Detect & Defend

Orange Cyberdefense Live

Level Up - Compliance meets Cybersecurity

Programm

Inhalt

Cheating is over!

Seien Sie dabei, wenn Compliance auf Cybersecurity trifft. Die Einführung von NIS2 und DORA zwingt Unternehmen, ihre IT-Security-Maßnahmen deutlich zu verbessern, um regulatorischen Anforderungen gerecht zu werden.

Wir stellen diese Anforderungen vor und verraten Ihnen die Geheimnisse aka Zaubertränke für die Umsetzung dieser Anforderungen.
Getreu unserem diesjährigen Motto „Level Up - Compliance meets Cybersecurity“ wollen wir nicht nur bei den Konferenzthemen und -inhalten eine Schippe drauflegen, sondern Sie mit uns auf die nächste Stufe zur ultimativen Cyber-Resilienz & Compliance heben.

Weitere Infos und Anmeldung

unter www.orangecyberdefense.com/de/detect-defend/

Keynotes:

Marc Wallert

Entführungsüberlebender, Resilienz-Experte und Bestseller-Autor

Marc Wallert gilt als Deutschlands bekanntester Resilienz-Experte. Im Jahr 2000 überlebte er eine Entführung und 20 Wochen Geiselhaft im philippinischen Dschungel. Es folgen 20 bewegte Jahre Managerkarriere, Burnout inklusive. Ein Leben voller Rückschläge und Erfolge, ein spezieller Mix aus Führungs- und Entführungserfahrung.

Lassen Sie sich auf der Detect & Defend 2024 von Marc in den Dschungel entführen und gehen Sie innerlich gestärkt wieder heraus. Der Profi lehrt Ihnen praktische Resilienz-Techniken für Ihren persönlichen Dschungel – im Leben und im Business.

Prof. Dr. Dennis-Kenji Kipker

Jurist & Experte für IT-Sicherheitsrecht

Dennis-Kenji Kipker ist Professor für IT-Sicherheitsrecht in Bremen sowie Gastprofessor an der privaten, durch die Soros Foundation begründeten Riga Graduate School of Law in Lettland. Hier forscht er zu Themen an der Schnittstelle von Recht und Technik in der Cybersicherheit, Konzernstrategie sowie zu digitaler Resilienz im Kontext globaler Krisen.

Dr. Oliver Korn

Professor Hochschule Offenburg

Dr. Oliver Korn ist Professor für Human Computer Interaction an der Hochschule Offenburg und Direktor des Affective & Cognitive Institute (ACI). Zudem ist er Prodekan für Forschung und leitet das Zentrum für Entrepreneurship (OGFLab). Forschungsschwerpunkte sind kontextbewusste, intelligente Systeme, Affective Computing, Augmented, Virtual und Mixed Reality sowie Gaming und Gamification.

Detect & Defend
Orange Cyberdefense Live

Agenda Frankfurt am Main – 17.04.2024

08:00–09:00 Uhr: **Registrierung**

09:00–09:15 Uhr: **Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der Orange Cyberdefense Germany**

09:15–10:00 Uhr: **Keynote Marc Wallert**

Zeit	Innovation & Solution Track	Try & Tech Track	Zeit
10:30–11:00	**Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun?** presented by Orange Cyberdefense	**One day in a SOC - Erwartung vs. Realität** presented by Orange Cyberdefense	10:30–11:15
11:10–11:40	**Game On: Prüfungsfest & sicher durch die Level der Compliance** presented by Splunk		
11:50–12:20	**Reframe your SASE ambitions to SASE 2.0** presented by Palo Alto Networks	**Zero Trust erfordert deviceTRUST – „Always verify" auf einem neuen Level** presented by Orange Business	11:30–12:15

12:20–13:30 Uhr: **Lunch**

13:30–14:15 Uhr: **Keynote Dr. Dennis-Kenji Kipker**

14:25–14:55	**Generative AI in Cyber Security: Danger or Gamechanger?** presented by Sentinel One	**Kenne Deinen Feind: Threat Modeling & MITRE Detection Engineering Assessment** presented by Orange Cyberdefense	14:25–15:35
15:05–15:35	**Der neue Boss im Game: Security mit Google Chronicle** presented by Google		

15:35–16:05 Uhr: **Tea & Networking**

16:05–16:35	**Über den Wolken muss die Freiheit wohl grenzenlos und sicher sein! Mit Netskope in neue Security-Dimensionen!** presented by Netskope	**The playbook for emergencies: cyber crisis management - You have been hacked. Now what? (ENG)** presented by Orange Cyberdefense	16:05–16:50
16:45–17:15	**Insights Unleashed: Modern SIEM Monitoring Strategies for Robust Cyberdefense** presented by Orange Cyberdefense		
17:25–17:55	**Compliance durch Managed OT-Security** presented by Orange Cyberdefense	**Erfahrungsbericht: MDR-Service aus dem CyberSOC bei Blanc & Fischer** presented by Orange Cyberdefense & Blanc & Fischer	17:05–17:50

17:55–19:00 Uhr: **Get together mit Getränken**

Innovation & Solution Track - Max 1

10:30 | Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun? presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Die NIS2 Richtlinie wurde am 14. Dezember 22 verabschiedet. Nach wie vor sind genaue Details der Umsetzung in Deutschland teilweise unklar. Allerdings müssen die Anforderungen bis zum 14. Oktober 24 umgesetzt sein. Das ist nicht mal mehr ein halbes Jahr! Also höchste Eisenbahn zu reagieren. In diesem Vortrag werden wir auf die Kerninhalte eingehen: Wer ist betroffen, was muss umgesetzt werden, wie könnte das aussehen? Und natürlich wie Orange Cyberdefense Sie dabei unterstützen kann.

11:10 | Game On: Prüfungsfest & sicher durch die Level der Compliance. presented by Marcel Seifert, Senior Partner Solutions Advisor, Splunk

Fakten schaffen - Die Koexistenz aus Compliance & Cybersecurity. Wie stellen Sie sicher, dass …? - Auf mögliche Auditor-Fragen sollten Teams, für die Sie zuständig sind, vorbereitet sein (was sie aber oft nicht sind).

11:50 | Reframe your SASE ambitions to SASE 2.0 presented by Markus Reiniger, Channel Systems Engineer - Prisma SASE, Palo Alto Networks

Die Revolution für Security und Business-Operations. Erzielen Sie einen unternehmensweiten Mehrwert für Ihre S(A)SE Strategie. KI-Erweiterung und risikobasierte, kontextbezogene Datenanalyse werden die Spielregeln für Cybersecurity-Operations verändern. Integrieren Sie den zukunftssicheren Cloud Native Plattform-Ansatz von Palo Alto und die Top Services von Orange Cyberdefense. Tauchen Sie ein in die Zukunft der IT-Sicherheit mit dem Vortrag über Secure Access Service Edge (SASE). Wir stellen Ihnen die bahnbrechenden Konzepte von SASE vor und zeigen Ihnen, wie Sie Ihre Sicherheitsarchitektur auf die nächste Stufe heben können. Machen Sie sich bereit für eine Reise durch die fortschrittlichen Technologien, die Ihre Netzwerksicherheit transformieren werden.

13:30 | Keynote Dr. Dennis-Kenji Kipker

14:25 | Generative AI in Cyber Security: Danger or Gamechanger? presented by Matthias Canisius, Sales Director Germany, Sentinel One

Die Diskussionen um den Einsatz der generativen Künstlichen Intelligenz (KI) sind derzeit allgegenwärtig. Wo liegen die Gefahren, die von der KI für die Cybersicherheit ausgehen? Wie machen sich Angreifer die KI zu Nutze und was ist eigentlich generative KI? Und wie können wir den Spieß umdrehen und KI zum Schutz vor Cyberangriffen einsetzen?

15:05 | Der neue Boss im Game: Security mit Google Chronicle presented by Pietro Verzi, Partner Customer Engineer, Global Security Sales, Google

Google Chronicle ist der neue Player im SIEM Game. Was zeichnet Chronicle aus, und warum haben wir uns entschieden, Partner von Google für Chronicle zu werden?

16:05 | Über den Wolken muss die Freiheit wohl grenzenlos und sicher sein! Mit Netskope in neue Security-Dimensionen. presented by Frank Barthel, Manager Solution Engineering, Netskope

Der KI-Trend wird sich in den nächsten Jahren fortsetzen, da immer mehr Unternehmen ihre KI-Fähigkeiten für die Gegenwart und die Zukunft ausbauen. Diese Session beleuchtet praktische und effektive Strategien zur sicheren Implementierung von ChatGPT in Unternehmensumgebungen unter Verwendung von Netskope. Wir werden auf Datenschutz, Zugriffskontrolle und Bedrohungsabwehr eingehen, um sicherzustellen, dass die innovative Sprachverarbeitungstechnologie verantwortungsbewusst und geschützt genutzt werden kann. Erfahren Sie, wie Netskope dabei hilft, die Vorteile von ChatGPT in Unternehmen zu maximieren, ohne dabei Sicherheitskompromisse einzugehen. Außerdem erhalten Sie praktische Anleitungen für die Anwendung von Zero Trust, Risiko- und Sicherheitsmanagement auf KI-Systeme.

16:45 | Insights Unleashed: Modern SIEM Monitoring Strategies for Robust Cyberdefense presented by Joachim Schuster, Lead SIEM Specialist/Solution Architect, Orange Cyberdefense

In der Session liegt der Fokus auf der wichtigen Rolle des Überwachens von (SIEM)-Systemen. Ein effizientes Monitoring ist von entscheidender Bedeutung, um sicherzustellen, dass das SIEM-System optimal funktioniert und effektiv auf aktuelle Bedrohungen reagieren kann. Schlüsselthemen umfassen die proaktive Identifizierung von Konfigurationsproblemen, die Integration von automatisierten Überprüfungen und die Optimierung von SIEM-Monitoring-Strategien für eine effektive Leistung.

17:25 | Compliance durch Managed OT-Security presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Nehmen Sie an einem spannenden Vortrag mit unseren Experten teil, in der wir den kritischen Bereich der Cybersecurity in der Industrie beleuchten. Erfahren Sie, wie unsere ‚Secure Industrial Managed LAN Services' dabei helfen können, anspruchsvolle Sicherheitsvorschriften einzuhalten. Gewinnen Sie wertvolle Einblicke in die Nutzung dieser Services, um Compliance- Anforderungen in industriellen Umgebungen zu erfüllen und die OT-Cybersecurity zu optimieren.

Try & Tech Track - Max 2

10:30 | One day in a SOC - Erwartung vs. Realität.
presented by Matthias Bissinger, Head of CyberSOC Germany, Orange Cyberdefense

Sie haben sich schon immer gefragt, was die Typen in schwarzen Kapuzenpullis den ganzen Tag tun, um Ihre Umgebungen und Netzwerke zu überwachen? Tragen die überhaupt schwarze Kapuzenpullis? Seien Sie dabei, wenn wir Ihre Vorstellungen unserer Realität gegenüberstellen und Sie auf einen Tag im Leben eines SOC-Teams mitnehmen.

11:30 | Zero Trust erfordert deviceTRUST – „Always verify" auf einem neuen Level.
presented by Matthias Schlimm, Principal Architect, Login Consultants

Im Zusammenhang mit der Multi-Faktor-Authentifizierung spielen Informationen über das Gerät des Benutzers eine immer wichtigere Rolle. Die sogenannte „Device Posture" ist in diesem Kontext zu einem Thema für alle großen Anbieter und Kunden geworden. Sprich: die Bewertung, welche Gefahren von einem Device ausgehen können.
Um Sicherheitsangriffe zu vermeiden, muss die Zugangskontrolle zu digitalen Arbeitsplätzen und Anwendungen dynamisch sein. Heißt:
Je nachdem, ob die Sicherheits- oder Compliance-Bedingungen des zugreifenden Geräts erfüllt sind oder nicht, muss es für Unternehmen möglich sein, die Zugriffskontrolle jederzeit zu gewähren oder zu widerrufen.
Die Lösung: deviceTRUST bietet höhere Sicherheit für Remote- (Citrix, AVD, VMware Horizon, etc.), lokale und Microsoft SaaS-Umgebungen und bereichert eine Zero-Trust-Strategie um „kontextbasierte Sicherheit" – bei gleichbleibend hoher Benutzerfreundlichkeit!

14:25 | Kenne Deinen Feind: Threat Modeling & MITRE Detection Engineering Assessment.
presented by Simone Kraus, Security Analyst, Orange Cyberdefense

Es hat sich gezeigt, dass viele Unternehmen zwar über Prozesse zur Entwicklung von Use Cases für ihre Sicherheitstools wie SIEM verfügen, die Auswahl jedoch häufig nicht einem „Threat Informed Defense Approach" folgt. Dieser Ansatz zielt darauf ab, Angreifer und ihre Angriffstechniken technisch zu verstehen und Cyberangriffe erfolgreich abzuwehren.
In diesem Workshop lernen Sie, wie Sie ein systematisches Assessment durchführen, um Bedrohungsakteure und ihre TTPs sichtbar zu machen und Schwachstellen in der Abwehr zu identifizieren.
Wir zeigen Ihnen, wie Sie Ihr Detection Engineering und Threat Hunting optimieren können und wie Sie die neu gewonnenen Erkenntnisse nutzen können, um selbst reale Angriffe auf Basis Ihrer eigenen IT-Systemlandschaft zu simulieren oder zu emulieren.
Zudem erfahren Sie, wie Sie MITRE ATT&CK Techniken nicht nur priorisieren können, sondern auch wie Sie die neu gewonnen Kenntnisse nutzen, um zeitnah Ihre Sicherheitslücken zu schließen.
Der Workshop ist praxisorientiert; wir werden gemeinsam Use Cases erstellen. Eine Voranmeldung wird empfohlen, um einen temporären Zugang zur Tidal Cyber Enterprise Edition zu erhalten und die Plattform selbst zu testen. (Es wird empfohlen einen Laptop mitzubringen.)

16:05 | The playbook for emergencies: cyber crisis management - You have been hacked. Now what? (ENG).
presented by Simen Van der Perre, Strategic Advisor, Orange Cyberdefense

Discover actionable strategies for navigating cyber crisis by drawing insights from iconic moments in the IT Crowd TV show. Join us for an interactive session that explores the parallels between cyber crisis management and a not-so-well-executed fire drill. Learn how to enhance organizational preparedness and effectively tackle cyber threats with practical tips and guidance.

17:05 | Erfahrungsbericht: MDR-Service aus dem CyberSOC bei BLANC & FISCHER
presented by Michael Schrenk, Sales Manager, Orange Cyberdefense & Marc-Andre Pantea, Corporate Information Security Officer, BLANC & FISCHER Corporate Services

BLANC & FISCHER berichtet in diesem Vortrag über ihren Weg zum Einsatz eines SOC mit MDR-Services. Was war die Motivation? Warum hat sich das Management für den Invest entschieden? Wie sind sie das Thema angegangen? Warum haben sie sich für Orange Cyberdefense entschieden? Welche Herausforderungen gab es auf dem Weg bis zum Go-Live? Und was haben sie unterschätzt und empfehlen anderen Unternehmen aus dieser Erfahrung heraus?

Detect & Defend
Orange Cyberdefense Live

Agenda Füstenfeldbruck – 24.04.2024

08:00–09:00 Uhr: **Registrierung**

09:00–09:15 Uhr: **Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der Orange Cyberdefense Germany**

09:15–10:00 Uhr: **Keynote Marc Wallert**

Zeit	Innovation Track - Stadtsaal	Solution Track - Säulensaal	Try & Tech Track - Kleiner Saal	Zeit
10:30–11:00	**Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun?** presented by Orange Cyberdefense	**Über den Wolken muss die Freiheit wohl grenzenlos und sicher sein! Mit Netskope in neue Security-Dimensionen!** presented by Netskope	**Purple Teaming: The Next Level in Your Security Maturity (ENG)** presented by Sensepost	10:30–11:15
11:10–11:40	**Ransomware is everywhere** presented by Login Consultants und Orange Cyberdefense	**Die ultimative Spielanleitung: das Security Awareness Training zur Erfüllung von NIS2-Anforderungen** presented by Proofpoint		
11:50–12:20	**The playbook for emergencies: cyber crisis management - You have been hacked. Now what? (ENG)** presented by Orange Cyberdefense	**XDR vs. SIEM – Die Evolution der Cybersecurity Ansätze** presented by Vectra AI	**One day in a SOC - Erwartung vs. Realität** presented by Orange Cyberdefense	11:30–12:15

12:20–13:30 Uhr: **Lunch**

13:30–14:15 Uhr: **Keynote Dr. Dennis-Kenji Kipker**

14:25–14:55	**Künstliche Intelligenz in der Cybersecurity – Ein Spiel mit dem Feuer?** presented by Orange Cyberdefense	**Reframe your SASE ambitions to SASE 2.0** presented by Palo Alto Networks	**Kenne Deinen Feind: Threat Modeling & MITRE Detection Engineering Assessment** presented by Orange Cyberdefense	14:25–15:35
15:05–15:35	**Fortifying Tomorrow: Embracing Cloud Innovation & Mastering Legacy Infrastructure Security (ENG)** presented by Orange Business	**Generative AI in Cyber Security: Danger or Gamechanger?** presented by Sentinel One		

15:35–16:05 Uhr: **Tea & Networking**

16:05–16:35	**Die Orange-Cyberdefense-Engine: Information ist alles!** presented by Orange Cyberdefense	**Upgrade your Email Security! Mit Mimecast, KI und Alliance Partnern den Angriffsvektor #1 absichern** presented by Mimecast	**Turning the Tide with a Threat-Informed Defense Approach (ENG)** presented by Attack IQ	16:05–16:50
16:45–17:15	**From Level Zero to Zero Trust: Risiko- und praxisorientiertes Network Security Assessment** presented by Orange Cyberdefense	**Game On: Prüfungsfest & sicher durch die Level der Compliance** presented by Splunk		

17:15–23:00 Uhr: **Abendevent**

Innovation Track - Stadtsaal

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Marc Wallert

10:30 | Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun? presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Die NIS2 Richtlinie wurde am 14. Dezember 22 verabschiedet. Nach wie vor sind genaue Details der Umsetzung in Deutschland teilweise unklar. Allerdings müssen die Anforderungen bis zum 14. Oktober 24 umgesetzt sein. Das ist nicht mal mehr ein halbes Jahr! Also höchste Eisenbahn zu reagieren. In diesem Vortrag werden wir auf die Kerninhalte eingehen: Wer ist betroffen, was muss umgesetzt werden, wie könnte das aussehen? Und natürlich wie Orange Cyberdefense Sie dabei unterstützen kann.

11:10 | Ransomware is everywhere
presented by Thomas Jupe, Portfolio Manager, Orange Cyberdefense & Matthias Pfeffer, Senior Architect Modern Workplace, Login Consultants

Stellen Sie sich vor, Cyberkriminelle haben sämtliche Unternehmensdaten verschlüsselt und das gesamte System kommt zum Erliegen. Nun müssen Sie schnell handeln, um den Geschäftsbetrieb wieder aufnehmen zu können. Wie lösen Sie dieses Problem in kürzester Zeit so, dass sich der Schaden auf das Minimum reduziert und ohne, dass die Daten im Darknet landen? Was ist dabei für Sie der größte Nutzen, wenn Sie mit Orange zusammenarbeiten?

- Welche Synergien und Vorteile entstehen für Sie bei der Zusammenarbeit mit Orange Business und Orange Cyberdefense
- Der gesicherte, moderne Arbeitsplatz aus einer Hand!
- Wie sieht eine optimale Secure Modern Workplace Journey für Ihr Unternehmen aus
- Tenant Setup und Sicherheitsgrundlagen optimal aufsetzen
- Identität und Zugang bestmöglich sichern
- Endpoint und Devices vor Ransomware Attacken schützen
- Wertvolle Beispiele anhand von zwei User Stories, welche unsere Services verständlich auf den Punkt bringen

11:50 | The playbook for emergencies: cyber crisis management – You have been hacked. Now what? (ENG)
presented by Simen Van der Perre, Strategic Advisor, Orange Cyberdefense

Discover actionable strategies for navigating cyber crisis by drawing insights from iconic moments in the IT Crowd TV show. Join us for an interactive session that explores the parallels between cyber crisis management and a not-so-well-executed fire drill. Learn how to enhance organizational preparedness and effectively tackle cyber threats with practical tips and guidance.

13:30 | Keynote Dr. Dennis-Kenji Kipker

14:25 | Künstliche Intelligenz in der Cybersecurity – Ein Spiel mit dem Feuer? presented by Fabian Beutel, Head of Consulting, Orange Cyberdefense

Mit ChatGPT hat sich in nur wenigen Wochen eine KI Technlologie einer breiten Masse auch nicht technisch interessierter Menschen eröffnet. Microsoft bringt mit „Copilot“ KI direkt in den Office-Einsatz. Doch bei aller Euphorie, gibt es auch kritische Fragestellungen, mit denen sich insbesondere Firmen rasch auseinandersetzen müssen. Neben der Vertraulichkeit der externen Quellen werden Datenschutz, Evasion, Poisoning und Backdoor Angriffe auch bei KI Anwendungen schnell in den Fokus der Sicherheitsabteilungen rücken.

15:05 | Fortifying Tomorrow: Embracing Cloud Innovation & Mastering Legacy Infrastructure Security (ENG)
presented by Johny Gasser, Strategist & Advisor – Cyber Security and Risk Management, Orange Business

16:05 | Die Orange-Cyberdefense-Engine: Information ist alles! presented by Philipp Rieblinger, Security Consultant, Orange Cyberdefense

Eine Game-Engine ist das Framework, auf dem das eigentliche Spiel läuft. Was aber wäre unsere Engine als Unternehmen? „Informationsgetriebene Sicherheit“ ist ein wichtiger Baustein unserer Unternehmensphilosophie. Dieser Vortrag beleuchtet die Rolle von Informationen und wie wir sie bei der Angriffserkennung nutzen, ganz nach dem Motto „Detect & Defend“.

16:45 | From Level Zero to Zero Trust: Risiko- und praxisorientiertes Network Security Assessment
presented by Christian Thiem, Senior Security Consultant, Orange Cyberdefense

Zero Trust nur ein Buzzword? Mikrosegmentierung nur ein Mythos? Keineswegs! Nachdem wir zunächst die Begrifflichkeiten geklärt haben, geht es direkt an das Eingemachte!
Wir stellen Ihnen vor, wie wir im Rahmen eines Assessments die Network Security Posture Ihrer IT-Infrastruktur analysieren, Lücken identifizieren und konkrete Lösungen anbieten und wie wir dies im letzten Jahr bereits bei mehreren Kunden erfolgreich umgesetzt haben.

Solution Track - Säulensaal

10:30 | Über den Wolken muss die Freiheit wohl grenzenlos und sicher sein! Mit Netskope in neue Security-Dimensionen!
presented by Thomas Oltmanns, Channel Sales Engineer, Netskope

Der KI-Trend wird sich in den nächsten Jahren fortsetzen, da immer mehr Unternehmen ihre KI-Fähigkeiten für die Gegenwart und die Zukunft ausbauen. Die Session beleuchtet praktische und effektive Strategien zur sicheren Implementierung von ChatGPT in Unternehmensumgebungen unter Verwendung von Netskope. Wir werden auf Datenschutz, Zugriffskontrolle und Bedrohungsabwehr eingehen, um sicherzustellen, dass die innovative Sprachverarbeitungstechnologie verantwortungsbewusst und geschützt genutzt werden kann. Erfahren Sie, wie Netskope dabei hilft, die Vorteile von ChatGPT in Unternehmen zu maximieren, ohne dabei Sicherheitskompromisse einzugehen. Außerdem erhalten Sie praktische Anleitungen für die Anwendung von Zero Trust, Risiko- und Sicherheitsmanagement auf KI-Systeme.

11:10 | Die ultimative Spielanleitung: das Security Awareness Training zur Erfüllung von NIS2-Anforderungen
presented by Henning Hanke, Channel Account Manager, Proofpoint & Alexander Sebestian, Staff Channel Sales Engineer Proofpoint

Das Security Awareness Training von Proofpoint bietet eine umfassende Spielanleitung zur Erfüllung der NIS2-Anforderungen. Diese Präsentation beleuchtet die entscheidende Rolle von Sicherheitsbewusstseinstrainings im Kontext der NIS2-Compliance. Es werden die verschiedenen Aspekte des Trainings hervorgehoben, darunter interaktive Lernmodule, praxisnahe Szenarien und maßgeschneiderte Inhalte. Die ultimative Spielanleitung von Proofpoint zielt darauf ab, das Bewusstsein für Sicherheitsrisiken zu schärfen, die Mitarbeiter zu befähigen, Bedrohungen zu erkennen und bewährte Praktiken in der Cybersecurity zu fördern. Diese Präsentation bietet einen Einblick in die Wirksamkeit dieses Trainingsprogramms und seine Bedeutung für die Einhaltung der NIS2-Richtlinien.

11:50 | XDR vs. SIEM – Die Evolution der Cybersecurity Ansätze
presented by Michael Tapken, Manager Commercial Sales Germany, Vectra

XDR (Extended Detection and Response), als aufkommende Technologie, verspricht eine umfassendere und proaktivere Sicherheitsstrategie durch die Integration verschiedener Sicherheitskontrollen und Analyse von Telemetriedaten in Echtzeit. Im Gegensatz dazu hat SIEM (Security Information and Event Management) bereits eine etablierte Präsenz und bietet eine zentrale Plattform zur Erfassung, Analyse und Korrelation von Sicherheitsereignissen aus verschiedenen Quellen. Der Vortrag beleuchtet die Unterschiede zwischen den beiden Ansätzen, ihre jeweiligen Vor- und Nachteile sowie ihre Rolle in der modernen Cybersicherheitslandschaft. Letztendlich werden die Herausforderungen und Chancen diskutiert, die sich aus der Wahl zwischen XDR und SIEM für Organisationen ergeben.

14:25 | Reframe your SASE ambitions to SASE 2.0
presented by Markus Reiniger, Channel Systems Engineer - Prisma SASE, Palo Alto Networks

Die Revolution für Security und Business-Operations. Erzielen Sie einen unternehmensweiten Mehrwert für Ihre S(A)SE Strategie. KI-Erweiterung und risikobasierte, kontextbezogene Datenanalyse werden die Spielregeln für Cybersecurity-Operations verändern. Integrieren Sie den zukunftssicheren Cloud Native Plattform-Ansatz von Palo Alto und die Top Services von Orange Cyberdefense. Tauchen Sie ein in die Zukunft der IT-Sicherheit mit dem Vortrag über Secure Access Service Edge (SASE). Wir stellen Ihnen die bahnbrechenden Konzepte von SASE vor und zeigen Ihnen, wie Sie Ihre Sicherheitsarchitektur auf die nächste Stufe heben können. Machen Sie sich bereit für eine Reise durch die fortschrittlichen Technologien, die Ihre Netzwerksicherheit transformieren werden.

15:05 | Generative AI in Cyber Security: Danger or Gamechanger? presented by Matthias Canisius, Sales Director Germany, Sentinel One

Die Diskussionen um den Einsatz der generativen Künstlichen Intelligenz (KI) sind derzeit allgegenwärtig. Wo liegen die Gefahren, die von der KI für die Cybersicherheit ausgehen? Wie machen sich Angreifer die KI zu Nutze und was ist eigentlich generative KI? Und wie können wir den Spieß umdrehen und KI zum Schutz vor Cyberangriffen einsetzen?

16:05 | Upgrade your Email Security! Mit Mimecast, KI und Alliance Partnern den Angriffsvektor #1 absichern. presented by Marius Holmer, Team Lead Commercial Sales DACH, Mimecast

Die Wichtigkeit einer guten E-Mail Security Lösung ist den meisten Unternehmen durchaus bekannt. Durch neuartige Angriffsvarianten, wie QR-Code Attacken oder KI-basierte Angriffe, müssen Unternehmen in der Lage sein, auch ihnen bis dahin unbekannte Gefahren möglichst schnell abwehren zu können. Mimecast unterstützt mit seiner dynamischen Plattform Unternehmen, die auf diese Verschärfung der Cyberangriffe reagieren wollen, indem sie Unternehmen unterstützt diese neuen und komplexen Offensiven abzuwehren ohne dabei den Workload der meist voll ausgelasteten IT-Mannschaft zu strapazieren.

16:45 | Game On: Prüfungsfest & sicher durch die Level der Compliance. presented by Marcel Seifert, Senior Partner Solutions Advisor, Splunk

Fakten schaffen - Die Koexistenz aus Compliance & Cybersecurity. Wie stellen Sie sicher, dass …? - Auf mögliche Auditor-Fragen sollten Teams, für die Sie zuständig sind, vorbereitet sein (was sie aber oft nicht sind).

Try & Tech Track - Kleiner Saal

10:30 | Purple Teaming: The Next Level in your Security Maturity (ENG) presented by Leon Jacobs, Chief Technology Officer, SensePost

It‘s become increasingly evident that we simply dont have the luxury of time when it comes to cyber challenges. Incidents happen fast, and our ability to respond quickly and accurately needs to be almost instinctive. In this workshop I‘ll introduce the concept of purple teaming and how its fast, iterative feedback loop can meaningfully empower your blue team to better detect and respond to the next incident.

11:30 | One day in a SOC - Erwartung vs. Realität
presented by Matthias Bissinger, Head of CyberSOC Germany, Orange Cyberdefense

Sie haben sich schon immer gefragt, was die Typen in schwarzen Kapuzenpullis den ganzen Tag tun, um IhreUmgebungen und Netzwerke zu überwachen? Tragen die überhaupt schwarze Kapuzenpullis? Seien Sie dabei, wenn wir Ihre Vorstellungen unserer Realität gegenüberstellen und Sie auf einen Tag im Leben eines SOC-Teams mitnehmen.

14:25 | Kenne Deinen Feind: Threat Modeling & MITRE Detection Engineering Assessment.
presented by Simone Kraus, Security Analyst, Orange Cyberdefense

Es hat sich gezeigt, dass viele Unternehmen zwar über Prozesse zur Entwicklung von Use Cases für ihre Sicherheitstools wie SIEM verfügen, die Auswahl jedoch häufig nicht einem „Threat Informed Defense Approach“ folgt. Dieser Ansatz zielt darauf ab, Angreifer und ihre Angriffstechniken technisch zu verstehen und Cyberangriffe erfolgreich abzuwehren.
In diesem Workshop lernen Sie, wie Sie ein systematisches Assessment durchführen, um Bedrohungsakteure und ihre TTPs sichtbar zu machen und Schwachstellen in der Abwehr zu identifizieren.
Wir zeigen Ihnen, wie Sie Ihr Detection Engineering und Threat Hunting optimieren können und wie Sie die neu gewonnenen Erkenntnisse nutzen können, um selbst reale Angriffe auf Basis Ihrer eigenen IT-Systemlandschaft zu simulieren oder zu emulieren.
Zudem erfahren Sie, wie Sie MITRE ATT&CK Techniken nicht nur priorisieren können, sondern auch wie Sie die neu gewonnen Kenntnisse nutzen, um zeitnah Ihre Sicherheitslücken zu schließen.

Der Workshop ist praxisorientiert; wir werden gemeinsam Use Cases erstellen. Eine Voranmeldung wird empfohlen, um einen temporären Zugang zur Tidal Cyber Enterprise Edition zu erhalten und die Plattform selbst zu testen. (Es wird empfohlen einen Laptop mitzubringen.)

16:05 | Turning the Tide with a Threat-Informed Defense Approach (ENG) presented by Andrew Habibi-Parker, Senior Technical Director, EMEA, Attack IQ

Doing the same thing time and time again and expecting a different result is the accepted definition of madness, yet in cyber security we seem resolutely stuck on that trajectory. What if there was a different way to manage the increasing cyber security challenge we all face, that’s more specific to your business risks? A Threat-Informed Defense approach is that different way. Join us to learn what a Threat-Informed Defense approach is, how it can help you focus your cyber security efforts, and how organisations are benefitting from this methodology today.
Eine Voranmeldung ist empfohlen.

Detect & Defend
Orange Cyberdefense Live

Agenda Füstenfeldbruck – 25.04.2024

08:00–09:00 Uhr: **Registrierung**

09:00–09:15 Uhr: **Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der Orange Cyberdefense Germany**

09:15–10:00 Uhr: **Keynote Dr. Oliver Korn**

Zeit	Innovation Track - Stadtsaal	Solution Track - Säulensaal	Try & Tech Track - Kleiner Saal	Zeit
10:30–11:00	**Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun?** presented by Orange Cyberdefense	**Coverage Mapping with Threat-Informed Defense (ENG)** presented by Tidal Cyber	**Cyber Threat Intelligence workshop: Is Orange Cyberdefense really intelligence-led? (ENG)** presented by Orange Cyberdefense CERT-Team	10:30–11:15
11:10–11:40	**The playbook for emergencies: cyber crisis management – You have been hacked. Now what? (ENG)** presented by Orange Cyberdefense	**Der neue Boss im Game: Security mit Google Chronicle** presented by Google		
11:50–12:20	**Podiumsdiskussion: Gemeinsam die Welt der Microsoft-Security rocken.** presented by Orange Cyberdefense & WTS Group AG	**CAASM: Turn Asset Management Into An Asset To Your Business (ENG)** presented by Axonius	**Schneller, Stärker, Sicherer: AWS-Incident-Response mit Level-Up-Speed** presented by Orange Cyberdefense	11:30–12:15
12:20–13:30 Uhr: **Lunch**				
13:30–14:00	**Erfahrungsbericht: MDR-Service aus dem CyberSOC bei Blanc & Fischer** presented by Orange Cyberdefense & Blanc & Fischer	**Achievement unlocked: Sicherer Einsatz von ChatGPT & Co. - Managed Data Loss Prevention von Orange Cyberdefense** presented by Forcepoint	**Interaktives Planspiel: Simulation eines Cyber-Angriffs** presented by Bayerisches Landeskriminalamt - Cybercrime	13:30–14:15
14:10–14:40	**Insights Unleashed: Modern SIEM Monitoring Strategies for Robust Cyberdefense** presented by Orange Cyberdefense	**Next level unlocked mit oldschool KI** presented by Blackberry		
14:50–15:20	**Podiumsdiskussion Incident Response** presented by Orange Cyberdefense & Hitzler Ingenieure	**Compliance durch Managed OT-Security** presented by Orange Cyberdefense	**Level Up on your Data Management Strategy - How to build a data engine for your security data** presented by Cribl	14:30–15:15
15:20–16:00 Uhr: **Tea & Networking**				

Innovation Track - Stadtsaal

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Dr. Oliver Korn

10:30 | Cheating is over. NIS2 & KRITIS stehen vor der Tür. Und nun? presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Die NIS2 Richtlinie wurde am 14. Dezember 22 verabschiedet. Nach wie vor sind genaue Details der Umsetzung in Deutschland teilweise unklar. Allerdings müssen die Anforderungen bis zum 14. Oktober 24 umgesetzt sein. Das ist nicht mal mehr ein halbes Jahr! Also höchste Eisenbahn zu reagieren. In diesem Vortrag werden wir auf die Kerninhalte eingehen: Wer ist betroffen, was muss umgesetzt werden, wie könnte das aussehen? Und natürlich wie Orange Cyberdefense Sie dabei unterstützen kann.

11:10 | The playbook for emergencies: cyber crisis management – You have been hacked. Now what? (ENG)
presented by Simen Van der Perre, Strategic Advisor, Orange Cyberdefense

Discover actionable strategies for navigating cyber crisis by drawing insights from iconic moments in the IT Crowd TV show. Join us for an interactive session that explores the parallels between cyber crisis management and a not-so-well-executed fire drill. Learn how to enhance organizational preparedness and effectively tackle cyber threats with practical tips and guidance.

11:50 | Podiumsdiskussion: Gemeinsam die Welt der Microsoft-Security rocken.
presented by Thomas Jupe, Portfolio Manager, Orange Cyberdefense, Matthias Pfeffer, Senior Architect Modern Workplace, Login Consultants & Thomas Wimschneider, CIO, WTS Group AG

Tauchen Sie ein in die fesselnde Partnerschaft zweier führender Unternehmen, die sich auf Microsoft-Security spezialisiert haben. In diesem Podiumsvortrag stehen nicht nur innovative Lösungen im Mittelpunkt, sondern auch die Erfolgsgeschichte einer fruchtbaren Zusammenarbeit. Die beiden Unternehmen präsentieren gemeinsam das Microsoft Security Architecture Poster, ein wegweisendes Werkzeug für die Gestaltung einer robusten Sicherheitsinfrastruktur.

Ein besonderes Highlight dieses Vortrags ist die Präsentation eines aktuellen IT-Projekts, das in enger Kooperation mit einem Kunden realisiert wurde. Durch ein Praxisbeispiel erhalten die Zuhörer Einblicke in die praktische Umsetzung der Sicherheitskonzepte und können von den Erfahrungen des Kunden profitieren. Erleben Sie, wie durch die gebündelte Expertise und das Engagement der Partnerunternehmen Sicherheitslösungen entwickelt werden, die den Anforderungen moderner IT-Landschaften gerecht werden.

Dieser Vortrag bietet nicht nur einen Einblick in die neuesten Entwicklungen im Bereich Microsoft Security, sondern auch wertvolle Einblicke in bewährte Praktiken und erfolgreiche Partnerschaften. Seien Sie dabei, wenn Innovation und Zusammenarbeit zu mehr Sicherheit in der digitalen Welt führen.

13:30 | Erfahrungsbericht: MDR-Service aus dem CyberSOC bei BLANC & FISCHER
presented by Michael Schrenk, Sales Manager, Orange Cyberdefense & Daniel Lutz, IT Services | Risk, Security and Compliance Management, BLANC & FISCHER Corporate Services

BLANC & FISCHER berichtet in diesem Vortrag über ihren Weg zum Einsatz eines SOC mit MDR-Services. Was war die Motivation? Warum hat sich das Management für den Invest entschieden? Wie sind sie das Thema angegangen? Warum haben sie sich für Orange Cyberdefense entschieden? Welche Herausforderungen gab es auf dem Weg bis zum Go-Live? Und was haben sie unterschätzt und empfehlen anderen Unternehmen aus dieser Erfahrung heraus?

14:10 | Insights Unleashed: Modern SIEM Monitoring Strategies for Robust Cyberdefense
presented by Joachim Schuster, Lead SIEM Specialist / Solution Architect, Orange Cyberdefense

In der Session liegt der Fokus auf der wichtigen Rolle des Überwachens von (SIEM)-Systemen. Ein effizientes Monitoring ist von entscheidender Bedeutung, um sicherzustellen, dass das SIEM-System optimal funktioniert und effektiv auf aktuelle Bedrohungen reagieren kann. Schlüsselthemen umfassen die proaktive Identifizierung von Konfigurationsproblemen, die Integration von automatisierten Überprüfungen und die Optimierung von SIEM-Monitoring-Strategien für eine effektive Leistung.

14:50 | Podiumsdiskussion Incident Response
presented by Ralf Czekalla, Head of Business Development, Orange Cyberdefense & Hitzler Ingenieure

Ein Cyber Incident kann jeden treffen. Was geschieht bei und mit den Betroffenen? Was sind die Schritte während eines Incident-Response-Einsatzes? All das erfahren Sie bei unserer spannenden Podiumsdiskussion!

Solution Track - Säulensaal

10:30 | Coverage Mapping with Threat-Informed Defense (ENG) presented by Ian Davila, Lead Adversary Emulation Engineer, Tidal Cyber

As threats emerge and adversaries‘ TTPs progressively change, the ability to rapidly assess relevant coverage across multiple defensive stacks becomes increasingly important. By pairing the threats most relevant to an organization with the tools in an organization‘s defensive stack, we can take a quick snapshot in time to assess and determine priorities.

Threat reports and repositories now contain detections around recently observed indicators & behaviors (a positive trend), it is tempting to think that deploying only those detections means successful implementation of „threat-informed defense“. However, our research suggests adversaries are evolving their tactics, techniques, & procedures with increasing frequency and in ways that specifically target parts of the attack surface that are especially challenging to defend.

Layering (and distributing) defensive capabilities against today‘s threats is essential but making a quick assessment of coverage – that is both deep and wide – for each new threat is near-impossible if using traditional approaches. This talk will review Threat-Informed Defense workflows for speeding up coverage assessments through threat & defensive prioritization with the Tidal Cyber Enterprise platform.

11:10 | Der neue Boss im Game: Security mit Google Chronicle presented by Pietro Verzi, Partner Customer Engineer, Global Security Sales, Google

Google Chronicle ist der neue Player im SIEM Game. Was zeichnet Chronicle aus, und warum haben wir uns entschieden, Partner von Google für Chronicle zu werden?

11:50 | CAASM: Turn Asset Management Into An Asset To Your Business (ENG) presented by Tapio Väärämäki, Senior Channel Manager, Axonius

IT and security are undeniably dynamic. A few years from now — let alone a few months from now — it‘s impossible to predict where we‘ll be. One thing’s for certain, though: complexity in cybersecurity is inevitable, and it’s increasing.

Simply put, more complexity equals less visibility. But emerging technology Cyber Asset Attack Surface Management (CAASM) can help. CAASM provides a strategic, contextual, unified view of all assets through API integrations with existing tools, data correlation at scale, and querying capabilities to find and respond to gaps — helping IT and security teams adapt to the needs of their modern environments and control complexity.

Join this session to learn:

- How the CAASM category came to be
- Why the emergence of CAASM is so timely
- How CAASM transforms your teams’ understanding of assets and ability to take action

13:30 | Achievement unlocked: Sicherer Einsatz von ChatGPT & Co. - Managed Data Loss Prevention von Orange Cyberdefense. presented by Stephan Hanke, Senior Sales Engineer, Forcepoint

Neue Technologien ermöglichen neue Arbeitsweisen. Generative KI wie ChatGPT & Co. bieten vielfältige Einsatzmöglichkeiten zur Effizienzsteigerung, bergen aber auch großes Risiko eines ungewollten Informationsabflusses. Forcepoint und Orange Cyberdefense präsentieren den neuen Service Managed Data Loss Prevention, um Sie nicht nur vor den Herausforderungen der künstlichen Intelligenz zu schützen, sondern um Sie auf Ihrer gesamten Data Security Journey zu begleiten.

14:10 | Next level unlocked mit oldschool KI presented by Simon Bilek, Principal Sales Engineer EMEA, Blackberry

Die stetige Weiterentwicklung von Technologien und das Aufkommen von generativer KI, eröffnet neue Chancen für die Cybersicherheit als auch die Bedrohungsakteure. Gemeinsam mit Ihnen gehen wir auf die richtigen Fragen ein, mit dessen Antworten Sie im Nachgang beurteilen können, ob Lösungen einen Mehrwert und ROI bieten und nicht nur ein Marketing-Hype sind.

14:50 | Compliance durch Managed OT Security presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Nehmen Sie an einem spannenden Vortrag mit unseren Experten teil, in der wir den kritischen Bereich der Cybersecurity in der Industrie beleuchten. Erfahren Sie, wie unsere ‚Secure Industrial Managed LAN Services‘ dabei helfen können, anspruchsvolle Sicherheitsvorschriften einzuhalten. Gewinnen Sie wertvolle Einblicke in die Nutzung dieser Services, um Compliance- Anforderungen in industriellen Umgebungen zu erfüllen und die OT-Cybersecurity zu optimieren.

Try & Tech Track - Kleiner Saal

10:30 | Cyber Threat Intelligence workshop: Is Orange Cyberdefense really intelligence-led? (ENG)
presented by Emma Langlet, International Business Developer, Orange Cyberdefense CERT-Team

Deep dive into the cybercrime underground: how ransomware evade law enforcement operations and mislead defenders?

- Discover World Watch's unique ransomware cartography from 2014 to 2024
- Learn how CERT Orange Cyberdefense analysts use custom toolings for their CTI investigation
- Improve your knowledge about the ransomware ecosystem and inherent labor division

11:30 | Schneller, Stärker, Sicherer: AWS-Incident-Response mit Level-Up-Speed
presented by Ante Popic, Security Engineer, Orange Cyberdefense

Im sich stetig wandelnden Feld der Cyber-Sicherheit ist die Kunst, auf Sicherheitsvorfälle mit der richtigen Mischung aus Schnelligkeit und Sachverstand zu reagieren, absolut zentral. Obwohl zahlreiche Organisationen eine solide theoretische Basis in Bezug auf Angriffsmuster und Analysetechniken aufweisen, fehlt es oft an der essenziellen praktischen Erfahrung, diese Kenntnisse effektiv in die Praxis umzusetzen.
In unserem Workshop enthüllen wir die Geheimnisse hinter Adversary Emulation und Incident Response in AWS. Wir führen Sie durch die Gestaltung eines Labs in AWS, das speziell dafür entwickelt wurde, um realistische Angriffsszenarien zu simulieren und darauf zu reagieren.

13:30 | Interaktives Planspiel: Simulation eines Cyber-Angriffs.
presented by Bayerisches Landeskriminalamt - Cybercrime

Innerhalb des Planspiels führen wir Sie durch einen simulierten Cyber-Angriff auf ein Unternehmen. Sie müssen verschiedene Fragestellungen lösen und lernen spielerisch, welche Dimensionen bei einem Angriff auf Sie zukommen können und was dann geeignete Maßnahmen sind.

14:30 | Level Up on your Data Management Strategy - How to build a data engine for your security data
presented by Christoph Dittmann, Sr. Solution Engineer, Cribl

Die Bewältigung der Flut an Security relevanten Daten und deren enormes Volumen entscheidet darüber, ob ein Angriff erkannt oder eine kritische Warnung übersehen wird. Laut IDC wächst die Datenmengen um 28% pro Jahr, sodass sich die Gesamtmenge der Daten in nur drei Jahren verdoppeln wird! Wie können Ihre Teams und SIEM/SOAR/XDR-Tools diese Daten weiterhin sammeln, verarbeiten, weiterleiten und analysieren, ohne dass die Qualität beeinträchtigt wird oder die Kosten steigen? Nehmen Sie an dieser Session teil, um zu erfahren, wie Sie eine effektive Daten-Engine und Strategie für Ihre Sicherheitsdaten aufbauen können:

- Optimieren Sie die Einbindung und Verwaltung neuer Datenquellen in Ihre SIEM/XDR-Lösungen
- Reichern Sie Sicherheitsdaten in Echtzeit mit Threat Intelligence, GeoIP, Asset-Informationen und vielem mehr an, um schneller auf Bedrohungen reagieren zu können
- Analysieren, sammeln, verarbeiten und leiten Sie Ihre Daten in jedem Umfang, in offenen Formaten, mit völliger Freiheit weiter ohne Anbieterbindung
- Datenverarbeitung und -sammlung an der Quelle – skalierbar – und Erweiterung Ihrer Optionen im Umgang mit den Daten
- Führen Sie föderierte „search-in-place"-Abfragen auf beliebigen Daten in jedem Format und an jedem Aufbewahrungsort durch, um Ihre Analysen durchzuführen, ohne dass die Kosten oder die Komplexität der erstmaligen Übertragung, Verarbeitung und Speicherung der Daten erforderlich sind

Locations & Anfahrt

House of Logistics & Mobility (HOLM)
Bessie-Coleman-Straße 7
60549 Frankfurt am Main
www.frankfurt-holm.de

Getting there:

Anreise mit den öffentlichen Verkehrsmitteln:
Das HOLM liegt unmittelbar an der S-Bahn-Haltestelle „Gateway Gardens“ und ist mit den Linien S8 und S9 direkt aus Frankfurt, Hanau, Mainz, Offenbach und Wiesbaden zu erreichen. Alternativ halten folgende Buslinien in Fußnähe:
Busse X17, 77: Haltestelle „Thea-Rasche-Straße“
Busse X19, 61/62: Haltestelle „Kreisel Unterschweinstiege“

Anreise mit dem PKW:
Das HOLM liegt direkt am Autobahnkreuz A5/A3, neben dem Flughafen Frankfurt.

Parken direkt an der Location ist nicht möglich, nutzen Sie bitte die Parkangebote der umliegenden zu Fuß erreichbaren Hotels, beispielsweise PARK INN BY RADISSON Frankfurt Airport (Amelia Mary Earhart Str.10, 60549 Frankfurt am Main), HYATT PLACE Frankfurt Airport (De Saint Exupéry Strasse 4, 60549 Frankfurt am Main) oder HOLIDAY INN Frankfurt Airport (Bessie Coleman Strasse 16, 60549 Frankfurt am Main).

Veranstaltungsforum Fürstenfeld
Fürstenfeld 12
82256 Fürstenfeldbruck
www.fuerstenfeld.de

Getting there:

Anreise mit den öffentlichen Verkehrsmitteln:
Die S-Bahnlinie 4 bietet im 20-Minuten-Takt eine regelmäßige Verbindung nach München. Die S-Bahn-Station „Fürstenfeldbruck“ liegt rund zehn Minuten Fußweg vom Veranstaltungsforum entfernt.

Anreise mit dem PKW:
A96 München-Lindau: Ausfahrt „Germering Nord“ oder A 8 München-Stuttgart: Ausfahrt „Dachau/FFB“. Im Stadtgebiet Fürstenfeldbruck ist das „Kloster Fürstenfeld / Veranstaltungsforum“ gut ausgeschildert. Kostenfreie Parkplätze finden Sie direkt am Veranstaltungsforum (Fürstenfelder Straße).

Wenn Sie für Ihre Anfahrt ein Navigationsgerät nutzen, geben Sie bitte folgende Adresse ein: 82256 Fürstenfeldbruck, Zisterzienserweg (nicht „Fürstenfeld 12“!). Sie werden dann automatisch auf einen großen kostenfreien Parkplatz direkt gegenüber des Veranstaltungsforums geführt.

powered by:

ATTACKIQ®

netskope

AXONIUS

NOZOMI NETWORKS

BlackBerry® | Cybersecurity

paloalto® NETWORKS

Cribl®

proofpoint™

Forcepoint

SentinelOne®

Google Cloud

splunk>®

Microsoft

TIDAL CYBER
THREAT-INFORMED DEFENSE

mimecast™

VECTRA®

www.orangecyberdefense.de