web: defence.nrw



enclaive: The trust layer for the cloud(s)

Enclaive ist ein deutsches Deep-Tech-Sicherheitsunternehmen, das die führende postquanten-sichere, vertrauliche Multi-Cloud-Plattform entwickelt: die Vertrauensschicht, die jede Infrastruktur, jede Arbeitslast und jedes KI-System überprüfbar, vertrauenswürdig und vertraulich macht.

Die Einführung der Cloud in regulierten Branchen stockt aufgrund einer Frage: Wer kann Ihre Daten einsehen, während sie verarbeitet werden? Die enclaive Multi-Cloud-Plattform (eMCP) gibt darauf eine Antwort. Basierend auf Confidential computing hält die eMCP Daten, Code und KI-Workloads im Ruhezustand, während der Übertragung und – erstmals umfassend – auch während der Nutzung verschlüsselt: verschlüsselt sogar während der Verarbeitung, geschützt sogar vor dem Cloud-Anbieter, dem Hypervisor und den darunter liegenden Administratoren.

Unternehmen aus den Bereichen Finanzdienstleistungen, Gesundheitswesen, Versorgungswirtschaft, öffentlicher Sektor und Verteidigung stellen Anwendungen in den Clouds ihrer Wahl (öffentlich, privat, souverän oder vor Ort) bereit und betreiben diese mit minimalen Änderungen an bestehenden Architekturen. Die Plattform kombiniert vertrauliche virtuelle Maschinen und Kubernetes, während der Nutzung verschlüsselte Datenbanken, ein virtuelles HSM für souveränes Schlüsselmanagement („Bring and Hold Your Own Key"), Workload-Identitäts- und Zugriffsmanagement mit Fernattestierung („not attested, no key") sowie eine GenAI-Firewall für konforme Unternehmens-KI. Postquantenkryptografie schützt langlebige Daten vor „Harvest-now, decrypt-later"-Angriffen.

Das Ergebnis: nachprüfbare Datenhoheit und ein klarer Weg zur Einhaltung von NIS2, DORA, KRITIS und DSGVO – ohne komplettes Austauschen bestehender Systeme.

enclaive stellt die Confidential-Computing-Schicht der deutschen GovTech-Plattform bereit und wurde in die NATO-DIANA-2026-Kohorte aufgenommen. Das 2022 gegründete Unternehmen hat seinen Hauptsitz im Rhein-Main-Gebiet und eine Niederlassung in Berlin. Zu seinen Investoren zählen Join Capital, der Amadeus APEX Technology Fund und Auriga Cyber Ventures. Weitere Informationen unter enclaive.io. ■

enclaive

STAND-NUMMER B13

enclaive GmbH
Philipp-Keim-Straße 1
65719 Hofheim am Taunus
E-Mail: contact@enclaive.io
Web: www.enclaive.io

Souveräne Cybersecurity: Angriff und Verteidigung in einer Plattform

Die Enginsight GmbH ist ein deutscher Cybersecurity-Hersteller, der Behörden und öffentliche Verwaltungen ermöglicht ihre IT-Sicherheit selbst in die Hand nehmen: Angriffsfläche reduzieren, Bedrohungen früher erkennen, schneller reagieren.

Lokale Softwarehersteller sind wichtiger denn je, denn ...

- Digitale Souveränität braucht Substanz und keine leeren Versprechungen: Betrieb On-Premises, in der Private Cloud oder EU-Cloud — volle Datenhoheit, Rechtsrahmen Deutschland, kein CLOUD Act, keine Backdoors. Eigene Codebasis, entwickelt in Jena.

- Made in Germany, ISO 27001 zertifiziert: Kein Produkt-Zoo aus Einzellösungen, sondern eine Plattform für Schwachstellenerkennung, Monitoring, SIEM und automatisierte Reaktion.

- Regulatorik im Blick: Unterstützt bei NIS2, BSI IT-Grundschutz und KRITIS-Anforderungen — direkt über die Plattform oder gemeinsam mit unseren Partnern.

- Eigener Betrieb oder begleiteter Service: Betreiben Sie Ihr Security Operations Center selbst oder ergänzen Sie es um einen optionalen 24/7-Service für Managed Detection and Response (MDR) aus einem deutschen Cyber Defence Center.

- Transparent statt Blackbox: offene Erkennungslogik, offene Playbooks. Ihr Know-how bleibt bei Ihnen.

- AirGap-Fähigkeit für höchstes Vertrauen in kritischen Umgebungen

ENGINSIGHT

STAND-NUMMER B13

Enginsight GmbH
Leutragraben 1, 07743 Jena
Telefon: +49 36 41 27 14 966
E-Mail: hello@enginsight.com
Web: www.enginsight.com







Ready, when **intelligence matters**

When threats emerge, defense and public safety need resilient encryption and zero downtime. Ericsson's next-generation Mission Critical Networks deliver both.

Ericsson's high-performing, programmable networks provide connectivity for billions of people every day. For 150 years, Ericsson has pioneered communication technology, delivering mobile communication and connectivity solutions for service providers and enterprises around the world.

As a leader in the transformation of mission-critical communications, Ericsson delivers secure, resilient and high-performance mobile broadband networks built on 3GPP standards. Our Mission Critical Networks portfolio serves public safety, defense, utilities, rail and digital airspace with scalable, future-proof solutions. Our offering goes beyond connectivity; it is about enabling national resilience, operational excellence and long-term growth for customers and partners.

Discover next-generation technologies for modern defense and safety operations:

- **Ericsson Ultra Compact Core** bringing 5G core network capabilities into a highly portable, energy-efficient format, enabling secure and reliable connectivity in demanding environments, from temporary deployments to tactical edge scenarios. It supports rapid set-up, operational flexibility and mission continuity where robustness and mobility are essential.

- **Integrated Sensing and Communication (ISAC)** is a transformative innovation that turns mobile network infrastructure into systems that are capable of both communication and sensing movement in their surrounding environment. By analysing radio signal reflections, the system enables detection of objects such as aerial drones, at a nationwide scale and for a lower cost than comparable sensor systems.

ERICSSON

STAND-NUMMER F12

Ericsson GmbH
Prinzenallee 21, 40549 Düsseldorf, Germany
Phone: +49 211 5340
E-Mail: communications.germany@ericsson.com
Web: www.ericsson.com



Geoinformation ist die digitale Infrastruktur für die Gesamtverteidigung

Gesamtverteidigung braucht ein gemeinsames Lagebild: Wo befinden sich Kräfte und Ressourcen? Welche Verkehrswege und Infrastrukturen sind verfügbar, wo entstehen Engpässe, Risiken oder Abhängigkeiten? Dafür müssen militärische und zivile Informationen organisationsübergreifend verbunden und schnell in handlungsrelevante Erkenntnisse übersetzt werden.

Mit ArcGIS stellt Esri eine etablierte, sichere Geoinformationsplattform bereit. Sie verknüpft Geo-, Fach- und Echtzeitdaten räumlich und zeitlich und macht sie für Planung, Führung und Zusammenarbeit nutzbar.

Vom Geodatensatz zum gemeinsamen Lagebild

Für Landes- und Bündnisverteidigung, Gesamtverteidigung und OPLAN DEU ist ein aktuelles digitales Abbild des Einsatzraums entscheidend. ArcGIS integriert Daten zu Gelände, Verkehr, Infrastruktur, Logistik, Sensoren, Ressourcen und Lageentwicklungen. So entstehen digitale Lagebilder und Zwillinge für fundierte Entscheidungen.

Ob Host Nation Support und RSOM, militärische Mobilität, resiliente Logistik, Schutz kritischer Infrastruktur, Sensor-to-COP oder Geo-Intelligence: Der Raum verbindet alle Informationen.

Geo als Service – nicht als Insellösung

ArcGIS stellt Geodaten, Analysen und Dienste über Standards und Schnittstellen für Lagezentren, Planungssysteme, mobile Anwendungen sowie Führungs- und Informationssysteme bereit. Ein gemeinsamer Geo-Service-Layer verbindet Systeme, Organisationen und Datenquellen. KI unterstützt Analysen und Entscheidungen; über den offenen Standard MCP können auch externe KI-Anwendungen Funktionen der Plattform nutzen.

Bewährte Technologie im Partnerökosystem

Als standardisierte COTS-Basis lässt sich ArcGIS durch Systemintegratoren, Industriepartner, Behörden und Streitkräfte in bestehende Enterprise-IT-Architekturen integrieren. Sichere Betriebsmodelle, internationale Erfahrung, ein starker europäischer Footprint und lokale Partner unterstützen resiliente Einsatzszenarien. Geoinformation ist damit mehr als eine Karte: Sie ist digitale Infrastruktur für eine vernetzte, handlungsfähige Gesamtverteidigung. ■

esri Deutschland
THE SCIENCE OF WHERE

STAND-NUMMER F01

Esri Deutschland GmbH, Ringstr. 7, 85402 Kranzberg
E-Mail: info@esri.de
Telefon: +49 89 207 005 1200
Web: www.esri.de



FAST LTA

Resilienz beweist sich im Ernstfall: wenn ein Backup nach einem Ransomware-Angriff tatsächlich zurückspielt und ein Archiv Jahre später vor Gericht noch unverändert vorliegt. FAST LTA liefert seit über 20 Jahren genau diese Infrastruktur für Bundeswehr, Behörden und die Sicherheits- und Verteidigungsindustrie, entwickelt und gefertigt in München. Internes Wissen bleibt dabei nutzbar, ohne dass es das Haus verlässt.

Diese Zuverlässigkeit beginnt bei der Lieferkette. Wir entwickeln, fertigen und supporten ausschließlich in München, jede kritische Komponente lässt sich nachvollziehen, ohne Black-Box-Bauteile. Das erfüllt die Anforderungen an Lieferkettensicherheit aus NIS2 und § 30 BSIG bereits heute und ist auf den kommenden EU Cyber Resilience Act ausgelegt. Der Zugriff durch fremde Akteure entfällt strukturell.

Der physische Air Gap trennt Backups vollständig vom Netz, Hardware-WORM macht Archive unveränderlich und KPMG-zertifiziert, lokales KI-Inferencing respektiert die bestehenden Zugriffsrechte aus Active Directory.

Bundesarchiv und Deutsches Zentrum für Luft- und Raumfahrt vertrauen bereits auf FAST LTA. Silent Bricks, Silent Cubes und Silent AI setzen das um, im Einklang mit NIS2, KRITIS-Dachgesetz und BSI-Grundschutz.

Wir zeigen an unserem Stand, wie sich gesicherte Lieferkette und souveräne Infrastruktur in der Praxis verbinden. Kommen Sie gerne auf uns zu. ■

FAST LTA

STAND-NUMMER F09

FAST LTA GmbH
Tölzer Straße 1, 81379 München
Telefon: +49 89 89 047-0
E-Mail: info@fast-lta.de
Web: www.fast-lta.de



Human as **Sensor and Receiver**

Vernetztes Situationsbewusstsein und operative Handlungsfähigkeit

Unter „Human as Sensor and Receiver" verbinden INTEC, Balcony und NeuralTactics Echtzeitkoordination mit KI-Analyse von Emotionen und Verhaltensmustern zur Entscheidungsunterstützung. Die Lösung vernetzt Einsatzkräfte, Führungs- und Leitstellen, Behörden und Zivilpersonen über Organisations- und Zuständigkeitsgrenzen hinweg. Betroffene im Gefährdungsbereich werden informiert und aktiv eingebunden: Beobachtungen, Meldungen und Feedback fließen direkt in die operative Koordination ein.

So entsteht ein gemeinsames Situationsbewusstsein. Informationen aus dem Einsatzraum werden schneller verfügbar, bewertbar und handlungsrelevant. Die Lösung stärkt die Handlungsfähigkeit bei zeitkritischer Zusammenarbeit verschiedener Organisationen, Einheiten und Verantwortlicher.

Einsatzfelder sind Krisenmanagement, Evakuierung, Bevölkerungsschutz, kritische Infrastrukturen sowie Polizei, Bundeswehr und Spezialkräfte in dynamischen, komplexen Lagen.

Drei Partner. Eine integrierte Lösung.

INTEC übernimmt als Generalunternehmer Systemintegration und Lifecycle Management – von Hardware, Plattform und Komponenten über Training bis zur Weiterentwicklung.

Balcony stellt eine produktreife Plattform für Echtzeitkoordination und Geo-Messaging bereit. Sie erfasst Informationen ortsbezogen, teilt sie sicher und koordiniert Maßnahmen bidirektional – mit Zivilpersonen.

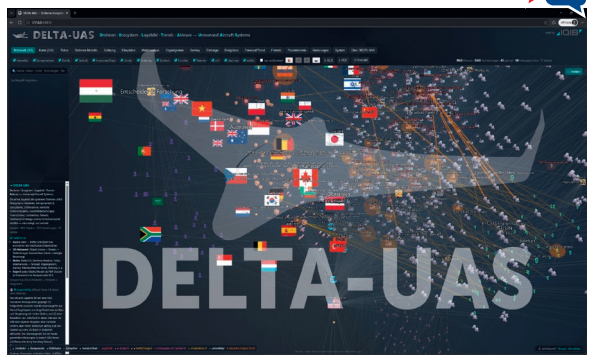
NeuralTactics ist ein deutsches KI-Unternehmen mit eigenen, lokal erprobten Modellen. Diese erkennen Emotionen und Verhaltensmuster aus Video, Text und Audio. Die Lösung unterstützt Einsatzleitungen, Sicherheitsbehörden, Bundeswehr, Spezialkräfte und kritische Infrastrukturen zivil und sicherheitsbezogen. ■

INTEC GROUP

STAND-NUMMER F06

INTEC Industrie-Technik GmbH
Taunusstraße 36, 80807 München
Telefon: +49 89 85 63 34 90
E-Mail: info@intec.group | Web: www.intec.group





Institut für **qualifizierende Innovationsforschung und -beratung** GmbH

Lösungen für morgen: Transformation gestalten | Resilienz stärken | Impact steigern

Die Resilienz des gesamtstaatlichen Sicherheitsökosystems hängt von schnellen, fundierten Entscheidungen in komplexen Situationen ab. IQIB schafft als innovativer Think and Do Tank mit Data Intelligence-Lösungen, KI-gestützte Analysen und integrierten Simulationen Klarheit in Bedrohungslagen. Interaktive Visualisierungen und dynamische Lagebilder legen die Grundlage für sicherheitsrelevante Entscheidungen.

Durch Datenrecherchen, Systemanalysen und den strukturierten Dialog zwischen Wissenschaft und Praxis schafft IQIB eine umfassende Wissensbasis über Silogrenzen hinweg und macht Zukunftsszenarien greifbar.

Besuchen Sie IQIB am Stand B04 und lernen Sie unsere Lösungen und Tools kennen:

Dynamische Lagebilder: IQIB analysiert im Pilotprojekt „DELTA-UAS" in Echtzeit das Entwicklungs-, Herstellungs-, Einsatzökosystem ziviler sowie militärischer Drohnen und stellt Finanzierungsströme und Beteiligungsverhältnisse in Firmengeflechten transparent dar. Dabei werden neben Netzwerkdarstellungen und GIS-Visualisierungen auch Patentdaten berücksichtigt und auf neue Trends untersucht. Drohnen-Sichtungen können mit GPS-Daten eingespeist und identifizieren werden. Neue Informationen fließen direkt in ein Tickersystem.

Smarte, resiliente Energiesysteme: Mit eigenen, praxisorientierten Ansätzen analysiert IQIB Bedrohungsszenarien wie zum Beispiel Cyberattacken auf zukünftige Energiesysteme. Das im Rahmen des Projekts ReMoDigital für das Bundeswirtschaftsministerium entwickelte Stress-Test-Tool ermöglicht eine dynamische Analyse der Resilienz von Digitalisierungslösungen in der Energiewende.

IQIB – Institut für qualifizierende Innovationsforschung und -beratung ist eine Tochtergesellschaft des Deutschen Zentrums für Luft- und Raumfahrt e. V. (DLR). ■

IQIB

STAND-NUMMER B04

IQIB - Institut für qualifizierende Innovationsforschung und -beratung GmbH
Kurgartenstr. 1, 53474 Bad Neuenahr-Ahrweiler
Ansprechpartner:
Ulrich Hofmann | ulrich.hofmann@iqib.de
Dr. Bert Droste-Franke | bert.droste-franke@iqib.de
Weitere Informationen: www.iqib.de



itWatch im Fokus

itWatch stellt patentierte IT-Sicherheit her – Made in Germany. Im Fokus stehen die netztrennende Datenschleuse mit Datenwäsche, der Schutz gegen Datendiebstahl (Data Loss Prevention - DLP), technische Vertrauensketten von der Tastatur bis zu den Daten und deren organisatorische Einbettung durch rechtsverbindliche Dialoge, Endpoint Security sowie Mobile Security und Verschlüsselung.

Die seit 1997 entwickelten Produkte zeichnen sich durch hohe Sicherheit aus, belegt durch den Einsatz in VS-NfD und GEHEIM klassifizierten Umgebungen (höher als CC EAL 4+ zu bewerten).

Unsere Cybersecurity-Lösungen für Sie

itWash | Netztrennende Datenschleuse mit Datenwäsche und Workflow: Daten von extern (Internet, Mail, mobilen Datenträgern) werden in sicherer, technisch entkoppelter Umgebung auf schädliche Elemente geprüft und von jeglichem potenziell schädlichen Code befreit. | *www.itWash.de*

CleanFile | Gewaschene Daten sicher an Drittsysteme übergeben

CodeIntegrity | Sicheres air-gapped Patchmanagement

itWESS | Die itWatch Enterprise Security Suite (itWESS) ist eine zentral gemanagte, mandantenfähige Endpoint Security mit EDR-Funktion. Sie verfügt über 14 Module mit Device Control, Application Control, Content Control, Print Control, Verschlüsselung, eingebautem SIEM, Risikomonitoring, benutzerverwendbare Sandboxen sowie Isolierung zur Härtung der Systeme. | *www.itWESS.de*

itWatch GmbH

STAND-NUMMER F15

itWatch GmbH, Aschauer Str. 30, 81549 München
Telefon: +49 89 62030100
Telefax: +49 89 620301069
E-Mail: info@itWatch.de
Web: www.itWatch.de





Elektromagnetische Überlegenheit durch integrierte Lösungen

Das elektromagnetische Spektrum ist eine strategische Ressource und entscheidend für Führungsfähigkeit, Lagebewusstsein und den Erfolg militärischer Operationen. In einem zunehmend komplexen und umkämpften Umfeld benötigen Streitkräfte durchgängige, sichere und interoperable Lösungen, mit denen sie das Spektrum planen, verwalten, überwachen und verteidigen können.

- LS telcom unterstützt Verteidigungsorganisationen entlang der gesamten EMSO-Wirkungskette. mySPECTRA for Defense ermöglicht das zentrale Management von Frequenzen, Systemen und Plattformen sowie die Koordination nationaler, multinationaler und streitkräftegemeinsamer Frequenzplanungen.

- SPECTRAemo unterstützt die taktisch-operative Funkeinsatzplanung mit Abdeckungsprognosen, Interferenzanalysen und Funktionen zur Frequenzoptimierung.

- LS OBSERVER überwacht das elektromagnetische Spektrum kontinuierlich, erkennt, analysiert und lokalisiert ungewöhnliche oder nicht autorisierte Signale. Land- und drohnengestützte Komponenten erweitern die Möglichkeiten zur Funkaufklärung, Drohnenerkennung und Bewertung eigener Kommunikationsnetze.

Die softwaredefinierten Lösungen von LS telcom lassen sich in bestehende IT-, C2-, BMS- und EW-Systemlandschaften sowie in Funkgeräte und Hardware unterschiedlicher Hersteller integrieren. Darüber hinaus realisiert das Unternehmen kundenspezifische, schlüsselfertige Systeme für geschützte Fahrzeuge, mobile Shelter, maritime Einheiten und UAV-Plattformen.

Mit mehr als 30 Jahren Erfahrung ist LS telcom ein verlässlicher Partner für Streitkräfte und Sicherheitsorganisationen weltweit. Treffen Sie unsere Experten beim AFCEA Bonner IT-Dialog und sprechen Sie mit uns über Ihre operativen Anforderungen.

LS telcom Smart Spectrum Solutions

STAND-NUMMER B02

LS telcom AG
Im Gewerbegebiet 31-33, 77839 Lichtenau
Telefon +49 72 27 95 35 600
E-Mail: info@lstelcom.com
Web: www.lstelcom.com



Das Materna Headquarter in Dortmund

Digitale Resilienz mit Materna

Die sicherheitspolitische Zeitenwende verändert auch die Anforderungen an die Digitalisierung von Staat, Verwaltung und Streitkräften. Gefragt sind Lösungen, die im Alltag funktionieren und in Krisen belastbar bleiben: souveräne IT-Architekturen, geschützte Datenräume, resiliente Infrastrukturen und ein sicherer Austausch sensibler Informationen.

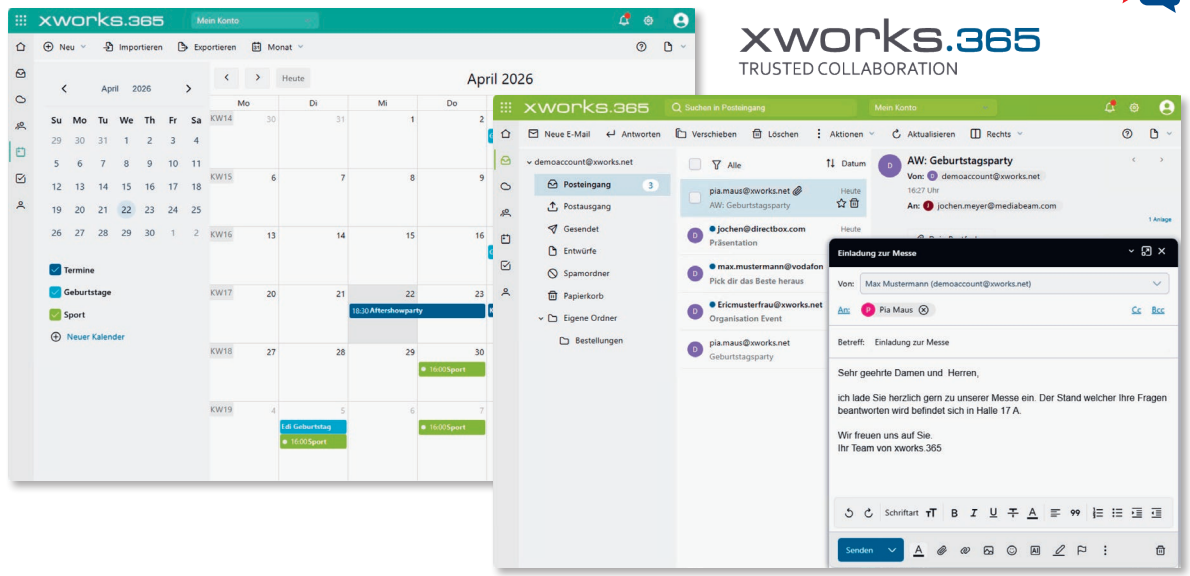
Materna wurde 1980 in Dortmund gegründet und ist bis heute ein inhabergeführtes Familienunternehmen. Die Gruppe beschäftigt weltweit mehr als 4.500 Mitarbeitende an über 40 Standorten und begleitet seit vielen Jahren öffentliche Auftraggeber bei der digitalen Transformation. Den Bereich Defence baut Materna gezielt weiter aus: Im Mittelpunkt stehen praxiserprobte Lösungen für Führungsfähigkeit, Lagebilder, sichere Kommunikation, Logistik und den Schutz kritischer Infrastrukturen.

Ein Schwerpunkt liegt auf der Verbindung von ziviler und militärischer Handlungsfähigkeit. Moderne Logistik- und Verkehrssysteme, digitale Planungswerkzeuge und KI-gestützte Verfahren können dazu beitragen, Abläufe nachvollziehbarer zu machen, Versorgungswege zu sichern und Entscheidungen unter Zeitdruck besser vorzubereiten. Auch der digital unterstützte Schutz von Liegenschaften gewinnt weiter an Bedeutung.

Als Unternehmen in Privatbesitz steht Materna für langfristige Partnerschaften, kontinuierliche Investitionen in Kompetenzen „Made in Germany“ und verlässliche Umsetzung in sicherheitskritischen Umgebungen. Beim Bonner IT-Dialog zeigt Materna, wie digitale Souveränität, Resilienz und Defence-Kompetenz zusammenwirken können, um staatliche Handlungsfähigkeit nachhaltig zu stärken. ■

STAND-NUMMER S13

Materna Information & Communications SE
Robert-Schuman-Straße 20, 44263 Dortmund
E-Mail: sales@materna.group
Web: www.materna.de/bw



xworks.365
TRUSTED COLLABORATION

Digitale Zusammenarbeit. Souverän, sicher und aus Deutschland.

Moderne digitale Arbeitsplätze müssen einfach nutzbar, sicher und zuverlässig betreibbar sein. Gleichzeitig gewinnen Datenschutz, digitale Souveränität und die Unabhängigkeit von einzelnen Plattformanbietern erheblich an Bedeutung.

Dafür entwickelt und betreibt mediaBEAM xworks.365 – eine modulare Plattform für Kommunikation, Zusammenarbeit und digitale Prozesse. Sie verbindet E-Mail, Kalender, Kontakte, Aufgaben, Cloud-Speicher, Chat, Videokonferenzen, Notizen, Teamräume und Workflows in einer gemeinsamen Arbeitsumgebung. Über REST-APIs lassen sich Fachverfahren, Identitätsdienste und weitere Anwendungen integrieren.

xworks.365 wird in Deutschland entwickelt und in deutschen Rechenzentren betrieben. Die Plattform eignet sich für Unternehmen und öffentliche Organisationen ebenso wie für IT-Dienstleister und Telekommunikationsanbieter. Sie kann als Managed Service, in einer dedizierten Umgebung und projektabhängig auch innerhalb der eigenen Infrastruktur bereitgestellt werden. Mandantenfähigkeit, Single Sign-on, automatisierte Provisionierung und umfassende Individualisierung unterstützen unterschiedliche Betriebsmodelle. Partner können xworks.365 vollständig unter eigener Marke anbieten.

mediaBEAM entwickelt und betreibt seit 1999 hochverfügbare Kommunikations- und Collaboration-Plattformen. Diese Verbindung aus Softwareentwicklung und praktischer Betriebserfahrung prägt xworks.365: eine souveräne Plattform für den zuverlässigen Einsatz im Alltag.

Besuchen Sie uns an Stand F10. Wir sprechen gerne über Ihre Anforderungen und einen realistischen Einstieg. ■

STAND-NUMMER F10

mediaBEAM GmbH
Erhardstraße 3, 48683 Ahaus
Telefon: +49 25 61 695-0
E-Mail: contact@mediabeam.com
Web: mediabeam.com | xworks.net





Die Mitte trägt die Krise

Orchestrierung, Eigenleistungsfähigkeit und Wiederverwendung als Beitrag zur Resilienz

Sicherheitsrelevante Lagen entscheiden sich selten an der Technik. Lagebilder, Fachverfahren und Kommunikationssysteme sind vorhanden. Was fehlt, ist die verbindende Ebene, auf der aus Lage ein Urteil, aus Urteil eine Entscheidung und aus Entscheidung koordinierte Wirkung wird. Genau diese Orchestrierung ist der Kern von Pega.

Führen statt verwalten

Regeln und Decisioning sind eingebaut, nicht angeflanscht. Case Management hält fest, wo ein Vorgang steht, wer zuständig ist und was als Nächstes geschieht. Prozesse laufen medienbruchfrei über Ressort- und Systemgrenzen, Prioritäten bleiben steuerbar, jeder Schritt ist revisionssicher dokumentiert. Bestehende Kernsysteme werden eingebunden, nicht ersetzt.

Eigenleistungsfähigkeit als Resilienzfaktor

Ein Verfahren, das sich erst nach Monaten ändern lässt, hilft in der Lage nicht. Mit Low Code und No Code passen Fachverantwortliche Abläufe innerhalb klarer Leitplanken selbst an, während Rollen, Rechte und Sicherheitsstandards kontrolliert bleiben. Anpassung geschieht in Tagen, nicht in Vergabezyklen.

Wiederverwenden statt neu bauen

Die objektorientierte, modellbasierte Architektur macht Wiederverwendung zum Prinzip: Prozesse werden konfiguriert statt programmiert, einmal gebaute Bausteine in weiteren Behörden und Anwendungsfällen erneut genutzt und lageangepasst variiert. Diesem Anspruch folgt Pega seit über 40 Jahren unter dem Leitgedanken „Build for Change“. Weil vieles ab Werk vorliegt, entstehen erste tragfähige Ergebnisse in Wochen statt Jahren.

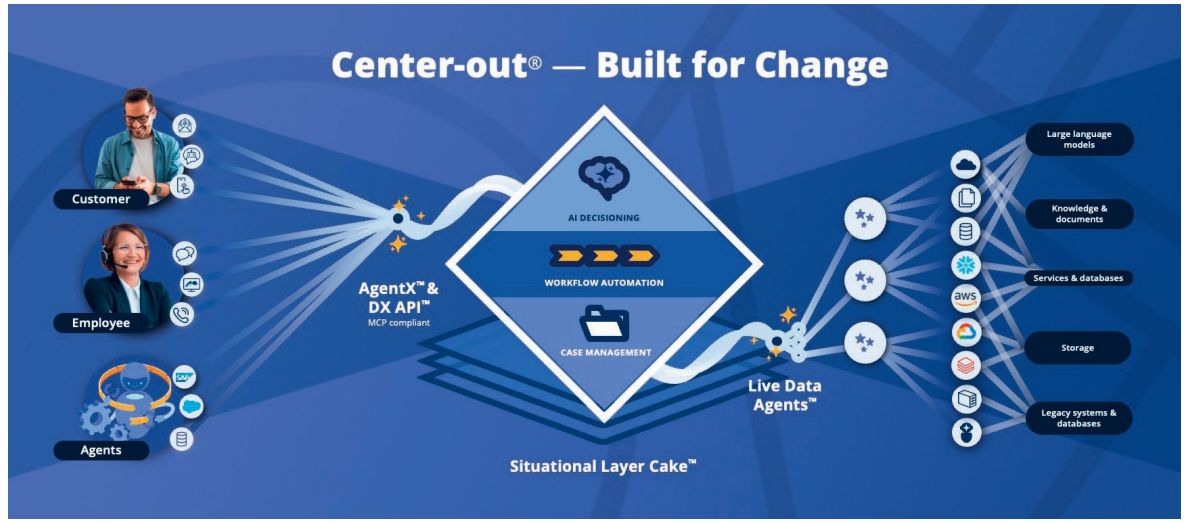
PEGA®

STAND-NUMMER
F11

Verbindung schaffen

Schon heute ist Pega an mehreren Enden der zivil-militärischen Zusammenarbeit im Einsatz. Jetzt gilt es, mit Ihnen die Verbindung anzudenken und die Wirkung zu erhöhen. Für einen ersten Schritt muss selten neu beschafft werden. Kommen Sie an Stand F11 vorbei.







Fortsetzung »»



Der Agent denkt, der Workflow lenkt

Warum die Zukunft KI-Agenten braucht – und eine Ebene, die sie steuert

Die nächste Stufe der Handlungsfähigkeit ist ohne KI nicht erreichbar. Agenten lesen Dokumente, erkennen Zusammenhänge, bereiten Entscheidungen vor und übernehmen Schritte. Damit daraus belastbare Fähigkeit statt Experimente wird, gilt es, die Power von KI-Agenten mit der Verlässlichkeit von Workflows zu verbinden.

Agenten mit klarer Rolle

Konversations-, Wissens-, Automations- und Workflow-Design-Agenten wirken an verschiedenen Stellen eines Vorgangs: von der Aufnahme über Prüfung und Bearbeitung bis zur Lösung. Der Agent denkt, der Workflow lenkt, und Case Management hält fest, was geschehen ist.

Steuerung entscheidet über Erfolg

Arbeiten mehrere Agenten an einem Prozess, entscheidet die Steuerung. Sie legt fest, welche Rolle jeder Agent innehat, wie Daten fließen und wo Ergebnisse geprüft werden, samt Regelungen für Störfälle und Situationen mit menschlichem Zutun. Sind diese Vorgaben in den Agenten selbst verankert, drohen Unübersichtlichkeit, Widersprüche und hoher Wartungsaufwand. Eine eigene Orchestrierungsebene schafft Struktur.

Human in the Lead

Für kritische Entscheidungen genügt ein nachgelagerter Human in the Loop nicht. Notwendig ist ein Human in the Lead, der den Handlungsspielraum der KI vorab absteckt und an definierten Interventionspunkten eingreift. Was orchestriert läuft, ist zugleich messbar: Prozessdaten und Audit-Trail entstehen im Regelbetrieb und zeigen nach der Übung, wo die Kette gerissen ist.

Belastbar über Organisationsgrenzen

Übergreifende Zusammenarbeit trägt nur, wenn jede Organisation ihren Anteil und ihre Grenzen kennt. Sicherheit, Betrieb und Zertifizierungen bringt die Plattform mit. Der Maßstab liegt weniger auf maximaler Automatisierung als auf orchestrierten Entscheidungsprozessen. Nur so bleibt der Staat auch im Krisenfall handlungsfähig. ■



PEGA®

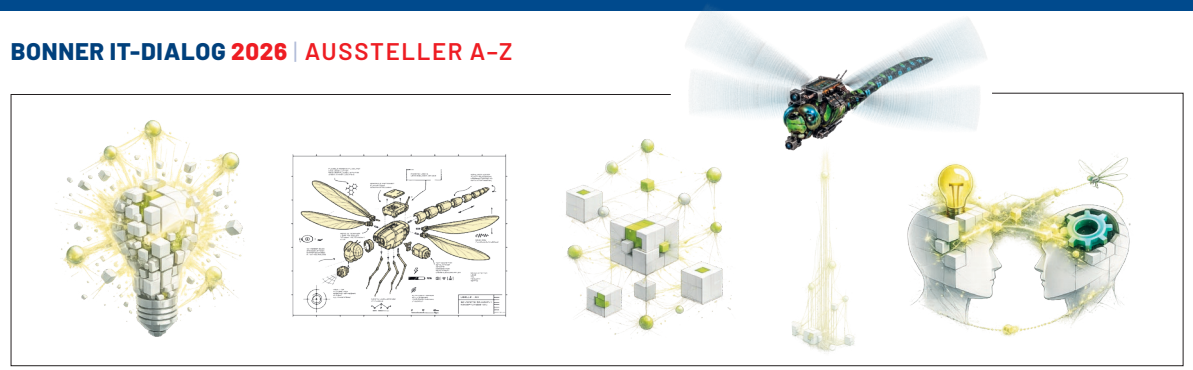
STAND-NUMMER F11

Pegasystems GmbH | Weisses Quartier,
St. Martin Straße 74, 81541 München
Ansprechpartner Defense:
Fabian Kretschmer
(Advisor & Strategic Client Executive)
E-Mail: fabian.kretschmer@pega.com
Web: www.pega.com

ÜBER PEGASYSTEMS

Bekannt ist Pegasystems für über vier Jahrzehnte Innovationstätigkeit. Das 1983 von CEO Alan Trefler gegründete Unternehmen wird bis heute von seinen Ideen geprägt. Mehr als 5.000 Mitarbeitende weltweit, patentierte Softwareinnovationen und ein robustes Partnernetzwerk bilden das Fundament.

Pegasystems bietet eine Plattform, mit der Unternehmen geschäftskritische Prozesse steuern und weiterentwickeln können. KI und eine bewährte Architektur sorgen für flexible, skalierbare Abläufe – mit dem Ziel, die Softwareentwicklung so zu gestalten, dass Kundenprozesse optimal laufen. Weltweit vertrauen führende Unternehmen auf Pegasystems, um Kundenbindung zu stärken, operativ effizienter zu werden und Altsysteme zu modernisieren.



Schnittstelle zwischen Mensch und Technologie

Die Plusbringer erschaffen die Schnittstelle zwischen Mensch und Technologie für die Herausforderungen kritischer Infrastrukturen. Wir verbinden Interface, System und Datenfluss zu zuverlässigen Lösungen. Sicher, beherrschbar und bereit für Ihren realen Einsatz.

Ihr Plus. Wir. Die Plusbringer begleiten ihre Kunden persönlich und lösungsorientiert durch den gesamten Entwicklungsprozess. Gemeinsam präzisieren sie Anforderungen und übersetzen diese in konkrete, unternehmensgerechte Lösungen.

Ein Team. Eine Mission. Schwäbisch. Bodenständig. Verlässlich. Interdisziplinäre Teams entwickeln intuitive, sichere und zuverlässige Systeme für Defense, Automotive, Medical Devices und den Public Sector – für kritische Situationen.

Vier Standorte. Fachübergreifend verbunden. In Dettingen an der Erms, Kassel, Erlangen und Berlin bündeln die Plusbringer ihre Kompetenzen. Gestaltung, Bedienkonzept, Software, Systemarchitektur, Integration und Erprobung greifen nahtlos ineinander. So entstehen INNOVATIVE MISSION CRITICAL SYSTEMS, die sicher beherrschbar und zuverlässig bedienbar bleiben. Alles, was du brauchst.

Nichts, was du nicht brauchst. Die Plusbringer verbinden Benutzeranforderungen mit technischen Rahmenbedingungen, integrieren Komponenten und stellen Informationen schnell und situationsgerecht bereit.

In fünf Schritten von der Idee zur Serienreife.

» Im INNOVATION LAB nehmen Ideen in kreativer Zusammenarbeit Gestalt an.

» Beim FEATURE PROTOTYPING entstehen daraus erlebbare Funktionen, die gezielt geprüft und validiert werden.

» Die SYSTEMENTWICKLUNG UND INTEGRATION verbindet Serienkomponenten zu robusten, skalierbaren und intelligent vernetzten Gesamtsystemen.

» Das SYSTEM TESTING prüft und validiert komplexe Systeme unter realistischen Bedingungen – von der Integration bis zur Serienabnahme.

» Die TECHNISCHE BERATUNG macht kritische Anforderungen verständlich und übersetzt sie in klare, zukunftsfähige und hochverfügbare Lösungen.

Lassen Sie Ihrer Idee freien Lauf. Besuchen Sie uns am Stand B03. Wir freuen uns auf einen innovativen Austausch mit Ihnen. ■

die Plusbringer

STAND-NUMMER B03

die Plusbringer GmbH
Kiefernweg 15, 72581 Dettingen
Telefon: +49 71 23 37 410 50
info@dieplusbringer.de
www.dieplusbringer.de/libelle



True Spectrum Dominance in all domains

Rohde & Schwarz is one of the world's leading suppliers and a reliable partner for armed forces, security authorities and industry partners.

The globally operating technology group develops, designs, manufactures and implements turnkey end-to-end solutions for secure communications, SIGINT/EW, intelligence, CUAS, test & measurement, and security. Its solutions and capabilities support multi-domain operations by ensuring true spectrum dominance in all domains and along the complete signal chain. ■

ROHDE&SCHWARZ
Make ideas real

STAND-NUMMER S01

Rohde & Schwarz Vertriebs-GmbH
Sicherheit und Verteidigung
Frankfurter Straße 720–726, 51145 Köln
Telefon: +49 2203 8077-12
E-Mail: vertrieb-sv@rohde-schwarz.com
Web: www.rohde-schwarz.com



Palaschka Parchomenko Curvello, Head of Sales Projects, Dirk Kotala-Wilhelm, Head of Product Sales, Thomas Wolf, Geschäftsführer

Moderne Verwaltungs-IT braucht mehr als Software

Sie braucht einen Partner, der versteht, worauf es ankommt: komplexe Fachlichkeit, gewachsene IT-Landschaften und die Menschen, die täglich damit arbeiten. Scopeland Technology verbindet dieses Verständnis mit moderner Technologie. Seit mehr als 25 Jahren entwickeln wir Fachverfahren für Bundes- und Landesbehörden – von Liegenschaften und Logistik über Personal bis zu Genehmigungen.

Dabei denken wir nicht in Standardlösungen: Wir entwickeln neu, wo bestehende Verfahren an Grenzen stoßen, und schaffen Anwendungen, wo bisher keine passende Lösung existiert. Mit Low-Code entstehen individuelle Fachverfahren schnell, kontrolliert und wirtschaftlich – und damit nicht nur Anwendungen mit KI, sondern auch KI-Anwendungen; KI dort, wo sie Mehrwert bringt.

SCOPELAND reicht von der weißen bis in die grüne IT. Bestehende Systeme müssen nicht ersetzt werden: Es entstehen Schnittstellen und Anwendungen, die sich in vorhandene IT-Landschaften integrieren und mit ihnen weiterentwickeln – auch bei besonders hohen Anforderungen. Mit jedem Projekt wird es einfacher: Ist die technologische Basis einmal gewählt, baut jedes weitere Fachverfahren darauf auf – zügig und wirtschaftlich, statt jedes Mal von vorn. Ändern sich Gesetze, Zuständigkeiten oder Prozesse, setzen wir das modellgetrieben schnell um – ohne lange Releasezyklen.

Was uns ausmacht: Wir sind nicht nur Produkthersteller, sondern Entwicklungspartner – von der ersten Idee bis zum laufenden Betrieb. Mehr als 500 große Verwaltungs-IT-Projekte belegen das: bewährt in Bund und Ländern, von BAMF und Bundesnetzagentur bis zu den Feuerwehren Berlin und Hamburg.

So wird digitale Handlungsfähigkeit machbar – mit Fachverfahren, die sich an der Realität orientieren und mit ihr weiterentwickeln. ■

SCOPELAND® TECHNOLOGY

STAND-NUMMER B03

Scopeland Technology GmbH
Düsterhauptstraße 39-40, 13469 Berlin
Telefon: +(49) 30 209 670-0
E-Mail: sales@scopeland.de
Web: www.scopeland.de



Secure. Reliable. **Trusted.**

SCOTTY ist eine Technologieplattform für sichere, zuverlässige und hochverfügbare Kommunikation in sicherheitskritischen Umgebungen. Das System wird von zivilen und militärischen Organisationen weltweit genutzt, um unter allen Umständen Informationen auszutauschen und ein gemeinsames Lagebild zu schaffen. Das Hauptziel von SCOTTY ist es, Informations- und Kommunikationssysteme bereitzustellen, die auch unter schwierigen Bedingungen funktionieren. Dabei können Daten über Kabel-, Funk- oder Satellitennetzwerke übertragen werden und sind für Einsätze an Land, auf See und in der Luft geeignet.

Ein zentrales Element ist das gemeinsame Lagebild (Common Operational Picture – COP). Dieses ermöglicht es Entscheidungsträgern, Informationen aus verschiedenen Quellen – etwa Kameras, Sensoren oder Einsatzkräften – zusammenzuführen und in Echtzeit auszuwerten. Dadurch können schneller fundierte Entscheidungen getroffen werden.

Wichtige Produkte und Technologien:

SCOTTY Extended Connect: Echtzeit-Kommunikation zwischen Einsatzkräfte und Entscheidern/Integration von Video- und Datenströmen über verschiedene Netzwerke

SCOTTY Silentio: Abhörsichere Besprechungsräume („Raum-im-Raum")/Schutz vor akustischen und elektromagnetischen Abhörversuchen

SCOTTY Una Omnia: Modulares Kommunikationssystem/Anpassbar mit Komponenten wie Video-Codecs, Funkmodulen, Netzwerk-Switches oder CPU-Boards

SCOTTY Video Conference: Sichere Videokonferenzlösungen für klassifizierte Umgebungen/Kommunikation bis zur Sicherheitsstufe „NATO-geheim" möglich

SCOTTY Multimodal Connectivity: Resiliente Netzwerke mit redundanten Knoten/Automatische Übernahme bei Ausfall einzelner Komponenten

SCOTTY Secure End-Point: Sichere Endgeräte für Daten-, Video und Sprachkommunikation/Verschlüsselte Netzwerkanbindung und Integration von Sensoren oder Kameras ■

SCOTTY

STAND-NUMMER B14

SCOTTY Group Austria GmbH
Teslastraße 4
8074 Raaba-Grambach, Österreich
E-Mail: j.kalcher@scotty.group
Telefon: +43 316 409 426



MINERVA – die neue deutsche SIEM-Lösung der sedevo (Teil der EWERK Gruppe)

Hybride Bedrohungen, Cyberangriffe auf kritische Infrastrukturen und wachsender regulatorischer Druck durch NIS2 und BSIG verlangen nach einer Sicherheitsarchitektur, die volle Lagehoheit garantiert – ohne Abhängigkeit von nicht-europäischen Cloud- oder Software-Anbietern. Wer auf US-Hyperscaler-Technologie setzt, riskiert Datenzugriffe durch CLOUD Act oder FISA 702 – ein Kontrollverlust, den Streitkräfte und Sicherheitsbehörden sich nicht leisten dürfen.

sedevo begegnet dieser Herausforderung mit MINERVA, der neuen deutschen SIEM-Lösung – vollständig quelloffen entwickelt und in deutschen Rechenzentren betrieben. Der Name ist Programm: Wie die Göttin der Weisheit, der taktischen Kriegsführung und Hüterin des Wissens verschafft MINERVA den entscheidenden Lageüberblick – durchgängige Transparenz über Bedrohungen, souveräne Datenhoheit und Nachvollziehbarkeit für Kommandostrukturen und Auditoren gleichermaßen.

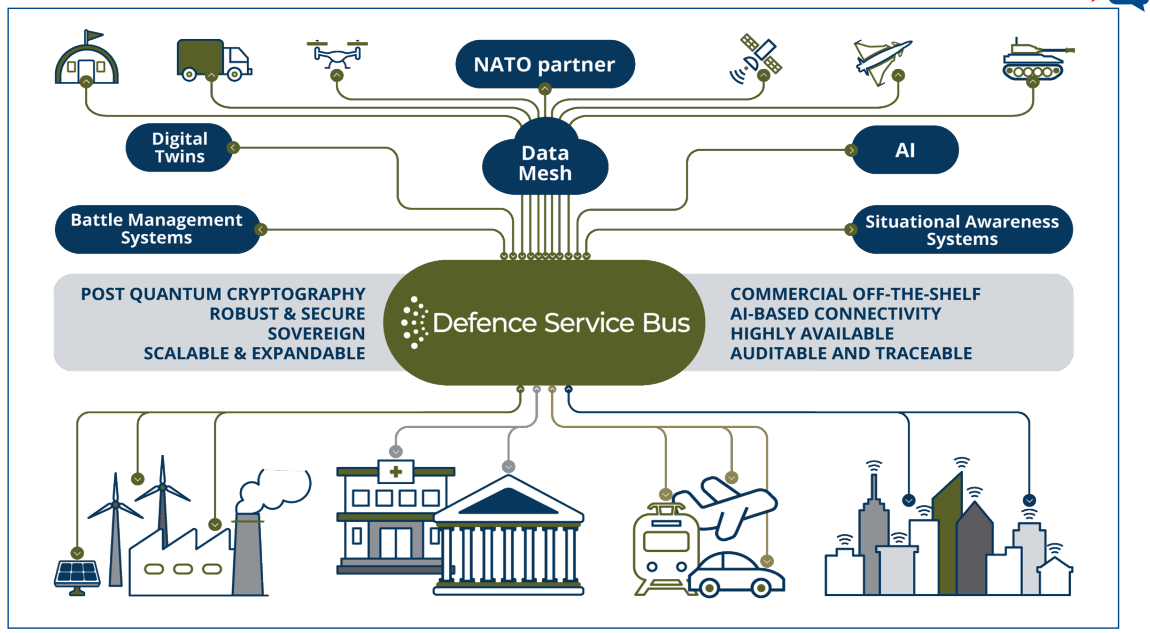
Ergänzt wird MINERVA durch ein breites Bündel souveräner Cyber-Security-Services: Managed EDR, Identity- und Access-Management, Schwachstellen- und Angriffsflächenmanagement sowie Supply-Chain- und KI-Governance-Lösungen – realisiert mit ausgewählten deutschen und europäischen Technologiepartnern.

Das Ergebnis: ein Sicherheitsportfolio für Bundeswehr und innere Sicherheit, das Gefechtsfeld- und Behördenanforderungen an digitale Souveränität erfüllt – skalierbar vom Einstieg bis zum vollständig verwalteten Security Operations Center. ■

sedevo

STAND-NUMMER F14

Sedevo – Teil der EWERK Group Services GmbH
Brühl 24, 04109 Leipzig
Telefon: +49 341 426 49-99
E-Mail: info@ewerk.com
Web: www.ewerk.com



Resilienz braucht **Interoperabilität**

Sicherheit und Handlungsfähigkeit entstehen dort, wo Informationen zuverlässig über Organisations-, System- und Zuständigkeitsgrenzen hinweg verfügbar sind. Genau hier setzt soffico an.

Als inhabergeführtes deutsches Softwareunternehmen steht soffico für technologische Souveränität und verlässliche Leistungserbringung aus Deutschland. Von der Softwareentwicklung über Beratung und Implementierung bis zu Betrieb und Support werden sämtliche Leistungen in Deutschland erbracht.

Mit dem Defence Service Bus (DSB) schafft soffico eine herstellerneutrale Integrations- und Governance-Schicht für sicherheitskritische Datenflüsse. Der DSB verbindet bestehende Führungs-, Lagebild-, Fach- und Sensorsysteme, ohne diese zu ersetzen. Unterschiedliche Schnittstellen, Protokolle und Datenmodelle werden integriert, Informationen strukturiert bereitgestellt und Datenflüsse sicher und nachvollziehbar gesteuert.

Gleichzeitig unterstützt der DSB die Überführung verteilter Informationen in staatlich beherrschte Data-Mesh-Strukturen – im zivilen wie im militärischen Umfeld. Daten werden damit aus proprietären Silos herausgelöst, fachlich strukturiert, mit klaren Zugriffs- und Governance-Regeln versehen und für eine souveräne Weiterverwendung verfügbar gemacht. Dies schafft zugleich eine belastbare Datengrundlage für den kontrollierten und regulierten Einsatz von KI.

Damit adressiert der DSB eine zentrale Voraussetzung für Resilienz: Nicht einzelne Systeme entscheiden, sondern die Fähigkeit, vorhandene Informationen souverän, interoperabel und organisationsübergreifend nutzbar zu machen. ■

soffico

STAND-NUMMER F03

Dr. Sebastian Heger *(Produktmanagement)*
E-Mail: sebastian.heger@soffico.de
Telefon: +49 151 15 58 30 97
Bernd Hellinger *(Director Defence)*
E-Mail: bernd.hellinger@soffico.de
Telefon: +49 152 225 444 79



Prädiktive Lagebilder Hybrid Threat Intelligence durch Osavul, Splunk und Cisco

Angesichts der Zunahme hybrider Bedrohungen – einer Kombination aus Cyberangriffen, Spionage und Desinformation – reicht reaktive Sicherheit nicht mehr aus. Im Rahmen eines souveränen, integrierten Ökosystems bieten wir der Bundeswehr, Organisationen der Nationalen Sicherheit und Unternehmen mit kritischer Infrastruktur die erforderlichen Technologien zur Herstellung des notwendigen Informationsvorsprungs.

Strategische Informationshoheit: Die Kooperation von Osavul, Splunk und Cisco fusioniert OSINT-Daten mit internen, hochsensiblen Informationen. So verwandeln wir fragmentierte Signale in präzise, entscheidungsreife Lagebilder.

Unsere Vorteile für die Bundeswehr: Souveräne „AI-in-a-Box“: Unsere Lösung ist für höchste Sicherheitsansprüche konzipiert. Die OnPrem-Bereitstellung mittels AI-POD in einer Secure AI Factory ermöglicht die Verarbeitung klassifizierter Daten bei maximaler eigener Datenhoheit.

Augmented SOC & Observability: Durch die Symbiose aus Splunk-SIEM und Full-Stack Observability erhalten Sie eine lückenlose Sichtbarkeit über alle IT/OT-Umgebungen hinweg. Wir erweitern die klassische Security um hybride Risikoprognosen und erkennen Angriffsvektoren in Echtzeit.

Automatisierte Verteidigung: Durch die Kopplung mit Cisco-Cybersecurity-Lösungen werden Gegenmaßnahmen nahtlos eingeleitet. Ob Schutz kritischer Infrastrukturen oder militärischer Missionen: Wir minimieren Reaktionszeiten durch KI-gestützte Playbooks.

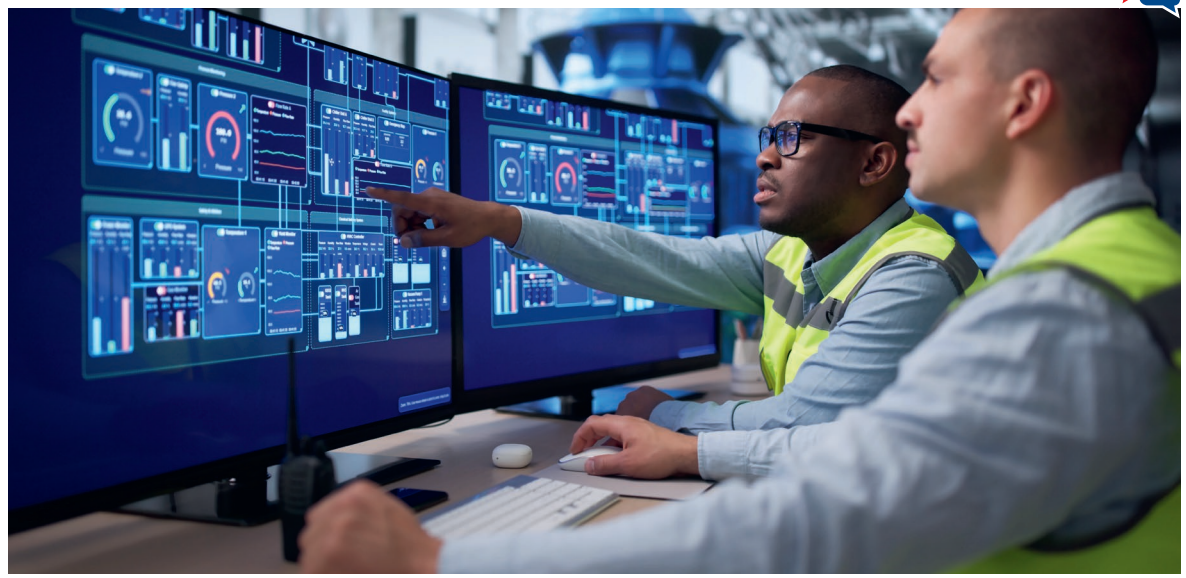
Vom Reagieren zum Agieren: Wir identifizieren Angriffsmuster (Wer, Wie, Wo, Wann), bevor der Schaden entsteht. Das entlastet das Personal, ermöglicht ein einheitliches Lagebild für J2/J6-Stäbe und schafft die Basis für präemptive Maßnahmen.

Mit der kombinierten Stärke von One Cisco und Osavul schaffen wir eine Brücke zwischen digitaler Infrastruktur und strategischer Analyse. Wir schützen, was zählt – souverän, sicher und mit entscheidendem Informationsvorsprung. ■

splunk> a CISCO company

STAND-NUMMER F13

Cisco Systems GmbH
Parkring 20, 85748 Garching
Telefon: +49 151 4221 4987
E-Mail: pstrassb@cisco.com
Web: www.splunk.com



SThree ist die globale Workforce Consultancy für MINT

Seit 1986 bringen wir Unternehmen mit hoch qualifizierten Spezialistinnen und Spezialisten aus IT, Engineering, Life Sciences und weiteren technischen Disziplinen zusammen.

Unser Angebot reicht von strategischer Workforce-Beratung über die Vermittlung von Fachkräften in Festanstellung, Arbeitnehmerüberlassung und Freelance-Modellen bis hin zu projektbasierten Lösungen mit klarer Ergebnisverantwortung. Mit mehr als 2.700 Mitarbeitenden in 34 Büros und elf Ländern verbinden wir globale Reichweite mit fundierter lokaler Marktkenntnis. So schaffen wir flexiblen Zugang zu der Expertise, die Unternehmen für ihre Transformation und ihr nachhaltiges Wachstum benötigen.

SThree im Bereich Defense & Public Sector
SThree schafft Zugang zu der Expertise, die sicherheitskritische Projekte voranbringt.

Als spezialisierte STEM Workforce Consultancy unterstützt SThree öffentliche Institutionen, Unternehmen der Verteidigungsindustrie sowie Beratungs- und IT-Dienstleister mit Defence-Fokus. Unsere Expertise reicht von Cybersecurity, Cloud, Softwareentwicklung und SAP über Data und AI bis zu Systems Engineering, Fertigung, Qualitätssicherung, Compliance und Programmmanagement.

SThree verfügt über Erfahrung in sicherheitskritischen Projekten und unterstützt sowohl bei der Auswahl geeigneter Spezialistinnen und Spezialisten als auch bei den erforderlichen Eignungs- und Überprüfungsprozessen. Unternehmen und Institutionen erhalten umfassend Zugang zu einem breiten STEM-Netzwerk, ohne auf spezialisierte Marktkenntnis verzichten zu müssen. ■

Ein Partner. Flexible Modelle. Die richtige Expertise für sicherheitsrelevante Projekte.

s|three

STAND-NUMMER F04

Querstraße 7
60322 Frankfurt am Main
Web: www.sthree.com





SUSE: **Digitale Souveränität** als Basis für mehr Resilienz

SUSE wurde 1992 in Nürnberg gegründet und ist heute Europas größter Anbieter von Open Source Software. Seit mehr als drei Jahrzehnten arbeiten wir eng mit der weltweiten Entwickler-Community zusammen und verwandeln Innovationen in unternehmenstaugliche Lösungen für geschäfts- und missionskritische Umgebungen. Die souveräne und offene Infrastruktur von SUSE bildet die Grundlage für unterschiedlichste digitale Anwendungen – von klassischen Enterprise-Workloads bis hin zu Private AI.

Mit Lösungen für Linux, Cloud Native, Edge Computing und KI unterstützt SUSE Unternehmen und öffentliche Auftraggeber dabei, moderne IT-Infrastrukturen aufzubauen und sicher zu betreiben. Unsere Lösungen lassen sich in hybriden Umgebungen einsetzen – von On-Premises-Rechenzentren über Multi-Cloud-Umgebungen bis zu dezentralen Standorten – und gewährleisten durchgängige Transparenz und zertifizierte Sicherheit.

Offene Standards und die Unterstützung heterogener IT-Landschaften sorgen für Wahlfreiheit und ermöglichen es Organisationen, die Kontrolle über ihren gesamten Technologie-Stack zu behalten. SUSE bietet beispielsweise die einzige Plattform, um jede Linux- und Kubernetes-Distribution zu verwalten.

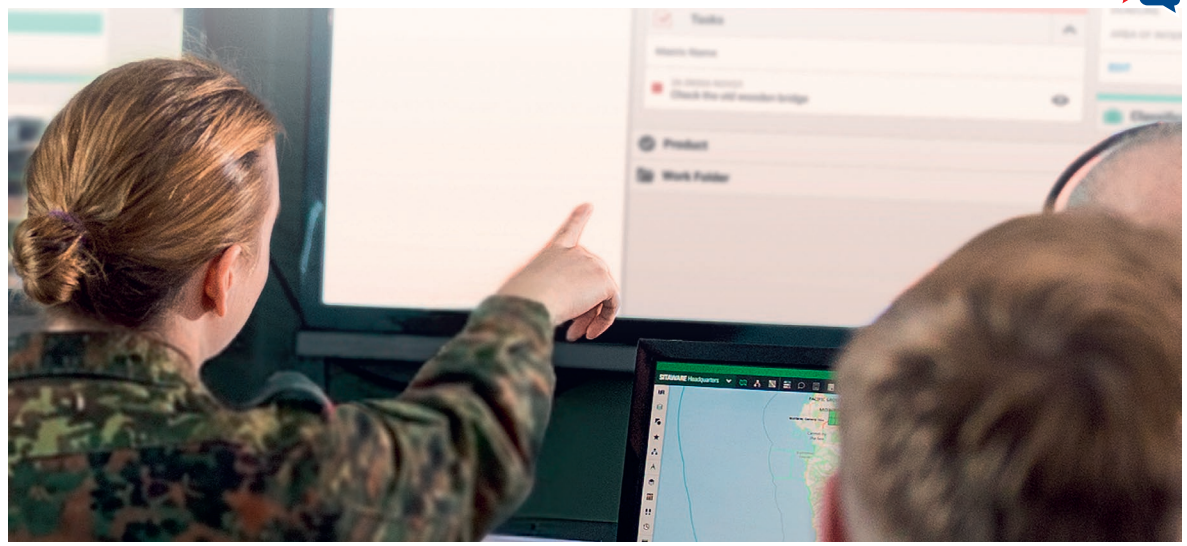
Diese technologische Unabhängigkeit ist eine wesentliche Voraussetzung für digitale Souveränität und damit für die Resilienz von Staat, Wirtschaft und Gesellschaft. Angesichts veränderter geopolitischer Rahmenbedingungen müssen Organisationen Vendor Lock-ins vermeiden, um in jeder Situation handlungsfähig zu bleiben.

Beim Bonner IT-Dialog möchte SUSE mit Vertretern aus Streitkräften, Zivilschutz, Politik und Verwaltung darüber diskutieren, wie offene Technologien zu einem leistungsfähigen gesamtstaatlichen Sicherheitsökosystem beitragen können. ■

SUSE

STAND-NUMMER F07

SUSE Software Solutions Germany GmbH
Frankenstraße 146, 90461 Nürnberg
Telefon: *+49 911 740 530*
E-Mail: *kontakt-de@suse.com*
Infos: *www.suse.com/verteidigung*



Ein Lagebild für den **gesamtstaatlichen Ernstfall**

Systematic entwickelt seit vier Jahrzehnten hochspezialisierte IT-Lösungen, mit der Streitkräfte, Sicherheitsbehörden und das Gesundheitswesen planen und entscheiden. Über Erfolg entscheiden dabei selten einzelne Fähigkeiten, sondern ihr Zusammenspiel. Im Ernstfall greifen Militär, Verwaltung, Zivilschutz und Betreiber kritischer Infrastruktur ineinander.

Dafür liefert die SitaWare Suite die digitale Grundlage: eine offene Architektur, die militärische und zivile Lageinformationen, logistische Abläufe und offene Quellen über Ressort-, Dimensions- und Landesgrenzen hinweg zusammenführt. Den Kern bilden SitaWare Headquarters, SitaWare Frontline und SitaWare Edge für das gemeinsame Lagebild über alle Führungsebenen. Darauf setzen dimensionsspezifische Module und Add-Ons auf, etwa SitaWare Maritime, Air C2, Targeting, Joint Fires oder die medizinische Notfallversorgung.

Was die Suite zusammenführt, wertet SitaWare Insight aus: KI-gestützte Datenerfassung, -speicherung und -analyse. So werden aus großen Datenmengen belastbare Lagebewertungen. Mit agentischer KI geht Systematic den nächsten Schritt: Sie erhält eine Aufgabe und identifiziert, welche Daten sie benötigt und welche Handlungsoptionen bestehen. Der Mensch bleibt in der Entscheidungsschleife.

SitaWare ist bei mehr als 50 Nationen im Einsatz, darunter über 20 NATO-Verbündete und die NATO-Kommandostruktur. Bei der Bundeswehr ist SitaWare als Teil des Mission Enabling Service Bundeswehr (MESBw) dimensionsübergreifend in unterschiedlichen Ausprägungen etabliert, als Basis eines einheitlichen Software-Ökosystems.

Deutschland hat die Fähigkeiten. Der Bonner IT-Dialog fragt nach ihrer Verkettung. Systematic zeigt, wie daraus ein gemeinsames Lagebild wird. ■

SYSTEMATIC

STAND-NUMMER F05

Systematic GmbH
Im Zollhafen 14, 50678 Köln
Telefon: *+49 221 29 29 43 19*
E-Mail: *more.info.de@systematic.com*
Web: *www.systematic.com*



Wo jede Verbindung zählt.

Robuste Netzwerke für missionskritische Anwendungen

Wenn Kommunikation über den Erfolg einer Mission entscheidet, ist Ausfallsicherheit keine Option, sondern Voraussetzung. Westermo entwickelt robuste, cybersichere Netzwerklösungen für den Einsatz unter härtesten Bedingungen — zu Lande, zu Wasser und in mobilen Führungssystemen.

Europäische Ingenieurskunst, europäische Lieferkette

Seit über 50 Jahren entwickeln und fertigen wir in Europa. Das reduziert Versorgungsrisiken, sichert Qualität und garantiert langfristige Verfügbarkeit — entscheidend für Verteidigungsprogramme mit Laufzeiten über Jahrzehnte.

Belegbar robust:

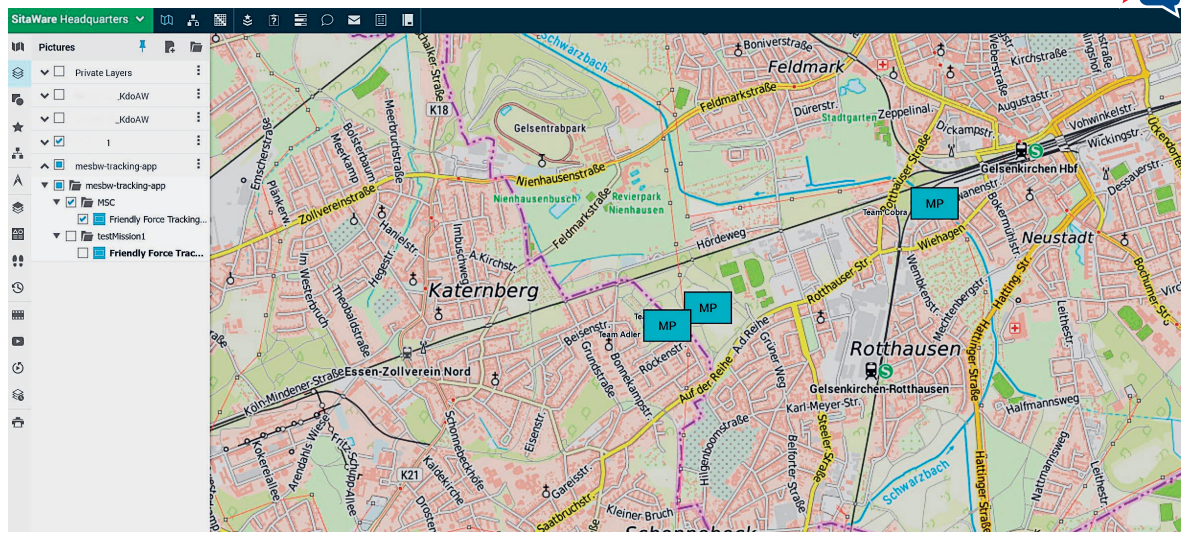
- IEC 62443-4-2 SL2 zertifiziert
- MIL-STD-810
- EMC
- IP65
- – 40 °C bis + 70 °C lüfterlos
- 15 Jahre Produktlebenszyklus
- 30.000 automatisierte Tests pro Woche

Westermo — seit 1975. Über 40 Länder.
Teil der börsennotierten Ependion-Gruppe. ■



STAND-NUMMER **F02**

Rainer Grumann
Sales Director Defence DACH
Telefon: +41 (0) 79 882 55 18
E-Mail: rainer.grumann@westermo.com
Web: www.westermo.com/defence



Die zentrale Rolle des **Cyber- und Informationsraumes** (CIR)

In aktuellen und zukünftigen Konflikten spielt der Cyber- und Informationsraum (CIR) eine entscheidende Rolle. Informationen müssen schnell und sicher gewonnen, ausgewertet und übermittelt werden. Sie sind Voraussetzung für ein Lagebild in Echtzeit. Die Teilstreitkraft CIR stellt hierfür als „zentrales Nervensystem" wesentliche Fähigkeiten wie IT-Services, Aufklärung, Einsatzunterstützung aus dem Weltraum, Cyberoperationen, Elektromagnetische Kampfführung, Operative Kommunikation und Geoinformationen bereit. Darüber hinaus trägt sie in ihrer Rolle als Treiber der Digitalisierung der Bundeswehr dazu bei, technologische Innovationen zu erschließen.

Das Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung CIR (ZDigBw)

Das ZDigBw entwickelt und erprobt Software, integriert IT-Services in das IT-System der Bundeswehr und gewährleistet die Qualitätssicherung – von der Konzeption über die Entwicklung bis hin zur Integration und Nutzung. Es verantwortet mit seinen Produkten die Fähigkeitsentwicklung im Cyber- und IT-Bereich sowie im Militärischen Nachrichtenwesen, in der Elektronischen Kampfführung und in der Informationssicherheit.

MESBwTrackingApp

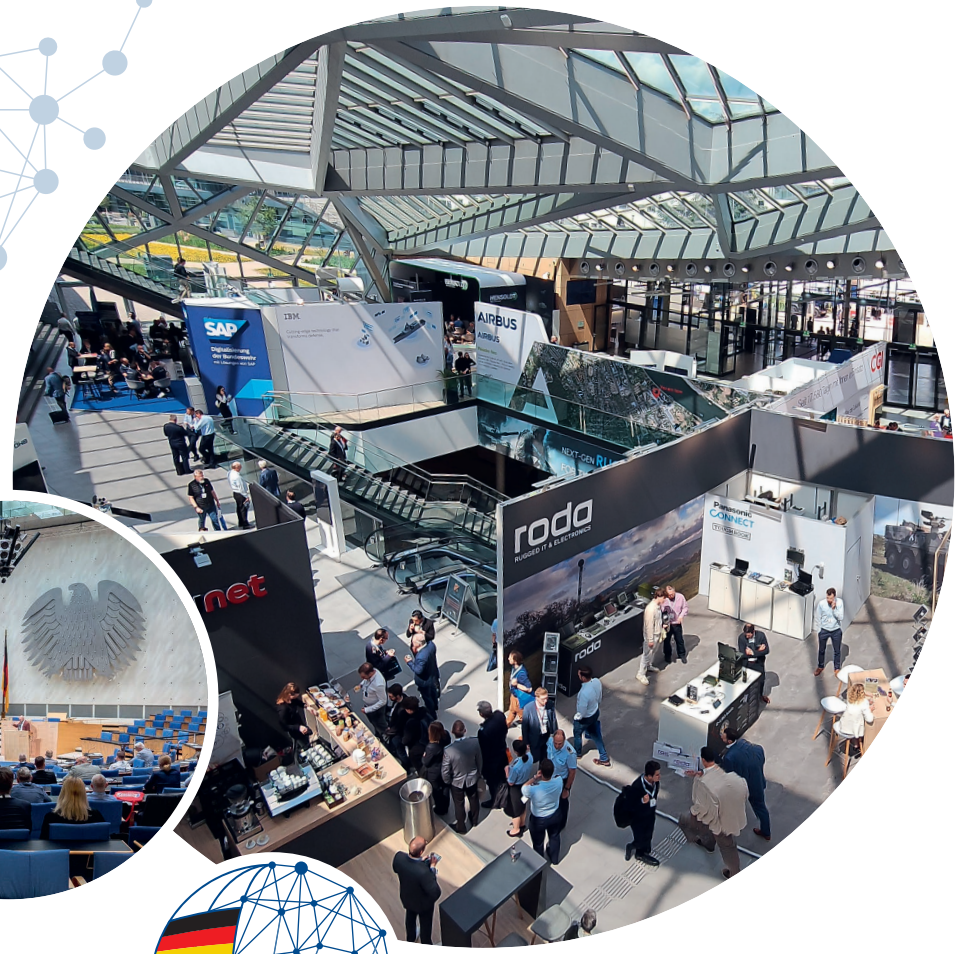
Mit der MESBwTrackingApp schließt das ZDigBw eine Lücke bei der Durchführung und Überwachung von militärischen Aufträgen: Erstmals ermöglichen wir Echtzeit-Positionstracking von Transporten, Märschen oder vergleichbaren Aufträgen direkt in SitaWareHQ – nahtlos integriert über das dienstliche EMM-Smartphone, und das im VS-NfD-Umfeld. Truppenführer behalten die Kontrolle, Einsatzzentralen entscheiden präziser, Transporte werden sicherer und effizienter. Keine blinden Flecken oder zeitversetzte manuelle Nachmeldungen mehr, sondern volle Transparenz in Echtzeit. ■

STAND-NUMMER **B01**

***ZDigBw** | Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum*
Fontainengraben 150, 53123 Bonn
Web: www.cir.bundeswehr.de

40. AFCEA Fachaus stellung 2027

World Conference Center Bonn



AFCEA Bonn e.V.

Scan me

Allgemeine Informationen
und Informationen für
Besucher und Aussteller

25./26. Mai 2027

DIE Plattform für sicherheitsrelevante Digitalisierung

Digitale Souveränität | Einsatzfähigkeit | Vernetzung

Wir freuen uns auf Ihren Besuch

- Die zentrale Plattform für den Austausch zwischen Bundeswehr, Behörden, Organisationen mit Sicherheitsaufgaben, Industrie, Forschung und Technologieanbietern
- Fachliche Tiefe, relevante Begegnungen und die Einordnung technologischer Entwicklungen in einem sicherheitspolitisch geprägten Umfeld
- Relevanz entsteht dort, wo Technologie auf reale Anforderungen trifft.

25./26. Mai 2027

WCCB Bonn

www.afcea.de

Mitglied werden bei AFCEA Bonn e. V.

Über 880 persönliche Mitglieder und 84 Mitgliedsfirmen

Vorteile für Mitglieder

- ✓ Wissenssteigerung im beruflichen Interesse
- ✓ Know-how-Transfer zwischen Anwendern und Entwicklern
- ✓ Synergien durch Fachkontakte zwischen Entwicklern und Produzenten
- ✓ Kostenlose Teilnahme an den Fachveranstaltungen
- ✓ Kostenloser Bezug der Zeitschrift „Signal"
- ✓ Besuche von Veranstaltungen ausländischer Chapter zu günstigen Reisekonditionen
- ✓ Mitgestaltung der Vereinsaktivitäten

Persönliche Mitgliedschaft
Korporative Mitgliedschaft
Außer einer persönlichen Mitgliedschaft als Einzelperson, kann eine Teilnahme auch als Vertreter eines korporativen Mitglieds erfolgen. Korporative sind juristische Personen, (Firmen und Körperschaften), die, je nach gewählten Status eine Anzahl ihrer Mitarbeiter zur Teilnahme an AFCEA Bonn e. V. benennen.

Scan me

Hier Mitglied werden!

Wie andere Chapter bietet auch AFCEA Bonn e. V. für Mitglieder und Interessierte bis zum Alter von rund 40 Jahren eigene Aktivitäten. Zielgruppen sind junge Soldaten und zivile Mitarbeiter, die nach dem Studium im IT-Umfeld tätig sind, Studierende und junge Fach- und Führungskräfte aus Bundeswehr, Industrie und Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Im Bonner Verein bringen sich die Emerging Leaders mit einem eigenen Arbeitskreis ein.

Die Emerging Leaders bieten:

» Hochrangige Kontakte zu Behörden und Firmen
» Lehrreiche Informationsveranstaltungen
» Erfahrungsaustausch, auch international
» Kontakte für Berufseinstieg und Karriere
» Interessante Exkursionen
» Kooperative Arbeitskreise



Seit 2008 ist AFCEA Bonn e. V. von seinem Dachverband in jedem Jahr als „Model Chapter of the Year" ausgezeichnet worden.

NEU!

Original AFCEA Fachausstellungs- und BITD-

Patch



zum BITD-Preis
von **5,– Euro**
(nur Barzahlung möglich)

PATCH

Erhältlich vor Ort am **BITD/AFCEA Aussteller-Stand S7** (Saal Schumann)



Nachwuchsförderung mit Ehrung: Die Preisverleihung findet jährlich auf der Bühne des Bonner IT-Dialoges statt.

AFCEA **Studienpreis**

für herausragende Masterarbeiten in den Fachbereichen Angewandte Informatik, Nachrichtentechnik, Automatisierungstechnik

AFCEA Bonn e. V. verleiht seit 2008 jährlich einen Studienpreis, der pro Jahr mit insgesamt 20.000 Euro dotiert ist. Zudem erhalten alle Preisträger eine Jahres-Mitgliedschaft bei AFCEA Bonn e. V. Der Verein fördert damit die wissenschaftliche Qualifikation junger Wissenschaftler/innen, die hervorragende Master-, beziehungsweise Diplom-, Magisterarbeiten auf den Gebieten Angewandter Informatik, Nachrichtentechnik oder Automatisierungstechnik erstellt haben. Auch Bachelorarbeiten sind zugelassen, jedoch werden an alle Arbeiten dieselben Maßstäbe angelegt. Der Studienpreis finanziert sich mit Erlösen aus der Fachausstellung.

Die Jury setzt sich aus Persönlichkeiten aus der universitären Lehre, der Forschung sowie der einschlägigen Industrie zusammen und bewertet nach folgenden Kriterien.

Erkenntnisgewinn: Bewertet wird der Neuigkeitsgehalt der Ergebnisse in Bezug auf eine Verbreiterung der Wissensbasis im jeweiligen Fachgebiet, die Originalität der Idee und damit die innovative Lösung für die gegebene Aufgabenstellung.

Praktische Relevanz: Es soll eine aktuelle Fragestellung aus einem der Fachgebiete „Angewandte Informatik“, „Nachrichtentechnik“ oder „Automatisierungstechnik“ behandelt werden. Eine Transfer- beziehungsweise Umsetzungsmöglichkeit der Ergebnisse in die Praxis muss erkennbar sein. Die Notwendigkeit für eine Lösung des gestellten Problems beziehungsweise resultierende Rationalisierungspotentiale und Qualitätsverbesserungen sowie zukünftige Perspektiven müssen erkennbar sein. Hinweise auf praktische Erprobungen,zum Beispiel Feldtests, sind hilfreich.

Klarheit von Gedankenführung und Darstellung: Wesentlich sind eine klare Beschreibung der Aufgabenstellung, die Schlüssigkeit der Gedankenführung ausgehend von der Problemstellung über die Herangehensweise bei der Lösungssuche, der Herleitung der Ergebnisse bis hin zur Interpretation der Ergebnisse. Der Sachverhalt muss klar strukturiert, sowie in sachlicher und sprachlich präziser Art dargestellt sein. Abbildungen müssen verständlich und übersichtlich aufgebaut sein.

Schwierigkeitsgrad: Entscheidend für die Bewertung in diesem Bewertungspunkt sind die Sicherheit bei der wissenschaftlichen Methodik, die Fundiertheit bei der Auseinandersetzung mit dem Stand der Technik, der Umgang mit Daten und Quellen sowie die Qualität der Literaturzusammenstellung. ■

Am 7. Oktober stellt AFECA Bonn e. V. die Preisträger 2026 im Rahmen des Bonner IT-Dialogs vor und würdigt die Sieger.

AFCEA Bonn e. V.
Borsigallee 2 · 53125 Bonn
Telefon: +49 228 925 82 52
E-Mail: buero@afcea.de
www.afcea.de

BONNER IT DIALOG 2026

wird veranstaltet von

AFCEA Bonn e.V.

© AFCEA Bonn e. V. 09-2026