
Detect
Defend &
Orange Cyberdefense Live
Der Kongress für
digitale Sicherheit

Programm

Erleben Sie Cybersecurity aus der Pole Position!

Starten Sie beim Grand Prix of Cybersecurity, wo Geschwindigkeit, Strategie und Präzision über den Erfolg in der digitalen Welt entscheiden. Compliance und Innovation gehen hier Hand in Hand, und jede Herausforderung lässt sich souverän meistern. Die Einführung von NIS2 und DORA mag komplex erscheinen – wir liefern Ihnen nicht nur das Fahrzeug, sondern auch das Setup, um jede Aufgabe zu bewältigen.

Erleben Sie die Dynamik der Cyberabwehr hautnah – dieses Jahr in Fürstenfeldbruck und Köln. Auf mehreren Bühnen erwarten Sie technische Deep Dives, praxisnahe Fallstudien und visionäre Ansätze, die zeigen, wie regulatorische Anforderungen zu echten Wettbewerbsvorteilen werden. Setzen Sie aufs richtige Team, die beste Strategie – Ihre Cybersecurity ist Ihr Podium und Ihr Sieg.

Keynote:

Heiko Wasser

Blick hinter die Kulissen der Formel 1 – Motivation und Teamwork

In seiner inspirierenden Keynote zeigt Heiko Wasser, Deutschlands bekanntester Formel-1-Kommentator, wie Hochleistungsmotorsport und Cybersicherheit auf verblüffende Weise zusammenhängen. In beiden Welten entscheiden Schnelligkeit, strategisches Denken und ein perfekt eingespieltes Team über Sieg oder Niederlage. Mit spannenden Filmsequenzen von der Rennstrecke, authentischen Anekdoten aus seiner jahrzehntelangen Kommentatorenlaufbahn und hintergründigen Einblicken vermittelt er, was Siegermentalität wirklich bedeutet. Dabei wird deutlich, warum Spitzenleistung nie nur individuelle Leistung ist, sondern immer das Ergebnis einer starken, engagierten Gemeinschaft, auf der Rennstrecke wie in der Welt der Cybersecurity.

powered by:

Axonius
Qualys
algosec
NOZOMI NETWORKS
netskope
Cribl
paloalto NETWORKS
Nucleus
rubrik
PENTERA
splunk>
VMRAY
SECTIGO
proofpoint
Akamai
Forcepoint

www.orangecyberdefense.de

Detect & Defend
Orange Cyberdefense Live

Agenda Köln - 20.05.2026

08:00–09:00 Uhr: **Registrierung**

09:00–09:15 Uhr: **Eröffnung durch Michael Schrenk, Division Manager Sales & Götz Weinmann, Senior Business Development Manager**

09:15–10:00 Uhr: **Keynote Heiko Wasser**

Zeit	Track 1 - Historische Empfangshalle	Track 2 - Racing Lounge	Track 3 - Zeppelin Lounge	Butzweilerhof
10:30–11:00	Data Security Track 1: **DLP-Projekte sicher ans Ziel – Discovery & Visibility als Gamechanger** presented by Orange Cyberdefense	**KI-basierte Managed Security Services: Vom Reagieren zum Rennvorsprung** presented by Orange Cyberdefense	**Die Compliance-Rennstrecke meistern: Mit KI-gestützter Segmentierung an die Spitze** presented by Akamai	**DORA Round-table** presented by Orange Cyberdefense
11:15–11:45	Date Security Track 2: **Data-Security-by-Design im KI-Ökosystem** presented by Orange Cyberdefense	**Sichere und schnelle Datenwiederherstellung, warum Backup heute nicht mehr genug ist** presented by Rubrik	**Podiumsdiskussion: Ein Incident ist wie ein Crash: Man hofft, dass er nie passiert** presented by Orange Cyberdefense, SKW Schwarz	
12:00–12:30	Data Security Track 3: **Die Pole Position in Datenklassifizierung: KI-gestütztes DSPM für maximale Transparenz** presented by Forcepoint	**Tuning im Fahrwerk des SIEM: Ingest optimieren, Migration beschleunigen** presented by Orange Cyberdefense	**Code to Cloud to SOC: Komplexität reduzieren, operative Exzellenz steigern** presented by Palo Alto Networks	
12:30–13:45 Uhr: **Lunch**				
13:45–14:15	**CyberSOC Praxis Insights – Angriffstrends im digitalen Rennen und ein Cyber-Spionagefall** presented by Orange Cyberdefense	Security Awareness Track 1: **Awareness als Vorsprung im Cyber-Rennen** presented by Orange Cyberdefense	**Die Architektur der Widerstandsfähigkeit: Von lückenloser Sichtbarkeit zu echter Cyber-Resilienz** presented by Axonius	**Vom Spaghetti-Netzwerk zur Zero-Trust-Architektur** presented by Akamai
14:30–15:00	**Post Quantum: Die unsichtbare Gefahr, warum heutige Verschlüsselung riskant ist** presented by Orange Cyberdefense	**OT Cybersecurity - von der Regulierung zur Umsetzung** presented by Orange Cyberdefens, SKW Schwarz, Weidmüller	Security Awareness Track 2: **Full Speed mit AI – doch wer sitzt wirklich am Steuer?** presented by Orange Cyberdefense	**Navigating Ransomware with Intelligence & Precision** presented by Orange Cyberdefense
15:15–15:45	**200 Tage sind erst der Anfang – Anpassung an verkürzte Zertifikatslaufzeiten** presented by Sectigo		Security Awareness Track 3: **Startklar für sichere KI: Die ersten Schritte zur Absicherung interner KI-Systeme** presented by Orange Cyberdefense	
15:45–16:15 Uhr: Tea & Networking				
16:15–16:45	**Wie ein Boxenstopp bei Profis Ihre Detection und Response optimiert und den Rennsieg zur Formsache macht** presented by Orange Cyberdefense	**tbd.** presented by Proofpoint	**SOC Skills: Eine praxisnahe Preview für moderne Incident-Response** presented by Orange Cyberdefense	**NIS2 in der Praxis: Vom ersten Check bis zur vollständigen Umsetzung** presented by Orange Cyberdefense
17:00–17:30	**Big Data 4 Security - und wieso auch Ihre KI davon profitiert** presented by Orange Cyberdefense	**Feedback & Roadmap – Exklusiv für Managed Security Services Kunden** presented by Orange Cyberdefense	**Vom IT-Risiko zum Geschäftsrisiko: Cyberresilienz als Chefsache** presented by Orange Cyberdefense	

17:30–22:00 Uhr: **Get Together im Restaurant der Motorworld „El Carrito“**

Track 1 - Historische Empfangshalle

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Heiko Wasser

10:30 | Data Security Track 1: Data Security 2.0: DLP-Projekte sicher ans Ziel – Discovery & Visibility als Gamechanger presented by Malte Rabenseifner, Manager Security Consulting, Orange Cyberdefense

Data Security ist mehr als nur Data Loss Prevention… - und unverzichtbar für jedes Unternehmen. Doch Data Security ist komplex und traditionelle Ansätze bringen hohe Projektrisiken mit sich. In der Praxis scheitern viele DLP-Initiativen. Unser Discovery-&-Visibility-Ansatz macht alle Datenbestände, Schattenplattformen und riskante Datenströme sichtbar – und Ihr Projekt damit steuerbar. Wir stellen Ihnen vor, wie Sie DLP-Projekte endlich sicher on track bringen. Verpassen Sie nicht unsere dreiteilige Vortragsreihe auf der Detect & Defend und bringen Sie sich in Pole Position, um Data Security ganzheitlich in Ihrer Organisation aufzustellen.

11:15 | Data Security Track 2: Data-Security-by-Design im KI-Ökosystem: Architekturprinzipien für den Schutz von sensiblen Daten presented by Thomas Jupe, Senior Business Development Manager & Nico Mehlhose, Security Consultant, Orange Cyberdefense

Wir zeigen eine architekturorientierte Sicht auf die Schutzmechanismen, die für Ihre Data Security in Ihrem KI-Rennen von Bedeutung sind. Der Vortrag führt durch modulare Bausteine wie Data Discovery, Classification, Handling, Policy-Orchestrierung, Privacy-Enhancing Techniques und technische Mechanismen, die eine Zusammenarbeit mit KI-Agenten ermöglichen, ohne die Datenhoheit zu gefährden. Die KI-Experten von Orange Cyberdefense bieten Ihnen Einblick in ihr Knowhow und zeigen Ihnen dabei, wie Sie Ihre KI-Initiativen sicher und skalierbar zu machen.

12:00 | Data Security Track 3: Die Pole Position in Sachen Datenklassifizierung: Forcepoint DSPM powered by AI presented by Konrad Langhammer, Territory Account Manager, Forcepoint

Komplexe Cloud- und Hybridumgebungen machen es heute schwerer denn je zu wissen, wo sensible Daten liegen und welche Risiken daraus entstehen. Datenklassifizierung wird damit zum zentralen Erfolgsfaktor moderner Sicherheitsstrategie. In diesem Vortrag zeigen wir, wie Forcepoint DSPM mit seiner AI-Mesh-Technologie automatisiert erkennt, wo kritische strukturierte und unstrukturierte Daten liegen, wie sie genutzt werden und verborgene Risiken sichtbar macht. Anhand praxisnaher Beispiele erhalten Sie einen Einblick in typische Schwachstellen, etwa Schatten-IT, unklare Datenverantwortlichkeiten und fehlende Transparenz über Datenflüsse. Außerdem erfahren Sie, wie moderne Data-Security-Konzepte die Erfüllung von Compliance-Vorgaben wie die DSGVO unterstützen – ohne dabei den Geschäftsbetrieb auszubremsen. Abschließend erhalten Sie konkrete Handlungsempfehlungen, um Ihre Organisation in Sachen Datenklassifizierung und Datensicherheit in die Pole Position zu bringen: von der Bestandsaufnahme bis zur kontinuierlichen Überwachung.

13:45 | CyberSOC Insights – Angriffstrends im digitalen Rennen und ein Cyber-Spionagefall aus der Praxis presented by André Henschel, Analyst Cyber Security, Orange Cyberdefense

Hunderte Cyberangriffe werden jeden Monat von dem CyberSOC der Orange Cyberdefense detektiert und analysiert. Dazu gehören groß angelegte Angriffskampagnen sowie gezielte Angriffe auf einzelne Organisationen. Ein Überblick über die Cyber-Bedrohungslage wird anhand der vom CyberSOC bearbeiteten Vorfälle dargestellt, um Trends und häufige Angriffsmethoden aufzuzeigen. Tiefere Einblicke gibt es zu einem gezielten Cyberangriff gegen ein großes Industrieunternehmen, welcher mit einer scheinbar harmlosen Jobanfrage begann.

14:30 | Post Quantum: Die unsichtbare Gefahr: Warum aktuelle Verschlüsselung heute ein Risiko ist presented by Dr. Mohammed Meziani, Senior Security Consultant, Orange Cyberdefense

Quantencomputer werden oft als rein theoretisches Konzept missverstanden, doch sie stellen bereits heute eine reale Gefahr für unsere Datensicherheit dar. Das Problem ist konkret. Angreifer speichern bereits jetzt sensible Daten, um sie in wenigen Jahren mit Quantenrechnern zu knacken („Harvest Now, Decrypt Later").
In diesem Vortrag erklären wir, warum unsere aktuellen Passwörter und Zertifikate bald wertlos sein könnten. Wir werfen einen verständlichen Blick auf die Post-Quanten-Kryptografie (PQC), die digitale Schutzmauer der Zukunft. Sie erfahren, welche Daten besonders gefährdet sind und wie Sie in drei einfachen Schritten damit beginnen können, Ihre Kommunikation und Infrastruktur „quantensicher" zu machen, bevor es zu spät ist.

15:15 | 200 Tage sind erst der Anfang – Anpassung an verkürzte Zertifikatslaufzeiten presented by Johannes Goldbach, Senior Enterprise Strategic Account Manager, Sectigo

Verkürzte Zertifikatslaufzeiten von 200 Tagen – genauer gesagt 199 Tagen – markieren einen grundlegenden Wandel im Bereich Digital Trust. Die stufenweise weitere Reduzierung der Gültigkeitszeiträume ist bereits beschlossen und wird Organisationen nachhaltig fordern. Diese Session zeigt, welche Auswirkungen das auf Sicherheit, Automatisierung und Compliance hat – und wie Unternehmen ihre Zertifikatslandschaften resilient, skalierbar und zukunftssicher aufstellen.

Track 2 - Racing Lounge

16:15 | Wie ein Boxenstopp bei Profis Ihre Detection und Response optimiert und den Rennsieg zur Formsache macht
presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Die Bedrohungslage in Security Operations wird durch KI-Angriffe, zunehmende Tool-Komplexität und knappe Ressourcen verschärft, wodurch Detektionslücken und verzögerte Reaktionen entstehen. Kaum Transparenz darüber, welche Angriffe erkannt werden, kombiniert mit dem Wunsch nach Datenhoheit, erhöht Risiko und False Positives. Der Boxenstopp-Ansatz mit sensorbasierter Detection Engineering, Threat Hunting und automatisierter Reaktion ermöglicht rechtzeitige Wartungspunkte; unsere technologieunabhängige SOC-Consulting-Lösung bietet flexible Modelle, Strategy-Workshops und Security-Maturity-Assessments, um Erkennungsdeckung, Transparenz und Reaktionsgeschwindigkeit messbar zu verbessern.

17:00 | Big Data 4 Security - und wieso auch Ihre KI davon profitiert presented by Jana Werker, Security Analyst, Orange Cyberdefense

Spätestens seit dem Trending von KI ist Big Data nicht mehr das große Buzzword am IT Security Horizont. Warum Datenhygiene, Datenstrategie und Big Data Philosophie nicht nur dennoch sondern gerade durch den KI-Aufschwung relevanter denn je sind und wo der Mehrwert schlummert - ein gedanklicher Ausflug auf Basis von Splunk.

10:30 | KI-basierte Managed Security Services: Vom Reagieren zum Rennvorsprung presented by Niklas Klotz, VP Business Success, Orange Cyberdefense

Orange Cyberdefense zeigt, wie wir die nächste Generation von Managed Security Services entwickeln, die vollständig auf Künstlicher Intelligenz basieren und einen integrierten Plattformansatz verfolgen. Dabei vereinen wir Threat Intelligence, Exposure Management, Posture Management sowie Detection und Response, um eine proaktive, effiziente und skalierbare Sicherheitsstrategie zu ermöglichen. Erfahren Sie, wie diese innovative Lösung Ihre Sicherheitsarchitektur transformiert und Sie optimal auf die Herausforderungen der digitalen Ära vorbereitet.

11:15 | Sichere und schnelle Datenwiederherstellung, warum Backup heute nicht mehr genug ist presented by Nina Kessler, Inside Account Executive & Julius Baumgartner, Account Executive, Rubrik

Ein erfolgreicher Cyberangriff – die Angreifer sind bereits im Tenant, Systeme kompromittiert, Daten verschlüsselt. Jetzt zählt jede Minute. Ziel ist die schnelle Wiederherstellung einer „Minimal Viable Company“, um den Geschäftsbetrieb aufrechtzuerhalten. Mit unveränderlichen Backups, Air-Gap-Architekturen, KI-gestützter Anomalieerkennung und orchestrierter Recovery zeigt Rubrik, warum klassisches Backup 2026 nicht mehr ausreicht und echte Cyberresilienz entscheidend ist.

12:00 | Tuning im Fahrwerk des SIEM: Ingest optimieren, Migration beschleunigen presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

In vielen Security-Setups entscheidet nicht nur welche Logs vorhanden sind, sondern vor allem wie schnell, wie vollständig und in welcher Qualität sie in SIEM & Analyse-Tools ankommen. Der Vortrag zeigt, wie Data Stream Processing genau diese Engpässe adressiert: durch smarte Datenreduktion, intelligentes Routing und eine kontrollierte, „sanfte“ Migration. So lassen sich Lizenz-, Speicher- und Ingest-Kosten senken, Retention und Compliance verbessern und gleichzeitig die Performance für Incident-Erkennung erhöhen. Diskutiert wird außerdem, wie mit einer Security-Data-Pipeline Daten zwischen Zielsystemen (z. B. SIEM/Observability/Archiv) effizient verteilt werden. Ziel ist, aus der Logflut einen belastbaren „Performance-Flow“ zu machen—wie im Rennsport: schneller, datenreicher und mit klarer Kontrolle.

13:45 | Security Awareness Track 1: Awareness als Vorsprung im Cyber-Rennen presented by Franziska Strohmeier, Security Consultant, Orange Cyberdefense

In unserer schnellebigen und sich ständig weiter entwickelnden Welt ist es so wichtig wie noch nie, sich dessen bewusst zu sein, was um einen herum passiert, aware zu sein. Diese Fähigkeit kann Leben retten, Geld retten, ein Image rettten und noch vieles mehr. Dieser Vortrag soll aufzeigen, warum dem Thema Awareness mehr Bedeutung beigemessen werden sollte, als Security-Tool, manuelle Präventionsmaßnahme und life-skill. Anhand praktischer Beispiele aus dem (Arbeits-) Alltag wird aufgezeigt, wo und wie zielgerichtete Awareness Maßnahmen Menschen und Unternehmen vor Schaden bewahren können und nachhaltig zur Unternehmenssicherheit beitragen. Weil Awareness mehr sein kann als eine einschläfernde Pflichtveranstaltung.

14:30 | OT Cybersecurity - von der Regulierung zur Umsetzung presented by Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense & SKW Schwarz & Weidmüller

Cybersecurity ist ein komplexes Thema, das kaum noch zu übersehen ist. Viele Tools, Lösungen und Hersteller machen das System unübersichtlich. Zudem kommen zahlreiche EU-Regulierungen wie AI Act, CRA und NIS2. Eine neue Domäne, die bisher vernachlässigt wurde, ist OT Cybersecurity (auch bekannt als ICS, Manufacturing, IACS). Durch CRA und NIS2 wird die Umsetzung erschwert, da hier Verfügbarkeit und Sicherheit wichtiger sind als Vertraulichkeit. Laufzeiten von 5 bis 15 Jahren, eingeschränkte Patches und Nicht-Ausschalten sind üblich. Daher ist es wichtig, die regulatorischen Anforderungen zu verstehen und schrittweise umzusetzen.

16:15 | presented by Proofpoint

17:00 | Feedback & Roadmap – Exklusiv für Managed Security Services Kunden presented by Niklas Klotz, VP Business Success & Michael Schrenk, Division Manager Sales, Orange Cyberdefense

Dieser Slot bietet Kunden, die bereits die Managed Security Services von Orange Cyberdefense nutzen, wohin die Reise mit dem anstehenden Portfolio Release 2026 hingeht. Dazu wird die Stimme den Kunden gegeben, um Feedback zur Roadmap sowie Wünsche zur Optimierung und Anforderungen an die Services zu geben.

Verantwortlichkeiten fehlen. Für IT Fachkräfte bedeutet das: weniger Rechtfertigungsdruck, mehr Unterstützung. Für Führungskräfte: ein realistischer Blick auf die finanziellen und operativen Risiken, die aus technischen Schwachstellen entstehen.

Track 3 - Zeppelin Lounge

10:30 | Die Compliance-Rennstrecke meistern: Mit KI-gestützter Segmentierung an die Spitze presented by Andreas Steiner, Senior Enterprise Security Architect, Akamai

Regulatorische Meilensteine wie NIS2 und DORA definieren die neue Ideallinie der Cybersicherheit. Die klassische Netzwerksegmentierung gleicht jedoch oft einem riskanten Motorumbau bei Tempo 200 im Blindflug. In dieser Session zeigen wir, wie Sie mit der Akamai Guardicore Generative Policy Engine (GPE) das Regel-Chaos hinter sich lassen. Erfahren Sie, wie KI-gestützte Analysen des realen Datenverkehrs automatisch passgenaue Policies generieren. Sichern Sie Ihre kritischen Assets ohne Betriebsunterbrechungen ab und fahren Sie mit messbarer Compliance sicher über die Ziellinie.

11:15 | Podiumsdiskussion: Ein Incident ist wie ein Formel-1-Crash: Man hofft, dass er nie passiert
mit Matthias Orthwein, Rechtsanwalt, SKW Schwarz &
Rakhim Mirzaev, Digital Forensics & Incident Response, Orange Cyberdefense &
Philipp Seebohm, Cyberversicherungsexperte &
Joachim Schuster, Solution Architekt, Orange Cyberdefense &
hosted by Markus Neumaier, Head of Security Operations Central Europe, Orange Cyberdefense

Die Podiumsdiskussion beleuchtet den gesamten Lebenszyklus eines Cybervorfalls im Kontext der Anforderungen der NIS2-Richtlinie und Beyond. Von der strategischen und organisatorischen Vorbereitung über die technische Incident Response bis hin zu Meldepflichten und Lessons Learned. Auf dem Podium treffen unterschiedliche Perspektiven aufeinander: ein Anwalt für IT-Recht, ein Cyberversicherer, ein Incident Responder sowie ein Cyber Security Solution Architekt. Gemeinsam diskutieren sie, wie Unternehmen sich effektiv auf Sicherheitsvorfälle vorbereiten, welche Schritte im Ernstfall entscheidend sind, welche rechtlichen und regulatorischen Verpflichtungen gelten und wie aus jedem Vorfall nachhaltige Verbesserungen entstehen können. Abschließend werden Fragen aus dem Publikum aufgegriffen, um konkrete Herausforderungen und Praxisbeispiele zu adressieren.

12:00 | Code to Cloud to SOC: Komplexität reduzieren, operative Exzellenz steigern presented by Marino Wiegand, Partner Development Manager Cortex, Palo Alto Networks

Das Paradoxon: Mehr Tools führen oft zu mehr Komplexität statt Sicherheit. Wir zeigen, wie Sie diesem Teufelskreis durch Konsolidierung entkommen. Die Cortex-Plattform vereint den gesamten Sicherheitszyklus – von Code zu Cloud bis zum SOC. Erfahren Sie, wie dieser integrierte Ansatz nicht nur Sicherheitslücken schließt, sondern durch massive Effizienzgewinne echten Business Value liefert.

13:45 | Die Architektur der Widerstandsfähigkeit: Von lückenloser Sichtbarkeit zu echter Cyber-Resilienz presented by Thomas Loquai, Senior Technical Account Manager, Axonius

Sicherheit beginnt nicht bei komplexen Algorithmen, sondern bei der Antwort auf eine einfache Frage: Wissen wir, was wir schützen müssen? In diesem Slot zeigen wir, wie Unternehmen durch ein systematisches Asset-Management die Kontrolle über ihre digitale Infrastruktur zurückgewinnen. Wir beleuchten den Weg von der Identifikation blinder Flecken (Scope & Discover) und demSchließen von Sicherheitslücken (Fix Coverage) bis hin zurVeredelung der CMDB-Datenqualität. Erfahren Sie, wie eine saubere Datenbasis dieReaktionsgeschwindigkeit bei Vorfällen (Incident Response) drastisch erhöht und eine gezielteRisikopriorisierung ermöglicht. Das Ziel: Ein messbares Fundament fürCyber-Resilienz, das auch unter Druck standhält – ohne sich auf vage Versprechungen zu verlassen.

14:30 | Security Awareness Track 2: Full Speed mit AI – doch wer sitzt wirklich am Steuer? presented by Holger Fastenrath, Team Lead CyberSOC, Orange Cyberdefense

AI bestimmt direkt oder indirekt unseren Arbeitsalltag, die Kommunikation mit Kunden und beeinflusst unsere Entscheidungen durch Informationsaufbereitung und -bewertung. Oft erhält sie dabei auch Administrationsrechte, Zugang zu sensibelsten Informationen, Zugriff auf das Internet oder ist selbst aus dem Internet erreichbar und wird dadurch unbemerkt zum riskantesten Mitarbeiter im Unternehmen. Weniger oft ist klar, von welchem Mitarbeiter sie wo eingesetzt wird, wer wie mit AI interagiert, auf welche Daten sie zugreift, wohin sie Daten speichert und ob sie sich dabei an die Rechte- & Rollenkonzepte hält, denen die Nutzer der AI unterliegen. Wir zeigen Ihnen, wie sich AI kontrollieren lässt und kein „Deus Ex Machina“ bleibt. Dabei betrachten wir aktuelle Angriffe auf AI-basierte Clouddienste und zeigen wie selbst lokal gehostete AI-Modelle von Angreifern ausgenutzt werden können.

15:15 | Security Awareness Track 3: Startklar für sichere KI: Die ersten Schritte zur Absicherung interner KI-Systeme presented by Nico Mehlhose, Security Consultant, Orange Cyberdefense

Diese Präsentation skizziert die ersten Schritte zur Sicherung von AI-Systemen in einem Unternehmen. Es werden Methoden wie das AI-Maturity Assessment und die Identifikation von Shadow-AI-Systemen vorgestellt. Zudem werden kurz weitere Maßnahmen zur Verbesserung und Erweiterung der AI-Sicherheit/Compliance erläutert. Ziel ist es, praktische Orientierungshilfen und ein grundlegendes Verständnis dafür zu vermitteln, worauf es am Anfang der Sicherung von KI-Systemen ankommt.

16:15 | SOC Skills: Eine praxisnahe Preview für moderne Incident-Response presented by Pierre Kroma, Trainer für Orange Cyberdefense

Wie erkennen und bewerten SOC-Analysten Sicherheitsvorfälle unter Echtzeitdruck? Diese praxisnahe Preview zeigt, wie Alerts zu handhabbaren Incidents werden und wie komplexe Angriffsketten analysiert werden. Anhand realistischer Beispiele vermittelt der Vortrag zentrale Methoden, Denkweisen und Herausforderungen moderner Incident-Response. Er gibt einen Einblick, welche Fähigkeiten in der Trainingsreihe „Fast Track SOC Analyst“ und „Fast Track SOC Analyst Advanced“ von Orange Cyberdefense mit 90% Praxisanteil vollumfänglich vermittelt werden.

17:00 | Vom IT-Risiko zum Geschäftsrisiko: Cyberresilienz als Chefsache presented by Thomas Wisdorf, Senior Sales Manager, Orange Cyberdefense

Cyberangriffe sind längst ein zentrales Geschäftsrisiko – doch in vielen Unternehmen bleibt die Verantwortung dafür auf der technischen Ebene hängen. IT Teams kämpfen täglich mit Schwachstellen, Incident Druck und komplexen Systemen, während das Management die geschäftlichen Auswirkungen oft unterschätzt oder zu spät erkennt. Genau hier setzt der Vortrag an. Er zeigt, warum Cyberresilienz nicht im SOC beginnt, sondern im Vorstand und weshalb technische Maßnahmen allein nicht ausreichen, wenn strategische Entscheidungen, Priorisierung und klare Verantwortlichkeiten fehlen. Für IT Fachkräfte bedeutet das: weniger Rechtfertigungsdruck, mehr Unterstützung. Für Führungskräfte: ein realistischer Blick auf die finanziellen und operativen Risiken, die aus technischen Schwachstellen entstehen.

Der Vortrag macht deutlich, dass Cybersecurity nur dann funktioniert, wenn Management und IT gemeinsam handeln. Denn wie der Vortrag betont: „Security wird technisch diskutiert – aber geschäftlich nicht entschieden.“ Wer verstehen will, wie Unternehmen schneller entscheiden, besser vorbereitet sind und echte Resilienz aufbauen, findet hier die Antworten.

Butzweilerhof Lounge

10:30 | Exklusiver DORA Roundtable presented by Markus Thiel, QMS, Auditor and Compliance Principal Leader & David Mayer, Manager Security Consulting, Orange Cyberdefense

Dieser exklusive Roundtable widmet sich den aktuellen Herausforderungen und Umsetzungsfragen rund um den Digital Operational Resilience Act (DORA). Die Veranstaltung findet im vertraulichen Rahmen unter NDA und ausschließlich nach Voranmeldung statt und richtet sich gezielt an Praktiker aus direkt von der DORA betroffenen Organisationen. Um einen vertrauensvollen und praxisnahen Dialog sicherzustellen, sind Technologieanbieter, Aufsichtsbehörden sowie Vertreter anderer Beratungshäuser von der Teilnahme ausgeschlossen. Ziel des Formats ist ein offener, fachlich fundierter Austausch zu den in der jeweiligen Funktion aktuell relevanten Themen – von operativen Fragestellungen bis hin zu Aspekten der IKT-Kontrollfunktion und des Non-Financial Risk Managements. Die Teilnehmer bringen eigene Erfahrungen, Problemstellungen und Lösungsansätze ein und profitieren im Gegenzug von den Perspektiven und Best Practices der Gruppe. Der Roundtable bietet damit einen geschützten Raum für ehrlichen Erfahrungsaustausch, kritische Diskussionen und konkrete Impulse zur DORA-Umsetzung jenseits von Theorie und Standardansätzen.

13:45 | Hands-on Boxenstopp: Vom Spaghetti-Netzwerk zur Zero-Trust-Architektur in presented by Akamai

In diesem interaktiven Workshop wechseln wir von der Tribüne direkt ins Cockpit. Erleben Sie live, wie wir ein unübersichtliches „Spaghetti-Netzwerk“ aus IT-, Cloud- und OT-Komponenten strukturieren. Wir zeigen Schritt für Schritt, wie Sie mit Akamai Guardicore innerhalb von Minuten prädiktive Sicherheitsrichtlinien erstellen. Lernen Sie anhand der Generative Policy Engine (GPE), wie Sie durch datenbasierte „Readiness“-Metriken fundierte Entscheidungen treffen und Mikrosegmentierung in der Praxis scharfschalten – völlig ohne den laufenden Betrieb zu stören.

14:45 | Crisis Command: Navigating Ransomware with Intelligence & Precision (ENG) presented by Erik Van Dijk, Product Manager & Paul Treffers, Country Lead NL/DE CSIRT, Orange Cyberdefense

When ransomware strikes, it feels less like a technical incident and more like a Formula 1 race at full speed. Every second counts, and decisions based on incomplete or unclear data can quickly derail response efforts.

This session is designed for analysts and decison makers operating under pressure. It focuses on how to turn fragmented data into actionable intelligence, prioritize signal over noise, and provide clear decision support during a live crisis. Learn how to maintain situational awareness and deliver precise, timely insights when they matter most. This session puts you in that cockpit showing how intelligence-led decisions and precise execution, grounded in real-world Incident Response expertise, turn chaos into control when it matters most.

16:15 | NIS2 in der Praxis: Vom ersten Check bis zur vollständigen Umsetzung, ein ganzheitlicher Workshop für Unternehmen presented by SKW Schwarz & Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense

Dieser Workshop führt Unternehmen Schritt für Schritt durch die zentralen Anforderungen der NIS2 Richtlinie und zeigt praxisnah, wie eine vollständige Umsetzung gelingt. Zu Beginn wird gemeinsam mit einem Partner eine fundierte Betroffenheitsanalyse durchgeführt, um zu klären, ob und in welchem Umfang die Organisation unter NIS2 fällt. Darauf aufbauend folgt eine detaillierte Gap Analyse, die bestehende Sicherheitsmaßnahmen mit den regulatorischen Vorgaben abgleicht und konkrete Handlungsfelder sichtbar macht. Anschließend entwickeln wir einen maßgeschneiderten Umsetzungsplan und begleiten die Teilnehmenden bei der strategischen, organisatorischen und technischen Umsetzung der NIS2 Pflichten. Abgerundet wird der Workshop durch eine kompakte Vorstellung unseres NIS2 Trainings speziell für C Level Entscheider, das Führungskräften die regulatorischen Anforderungen, Risiken und Verantwortlichkeiten verständlich und praxisorientiert vermittelt.