Salle Cybersécurité

9h	Ouverture et petit-déjeuner
10h	**Comment la réglementation peut-elle contribuer à améliorer le niveau de cybersécurité et à encourager la mise en place d'une stratégie de la donnée dans les entreprises ?** Par Aurélie Klein, FIDAL
	Découvrez comment la nouvelle règlementation européenne entend contribuer à améliorer le niveau de cybersécurité et à encourager la mise en place d'une stratégie de données au sein des organisations. Comment valoriser ses données, quel cadre juridique pour les données générées à partir d'objets connectés, cet atelier sera l'occasion de vous présenter ; de manière pratique, ces nouvelles obligations consistant, notamment, en un travail de documentation et de gestion des risques, grâce à des exemples concrets d'entreprises industrielles ayant adopté une approche R&D legal by design.
11h	**On a mis du Chaos 🧨 en production à Carrefour** Par François Berthault, Les Filles & les Garçons de la Tech
	Ce soir, on casse la Prod à Carrefour ! çà vous dit ? Venez observer comment on a pu organiser nos "Chaos Night" dans les équipes ! Le Chaos engineering propose de créer des dysfonctionnements dans les composants applicatifs ou les éléments d'infrastructures afin de construire un système plus robuste. Nous diminuons les impacts, évitons les incidents et gagnons en confiance dans notre écosystème.

12h	Déjeuner & networking
14h	**Quand Ansible ne suffit plus : orchestrer 236 firewalls d'une infrastructure critique chez Enedis** Par Lucas Galton, KLANIK et Henri Sourdet, ENEDIS
	Comment fait-on passer 22000 minutes en une heure ? On pourrait croire au début d'une mauvaise blague, mais c'est la question qui s'est imposée à mon arrivée chez Enedis. Plus exactement, c'est le temps qu'il aurait fallu à Ansible pour piloter l'ensemble des firewalls de notre infrastructure, dans l'implémentation faite à l'époque. Ce talk est un retour d'expérience dans le cadre de la construction d'un cloud privé (basé sur Openstack) chez Enedis : sur cette infrastructure critique, les besoins de sécurité ont conduit à l'installation de centaines de firewalls de différents constructeurs (Fortinet, Palo Alto, Checkpoint ...) au sein des datacenters du gestionnaire du réseau de distribution électrique français. L'occasion d'un aperçu sur cette infrastructure, et de revenir sur les défis qu'elle représente: comment piloter tous ces firewalls de manière performante, offrir une interface unifiée, et s'intégrer à la plateforme cloud ? Surtout, comment allier exigences de sécurité, processus de validation de l'entreprise, et déploiement "as-code" des applications ? Quand la boîte à outils classique du SRE rend les armes, nous montrerons comme ce projet d'orchestrateur sur mesure, développé en Golang, nous permet d'allier philosophie Devops et sécurité de l'entreprise dans ce contexte unique. La solution présentée a été créée spécifiquement pour les besoins d'Enedis, et ne présente pas un produit commercialisé. Le talk est un pur REX, donné conjointement avec Henri Sourdet, salarié d'Enedis et manager de l'équipe assurant le déploiement et la maintenance du cloud Openstack.

15h	**Habilite-moi si tu peux !** Par Benjamin Gakic, BPI
	Habilitations, un sujet à ne pas négliger. Les habilitations sont souvent le parent pauvre des DSI et des sociétés informatiques. Faites à la main pour les plus petites et pas forcément mieux pour les plus grandes, jamais ou mal recertifiées, les habilitations doivent suivre le scale up des entreprises et rapidement se voir outillées et automatisées. L'implication des collaborateurs dans le modèle d'habilitation et leur responsabilisation dans le cycle de vie des droits sont essentiels pour ne pas créer de failles exploitables. Nous ne nous y sommes pas forcément bien pris et nous avons eu beaucoup de mal à rattraper le coup, mais que faut-il dont ne pas négliger ? Venez découvrir les voies à ne pas suivre et celles qui nous ont permis de rattraper le coup.
16h	Pause café & goûter
16h30	**Ma vie en vente flash sur le Dark Web ?!** Par Nicolas Comet, UBISOFT
	On se sent inatteignable : on travaille dans l'IT, on a été formé à la cybersécurité. On utilise un gestionnaire de mots de passe forts et uniques, du MFA. On n'ouvre pas les pièces jointes inconnues. On sait reconnaître à dix kilomètres ces faux mails de promos, de colis non livrés. Bref, on ne risque pas grand chose. Puis, un jour, la veille d'un week-end de pont, on reçoit un petit message de la sécurité de son entreprise : « Hey, l'intégralité de tes mots de passe pros et persos sont en vente sur le Dark Web, il faut agir, vite. » « ... » 💔😰 Je vous propose de vous raconter comment j'en suis arrivé là, de la chance que j'ai eu que quelqu'un s'en rende compte. Comment j'ai réparé ça. On verra par quelles routines on peut essayer au mieux de se prémunir de ce qui m'est arrivé, quels outils aident à combattre cela, comment éviter au maximum ce moment de panique totale que je ne souhaite à personne. On abordera aussi ce qui m'a permis de limiter la casse. Qu'aucun système ni aucune personne n'est infaillible.

17h30	**L'analyse comportementale au service de la sécurité de votre production** Par Rachid Zarouali, SEVENSPHERE
	Lorsque l'on parle de sécurité, on y associe souvent une usine logicielle sécurisée, un scanner de vulnérabilité, un WAF, ... Mais tout cela n'est que la partie émergée de l'iceberg, le sujet de la sécurité est beaucoup plus vaste qu'il n'y paraît. "la CI/CD montre qu'on est secure, on a déployer en production, donc on est secure" Que se passe-t-il si une application déployée en toute sécurité le lundi, devient sensible à un CVE critique le vendredi ? Comment maintenir un niveau de sécurité optimale, sans devoir forcément passer par une nouvelle phase de déploiement (souvent en urgence)? C'est là que l'analyse comportementale vient à votre secours. mais au fait ? qu'est ce que c'est ? et surtout en quoi cela peut-il vraiment vous aider ? Je vous propose de répondre à ces questions ensemble et de découvrir comment cela peut protéger votre production de faille critique et complexe à patcher (indice: log4j / dirtypipe/ ...) et ce quelque soit l'environnement d'exécution.