SECURITY DAY 2025

CANCOM

Schloss Schönbrunn Tagungszentrum, Apothekertrakt, 1130 Wien

		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 AG*			
09:25 - 10:00		**Keynote** **Beyond Firewalls, Security Challenges in the Era of AI-Tipping Points** **Christian Wenner** *VP Strategy & Portfoliomanagement, CANCOM Austria*			
10:00 - 10:35		**CANCOM** **Aktuelle Schwachstellen & Bedrohungen** **Manfred Halper** *Director RED Team | CANCOM Austria*			
10:35 - 11:10		**COFFEE BREAK IN DER PARTNER AREA**			
11:10 - 11:30	PLATINUM SPONSORS	**Security auf Höchstleistung:** **Ihre Infrastkutur modernisiert durch ThreatCloud AI** Phishing bleibt einer der meistgenutzten Angriffsvektoren, weshalb innovative Lösungen zum Schutz von E-Mail- und Collaboration-Services unabdingbar sind. Gleichzeitig erfordern hybride IT-Umgebungen moderne Sicherheitsarchitekturen, um einen ganzheitlichen Schutz zu gewährleisten – durch Hybrid Mesh Firewall-Plattformen inkl. SASE. Um Angreifern einen Schritt voraus zu sein können Sie mit Infinity External Risk Managmenet Bedrohungen erkennen und entschärfen, bevor Sie zu Sicherheitsvorfällen werden. Erfahren Sie, wie Sie Ihre IT-Infrastruktur modernisieren, Risiken minimieren und gleichzeitig Effizienz und Sicherheit maximieren. **Patrick Fetter** *Technical Solutions | Check Point Software Technologies*	Security Operations Track	**Einsichten und Erfahrungen aus Ransomware-Angriffen:** In dem Vortrag werden Vorgehensweisen und Taktiken betrachtet, die von Ransomware-Akteuren häufig eingesetzt werden, um organisationale Infrastrukturen anzugreifen und zu kompromittieren. Wir werden Möglichkeiten aufzeigen und besprechen, diese Vorgehensweisen und Taktiken besser zu entdecken und auf diese zu reagieren sowie eine allgemeine Stärkung der Sicherheitsarchitektur zu erreichen, die sich als widerstandsfähiger gegen diese und andere Bedrohungsarten erweist. **Stefan Voemel** *Consulting Director, Unit 42 | Palo Alto Networks*	Networrk Security & Connectivity Track	**„ Secure Application Connectivity Management in Hybriden Umgebungen mit AlgoSec Horizon“** Unternehmen fehlt es oft an der nötigen Visibilität, um die Anwendungsanbindungen in hybriden IT-Umgebungen effektiv zu managen. Die AlgoSec Horizon Plattform vereinfacht und visualisiert diese Verbindungenanforderungen durch eine Applikation-zentrierte Sicht auf die Netzwerkinfrastruktur. Mit der intelligenten Automatisierung von Sicherheitsrichtlinien, präzisem Risikomanagement und kontinuierlicher Compliance-Prüfung steigert die Plattform die Effizienz Ihres IT-Betriebs, minimiert Risiken, vermeidet Ausfallzeiten und fördert gleichzeitig die Agilität Ihrer Anwendungen – alles bei maximaler Transparenz und Kontrolle. **Sidney Ross** *Regional Sales Engineer Switzerland & Austria | Algosec*	Management Track	**Microsoft Security:** **vom Grundschutz zur Hochsicherheit in einfachen Schritten.** Erfahren Sie, wie Sie - ausgehend vom Client - von den grundlegenden Sicherheitsfunktionen in ihrer Microsoft 365 Subscription zu einer umfassenden Sicherheitslösung gelangen. Wir zeigen Ihnen, wie Sie das Optimum aus ihren bestehenden Subscriptions holen, durch zusätzliche Add-ons Ihre Sicherheitsmaßnahmen erweitern und schließlich mit Microsoft 365 E5 und Azure Services wie Microsoft Sentinel und Defender for Cloud eine erstklassige Sicherheitsstrategie entwickeln können. **Stefan Baresch** *Sr. Partner Solution Architect | Microsoft*
11:35 - 11:55	PLATINUM SPONSORS	**Risiken im Griff – Angriffsflächen intelligent reduzieren mit CrowdStrike Exposure Management** Je größer die digitale Angriffsfläche, desto größer das Risiko. CrowdStrike Falcon® Exposure Management schafft klare Sicht auf alle internen und externen IT-Assets, bewertet Schwachstellen in Echtzeit und hilft Teams, gezielt dort zu handeln, wo es zählt. So lassen sich Risiken schnell priorisieren, Sicherheitslücken schließen und potenzielle Angriffe frühzeitig verhindern. Der Schlüssel zu einer proaktiven Sicherheitsstrategie – effektiv, skalierbar und intelligent vernetzt. **Alexander Kriechbaum** *Sales Engineer | Crowdstrike*	Security Operations Track	**Disrupt modern attacks with Network Evidence** Corelight transforms network and cloud activity into evidence so that data-first defenders can stay ahead of ever-changing attacks. Delivered by our Open NDR Platform, Corelight's comprehensive, correlated evidence gives you unparalleled visibility into your network. This evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks. Our on-prem and cloud sensors go anywhere to capture structured, industry-standard telemetry and insights that work with the tools and processes you already use. Corelight's global customers include Fortune 500 companies, major government agencies, and research universities. **Ken Greene** *Director of Partners, EMEA | Corelight EN*	Networrk Security & Connectivity Track	**NAC (Network Access Control) we can** Egal, ob wir über IT/OT sprechen, schnell kommt die Frage auf, wie integrieren wir eine große Anzahl von verschiedensten Geräten auf sichere Art und Weise in unser Netzwerk. Wo können wir Zertifikate verwenden? Wie können wir Geräte ohne Dot1x authentifizieren, weil diese Methode nicht (praktikabel) implementiert ist? Kann man in die NAC-Welt auch andere Security-Systeme integrieren und wie praktikabel ist das? Mit Aruba ClearPass, Cisco ISE und macmon NAC finden wir gemeinsam die passende Lösung für Ihre Umgebung UND lösen im Vorbeigehen auch noch viele andere Probleme (Client-Insight, Komplexität, manuelle Eingriffe wegen Standard-Changes, ...). **Michael Höflmaier** *System Engineer | CANCOM Austria*	Management Track	**Warum Mitarbeiter Daten Ihres Unternehmens stehlen und wie man damit umgeht.** In unserer modernen IT-Welt konzentrieren wir uns ständig darauf, externe Bedrohungen zu verhindern. Dabei übersehen wir oft eine der größten Bedrohungen: Insider in unseren eigenen Reihen. Wirtschaftsspionage, hohe Mitarbeiterfluktuation und Korruption sind nur einige Gründe, warum Personen Daten von ihren eigenen Unternehmen stehlen könnten. Zudem reicht eine einzige kompromittierte Identität aus, damit ein Angreifer vom Außenseiter zum Insider wird. Diese Handlungen bleiben oft unbemerkt, da sie unter dem Deckmantel legitimer Autorisierung erfolgen. Darüber hinaus haben Mitarbeiter in der Regel Zugang zu weit mehr Daten, als sie für ihre Arbeit benötigen. Generative KI fügt diesem Problem eine weitere Komplexitätsebene hinzu. **Sven Carlsen** *Sales Engineer | Varonis*
12:00 - 12:20	PLATINUM SPONSORS	**Better Together - Cisco und Splunk und das ‚SOC of the Future‘** Als ehemaliger Cisco Veteran und jetzt Splunk Österreich Sales Director gibt Ihnen Markus Hatz Einblicke über die Zukunftsstrategie von Cisco und Splunk im Bereich SIEM/SOC. Darüber hinaus erfahren Sie, warum Cisco und Splunk zusammen mehr Sicherheit und Visibilität in Ihr Security Operation Center bringen und die digitale Resilienz Ihres Unternehmens stärken. **Markus Hatz** *Splunk Regional Sales Director Austria | Cisco*	Security Operations Track	**Pyongyang‘s Digital Deception: Unmasking North Korean IT Scams** Dieser Vortrag befasst sich mit der alarmierenden Zunahme nordkoreanischer Agenten, die sich als legitime IT-Experten ausgeben, globale Organisationen infiltrieren und erhebliche Risiken für die Cybersicherheit darstellen. Erfahren Sie mehr über die angewandten Taktiken, die Auswirkungen auf das Unternehmen und Strategien zum Schutz vor dieser komplexen Bedrohung. **Joël Giger** *Senior Consultant - Intelligence Advisory Services EMEA | Recorded Future*	Networrk Security & Connectivity Track	**AI-Powered Firewalls And Self-Healing and Automated Converging Networks** Entdecken Sie, wie modernste Fortschritte in der Cybersicherheit – darunter eine leistungsstarke KI-/ML-Engine und die tiefgreifende Integration mit Data Loss Prevention – den Schutz sensibler Daten stärken und wie die neuesten Innovationen in der einzigen selbstheilenden, autonomen WAN-Edge-Lösung der Branche ihnen helfen kann! **Markus Hirsch** *Manager System Engineering | Fortinet* **Stephan Bacher** *System Engineer | Fortinet*	Management Track	**Business Continuity: Mehr als ein Tool – der Faktor Mensch und Methode** Während sich viele Security-Lösungen auf Technik konzentrieren, geht es im Business Continuity Management um systematisches Vorgehen, Verantwortlichkeiten und gelebte Prozesse. Wir zeigen, wie ein wirksames BCMS aufgebaut wird – und warum Technik allein im Ernstfall nicht reicht. **Erwin Zierler** *Senior Consultant mit Schwerpunkt ISMS, BCM | Calpana*
12:20 - 13:25		**LUNCH BREAK IN DER PARTNER AREA**			
13:25 - 13:55		**Tagebuch eines Red Teamers** **Marcel Schnideritsch** *Senior Pentester | CANCOM Austia* **Marco Dermutz** *Senior Information Security Auditor | CANCOM Austia*			
14:00 - 14:20	PLATINUM SPONSORS	**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 | HPE Aruba*	Secure Infrastructure Track	**„Die Wahrheit liegt im Posteingang“** In der Geschäftswelt kommunizieren wir die Wahrheit – oder das, was wir dafür halten – meist per E-Mail. Doch in einer Welt, in der fast alles digital geschieht, stellt sich die Frage: Wem – oder was – können wir wirklich trauen? Vertrauen in die Identität des Kommunikationspartners, die Integrität der Nachricht und die Vertraulichkeit der Übertragung bilden das Fundament digitaler Beziehungen – und sind der Schlüssel zu nachhaltigem Geschäftserfolg. In diesem Kurzvortrag werfen wir einen frischen Blick auf unser wichtigstes Kommunikationswerkzeug: die E-Mail. Und wir zeigen, wie sich damit echtes Vertrauen aufbauen lässt – einfach, sicher und nachvollziehbar. **Roman Stadlmair** *Country Manager SEPPmail | Seppmail*	Networrk Security & Connectivity Track	**Eliminating Security Blind Spots with Network Visibility** In the face of increasing cyber threats, achieving comprehensive network security is crucial. This presentation will explore how Keysight packet brokers play a pivotal role in enhancing network visibility and eliminating security blind spots. By efficiently aggregating, filtering, and distributing network traffic, Keysight packet brokers ensure that security tools receive the right data at the right time. **Cristian Lazar** *Sr. Solutions Engineer | Keysight*	Network Security	**Hilfe, mein Netzwerk lebt! Aber wie?** **CANCOM Inventory Engine (IE): Professionelles Asset-, Lifecycle- und Vulnerabilty-Management für Ihre Netzwerk-Infrastruktur** Wir zeigen Ihnen, wie Sie mithilfe dieses CANCOM Eigenproduktes sämtliche Hardware- und Software-Assets Ihres Netzwerks stets im Auge behalten können. Veränderungen der Installed Base werden mithilfe der IE Snapshot Technologie nachvollziehbar und belegbar gemacht. Bislang aufwendige Tätigkeiten (z.B. HW & SW Lifecycle-Management, Lizenzmanagement, Budgetierungsprozesse, Kostenumlagen) können zukünftig mittels „Knopfdruck“ einfach und rasch erledigt werden. Behalten Sie mithilfe der IE zudem den Überblick über eingesetzte SW-Versionen und managen Sie diese auf Basis von Empfehlungen des Herstellers. Nutzen Sie die zahlreichen Funktionen der Lösung, um Compliance-Vorgaben (z.B. NIS-2, DORA) zu Ihrer Netzwerk-Infrastruktur zu erfüllen und CISO's und Auditoren die notwendigen Informationen bereitzustellen. Reagieren Sie auf neue Vulnerabilities und dokumentieren Sie die gesetzten Schritte mithilfe dieser Lösung. Asset-, Lifecycle- und Vulnerabilty-Daten sind über das GUI, sowie Reports und über die integrierte REST API flexibel nutzbar und jederzeit auch für Drittsysteme (z.B. ITSM, SIEM) verfügbar. Vereinfachen Sie das Management Ihrer Netzwerk-Infrastruktur – mithilfe der CANCOM Inventory Engine! **Thomas Gerbafczits** *Head of Network Solution Design | CANCOM*
14:25 - 14:45	PLATINUM SPONSORS	**Datenschutz in Zeiten von Copilot(en)** Datenverluste verursachen stets Kosten, die durch Geldverlust (Intellectual Property), regulatorische Strafen oder Reputationsschäden erheblich sein können. Unkontrollierter Einsatz von Copiloten erhöht das Risiko von Datenschutzverletzungen und Datenverlust. Der Vortrag behandelt Herausforderungen wie „Oversharing“ und „AI Prompts“ sowie deren Lösungen durch Microsoft Purview. **Klaus Reiter** *Technical Specialist Compliance | Data Security | Microsoft*	Secure Infrastructure Track	**Bridging Distance Safely:** **Secure Remote Access in Industrial Operations** In einer zunehmend vernetzten Industrielandschaft ist sicherer Fernzugriff essenziell für den effizienten Betrieb und die Wartung von Produktionsanlagen. Der Vortrag „Bridging Distance Safely: Secure Remote Access in Industrial Operations“ beleuchtet die Herausforderungen und Risiken bei der Implementierung von Remote-Access-Lösungen in industriellen Umgebungen. Es werden bewährte Methoden, aktuelle Sicherheitsstandards sowie praktische Ansätze vorgestellt, um Produktionsnetzwerke zuverlässig vor Cyberbedrohungen zu schützen und gleichzeitig den Zugriff für Servicepartner und interne Teams effizient zu gestalten. **Martin Lampel** *Director OT Security Solutions, System Integration | CANCOM Austria*	Networrk Security & Connectivity Track	**„Stay in control in a Hyperconnected World – The Key to Success through a Hybrid Mesh Architecture“** In einer zunehmend hypervernetzten Welt, in der Unternehmen mit einer Vielzahl an Geräten, Anwendungen und Sicherheitsbedrohungen konfrontiert sind, wird die Kontrolle über die komplexe IT-Infrastruktur immer anspruchsvoller. Die ständig wachsende Zahl an Systemen, die zunehmenden Cyberbedrohungen und die Notwendigkeit, schnell auf Veränderungen zu reagieren, stellen enorme Herausforderungen dar. Eine zentrale Plattform hilft, diese Komplexität zu meistern, Sicherheitslösungen effizient zu verwalten und eine umfassende Übersicht über alle Systeme zu erhalten. Die Einführung einer Single Management Platform und Umsetzung einer Hybrid Mesh Architektur ermöglicht es Unternehmen, Risiken zu minimieren, Bedrohungen frühzeitig zu erkennen sowie gezielt zu bekämpfen und gleichzeitig die Betriebskosten zu senken – der Schlüssel zum Erfolg in einer vernetzten und unsicheren Welt. **Philipp Slaby** *SE Manager Austria | Checkpoint*	Network Security	
14:45 - 15:20		**COFFEE BREAK IN DER PARTNER AREA**			
15:20 - 15:40	TRENDS & NEWS	**New Technologies approaching - News der RSA Conference** Neuigkeiten von der RSA Conference, Einblicke in neue Technologien, welche Probleme Top Unternehmen im Bereich Cyber Security adressieren, wie AI die Cyber Kill Chain autonomisiert. Verschaffen Sie sich einen Überblick über die spannensten Innovationen im Bereich Cyber Security. **Kevin Mühlböck** *Senior Technical Specialist | CANCOM Austria*	Cloud Security Track	**Introducing Successful Cloud Security** Betrachtet man alle realen Sicherheitsverletzungen in der Cloud, so gibt es sehr selten nur einen Faktor, der zu einer Sicherheitsverletzung führt; sie ist fast immer vielschichtig und umfasst die Ausnutzung von Schwachstellen und Fehlkonfigurationen. Zwar sind bewährte Sicherheitsverfahren für die Konfiguration von Cloud-Ressourcen und -Diensten bekannt, doch in der Realität werden diese Verfahren nicht befolgt. Eine der führenden Malware in der Cloud sind Kryptominers, die sowohl Schwachstellen als auch Fehlkonfigurationen ausnutzen, um Cloud-Ressourcen zu kapern. Dabei handelt es sich nicht um isolierte, sondern um miteinander verknüpfte Probleme, bei denen das Vorhandensein eines Risikofaktors einen anderen verstärken kann, wodurch sich das Potenzial für Sicherheitsverletzungen erhöht. Diese erweiterte Perspektive unterstreicht die Notwendigkeit einer ganzheitlichen Sicherheitsstrategie, die alle Facetten der Cloud-Sicherheit berücksichtigt. Es geht darum, die Sicherheitslücken zu schließen, die Konfigurationen zu verschärfen und wachsam gegenüber den sich entwickelnden Malware-Bedrohungen zu sein. **Christian H. von Hößlin** *Sales | Qualys*	Networrk Security & Connectivity Track	**SSE - Best practises für sichere Applikationen und Daten Zugriff** Die Traditionellen VPN Netzwerke haben ausgedient, der Perimeter-basierte Sicherheitsansatz ist nicht mehr zeitgemäß. Die HPE Aruba Networking SSE Lösung bietet einen Fernzugriff für Mitarbeiter und externe Geschäftspartner mittels Zero-Trust Methode an. Ein universeller Zugang auf Business Resourcen mit einheitlicher Policy - onprem und remote, beste User Experience, beste Performance. **Thomas Latzer** *SASE Sales Specialist | HPE Aruba*	
15:45 - 16:05	TRENDS & NEWS	**Quantum-safe Communication Technologies** Andreas Neuhold verfügt über mehr als 15 Jahre Erfahrung in der Entwicklung und dem Betrieb von Kernkomponenten für Kabel-, Glasfaser- und mobilen Internetzugang für führende internationale Tier-1 ISPs. Zu seinen jüngsten Tätigkeiten gehören Projekte und F&E zur Entwicklung neuer Cybersicherheitstechnologien wie Quantum Secure VPN mit Quantum Key Distribution (QKD) und Post Quantum Crypto (PQC). #qkd, #pqc, #wireguard, #qcicat **Andreas Neuhold** *Senior Technical Specialist | CANCOM Austria*	Cloud Security Track	**Kontrolle über die Schatten-IT – SaaS-Sicherheit mit CrowdStrike Falcon Shield** SaaS-Anwendungen sind aus dem Geschäftsalltag nicht mehr wegzudenken – doch jede App bringt eigene Sicherheitsrisiken mit sich. CrowdStrike Falcon Shield (SSPM) bietet Sicherheitsteams vollständige Transparenz und Kontrolle über alle geschäftskritischen SaaS-Anwendungen. Durch kontinuierliche Überwachung und proaktives Risikomanagement behalten Sie den Überblick über Nutzer, Geräte, Daten und nicht-menschliche Identitäten – und schützen Ihr Unternehmen effektiv vor Fehlkonfigurationen, Datenverlust und unbemerktem Zugriff. **Philip Scheidl** *Sales Engineer | Crowdstrike*	Networrk Security & Connectivity Track	**Moderne Segmentierung mit Cisco Hybrid Mesh Firewall** Die Cisco Zero-Trust-Segmentierung schließt als erster verfügbarer Service die Lücke zwischen Sicherheits- und Netzwerkebene und bringt diese in einer Lösung zusammen, indem Services direkt in das Netzwerk eingebettet werden. **Adil Hussein** *Cybersecurity Channel Technical Solutions Specialist | Cisco*	
16:10 - 16:30	TRENDS & NEWS	**Arbeit, Arbeit – die dunkle Seite des Schwachstellen Managements** Im Jahr 2025 ist „Vulnerability Management“ nicht nur begrifflich in verschiedenen Compliance Vorgaben vertreten, sondern inzwischen auch technisch nicht mehr aus der SecOps Werkzeugkiste wegzudenken. Mit einem Blick in die Erfahrungswerte aus Kundenprojekten der letzten Jahre werfen wir ein Auge auf Fallstricke und Lösungen rund um das Thema Schwachstellen Management. **Dan Jung** *Senior Security Operations Consultant | CANCOM Austria*	Cloud Security Track	**Vier echte Beispiele, wie Tenant-Misskonfiguration zur Katastrophe führte** In dieser Session zeigen Lukas Reicher und Sebastian Gritsch anhand von vier realen Vorfällen, wie schnell eine falsch konfigurierte Microsoft 365-Umgebung zu gravierenden Sicherheitslücken führen kann. Als CANCOM AT betreuen wir rund 700 Tenants vom Mittelstand bis zum Enterprise-Segment und sehen täglich, wie komplex und volatil die Cloud-Welt ist. Neue Features, neue Namen – wer hier nicht ständig am Ball bleibt, verliert leicht den Überblick. Wir sprechen über Oversharing, fragwürdige Mailflows, die geschickt an MX-Gateways vorbei manövrieren, und wie Gäste ganz unbemerkt weitere Gäste einladen können. Unser Service hilft, genau solchen Risiken vorzubeugen – automatisiert, effektiv und entlastend für Ihre IT. Lernen Sie aus den Fehlern anderer, bevor es Sie selbst trifft. **Sebastian Gritsch** *System Engineer M365 | CANCOM* **Lukas Reicher** *Director Datacenter IT Solutions Applications | CANCOM*	Networrk Security & Connectivity Track	
16:40 - 17:00	TRENDS & NEWS	**Abschlussvortrag** *CANCOM Austria*			
17:00-17:10		**Recap und Verlosung**			
Im Anschluss (18:00 Uhr)		**Chill & Cheers: Der perfekte Abschluss.** **Food, drinks, networking.**			