Présentation du service de Détection et de Réponse Managé (MDR)

par U.NEAT

Guillaume Guilhen : 06 87 05 25 90

guillaume@uneat.fr

uneat.fr

Qui sommes-nous?

U.NEAT est une société spécialisée des services de cybersécurité composées de professionnels expérimentés et formés chez les partenaires éditeurs

Uneat

U.NEAT - éléments clés

U.NEAT est une entreprise de services numériques dont les acteurs veillent à la sécurité de clients publics ou privés, grands groupes, ETI et PME.

2 pôles d'activités
- Managed Security Services provider
- Consulting Management de la sécurité, Sécurité applicative et des opérations

Proximité auprès des clients :
U.NEAT est présent en Ile de France, Auvergne Rhône-Alpes, et Provence Alpes Côte d'Azur afin de garantir un haut niveau de réactivité

Expertise et Qualité
Équipes composées de consultant(e)s doté(e)s de fortes expériences terrain (techniques, organisationnelles et métiers)

Responsabilité Sociale des Entreprises (RSE):
U.NEAT délègue à ses équipes une journée par mois
Cette journée est consacrée à un engagement personnel ou RSE
U.NEAT fournit un accès à 1200 associations engagées pour la Société.

Clients

DESCOURS & CABAUD

BOIRON

Casino

MINISTÈRE DE L'INTÉRIEUR

OSCARO

autodistribution

esri

MUTEX GROUPE VYV

doyen AUTO FRANCE

locam

Partenaires stratégiques

STORMSHIELD

IO SEKOIA.IO

HARFANGLAB

U.NEAT au cœur des dernières technologies de SOC

U.NEAT a établi des partenariats avec les éditeurs français de solutions EDR et XDR les plus avancés technologiquement

U.NEAT et ses partenaires sont des structures agiles constituées d'équipes fortement expérimentées en cybersécurité

U.NEAT partage avec ses partenaires des critères de qualité identiques : proximité, réactivité, adaptabilité, et service

U.NEAT forme et certifie ses consultants analystes du SOC directement chez ses partenaires

Définition du SOC

Le Security Operation Center, c’est une équipe et des applications, permettant de détecter, analyser et remédier aux cyber attaques.

Le SOC surveille et analyse l'activité sur les postes de travail, les serveurs, les réseaux, les bases de données, les applications, les sites Web et autres systèmes, à la recherche de signaux faibles ou de comportements anormaux qui pourraient être le signe d’une cyber attaque.

Définition du MSSP

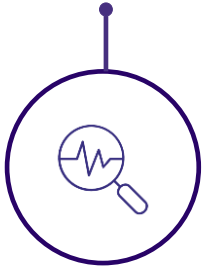
Le ‘Managed Security Services Provider’, c’est une société de services à qui des clients sous-traitent une activité de SOC.
L’intérêt de cette sous-traitance pour les clients est de disposer de compétences rares à des coûts abordables, car mutualisées entre plusieurs clients.

Uneat

Quelles sont les activités de l'équipe SOC de U.NEAT?

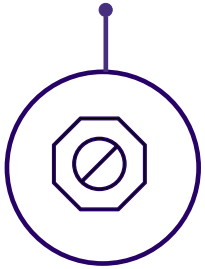
RUN DU SOC

Analyse des attaques



- Investigation
- Tri des faux positifs
- Interactions avec IT Client

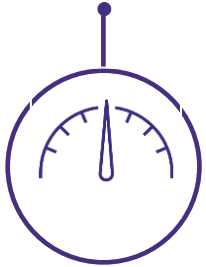
Réponse aux attaques



- Limitation délai d'intervention
- Amélioration automatisation
- Fine tuning des règles

PILOTAGE DU SOC

Mesure de la performance



- Selon KPI définis en build
- Pentesting
- Phishing

Reporting des activités

- Selon KPI définis en build
- Dashboards personnalisés
- Tests de performances

Amélioration continue

Monitoring via les agents SES et la console XDR

L’équipe des analystes de U.NEAT sont expérimentés et certifiés

RUN DU SOC

Aucun silo dans le traitement
Analyses de bout en bout par les équipes U.Neat

ERIC / DOCITE / JEAN
Analystes SOC

Parfaits compléments de Ludovic. Vous les verrez peu, mais ce sont eux qui font le job au quotidien. Quand une menace est stoppée bien en amont, c’est grâce à eux.

LUDOVIC
Analyste Référent

C’est le « costaud » dans l’équipe d’analyse et de réponse.
Des situations compliquées, il en a connues, et il aime vraiment ça !
Il est à votre écoute et il est également votre support lorsque la situation d’analyse se complique.

PILOTAGE DU SOC

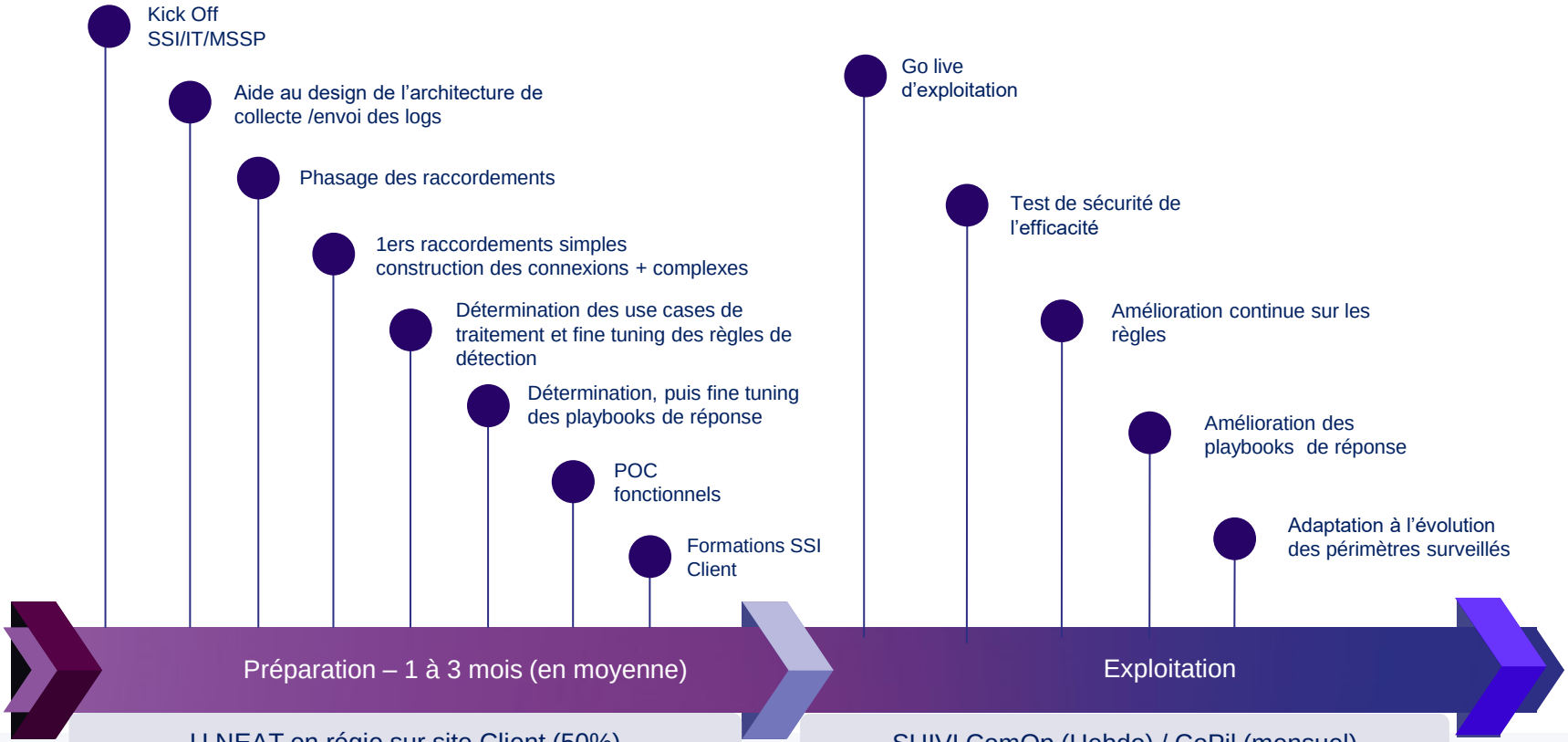
Accompagnement personnalisé
Relation de proximité

MATHIEU
SOC Manager

Il initialise votre prestation SOC dans vos locaux avec vos équipes IT et sécurité. Il teste et valide avec vous les scénarios de réponse, il reste ensuite votre contact privilégié.

Exemple de planning d'intégration et d'exploitation du SOC

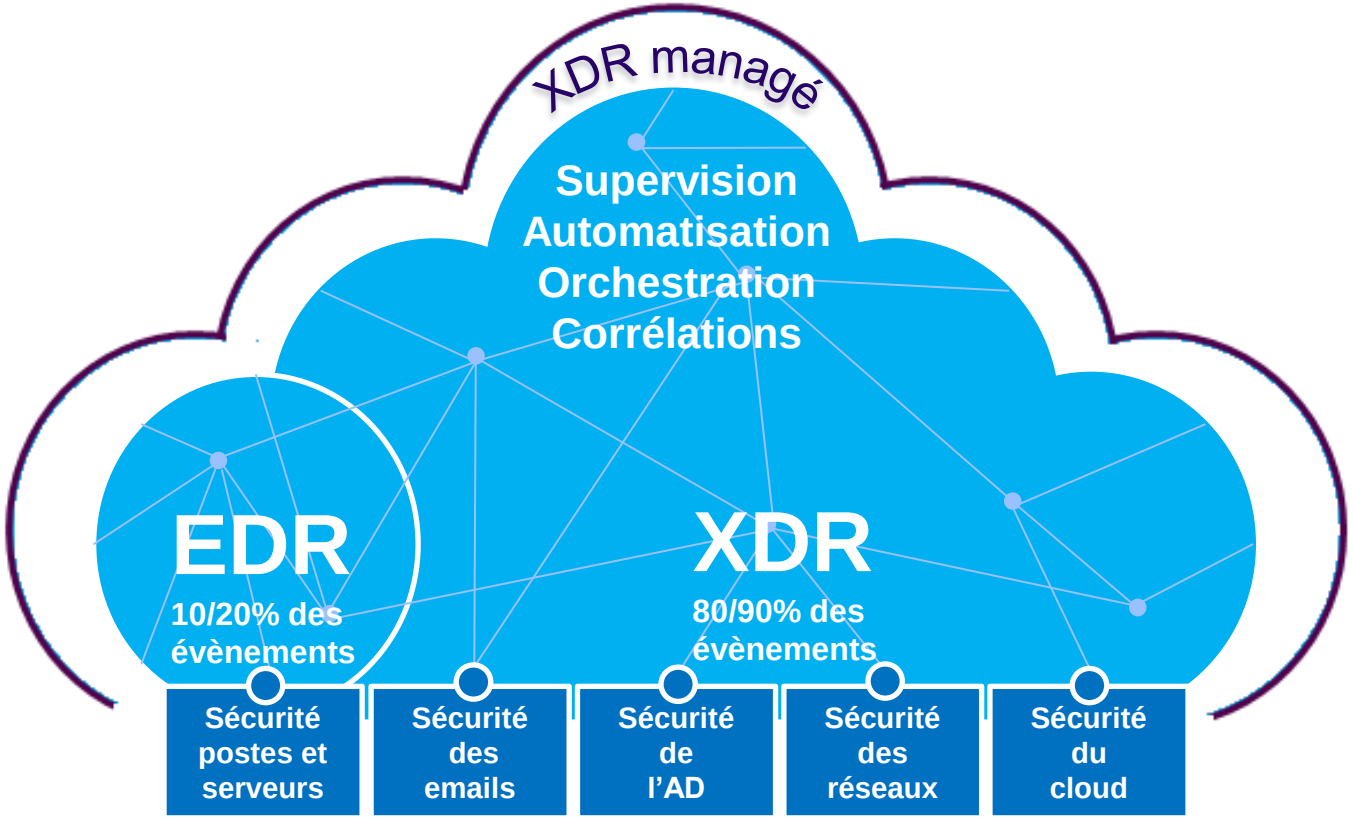
Démarrer un service de SOC managé prend en moyenne 1 à 3 mois



Outillage du SOC, la Combinaison d'un EDR et d'un XDR

Endpoint Detection & Response : EDR = agent installé sur les postes de travail et serveurs surveillant leur activité

Extended Detection & Response : XDR = application de monitoring de l'ensemble du système d'information



Offre de services de U.NEAT

Le SOC est opéré par U.NEAT, mais il est construit sur mesure pour Client avec ses équipes IT selon ses règles sécurité et son environnement technique.

Offre MSSP de U.NEAT

Management du SOC

SOC Cyber Defense Center

- Déploiement des outils et des services SOC
- Monitoring des cyberattaques sur les systèmes d'information
- Adaptation en continu aux évolutions des systèmes d'information
- Comitologie avec reportings personnalisés

Services optionnels

SOC Prepare

- Entrainement à gestion de crise
- Tests d'intrusion (Pentests)
- Campagnes de phishing

SOC Cure

- Accompagnement aux traitements post incident
- Rétablissement à une situation nominale après désastre
- SLA d'Intervention possible en 4h, même en HNO

Une offre cyber totalement souveraine

La technologie est française

Vos données sont hébergées et traitées en France

Les équipes sont françaises et localisées en France

QUESTIONS / REPONSES

U.NEAT.FR

Guillaume Guilhen
Directeur Cyber Defense Center
Guillaume@U.NEAT.fr
+33 6 87 05 25 90

16 rue Washington
75008 Paris
50 rue de la République
69002 Lyon