Pourquoi faire un Proof of Value ?

Un "Proof of Value" (POV) est une manière très simple d'évaluer et de tester la plate-forme de dernière génération Darktrace. Darktrace vous aide à considérablement renforcer votre cyber-défense. Le POV permettra de comprendre pourquoi nos clients parmi les plus grandes entreprises dans le monde comptent sur Darktrace pour détecter des menaces inconnues de façon dynamique et se défendre contre les cyber-attaques lancées de l'intérieur ou de l'extérieur de votre organisation.

Détecter des Anomalies Dont Vous Ignorez Encore l'Existence

- Darktrace Cyber Intelligence Platform (DCIP) trouvera des menaces réelles – préexistantes aussi bien qu'émergentes – qu'aucun autre outil de sécurité ne pourra détecter.
- Le moteur de détection des menaces est pour la première fois basé sur des mathématiques probabilistes de pointe appliquées au SI de votre entreprise.

Avoir Une Vue Globale

- DCIP crée une vue globale de tous vos équipements (ordinateurs, portables, etc.) et de toutes les personnes qui sont connectées à votre réseau, établissant des modèles comportementaux complexes pour chacun d'entre eux et offrant une adaptation des paramètres des modèles en temps réel.
- Vos analystes accèderont à notre interface innovante de supervision en 3D, le Threat Visualizer, leur permettant de visualiser les comportements émergents et les anomalies en temps réel.

Bénéficier des Investigations Experts

- Darktrace emploie des experts dans la cyber-sécurité qui travailleront avec vous pour analyser les résultats trouvés avec le DCIP et examiner toute activité douteuse.
- L'expérience opérationnelle de nos équipes est sans équivalent dans la cyber-sécurité.
- Nous vous présenterons des rapports hebdomadaires (*Threat Intelligence Reports*) et nous vous proposerons une formation technique complète.

Comment fonctionne un POV?

1) Nous récupérons les données

DCIP consomme du trafic réseau brut, en utilisant les moyens suivants pour le récupérer :

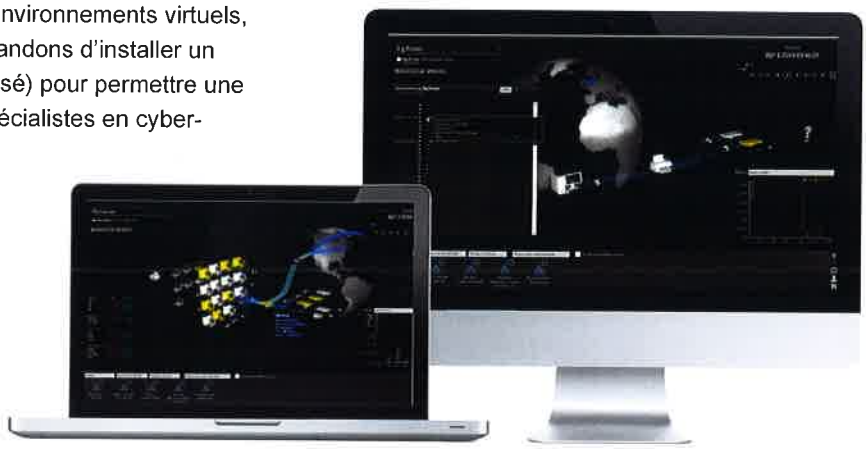
- Balayage de ports de vos équipements réseau existants
- Insertion ou réutilisation d'un 'tap' réseau
- Accès à des entrepôts de données réseau existants

2) Nous installons Darktrace

Une seule appliance Darktrace prend 2U d'espace et la durée de l'installation est d'environ 2 heures.

3) Nous analysons vos données

Darktrace ingère passivement les données du réseau. Nous n'envoyons aucunes des données à des environnements virtuels, ni à des tierces personnes. Nous recommandons d'installer un VPN (un service d'accès à distance sécurisé) pour permettre une assistance technique complète, de nos spécialistes en cyber-sécurité.



Calendrier

TEMPS	ÉTAPE	VOS RESSOURCES	RESSOURCES DARKTRACE
Avant POV	Examiner le document de planning Réunion avec le bon contact de votre équipe	Un contact technique de votre équipe de sécurité	Chargé de clientèle et ingénieur technico-commercial
Premier jour	Installation (2 heures); connexion VPN	Un contact technique de votre équipe de sécurité	Chargé de clientèle et ingénieur technico-commercial
Semaine 1	Modélisation du réseau et des comportements 'normaux' Première *Threat Intelligence Report*	Un analyste de sécurité	Un spécialiste de cyber-sécurité
Semaines 2-4	*Threat Intelligence Reports* (hebdomadaires)	Un analyste de sécurité	Un spécialiste de cyber-sécurité
Fin de POV	Evaluation du POV et discussion de la prochaine étape	Un sponsor exécutif	Un cadre supérieur

Ressources nécessaires

Avec VPN

Avec l'accès VPN, vous recevrez l'assistance technique complète de nos spécialistes en cyber-sécurité.

- Accès VPN (à distance sécurisé) à l'appliance Darktrace
- Un contact technique

Sans VPN

Sans l'accès VPN, la participation de nos spécialistes en cyber sécurité sera plus limitée

- Accès à l'appliance Darktrace par WebEx
- Un contact technique

Considérations légales et de sécurité

- Vous gardez le contrôle de vos données et de l'installation
- La récupération des données est entièrement passive
- Il n'y a pas de perturbations de l'activité du réseau et de l'entreprise
- Les données seront détruites de manière sécurisée si vous choisissez de ne pas avancer au-delà du POV
- Un accord légal sera requis pour activer l'appareil Darktrace
- Les données seront enlevées des disques à l'achèvement du POV

A propos de Darktrace

Darktrace est une des sociétés avec la plus forte croissance dans la cyber-défense, leader d'un nouveau type de solutions appelé « Entreprise Immune System ». Le socle technologique innovant est basé sur des avancées récentes dans le domaine des mathématiques probabilistes bayésiennes, développées à l'Université de Cambridge. Darktrace adresse les cyber-menaces internes et externes grâce à sa capacité unique à détecter, en temps réel, des modes d'attaques qui n'ont pas encore été cartographiés. La technologie innovante de Darktrace analyse en permanence les comportements de chaque machine, chaque individu et de l'entreprise dans sa globalité tout en s'adaptant dynamiquement à leur évolution. De nombreux groupes internationaux dans les secteurs de l'énergie, des services publics, de la finance, des télécommunications, de la distribution et des transports s'appuient sur la plateforme auto-apprenante de Darktrace pour détecter les activités anormales dans l'entreprise. Darktrace a été fondée par des spécialistes de l'apprentissage automatique renommés internationalement et des experts du renseignement. Le siège de la société est établi à Cambridge au Royaume-Uni, avec des bureaux à Paris, Londres, Milan, New York, San Francisco et Washington D.C.

T: +33 6 08 18 70 92 E: info@darktrace.fr www.darktrace.fr