Detect & Defend

Orange Cyberdefense Live

The orange side of life!

orange™

Programm

Weitere Infos und Anmeldung

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

Lösungen, keine Probleme...
Nutzen Sie also die Gelegenheit: Informieren Sie sich in zwangloser Atmosphäre über die aktuellsten IT-Security Hot Topics und tauschen Sie sich aus. Wir zeigen Ihnen, wie wir Sicherheitsprobleme lösen, und sie davor bewahren.

Erleben Sie IT-Security aus einer neuen Perspektive.
IT-Sicherheit ist ein komplexes Thema? Natürlich, aber das sollte unser Problem sein, nicht Ihres!

Zusammen mit unseren Partnern sorgen wir dafür, dass Sie sich keine Sorgen machen müssen. Wir finden, was Sie brauchen und übernehmen Lieferung & Implementierung. Und bei Bedarf kümmern wir uns auch um den Betrieb.

Inhalt

Programmübersicht Fürstenfeldbruck....4
Programmübersicht Frankfurt am Main....12
Keynotes....18
Locations & Anfahrt....20
Sponsoren....22

The orange side of life

Detect & Defend
Orange Cyberdefense Live

Tag 1

23.03.2023
Fürstenfeldbruck

08:00–09:00 Uhr: Registrierung			
09:00–09:30	**Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der Orange Cyberdefense Germany**		
09:30–10:15	**Keynote: Thomas Huber aka. ein Huberbua**		
Zeit	Stadtsaal	Säulensaal	Kleiner Saal
10:30–11:15	**Ein Tag im Leben des Brian - LIVE DEMO.** presented by Netskope	**Licht im Dunkeln - Sensible Inhalte in Dark Data aufspüren, klassifizieren und schützen.** presented by Forcepoint	**Die Angriffskette beginnt und endet bei den Menschen.** Warum eine Mitarbeiter-zentrierte Security Strategie Ihr Organisations-Risiko mindert. presented by Proofpoint
11:30–12:15	**Needle, haystack, done. Oder: Ein Plädoyer für die erste Verteidigungslinie.** presented by Splunk	**Die Magie der Deception: Angreifer sind fast immer schneller als Verteidiger.** Machen Sie Deception-Technologie zu einem Teil Ihrer IT/OT-Sicherheitsstrategie. presented by Fortinet	**Eine sichere Cloud-Infrastruktur (-as-code).** presented by Orange Cyberdefense
12:15–13:15 Uhr: Lunch			
13:15–14:00	**Alles im Gleichgewicht! Zero Trust im Einklang mit Security Operations.** presented by Palo Alto Networks	**Stay positive. Cyberkriminelle wollen Sie um jeden Preis: Ihre Identitäten und Ihre Daten. Kriegen Sie aber nicht.** presented by Thales	**The Orange Side of Converged OT & IT Security Service.** presented by Orange Cyberdefense
14:15–15:00	**M365 ist großartig: Für Kunden und Cyberkriminelle - mit Mimecast nur für Kunden.** presented by Mimecast	**AI über AI: Was ChatGPT über Attack Signal Intelligence von Vectra AI sagt.** presented by Vectra Networks	**ICS und IoT Threat Landscape.** presented by Nozomi Networks
15:00–15:30 Uhr: Tea & Networking			
15:30–16:15	**Orange Cybersecurity and beyond.** presented by Orange Cyberdefense	**Bedrohungsanalyse in Echtzeit – so bleiben Sie vor Ransomware sicher.** presented by Cybereason	
16:30–17:15	**SaaS-Daten in Salesforce, ServiceNow, M365 und Co. effektiv schützen** presented by AppOmni	**Sonnige Aussichten mit MITRE ATT&CK and D3FEND: Wo startet man bei agilen Projekten?** presented by Orange Cyberdefense	
17:15–20:00 Uhr: The orange side of life – Get together & Fingerfood			

Stadtsaal

10:30 | Ein Tag im Leben des Brian - LIVE DEMO.
presented by Netskope

Die Cloud-Transformation und die Möglichkeit von überall zu arbeiten, haben die Art und Weise verändert, wie Sicherheit umgesetzt werden muss. Netskope beobachtet und antizipiert diese Veränderungen und arbeitet mit Ihnen zusammen, um Benutzer und Daten zu schützen, unabhängig davon, wo sie sich befinden.

11:30 | Needle, haystack, done. Oder: Ein Plädoyer für die erste Verteidigungslinie.
presented by Splunk

Splunk ist nicht nur ein SIEM sondern eine Plattform, die auch in verschiedenen anderen Bereichen eingesetzt wird. Erfahren Sie mehr über Beispiele und inwiefern auch die erste Verteidigungslinie einen Nutzen von Splunk hat.

13:15 | Alles im Gleichgewicht! Zero Trust im Einklang mit Security Operations.
presented by Palo Alto Networks

Daten, Geräte, Anwender und Applikationen sind heutzutage überall verteilt und damit ein ständiges Sicherheitsrisiko für Ihr Unternehmen. Mit einem Zero Trust-Ansatz gewährleisten Sie fortlaufend kontrollierten Zugriff auf Ihr Netzwerk, ganz nach dem Prinzip “Vertraue niemanden, verifiziere jeden”. Doch damit das Konzept reibungslos funktioniert und eine optimale Nutzererfahrung gewährleistet wird, ist es erforderlich, externe Bedrohungen jederzeit effizient zu erkennen, zu analysieren und zu bewerten.

Erfahren Sie in der Session, wie Sie Gefahrenabwehr und -vorbeugung miteinander in Einklang bringen und so einen Grundstein für ein modernes sicheres Netzwerk legen.

14:15 | M365 ist großartig: Für Kunden und Cyberkriminelle - mit Mimecast nur für Kunden.
presented by Mimecast

M365 ist der de-facto-Standard für E-Mail & Collaboration. Das macht M365 zur „Most-Targeted-Plattform“. In dieser Session zeigen wir aktuelle E-Mail-Angriffsdaten aus unserem M-SOC rund um Impersonation, Phishing und schädliche Attachments.

Mimecast schützt gegen diese Angriffe ganzheitlich in allen relevanten Disziplinen: PROTECT, DETECT, RESPONSE - durch unsere Kernprodukte und durch die wirkungsvollen API-Integrationen in andere Security-Plattformen.

15:30 | Orange Cybersecurity and beyond.
presented by Orange Cyberdefense

Orange ist ein globaler Telko-, Technologie- und Cybersecurity-Anbieter, Data Spezialist und Beratungsunternehmen. In den weltweiten Angeboten nimmt Cybersecurity eine immer wichtigere Rolle ein.

Strategisch betrachtet: Wie können dadurch konkrete Mehrwerte und Nutzen erzeugt werden. Dies wollen wir an Beispielen aus der Sicht unserer Spezialisten aufzeigen.

16:30 | SaaS-Daten in Salesforce, ServiceNow, M365 und Co. effektiv schützen.
presented by AppOmni

Sicherheitsteams müssen immer komplexere, vernetzte SaaS-Umgebungen schützen. SaaS-Plattformen sind das Herz kritischer Geschäftsprozesse und verarbeiten vertrauliche Daten. Durch von Kunden selbst verursachte Fehlkonfigurationen sind diese Daten oft für jedermann über das Internet frei zugänglich. Mangelnde Transparenz und fehlende automatisierte Kontrollen stellen Sicherheitsteams vor enorme Herausforderungen. Haben interne und externe Benutzer die richtigen Zugangsrechte? Welche 3rd Party Apps sind angebunden und welche Berechtigungen haben diese? Welche Konfigurationen sind überhaupt sicherheitsrelevant, wie sollten sie korrekt konfiguriert sein und wie können sie kontinuierlich und automatisiert überwacht werden?

In dieser Session erfahren Sie mehr über:

- Die häufigsten Fehlkonfigurationen und Datenrisiken in geschäftskritischen SaaS-Anwendungen
- Die wichtigsten Komponenten eines umfassenden SaaS-Sicherheitsprogramms
- Warum mehr als 20% der Fortune-100 Unternehmen mit AppOmni diese kritische Lücke schließen

Säulensaal

10:30 | Licht im Dunkeln - Sensible Inhalte in Dark Data aufspüren, klassifizieren und schützen.
presented by Forcepoint

Wissen Sie wo sich sensible Informationen in ihrem Unternehmen befinden, wer darauf Zugriff hat und wie die Gefahrenlage genau aussieht?

Ein durchgängiger Datenschutz addressiert all diese Herausforderungen in vier Schritten: Data Discovery, KI-gestützte Datenklassifizierung, Monitoring und DLP-Schutzmaßnahmen. Erfahren Sie wie sich das alles konkret umsetzen lässt.

11:30 | Die Magie der Deception: Angreifer sind fast immer schneller als Verteidiger. Machen Sie Deception-Technologie zu einem Teil Ihrer IT/OT-Sicherheitsstrategie.
presented by Fortinet

Angriffe werden heutzutage immer schneller ausgeführt und können dies mit überraschender Intensität und Volumen tun, da Bedrohungsakteure kontinuierlich investieren und Innovationen vornehmen.

Infolgedessen beträgt die durchschnittliche Zeit, die ein Angreifer benötigt, um in ein System einzudringen und Berechtigungen zu erlangen, bei wenigen Stunden.

Gleichzeitig ist es das Ziel vieler Verteidiger, eine Verletzung innerhalb von 8-12 Stunden zu beseitigen.

Die durchschnittliche Eindämmungszeit liegt jedoch tatsächlich eher bei drei bis fünf Tagen. Und das nach der Erkennung!

Wenn Sie das übliche Katz-und-Maus-Spiel ändern möchten, hören sie in diesem Vortrag wie Deception-Technologien eingesetzt werden können, um ein endloses Labyrinth zu schaffen, das eine Maus zwingen wird, bald aufzugeben.

13:15 | Stay positive. Cyberkriminelle wollen Sie um jeden Preis: Ihre Identitäten und Ihre Daten. Kriegen Sie aber nicht.
presented by Thales

Zuerst Identitäten-Diebstahl, dann Datendiebstahl, dann Ransomware-Erpressung: das wollen Sie unter allen Umständen vermeiden. Wir zeigen wie Sie Ihr Unternehmen mit der Kombination aus Access Management und Verschlüsselung erfolgreich gegen Identitäts- und Datenraub schützen können.

14:15 | AI über AI: Was ChatGPT über Attack Signal Intelligence von Vectra AI sagt.
presented by Vectra

Attack Signal Intelligence ist die Antwort von Vectra AI auf eine bessere Abdeckung, bessere Klarheit und bessere Kontrolle von Cyberangriffen. Anstelle dem ständig wachsenden „MEHR“ auf der Anforderungsseite mit MEHR Daten, MEHR Tools, MEHR Manpower zu begegnen - liefert Vectra AI die notwendigen Daten, die besseren Detections und die richtigen Prioritäten im täglichen Kampf zur rechtzeitigen Erkennung und Verhinderung von Cyberangriffen.

Christoph Riese, Matthias Schmauch und ChatGPT (LIVE) führen durch das Programm und umreissen:

1. Was ist Attack Signal Intelligence (und befragen dazu ChatGPT)?
2. Wie passt das z.B. in eine Splunk oder Microsoft XDR Strategie?
3. Welche aktuellen Angriffe wurden bei Kunden erkannt und verhindert?

15:30 | Bedrohungsanalyse in Echtzeit – so bleiben Sie vor Ransomware sicher.
presented by Cybereason

Gerade im Bereich Cyber-Security geht es um Geschwindigkeit. Wie schnell wird ein Angriff erfasst, triagiert, isoliert und wann erfolgt eine erfolgreiche Remediation?

Cybereason bietet die Werkzeuge, um genau diese Prozesse möglichst automatisiert und in Rekordzeit durchzuführen. Durch unsere einfach zu bedienende grafische Oberfläche bieten wir Ihnen eine Lösung, um in Echtzeit alle Angriffe abzuwehren. (Ausgezeichnet von MITRE und Gartner)

Erfahren Sie in diesem Vortrag mehr über unsere einzigartige MalOp-Technologie oder eine On-Premise Installation im Zusammenhang mit der KRITIS-Verordnung.

Bleiben auch Sie “undefeated in the fight against ransomware”!

16:30 | Sonnige Aussichten mit MITRE ATT&CK and D3FEND: Wo startet man bei agilen Projekten?
presented by Orange Cyberdefense

Die MITRE ATT&CK ist eine wissensbasierte Matrix, die Unternehmen helfen soll Taktiken und Techniken potenzieller Angreifer zu verstehen. Gemeinsam mit der D3FEND spielt die MITRE ATT&CK eine wichtige Rolle für die Industrie. Viele der Sicherheitslösungen orientieren sich anhand der MITRE ATT&CK.

Doch wo soll man beginnen, wenn hunderte Techniken existieren und die Anzahl der Bedrohungen und Angreifer steigt?

Welche Techniken sind besonders wichtig und wie kann man sich schnellstmölgich schützen vor beispielsweise Phishing oder Ransomware?

Wie kann man seine Security Controls nicht nur verbessern sondern auch den Fortschritt messen? Thread Informed Defense ist dabei eine hervorragende Hilfe.

Simone Kraus zeigt Ihnen anhand einiger Beispiele, wie sie mit Hilfe der MITRE ATT&CK Ihre Systeme effizienter schützen können und wie Sie dabei schnellstmöglich Mitigationen sowie Detektionen finden können, aber auch präventiv Angriffe verhindern können.

Kleiner Saal

10:30 | Die Angriffskette beginnt und endet bei den Menschen. Warum eine Mitarbeiter-zentrierte Security Strategie Ihr Organisations-Risiko mindert.
presented by Proofpoint

Die meisten Sicherheitsbedrohungen werden durch menschliches Fehlverhalten oder Absicht ausgelöst. Angesichts dieser Bedrohungslage ist es unerlässlich, dass Unternehmen ihren Fokus auf diejenigen setzen, die am verletzlichsten sind: ihre MitarbeiterInnen und Mitarbeiter.

Proofpoint bietet seit mehr als 20 Jahren Lösungen für Unternehmen, die erkannt haben, dass die Cybersecurity Strategie Teamsport ist und nicht allein Aufgabe des CISO.

11:30 | Eine sichere Cloud Infrastructure(-as-code).
presented by Orange Cyberdefense

Betrachtet man die Agenden der aktuellen und geplanten IT-Projekte von Unternehmen, so gewinnen die Begriffe Cloud-Dienste und Cloud-Infrastruktur immer mehr an Bedeutung.

Speziell Letzteres zwingt IT-Experten dazu, sich den Konzepten der Cloud-Infrastruktur zu widmen, neue Architekturen zu entwerfen und die Bandbreite an Clouddiensten kennenzulernen. Auch in der Cloud spielt die Sicherheit der IT-Systeme eine zentrale Rolle, denn dafür ist immer noch der Nutzer verantwortlich. In diesem Vortrag zeigen wir Ihnen, wie Sie eine sichere Netzwerkarchitektur gestalten und Third-Party Next-Generation Firewalls skalierbar in ihre Umgebung einbetten können und verwenden dabei Infrastructure-as-Code, um den Provisionierungsprozess der Umgebung zu standardisieren, zu vereinfachen und zu beschleunigen.

13:15 | The Orange Side of Converged OT & IT Security Service.
presented by Orange Cyberdefense

Industrielle Unternehmen verwirklichen zunehmend mehr eine möglichst nahtlose Verbindung zwischen Operational Technology (OT) und der traditionellen Information Technology (IT). Damit kann die Produktivität und Performance gesteigert werden und durch unternehmensweite Auswertungen von unterschiedlichen Daten mehr Transparenz für Entscheidungen geschaffen werden.

Solche digitalen Prozesse bieten oft auch mehr Angriffspunkte, welche es abzusichern gilt. Ein ganzheitlicher Risiko- Minimierungsansatz beinhaltet viele einzelne Elemente, welche in einem sinnvollen Zusammenspiel heutigen Sicherheitsanforderungen entsprechen müssen.

Orange Cyberdefense zeigt in diesem Vortrag einen Lösungsansatz, wie Cybersecurity Technologien und Services erfolgreich in der Industrie harmonisieren können.

14:15 | ICS und IoT Threat Landscape.
presented by Nozomi Networks

- Die anfälligsten Branchen mit Statistiken zu vulnerablen Produkten und die am häufigsten ausgenutzten Arten von Schwachstellen - gemäß der Klassifikation der Common Weakness Enumeration (CWE).
- Hacktivisten nutzen Malware, um „nation state“-ähnliche destruktive Angriffe auf kritische Infrastrukturen zu starten.
- Exklusive Daten von Nozomi Networks zu kritischen Angriffswarnungen und gängigen Malware-Kategorien, die Unternehmen, OT und IoT betreffen.
- Erkenntnisse aus custom Honeypots darüber, wie böswillige Botnets versuchen auf das Internet der Dinge (IoT) zuzugreifen - wie z.B. Krankenhaussysteme aufgrund der Sensibilität ihrer Daten und der Abhängigkeit von kritischen Systemen für den Betrieb zunehmend ins Visier genommen.
- Empfehlungen für die in 2023 zu erwartende Bedrohungslandschaft und den zu erwartenden explosiven Anstieg an IoT Devices.

Detect & Defend

Orange Cyberdefense Live

The orange side of life

	08:00–09:00 Uhr: Registrierung	
09:00–09:30	**Eröffnung der Fachkonferenz durch Dr. Matthias Rosche, General Manager der Orange Cyberdefense Germany**	
09:30–10:15	**Keynote: Mia Landsem, Ethical Hackerin bei Orange Cyberdefense Norwegen**	
	Coffee & Tea	
Zeit	Max 1	Max 2
10:45–11:30	**The Orange Side of Converged OT & IT Security Service.** presented by Orange Cyberdefense	**Needle, haystack, done. Oder: Ein Plädoyer für die erste Verteidigungslinie.** presented by Splunk
11:45–12:30	**Ein Tag im Leben des Brian - LIVE DEMO.** presented by Netskope	**Orange Cybersecurity and beyond.** presented by Orange Cyberdefense
	12:30–13:15 Uhr: Lunch	
13:15–14:00	**AI über AI: Was ChatGPT über Attack Signal Intelligence von Vectra AI sagt.** presented by Vectra Networks	**Alles im Gleichgewicht! Zero Trust im Einklang mit Security Operations.** presented by Palo Alto Networks
14:15–15:00	**SaaS-Daten in Salesforce, ServiceNow, M365 und Co. effektiv schützen.** presented by AppOmni	**Eine sichere Cloud-Infrastruktur (-as-code).** presented by Orange Cyberdefense
	15:00-15:30 Uhr: Coffee & Tea	
15:30–16:15	**Bedrohungsanalyse in Echtzeit – so bleiben Sie vor Ransomware sicher.** presented by Cybereason	**Sonnige Aussichten mit MITRE ATT&CK and D3FEND: Wo startet man bei agilen Projekten?** presented by Orange Cyberdefense
	16:15–20:00 Uhr: The orange side of life – Get together & Fingerfood	

Tag 2

30.03.2023
Frankfurt

Max 1

10:45 | The Orange Side of Converged OT & IT Security Service.
presented by Orange Cyberdefense

Industrielle Unternehmen verwirklichen zunehmend mehr eine möglichst nahtlose Verbindung zwischen Operational Technology (OT) und der traditionellen Information Technology (IT). Damit kann die Produktivität und Performance gesteigert werden und durch unternehmensweite Auswertungen von unterschiedlichen Daten mehr Transparenz für Entscheidungen geschaffen werden.

Solche digitalen Prozesse bieten oft auch mehr Angriffspunkte, welche es abzusichern gilt. Ein ganzheitlicher Risiko- Minimierungsansatz beinhaltet viele einzelne Elemente, welche in einem sinnvollen Zusammenspiel heutigen Sicherheitsanforderungen entsprechen müssen.

Orange Cyberdefense zeigt in diesem Vortrag einen Lösungsansatz, wie Cybersecurity Technologien und Services erfolgreich in der Industrie harmonisieren können.

11:45 | Ein Tag im Leben des Brian - LIVE DEMO.
presented by Netskope

Die Cloud-Transformation und die Möglichkeit von überall zu arbeiten, haben die Art und Weise verändert, wie Sicherheit umgesetzt werden muss. Netskope beobachtet und antizipiert diese Veränderungen und arbeitet mit Ihnen zusammen, um Benutzer und Daten zu schützen, unabhängig davon, wo sie sich befinden.

13:15 | AI über AI: Was ChatGPT über Attack Signal Intelligence von Vectra AI sagt.
presented by Vectra Networks

Attack Signal Intelligence ist die Antwort von Vectra AI auf eine bessere Abdeckung, bessere Klarheit und bessere Kontrolle von Cyberangriffen. Anstelle dem ständig wachsenden „MEHR“ auf der Anforderungsseite mit MEHR Daten, MEHR Tools, MEHR Manpower zu begegnen - liefert Vectra AI die notwendigen Daten, die besseren Detections und die richtigen Prioritäten im täglichen Kampf zur rechtzeitigen Erkennung und Verhinderung von Cyberangriffen.

Christoph Riese, Matthias Schmauch und ChatGPT (LIVE) führen durch das Programm und umreissen:

1. Was ist Attack Signal Intelligence (und befragen dazu ChatGPT)?
2. Wie passt das z.B. in eine Splunk oder Microsoft XDR Strategie?
3. Welche aktuellen Angriffe wurden bei Kunden erkannt und verhindert?

14:15 | SaaS-Daten in Salesforce, ServiceNow, M365 und Co. effektiv schützen.
presented by AppOmni

Sicherheitsteams müssen immer komplexere, vernetzte SaaS-Umgebungen schützen. SaaS-Plattformen sind das Herz kritischer Geschäftsprozesse und verarbeiten vertrauliche Daten. Durch von Kunden selbst verursachte Fehlkonfigurationen sind diese Daten oft für jedermann über das Internet frei zugänglich. Mangelnde Transparenz und fehlende automatisierte Kontrollen stellen Sicherheitsteams vor enorme Herausforderungen. Haben interne und externe Benutzer die richtigen Zugangsrechte? Welche 3rd Party Apps sind angebunden und welche Berechtigungen haben diese? Welche Konfigurationen sind überhaupt sicherheitsrelevant, wie sollten sie korrekt konfiguriert sein und wie können sie kontinuierlich und automatisiert überwacht werden?

In dieser Session erfahren Sie mehr über:

- Die häufigsten Fehlkonfigurationen und Datenrisiken in geschäftskritischen SaaS-Anwendungen
- Die wichtigsten Komponenten eines umfassenden SaaS-Sicherheitsprogramms
- Warum mehr als 20% der Fortune-100 Unternehmen mit AppOmni diese kritische Lücke schließen

15:30 | Bedrohungsanalyse in Echtzeit – so bleiben Sie vor Ransomware sicher.
presented by Cybereason

Gerade im Bereich Cyber-Security geht es um Geschwindigkeit. Wie schnell wird ein Angriff erfasst, triagiert, isoliert und wann erfolgt eine erfolgreiche Remediation?

Cybereason bietet die Werkzeuge, um genau diese Prozesse möglichst automatisiert und in Rekordzeit durchzuführen. Durch unsere einfach zu bedienende grafische Oberfläche bieten wir Ihnen eine Lösung, um in Echtzeit alle Angriffe abzuwehren. (Ausgezeichnet von MITRE und Gartner)

Erfahren Sie in diesem Vortrag mehr über unsere einzigartige MalOp-Technologie oder eine On-Premise Installation im Zusammenhang mit der KRITIS-Verordnung.

Bleiben auch Sie “undefeated in the fight against ransomware”!

Max 2

10:45 | Needle, haystack, done. Oder: Ein Plädoyer für die erste Verteidigungslinie.
presented by Splunk

Splunk ist nicht nur ein SIEM sondern eine Plattform, die auch in verschiedenen anderen Bereichen eingesetzt wird. Erfahren Sie mehr über Beispiele und inwiefern auch die erste Verteidigungslinie einen Nutzen von Splunk hat.

11:45 | Orange Cybersecurity and beyond.
presented by Orange Cyberdefense

Orange ist ein globaler Telko-, Technologie- und Cybersecurity-Anbieter, Data Spezialist und Beratungsunternehmen. In den weltweiten Angeboten nimmt Cybersecurity eine immer wichtigere Rolle ein.

Strategisch betrachtet: Wie können dadurch konkrete Mehrwerte und Nutzen erzeugt werden. Dies wollen wir an Beispielen aus der Sicht unserer Spezialisten aufzeigen.

13:15 | Alles im Gleichgewicht! Zero Trust im Einklang mit Security Operations.
presented by Palo Alto Networks

Daten, Geräte, Anwender und Applikationen sind heutzutage überall verteilt und damit ein ständiges Sicherheitsrisiko für Ihr Unternehmen. Mit einem Zero Trust-Ansatz gewährleisten Sie fortlaufend kontrollierten Zugriff auf Ihr Netzwerk, ganz nach dem Prinzip “Vertraue niemanden, verifiziere jeden”. Doch damit das Konzept reibungslos funktioniert und eine optimale Nutzererfahrung gewährleistet wird, ist es erforderlich, externe Bedrohungen jederzeit effizient zu erkennen, zu analysieren und zu bewerten.

Erfahren Sie in der Session, wie Sie Gefahrenabwehr und -vorbeugung miteinander in Einklang bringen und so einen Grundstein für ein modernes sicheres Netzwerk legen.

14:15 | Eine sichere Cloud Infrastructure(-as-code).
hosted by Orange Cyberdefense

Betrachtet man die Agenden der aktuellen und geplanten IT-Projekte von Unternehmen, so gewinnen die Begriffe Cloud-Dienste und Cloud-Infrastruktur immer mehr an Bedeutung.

Speziell Letzteres zwingt IT-Experten dazu, sich den Konzepten der Cloud-Infrastruktur zu widmen, neue Architekturen zu entwerfen und die Bandbreite an Clouddiensten kennenzulernen. Auch in der Cloud spielt die Sicherheit der IT-Systeme eine zentrale Rolle, denn dafür ist immer noch der Nutzer verantwortlich. In diesem Vortrag zeigen wir Ihnen, wie Sie eine sichere Netzwerkarchitektur gestalten und Third-Party Next-Generation Firewalls skalierbar in ihre Umgebung einbetten können und verwenden dabei Infrastructure-as-Code, um den Provisionierungsprozess der Umgebung zu standardisieren, zu vereinfachen und zu beschleunigen.

15:30 | Sonnige Aussichten mit MITRE ATT&CK and D3FEND: Wo startet man bei agilen Projekten?
presented by Orange Cyberdefense

Die MITRE ATT&CK ist eine wissensbasierte Matrix, die Unternehmen helfen soll Taktiken und Techniken potenzieller Angreifer zu verstehen. Gemeinsam mit der D3FEND spielt die MITRE ATT&CK eine wichtige Rolle für die Industrie. Viele der Sicherheitslösungen orientieren sich anhand der MITRE ATT&CK.

Doch wo soll man beginnen, wenn hunderte Techniken existieren und die Anzahl der Bedrohungen und Angreifer steigt?

Welche Techniken sind besonders wichtig und wie kann man sich schnellstmölgich schützen vor beispielsweise Phishing oder Ransomware?

Wie kann man seine Security Controls nicht nur verbessern sondern auch den Fortschritt messen? Thread Informed Defense ist dabei eine hervorragende Hilfe.

Simone Kraus zeigt Ihnen anhand einiger Beispiele, wie sie mit Hilfe der MITRE ATT&CK Ihre Systeme effizienter schützen können und wie Sie dabei schnellstmöglich Mitigationen sowie Detektionen finden können, aber auch präventiv Angriffe verhindern können.

Keynotes:

Thomas Huber

Der Extrembergsteiger bei der Detect & Defend in Fürstenfeldbruck

Der Speedkletterer Thomas Huber, auch bekannt als der ältere Bruder der Huberbuam (bekannt aus Film & Fernsehen), erzählt in Fürstenfeldbruck mithilfe von faszinierenden Bildern und Filmsequenzen über Scheitern und Erfolg, über Taktik und Gefühl, über Abwarten und Durchstarten und über Werte und Ihre Umsetzung. Er zeigt mit seinen bildgewaltigen Expeditionen, dass der Schlüssel zum Erfolg die mutige Gemeinschaft ist und die Unmöglichkeit nur im eigenen Denken existiert.

Mia Landsem

Die Ethical Hackerin bei der Detect & Defend in Frankfurt am Main

Mia Landsem, Ethical Hackerin bei Orange Cyberdefense Norwegen spricht in Frankfurt über das tägliche Leben als Ethical Hackerin und erzählt wie sie in ihrer Freizeit Cyber-Opfern hilft.

Locations & Anfahrt

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.

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.

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

Getting there:

Anreise mit den öffentlichen Verkehrsmitteln:

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

Anreise mit dem PKW:

Das HOLM liegt direkt am Autobahnkreuz A5/A3, neben dem Flughafen Frankfurt. Nutzen Sie die oben angegebene Adresse für Ihr Navigationsgerät.

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

powered by:

AppOmni

NOZOMI NETWORKS

cybereason

paloalto NETWORKS

Forcepoint

proofpoint

FORTINET

splunk>

mimecast

THALES

netskope

VECTRA