CENTRE DE CYBER-ENTRAÎNEMENT

PROGRAMME DES CONFÉRENCES

EXTRAIT DU PROGRAMME DES CONFÉRENCES DÉJÀ VALIDÉES

IT Partners 2022

L'ÉVÉNEMENT DU CHANNEL IT, TÉLÉCOMS & AUDIOVISUEL

15 & 16 JUIN
DISNEYLAND® PARIS

JOUR 1

La réalité des cybermenaces en TPE/PME et collectivités

Fabrice Koszyk

La ville et l’entreprise sont désormais ouvertes sur le monde. Les réseaux sont interconnectés mondialement et nos données sont exposées au regard de tous. On enregistre 1 cyber-attaque toutes les 2 secondes en moyenne dans le monde. Connaître la menace c’est déjà protéger son entreprise. Comment cartographier les vulnérabilités des organisations simplement ? Quelle est la réalité terrain des attaques journalières bloquées pour les TPE/PME ? Et quelles actions correctives engager grâce à ces outils pour reprendre le contrôle de son SI ?

CEO de Serenicity

Anticiper et maîtriser la menace ransomware

François Esnol-Feugeas

La prévention des ransomwares est un défi de taille pour les PME. Pour garantir la pérennité de leur activité, celles-ci doivent choisir les bons outils pour faire face à une menace qui s'industrialise. Avec la croissance des groupes criminels et des plateformes de Ransomware as a service, les PME sont devenues la cible n°1. Les stratégies de sauvegarde suffisent-elles à parer la menace ? Comment protéger efficacement les données face aux attaques ?

CEO d'Oxibox - Président de FIRST

L'assurance cyber, nouvel incontournable pour les TPE x PME

Jules Veyrat

Les cyberattaques connaissent un niveau jamais égalé auparavant. D’un côté, les techniques d’attaques se complexifient et se diversifient, et de l’autre côté, les TPE x PME sont les plus ciblées. Combiner assurance et protection est devenu un incontournable pour lutter contre le risque n°1 en entreprise. Quelles recommandations pour vos clients en matière d'assurance cyber ? Comment les accompagner avec des outils simples et accessibles ?

CEO de Stoïk

Quel objectif de sécurité cyber se fixer pour une PME ?

Michael Monerau

Pour le dirigeant de PME, le risque cyber reste à ce jour insaisissable. La cybercriminalité explose. Les exigences des partenaires économiques ne cessent de croître. Les réponses technologiques sont nombreuses mais souvent complexes à appréhender et à mettre en place. Une question reste en suspens, comment adapter la sécurité numérique de son entreprise aux enjeux du quotidien. Nous présenterons les clés de lecture permettant au dirigeant d'arbitrer ses choix technologiques comme organisationnels afin de structurer sa cyber-sécurité sereinement.

CEO de Qontrol

Les menaces liées aux noms de domaines

Murielle Bochaton

Le nom de domaine est un actif stratégique de l’entreprise. Il conditionne l’accès aux services clés mais est exposé à de nombreux risques : phishing, attaques DDoS, compromission des données et des systèmes etc...Quelle stratégie de défense adopter ? Quelles sont les bonnes pratiques pour les TPE/PME ?

Directrice commerciale chez Nameshield

JOUR 2

Human Hacking Demo – Démonstration d’attaques contre les VIP & Key People des entreprises.

Au cours de cette session, vous assisterez à une démonstration d’attaques contre les dirigeants et personnes clefs des organisations réalisée par un Expert en Cybercriminalité. Vous découvrirez les coulisses des attaques : les méthodes à base d’OSINT et d’ingénierie sociale pour cibler, atteindre les personnes et mettre à mal toute l’entreprise. Aujourd’hui, la réussite des attaquants tient dans la facilité à trouver et exploiter les données personnelles exposées sur les réseaux sociaux et le darkweb.
A la fin de cette session, nous vous expliquons comment réussir l’intégration de la protection de l’humain dans les systèmes de cyberdéfense actuels.

Arnaud Gardin

Chief Business Development & Partnerships Officer

Fabrice Litaize

Expert en cybercriminalité

Le Bug bounty, une approche sécurité « offensive » orientée vers le résultat

Avec l’accélération de la transformation numérique, les équipes de développement produisent de plus en plus de code, de plus en plus vite, entraînant la création de plus de vulnérabilités, le tout sur des surfaces d’attaques toujours plus importantes. Les solutions du marché peinent à répondre à ce besoin de détection de vulnérabilités régulier, voir continue, qui n’est plus uniquement réservé aux entreprises de la Tech, mais qui se généralise dans les entreprises de toutes tailles et de tous secteurs d’activités. Le bug Bounty vient répondre à ce défi d’une informatique moderne. Alors qu’est-ce que le Bug bounty ? Quelle valeur le modèle apporte-t-il par rapport aux approches traditionnelles. Existe-t-il des pré-requis ou des bonnes pratiques pour se lancer ?

Lionel Pascaud

Team Leader chez Yeswehack

Comment répondre aux inquiétudes de cybersécurité de vos clients ? Devenir MSSP.

Petites ou grandes, toutes les entreprises subissent les menaces cyber. Mais toutes ne savent pas comment s'y prendre et se tournent vers leurs prestataires, fournisseurs, ou partenaires IT. Comment les aider à maîtriser la multiplication des menaces ? Quelle surveillance mettre en place en environnement PME ? Comment construire une offre de services de sécurité managés (MSSP) ?

Audrey Evon

Channel Manager, SEKOIAIO chez Sekoia

Les menaces liées aux sites et Applications Web : comment s’en protéger ?

L’exposition de l’entreprise se fait en premier lieu par le web : simple vitrine corporate ou applications métiers au coeur du business de l’entreprise, elles sont aujourd’hui la première surface d’attaque. Recrudescence des attaques web, automatisation des attaques par l’usage des robots et de l’IA, toutes les entreprises sont visées.
Comment protéger ses applications web face à ces nouvelles attaques et malgré un manque critique de ressources cyber ?

Olivier Arous

CEO d'Ogo Security