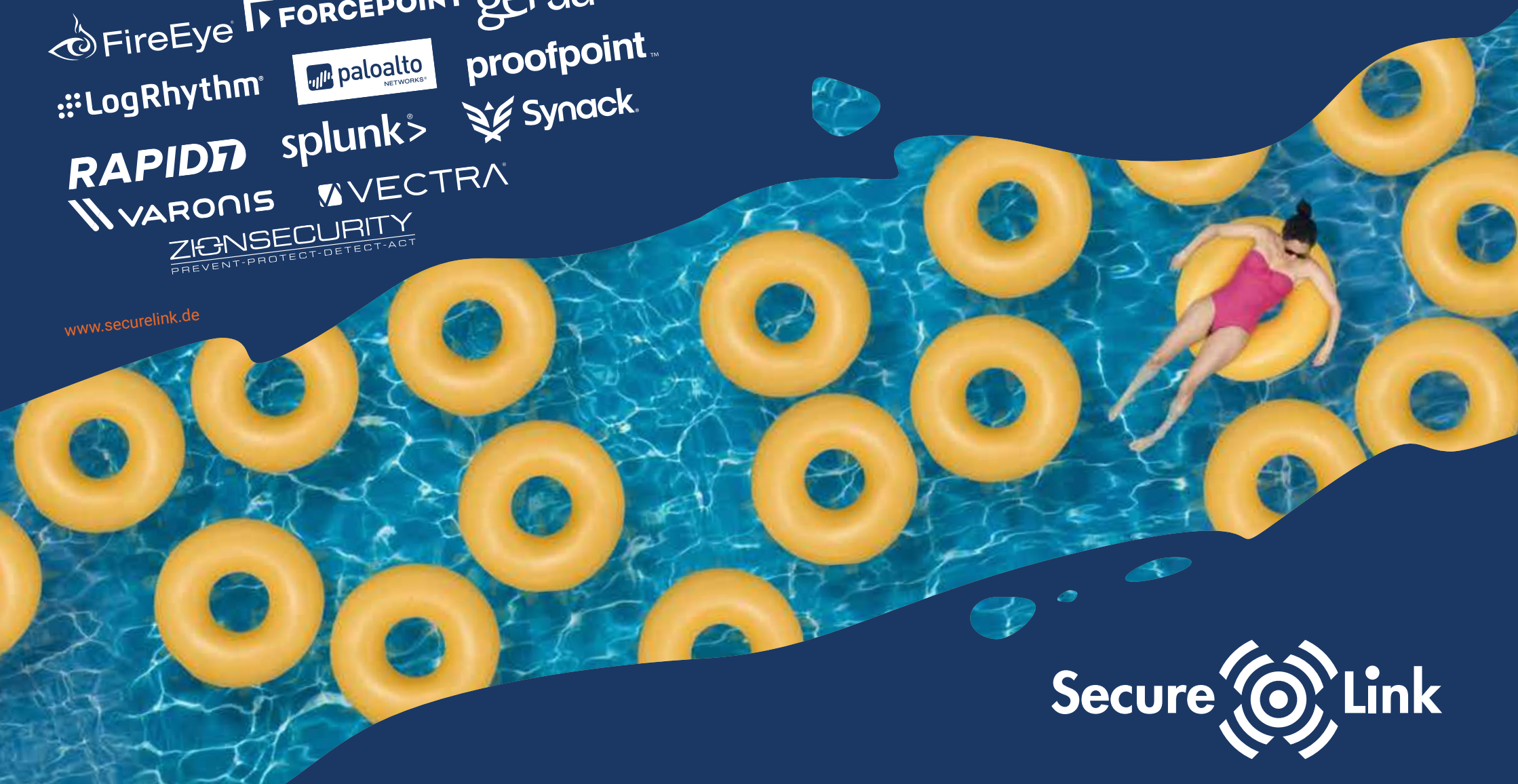
powered by:

agileSI
algosec
Blueliv.
Check Point SOFTWARE TECHNOLOGIES LTD.
CYLANCE
DEMISTO
digital shadows_
exabeam
F5
FireEye
FORCEPOINT
genua
LogRhythm
paloalto NETWORKS
proofpoint
RAPID7
splunk>
Synack
VARONIS
VECTRA
ZIGNSECURITY
PREVENT-PROTECT-DETECT-ACT

www.securelink.de

DETECT DEFEND 19

CYBER DEFENSE
made easy



Secure Link

DETECT & DEFEND 19

Programm

Weitere Infos und Anmeldung

unter www.detect-defend.de

CYBER DEFENSE
made easy

Lösungen, keine Probleme...

Wir haben eine gute Nachricht für Sie: Die IT-Welt geht nicht unter! Trotz der Meldungen über Hacker-angriffe, Datenverlust und staatliche Cyberattacken – seien Sie beruhigt: Es gibt für jedes Problem eine Lösung.

Gönnen Sie sich eine Auszeit auf der Detect & Defend 2019 und sehen Sie, warum es keinen Grund gibt, die Digitalisierung zu fürchten.

Erleben Sie IT-Security aus einer neuen Perspektive.

IT-Sicherheit ist ein komplexes Thema? Natürlich, aber das sollte unser Problem sein, nicht Ihres!

Mit den besten Partnern der Branche sorgen wir dafür, dass Sie sich entspannen können. Wir finden was Sie brauchen und übernehmen Lieferung & Implementierung. Und bei Bedarf kümmern wir uns auch noch um den Betrieb.

Erleben Sie, wie entspannt Cybersecurity sein kann – auf der Detect & Defend 2019!

CYBER DEFENSE
made easy

DETECT DEFEND 19

DAY 1

Zeit	Track 1 - Vorträge	Track 2 - Vorträge	Track 3 - Workshops	Track 4 - Workshops
	08:00 - 09:00 Uhr: Registrierung			
09:00-09:30	Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der SecureLink Germany			
09:30-10:15	Entspannte Keynote: Markus Hofmann, Gedächtnistrainer			
10:30-11:15	Von SIEM zu Next-Gen SIEM: Neue Lösungen zur schnelleren Detektion und Reaktion von und auf Cyber-Bedrohungen *presented by LogRhythm*	Breach Detection Made Easy! Understanding AI in network detection and response [ENG] *presented by Vectra*	KI-Roundtable. Chancen und Risiken der künstlichen Intelligenz in der IT-Security. *hosted by SecureLink*	Cyber Attack Simulation LIVE. *hosted by FireEye*
11:30-12:15	Compliance- und Governance-Standards in der Public Cloud. *presented by Check Point*	Multi-Cloud Security and Compliance Made Easy. *presented by Palo Alto Networks*		
	12:15-13:15 Uhr: Lunch			
13:15-14:00	This is what happened! Eward Driehuis presents the Annual Security Report. *presented by SecureLink*	Heiter & wolkig: Wie Sie Ihre Multi-Cloud-Umgebung mit Ihrer IT-Sicherheit in Einklang bringen *presented by F5*	Roundtable: User Monitoring vs. Data privacy. *hosted by Forcepoint*	Ausbildung von SOC-Experten – Made Easy. *hosted by SecureLink*
14:15-15:00	SIEM Modernization - The Smarter Way. *presented by Exabeam*	Endpoint Protection Made Easy! Künstliche Intelligenz. Vom Hype zum Werkzeug. *presented by Cylance*		
	15:00-15:30 Uhr: Tea & Networking			
15:30-16:15	You have been breached - Ein Tag im Leben eines gehackten Unternehmens. *presented by Blueliv*	Cyber Defense Made Easy - Die Kur für Ihre Angriffserkennung *presented by SecureLink*	Secure Development Life Cycle and the lack of Security Expertise with Development Professionals *hosted by Zion Security*	Demo *hosted by Demisto*
16:30-17:15	Ganz entspannt bleiben bei Malware und Phishing: Secure E-Mail Made Easy! *presented by Proofpoint*	Cyber Defense with Ease - Ask your Data and mature *presented by Splunk*		
17:30-18:00	Wrap Up & After Hour Session			
	ab 18:00 Uhr: Cyber Defense Made Easy -Abendevent			

Track 1 - Vorträge

10:30 | Von SIEM zu Next-Gen SIEM: Neue Lösungen zur schnelleren Detektion und Reaktion von und auf Cyber-Bedrohungen.
presented by LogRhythm

- Welche Fähigkeiten sollte ein Next-Gen SIEM-System unbedingt besitzen und wieunterscheidet sich diese von herkömmlichen SIEM-Lösungen
- Ein Reifegrad-Modell hilft ihnen, ihre aktuellen Möglichkeiten der Detektion und Reaktion zu bewerten.
- Außerdem gibt es Ihnen Unterstützung es bei der Auswahl der nächsten sinnvollen Schritte, um Ihre Situation zu verbessern, sowie hilft bei der Analyse, ob und wie sich Ihre Investments auszahlen.
- Wir zeigen wie Sie mit erweiterten Analysen, UEBA Anomalie-Erkennung, sowie der Automatisierung und Orchestrierung (SOAR) des Security-Workflows Bedrohungen besser zu erkennen und zu minimieren sind.

11:30 | Compliance- und Governance-Standards in der Public Cloud.
presented by Check Point

- CloudGuard mit Dome9 ist eine umfassende Plattform für die Automatisierung von Sicherheit und Compliance in der Public Cloud und bietet Transparenz, kontinuierliche Compliance, aktiven Schutz und Bedrohungserkennung
- CloudGuard Dome9 ist eine API-basierte SaaS-Plattform, die sich nativ mit Amazon Web Services (AWS), Microsoft Azure und der Google Cloud Platform (GCP) integriert.
- Es bietet Leitplanken, um Ihre Angriffsfläche zu minimieren und stellt sicher, dass Sie die Compliance- und Governance-Standards in der Public Cloud erfüllen.

13:15 | This is what happened! Eward Driehuis presents the Annual Security Report [ENG].
presented by SecureLink

Jedes Jahr publiziert SecureLink den Annual Security Report. Dabei werden Trends beschrieben, abgeleitet aus Beobachtungen, die wir in unseren fünf Cyber Defense Centers (CDCs) das Jahr hindurch machen.

Eward Driehuis zeigt, warum die Daten relevant sind und wie sie Entscheidern helfen können, sich vorzubereiten.

14:15 | SIEM Modernization - The Smarter Way.
presented by Exabeam

- SIEM ist notwendig, aber der Betrieb ist aufwendig und teuer. Exabeam löst das Problem mit modernen Analysemethoden wie Machine Learning und Data Science.
- Mit weniger Personal bessere Ergebnisse zu erzielen ist „zu schön um wahr zu sein“. Das ist übrigens ein Zitat eines Exabeam Kunden.
- Erfahren Sie in einer Live-Demo Alles über die Funktionen der Lösung.

15:30 | You have been breached: Ein Tag im Leben eines gehackten Unternehmens.
presented by Blueliv

- Was haben der japanische Elektronikkonzern Sony, die US-amerikanische Hotelkette Marriott und der US-amerikanische Fahrdienstleister Uber mit dem Deutschen Bundestag gemeinsam? Sie alle haben für Schlagzeilen gesorgt – und zwar ganz anders als ihnen lieb ist. Denn vertrauliche Daten gelangten an die Öffentlichkeit.
- Man kann davon ausgehen, dass Unternehmen dieser Größenordnung und Einrichtungen wie der Bundestag um die Gefahren wissen und auch Vorkehrungen getroffen haben. Und dennoch wurden sie Opfer. Kann man überhaupt vorbeugen oder ist man den Hackern einfach ausgeliefert? Hundertprozentigen Schutz gibt es nicht. Aber man kann durchaus etwas tun.
- In diesem Vortrag zeigt Blueliv auf, wie die Hacking-Industrie gestohlene Zugangsdaten abschöpft und sie anschließend zu Geld macht. Anschließend wird dargestellt, wie Sie sich mittels Targeted Threat Intelligence erfolgreich gegen diese Angriffe wehren und so das Haupteinfallstor für Hacker schließen können.

16:30 | Ganz entspannt bleiben bei Malware und Phishing: Secure E-Mail Made Easy!
presented by Proofpoint

- Der Mensch steht immer mehr im Mittelpunkt aktueller Cyber-Angriffe. Durch die Nutzung moderner Technologien und zentralisierter Dienste hat sich das Arbeiten von Heute verändert.
- Proofpoint erläutert, welches Risiko damit verbunden ist, welche Auswirkungen es haben kann und wie Unternehmen sich schützen können.

Track 2 - Vorträge

10:30 | Breach Detection Made Easy!
Understanding AI in network detection and response [ENG]
presented by Vectra

In this session we'll examine how AI works in threat detection and response, and can reduce cyber risk by:

- Automating threat detection with always-learning behavioural models that detect attackers, not just anomalies in real time to enable quick, decisive response and a logical investigative starting point
- Exposing hidden attackers by examining Network metadata, logs and cloud that reveal hidden attackers in workloads and user / IoT devices. Even in encrypted traffic.
- Empower threat hunters to launch deeper incident investigations and hunt retrospectively for covert attackers.

11:30 | Multi-cloud security and compliance made easy.
presented by Palo Alto Networks

- PAN Sicherheitslösungen bei Amazon AWS, Microsoft Azure und Google Cloud,
- Redlock (Schwerpunkt) und Aperture,
- Online Demo mit Offline Backup

13:15 | Heiter & wolkig: Wie Sie Ihre Multi-Cloud-Umgebung mit Ihrer IT-Sicherheit in Einklang bringen!
presented by F5

In einem zunehmenden digitalen Geschäftsumfeld repräsentieren die Anwendungen das Business eines Unternehmens, sie sind Kommunikationsmittel und Bindeglied zu Kunden und Partnern. Die notwendige Flexibilität und die Business-Agilität, um sich in hart umkämpften Märkten Wettbewerbsvorteile zu sichern, können nur durch moderne IT-Architekturen wie z.B. cloudbasierte Services wie IaaS, PaaS oder SaaS verwirklicht werden. Doch wie so oft bergen neue Chancen auch neue Herausforderungen und Risiken, hier sind es insbesondere oftmals existentielle Fragen der IT-Sicherheit.

Der Vortrag von F5 zeigt den unaufhaltbaren Weg in die Cloud auf und beleuchtet die unterschiedlichen Konzepte von Private-, Public- und Multicloud unter besonderer Berücksichtigung der Anforderungen an die IT-Sicherheit und stellt dar, dass Sie bei der „Cloud-Security" keinerlei Abstriche machen oder Kompromisse eingehen müssen.

14:15 | Endpoint Protection Made Easy!
Künstliche Intelligenz. Vom Hype zum Werkzeug.
presented by Cylance

- KI ist steinalt. Warum ist das Thema jetzt hip?
- Wie künstliche Intelligenz die Endgerätesicherheit revolutioniert
- Cyberangriffe erkennen und stoppen, präventiv und voraussagend

15:30 | Cyber Defense Made Easy -
Die Frischzellen-Kur für Ihre Angriffserkennung.
presented by SecureLink

- Wir zeigen Ihnen wie Sie trotz veränderter Bedrohungssituation relaxed bleiben.
- SIEM-Fit-Kurs, Netzwerkverhaltenskur oder Intelligence-Massage – Mit dem Threat Detection Framework zeigen wir, welche Anwendungen den CISO entspannen.

16:30 | Cyber Defense with Ease – Ask your Data and mature.
presented by Splunk

Wie kann ich Maschinendaten für meine Verteidigung nutzen – schneller bei Angriffen reagieren und dabei weniger Spezialisten einsetzen?

- Ein Zuhause für alle Datenarten und Datenmengen
- Einsichten und Konsequenzen (SE)
- Das Wichtige zuerst. Das ganze Bild (ES/PCI/UBA)
- Und jetzt noch einfacher (Phantom/VictorOps)

Track 3 - Workshops

10:30 | KI-Roundtable
hosted by SecureLink

- Künstliche Intelligenz, Machine Learning und Deep Learning sind brandaktuelle Themen, die zunehmend auch in der IT-Security Einzug halten. Doch was verbirgt sich dahinter, welche Chancen bieten sich für die IT-Security?
- Können Algorithmen und selbstlernende Systeme den Fachkräftemangel abfedern, oder benötigen wir noch mehr Spezialisten?
- Und wo Licht ist, fällt auch Schatten: welchen Einfluss hat KI auf der Seite der Angreifer? Können klassische Security Architekturen neuen Bedrohungen standhalten?

13:15 | Roundtable: User Monitoring vs. Data Privacy.
hosted by Forcepoint

Der Risikofaktor Mensch:

- Überwachung der Mitarbeiter: Erlaubt?
- Welche Möglichkeiten stehen zur Verfügung?
- Thema Datenschutz
- Wie es funktioniert

15:30 | Secure Development Life Cycle and the lack of Security Expertise with Development Professionals [EN].
hosted by Zion Security

- If SDLC is the egg, and application security architects are the chicken, what should come first? There is a clear growing need of secure coding and application lifecycle management to keep critical applications secure to protect your users, customers and your business.
- Security has evolved from a nice-to-have over a must, towards a state-of-mind.
- This workshop deals with challenges of finding methods AND professionals to bring that strategy to life.

Track 4 - Workshops

10:30 | Cyber Attack Simulation. LIVE
hosted by FireEye

- They‘re inside your network – now what? If you don´t know how to manage a Cyber Attack, a crisis can become a disaster. Let’s change that.
- Join us for a Cyber Attack Simulation and find out the right way to manage events inside and outside of your company when a Cyber Attack occurs. Practical and engaging to understand threats and risks and responses.
- Build confidence in taking the right actions that will protect your company in the event of an attack.
- Gain deep understanding of the consequences of specific actions.
- Participate in a real time attack to take back control as an attendee, you will spend time with an Mandiant consultant to evaluate your organizations ability to effectively execute your cyber incident response plan through scenario gameplay.
- Recommendations are given based on real-world incident response best practices.

13:15 | Ausbildung von SOC-Experten – Made Easy!
hosted by SecureLink

- Expertenmangel? Wir kümmern uns um die Ausbildung ihrer SOC-Mitarbeiter.
- Fehlende Notfallübungen? Schicken Sie Ihre Mitarbeiter auf unser hyperrealistisches Battlefield.
- Unsicherer Umgang? Lernen Sie von erfahrenen Analysten der SecureLink CDCs.

15:30 | Demo
hosted by Demisto

- Inhalte folgen
- Inhalte folgen
- Inhalte folgen

DETECT DEFEND 19

CYBER DEFENSE made easy

DAY 2

08:00 - 09:00 Uhr: Registrierung & Weißwurstfrühstück

Zeit	Track 1 - Vorträge	Track 2 - Vorträge	Track 3 - Workshops	Track 4 - Workshops
9:00-9:45	Zurücklehnen und Testen lassen: So geht modernes Pentesting *presented by Synack*	Schönheit kommt von innen – Das Böse auch: Insider Bedrohungen *presented by Forcepoint*	From protection to prevention Made Easy! *hosted by Cylance*	Cyber Defense Made Easy – Die Frischzellenkur für Ihre Angriffserkennung *hosted by SecureLink*
10:00-10:45	Entspannter Jagd-Trip: Intelligence-Led Hunting und Augmented Cyber Defense *presented by FireEye*	Sleeping with the Enemy - Fernwartung mit gutem Gewissen *presented by genua*		
11:00-11:45	Compliance Reporting mit einem Klick: Wie einfach ERP Monitoring sein kann *presented by agileSI™*	Schwachstellen-Management Made Easy - Entspannt das Backlog bewätigen *hosted by Rapid7*	AI in Action: Security that Thinks! *hosted by Vectra Networks*	Hands-On Workshop - Angriffe und Probleme in der Infrastruktur schnell identifizieren und effektiv reagieren mit einer Next-Gen SIEM Plattform *hosted by LogRhythm*
12:00-12:45	Threat Intelligence mit Fokus *presented by Digital Shadows*	Cybersecurity- und Compliance automatisiert und aus einem Guss *presented by Varonis*		
12:45-13:45 Uhr: Lunch				
13:45-14:30	Zufriedene Maschinen: OT-Security *presented by SecureLink*	Sicherheit in Cloud-Applikationen *presented by Check Point*	Live-Hack: OWASP 1op 10 [ENG] *hosted by SecureLink*	Ausbildung von SOC-Experten – Made Easy. *hosted by SecureLink*
14:45-15:30		Movin' On Up to the Cloud: Migrating your Application Connectivity Easily and Securely *presented by algosec*		
15:30-16:00		Wrap Up		
Abreise				

Track 1 - Vorträge

09:00 | Zurücklehnen und Testen lassen: So geht modernes Pentesting.
presented by Synack

- Traditionelles Pentesting ist nicht gut genug um sich gegen immer raffiniertere Cyber-Attacken zu schützen.
- Neuer Cloud-basierter Testservice setzt große Teams ein (im Durchschnitt 30-50) von internationalen hochkarätigen Sicherheitsforschern.
- Erste schwerwiegende Schwachstellen oft gefunden innerhalb von Stunden!
- Fallstudien deutscher, schweizerischer und europäischer Kunden.

10:00 | Entspannter Jagd-Trip: Intelligence-Led-Hunting und Augmented Cyber Defense.
presented by FireEye

- Wie Intelligence und die Erfahrung aus Incident Response bei einer pro-aktiven Cyber Defense helfen und so unverzichtbar sind.
- Lernen Sie weshalb Technologie, im Sinne von ausgefeilten Algorithmen und KI, alleine nicht ausreichend und weshalb der Faktor Mensch unverzichtbar ist.

11:00 | Compliance Reporting mit einem Klick: Wie einfach ERP Monitoring sein kann.
presented by agileSI™

Anhand eines konkreten Beispiels wird der Weg von der Ausgangslage über die Ziel- und Scope-Definition bis hin zur Umsetzung einer smarten SAP® Security Strategie beim Kunden mit agileSI™ beschrieben.

- Kein SIEM im Einsatz
- SAP® nicht in Security Strategie eingebunden
- Wie erreicht man SAP® Security dennoch smart & easy?

12:00 | Threat Intelligence mit Fokus.
presented by Digital Shadows

- Das Unternehmen ist längst in der Cloud, die KI-Systeme berechnen fleißig die Zukunft und im IoT ist vom Fertigungsband in der Fabrik bis zur Kaffeemaschine im Büro alles vernetzt.
- Wie steht es aber in Sachen IT-Sicherheit und Digitale Risiken?
- Mit jedem Schritt in Richtung digitale Transformation wächst die Angriffsfläche für Organisationen – sowohl hinsichtlich Unternehmensreputation als auch Marken- und Datenschutz. Wer digitales Neuland betritt, muss also die Cyberbedrohungslandschaft mit ihren digitalen Risiken überblicken und verstehen.
- Digitales Risikomanagement und Threat Intelligence gehören fest in die IT-Sicherheitsstrategie von Unternehmen verankert. Nur so lassen sich digitale Bedrohungen frühzeitig erkennen und erfolgreich abwehren.“

13:45 | Zufriedene Maschinen: OT-Security
presented by SecureLink

- Welche technischen Lösungen gibt es heute zur Absicherung von Produktionsanlagen und wie können diese eingesetzt werden?
- Dazu werden die Ansätze der Hersteller, aktuelle Gegebenheiten im OT-Umfeld und etwaige Fallstricke erläutert und betrachtet.

Track 2 - Vorträge

09:00 | Schönheit kommt von innen – Das Böse auch: Insider Bedrohungen.
presented by Forcepoint

Denn Firewalls werden durchbrochen, 0-Day Malware modifiziertsich selbst, die eigenen Mitarbeiter arbeiten irgendwo in der Cloud, externe Personen brauchen Zugang zum Unternehmensnetz.

Was früher innerhalb der Mauern war ist heute draußen in der Cloud, wer draußen war muss zur Prozessoptimierung rein gelassen werden. Last but not least, eine der größten Schwachstellen in jedem IT Sicherheitskonzept ist obendrein noch: Der Mensch. Die Lösung: Der Mensch.

Forcepoint’s Human Centric Security approach steht für einen Strategiewandel in der Cyber Defense. Denn in einer Gegenwart praktisch ohne Perimeter, wirkt der klassische Security Ansatz „welcher Content ist gut und welcher ist böse“ immer weniger.

Die Menge an Daten wächst unaufhörlich, sie ohne Kontext in zwei Gruppen zu unterteilen ist vielfach unmöglich und klare Grenzen, an denen überhaupt sinnvoll kontrolliert werden kann, verschwinden im Cloud Zeitalter immer mehr. Risiko-Szenarien, die im Inneren eines Unternehmens entstehen, hinter der Defense, sind nur sehr schwer zu identifizieren. Getreu dem Motto, wer erst mal drin ist, kann machen was er will.

Deshalb geht es bei der Technologie von Forcepoint um die Gewährleistung sicheren Verhaltens. Human Centric Security ist die effektivste Kombination aus UEBA (User Entity & Behaviour Analytics) und dynamischen DLP (Data Leackage Prevention) Regelwerken, zum Schutz von Geschäftsprozessen und Daten.

Hierdurch sind Innovationen schneller nutzbar und Security bremst nicht mehr, weil die Art der verwendeten Daten und das Verhalten des Benutzers über die Aktivierung von Defense-Mechanismen automatisch entscheiden. „Free the good and stop the bad."

10:00 | Sleeping with the Enemy – Fernwartung mit gutem Gewissen.

presented by genua

- Schnelligkeit und Effizienz sind Begriffe, die nicht erst seit der Revolution der Industrie 4.0 große Bedeutung erlangt haben. Der Stillstand von Maschinenanlagen kann schnell ins Geld gehen und das Thema Wartung wird nicht nur wichtiger, sondern auch komplexer.
- Fernwartung - regelmäßig und durch Experten - hat sich hier als effektive Lösung etabliert. Doch aus Sicht der IT Security können derlei Maßnahmen schnell zum Albtraum werden. Damit das nicht passiert, bietet genua hochsichere, flexible und leicht zu bedienende Fernwartungslösungen, damit Verantwortliche sich mit einem guten Gewissen zurück lehnen können.

11:00 | Entspannt das Backlog bewältigen – mit weniger Ressourcen.

presented by Rapid7

Bei jedem Scan identifizieren Sie mehr und mehr Risiken, die Ihrer Aufmerksamkeit bedürfen? Ihre To-Do-Liste wächst stetig, aber eine saubere Priorisierung der Aufgaben kostet Zeit, die Sie eigentlich nicht haben?

Wenn Ihnen dieses Szenario bekannt vorkommt, lassen Sie uns darüber reden. Wir zeigen Ihnen, wie Sie die Situation verbessern können:

- Effiziente Zusammenarbeit zwischen Security-, IT- und Development-Teams bei der Beseitigung von Schwachstellen.
- Ausgleichende Maßnahmen, wenn sich Schwachstellen mal nicht sofort beseitigen lassen.
- Wie mit Automatisierung die Zusammenarbeit vereinfacht und den Patching-Prozess beschleunigt.
- Strategisches Vorgehen bei Ihrem Schwachstellen-Management-Programm

12:00 | Cybersecurity- und Compliance automatisiert und aus einem Guss.

presented by Varonis

- Es ist heute wichtiger denn je, dass IT-Probleme als existenzielle Bedrohungen für das Business schnell gelöst werden. Wichtig sind hier zuverlässige Warnsysteme, aber auch die Forensik wird immer umfangreicher, je sensibler die gespeicherten Daten werden.
- Compliance und Regelungen wie HIPPA, PCI oder die DSGVO können heute immer stärker in automatisierter Weise gesichert werden: Mit Software-Lösungen die das Risiko von internen und externen Bedrohungen automatisiert reduzieren und Compliance (automatisch) gewährleisten.

13:45 | Sicherheit in Cloud-Applikationen.

presented by Check Point

- Die Sicherheitslösung für die Prävention von Cyber-Attacken und Identitätsdiebstahl auf SaaS Anwendungen wie Office365, Gmail, Dropbox, Salesforce.com.

14:45 | Movin' On Up to the Cloud: Migrating your Application Connectivity Easily and Securely.

presented by algosec

- Migrating applications to the cloud or to another data center is a complex and risky process. You need to understand the applications you are currently running and later define and map the existing application connectivity flows.
- If done manually, the process becomes time-consuming and prone to errors. A single mistake could, potentially, cause outages, compliance violations and security gaps.
- In this presentation we will explore how to simplify and accelerate large-scale complex application migrations while sustaining full security.

Track 3 - Workshops

09:00 | From protection to prevention Made Easy!
hosted by Cylance

- Lernen Sie in diesem Workshop wie Sie mit CylancePROTECT und CylanceOPTICS die Integrität Ihrer Endpoints wirklich schützen – powered by ML.
- Vorstellung der Funktionalitäten der jeweiligen Produkte
- reale Malwareangriffe, maliziöse E-Mail Anhänge und wirkliches Angreiferverhalten live erleben
- Wirkliche Best Practices vs. Benchmark Konfigurationen

11:00 | AI in Action: Security that Thinks! [ENG]
hosted by Vectra Networks

Using a live system, we'll work through some common uses of the Cognito AI platform and how to use it detect attackers in real time and perform conclusive incident investigations.

- Cognito Detect
- Initial detections, prioritising high risk attacks, gaining contextual understanding
- Identifying attack campaigns multiple hosts
- Triage, Notifications, Reporting
- Deployment considerations
- Cognito Recall
- Threat hunting
- Historical forensic investigations
- Integration with Cognito Detect
- No PowerPoint, all demos!

13:45 | Live-Hack: OWASP 1op 10 [ENG]
hosted by SecureLink

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain secure web applications. They release a top 10 of the most seen web application vulnerabilities based on inputs from security professionals all over the world. We developed a vulnerable web application for this workshop to demonstrate how we identify and exploit each listed vulnerability, so that you have a better understanding on:

- What is the vulnerability?
- How complex is its exploitation?
- What is the potential impact behind it?

The web application will be available to you so that you can test and play with the different vulnerabilities and exploits.

Track 4 - Workshops

09:00 | Cyber Defense Made Easy – Die Frischzellenkur für Ihre Angriffserkennung.
hosted by SecureLink

- Wir zeigen Ihnen wie Sie trotz veränderter Bedrohungssituation relaxed bleiben.
- SIEM-Fit-Kurs, Netzwerkverhaltenskur oder Intelligence-Massage – Mit dem Threat Detection Framework zeigen wir welche Anwendungen den CISO entspannen.

11:00 | Hands-On Workshop – Angriffe und Probleme in der Infrastruktur schnell identifizieren und effektiv reagieren mit einer Next-Gen SIEM Plattform.
hosted by LogRhythm

- Der Workshop ist für alle Anwender und Entscheidungsträger gedacht, die sich aktuell mit den Themen Log Management, SIEM, UEBA, DSGVO, ISMS Monitoring, sowie Security Automation und Orchestrierung beschäftigen.
- Sie lernen ein Reifegrad-Modell kennen, welches es Ihnen ermöglicht, ihre aktuellen Möglichkeiten der Detektion und Reaktion zu bewerten. Auch hilft es bei der Auswahl der nächsten sinnvollen Schritte, um Ihre aktuelle Situation zu verbessern.
- Im praktischen Hands-on Teil setzen Sie dieses theoretische Wissen anhand ausgewählter Use Cases mit einem sechsstufigen Best Practice Leitfaden, dem sogenannten Threat Lifecycle Management um.

13:45 | Ausbildung von SOC-Experten – Made Easy.
hosted by SecureLink

- Expertenmangel? Wir kümmern uns um die Ausbildung ihrer SOC-Mitarbeiter.
- Fehlende Notfallübungen? Schicken Sie Ihre Mitarbeiter auf unser hyperrealistisches Battlefield.
- Unsicherer Umgang? Lernen Sie von erfahrenen Analysten der SecureLink CDCs.

KEYNOTE:
Markus Hofmann

Denkartist bei der Detect & Defend

Massage für die grauen Zellen: Damit Sie uns in guter Erinnerung behalten, haben wir diesmal einen der inspirierendsten und effektivsten Gedächtnistrainer Europas eingeladen.

Sein Versprechen: Der Weg zu mentaler Fitness ist eine leichte Übung für uns alle.

Auf anregende Weise vermittelt er Lern- und Merktechniken, die jeder sofort für sich umsetzen kann.

LOCATION:
Anfahrt, Hotel

Veranstaltungsforum Fürstenfeld (bei München)
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.

Areise mit dem PKW:
A 96 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.

Hotelempfehlungen:

Fürstenfelder Hotel
In unmittelbarer Nachbarschaft bietet das Fürstenfelder Hotel 98 Nichtraucherzimmer mit Klimaanlage, Minibar, VoIP-Telefon, Safe, Internetanschluss und Flatscreen-TV. Bio-Frühstücks-Büffet, W-LAN und Parkplätze sind im Zimmerpreis enthalten.

Preis: ca. 115€ das Einzelzimmer ‚Standard' / Nacht inkl. Frühstück, Parkplatz, Internetzugang, Zugang zu Fitnessraum und Sauna.

Adresse: Mühlanger 5, 82256 Fürstenfeldbruck

Romantik Hotel zur Post
Liebevoll eingerichtete Nichtraucher-Zimmer im Biedermeierstil, gutes Restaurant, idyllischer Innenhof, Lift, Parkplätze, Lärmstoppfenster, u.v.m.

Preis: ca. 105€ das Zimmer ‚Business' / Nacht; 120€ das Zimmer ‚Komfort' / Nacht; beide Zimmer inkl. Frühstück, Parkplatz und Wi-Fi.

Adresse: Hauptstraße 7, 82256 Fürstenfeldbruck

Hotel Hartmann
Gepflegtes Hotel im Zentrum von Fürstenfeldbruck mit komfortabel ausgestatteten Zimmern (Tel., TV, WLAN) und reichhaltigem Frühstück. Hauseigener großer Parkplatz, Lärmstoppfenster, schöne Lage direkt an der Amper.

Preis: ca. 90€ das Einzelzimmer / Nacht inkl. Frühstück und Parkplatz.

Adresse: Leonhardsplatz 1, 82256 Fürstenfeldbruck