Agenda

Cyber Defense Hack - Der Feind in Deinem Netzwerk

13:30 - 13:40 Uhr	**Welcome - Begrüßung** Christian Gäbel & Marcel Sievers, pco, Robert Wortmann, Trend Micro
13:40 - 14:00 Uhr	**Praxisbericht | Beleuchtung der Detection & Response und SOC Anforderungen aus Business- und Techniksicht** Christian Gäbel & Marcel Sievers, pco, Waldemar Stirtz, Polipol
	Business Slots
14:10 - 14:55 Uhr	**XDR - die neue Silver Bullet oder doch nur ein neues Buzzword?** Ist Endpoint Detection and Response (EDR) noch ausreichend oder kann ich ohne Extended Detection and Response (XDR) keine ausreichende Sicherheit mehr gewährleisten? Ab wann benötige ich eigentlich ein SIEM oder SOAR? In dieser Präsentation wollen wir verschiedene nicht produktspezifische Technologien diskutieren, Grenzen aufzeigen und unsere eigene Sicht auf die Zukunft der Erkennungs- und Reaktionstechnologien sowie damit verbundene Services darlegen. *Robert Wortmann, Trend Micro*
14:55 - 15:30 Uhr	**Kaffeepause**
15:30 - 16:30 Uhr	**Sorgenfreier Service-Betrieb durch das pco Security Operation Center (SOC)** Wo gearbeitet wird, fallen Telemetriedaten an. Wir in der IT, sollten diese Daten keinesfalls in den Speichern der Geräte versauern lassen, bis sie nach einem definierten Zeitraum einfach überschrieben werden. Mit dem pco SOC haben wir uns auf die Fahne geschrieben, diesen Daten ein Zuhause zu geben, um sie in Echtzeitanalysen zu verwerten und Bedrohungen frühzeitig zu erkennen. Die Betrachtung eines Teilbereichs ist wie ein Mensch mit einem Auge. Doch wie heißt es immer „mit dem Zweiten sieht man besser". *Dennis Grüschow & Justin Schreiner, pco*
16:30 - 17:00 Uhr	**Ransomware - Chronologie einer Katastrophe** Ransomware ist seit Jahren eine stetige Bedrohung für Unternehmen weltweit. Immer wieder werden Teile oder sogar ganze Unternehmen verschlüsselt - doch wieso richtet diese Art der Attacke immer wieder so immensen Schaden an? In diesem Vortrag werden wir eine schwerwiegende Ransomware Attacke aus dem echten Leben beleuchten. Dabei gehen wir nicht nur auf die Attacke selbst, sondern unter anderem darauf ein, was in den Jahren vor der eigentlichen Attacke geschah. Was waren in diesem konkreten Fall technische, aber auch organisatorische Versäumnisse, die dem Threat Actor die Möglichkeit boten anzugreifen? Und wie sieht eigentlich das Geschäftsmodell hinter Ransomware aus? *Robert Wortmann, Trend Micro, Marcel Sievers, pco, Waldemar Stirtz, Polipol*
	Technik Slot
14:00 - 17:00 Uhr	**Capture the Flag** Mit „Capture the Flag" präsentieren wir eine virtuelle Umgebung, die von einem Hackerangriff gestraft wurde. Das Problem: Die installierte Trend Micro Lösung zeigt Dir erste Anzeichen für einen Angriff, nun gilt es zu analysieren was genau passiert ist. Um die Challenge zu gewinnen musst Du mit Deinem Team herausfinden, wie es zu den Infektionen kam, ob weitere Clients betroffen sind und auch welche Daten verloren gegangen sind. Dein Vorteil: Der Vision One Endpoint Sensor hat alles mitgeschnitten, sodass der Angriff nachgestellt und wichtige Erkenntnisse zu weiteren infizierten Systemen daraus geschlossen werden können. *Timo Wege, Trend Micro*
ab 17:00 Uhr	**Get together** *Feierabendbier | Formel 1 Simulator | Virtual Reality*