SECURITY DAY 2024

CANCOM

	Track 1 - Raum Maria Theresia	Track 2 - Raum Sophie	Track 3 - Raum Maximilian	Track 4 - Raum Sissi
08:30 Uhr	**Registrierung und Frühstück**			
09:15 - 09:25	**Begrüßung durch Dietmar Wiesinger** *Mitglied des Vorstands | CANCOM Austria*			
09:25 - 10:00	**Keynote** **KI als Cybersecurity-Bedrohung** KI-generierte Bilder bergen Risiken wie Betrug, Cybermobbing und gesellschaftliche Manipulation. Betrüger nutzen etwa realistische Darstellungen von Führungskräften in Phishing-E-Mails, um Mitarbeiter zu schädlichen Handlungen zu verleiten. Auch können solche Bilder für Mobbing oder zur Rufschädigung eingesetzt werden, mit potenziellen Auswirkungen auf das Wahlverhalten und das Wirtschaftsklima. Eine Studie hat zudem gezeigt, dass derzeitige Erkennungstools für KI-generierte Inhalte unzureichend sind, da ihre Genauigkeit stark abnimmt, wenn sie mit manipulierten Inhalten konfrontiert werden. Dennoch ist es wichtig, sensibel für solche Bilder zu werden, um Manipulationen zu entlarven. In einem Vortrag werden Fehler und Kinderkrankheiten in KI-Grafiken untersucht und Methoden zur Sensibilisierung diskutiert, darunter das Erkennen von Inkonsistenzen und die Nutzung klassischer Techniken wie der reversen Bildersuche. **Andre Wolf** *MIMIKAMA*			
10:00 - 10:35	**CANCOM** **Aktuelle Schwachstellen & Bedrohungen** *Die Cyber Security Trends der CANCOM Austria AG bringen das Thema IT-Sicherheit mit Zahlen, Fakten anhand aktueller Fallbeispiele auf den Punkt: Schwachstellen und Bedrohungsszenarien, Angriffsmethoden sowie Gegenstrategien & Securitylösungen zeichnen ein Bild der aktuellen Sicherheitslage. Cyberkriminalität lässt sich 2024 nur mit umfassenden und strukturierten IT-Security Lösungen wirksam bekämpfen.* **Manfred Halper** *Director RED Team | CANCOM Austria*			
10:35 - 11:10	**COFFEE BREAK IN DER PARTNER AREA SPONSORED BY ARUBA**			
11:10 - 11:30	**Netzwerk Segmentierungsstrategien, aufgeteilt in Makro- Mikro- sowie Nanosegmentierung als auch die Remediation Werkzeuge von Cisco.** Cisco TrustSec verwendet Tags, um logische Gruppenprivilegien darzustellen. Dieses Tag, Security Group Tag (SGT) genannt, wird in Zugriffsrichtlinien verwendet. Das SGT ist bekannt und wird zur Durchsetzung des Datenverkehrs durch Cisco-Switches, Router und Firewalls verwendet. Cisco TrustSec ist in drei Phasen definiert: Klassifizierung, Verbreitung und Durchsetzung. Eine konvergente Multicloud-Richtlinie kann stufenweise erstellt und verwaltet werden, angefangen bei Anwendungs-Workloads bis hin zu den Endpunkten. Viele Kunden fordern eine Synchronisierung der Workload- und Rechenzentrums-Perimeterrichtlinien, um die Firewall-Richtlinienverwaltung im Allgemeinen zu verbessern. Beispielsweise kann eine umfassende sichere Workload-Richtlinie mit den Richtlinien derAWS VPC Network Security Group synchronisiert werden, auf denen EC2-Agenten und serverlose Appsausgeführt werden. Über die Grenzen des Rechenzentrums hinaus kann die Workload-Richtlinien-Enginemit Netzwerk-Firewalls synchronisiert werden, um die betriebliche Effizienz zu verbessern. **Andreas Hack** *Technical Solutions Architect - Security | CISCO*	**Applikationen ohne Grenzen: der Weg zu einer Benutzer-zentrierten Security** Security Konzepte von damals können heutzutage einfach nicht mehr die gleichen Schutzmaßnahmen liefern, wenn man als Unternehmen seinen Mitarbeitern eine moderne Art des Arbeitens bieten möchte. Früher gab es eine klare Abtrennung zwischen dem internen Netz und dem Internet. Die Grenzen verschwinden aber auf Grund von Cloud, mobilen Applikationen und SaaS Diensten. Der Weg führt von einer Standort-zentrierten Security hin zu einer Benutzer-zentrierten Security. Cyber Angriffe müssen von den End Usern ferngehalten werden und Gefahren bereits in der SaaS Applikation hinausgefiltert werden. **Patrick Fetter** *Security Consultant | Check Point Software Technologies*	**Unveiling the Dark Secrets of i-SOON: Einblick in China's Cyberspionage-Ökosystem** Diese Präsentation beleuchtet das kürzlich aufgedeckte Datenleck von i-SOON, einem in China ansässigen Cybersicherheitsunternehmen, das in offensive Cyberspionage-Operationen für chinesische Regierungskunden verwickelt ist. ⌄ Enthüllung des kürzlich aufgedeckten Datenlecks von i-SOON ⌄ Einblicke in das Innenleben von Chinas Cyberspionage-Ökosystem ⌄ Schärfung des Bewusstseins für die sich entwickelnde Landschaft der Cyberbedrohungen **Julian Kanitz** *Lead Sales Engineer DACH | Recorded Future*	**Securing the Industrial Edge: A Comprehensive Guide to OT Security and Network Architecture** Die industrielle Evolution erfordert eine robuste OT-Sicherheitsstrategie. Dieser Beitrag bietet einen Überblick über das Purdue-Modell, die Wichtigkeit einer Netzwerksegmentierung und das Schaffen von Zonen. Darüber hinaus beleuchten wir die Konvergenz von IT- und OT-Umgebungen sowie die Notwendigkeit eines effektiven Netzwerkmonitorings, um industrielle Systeme vor modernen Bedrohungen zu schützen. **Martin Lampel** *Director OT Security Solutions | CANCOM Austria* **Theresa Meiksner** *OT - Security Analyst, CANCOM Defense Center | CANCOM Austria*
11:35 - 11:55	**VPN als Einfallstor für Cyberkriminelle – und wie man sichere Abhilfe schafft mit HPE Aruba Networking SSE** Remote-Connectivity ist aus dem Arbeitsalltag nicht mehr wegzudenken. 96% aller Unternehmen setzten dabei auf VPN – und öffnen damit Cyberkriminellen (unbewusst) die Tür ins Unternehmen. Mit Zero Trust Network Access können eine sichere Alternative implementieren und weitere Security Dienste über die HPE Aruba Networking Secure Service Edge Plattform beziehen. Erfahren Sie in diesem Vortrag, wo die Risiken und Probleme einer VPN-Lösung liegen und wie Sie von dem Wechsel auf HPE Aruba Networking SSE profitieren können. **Elisabeth Berg** *Business Development Manager SASE Central Europe | Aruba*	**VMware Cloud Foundation (VCF) + vDefend (former NSX) - Die Basis für eine sichere OnPremis Infrastruktur** VMware Cloud Foundation ist die komplette Virtualisierungsplattform von VMware. Als AddOn dazu gibt es die Security Lösung namens vDefend. Das ist eine Netzwerk Virtualisierungs- und Sicherheitsplattform, welche erweiterte Sicherheitsdienste dynamisch in das Software-Defined Rechenzentrum einfügt. Eine software-basierte Firewall (vDefend Distributed Firewall, DFW) ist eine verteilte, horizontal skalierte interne Firewall, die den gesamten horizontalen Datenverkehr über alle Workloads hinweg ohne Netzwerkänderungen schützt und dadurch das Bereitstellungsmodell für die Sicherheit erheblich vereinfacht. **Andreas Schober** *Solution Engineer | VMware by Broadcom*	**A Million Ways to kill your SOC** Im Bereich Managed SOC hat CANCOM im DACH Raum eine führende Rolle. Seit einigen Jahren setzen wir bei unseren Kunden erfolgreich SOC Projekte um. In diesem Vortrag von Lukas Seidl zeigen wir diese Projekte einmal von der anderen Seite - Wir geben einen Einblick aus der Praxis über die gängigsten Methoden wie man ein SOC bereits in der Implementierungsphase, spätestens aber in der Betriebsphase erfolgreich „gegen die Wand fährt". **Lukas Seidl** *Principal SOC Release & Deployment Manager | CANCOM Austria*	**Wie man ein Kraftwerk in 20 min abdreht** Im Energieversorgerbereich werden Prozessleitsysteme eingesetzt, welche eine zentrale Rolle für den reibungslosen Ablauf der jedweiligen Prozesse umfassen. Nicht selten bleiben ihre Sicherheitsrisiken aber im Verborgenen. Dieser Vortrag gibt einen Einblick in die Schwachstellen und Cyber Security dieser System und zeigt, wie digitale Zwillinge von Industriesteuerungen eine zentrale Rolle im Zuge dessen bekommen. Wir zeigen, wie ein scheinbar - unscheinbares Notebook in 20 Minuten das gesamte Kraftwerk damit lahmlegen kann. Dieses Praxisbeispiel aus OT & IIoT Security ist ein Denkanstoss zu einer Variante, Sicherheitsmaßnahmen weiter zu verstärken und vor allem kritische Systeme entsprechend zu schützen. **Mario-Valentin Trompeter** *Geschäftsführer | CyberDanube*
12:00 - 12:20	**Unified Security Operations Platform (XDR+SIEM+AI+more)** The platform combines the best of SIEM, XDR and threat intelligence with advanced generative AI to provide a fully integrated set of tools for defenders - in a single portal. **Stefan Baresch** *Sr. Cloud Solution Architect | Microsoft*	**DC Microsegmentation mit dem Aruba CX10000 Switch** Zero Trust Security erfordert eine komplexe Segmentierung der Workloads und Services in Ihrem Rechenzentrum. Aruba CX10k mit seiner integrierten 800G Firewall visualisiert Ihnen sofort Ihre gesamte Server-zu-Server Kommunikation und hilft Ihnen komplexe Policies für Ihr gesamtes Rechenzentrum zu aktivieren. Somit erreichen Sie eine durchgängige Microsegmentierung mit wenig administrativen und operativen Aufwand zu einem Bruchteil der Kosten der heutigen DC Segmentierung Lösungen. **Homan Behrouzi** *AMD Pensando Sales DACH | Aruba*	**Network Detection and Response - Blindspots eliminieren. Angriffe schneller erkennen.** Schützen Sie Ihr Netzwerk vor den ständig weiterentwickelten Cyber-Bedrohungen durch frühzeitige Erkennung! Denn eine robuste Firewall oder eine EDR-Lösung reichen dafür heutzutage nicht mehr aus. Es braucht einen vielschichtigen Ansatz. Dabei hat sich Network Detection and Response (NDR) als wichtige Komponente herauskristallisiert. Die hohe Wirksamkeit bei der Stärkung der Cybersicherheitsabwehr wird in der Branche zunehmend anerkannt und akzeptiert. **Timo Jobst** *Systems Engineer | Corelight*	**CRISAM® GRC Plattform zur NIS 2.0/DORA Umsetzung** Unternehmen sehen sich heute mit einer Flut an Compliance-Anforderungen aus Normen, Regulativen und Gesetzen konfrontiert. Diese Komplexität belastet Organisationen, Budgets und Entscheidungsträger enorm und erzwingt eine holistische und workflow-basierte Lösung. Die CRISAM® GRC Plattform vereint Governance-, (IT-)Risiko- und Compliance-Disziplinen, die alle Beteiligten über die Organisationsgrenzen hinweg workflowbasiert involviert und interne sowie externe Kontrollen, Audits und Zertifizierungen vorbereitet und proaktiv unterstützt. Verschaffen Sie sich einen Überblick über die Einsatzbereiche und Fähigkeiten! **Mag. Juergen Gaechter** *Head of Sales | CALPANA business consulting GmbH*
12:20 - 13:25	**LUNCH BREAK IN DER PARTNER AREA**			
13:25 - 13:55	**Tagebuch eines Red Teamers - Feuer am Dach** Liebe Leute, es brennt lichterloh! Unternehmen werden unaufhörlich Opfer von Cyberkriminalität und Belegschaften sind kurz davor auszubrennen, während sie versuchen, dagegen anzukämpfen. Zwischen RCE-Hotfix-Patches und Projektdeadlines erscheinen wir, um Tatsachen aufzudecken, die lieber unter den Teppich gekehrt werden. Freut euch auf Geschichten, die Licht in die dunklen Ecken der digitalen Welt werfen! **Philipp Allmer** *Information Security Auditor | CANCOM Austia* **Philipp Reiter** *Information Security Auditor | CANCOM Austia*			
14:00 - 14:20	**Cyber crime in hypergrowth mode - How to build efficient resilience** Angetrieben durch geänderten Marktbedingungen haben Cloud-Dienste, Smartphones, die Kommerzialisierung von Cyberkriminalitätswerkzeugen im Darknet sowie AI Technologien das Spielfeld verwandelt. Erfahren Sie, wie die Check Point Infinity Platform Ihnen durch kollaborativen Sicherheitstools und innovativen Technologien zur Preventation hilft nicht nur zu reagieren, sondern proaktiv Cyberbedrohungen entgegenzuwirken und eine starke Resilienz aufzubauen. **Philipp Slaby** *Security Engineering | Check Point*	**Die Cisco Zero Trust Architektur** Die Cisco Zero Trust-Lösung bietet Benutzer- und Anwendungssicherheit in der gesamten Architektur. Sowohl persönliche Bring-Your-Own-Device (BYOD) als auch vom Unternehmen ausgegebene Geräte werden einem adaptiven Multi-Faktor-Authentifizierungsprozess (risikobasierte Authentifizierung)unterzogen und erhalten den am wenigsten privilegierten Zugriff mit kontinuierlicher Vertrauensüberwachung. **Syed Adil Hussain** *Technical Solutions Architect - Security | CISCO*	**Absicherung kritischer IT/OT Infrastruktur im Hinblick auf Zero Trust im Kontext von NIS 2.0 / DORA / IEC 62443** Bis 17. Oktober 2024 muss die NIS 2.0 Richtlinie umgesetzt sein. Auch hier spielt Zero Trust eine wesentliche Rolle. Nicht nur deshalb ist es für Unternehmen sehr wichtig die „Verwaltung von privilegierten Zugriffen, der Anmeldeinformationen und des Zugriffs auf Administratorebene und Weg zu einer passwortlosen Umgebung" sicherzustellen – nicht nur aber auch für den kontrollierten Zugriff von Partnern, Lieferanten und andere. Im Vortrag zeigen wie ihnen welche Möglichkeiten seitens SSH zur Verfügung gestellt werden und wie diesen den Zero Trust Ansatz unterstützen. **Dietmar Wyhs** *Director Sales CEEME (Central-, Eastern Europe and Meadle East Region) | SSH*	**SOS Cyber Attacke! Bereit für den Ernstfall mit der Disaster Recovery Architecture der CANCOM!** Wenn der Fall der Fälle eintritt, möchten wir unsere Daten bestmöglich geschützt wissen. Doch klassische Disaster-Recovery-Architecture wie Strecheed-Datacenter oder Cluster/Datenspiegelung sind gegen Cyber-Attacken nicht wirksam. Diese Bedrohungen sind mit dem Fokus auf einen Technologiebereich (z.B. Backup oder Security) alleine nicht abzuwehren. Daher sind umfassende Vorbereitungen essentiell. Ein Disaster Recovery Konzept ist die beste Sicherheit, die man haben kann. **Lukas Reicher** *Director Datacenter IT Solutions Applications | CANCOM Austria* **Harald Aichinger** *Solution Architect Datacenter Solutions - IT Infrastructure | CANCOM Austria*
14:25 - 14:45	**Modern XDR – what it is, what it isn´t** Das Akronym XDR wurde in den letzten Monaten in der Security-Branche an vielen Stellen genutzt – doch jeder meint damit etwas anderes. In diesem Vortrag möchten wir diese Begriffsverwirrung aufklären und darlegen was eine dem Stand der Technick entsprechende XDR Lösung bieten sollte. **Philip Scheidl** *Sales Engineer | Crowdstrike*	**Zero Trust - Von der Theorie zur Praxis** Das Konzept Zero Trust basiert darauf, die Dinge zu schützen, die am wichtigsten für ein Unternehmen sind. Genau diese unternehmenskritischen Assets müssen bestmöglich geschützt werden. Im Vortrag zeigen wir Ihnen unsere Sichtweise auf Zero Trust und unsere Vorgehensweise ein Zero Trust Konzept in einem Unternehmen zu entwickeln. **Peter Wendl** *Security Consultant | CANCOM Austria*	**Alles kann, NIS muss - Was Unternehmen und Behörden jetzt über NIS2 wissen sollten** Die Network-and-Information-Security-Richtlinie 2.0 (NIS2) bringt neue und strengere Vorschriften zur Cyber-Sicherheit. Sie gilt für viele Branchen – auch solche, die von bisherigen Regelungen nicht betroffen waren. Wir zeigen Ihnen auf, wie wir Sie konkret unterstützen können: ⌄ Erkennen und inventarisieren Sie alle bekannten und unbekannten Ressourcen, die mit Ihrer globalen hybriden IT-Umgebung verbunden sind – einschließlich lokaler Geräte und Anwendungen, mobiler Geräte, Endpunkte, Clouds, Container, OT und IoT. ⌄ Erhalten Sie mit CSAM erweiterte Einblicke und Details – einschließlich Hardware-/Software-Lebenszyklen (EOL/EOS), Softwarelizenz-Audits, kommerzieller und Open-Source-Lizenzen in Benutzung. ⌄ Regelbasierte Integrationen mit Qualys für ITSM-Tools (ServiceNow, JIRA) weisen automatisch Tickets zu und ermöglichen die Orchestrierung von Abhilfemaßnahmen – was die mittlere Zeit bis zur Abhilfe (mean time to remediation, MTTR) weiter reduziert. **Dirk Jankowski** *Solutions Architect Threat Detection & Response | Qualys*	**Apple Platform Security & DDM** Declarative Device Management (DDM) ist ein effektiver Ansatz zur Verwaltung von Geräten, der sich speziell auf die Durchsetzung von Betriebssystem-Updates konzentriert. Unser Vortrag beleuchtet allgemein das Thema Apple Platform Security, sowie die Bedeutung von OS-Update Enforcement innerhalb des DDM-Frameworks und dem damit verbundenen Paradigmenwechsel im MDM-Protokoll. Erfahren Sie, welche weiteren Vorteile DDM bietet und wie CANCOM Sie bei der Einführung oder beim Ausbau Ihrer Apple Device Management & Security Strategie für iOS/iPadOS und macOS Geräte unterstützen kann. **Michael Schiefele** *Senior Solution Sales Manager, Competence Center Modern Device Solutions | CANCOM GmbH*
14:45 - 15:20	**COFFEE BREAK IN DER PARTNER AREA SPONSORED BY ARUBA**			
15:20 - 15:40	**Risikomanagementmaßnahmen nach NIS-2** Von NIS-2 betroffene Einrichtungen müssen eine Reihe von Risikomanagementmaßnahmen umsetzen. Wir gehen der Frage nach, wie organisatorische, technische und operative Maßnahmen konkret aussehen können. **Jakob Gasser** *Information Security Consultant | CANCOM Austria*	**Evil-lution of Ransomware and why AI is required for Protection** A Single Infection is All it Takes! Ransomware attacks continue to unleash devastation on organizations, bringing operations to a grinding halt and inflicting substantial financial losses. These attacks continue to evolve in 2024. In this engaging session, John as he dives into the stages of an attack, empowering you with the latest adversaries' tactics, enabling you to fortify your defenses with 10 game-changing Best Practices ensuring your organization's resilience against the catastrophic impacts of ransomware attacks. **John Harrison** *Director, Evangelist NetSec and Unit 42, EMEAL | Palo Alto Networks*	**Secure Application Connectivity Anywhere** Business-Applikationen sind das Herzstück moderner Unternehmen, da sie die Effizienz steigern, die Produktivität verbessern und das Wachstum fördern. Eine schnelle Implementierung ist entscheidend, um Wettbewerbsvorteile zu erlangen und sich an sich ändernde Marktbedingungen anzupassen. Doch dabei darf die Sicherheit nicht vernachlässigt werden. Ein solides Management von Security Policies gewährleistet nicht nur den Schutz sensibler Daten, sondern auch die Einhaltung gesetzlicher Vorschriften. Letztendlich ermöglicht die Kombination aus schneller Implementierung und robustem Policy-Management Unternehmen, agil zu bleiben und gleichzeitig Sicherheit und Compliance zu gewährleisten. In diesem Vortrag demonstriert AlgoSec ihre Applikationsbasierendes Policy Management Lösung. **Sidney Ross** *Regional SE | Algosec* **Reinhard Eichborn** *Director strategic Partnerships | Algosec*	**QKD-Praktische Anwendung von Quantum Key Distribution in der Praxis** Wie mit Hilfe von Quantum Key Distribution Technologie im Rahmen eines von der EU und der Republik Österreich geförderten Forschungsprojektes unter der Leitung des AIT hochsicheres Schlüsselmaterial sicher zwischen zwei Rechenzentren kopiert werden konnte. Dieser Projekt zeigt wie bestehende Übertragungsstrecken veredelt werden können um hochsichere Datenanwendungen zu ermöglichen. **Thomas Mann** *CISO | CANCOM Austria*
15:45 - 16:05	**Step by Step: Der technische Blueprint für die NIS-2 Richtlinie** Entdecken Sie Schritt für Schritt die Kerntechnologien des NIS-2 Blueprints. Vom Konzept der Implementierung in der Infrastruktur - erfahren Sie, wie Sie die Anforderungen der NIS-2-Richtlinie effizient und sicher umsetzen können. **Kevin Mühlböck** *Security Consultant | CANCOM Austria*	**„SOC Reloaded" – Crowdstrike Next-Gen SIEM und das moderne SOC** Seit etwa 20 Jahren gibt es ein Verprechen von SIEM-Systemen: alle Logs zentralisieren, dann wird die Arbeit jedes Analysten einfacher. Die Realität sieht jedoch anders aus: schlechte Performance, viele False Positives, keine Reaktionsmöglichkeiten. Mit Crowdstrike NextGen SIEM geht es nun in ein neues Zeitalter, um das eigentliche Versprech**en von SIEM-Systemen endlich Realität werden zu lassen.** **Philip Scheidl** *Sales Engineer | Crowdstrike*	**Sicherheit von Webanwendungen - Vereinfacht durch Barracuda WAF-as-a-Service** Sie können Barracuda WAF-as-a-Service – ein über die Cloud bereitgestellter Service für Anwendungssicherheit – in wenigen Minuten aufsetzen und so einen vollständigen Schutz für alle Ihre Apps sicherstellen. Einfachheit mit Flexibilität. Barracuda WAF-as-a-Service bietet mit einem 3-Schritte-Bereitstellungsassistenten, vorgefertigten Vorlagen, einer leicht zu navigierenden Benutzeroberfläche und unbegrenzten Regelsätzen beispiellose Einfachheit. Umfassend skalierbar und global verfügbar. Barracuda WAF-as-a-Service ist bereit, alle Ihre Apps zu sichern. Es nutzt die umfassende globale Präsenz und Ressourcenflexibilität von Azure, um die Anforderungen an Skalierbarkeit und Verfügbarkeit jederzeit zu erfüllen. WAF-as-a-Service bietet Ihnen ein vollständiges Set an Funktionen und Fähigkeiten, um die umfängliche Sicherheit Ihrer Anwendungen zu gewährleisten. **Philipp Ortner** *Sales Engineer | Barracuda Networks AG*	
16:10 - 16:30	**NIS-2 und Versicherungsschutz – Kann die Cyber-Versicherung bei der Einhaltung der NIS-2 Vorschriften helfen?** Kerstin Keltner ist seit dem Jahr 2014 in der Versicherungsbranche in den Bereichen Cyber-Versicherung, Großschadenmanagement und Datenschutz tätig und derzeit als Prokuristin bei Aon Austria angestellt und für die Sparten Financial Lines & Cyber zuständig. Bereits im Studium hat sie sich auf die Bereiche IT- und Versicherungsrecht spezialisiert. Sie ist Lektorin an verschiedenen Weiterbildungseinrichtungen und publiziert regelmäßig zu den Themenbereichen Cyber-Versicherung, Datenschutz-, Versicherungsrecht. **Kerstin Keltner** *AON*	**Copilot for Security – defend at machine speed and scale** Microsoft Copilot for Security is a generative AI-powered security solution that helps increase the efficiency and capabilities of defenders to improve security outcomes at machine speed and scale. **Michael Fussthaler** *Sr. Technical Specialist | Microsoft* **Lukas Spitaler** *Sr. Security Specialist | Microsoft*	**FortiDeceptor: Mit Honig fängt man mehr Fliegen als mit Essig** Unternehmen & Organisationen verfügen heutzutage über eine Vielzahl an Mitteln und Wegen, um Angriffe zu erkennen und abzuwehren - diese setzen hoch-spezialisierte & abgestimmte Teams, exakte Segmentierung im Netzwerk und (oft) manuelle Reaktion voraus. Wie schafft man es durch einen „Zero false-positive" Ansatz effektiver und im Sekunden-Bereich auf moderne Bedrohungen zu reagieren, die Intentionen eines Angriffs zu verstehen und „Cyber-Security Schrauben" enger anzuziehen? **Teemu Schaabl** *Solutions Architect | Fortinet*	
16:40 - 17:00	**Offensive gewinnt Spiele, Defensive den Titel!** **Christian Sommer** *Director CANCOM Defense Center | CANCOM Austria* **Manfred Halper** *Director CANCOM RED Team | CANCOM Austria*			
17:00-17:10	**Recap und Verlosung**			
Im Anschluss (18:00 Uhr)	**Live-Übertragung des Fußball-EM-Spiels**			

PLATINUM SPONSORS

NIS-2 TRACK

Zero Trust TRACK

SOLUTIONS TRACK

Security Operations TRACK

OT Security Breakout Track

SOLUT. TRK