Crée par :

IT-tude Smart predictive analytics

ITrust IT SECURITY SERVICES

DETECTION D'ANOMALIES – ANALYSE COMPORTEMENTALE – BIG DATA CYBERSECURITE

Les équipes d'ITrust travaillent depuis 2007 sur des systèmes intelligents capables de détecter les signaux faibles au sein des systèmes d'information pour prévenir attaques et virus inconnus.
La grande expérience de nos ingénieurs lors de missions forensiques, d'audits ou d'expertises nous a permis de modéliser un moteur comportemental permettant de lutter notamment contre les APT (Advanced persistent threat).

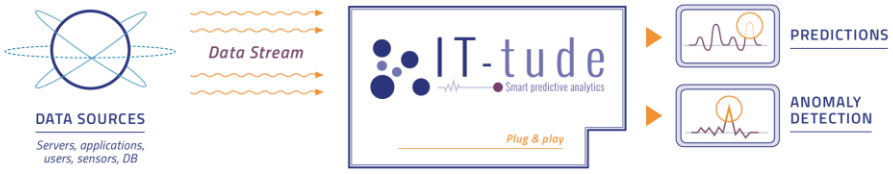
Notre équipe s'est spécialisée dans le traitement décisionnel des informations de sécurité de différentes applications, serveurs ou équipements de sécurité.
IT-tude a été développé pour fournir un système expert de détection d'anomalies basé sur des algorithmes intelligents qu'ITrust développe depuis 5 ans avec l'appui de 3 laboratoires internationaux.
Au sein d'ITrust nous développons les technologies Bigdata et Machine Learning au service des problématiques de Cybersécurité.

La détection des APT, virus et attaques inconnus comme service

L'approche d'IT-tude est de permettre aux entreprises d'atteindre un niveau de sécurité optimal tout en automatisant la détection d'un grand nombre de comportements malveillants, l'identification de signaux faibles, la perte et l'extraction de données confidentielles.
Utilisant les avantages du mode SaaS et Cloud, IT-tude combine des services performants avec un modèle de prestation sur mesure.

FONCTIONS GENERALES

IT-tude est un moteur d'analyse comportementale permettant de détecter les signaux faibles et les anomalies au sein des systèmes d'information.



3 entreprises sur 4 subissent des attaques ou piratages informatiques (source Verizon) cependant 90% sont pourtant équipées d'équipements de sécurité essentiels.
Les APT (menaces persistantes) , comportements malveillants, virus, etc outrepassent les défenses de sécurité existantes et aucun outil actuel ne permet de détecter ces attaques. Ces attaques laissent pourtant des empreintes de leur passage. Retrouver ces traces malveillantes sur une grande quantité de données et exploiter ses signaux est impossible avec les outils actuels.
IT-tude retrouve ces traces avec son système de détection d'anomalies automatisé. Il analyse en continu les comportements des systèmes d'information et recherche les signaux faibles dans la très grande quantité de données générées par les serveurs, applications, bases de données, équipements de réseaux et de sécurité. Il identifie de manière très précise les anomalies de sécurité d'une douzaine (et bien plus) de problèmes de sécurité régulièrement rencontrés.

BEST PRACTICES

*"**L'analyse comportementale** est la solution la plus plausible contre les APT"*
***Président de la NSA**, 2012*

AUTOMATISEZ LES TRAITEMENTS DE :

- **Detection d'APT**
- **Detection d'extraction de données**

Les APT sont des menaces complexes combinant souvent différents vecteurs et stratégies d'attaque, pouvant utiliser des techniques inconnues ou des failles zero-day, durant assez longtemps sans être détectées. Elles sont la plupart du temps ciblées.

Les APT et extractions de données frauduleuses ne sont actuellement pas détectées par les outils actuels. Ils constituent un nouveau paradigme en sécurité. La trop grande quantité de données à traiter et le manque de compétences d'experts capables de détecter les signaux faibles rendent caduque les outils et méthodes actuels.

RECOMPENSES

Lauréat du projet des investissements d'avenir de l'Etat Français

- Cloud v2 SVC

INVESTISSEMENTS D'AVENIR

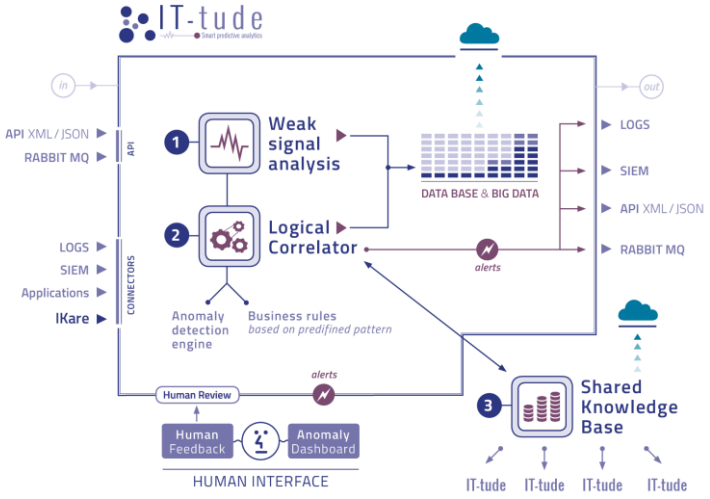
CARACTERISTIQUES

Un puissant outil de détection d'anomalies

IT-tude est un outil de sécurité nouvelle génération dont la richesse et la force résident dans l'utilisation de 3 moteurs complémentaires.
1/ Le **moteur de détection de signal faible** est issu de recherches poussées en algorithmes mathématiques.
2/ Le **moteur de corrélation métier** issu de l'expérience des ingénieurs et consultants sécurité.
3/ La **base de connaissance globale**, la mémoire d'IT-tude, qui identifie et collecte les comportements de tous les IT-tude des clients afin de faire bénéficier chacun d'eux de l'expérience des autres.

L'expertise Big Data

L'ensemble de ces 3 moteurs travaillent sur une base Bigdata externalisée (ou OnPremise) capable de traiter les grandes quantités de données.
1/ **Analyse & Apprentissage** : Statistique d'analyse, Processus d'apprentissage, Profil de sources de données
2/ **Corrélation et Intelligence** : Corrélation de l'analyse des différentes sources, Déviation de l'échantillon de données
3/ **Base de connaissance** partagée



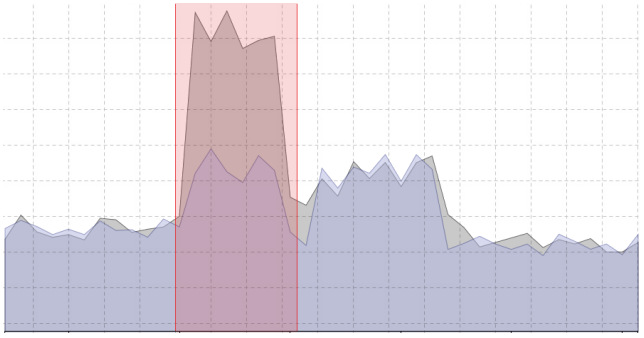
IT-tude est capable de traiter différentes données en entrées : données provenant de sources

- SIEM et Logs (connecteur SIEM),
- des messages AMQP (Rabit MQ,...)
- et des requêtes sur l'API IT-tude (JSON)

IT-tude renvoie des alertes et seuils d'anomalies (et la source de l'anomalie) par :

- logs (connecteur SIEM),
- Syslogs,
- AMQP,
- XML/JSON.

Des règles métier peuvent être implémentées et suivies dans le corrélateur métier. L'IHM permet d'afficher les corrélations, de suivre les déviances, permettant à l'utilisateur une interaction et un feedback



LA TECHNOLOGIE IT-TUDE EST UNIQUE AU MONDE.

AVANTAGES

Non-intrusif, Agentless

Son installation très simple en Saas « On Premise », adossée à un cloud privé ou public ne nécessite pas l'installation complexe d'autres modules. La technologie peut se baser sur n'importe quel outil déjà existant :
(SIEM, AD, application, BD…)
L'installation n'a aucun impact sur le fonctionnement du SI et ne nécessite pas l'installation d'agents tiers.

Moteur de dernière génération

La technologie 3D permet de détecter des anomalies (Virus, comportement, fraude, fuite, malveillance) là où aucun autre outil n'en est capable. Notamment grace à 5 algorithmes issus d'une recherche fondamentale de plusieurs années avec les plus grands laboratoires.

Plug&Play

IT-tude et son connecteur universel permettent de traiter tous types de données, de toutes les sources possibles.

Interface

L'interface ergonomique et l'utilisation en mode apprentissage permettent une installation et utilisation très simple pour les décideurs, comme pour les experts.

Capacité de détection et d'analyse

La capacité de détection d'IT-Tude permet d'augmenter la productivité et la capacité d'analyse des équipes chargées de la supervision. L'outil permet de diviser par 50 les temps d'analyse des données par les superviseurs.

Retour sur Investissement Immédiat

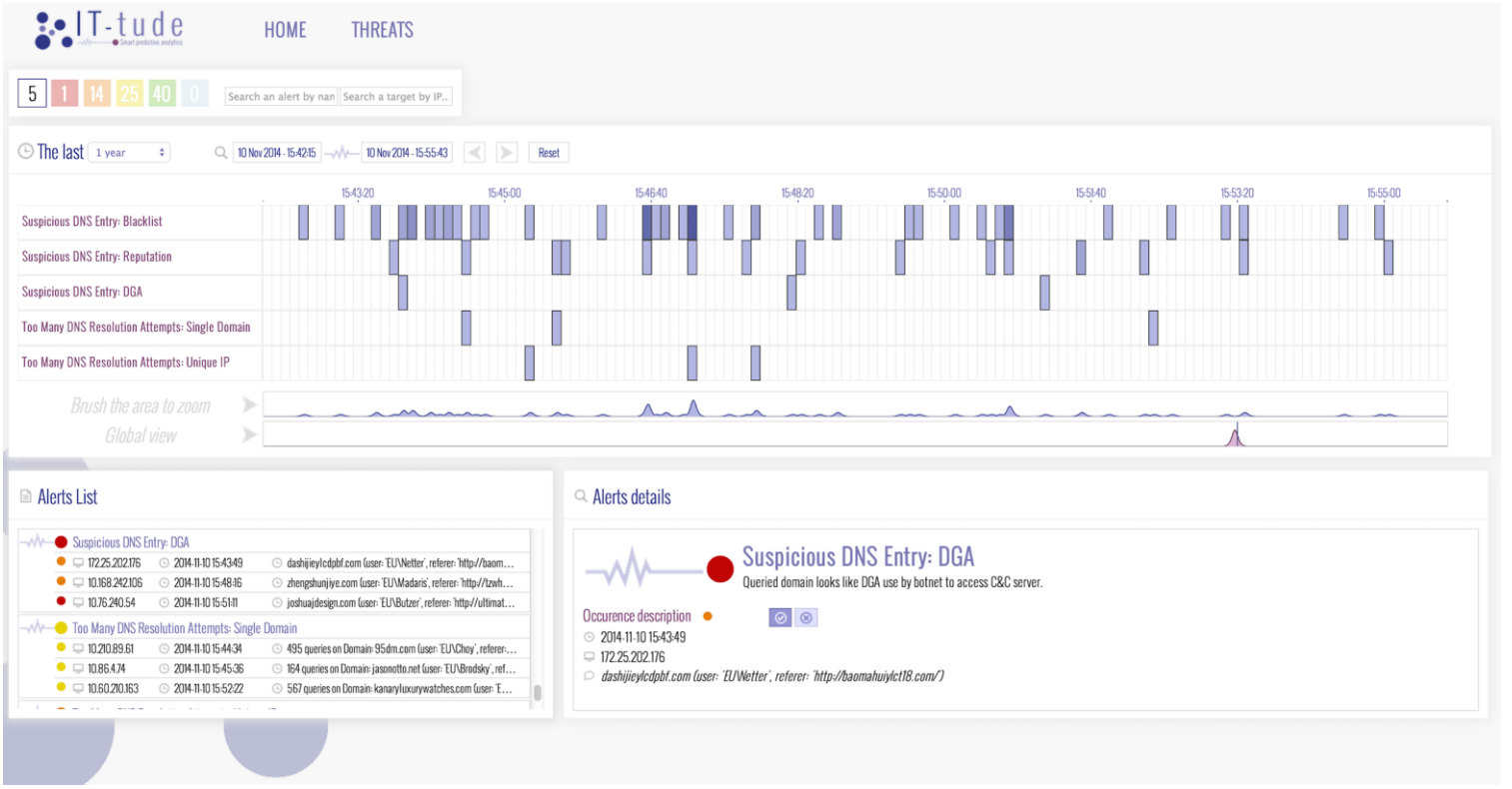
La technologie 3D (signaux faibles, corrélation métier, base de connaissance) de nouvelle génération est unique au monde, permettant notamment de diminuer par 20 les faux positifs et un temps de détection qui passe de 12 mois en moyenne à 1 semaine.

Confidentialité

La technologie n'est pas soumise au Patriot act, les données du client restent confidentielles. L'outil est développé en France et soumis à la législation européenne.

Evolutivité

IT-tude peut être complété par un module SIEM/Syslog pour les clients n'ayant pas de centralisation de données ou corrélateur de log (IT-tude standelone)



IT-tude
Smart predictive analytics

CAPACITES DE DETECTION

IT-tude est en mesure de traiter différents cas d'utilisation :

- L'analyse forensique et l'investigation (par exemple l'identification et cheminement d'une attaque)
- L'utilisation frauduleuse du SI
- Détecter une usurpation de droits
- Eviter une perte de données ou éviter l'espionnage
- Détecter des virus et attaques inconnus de type APT
- Prédire un crash, une indisponibilité de la production
- Respecter la conformité aux réglementations ou aux meilleures pratiques (SoC, BaleIII, PCI/DSS, …)
- Eviter une perte ou fraude financière
- Eviter le risque juridique
- Détecter l'attaque sur image de marque
- Maintenir le SI en conditions opérationnelles (MCO)

Plugin sur Splunk ou SIEM

Régulièrement enrichies par l'équipe R&D, le plugin facilement installable traite les signaux faibles issus d'infrastructures de supervision tels que Splunk, les SIEM ou les IAM tels que Oracle.

Standalone VM / POC

Elle s'adapte à votre structure, vos besoins et votre environnement et intègre une infrastructure de supervision de logs. Les maquettes réalisées chez le client permettent de customiser tout besoin propre à chaque client, notamment avec l'appui du centre d'expertise et Data Scientist d'ITrust.

Openstack

Remonte les anomalies propres aux infrastructures OpenStack

IT-tude peut être livré en cloud privé ou cloud public en Saas ou OnPremise

BENEFICES

- **20 fois MOINS de faux positifs**
- **Temps de détection diminué de 12 mois à 1 semaine**
- **Divise par 50 le temps consacré à la surveillance**
- **Détecte les malveillances inconnues**

Contact

Email : sales@itrust.fr
Tél : +33 (0)567.346.781
Adresse : ITrust, 55 avenue de l'Occitane
BP 67303
31670 Labège Cedex, France

www.itrust.fr
www.ikare-monitoring.com