
Detect
Defend &
Orange Cyberdefense Live
Art of Cyberdefense
08. Mai Eppstein
15. Mai Fürstenfeldbruck
22. Mai Dortmund

Programm

Inhalt

Werden Sie zum Künstler Ihrer eigenen IT-Security!

Tauchen Sie ein in die Welt der Cybersecurity, wo Compliance auf Kreativität trifft und aus Herausforderungen wahre Kunstwerke entstehen. Die Einführung von NIS2 und DORA stellt Unternehmen vor neue Aufgaben – doch keine Sorge: Wir liefern nicht nur den Pinsel, sondern auch die Palette an Lösungen, mit denen Sie diese Anforderungen meisterhaft umsetzen können.

Erleben Sie bei der Detect & Defend die Kunst der Cyberabwehr hautnah – dieses Jahr nicht nur in Frankfurt und Fürstenfeldbruck, sondern erstmals auch in Dortmund. Drei Bühnen, unzählige Perspektiven, ein Ziel: Ihre Sicherheit. Wir verbinden technische Tiefgänge mit visionären Ansätzen und zeigen Ihnen, wie Sie aus regulatorischen Vorgaben keine Bürde, sondern einen Rahmen für Innovation schaffen können.

Weitere Infos und Anmeldung

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

Keynotes:

Simon Pierro

KI-Magier

Simon Pierro ist ein weltweit gefeierter Pionier der digitalen Zauberkunst. Mit seiner einzigartigen Verbindung von technologischer Innovation und kreativer Magie erschafft er eine moderne Kunstform, die staunen lässt. Seine Shows sind eine faszinierende Verbindung von Illusion und Technologie, die komplexe Themen wie künstliche Intelligenz spielerisch und fesselnd erlebbar machen.

Erleben Sie auf der Detect & Defend 2025, wie Magie und Cybersicherheit zu einer packenden Einheit verschmelzen. Lassen Sie sich von Simon Pierro in eine Welt entführen, in der Technologie zur Bühne wird und Magie als Ausdruck künstlerischer Vision begeistert!

Gilles van Heijst

Head of Service Design & Architecture, Orange Cyberdefense

Picture this: a wide-eyed 9-year-old kid, glued to the flickering glow of an 8086 PC, its CGA 4-color graphics painting a world of wonder. That was me, and from that moment, I was utterly obsessed with the magic of bits and bytes. What started as a childhood crush turned into a lifelong love affair with IT—a journey that's taken me deep into the wilds of networking and security, where I've built a rock-solid foundation.

Now, at Orange Cyberdefense, I've worn multiple hats, always shouting from the rooftops about the power of Automation and Innovation. As Head of Service Design and Architecture, I'm the mad scientist in the lab, cooking up standards, streamlining onboarding automation, and gearing up for the next big thing: unleashing AI Agents to tackle tasks like the tech superheroes they are....“

Detect & Defend
Orange Cyberdefense Live

Agenda Eppstein - 08.05.2025

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 Simon Pierro

Zeit	Track 1 - Big Store	Track 2 - Offside	Track 3 - Skinny I	Track 4 - Skinny II
10:30–11:00	**Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit** presented by Palo Alto Networks	**Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury?** presented by Akamai	**OT Cybersecurity Best Practices** presented by Orange Cyberdefense	**DORA Roundtable** presented by Orange Cyberdefense
11:15–11:45	**Paint it Black: Live Analyse einer Black Basta Attack Campaign** presented by Orange Cyberdefense	**NIS2: wie man eine Machete einsetzt** presented by Orange Cyberdefense		
12:00–12:30	**Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert** presented by Sentinel One	**Best Practice: Implementierung eines SOC** presented by Trinks GmbH & Orange Cyberdefense		
12:30–13:45 Uhr: **Lunch**				
13:45–14:15	**Podiumsdiskussion: Das Spiel mit den Pinselstrichen: Compliance und die Kunst der Cyberverteidigung** presented by Matrix42	**Die Kunst der Proaktivität: Breach & Attack Simulation als kreatives Werkzeug für Sicherheit** presented by BestSecret	**Impuls: European sovereignty without banning all non-European vendors** presented by Orange Cyberdefense	
14:30–15:00	**Cyber is Art - Art is Experience - meet the Cyber Experience** presented by Orange Cyberdefense	**Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf?** presented by SKW Schwarz	**The Art of Awareness - Sensibilisierung in Zeiten von KI** presented by Orange Cyberdefense	
15:15–15:45	**Breaking down silos – Minimizing attack surface** presented by Axonius	**Schon mal über eine ganzheitliche Sicherheitsplattform nachgedacht?** presented by Google	**The Art of Finding a needle in the Haystack** presented by Orange Cyberdefense	
15:45–16:15 Uhr: Tea & Networking				
16:15–16:45	**Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE** presented by Orange Cyberdefense	**The Art of Social Engineering** presented by Orange Cyberdefense		
17:00–17:30	**OT Security – Innovation für die „letzte Meile“** presented by Weidmüller & Orange Cyberdefense	**One day in a SOC** presented by Orange Cyberdefense		
17:30–22:00 Uhr: **Abendevent**				

Track 1 - Big Store

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Simon Pierro

10:30 | Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit presented by Adela Vacaru, Team Lead Solutions Architects Cortex Cloud Germany, Palo Alto Networks

Cortex® Cloud vereint die nächste Version von Prisma® Cloud mit Cloud Detection & Response. SOC-Teams erhalten eine kontextgesteuerte Verteidigung – kontinuierlichen Schutz vom Code über die Cloud bis zum SOC. Dank der Plattformisierung werden Schwachstellen priorisiert, bevor sie zu aktiven Bedrohungen werden. Die Automatisierung schließt den Kreis bei kritischen Problemen und löst Risiken, bevor Angreifer sie ausnutzen. Basierend auf KI, Orchestrierung und Automatisierung, ergänzt durch die CNAPP-Funktionen von Prisma Cloud, müssen Sicherheitsteams nicht mehr mit getrennten Tools und Workflows navigieren, und die Arbeitsbelastung wird vereinfacht. Seien Sie Angreifern einen Schritt voraus – in Echtzeit und mit weniger Stress.

11:15 | Paint it Black: Live Analyse einer Black Basta Attack Campaign presented by Friedl Holzner, Team Lead CyberSOC & André Henschel, Analyst Cybersecurity, Orange Cyberdefense

Stellen Sie sich vor, Ihr Posteingang wird mit tausenden Spam-E-Mails überflutet – und genau in diesem Moment meldet sich Ihr IT-Support über Microsoft Teams, um Hilfe anzubieten. Kein Zufall, sondern ein gezielter Angriff.
Ende letzten Jahres beobachtete das Orange Cyberdefense CyberSOC eine Welle solcher Attacken, bei denen Malware eingeschleust und Ransomware-Angriffe vorbereitet wurden. In dieser Live-Demo zeigen wir, wie ein solcher Angriff abläuft – von den ersten Anzeichen eines bevorstehenden Angriffs, über Social Engineering Techniken und Malware Delivery bis hin zur Detektion und Analyse der ausgeführten Malware.

12:00 | Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert
presented by Oliver Weil, Enterprise Sales Representative, Sentinel One

Mit ausgefeilteren Angriffen, die auch auf KI zurückgreifen, kommen immer mehr klassische Sicherheitslösungen an ihre Grenzen. Doch autonome KI-Systeme versprechen auch eine schnellere und effektivere Bedrohungsserkennung. Aber sind sie wirklich zuverlässig? Wir werfen einen Blick auf Chancen, Herausforderungen und reale Anwendungsfälle.

13:45 | Podiumsdiskussion: Das Spiel mit den Pinselstrichen: Compliance und die Kunst der Cyberverteidigung presented by Thomas Langholz, Matrix42

In dieser Diskussion begrüßen wir Thomas Langholz von Matrix 42. Er wird erläutern mit welchen Herausforderungen der CISO eines Herstellers von Softwarelösungen für Enterprise Kunden alltäglich umgehen muss. Nicht nur die Kenntnis allerhand branchenfremder Kundenstandards ist hierbei Pflicht, es gilt auch den Spagat zwischen Security und Usability zu meistern. Und das nicht nur intern sondern vor allem auch für die Kunden!

14:30 | Cyber is Art - Art is Experience - meet the Cyber Experience presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Im ersten deutschen Cyber Experience Center der Orange Cyberdefense erlebt das Top Management hautnah wie sich ein Ransomware Angriff anfühlt, welche Auswirkungen zu erwarten sind und welche Entscheidungen zu treffen sind. Christopher Johannes und Götz Weinmann geben Einblicke in das Cyber Experience Center und lassen die Teilnehmer selbst spüren, was Sie in dem Cyber Experience Center erwartet.

15:15 | Breaking down silos – Minimizing attack surface presented by Andreas Bäumer, Senior Sales Engineer, Axonius

Cybersecurity frameworks and programs start from identifying the corporate hardware and software assets. Organisations are, however, struggling to create credible inventories as the relevant asset information is spread out into a number of point solutions such as endpoint management solutions, cloud infrastructure and directory services. The credible an up-to-date asset inventory is a foundation for all cybersecurity operations. This session will talk about moving from data silos into a comprehensive asset inventory that can be used to understand and validate organization attack surface, security controls and compliance.

16:15 | Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE presented by Kai Eggers, Senior Business Development Manager, Orange Cyberdefense

Coming soon

17:00 | OT Security – Innovation für die „letzte Meile“
presented by Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense & Wolfgang Schnurbusch, Business Development Manager IoT & Security, Weidmüller

IT-Verantwortliche aufgepasst: Während IT-Security etabliert ist, birgt die OT-Umgebung mit ihren oft unsicheren Feldbussen erhebliche Risiken für die Produktionssicherheit. Interne Angriffe, z.B. durch unbefugt angeschlossene Geräte, stellen eine reale Bedrohung dar. Wie schützen Sie Ihre kritische Fertigungsinfrastruktur? Weidmüller bietet mit seiner innovativen u-OS Plattform eine Lösung, die Maschinensteuerung und -überwachung vereint und so auch die unterste Ebene absichert. In Partnerschaft mit Orange Cyberdefense/Nozomi und Fortinet ermöglichen wir ganzheitliche Security-Pakete, um auch die spezifischen Anforderungen der OT zu erfüllen und Compliance mit NIS2 & Co. zu gewährleisten.

Track 2 - Offside

10:30 | Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury? presented by Martin Dombrowski, Software Defined Segmentation and Security Specialist, Enterprise Sales Executive, Akamai Technologies

In today's complex IT environments, securing the digital fortress requires more than just a strong perimeter. This presentation uses the metaphor of a castle to illustrate the power of segmentation with Akamai Guardicore Segmentation. Imagine a chef in the castle's kitchen – while trusted in their domain, they should never have access to the treasury. Through micro-segmentation, we ensure that internal roles and zones remain isolated, preventing lateral movement and containing breaches before they reach critical assets. Discover how Guardicore transforms your security architecture from walls to well-guarded rooms.

11:15 | NIS2: wie man eine Machete einsetzt presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Es kann schon eine Kunst sein alle notwendigen Anforderungen im Blick zu behalten. Noch wichtiger: Welche rechtlichen Verpflichtungen gibt es? Götz Weinmann zeichnet mit Ihnen einen Paragraphendschungel und wird im Anschluss gemeinsam mit Ihnen die wesentlichen Anforderungen herausarbeiten.

12:00 | Best Practice: Implementierung eines SOC presented by Sebastian Markl, Trinks GmbH & Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Die Trinks GmbH ist führender Getränkelogistiker mit 16 Standorten und 1700 Mitarbeitern in Deutschland. Damit ist das Unternehmen Teil der kritischen Infrastruktur Betreiber (KRITIS). Sebastian Markl wird in seinem Vortrag über die Migration und Erweiterung des Managed SOC berichten. Was lief gut, wo gab es Stolpersteine und was würde er heute wieder genauso machen. Ein Erfahrungsbericht vom Kunden und für Kunden: Seien Sie gespannt und stellen Sie ihre Fragen!

13:45 | Die Kunst der Proaktivität: Breach & Attack Simulation als kreatives Werkzeug für Sicherheit
presented by BestSecret

Wie ein Künstler verschiedene Techniken und Materialien ausprobiert, um ein Meisterwerk zu schaffen, testet eine Breach & Attack Simulation unterschiedliche Angriffsszenarien, um die Stärken und Schwächen eines Sicherheitssystems zu erkennen. Erfahren Sie hier, wie es der Onlinehändler Bestsecret mittels automatisierter Angriffssimulationen schafft, den Angreifern stets einen Schritt voraus zu sein.

14:30 | Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf?
presented by Fabian Bauer, Rechtsanwalt und IT-Rechtsexperte, SKW Schwarz

Die Umsetzung der NIS2 Anforderungen für Cybersicherheit kann nur im Zusammenspiel von Recht und Technik gelingen. Mit der Erfahrung aus Umsetzungsprojekten bei großen und mittelständischen Unternehmen verschiedener Branchen berichten die Experten direkt aus der Werkstatt, auf welche Fragen sie dabei stoßen und welche Lösungen sich als praktikabel bewiesen haben. Zugleich zeigen sie am praktischen Beispiel wie aus dem Zusammenspiel von Recht und Technik eine ehrliche Risikoanalyse und eine erfolgreiche Umsetzung gelingen können.

15:15 | Schon mal über eine ganzheitliche Sicherheitsplattform nachgedacht? presented by Google

Cyberbedrohungen entwickeln sich rasant – herkömmliche Abwehrmechanismen stoßen an ihre Grenzen. Google setzt mit seiner neuen SecOps-Architektur und der Integration von AI neue Maßstäbe in der Cybersicherheit. Erleben Sie, wie Google SecOps mit Gemini AI im Zusammenspiel mit den schlagkräftigen Services der Orange Cyberdefense Angreifern das Leben schwerer macht, und Unternehmen dabei hilft, Cyberbedrohungen effektiver zu erkennen und abzuwehren.
In einem Mix aus Präsentation und Live-Demo möchten wir Sie gerne auf die Reise der Orange Cyberfefense mit Google SecOps mitnehmen.

16:15 | The Art of Social Engineering presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Götz Weinmann zeigt die aktuellen Entwicklungen im Bereich Social Engineering:
Was versteht Orange Cyberdefense unter MS365 Fraud, und wie gehen die Angreifer vor?
Dabei demonstriert er einen trickreichen Social Engineering Angriff! Werden Sie auch darauf reinfallen? Nehmen Sie diese Challenge an!

17:00 | One day in a SOC presented by Lukas Mitterreiter, Analyst Cyber-security, Orange Cyberdefense

Ein Security Operations Center (SOC) ist das Rückgrat der Cybersicherheit. Diese Präsentation beleuchtet die täglichen Aufgaben und Herausforderungen eines SOC-Teams, von der Bedrohungserkennung bis zur Problemlösung, und zeigt dessen Schlüsselrolle im Schutz sensibler Daten.

Track 3 - Skinny I

10:30 | OT Cybersecurity Best Practices
presented by Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense

Ist das Kunst oder wie sichere ich meine OT Umgebung? Durch die digitale Transformation, die in der Industrie rasant voranschreitet, sehen sich Unternehmen in der Betriebstechnologie (OT) einer Vielzahl neuer Sicherheitsherausforderungen gegenüber. Cyberangriffe auf kritische Infrastrukturen können nicht nur zu finanziellen Verlusten führen, sondern auch die öffentliche Sicherheit und die Betriebsfähigkeit gefährden. In diesem Vortrag werden bewährte Methoden („Best Practices“) für die Cyber-Sicherheit in OT-Umgebungen vorgestellt.

13:45 | Impuls: European sovereignty without banning all non-Eurpean vendors presented by Orange Cyberdefense

Unsere agile und innovative Branche erlaubt es mir doch zu jeder Zeit einfach und unkompliziert, auch bei den aktuellen Herausforderungen durch geopolitische Ereignisse, „Business as usual“ zu praktizieren. Betrachtung aus unterschiedlichen Blickwinkeln ohne Stellung zu beziehen --> Consulting approach!

14:30 | The Art of Awareness - Sensibilisierung in Zeiten von KI
presented by Franziska Strohmeier, Security Consultant, Orange Cyberdefense

Der Vortrag beleuchtet die Schwierigkeiten, denen sich Unternehmen und Mitarbeitende im Bereich der Aufrechterhaltung der Cybersecurity Awareness in Bezug auf KI gestützte Technologien stellen müssen. Es werden die damit verbundenen bzw. dadurch entstehenden Risiken aber auch potenzielle Gegenmaßnahmen sowie Handlungsmöglichkeiten betrachtet, die dazu beitragen können, Unternehmen auch in der Zukunft wirksam gegen Angriffe von Außen, die auf die Schwachstelle Mensch abzielen, schützen zu können.

15:15 | The Art of finding a needle in the haystack
presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Threat Informed Defense in der Praxis: Unser Experte Götz Weinmann demonstriert praktisch, wie eine gute Threat Intelligence Plattform hilft, alles aus Ihrer Security Infrastruktur rauszuholen, worauf es bei TI ankommt und warum Threat Intelligence immer Bestandteil von Security Services sein sollte. Sie wollen es darauf anlegen? Bringen sie ihren IoC mit in den Talk und wir prüfen live, was unsere CERT Experten dazu sagen...

Track 4 - Skinny II

10:30 | DORA Roundtable
presented by Michael Schrenk, Principal Sales Manager, Orange Cyberdefense

Der DORA Roundtable bietet eine Plattform für Fachleute aus der Finanzbranche, um sich in einem vertraulichen Rahmen über die Umsetzung des Digital Operational Resilience Act auszutauschen. Der Roundtable richtet sich an Organisationen, die unter den Anwendungsbereich von Art. 2 DORA fallen und somit direkt von den neuen regulatorischen Vorgaben betroffen sind. Dabei geht es um Erfahrungsaustausch, regulatorische Anforderungen sowie Herauforderungen und Stolpersteine.
Voranmeldung erforderlich!

Detect & Defend
Orange Cyberdefense Live

Agenda Fürstenfeldbruck - 15.05.2025

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 Simon Pierro**

Zeit	Track 1 - Stadtsaal	Track 2 - Säulensaal	Track 3 - Kleiner Saal	Fürstenfelder 1
10:30–11:00	**Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit** presented by Palo Alto Networks	**Breaking down silos – Minimizing attack surface** presented by Axonius	**Renaissance der Cybersecurity: KI und das SOC der Zukunft** presented by Orange Cyberdefense	**DORA Round-table** presented by Orange Cyberdefense
11:15–11:45	**Paint it Black: Live Analyse einer Black Basta Attack Campaign** presented by Orange Cyberdefense	**Kontinuierliches adaptives Vertrauen – der Schlüssel zur Einführung von Zero Trust und SASE und wie man dorthin kommt** presented by Netskope	**Draw an informed picture of your adversaries (ENG)** presented by Tidal Cyber	
12:00–12:30	**Security Plattform Strategie schlägt Sammelsurium von Einzelprodukten** presented by Microsoft	**New Horizons in Managed Threat Detection** presented by Orange Cyberdefense	**OT Security – Innovation für die „letzte Meile“** presented by Weidmüller & Orange Cyberdefense	
	12:30–13:45 Uhr: **Lunch**			
13:45–14:15	**Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf?** presented by SKW Schwarz	**Erfahrungsbericht zum Einsatz von OT-Security bei Carl ZEISS AG** presented by Carl Zeiss & Orange Cyberdefense	**Schon mal über eine ganzheitliche Sicherheitsplattform nachgedacht?** presented by Google	**Splunk 4Rookies**
14:30–15:00	**Splunk bietet den Rahmen, die individuelle Ausgestaltung des Bildes übernehmen wir** presented by Splunk	**Cyber is Art - Art is Experience - meet the Cyber Experience** presented by Orange Cyberdefense	**Know Yourself: Strategies Employed for Understanding Your Attack Surface (ENG)** presented by Orange Cyberdefense	
15:15–15:45	**Automatische Klassifizierung & Data Loss Prevention: mit der eigenen KI zur vollen Kontrolle** presented by Forcepoint	**Schatten-KI und die Farbpalette für eine sichere und regulierte KI-Strategie** presented by Orange Cyberdefense	**Die zweite Verteidigungslinie** presented by Vectra Networks	
	15:45–16:15 Uhr: Tea & Networking			
16:15–16:45	**Compliance and Regulatory Challenges in OT: Best Practices for Adherence (ENG)** presented by Nozomi Networks	**Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE** presented by Orange Cyberdefense	**Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury?** presented by Akamai	**Splunk 4Rookies**
17:00–17:30	**Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert** presented by Sentinel One	**Thinking outside the box: The importance of tracking your Digital Risk (ENG)** presented by Orange Cyberdefense	**The Art of Cybersecurity: Ein Ransomware-Realitätscheck** presented by Pentera	
	17:30–22:00 Uhr: **Abendevent**			

Track 1 - Stadtsaal

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Simon Pierro

10:30 | Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit
presented by Stefan Mandl, Solutions Architect , Palo Alto Networks

Cortex® Cloud vereint die nächste Version von Prisma® Cloud mit Cloud Detection & Response. SOC-Teams erhalten eine kontextgesteuerte Verteidigung – kontinuierlichen Schutz vom Code über die Cloud bis zum SOC. Dank der Plattformisierung werden Schwachstellen priorisiert, bevor sie zu aktiven Bedrohungen werden. Die Automatisierung schließt den Kreis bei kritischen Problemen und löst Risiken, bevor Angreifer sie ausnutzen. Basierend auf KI, Orchestrierung und Automatisierung, ergänzt durch die CNAPP-Funktionen von Prisma Cloud, müssen Sicherheitsteams nicht mehr mit getrennten Tools und Workflows navigieren, und die Arbeitsbelastung wird vereinfacht. Seien Sie Angreifern einen Schritt voraus – in Echtzeit und mit weniger Stress.

11:15 | Paint it Black: Live Analyse einer Black Basta Attack Campaign
presented by Friedl Holzner, Team Lead CyberSOC & André Henschel, Analyst Cybersecurity, Orange Cyberdefense

Stellen Sie sich vor, Ihr Posteingang wird mit tausenden Spam-E-Mails überflutet – und genau in diesem Moment meldet sich Ihr IT-Support über Microsoft Teams, um Hilfe anzubieten. Kein Zufall, sondern ein gezielter Angriff. Ende letzten Jahres beobachtete unser CyberSOC eine Welle solcher Attacken, bei denen Malware eingeschleust und Ransomware-Angriffe vorbereitet wurden. In dieser Live-Demo zeigen wir, wie ein solcher Angriff abläuft – von den ersten Anzeichen eines bevorstehenden Angriffs, über Social Engineering Techniken und Malware Delivery bis hin zur Detektion und Analyse der ausgeführten Malware.

12:00 | Security Plattform Strategie schlägt Sammelsurium von Einzelprodukten presented by Frank Bunn, Senior Manager Security Partner Development, Microsoft

Seit Jahren ist Orange Cyberdefense sehr erfolgreich mit Implementierung & Management von Kundenumgebungen basierend auf dem umfangreichen Security Stack von Microsoft für heterogene Umgebungen. Waren es anfangs die Cloud SIEM Lösung Sentinel und die Defender Lösungen von M365, setzt Orange Cyberdefense nun verstärkt auf eine End-to-End Plattform Strategie unter Einbeziehung von Microsoft Data Security, Cloud Security und Identity & Access Management, was für die Kunden große Vorteile bringt. Lernen Sie in dieser Session mehr über die Microsoft Security Strategie und die Bedeutung der neuen Advanced Identity Lösung.

13:45 | Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf? presented by Dr. Matthias Orthwein, Rechtsanwalt und IT-Rechtsexperte, SKW Schwarz

Die Umsetzung der NIS2 Anforderungen für Cybersicherheit kann nur im Zusammenspiel von Recht und Technik gelingen. Mit der Erfahrung aus Umsetzungsprojekten bei großen und mittelständischen Unternehmen verschiedener Branchen berichten die Experten direkt aus der Werkstatt, auf welche Fragen sie dabei stoßen und welche Lösungen sich als praktikabel bewiesen haben. Zugleich zeigen sie am praktischen Beispiel wie aus dem Zusammenspiel von Recht und Technik eine ehrliche Risikoanalyse und eine erfolgreiche Umsetzung gelingen können.

14:30 | Splunk bietet den Rahmen, die individuelle Ausgestaltung des Bildes übernehmen wir presented by Markus Thiel, Senior Business Development Manager, Orange Cyberdefense & Marcel Seifert, Senior Partner Solutions Advisor, Splunk

Splunk ermöglicht Unternehmen, ihre individuellen Anforderungen an Sicherheits-, IT-, und Observability durch eine skalierbare Datenplattform effizient zu erfüllen. Erfahren Sie anhand konkreter Beispiele, wie Splunk dabei unterstützt - angefangen bei der Minimierung des Ausfallrisikos bis hin zur Stärkung digitaler Resilienz. Der Vortragsinhalt richtet sich sowohl an Bestandskunden wie auch Interessenten, die noch am Anfang ihrer Experience stehen.

15:15 | Automatische Klassifizierung & Data Loss Prevention: mit der eigenen KI zur vollen Kontrolle presented by Fabian Glöser, Team Lead Sales Engineering, Forcepoint

Nur wer den Überblick hat, kann präventiv Risiken vermeiden. Wissen Sie, wo Ihre sensiblen Daten liegen? Mit Forcepoint erreichen Sie umfassende Visibilität über Ihre Datenbestände. Gleichzeitig erhalten Sie Ihre eigene KI: Die vollautomatische Klassifizierung nimmt Ihnen mit höchster Treffsicherheit die Arbeit ab, ohne dass Sie Ihre Daten aus der Hand geben müssen. Und damit dies auch nicht anderweitig passiert, schützt Forcepoint Ihre Organisation mittels Data Loss Prevention vor Datenverlust. Gepaart mit Managed DLP von Orange Cyberdefense können Sie die Arbeit den Profis überlassen. Sie erhalten einen Überblick über das perfekte Zusammenspiel von Technologie und Knowhow.

16:15 | Compliance and Regulatory Challenges in OT: Best Practices for Adherence (ENG) presented by Sebastian Erlier-Yates, Technical Sales Engineer, Nozomi Networks

Navigating the evolving landscape of OT security regulations can be complex. With frameworks like NIS2, IEC 62443, and industry-specific mandates shaping security expectations, organizations must go beyond visibility to ensure compliance and resilience. As a trusted leader in OT & IoT security, Nozomi Networks delivers the technology and expertise organizations need to strengthen their security posture, streamline compliance, and maximize the value of their cybersecurity investments. We will explore the latest compliance challenges impacting OT environments, best practices for aligning security strategies with regulatory frameworks and how continuous, active and passive monitoring, risk assessment, and automated response can simplify adherence.

17:00 | Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert presented by Hans-Martin Röhrig, Enterprise Account Executive, Sentinel One

Mit ausgefeilteren Angriffen, die auch auf KI zurückgreifen, kommen immer mehr klassische Sicherheitslösungen an ihre Grenzen. Doch autonome KI-Systeme versprechen auch eine schnellere und effektivere Bedrohungsserkennung. Aber sind sie wirklich zuverlässig? Wir werfen einen Blick auf Chancen, Herausforderungen und reale Anwendungsfälle.

Track 2 - Säulensaal

10:30 | Breaking down silos – Minimizing attack surface
presented by Gerhard Dietz, Strategic Sales DACH, Axonius

Cybersecurity frameworks and programs start from identifying the corporate hardware and software assets. Organisations are, however, struggling to create credible inventories as the relevant asset information is spread out into a number of point solutions such as endpoint management solutions, cloud infrastructure and directory services.
The credible an up-to-date asset inventory is a foundation for all cybersecurity operations. This session will talk about moving from data silos into a comprehensive asset inventory that can be used to understand and validate organization attack surface, security controls and compliance.

11:15 | Kontinuierliches adaptives Vertrauen – der Schlüssel zur Einführung von Zero Trust und SASE und wie man dorthin kommt presented by Martin Hadersbeck, Netskope

Wahrscheinlich haben Sie den Begriff „SASE“ in jedem LinkedIn-Beitrag und Sicherheitstechnik-Blog der Branche gehört. Unseres ist anders – wir lassen die Theorie hinter uns. Unser Blueprint enthält alles, was Sie benötigen, um die Auswirkungen von Zero Trust innerhalb Ihrer SASE-Architektur vollständig zu verstehen.

12:00 | New Horizons in Managed Threat Detection
presented by Niklas Klotz, Director Product Management, Orange Cyberdefense

Als Konsequenz einer sich stetig verändernden Bedrohnungslandschaft steht eine effizienze Angriffserkennung zunehmend Herausforderungen gegenüber: mehr Daten, dynamische Bedrohungen und ineffizente Architekturen. Die Lösung hierzu liegt in einer strikten Fokussierung auf validierte Risiken durch eine kombination von Threat Intelligence und Exposure Management zur Steuerung der Angiffserkennung.

13:45 | Erfahrungsbericht zum Einsatz von OT-Security bei Carl ZEISS AG presented by Hansheinz Müller Philipps Sohn, Network Security Manager, Carl ZEISS AG & Michael Schrenk, Principal Sales Manager, Orange Cyberdefense

Die Carl ZEISS AG hat sich im Rahmen ihrer Cybersecurity-Strategie auch der Sicherheit Ihrer Produktionsumgebungen (OT) angenommen. Über die Erfahrungen bei der Feststellung des Status Quo, der Erarbeitung der Zielsetzung und eines geeigneten Vorgehens sowie der Evaluierung und Entscheidung für geeignete Lösungen wird in diesem Vortrag berichtet.

14:30 | Cyber is Art - Art is Experience - meet the Cyber Experience presented by Götz Weinmann, Senior Business Development Manager, Orange Cyberdefense

Im ersten deutschen Cyber Experience Center der Orange Cyberdefense erlebt das Top Management hautnah wie sich ein Ransomware Angriff anfühlt, welche Auswirkungen zu erwarten sind und welche Entscheidungen zu treffen sind. Christopher Johannes und Götz Weinmann geben Einblicke in das Cyber Experience Center und lassen die Teilnehmer selbst spüren, was Sie in dem Cyber Experience Center erwartet.

15:15 | Schatten-KI und die Farbpalette für eine sichere und regulierte KI-Strategie
presented by Fabian Beutel, Head of Consulting, Orange Cyberdefense

Während Unternehmen in den letzten Jahren große Fortschritte dabei gemacht haben, Schatten-IT unter Kontrolle zu bringen, entsteht mit der unkontrollierten Nutzung von KI-Tools eine neue Herausforderung: die Schatten-KI. Mitarbeiter nutzen KI-Anwendungen oft eigenständig – ohne IT-Freigaben, Sicherheitsüberprüfungen oder Compliance-Vorgaben.
Doch welche Risiken bringt das mit sich? In dem Vortrag beleuchten wir diese Herausforderungen und zeigen, wie Unternehmen eine sichere und regulierte KI-Strategie entwickeln können:

- Unerlaubter Einsatz von KI: Wenn Mitarbeitende ohne Genehmigung KI-Modelle nutzen, können vertrauliche Daten unkontrolliert verarbeitet werden.
- Überregulierung vs. Innovation: Wie lässt sich der Balanceakt zwischen Sicherheitsvorgaben und sinnvoller Nutzung von KI gestalten?
- Regulierter KI-Einsatz: Welche Lösungen helfen Unternehmen dabei, KI sicher und konform einzusetzen?

16:15 | Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE presented by Kai Eggers, Senior Business Development Manager, Orange Cyberdefense

In der IT-Security werfen wir mit Abkürzungen und Buzz-Words um uns – dabei gibt es aber oft zu einer Abkürzung mehrere Definitionen oder Abkürzungen werden für unterschiedliche Bedeutungen herangezogen. Am Beispiel von Secure Access Service Edge wollen wir uns daher an der Kunst versuchen, das Thema möglichst ohne oder zumindest mit weniger Abkürzungen darzustellen. Von einer Begriffsdefinition, über ein einfaches Architekturbild und einem Anwendungsfall mit einer kommerziellen Übersicht bis hin zu dem passenden Service von Orange Cyberdefense: Der Vortrag möchte dazu anregen, in unserem hochtechnisierten Umfeld einmal anders zu kommunizieren, ohne an Tiefe zu verlieren. Mehr Klarheit und Verständlichkeit durch Vereinfachung.

17:00 | Thinking outside the box: The importance of tracking your Digital Risk (ENG) presented by Grant Paling, Product Director, Orange Cyberdefense
Picking up where his earlier session left off, Grant shares multiple stories from the field about brand exploitation and exposed data, our current knowledge of the Open, Deep and Dark Web and exploring why digital risk protection should be an important part of your cybersecurity strategy and advice on how to play your part in creating a safer digital society overall.

Track 3 - Kleiner Saal

10:30 | Renaissance der Cybersecurity: KI und das SOC der Zukunft presented by Simon Krüger, CI Automation Expert, Orange Cyberdefense

Humanismus, Innovation und Forschritt prägen die Renaissance und man könnte argumentieren, dass KI und insbesondere LLMs für Cybersecurity eine ähnliche Ära ausrufen. Automatisierte Angriffe zu erstellen war noch nie so einfach und auch auf der Seite des Blue Teams versprechen Vendors revolutionäre Use Cases. Nun legt sich langsam der Staub und wir können gemeinsam einen realistischen Blick auf die Zukunft des SOC werfen und beleuchten wie aktuelle Entwicklungen in KI das Blue Team unterstützen und verändern werden. In einem Gedankenexperiment vergleichen wir ein traditionelles SOC mit der Skizze eines zukünftigen SOCs anhand eines Angriffes.

11:15 | Draw an informed picture of your adversaries (ENG) presented by Ian Davila, Lead Adversary Emulation Engineer, Tidal Cyber & David Engelhardt, Lead Consultant, Orange Cyberdefense

To draw a characterful picture of your adversaries you need to know them. How do they look, what do they do and what do they wear? You need information and then take that information and put it to use. Cyber Security is no different. You need to know who might be targeting you, what tactics, techniques and procedures they use and what defensive measures could help you to defend against those. Put your limited resources to use where they have the most meaningful impact and adjust to a changing threat landscape dynamically.

12:00 | OT Security – Innovation für die „letzte Meile“ presented by Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense & Wolfgang Schnurbusch, Business Development Manager, Weidmüller

IT-Verantwortliche aufgepasst: Während IT-Security etabliert ist, birgt die OT-Umgebung mit ihren oft unsicheren Feldbussen erhebliche Risiken für die Produktionssicherheit. Interne Angriffe, z.B. durch unbefugt angeschlossene Geräte, stellen eine reale Bedrohung dar. Wie schützen Sie Ihre kritische Fertigungsinfrastruktur? Weidmüller bietet mit seiner innovativen u-OS Plattform eine Lösung, die Maschinensteuerung und -überwachung vereint und so auch die unterste Ebene absichert. In Partnerschaft mit Orange Cyberdefense/Nozomi und Fortinet ermöglichen wir ganzheitliche Security-Pakete, um auch die spezifischen Anforderungen der OT zu erfüllen und Compliance mit NIS2 & Co. zu gewährleisten.

13:45 | Schon mal über eine ganzheitliche Sicherheitsplattform nachgedacht? presented by Google

Cyberbedrohungen entwickeln sich rasant – herkömmliche Abwehrmechanismen stoßen an ihre Grenzen. Google setzt mit seiner neuen SecOps-Architektur und der Integration von AI neue Maßstäbe in der Cybersicherheit. Erleben Sie, wie Google SecOps mit Gemini AI im Zusammenspiel mit den schlagkräftigen Services der Orange Cyberdefense Angreifern das Leben schwerer macht, und Unternehmen dabei hilft, Cyberbedrohungen effektiver zu erkennen und abzuwehren.

In einem Mix aus Präsentation und Live-Demo möchten wir Sie gerne auf die Reise der Orange Cyberfefense mit Google SecOps mitnehmen.

14:30 | Know Yourself: Strategies Employed for Understanding Your Attack Surface (ENG) presented by Grant Paling, Product Director, Orange Cyberdefense

In order to best utilise Threat Intelligence within your organisation, you must know what you are defending. Understanding your attack surface is vital as part of an intelligence-led security approach. We explore the impact of unidentified attack surfaces through some incident response war stories before turning the focus towards strategies to address the problem and how Cyber Threat Exposure Management is a vital component of your defensive capabilities.

15:15 | Die zweite Verteidigungslinie presented by Vectra Networks

Moderne IT-Infrastrukturen sind zunehmend hybrid – verteilt über lokale Netzwerke, Cloud-Dienste und SaaS-Anwendungen. Diese Komplexität eröffnet Angreifern neue Möglichkeiten, sich unentdeckt seitlich zu bewegen und klassische Verteidigungsmechanismen zu umgehen. Angesichts dieser Entwicklungen gewinnt künstliche Intelligenz in der Cybersicherheit an Bedeutung: Sie ermöglicht eine verhaltensbasierte Analyse von Netzwerk- und Cloud-Aktivitäten, erkennt subtile Anomalien und bietet Kontext für fundierte Entscheidungen im Incident Response. Wir beleuchten die Rolle von KI als zweite Verteidigungslinie in modernen Netzwerken und zeigen, wie sie hilft, dynamische Bedrohungen frühzeitig und effizient zu erkennen – unabhängig von der Infrastruktur.

16:15 | Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury? presented by Akamai Technologies

In today’s complex IT environments, securing the digital fortress requires more than just a strong perimeter. This presentation uses the metaphor of a castle to illustrate the power of segmentation with Akamai Guardicore Segmentation. Imagine a chef in the castle’s kitchen – while trusted in their domain, they should never have access to the treasury. Through micro-segmentation, we ensure that internal roles and zones remain isolated, preventing lateral movement and containing breaches before they reach critical assets. Discover how Guardicore transforms your security architecture from walls to well-guarded rooms.

17:00 | The Art of Cybersecurity: Ein Ransomware-Realitätscheck presented by Thorsten Kolb, Cyber Engineer Team Lead, Pentera

Ransomware ist nach wie vor die kritischste Cyber-Bedrohung für Unternehmen weltweit und hat ein noch nie dagewesenes Ausmaß und Wirkung erreicht. Trotz der Zerschlagung von zwei großen Ransomware-Gruppen – LockBit und ALPHV – bleibt das Gesamtvolumen der Angriffe weitgehend unverändert, wobei die Kosten bis 2031 voraussichtlich 265 Milliarden US-Dollar pro Jahr erreichen werden. Im Gegensatz zu den Statistiken muss Ransomware keine Frage des „Wann“ sein - Sicherheitsteams haben die Möglichkeit, sie in ein „Ob“ zu verwandeln.
In dieser Sitzung werden wir umsetzbare Strategien zur Stärkung Ihrer Cyber-Abwehrkräfte und zur Verbesserung der Widerstandsfähigkeit Ihres Unternehmens vorstellen.

Fürstenfelder 1

10:30 | DORA Roundtable presented by Michael Schrenk, Principal Sales Manager, Orange Cyberdefense

Der DORA Roundtable bietet eine Plattform für Fachleute aus der Finanzbranche, um sich in einem vertraulichen Rahmen über die Umsetzung des Digital Operational Resilience Act auszutauschen. Der Roundtable richtet sich an Organisationen, die unter den Anwendungsbereich von Art. 2 DORA fallen und somit direkt von den neuen regulatorischen Vorgaben betroffen sind. Dabei geht es um Erfahrungsaustausch, regulatorische Anforderungen sowie Herauforderungen und Stolpersteine.
Voranmeldung erforderlich!

13:45 | Splunk4Rookies presented by Splunk

Der Splunk4Rookies Workshop ist perfekt für Einsteiger, die die Grundlagen von Splunk verstehen und direkt anwenden möchten. Hier lernen Sie, wie Sie Daten sammeln, indizieren, analysieren und interaktive Dashboards erstellen.
Sie erhalten eine eigene Splunk-Instanz und führen erste Suchen durch, erstellen Statistiken und gestalten interaktive Dashboards, um wertvolle Erkenntnisse aus Ihren Daten zu gewinnen.
Alles, was Sie für die Teilnahme benötigen, ist ein Laptop mit einem Browser. Voranmeldung erforderlich!

Detect & Defend
Orange Cyberdefense Live

Agenda Dortmund - 22.05.2025

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 Gilles van Heijst**

Zeit	Track 1 - Saal 5	Track 2 - Saal 4	Saal 6
10:30–11:00	**Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit** presented by Palo Alto Networks	**Impuls: European sovereignty without banning all non-European vendors** presented by Orange Cyberdefense	
11:15–11:45	**Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury?** presented by Akamai	**Schatten-KI und die Farbpalette für eine sichere und regulierte KI-Strategie** presented by Orange Cyberdefense	**DORA Roundtable** presented by Orange Cyberdefense
12:00–12:30	**Konvergenz und Konsolidierung für mehr Sicherheit** presented by Fortinet	**Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf?** presented by SKW Schwarz	
12:30–13:45 Uhr: **Lunch**			
13:45–14:15	**Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert** presented by Sentinel One	**One day in a SOC** presented by Orange Cyberdefense	
14:30–15:00	**Cyber is Art - Art is Experience - meet the Cyber Experience** presented by Orange Cyberdefense	**Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE** presented by Orange Cyberdefense	**Splunk 4Rookies**
15:15–15:45	**Splunk bietet einen Rahmen, die individuelle Ausgestaltung des Bildes übernehmen wir** presented by Splunk	**The Art of Awareness - Sensibilisierung in Zeiten von KI** presented by Orange Cyberdefense	
15:45–16:15 Uhr: Tea & Networking			
16:15–16:45		**OT Security – Innovation für die „letzte Meile“** presented by Weidmüller & Orange Cyberdefense	**Splunk 4Rookies**
17:00–17:30			
17:30–18:00 Uhr: **Wrap Up**			

Track 1 - Saal 5

09:00 | Eröffnung der Fachkonferenz

09:15 | Keynote Gilles van Heijst: Are You SuperIntelligent AI Ready?

10:30 | Cortex Cloud, die Zukunft der Cloud-Sicherheit in Echtzeit presented by Songuel Ballikaya, Partner Development Manager, Palo Alto Networks

Cortex® Cloud vereint die nächste Version von Prisma® Cloud mit Cloud Detection & Response. SOC-Teams erhalten so eine kontextgesteuerte Verteidigung – kontinuierlichen Schutz vom Code über die Cloud bis zum SOC. Dank der Plattformisierung werden Schwachstellen priorisiert, bevor sie zu aktiven Bedrohungen werden. Die Automatisierung schließt den Kreis bei kritischen Problemen und löst Risiken, bevor Angreifer sie ausnutzen. Basierend auf KI, Orchestrierung und Automatisierung, ergänzt durch die CNAPP-Funktionen von Prisma Cloud, müssen Sicherheitsteams nicht mehr mit getrennten Tools und Workflows navigieren, und die Arbeitsbelastung der SOC-Analysten wird vereinfacht. Seien Sie Angreifern einen Schritt voraus – in Echtzeit und mit weniger Stress.

11:15 | Advance Cyber Resilience with Microsegmentation – What is the cook doing in the treasury? presented by Martin Dombrowski, Software Defined Segmentation and Security Specialist, Enterprise Sales Executive, Akamai Technologies

In today's complex IT environments, securing the digital fortress requires more than just a strong perimeter. This presentation uses the metaphor of a castle to illustrate the power of segmentation with Akamai Guardicore Segmentation. Imagine a chef in the castle's kitchen – while trusted in their domain, they should never have access to the treasury. Through micro-segmentation, we ensure that internal roles and zones remain isolated, preventing lateral movement and containing breaches before they reach critical assets. Discover how Guardicore transforms your security architecture from walls to well-guarded rooms.

12:00 | Konvergenz und Konsolidierung für mehr Sicherheit presented by Oliver Burgstaller, Product Sales Specialist SASE & SecOps, Fortinet

Sichere Konnektivität wurde im letzten Jahrzehnt aus verschiedenen Bausteinen aufgebaut. Dazu gehörten in der Regel Technologien verschiedener Anbieter, die SD-WAN, Firewall und eine Cloud-basierte Secure Web Gateway-Lösung für entfernte Niederlassungen und mobile Mitarbeiter unterstützen. Es ist an der Zeit, Netzwerk- und Sicherheitsdienste zu konsolidieren, die zu einer agileren, sichereren und kostengünstigeren IT-Umgebung führen.

13:45 | Autonome Cybersicherheit: Wie KI Bedrohungen in Echtzeit erkennt und neutralisiert presented by Markus Höning, Enterprise Account Executive, Sentinel One

Mit ausgefeilteren Angriffen, die auch auf KI zurückgreifen, kommen immer mehr klassische Sicherheitslösungen an ihre Grenzen. Doch autonome KI-Systeme versprechen auch eine schnellere und effektivere Bedrohungsserkennung. Aber sind sie wirklich zuverlässig? Wir werfen einen Blick auf Chancen, Herausforderungen und reale Anwendungsfälle.

14:30 | Cyber is Art - Art is Experience - meet the Cyber Experience presented by Christopher Johannes, Portfolio Manager, Orange Cyberdefense

Im ersten deutschen Cyber Experience Center der Orange Cyberdefense erlebt das Top Management hautnah wie sich ein Ransomware Angriff anfühlt, welche Auswirkungen zu erwarten sind und welche Entscheidungen zu treffen sind. Christopher Johannes und Götz Weinmann geben Einblicke in das Cyber Experience Center und lassen die Teilnehmer selbst spüren was Sie in dem Cyber Experience Center erwartet.

15:15 | Splunk bietet den Rahmen, die individuelle Ausgestaltung des Bildes übernehmen wir presented by Markus Thiel, Senior Business Development Manager, Orange Cyberdefense & Marcel Seifert, Senior Partner Solutions Advisor, Splunk

Splunk ermöglicht Unternehmen, ihre individuellen Anforderungen an Sicherheits-, IT-, und Observability durch eine skalierbare Datenplattform effizient zu erfüllen. Erfahren Sie anhand konkreter Beispiele, wie Splunk dabei unterstützt - angefangen bei der Minimierung des Ausfallrisikos bis hin zur Stärkung digitaler Resilienz. Der Vortragsinhalt richtet sich sowohl an Bestandskunden wie auch Interessenten, die noch am Anfang ihrer Experience stehen.

Track 2 - Saal 4

10:30 | Impuls: European sovereignty without banning all non-Eurpean vendors presented by Orange Cyberdefense

Unsere agile und innovative Branche erlaubt es mir doch zu jeder Zeit einfach und unkompliziert, auch bei den aktuellen Herausforderungen durch geopolitische Ereignisse, „Business as usual“ zu praktizieren. Betrachtung aus unterschiedlichen Blickwinkeln ohne Stellung zu beziehen --> Consulting approach!

11:15 | Schatten-KI und die Farbpalette für eine sichere und regulierte KI-Strategie presented by Fabian Beutel, Head of Consulting, Orange Cyberdefense

Während Unternehmen in den letzten Jahren große Fortschritte dabei gemacht haben, Schatten-IT unter Kontrolle zu bringen, entsteht mit der unkontrollierten Nutzung von KI-Tools eine neue Herausforderung: die Schatten-KI. Mitarbeiter nutzen KI-Anwendungen oft eigenständig – ohne IT-Freigaben, Sicherheitsüberprüfungen oder Compliance-Vorgaben. Doch welche Risiken bringt das mit sich? In dem Vortrag beleuchten wir diese Herausforderungen und zeigen, wie Unternehmen eine sichere und regulierte KI-Strategie entwickeln können:

- Unerlaubter Einsatz von KI: Wenn Mitarbeitende ohne Genehmigung KI-Modelle nutzen, können vertrauliche Daten unkontrolliert verarbeitet werden.
- Überregulierung vs. Innovation: Wie lässt sich der Balanceakt zwischen Sicherheitsvorgaben und sinnvoller Nutzung von KI gestalten?
- Regulierter KI-Einsatz: Welche Lösungen helfen Unternehmen dabei, KI sicher und konform einzusetzen?

12:00 | Praktisches Beispiel NIS2. Welche rechtlichen und technischen Fragen und Themen kommen auf? presented by Fabian Bauer, Rechtsanwalt und IT-Rechtsexperte, SKW Schwarz

Die Umsetzung der NIS2 Anforderungen für Cybersicherheit kann nur im Zusammenspiel von Recht und Technik gelingen. Mit der Erfahrung aus Umsetzungsprojekten bei großen und mittelständischen Unternehmen verschiedener Branchen berichten die Experten direkt aus der Werkstatt, auf welche Fragen sie dabei stoßen und welche Lösungen sich als praktikabel bewiesen haben. Zugleich zeigen sie am praktischen Beispiel wie aus dem Zusammenspiel von Recht und Technik eine ehrliche Risikoanalyse und eine erfolgreiche Umsetzung gelingen können.

13:45 | One day in a SOC presented by Lukas Mitterreiter, Analyst Cybersecurity, Orange Cyberdefense

Ein Security Operations Center (SOC) ist das Rückgrat der Cybersicherheit. Diese Präsentation beleuchtet die täglichen Aufgaben und Herausforderungen eines SOC-Teams, von der Bedrohungserkennung bis zur Problemlösung, und zeigt dessen Schlüsselrolle im Schutz sensibler Daten.

14:30 | Die Kunst, ohne Abkürzungen & technische Buzz-Wörter auszukommen – ein Selbstversuch am Beispiel SASE presented by Kai Eggers, Senior Business Development Manager, Orange Cyberdefense

In der IT-Security werfen wir mit Abkürzungen und Buzz-Words um uns – dabei gibt es aber oft zu einer Abkürzung mehrere Definitionen oder Abkürzungen werden für unterschiedliche Bedeutungen herangezogen. Am Beispiel von Secure Access Service Edge wollen wir uns daher an der Kunst versuchen, das Thema möglichst ohne oder zumindest mit weniger Abkürzungen darzustellen. Von einer Begriffsdefinition, über ein einfaches Architekturbild und einem Anwendungsfall mit einer kommerziellen Übersicht bis hin zu dem passenden Service von Orange Cyberdefense: Der Vortrag möchte dazu anregen, in unserem hochtechnisierten Umfeld einmal anders zu kommunizieren, ohne an Tiefe zu verlieren. Mehr Klarheit und Verständlichkeit durch Vereinfachung.

15:15 | The Art of Awareness - Sensibilisierung in Zeiten von KI presented by Franziska Strohmeier, Security Consultant, Orange Cyberdefense

Der Vortrag beleuchtet die Schwierigkeiten, denen sich Unternehmen und Mitarbeitende im Bereich der Aufrechterhaltung der Cybersecurity Awareness in Bezug auf KI gestützte Technologien stellen müssen. Es werden die damit verbundenen bzw. dadurch entstehenden Risiken aber auch potenzielle Gegenmaßnahmen sowie Handlungsmöglichkeiten betrachtet, die dazu beitragen können, Unternehmen auch in der Zukunft wirksam gegen Angriffe von Außen, die auf die Schwachstelle Mensch abzielen, schützen zu können.

16:15 | OT Security – Innovation für die „letzte Meile“ presented by Rainer Bäder, Senior Business Development Manager, Orange Cyberdefense & Bernd-Ulrich Wittwer, Product and Application Trainer, Weidmüller

IT-Verantwortliche aufgepasst: Während IT-Security etabliert ist, birgt die OT-Umgebung mit ihren oft unsicheren Feldbussen erhebliche Risiken für die Produktionssicherheit. Interne Angriffe, z.B. durch unbefugt angeschlossene Geräte, stellen eine reale Bedrohung dar. Wie schützen Sie Ihre kritische Fertigungsinfrastruktur? Weidmüller bietet mit seiner innovativen u-OS Plattform eine Lösung, die Maschinensteuerung und -überwachung vereint und so auch die unterste Ebene absichert. In Partnerschaft mit Orange Cyberdefense/Nozomi und Fortinet ermöglichen wir ganzheitliche Security-Pakete, um auch die spezifischen Anforderungen der OT zu erfüllen und Compliance mit NIS2 & Co. zu gewährleisten.

Saal 6

10:30 | DORA Roundtable presented by Michael Schrenk, Principal Sales Manager, Orange Cyberdefense

Der DORA Roundtable bietet eine Plattform für Fachleute aus der Finanzbranche, um sich in einem vertraulichen Rahmen über die Umsetzung des Digital Operational Resilience Act auszutauschen. Der Roundtable richtet sich an Organisationen, die unter den Anwendungsbereich von Art. 2 DORA fallen und somit direkt von den neuen regulatorischen Vorgaben betroffen sind. Dabei geht es um Erfahrungsaustausch, regulatorische Anforderungen sowie Herauforderungen und Stolpersteine.
Voranmeldung erforderlich!

13:45 | Splunk4Rookies presented by Splunk

Der Splunk4Rookies Workshop ist perfekt für Einsteiger, die die Grundlagen von Splunk verstehen und direkt anwenden möchten. Hier lernen Sie, wie Sie Daten sammeln, indizieren, analysieren und interaktive Dashboards erstellen.

Sie erhalten eine eigene Splunk-Instanz und führen erste Suchen durch, erstellen Statistiken und gestalten interaktive Dashboards, um wertvolle Erkenntnisse aus Ihren Daten zu gewinnen.

Alles, was Sie für die Teilnahme benötigen, ist ein Laptop mit einem Browser. Voranmeldung erforderlich!

Locations & Anfahrt

Botanical Eppstein

Am Quarzitbruch 9

65817 Eppstein

www.percuma.de/botanical/

Getting there:

Anreise mit den öffentlichen Verkehrsmitteln:
Aus Frankfurt am Main fährt die S2 Richtung Niedernhausen Bahnhof bis Eppstein-Brehmthal Bahnhof oder Niederjosbach, hier fährt jeweils ein Bus bis Eppstein-Bremthal Gewerbegebiet. Von hier aus sind es etwa 5 Minuten zu Fuß. Aus Wiesbaden fährt ein Bus bis Eppstein-Bremthal Gewerbegebiet.

Anreise mit dem PKW:
Das Botanical liegt direkt an der Autobahn A3 bei Frankfurt am Main. Nutzen Sie die Autobahnausfahrt Wiesbaden-Niedernhausen.

Navigieren Sie in die Nauroder Strasse, 65817 Eppstein-Bremthal. Es sind ausreichend Parkplätze vor Ort.

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.

Kongresszentrum Dortmund

Rheinlanddamm 200

44139 Dortmund

www.kongress-dortmund.de/

Getting there:

Anreise mit den öffentlichen Verkehrsmitteln:
Fahren Sie von Dortmund Hauptbahnhof mit der U45 Richtung/Haltestelle: Westfalenhallen. Fußweg bis zum Eingang West: Ca. 5 Minuten

Anreise mit dem PKW:
Navigieren Sie zu Rheinlanddamm 200 oder Sonderziel „Kongress Dortmund“. Separate Zufahrten und Ausschilderungen für die Eingänge Nord und West sind vorhanden. Die Parkplatzgebühr beträgt 10,00 EUR.

powered by:

www.orangecyberdefense.de