< UNDERGROUND >

1er novembre

Étude de cas

AcierTech est une entreprise manufacturière basée à Laval, Québec, Canada. Fondée en 1985, elle est spécialisée dans la fabrication de pièces en acier pour diverses industries, notamment l'automobile, l'aérospatiale et la construction.

Pour répondre aux besoins de l'industrie moderne, AcierTech a décidé d'implanter des technologies de pointe et d'adopter les principes de l'industrie 4.0. L'industrie 4.0 est un concept qui vise à intégrer les technologies numériques et les systèmes cyberphysiques dans les processus de fabrication pour améliorer l'efficacité, la productivité et la flexibilité.

L'implantation de l'industrie 4.0 aura un impact significatif sur la cybersécurité d'AcierTech. La convergence des technologies de l'information (TI) et des technologies opérationnelles (TO) crée de nouvelles opportunités pour les cybercriminels d'exploiter les vulnérabilités potentielles. Les systèmes informatiques interconnectés et les appareils intelligents utilisés dans le cadre de l'industrie 4.0 peuvent être des cibles attrayantes pour les attaques malveillantes.

Sylvestre Labouteille-Dacier, le CEO de l'entreprise, désire bien comprendre les enjeux avant d'entreprendre ce projet. Par exemple, quel est l'impact au niveau de l'assurance

pour l'entreprise? Connectwise, notre partenaire sera présent pour vous discuter de Cyber assurance. Ces dernières émettent également beaucoup de prérequis pour accepter d'assurer les entreprises.

Ces prérequis incluent souvent l'hygiène des environnements informatiques, des plans de continuité des opérations, un plan de réponses aux incidents mais aussi des outils de détections évolués. NOVIPRO discutera avec vous de la construction de ces plans et de l'évaluation de votre hygiène. Darktrace vous expliquera comment l'IA aide dans la détection, la réponse aux attaques avec une visibilité optimale de votre environnement tout en intégrant les playbooks créés dans le plan de réponse aux incidents dans leur outils.

Pour découvrir comment comprendre les enjeux de la mise en place de technologies, rencontrez notre partenaire Nozomi Network, qui vous présentera des cadres de référence des environnements opérationnels et comment leur solution aide à visualiser et à adresser les vulnérabilités de ces technologies.

Notre partenaire Fortinet sera aussi présent pour parler de l'importance du respect des cadres de références TO et de son approche dans la sécurisation de ces environnements ainsi que des bénéfices de la fabrique de sécurité dans la convergence des réseaux TI et TO.

Le CEO a désigné Cornelia Humanius, Directrice des ressources humaines, comme responsable de la mise en place de la conformité sur la loi C25. Cornelia est accompagnée par NOVIPRO avec leur CISO et leur avocat pour le respect de la loi. Cependant, elle vient d'apprendre que le département TI n'a aucune capacité de dresser un inventaire des données. Data Sentinel sera présent et discutera avec vous pour relever ce défi.

Le Acera Technoplomus, le CTO de l'entreprise, veut transférer des charges de travail vers l'infonuagique pour bénéficier des services Saa, mais, tout comme la plupart des entreprises, l'environnement sera en mode hybride pour une partie des services dans ces infrastructures locales. Notre partenaire Zscaler discutera avec vous du partage des responsabilités dans la sécurisation des services cloud.

L'équipe interne TI est à son minimum et AcierTech vit la même chose que toutes les entreprises : il est difficile de trouver des employées, ce qui force le département à utiliser beaucoup de ressources externes tout comme le directeur des opérations, Scadius Profibus, mais pour des raisons différentes. En effet, les équipements industriels sont supportés et maintenus par des fournisseurs externes.

Comprenez les risques associés aux accès privilégiés de ces consultants et découvrez comment vous protéger avec notre partenaire Delinea.

De plus, AcierTech a évalué la possibilité de mettre en place une équipe dédiée à la cybersécurité chargée de surveiller en permanence les activités suspectes sur le réseau et de prendre des mesures préventives en cas de menace imminente. Discutez avec notre partenaire Arctic Wolf afin de réaliser une vraie évaluation des coûts associés et des bénéfices d'utiliser le service d'Arctic Wolf.

L’équipe travaille également en étroite collaboration avec des experts externes en cybersécurité pour bénéficier de leur expertise et rester à jour sur les dernières tendances et techniques d’attaques.

Grâce à ces mesures proactives, AcierTech réussira à minimiser les risques liés à la cybersécurité tout en bénéficiant des avantages offerts par l’industrie 4.0. L’intégration des technologies numériques dans les processus de fabrication permettra à l’entreprise d’améliorer son efficacité opérationnelle, sa productivité et sa compétitivité sur le marché mondial.

En conclusion, l’implantation de l’industrie 4.0 aura un impact significatif sur la cybersécurité d’AcierTech. L’entreprise comprend qu’elle devra prendre des mesures supplémentaires pour protéger ses systèmes et ses données sensibles contre les menaces potentielles. Cependant, grâce à une approche proactive et à une collaboration étroite avec des experts en cybersécurité, AcierTech réussira à tirer parti des avantages offerts par l’industrie, 4.0 tout en maintenant un niveau élevé de sécurité informatique.

Veuillez noter que cette histoire est fictive et ne fait référence à aucune entreprise réelle. Elle est destinée à illustrer l’impact potentiel de l’industrie 4.0 et de la convergence des TI et TO sur la cybersécurité dans le secteur manufacturier.