Expertise en cybersécurité

devUp

Expertise en cybersécurité

Groupe M2I

Table des matières

Préambule

DevUP est une société experte dans en sécurité de l’information, spécialisée dans l’audit des systèmes d’information, la sûreté des applications, le test d’intrusion et la réponse à incident. Notre équipe a pour valeur de viser l’excellence dans l’expertise technique et fonctionnelle des domaines liés à la cybersécurité.

Une majorité de nos missions consistent à accompagner les organisations dans la mise en place d'un système de management de la sécurité de l'information (SMSI), la gestion des risques et des tests d'intrusion (pentest). La réponse à incident fait également partie de notre périmètre. Nous assistons nos clients, dans la veille cyber, mais aussi à répondre à une éventuelle cyber attaque qui aurait compromis un système d'information.

Pour rester cohérent avec les besoins du marché, DevUP participe activement au club EBIOS ou bien la formation de ses consultants pour la mise à jour des connaissances et le passage de certification.

Nos domaines d'expertise

• La gouvernance avec l'accompagnement SSI (audit et l'intégration ISO 27001), gestion des risques;
• la sécurité des applications (Appsec) et du DevOps (DevSecOps) avec l'intégration de cycle de développement sécurisé et audit de code;
• le test d'intrusion (Pentest), des infrastructures aux applications;
• réponse à incident avec la recherche de cyber attaques et la reprise d'un système d'information.

Quelques chiffres

• 30% de croissance en moyenne sur 4 ans
• 4 pôles d’expertises complémentaires afin de couvrir la sécurité des systèmes d'information
• 12 consultants sur des domaines d'expertise précis
• 5 membres au Club EBIOS
• Présent dans 3 régions. Île-de-France, Rennes et Nantes
• 3 formations attribuées aux collaborateurs de DevUP chaque année

Audit, conformité et gestion des risques

Intégrer et gérer la cybersécurité au quotidien

Les audits

Audit organisationnel

L'objectif : comparer les bonnes pratiques et exigences des normes ISO 27001, 27002 ou bien un référentiel interne. Une méthode « maison » inspirée de l'ISO 27002 et de ses mesures permet ainsi de créer une « scorecard » représentant l'état de santé du système d'information et ainsi créer un plan de remédiation.

Audit d'architecture et des configurations

Le but, évaluer les infrastructures de l'organisation avec une analyse des écarts basée sur les bonnes pratiques et recommandations ANSSI et CIS. Cette méthode se couple parfaitement avec la phase organisationnelle présentée ci-dessus et permet une recherche plus approfondie des défauts de sécurité sur le SI.

Audit des applications

Cet audit permet d'évaluer les bonnes pratiques en matière de développement et de code. Une revue de l'ensemble est mise en place afin d'élaborer un diagnostic précis du niveau de sécurité des applications WEB, MOBILE.

La conformité

Nous accompagnons également les organisations dans la mise en conformité de leur système d'informations en cybersécurité. Ceci se traduit par l'intégration et le suivi de la norme ISO 27001 ou d'autres réfentiels métiers. L'objectif est d'apporter notre expertise sur les sujets fonctionnels et techniques de la cybersécurité. Ces missions peuvent se dérouler sous forme de régie (plusieurs jours par mois) ou bien sur un nombre de jours prédéfinis.

Gestion des risques

La gestion des risques est un item de la cybersécurité incontournable. Il a pour objet de prévoir ce qui pourrait arriver de pire pour une organisation et d'intégrer les mesures adéquates. L'idée est d'avoir un bon équilibre en objectifs de sécurité et budgets. Nous pratiquons les méthodes EBIOS 2020 et EBIOS Risk Manager.

Sécurité des applications

75% des vulnérabilités sont applicatives

Cycle de développement sécurisé

Pour la sécurité des applications et l'intégration continue (DevOps), DevUP propose la mise en place d'un cycle de développement sécurisé (S-SDLC) dont l'objectif est d'introduire la sécurité au sein du processus de développement. Par la suite, nos consultants procèdent à l'élaboration de modèle de maturité afin de rester dans un processus d'amélioration continue idéal pour un pipeline DevOps. Un suivi en régie ou un accompagnement des managers en sécurité de l'information est possible pour la prise en main du S-SDLC. Pour nous épauler, nous utilisons des frameworks tels que BSIMM, OPENSAMM et SDL de chez Microsoft.

Formations des développeurs

Une des premières briques pour la sécurisation des applications est la formation, sensibilisation des développeurs. En effet, le monde de la cybersécurité étant très complexe, certaines bonnes pratiques sont à rappeler et parfois à apprendre. Les formations DevUP font un état de l'art de chaque couche de la sécurité applicative. Le code, l'administration système et la gouvernance sont étudiés avec une focale "Appsec".

Les chiffres

Les "hackers" peuvent attaquer les utilisateurs dans 9 applications Web sur 10. Les attaques incluent la redirection d'utilisateurs vers une ressource contrôlée par des pirates, le vol d'informations d'identification lors d'attaques de phishing et l'infection d'ordinateurs par des logiciels malveillants. (Source OWASP)

Durant l'année 2018, en moyenne, chaque application contenait 22 vulnérabilités, dont 4 de gravité élevée. (Source PTsecurity)

Une vulnérabilité sur cinq a une gravité élevée. (SourceOWASP)

Test d'intrusion

Mettre à l'épreuve son SI ou ses applications

Notre méthode

Il est conseillé de faire un test d'intrusion chaque année pour tout système d'informations ou applications contenant des informations sensibles. Cet exercice est indispensable pour minimiser l'impact des cybers attaques en localisant les différentes vulnérabilités d'un système avant les cybercriminels. Pour ce faire, nous utilisons des méthodes maison dérivées du "Testing guide OWASP" et PTES (Penetration Testing Execution Standard).

Afin de garder une approche transverse de la cybersécurité, nous mettons un point d'honneur à ajouter une vision risque aux résultats de nos tests d'intrusion, en mélangent gravité et vraisemblance technique à métier. Le processus est le suivant :

- Un questionnaire de pré-enagement est envoyé au commanditaire. Les réponses vont apporter aux collaborateurs de DevUP, l'ensemble des commodités pour la mission ainsi que la valeur métier du périmètre du test d'intrusion;
- nos collaborateurs envoient un contrat d'engagement au commanditaire, celui-ci le retourne signée;
- le test d'intrusion s'effectue suivant les règles fixées par commanditaire;
- un rapport regroupant l'ensemble des informations sur le déroulement de la mission, la gravité technique et métiers du test d'intrusion ainsi que les recommandations à apporter;
- une restitution est effectuée par notre équipe. Généralement dans les locaux du client.

Réponse à incident

Rétablir son système d'information

Notre méthode

Dans le cas où la sécurité d'un système ou d’une application a été compromise, une réponse aux incidents est alors nécessaire. Il arrive parfois que celles-ci soient affectées et nécessite l'intervention d'un spécialiste en investigation numérique.
DevUP vous accompagne dans la réponse à incident sur les systèmes et LAMP (Linux Apache Mysql PHP) afin de contenir la menace et
rétablir les applications et infrastrustures. Voici un exemple d’intervention afin d’éradiquer la menace sur un système d’information :

- Intervention d’urgence : analyse des périphériques suspects, analyse de malwares, reverse engineering et déchiffrement de tout élément lié à l’attaque;
- application de contre-mesures d’effacement indolore pour le SI : Takedown d’url de phishing, création de signatures de malwares, etc
- restauration des fichiers effacés, analyse du trafic réseau et des journaux d'événements.

La formation

Formez vos équipes à la cybersécurité

L'ESD Cybersecurity Academy

La formation de l'ensemble des collaborateurs en cybersécurité n'est plus une option mais obligation en cybersécurité. À titre d'exemple, si vous suivez la norme ISO 27001, un plan de formation est exigé chaque année.
Afin de répondre à ce besoin, nous avons créé l'ESD Cybersecurity Academy dont l'objectif est d'apporter des formations "prenium" en sécurité de l'information. Entre 500 et 700 stagiaires sortent d'une formation ESD Cybersecurity Academy chaque année, ce qui nous permet d'avoir un fort retour d'expérience et d'améliorer en continue nos formations.

Des formations sur le test d'intrusion, de la cyberdéfense ou bien de la gouvernance. Notre catalogue reste transverse à la cybersécurité tout comme notre vision. N'hésitez pas à nous décrire vos besoins, notre équipe ESD reviendra vers vous très rapidement.

Nos références

ils nous font confiance

Volkswagen France

CONSEIL D'ÉTAT

CLUBEBIOS

m2i Formation

AgroParisTech
INSTITUT DES SCIENCES ET INDUSTRIES DU VIVANT ET DE L'ENVIRONNEMENT
PARIS INSTITUTE OF TECHNOLOGY FOR LIFE, FOOD AND ENVIRONMENTAL SCIENCES

T&T CONSULTING
Trust in technology

Visiomed

ADENTS

SQLI DIGITAL EXPERIENCE

Nous contacter

Réseaux sociaux, téléphone, emails

Coordonnées

DevUP SAS
10 rue de Penthièvre
75008 - PARIS
FRANCE
SIRET n° 808 009 864

Téléphone : 08 05 62 60 00
Email : contact@devup.fr

Réseaux sociaux

https:/www.facebook.com/devupforappsec/

https://twitter.com/AppsecDevup/

https://www.linkedin.com/company/devup---sofware-security-startup/